



## **Sun Secure Global Desktop Software 4.3 Documentation Collection**

This file contains the complete documentation for Sun Secure Global Desktop Software 4.3 in PDF format. It is a simple capture of the HTML pages that make up the Secure Global Desktop documentation.

This file is unofficial and is not supported by Sun Microsystems, Inc.

Copyright © 2006 Sun Microsystems, Inc. All rights reserved.

# Sun Secure Global Desktop Software 4.3 Release Notes

These release notes contain important information about Sun Secure Global Desktop Software version 4.3, including system requirements, new features and enhancements, and known limitations and problems. Read this document before you install and use this release.

Part Number: 819-6253

---

## Revision History

Version	Description
November 2006	Additional known bugs and list of bug fixes.
October 2006	Additional known bugs and updated support for Certificate Authorities.
September 2006	First released version of release notes.
June 2006	Beta release.

---

## Contents

- [System Requirements](#)
  - [New Features in This Release](#)
  - [Changes in This Release](#)
  - [Fixes in This Release](#)
  - [End-Of-Support Statements](#)
  - [Known Bugs and Issues](#)
  - [Documentation Issues](#)
- 

## System Requirements

This section describes the system requirements for Sun Secure Global Desktop Software 4.3. It has the following sections:

- [Hardware Requirements](#)
- [Installation Platforms](#)
- [Operating System Modifications](#)
- [Web Server Requirements](#)

- Network Requirements
  - Supported Protocols
  - Security Support
  - Proxy Server Support
  - Supported Authentication Mechanisms
  - Supported Applications
  - Requirements for the Sun Secure Global Desktop Enhancement Module
  - Printing Support
  - Platform Support for the Secure Global Desktop Client
  - Platform Support for the Classic Webtop
- 

## Hardware Requirements

Use the following hardware requirements as a guide and not as an exact sizing tool. For detailed help with hardware requirements, contact a [Sun Secure Global Desktop Software sales office](#).

The requirements for a server hosting Secure Global Desktop can be calculated based on the **total** of the following:

- What is needed to install and run Secure Global Desktop.
- What is needed for each user who logs in to Secure Global Desktop on the server and runs applications.

The following are the requirements for installing and running Secure Global Desktop:

- 256MB free disk space, plus another 300MB at install time
- 256MB RAM
- 1GHz processor
- Network Interface Card (NIC)

**Note** This is *in addition to* what is required for the operating system itself and assumes the server will be used only for Secure Global Desktop.

The following are the requirements to support users who log in to Secure Global Desktop and run applications. The actual CPU and memory requirements can vary significantly depending on the applications used:

- 20MB for each user.
- On SPARC® platforms, 10MHz for each user.
- On x86 platforms, 15MHz for each user.

---

## Installation Platforms

The following are the supported installation platforms for Sun Secure Global Desktop Software 4.3:

Operating System	Supported Versions
Solaris™ Operating System (Solaris OS) on SPARC platforms	8, 9, 10
Solaris OS on x86 platforms	10
Red Hat Enterprise Linux (Intel x86 32-bit)	3, 4
Fedora Linux (Intel x86 32-bit)	Core 5
SUSE Linux Enterprise Server (Intel x86 32-bit)	9, 10

You may have to make some [operating system modifications](#).

---

## Operating System Modifications

You must make the following operating system modifications to the host **before** you install Secure Global Desktop. Without these modifications the software may not install properly or operate correctly.

### Linux Kernel 2.4+ (all distributions)

Make sure you allocate swap that is at least twice the size of physical memory. So if you have 1GB RAM, increase your swap to 2GB.

### Fedora Core 5

Secure Global Desktop will not install if the `libXp.so.6` library is not available on the host. This library was deprecated in Fedora Core 3. However the file is still available in the `libXp` package.

The `libXm.so.3` library is required to support 5250 and 3270 applications. The library is available in the `OpenMotif 2.2` package. The absence of this file no longer causes the installation to fail.

### SUSE Linux Enterprise Server 9 with Service Pack 2

Secure Global Desktop will not install if the `libgdbm.so.2` library is not available on the host. SUSE

Linux Enterprise Server 9 with Service Pack 2 contains version 3 of the library by default. You must obtain and install version 2 of the library before installing Secure Global Desktop.

## **SUSE Linux Enterprise Server 10**

Secure Global Desktop will not install if the `libgdbm.so.2` and `libexpat.so.0` libraries are not available on the host. SUSE Linux Enterprise Server 10 contains version 3 and version 1 of these libraries by default. You must obtain and install the required version of these libraries before installing Secure Global Desktop.

## **Solaris 8+ OS on SPARC Platforms**

Solaris OS comes in the following distributions: Core, End User, Development and Entire Distribution. You must install at least the End User distribution to get the necessary libraries required by Secure Global Desktop. If you do not, Secure Global Desktop will not install.

You should install the appropriate patches for your Solaris OS version. These are available from the [SunSolve Online](#).

**Note** The patches recommended by Sun Microsystems for Solaris OS may not apply to Siemens Solaris-based systems. For information about which patches to install on these systems, refer to your Siemens contact or the Siemens web site.

Secure Global Desktop requires the `/usr/lib/libsendfile.so` library. If this library is missing, Secure Global Desktop will not install. This library may be included with your SUNWcsl (Core Solaris Libraries) package or you may have to apply patch 111297-01 (available from the [SunSolve Online](#)) to get it.

## **Solaris 8 OS /dev/random Pseudo Device**

You will not be able to log in to Secure Global Desktop on Solaris 8 OS platforms if the host does not have the `/dev/random` pseudo device. You must install patch 112438-03 to obtain this device.

## **Using Solaris OS as an Application Server**

Each emulator session requires one pseudo-tty. For example, 50 users running 10 applications each on one application server requires 500 pseudo-ttys.

To set the number of pseudo-ttys, first back up your `/etc/system` file. Then edit the file and add the following line:

```
set pt_cnt=limit
```

where `limit` is the number of pseudo-ttys you require.

To create the new devices, reboot with the `-r` option.

See [SunSolve Online](#) for advice on increasing pseudo-ttys.

---

## Web Server Requirements

A web server is an essential part of a working Secure Global Desktop installation. Secure Global Desktop includes a web server, the Secure Global Desktop Web Server, that is pre-configured for use with Secure Global Desktop. The Secure Global Desktop Web Server consists of the following components:

Component	Version
Apache HTTP Server	1.3.36
mod_ssl	2.8.27
OpenSSL	0.9.8d
mod_jk	1.2.15
Apache Jakarta Tomcat	5.0.28
Apache Axis	1.2

The Secure Global Desktop Web Server is installed when you install Secure Global Desktop. However, you can use your own web server with Secure Global Desktop if you want. How you do this is described in the Secure Global Desktop Administration Guide.

---

## Network Requirements

You must configure your network for use with Secure Global Desktop:

- Hosts must have DNS entries that can be resolved by all clients.
- DNS lookups and reverse lookups for a host must always succeed.
- All client devices must use DNS.
- Client devices must be able to make TCP/IP connections to Secure Global Desktop on the following ports:
  - **3144/tcp** for standard (unencrypted) connections between client devices and Secure Global Desktop.
  - **80/tcp** for HTTP connections between client devices and the Secure Global Desktop Web Server. The port number may vary depending on the port selected on installation.
  - **443/tcp** for accessing an HTTPS web server.

- **5307/tcp** for SSL-based connections between client devices and Secure Global Desktop.
- To be able to run applications, Secure Global Desktop must be able to make TCP/IP connections to application servers. The ports you need to open depend on the types of application you are using, for example:
  - **22/tcp** for X and character applications using SSH.
  - **23/tcp** for Windows, X and character applications using telnet.
  - **3389/tcp** for Windows applications configured to use Windows Terminal Services.
  - **6010/tcp and above** for X applications

The Secure Global Desktop Administration Guide has detailed information about the ports used by Secure Global Desktop and how to use Secure Global Desktop with firewalls.

---

## Supported Protocols

Secure Global Desktop supports the following protocols:

- Microsoft Remote Desktop Protocol (RDP) version 5.2
  - Hypertext Transfer Protocol (HTTP)
  - HTTP over Secure Sockets Layer (HTTPS)
  - Secure Shell (SSH) version 2 or later
  - Citrix Independent Computing Architecture (ICA)
  - Telnet VT, American National Standards Institute (ANSI)
  - TN3270E
  - TN5250
- 

## Security Support

Secure Global Desktop supports secure connections from clients using the following protocols:

- Secure Socket Layer (SSL) version 3.0
- Transport Layer Security (TLS) version 1.0

The following encryption cipher suites are supported:

- RSA\_WITH\_AES\_256\_CBC\_SHA
- RSA\_WITH\_AES\_128\_CBC\_SHA
- RSA\_WITH\_3DES\_EDE\_CBC\_SHA
- RSA\_WITH\_RC4\_128\_SHA
- RSA\_WITH\_RC4\_128\_MD5

- RSA\_WITH\_DES\_CBC\_SHA

**Note** the Java technology client does not support any AES cipher suites.

Secure Global Desktop supports Base 64-encoded PEM-format X.509 certificates that have been signed with any of the following Certificate Authority (CA) certificates (root certificates):

- Baltimore CyberTrust Code Signing Root
- Baltimore CyberTrust Root
- Entrust.net CA
- Entrust.net Client CA 1
- Entrust.net Client CA 2
- Entrust.net Server CA 1
- Entrust.net Server CA 2
- Equifax Secure CA
- Equifax Secure eBusiness CA 1
- Equifax Secure eBusiness CA 2
- Equifax Secure Global eBusiness CA
- GeoTrust Global CA
- The Go Daddy Group, Inc. Class 2 CA
- GTE CyberTrust Root
- GTE CyberTrust Global Root
- GTE CyberTrust Root 5
- Starfield Technologies, Inc. Class 2 CA
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium CA
- Thawte Server CA
- <http://www.valicert.com>
- VeriSign Class 1 Public Primary CA - G1
- VeriSign Class 1 Public Primary CA - G2
- VeriSign Class 1 Public Primary CA - G3
- VeriSign Class 2 Public Primary CA - G1
- VeriSign Class 2 Public Primary CA - G2
- VeriSign Class 2 Public Primary CA - G3
- VeriSign Class 3 Public Primary CA - G1
- VeriSign Class 3 Public Primary CA - G2
- VeriSign Class 3 Public Primary CA - G3
- VeriSign Class 4 Public Primary CA - G2
- VeriSign Class 4 Public Primary CA - G3
- VeriSign/RSA Secure Server



Additional certificate types can be supported by installing the CA's certificate (the root certificate) for that CA.

---

## Proxy Server Support

To use Secure Global Desktop with a proxy server, the proxy server must support [tunneling](#).

For the **browser-based webtop**, you can use HTTP, Secure (SSL) or SOCKS v5 proxy servers.

For the **classic webtop**, the Java technology clients can use HTTP, Secure (SSL) or SOCKS v5 proxy servers. For the Native Clients, you can only use HTTP and SOCKS v5 proxy servers.

For SOCKS v5 proxy servers, Secure Global Desktop supports the Basic and No authentication required authentication methods. No server-side configuration is required.

---

## Supported Authentication Mechanisms

Secure Global Desktop supports the following mechanisms for authenticating users:

- Lightweight Directory Access Protocol (LDAP) version 3
- Microsoft Active Directory
- Network Information Service (NIS)
- Microsoft Windows Domains
- RSA SecurID
- Web server authentication (HTTP/HTTPS Basic Authentication), including Public Key Infrastructure (PKI) client certificates

## SecurID Authentication

Secure Global Desktop works with versions 4, 5 and 6 of the RSA ACE/Server.

SecurID authentication is not supported on Solaris OS on x86 platforms.

## Supported LDAP Directory Servers

As Secure Global Desktop supports version 3 of the standard LDAP protocol, you should be able to use the LDAP login authority and the LDAP search methods for classic web server authentication and third-party authentication with any LDAP version 3-compliant directory server. Secure Global Desktop supports this functionality on the following directory servers:

- Sun Java™ System Directory Server version 4.1+ (formerly known as Sun ONE, Netscape or iPlanet Directory Server)
- Microsoft Active Directory

Other directory servers may work, but are not supported.

The Active Directory login authority is only supported on Microsoft Active Directory.

The Directory Services Integration (sometimes known as webtop generation) functionality is supported on:

- Sun Java System Directory Server version 4.1+ (formerly known as Sun ONE, Netscape or iPlanet Directory Server)
- Microsoft Active Directory

Other directory servers may work, but are not supported.

---

## **Supported Applications**

You can use Secure Global Desktop to access the following types of applications:

- Microsoft Windows
  - Character applications running on Solaris OS, Linux, HP-UX and AIX
  - X applications running on Solaris OS, Linux, HP-UX and AIX
  - IBM mainframe and AS/400
  - Web applications (using HTML and Java technology)
- 

## **Requirements For Sun Secure Global Desktop Enhancement Module**

The Sun Secure Global Desktop Enhancement Module is software component that can be installed on an application server to provide the following additional functionality to Secure Global Desktop:

- Advanced load balancing
- Client drive mapping
- Seamless windows (from Windows application servers only)

The following are the supported installation platforms for the Enhancement Module:

Operating System	Supported Versions
Microsoft Windows	Windows Server 2003 Windows 2000 Server Microsoft Windows XP Professional
Solaris OS on SPARC platforms	8, 9, 10
Solaris OS on x86 platforms	10
Red Hat Enterprise Linux (Intel x86 32-bit)	3, 4
Fedora Linux (Intel x86 32-bit)	Core 5
SUSE Linux Enterprise Server (Intel x86 32-bit)	9, 10

On Microsoft Windows XP Professional platforms, only client drive mapping is supported. Seamless windows and advanced load balancing are not supported.

---

## Printing Support

Secure Global Desktop supports printing to PostScript, PCL and text only printers attached to the user's client device.

The Secure Global Desktop `tta_print_converter` script performs any conversion needed to format print jobs correctly for the client printer. To convert from Postscript to PCL, Ghostscript must be installed on the Secure Global Desktop server.

To support Secure Global Desktop PDF printing, Ghostscript version version 6.52 or later must installed on the Secure Global Desktop server. The Ghostscript distribution must include the `ps2pdf` program.

Secure Global Desktop supports printing with the Common Unix Printing System (CUPS). CUPS version 1.1.19 or later must be installed on the Secure Global Desktop server. Additional configuration is required.

When printing from a windows application that uses the Microsoft RDP protocol, Secure Global Desktop supports the printers supported by Windows 2000/2003. See the [Windows Printer Driver Support page](#) for details of supported printers.

---

## Platform Support for the Secure Global Desktop Client

To access Secure Global Desktop (at `http://server.example.com/sgd`), you need the Secure

Global Desktop Client and a supported web browser.

The Secure Global Desktop Client can operate in two modes:

- **Webtop mode** - the Client uses a special web page, called a webtop, to display the controls for a user's interaction with Secure Global Desktop. This is the default mode.
- **Integrated mode** - the Client displays the controls for Secure Global Desktop in the user's desktop Start Menu. Depending on other configuration factors, a web browser may only be needed for initial authentication and for determining proxy server settings.

The following table lists the supported client platforms, the supported web browsers, and the supported desktop menu systems when the Client is in integrated mode:

Supported Client Platform	Supported Web Browsers	Integrated Mode Support
Microsoft Windows XP Professional	Internet Explorer 6.0+ Netscape 6.0+ Mozilla (including Firefox) 1.4+	Microsoft Windows Start Menu
Microsoft Windows 2000 Professional	Internet Explorer 6.0+ Netscape 6.0+ Mozilla (including Firefox) 1.4+	Microsoft Windows Start Menu
Solaris 8+ OS on SPARC platforms	Netscape 6.0+ Mozilla (including Firefox) 1.4+	Sun Java Desktop System Start Menu
Solaris 10 OS on x86 platforms	Netscape 6.0+ Mozilla (including Firefox) 1.4+	Sun Java Desktop System Start Menu
Mac OS X 10.4+	Safari 2.0+	Not supported
Red Hat Enterprise Linux (Intel x86 32-bit) 3, 4	Netscape 6.0+ Mozilla (including Firefox) 1.4+	Gnome or KDE Start Menu
Fedora Linux (Intel x86 32-bit) Core 5	Netscape 6.0+ Mozilla (including Firefox) 1.4+	Gnome or KDE Start Menu
Fedora Linux (x86_64) Core 5	Netscape 6.0+ Mozilla (including Firefox) 1.4+	Gnome or KDE Start Menu

SUSE Linux Enterprise Server (Intel x86 32-bit) 8, 9	Netscape 6.0+ Mozilla (including Firefox) 1.4 +	Gnome or KDE Start Menu
Red Hat Desktop version 3.0	Netscape 6.0+ Mozilla (including Firefox) 1.4 +	Gnome or KDE Start Menu
SUSE Linux 9.1 Personal Desktop	Netscape 6.0+ Mozilla (including Firefox) 1.4 +	Gnome or KDE Start Menu

For x86\_64 platforms, only 32-bit versions of web browsers are supported.

Beta versions or preview releases of web browsers are not supported.

To support the following functionality, the web browser must have Java technology enabled:

- To automatically download and install the Secure Global Desktop Client.
- To display an application in a web browser.
- To determine proxy server settings from the user's default web browser.

The following are the supported Plug-ins for Java technology:

- Sun Java Plug-in version 1.5.0
- Sun Java Plug-in version 1.4.2

For best results, client devices must be configured for at least 256 colors.

**Serial port mapping** is only supported on Unix, Linux and Windows platforms.

## Platform Support for the Classic Webtop

To use the classic webtop (at <http://server.example.com/tarantella>) you need either the Sun Secure Global Desktop Native Client or the Java technology client running in a web browser.

The following table lists the supported client platforms and the supported web browsers and Native Clients for those platforms.

Supported Client Platform	Supported Web Browsers	Supported Native Client
---------------------------	------------------------	-------------------------

Microsoft Windows XP Professional	Internet Explorer 6.0+ Netscape 6.0+ Mozilla (including Firefox) 1.4+	Native Client for Microsoft Windows
Microsoft Windows 2000 Professional	Internet Explorer 6.0+ Netscape 6.0+ Mozilla (including Firefox) 1.4+	Native Client for Microsoft Windows
Solaris 8+ OS on SPARC platforms	Netscape 6.0+ Mozilla (including Firefox) 1.4+	Native Client for UNIX
Solaris 10 OS on x86 platforms	Netscape 6.0+ Mozilla (including Firefox) 1.4+	Native Client for UNIX
Mac OS X 10.4+		Native Client for Mac OS X
Red Hat Enterprise Linux (Intel x86 32-bit) 3, 4	Netscape 6.0+ Mozilla (including Firefox) 1.4+	Native Client for Linux
Fedora Linux (Intel x86 32-bit) Core 5	Netscape 6.0+ Mozilla (including Firefox) 1.4+	Native Client for Linux
SUSE Linux Enterprise Server (Intel x86 32-bit) 8, 9	Netscape 6.0+ Mozilla (including Firefox) 1.4+	Native Client for Linux
Red Hat Desktop version 3.0	Netscape 6.0+ Mozilla (including Firefox) 1.4+	Native Client for Linux
SUSE Linux 9.1 Personal Desktop	Netscape 6.0+ Mozilla (including Firefox) 1.4+	Native Client for Linux

Beta versions or preview releases of web browsers are not supported.

A supported web browser must have Java technology enabled. The following are the supported Plug-ins for Java technology:

- Sun Java Plug-in version 1.5.0
- Sun Java Plug-in version 1.4.2

Because of changes to security in Secure Global Desktop version 4.0, you cannot use the version 4.x

Native Clients or Java clients to connect to a version 3.x Secure Global Desktop server. You must use a version 3.x client instead.

For best results, client devices must be configured for at least 256 colors.

### Client limitations

The Native Clients and Java technology clients are no longer being actively developed, but they are still supported. Support for these client types will cease in a future release of Secure Global Desktop. The following lists the limitations of these client types:

- **Client drive mapping** is only supported by the Java technology client on Microsoft Windows client platforms.
  - **PDF printing** is only supported by the Native Client and Java technology client on Microsoft Windows client platforms.
  - **Audio** is only supported by the Native Client on Solaris OS, Linux, Mac OS X and Microsoft Windows client platforms.
  - **Seamless windows** is not supported.
  - **Smart cards** are only supported by the Native Client on Solaris OS, Linux and Microsoft Windows client platforms.
  - **Web server and third-party authentication** is not supported by the Native Client.
  - **Serial port mapping** is not supported.
- 

### New Features in This Release

The new features of Sun Secure Global Desktop Software 4.3 are:

- **Closer integration with client desktop systems**
  - [Integration with the Desktop Start Menu](#)
  - [Single Sign-on](#)
  - [Managing Client Configuration With Profiles](#)
  - [Mobile Proxy Server Configuration](#)
  - [Enhanced Command Line for the Secure Global Desktop Client](#)
  - [Manually Installable Secure Global Desktop Client](#)
- **Enhanced support for Windows, Unix and Linux applications**
  - [New X Server](#)
  - [PDF Printing for UNIX, Linux and Mac OS X Clients](#)
  - [Client Drive Mapping for UNIX and Linux Applications](#)
  - [Support for Serial Ports in Windows Applications](#)
  - [Support for the Remote Desktop on Microsoft Windows XP Professional](#)

- Support for Connections to the Console Session with Windows Server 2003 Terminal Services
  - **More Security**
    - Initial Connection Is Always Secure
    - Protecting Clients Against Unauthorized Servers
    - Controlled Copy and Paste
    - Support for SecurID for Application Server Authentication
  - **Support for Users in Different Locales**
    - Localized User Interface
    - Translated Documentation
    - Language Support in Expect Scripts
- 

## Integration with the Desktop Start Menu

The Secure Global Desktop Client can now operate in either of the following modes: Webtop mode and Integrated mode.

- **Webtop mode** - uses a web browser to display the webtop in the same way as previous releases. This is the default mode.
- **Integrated mode** - the webtop content (the links for starting applications) display in the desktop Start Menu so that users can run remote applications in the same way as local applications. Depending on how you configure Start Menu integration, there may be no need to use a web browser.

**Note** Integrated mode is the recommended mode if your organization prefers not to use Java™ technology on the client device. Integrated mode is not available for the *classic* webtop.

To use Integrated mode, the user must log in to Secure Global Desktop by clicking the Login link on their desktop Start Menu. Integrated mode is not available if you start a web browser and log in.

Working in integrated mode simplifies session management. Unlike the webtop, there are no controls for suspending and resuming applications. Instead, when the user logs out, the Client automatically suspends or ends all running emulator sessions. When the user logs in again, the Client automatically resumes all suspended sessions.

Printing is simplified too, printing is always "on" and print jobs go straight to the printer the user selected. Unlike the webtop, print jobs cannot be managed individually.

If the user needs to display a webtop, for example to resume a suspended application or manage printing, they can click the Webtop link on the Start Menu. The webtop is displayed in their default web browser.



If the user has arranged any of their webtop content to display in groups, those groups are also used in the Start Menu. If the group is configured to hide webtop content, the content does not display in the Start Menu.

To log out of Secure Global Desktop, the user clicks the Logout link on the Start Menu.

For details of which desktop systems can be used in integrated mode, see [Platform Support for the Secure Global Desktop Client](#).

---

## Single Sign-on

It is now possible to configure the Secure Global Desktop Client so that it starts automatically when a user logs in to their client device. The Client can also cache an authentication token that allows a user to start a webtop session automatically without having to log in manually. When the Client is configured in this way, users experience the benefits of a single sign-on.

Automatic login is achieved through a new authentication token login authority (ATLA). If the Client presents a valid authentication token, the user is automatically authenticated to Secure Global Desktop. To generate an authentication token, users must perform an initial log in using a web browser and then manually generate the authentication token by editing their profile. A separate token is needed for each Secure Global Desktop server the user connects to.

---

## Managing Client Configuration With Profiles

The desktop Start Menu and single sign-on features mean that the Secure Global Desktop Client requires some configuration to be able to connect to Secure Global Desktop. Not only that, different configurations may be needed in different situations, for example because the user is in the office or working at home. To be able to manage multiple Client configurations, this release introduces profiles as the method for storing a group of Client settings. Each profile allows you to configure the following:

- The URL to connect to.
- The operating mode of the Client, whether Webtop mode or Integrated mode.
- Whether automatic logins are enabled.
- Whether the Client should start automatically when the user logs in to their client device.
- Proxy server configuration, whether the settings are manually configured in the profile or determined from the web browser.
- Reconnection settings for controlling what happens when the Client loses its connection with Secure Global Desktop.
- Logging settings for controlling what information is written to the Client log file.
- The path to the PDF viewer to used for PDF printing on Solaris OS, Linux and Mac OS X clients.

Secure Global Desktop Administrators have full control over the creation of profiles. On an Administrator's webtop there is a new administration tool, Profile Editor, that allows you to create and edit profiles for organization, organizational unit (OU) and profile objects in the Tarantella System Objects organization. By defining profiles for these objects, Administrators can deploy common default Client configurations to users.

Administrators can also control whether users can create and edit their own profiles. User profile editing can be enabled array-wide, for an organization, for an OU or for individual users. By default, user profile editing is enabled. Users create and edit profiles from the Edit button on their webtop.

There is a system-wide default profile, which is configured to give users the standard webtop behavior available in previous releases. Administrators can edit this profile.

Once the Client is connected to Secure Global Desktop, the profile configured for the user is copied from the Secure Global Desktop server to the client device. If a user edits their profile, the changes are stored only on the client device.

---

## Mobile Proxy Server Configuration

When users connect to Secure Global Desktop from a variety of locations, there is often a need for different client proxy server settings. Ensuring that users have the correct proxy settings can also be difficult to administer. This release introduces mobile proxy server configuration which allows the Secure Global Desktop Client to use the profile to determine the proxy server settings. The profile allows proxy settings to be specified:

- **Manually** - the proxy settings are stored in the profile itself.
- **Automatically** - the proxy settings are obtained from the user's default web browser.

If the Client is running in Integrated mode and configured to use the web browser settings, the Client obtains the proxy settings by loading the URL specified in the profile in the user's default web browser. As the Client caches the settings it obtains, the Client can be configured to use the settings in the cache so that the user's default web browser only has to be started once.

**Note** to be able to determine the proxy settings from a web browser, the web browser must have Java technology enabled.

---

## Enhanced Command Line for the Secure Global Desktop Client

To support the use of profiles, the command line for the Secure Global Desktop Client on all platforms has been enhanced. There are now arguments to specify:

- The profile to use.

- The URL to connect to (overrides the URL in the profile).
- The preferred language to use.
- The application to start (for launching single applications).

These enhancements allow you to create your own scripts for starting the Client and for running single applications.

---

## Manually Installable Secure Global Desktop Client

To support running the Secure Global Desktop Client in Integrated mode or in environments that have web browsers without Java technology enabled, you can now manually download and install the Secure Global Desktop Client. You download the Client from a Secure Global Desktop Server at `http://server.example.com`. Click Install the Sun Secure Global Desktop Client.

---

## New X Server

This release includes a new X server, based on X11R6.8.2. The new X server delivered significant speed and bandwidth use improvements in benchmark tests when compared to version 4.2.

The updated server supports the following X extensions:

- BIG-REQUESTS
- BLINK
- DAMAGE
- DEC-XTRAP
- DOUBLE-BUFFER
- Extended-Visual-Information
- GLX
- MIT-SCREEN-SAVER
- MIT-SHM
- MIT-SUNDRY-NONSTANDARD
- NATIVE-WND
- RDP
- RECORD
- RENDER
- SCO-MISC
- SECURITY
- SGI-GLX
- SHAPE

- SYNC
- TOG-CUP
- X-Resource
- XC-APPGROUP
- XC-MISC
- XFIXES
- XFree86-Bigfont
- XTEST
- XTTDEV

The new X server also includes support for some additional X fonts. The Speedo font is no longer available.

### New Enable X Security Extension Attribute

X application objects have a new attribute, Enable X Security Extension (`--securityextension`), which allows you to enable the X Security Extension for an application. If you need to run an X application from a host that may not be secure, you should enable the X Security Extension and run the application in untrusted mode. This restricts the operations that the X application can perform in the X server and protects the display. X security only works with versions of SSH that support the `-Y` option. For OpenSSH, this is version 3.8 or later.

### PDF Printing for UNIX, Linux and Mac OS X Clients

The Secure Global Desktop Client on UNIX, Linux and Mac OS X client devices now supports PDF printing. On these clients, printing to a Secure Global Desktop PDF printer causes the document to be displayed in a PDF viewer where the file can be printed and/or saved. By default Secure Global Desktop supports the following PDF viewers.

Client Platform	Default PDF Viewer
Solaris OS on SPARC platforms	Adobe Reader (acroread)
Solaris OS on x86 platforms	GNOME PDF Viewer (gpdf)
Linux	GNOME PDF Viewer (gpdf)
Mac OS X	Preview.app

To be able to use a default viewer, the application must be on the user's PATH.

If an alternative PDF viewer is preferred, the **full path** to the alternative viewer can be specified in the profile used by the Secure Global Desktop Client.

**Note** when specifying a PDF printer on UNIX, Linux and Mac OS X client devices, there is no difference between the "Universal PDF" and "Print to Local PDF File" printers as the document is always displayed in a PDF viewer.

PDF printing on Microsoft Windows client devices is unchanged.

---

## Client Drive Mapping for UNIX and Linux Applications

Client drive mapping is now available for UNIX and Linux applications. This applies to the Secure Global Desktop Client, the Native Client and the Java technology client.

When you enable client drive mapping in Array Manager this enables client drive mapping for UNIX, Linux and Windows applications.

The attributes for managing access rights to client drives available for organization, organizational unit and person objects apply only to Windows client devices regardless of whether they are connected to Windows, UNIX or Linux applications.

As in the previous release, the drives that are mapped for UNIX, Linux and Mac OS X client devices are controlled by entries in the user's configuration file, `$HOME/.tarantella/native-cdm-config`.

For client drive mapping to be available for UNIX and Linux applications:

- The Sun Secure Global Desktop Enhancement Module must be installed and running on the UNIX and Linux application server. Currently you have to manually start the client drive mapping service with the `/opt/tta_tem/bin/tem startcdm` command.
- The application server must have an Network File System (NFS) server installed and running. The NFS server must export a directory that will be used for client drive mapping. By default, this is `/smb`. It is possible to specify a different directory in the `/opt/tta_tem/etc/client.prf` file. The entry in this file has the format `NFS_server/mount/mountpoint` .
- Client drive mapping must be enabled in the array.
- The Secure Global Desktop client drive mapping service must be started in the array, `tarantella start cdm`.
- The access rights to client drives must be configured in Object Manager (for Windows clients) and in the user's configuration file (UNIX, Linux and Mac OS X clients).

When client drive mapping is enabled, the user's client drives or file systems are available by default in the `My SGD drives` directory in the user's home directory. The `My SGD drives` directory is a symbolic link to the NFS share that is used for client drive mapping.

---

## Support for Serial Ports in Windows Applications

Users running Windows applications on a Windows Terminal Server can now access the serial ports on their client device.

To be able to access a serial port:

- COM port mapping must be enabled in the Terminal Services Configuration (it is by default).
- Serial port mapping must be enabled on the Array properties panel in Array Manager (it is by default).
- Access to serial ports must be enabled for either an organization, an organizational unit or person object. Access permissions can be inherited.
- Secure Global Desktop clients must be able to enumerate the serial ports on client devices. The Secure Global Desktop Administration Guide has details of how to map serial ports.

Users must have read-write access to the serial ports that they want to access.

Serial port mapping is available to the Secure Global Desktop Client and the Native Client running on Windows, Solaris and Linux client devices.

---

## Support for the Remote Desktop on Microsoft Windows XP Professional

Microsoft Windows XP Professional includes the Remote Desktop feature that allows you to access a computer using the Remote Desktop Protocol. You can now use Secure Global Desktop and Remote Desktop, for example, to give users to access their office PC when they are out of the office. Only full Windows desktop sessions are supported.

You can also install the Secure Global Desktop Enhancement Module on Windows XP Professional to provide support for client drive mapping. Advanced load balancing and seamless windows are not supported.

---

## Support for Connections to the Console Session with Windows Server 2003 Terminal Services

The Secure Global Desktop Terminal Services Client (`ttatsc`) now supports an additional `-console` option which allows you to connect to the console session with Windows Server 2003 Terminal Services.

You can specify this option with the Protocol Arguments (`--protoargs`) attribute on the Windows application object.

---

## Initial Connection Is Always Secure

When Secure Global Desktop is first installed, the initial connection between a Secure Global Desktop client and a Secure Global Desktop server is secured with SSL. However, after the user has logged in, the connection is downgraded to a standard connection. To be able to use SSL permanently for connections to Secure Global Desktop, you must enable Secure Global Desktop security services.

Port 5307/tcp is used for SSL-based connections between client devices and Secure Global Desktop. You may have to open this port in your firewall to allow clients to connect.

If you are using the array routes feature (`tarantella config edit --tarantella-config-array-netservice-proxy-routes`) and a route includes the `:ssl` option, you must configure the Secure Global Desktop SSL Daemon to accept unencrypted connections using the Accept plaintext on secure port attribute on the server-specific Security Properties panel in Array Manager (`tarantella config edit --security-acceptplaintext`).

---

## Protecting Clients Against Unauthorized Servers

As the Secure Global Desktop Client can now start and log in automatically, it is vital that users only connect to a host that is trusted. In this release, users must explicitly authorize the connection to Secure Global Desktop.

When a user connects to a Secure Global Desktop host for the first time, they see an Untrusted Initial Connection warning message that asks them whether they really want to connect to the host. The message displays the hostname and fingerprint of the security certificate for the server they are connecting to. Users should check these details **before** clicking Yes. Once a user has agreed to the connection, they are not prompted again unless there is a problem.

To ensure that users only connect to Secure Global Desktop servers that are trusted, Secure Global Desktop Administrators should:

- Provide users with a list of hostnames and fingerprints for the servers that are trusted. Use the `tarantella security fingerprint` command on each member of the array to obtain a list of fingerprints.
- Explain to users the security implications of agreeing to connect to server.

In a fresh installation, each Secure Global Desktop host has its own self-signed security certificate. Administrators should obtain and install a valid X.509 certificate for each Secure Global Desktop host.

**Note** If you are using the classic webtop, the Java technology client prompts users **every time** it connects to a Secure Global Desktop server. The Native Client **never** prompts users.

---

## Controlled Copy And Paste

Secure Global Desktop Administrators now have control over copy and paste operations in Windows and X application sessions. Administrators can configure copy and paste as follows:

- Copy and paste for Secure Global Desktop as a whole can be enabled or disabled.
- Copy and paste can be enabled or disabled for organization, organizational unit or person objects. This gives Administrators control over who is allowed to copy and paste.
- Applications can be assigned a Clipboard Security Level. Data can only be copied if the target application (the application *receiving* the data) has the same Clipboard Security Level or higher as the source application. This allows Administrators to secure the data available through particular applications.
- The Secure Global Desktop Client can be assigned a Clipboard Security Level. Data can only be copied to applications running on the client device if the Secure Global Desktop Client has the same Clipboard Security Level or higher as the source application. This allows Administrators to secure the flow of data outside of Secure Global Desktop.

If a user attempts a copy and paste operation that is not permitted, for example because of differing security levels, they paste the following message instead of the copied data:

```
Sun Secure Global Desktop Software: Copied data not available to this application
```

---

## Support for SecurID for Application Server Authentication

As well as using RSA SecurID to authenticate users to Secure Global Desktop, you can use SecurID for application server authentication when launching X and character applications.

To use SecurID authentication, you should first ensure that users can log to the application server in using SecurID before introducing Secure Global Desktop. When you are ready to use SecurID authentication, configure the application to use the `securid/unix.exp` Login script.

---

## Localized User Interface

This release contains localized user interfaces for:

- French
- Japanese
- Korean
- Simplified Chinese
- Traditional Chinese



By visiting a different URL or selecting a language on the Secure Global Desktop Web Server home page (<http://server.example.com>), users can run a webtop in their preferred language. The Secure Global Desktop Client too can be started in a preferred language.

The following are not localized:

- The administration tools Object Manager and Array Manager
- The classic webtop
- The Secure Global Desktop Native Client and Java technology client

---

## Translated Documentation

The following translations of Secure Global Desktop Documentation are available:

Language	Release Notes	Installation Guide	Administration Guide	User Guide
French	Yes	Yes	No	Yes
Japanese	Yes	Yes	Yes	Yes
Korean	Yes	Yes	No	Yes
Simplified Chinese	Yes	Yes	No	Yes
Traditional Chinese	Yes	Yes	No	Yes

Not all pages in the Administration Guide have been translated into Japanese.

---

## Language Support in Expect Scripts

The Expect scripts used to start applications on application servers have also been enhanced to support system prompts in different languages. By default, the languages supported by Secure Global Desktop are supported.

To allow the Expect scripts to work with system prompts in different languages, there is new Host Locale (`--hostlocale`) attribute on host objects that allows you to specify the locale of the host.

---

## Changes in This Release

Sun Secure Global Desktop Software 4.3 contains the following changes:

- Single Installable Package
  - SSL Daemon Always Running
  - User Preferences File on UNIX, Linux and Mac OS X Client Devices
  - Change to Window Close Action (--windowclose) Attribute
  - Support for PAM for UNIX User Authentication
  - Changes to PDF Printing
  - Client Certificates for Active Directory Login Authority
  - Changes to Secure Global Desktop Certificate Store
  - Licensing Changes
  - Change to Application Connection Methods
  - Change to Simultaneous Webtop Connections Attribute
  - Change to Mainframe (3270) Applications
- 

### **Single Installable Package**

This release introduces a single package for installing Secure Global Desktop. When you install Secure Global Desktop, you install all the packages that previously had to be installed separately (including the font packages). The use of the components is controlled by the license keys installed in the array.

---

### **SSL Daemon Always Running**

As the initial connection to Secure Global Desktop is now always secure, this means that the Secure Global Desktop SSL Daemon is always running even if Secure Global Desktop security services have not been enabled.

---

### **User Preferences File on UNIX, Linux and Mac OS X Client Devices**

In previous releases, a user preferences file was used to configure the Secure Global Desktop Client on UNIX, Linux and Mac OS X client devices. With the introduction of profiles, the preferences file is only used for the Native Client on these platforms.

---

## Change to Window Close Action (--windowclose) Attribute

In previous releases, the Window Close Action (--windowclose) attribute was only available to X applications that were configured to display using client window management. The use of this attribute has been extended to include X, Windows and character applications that are configured to display using an independent window.

The change means that closing an independent window may end or suspend the emulator session. The default is to end the session.

---

## Support for PAM for UNIX User Authentication

Secure Global Desktop now supports PAM (Pluggable Authentication Modules) for UNIX user authentication. The change affects the following login authorities:

- ENS
- UNIX User
- UNIX Group

Secure Global Desktop uses PAM for user authentication, account operations and password operations.

When you install Secure Global Desktop on Linux platforms, Setup automatically creates PAM configuration entries for Secure Global Desktop by copying the current configuration for the `passwd` program and creating the `/etc/pam.d/tarantella` file. On Solaris OS platforms, you can add a new entry for Secure Global Desktop (`tarantella`) in the `/etc/pam.conf` file if required.

Using PAM gives Secure Global Desktop Administrators more flexibility and control over UNIX user authentication, for example by adding new login tests, account limits, or valid password checks.

---

## Changes to PDF Printing

As a result of the changes introduced in this release to support PDF printing on UNIX, Linux and Mac OS X client devices, the Display Adobe Reader Print dialog (`--pdfprompt`) attribute has been removed from the Printing properties panel in Array Manager and from the Printing panel for organization, organizational unit and person objects in Object Manager.

This change means that when users print with the Universal PDF printer on Windows clients, the print job is automatically sent to the client's default printer. To be able to choose which client printer the print job is sent to, users must now select the Print to Local PDF File printer.

---

## Client Certificates for Active Directory Login Authority

When using the Active Directory login authority, there is a new Use Certificates checkbox on the Secure Global Desktop Login properties panel in Array Manager. If Active Directory is configured to require client certificate and you have created and installed a client certificate for Secure Global Desktop, then you no longer need to configure the username and password of a privileged user.

---

## Changes to Secure Global Desktop Certificate Store

The password used for the Secure Global Desktop certificate store (`/opt/tarantella/var/info/certs/sslkeystore`) is no longer hard-coded to `123456`. Instead each store now has a random password, which is stored in `/opt/tarantella/var/info/key`. Use this password with the `-storepass` and `-keypass` options when using `keytool`.

---

## Licensing Changes

Version 4.2 contained the following changes to licensing:

- Activation license keys are no longer required to enable an array.
- Named user licensing is no longer available.
- Maintenance and Right to upgrade license keys are no longer available.

If you upgrade from an earlier version your existing product license keys will be automatically converted and your existing Maintenance and Right to upgrade license keys will be deleted.

---

## Change to Application Connection Methods

From version 4.1, Secure Global Desktop no longer supports the `rlogin` and `rcmd` connection methods for starting applications. If you upgrade from an earlier version, you must change the connection method for any applications that use these methods.

---

## Change to Simultaneous Webtop Connections Attribute

From version 4.1, Secure Global Desktop uses a different attribute for the Maximum simultaneous

webtop connections setting (`--tuning-maxconnections`). If you upgrade from an earlier version, the default setting for this attribute will be applied.

---

## Change to Mainframe (3270) Applications

From version 4.0, Secure Global Desktop uses a different emulator for mainframe (3270) applications. 3270 character and 3270 X application objects are no longer available and have been replaced by a single 3270 application object. As the new 3270 application object has several new attributes, it is not possible to upgrade existing 3270 application objects. If you upgrade from an earlier version, your existing 3270 character and 3270 X applications will be deleted when you upgrade and you will need to re-configure them.

---

## Fixes in This Release

This section list the significant bug fixes contained in this release. They are divided into the following areas:

- [Administration Tools](#)
  - [Application Launch](#)
  - [Audio](#)
  - [Client Drive Mapping](#)
  - [Clients and Webtop](#)
  - [Emulation](#)
  - [Installation and Upgrade](#)
  - [Internationalization and Localization](#)
  - [Licensing](#)
  - [Other](#)
  - [Printing](#)
  - [Security](#)
  - [Server](#)
  - [User Authentication](#)
  - [Web Services](#)
- 

## Administration Tools

Reference	Description
6433525	<code>/usr/bin</code> owner is changed to <code>ttasys</code> on startup.
6436735	The <code>tarantella object new_xapp</code> command does not accept the <code>--accel</code> argument.
6437203	Object Manager shows a warning message after renaming an ENS object.
6445405	Shadowing from the command line takes an invalid session id.
6447937	X authority cookies should not be passed via environment.
6450323	Attributes cannot be specified in object creation but can be set in object edit.
6451537	<code>tarantella license</code> commands and Array Manager display obsolete software components.

## Application Launch

Reference	Description
6357003	The Native Client cannot launch a web browser on Solaris OS.
6357022	Native Client shifts up the full-screen webtop on Java Desktop System.
6392279	X authorization issue causes launch failure.
6401949	With <code>optimizelaunch</code> enabled in the <code>unix.exp</code> login script, the expired password handler does not work.
6405808	The filtering script ( <code>runsubscript.exp</code> ) is not being called during the launch process.
6416951	Error message is displayed when a new browser window application is ended with the 'X' button.
6419574	The authentication dialog returns corrupted data if the password has more than eight characters.
6427189	Launch failure when the host is not known to ssh.
6434660	Password expiry handling on application launch is broken.
6447551	There should only be one <code>ttacpe</code> process created for each webtop session.
6455378	Launch failure when ssh used over su for an application running on the Secure Global Desktop host.

6464809	# characters in system login banner cause automated launch process to fail.
6470173	Add support for SecurID ACE agent for PAM.
6475303	Custom Certificate Authority certificates not recognized and cause a prompt when launching in-place applications
6476180	Root window stays around when logging out of kiosk Gnome session.

## Audio

Reference	Description
6416384	RDP-based audio output stops playing when using a SunRay.

## Client Drive Mapping

Reference	Description
6409765	Error copying large(ish) files from client to server over a slow network in RDP sessions.

## Clients and Webtop

Reference	Description
6408157	Local X server application does not launch from the JSP webtop.
6417140	The webtop frame is blank after launching an application.
6417575	Unix Native Client using a proxy server: log in, log out, log in again and the Native Client hangs.
6417631	Unix Native Client: redraw problems with kiosk applications.
6424776	Secure Global Desktop Client produces errors and exits when logging out of the webtop.
6432133	The Native Client SEGVs if you close the connection progress window.
6465959	When Secure Global Desktop restarts, the Secure Global Desktop Client spins and sends out hundreds of network packets.
6468173	Wait cursor problem on SunRays.

## Emulation

Reference	Description
6381531	Edited <code>colormap.txt</code> intermittently ignored when security is enabled.
6386091	Windows Native Client and Citrix ICA X Client: possible key event incompatibility.
6415498	Character terminal session closes unexpectedly when function keys are pressed.
6417698	Scalable windows applications do not toggle when scroll lock pressed on Java Desktop System on Solaris 10 OS.
6426355	ttaxpe dies with SIGSEGV
6427789	Copy (ctrl+insert) causes X applications to hang.
6433273	Using the Native Client on Solaris OS, kiosk mode does not display correctly.
6435437	Child window sometimes comes up below the parent window using seamless windows.
6435489	Windows applications performance in 4.3.
6435527	Segmentation fault in the ttaxpe when running the HP monitoring tool.
6445467	Windows Logo keys do not work in a Terminal Services session.
6446469	Problems with the French locale and keymap.
6467368	Letter repeated twice in Remote Desktop Protocol session.
6471395	Timezone redirection fails to set correct time during daylight savings. Time always out by one hour.
6472959	ESC-NumLock does not work as expected from Solaris OS client/SunRay.

## Installation and Upgrade

Reference	Description
6355269	The default configuration for a Java Desktop Session loses some important configuration parameters.
6368390	Upgrade from 4.20.909 to later builds requires a maintenance or right to upgrade license.



6368675	Root certificates for secure LDAP servers are not retained during an upgrade.
6396629	Install fails during bean creation, server will not start.
6407985	Secure Global Desktop incorrectly handles large amount of free disk space at install.
6430913	Problems with <code>httpd.conf</code> file on upgrade.
6446020	Unable to uninstall Secure Global Desktop if the external DNS name is incorrect.
6453638	Cannot log in to a Secure Global Desktop server after an upgrade.
6462429	Secure Global Desktop is uninstalled even though user selected No.

## Internationalization and Localization

Reference	Description
6354105	In Configuration Wizard, the application list shows corrupt strings with multibyte characters.
6355226	The Connection Progress dialog cannot display multibyte characters.
6357040	Cannot copy and paste from Microsoft Windows to Solaris OS.
6357075	Cannot copy and paste from Microsoft Windows to Microsoft Windows.
6357606	Cannot copy and paste from Java Desktop System to Common Desktop Environment.
6362374	Client drive mapping daemon crashes with a localized <code>native-cdm-config</code> file.
6419511	Windows applications should have Unicode as the Euro symbol default.
6419523	Server LANG environment overrides client locale setting.
6447594	Client window mode mode should be accessed with an IP address instead of unix socket.
6450008	Problems generating an apostrophe with a Swedish keyboard.

## Licensing

Reference	Description
6466415	Secure LDAP does not work without security licenses installed.

## Other

Reference	Description
6375600	Authentication fails with ActivCard - Cyberflex 64k Smart Card (also bug ref 607218).
6384746	Able to read <code>.cgi</code> files via web browser.
6390126	A large number of users logging in in quick succession hangs the Secure Global Desktop server.
6393623	New browser window gets launched when new browser windows applications are launched with the CTRL key pressed.
6407855	Secure Global Desktop Server exits with error code 129, signal 0.
6408159	New blank browser window opens on exiting the application opened in new browser window mode.
6409117	Secure Global Desktop Enhancement Module for Intel Solaris appears to fail.
6410161	Using telnet to connect to localhost port 1023 causes the Protocol Engine Manager to use 100% CPU.
6418965	Client window manager applications display Minimize and Maximize buttons that are not present in original application.
6430243	Secure Global Desktop Apache includes development private paths and configurations.
6430396	Unable to copy paste to and from a WCP IWM session from the classic webtop.
6436155	Setting keepalive to 0 causes keepalives to be sent continuously.
6442142	Quitting Gnome session causes ttaxpe to use 100% CPU.
6446271	Secure Global Desktop Web Server starts but remains attached to the console.

## Printing

Reference	Description
6376221	Printer properties (such as paper size) do not appear to be stored between RDP sessions.
6406292	Driver name duplicated if printing is configured at OU and user level.

6421283	Windows Native Client detects DEFAULT_PRINTER_UNKNOWN when there is no printer configured on the client device.
6427852	Login delay induced by inaccessible network printer attached to client device.

## Security

Reference	Description
6419520	LDAP searches of Active Directory contacts AD servers in other regions for information.
6446338	The prompt for password change does not appear after a password has expired.
6446437	Cannot create an array after enabling SSL connections between array members.
6457984	Validate user input to the login box to prevent cross-site scripting attacks.
6468699	ttassl daemon core dumps due to sigsegv, signal 11.
6469123	Apply OpenSSL security patch secadv_20060905.txt
6476728	Apply OpenSSL security patch secadv_20060928.txt
6478735	Cascading Stylesheets vulnerability.

## Server

Reference	Description
6379743	<code>tarantella status</code> command report is incorrect when SSL connections between array members is enabled.
6392365	Array problems when one of the array members is not contactable.
6393745	Cannot successfully promote a secondary server to a primary if the primary server is down.
6445200	Array behavior when joining and detaching members of an array that is licensed.

## User Authentication

Reference	Description
-----------	-------------

6383417	If the <code>krb5.conf</code> file has errors, user login hangs and the server continuously writes exceptions to <code>jserver.log</code> .
6400123	Ambiguous login is not allowed if invalid credentials were provided the first time.
6415709	Active Directory authentication fails silently if one tree of a forest is not configured in the <code>krb5.conf</code> file.
6439688	Windows Native Client does not display an error message if an Active Directory password change fails.
6454261	Expect script updated for German Solaris OS applications.
6460263	Oberthur AuthentIC card not recognized when using Secure Global Desktop (fixed for Windows Clients only).
6465569	Active Directory PKI infrastructure does not failover to the next global catalog server.
6471877	SecurID login authority issues.

## Web Services

Reference	Description
6391262	Anonymous users can create and edit webtop groups. This info will be stored on disk and not cleaned up.
6427185	Secure Global Desktop Web Server exposes too much information.

## End-Of-Support Statements

Customers with a valid support agreement can upgrade to the latest version of [Sun Secure Global Desktop Software](#) free of charge.

The following table lists the end-of-support dates for previous Secure Global Desktop and Tarantella software products:

Software Product	Version	Supported Until
Secure Global Desktop Enterprise Edition	4.1	March 31, 2007
Secure Global Desktop Enterprise Edition	4.0	March 31, 2007
Secure Global Desktop Software Appliance	4.0	March 31, 2007

Secure Global Desktop Enterprise Edition	3.42	March 31, 2007
Tarantella Enterprise 3 (including TASP)	3.40	March 31, 2007

---

## Known Bugs and Issues

The following are the known bugs and issues with this release:

- [602423](#) - Terminal Emulators Cannot Distinguish Between the Return Key and the Keypad ENTER Key
- [6375418](#) - Non-ASCII Characters in Candidate Window and Status Window of Input Method Cannot Be Displayed
- [6448990](#) - Backslash and Yen Keys Produce the Same Character in Windows Applications
- [6456278](#) - Integrated Mode Does Not Work for the Root User on Solaris 10 x86 Platforms
- [6458111](#) - On SUSE Linux Enterprise Server 10 Client Devices, the Gnome Main Menu Crashes When Using the Integrated Client
- [6458548](#) - Renamed Start Menu Entries for the Sun Secure Global Desktop Client Are Not Honored
- [6463946](#) and [6463949](#) - Many Keys Do Not Work For Japanese Users in Applications That Display in a Web Browser Window
- [6464809](#) - System Login Banners Containing Characters Such as "#", "\$" or "=" Cause the Login Scripts to Fail When the Connection Method is SSH
- [6466958](#) - You Cannot Use Shift + Click or Control + Click With the Integrated Client
- [6470197](#) - Compiling Your Own Apache Modules for Use With the Secure Global Desktop Web Server Fails
- [6476194](#) - Shortcuts for the Integrated Client do not Display on the KDE Desktop Menu on SUSE Linux Enterprise Server 10
- [6476661](#) - Integrated Client Does Not Work as Expected With the Gnome Desktop on Red Hat Enterprise Linux 4
- [6477187](#) - Client Drive Mapping Fails if the Client for Microsoft Networks Is Not Enabled on a Microsoft Windows Application Server
- [6477549](#) - Integrated Client Does Not Work as Expected With the Gnome Desktop on Red Hat Enterprise Linux 3
- [6480880](#) - Integrated Client Does Not Work With Relocated Webtops
- [6481148](#) - Localized Text Is Not Used During Installation
- [6482912](#) - Secure Global Desktop Client Will Not Install Automatically Using Internet Explorer 7 With Microsoft Windows Vista
- [List of Applications in the Desktop Start Menu Are Not Sorted Alphabetically](#)
- [Start Menu Entries Do Not Display on Sun Java Desktop](#)
- [Users with Sun Type 7 Japanese Keyboards Cannot Input Characters Correctly Using Secure Global Desktop](#)

---

## 602423 - Emulators Cannot Distinguish Between the Return Key and the Keypad ENTER Key

### Problem

Secure Global Desktop X and character emulators cannot distinguish between the Return key and the keypad ENTER key on the user's client keyboard.

### Cause

A known issue.

### Solution

By default, the Secure Global Desktop Client and the Native Client map the keypad ENTER key to Return in both X and character emulator sessions. With additional configuration this behavior can be changed.

To change the behavior of the keypad ENTER key in a **character application** session, you need to set up a keymap for your character application object (`--keymap`) and add a mapping for KPENTER, for example:

```
KPENTER="hello"
```

To change the behavior of the keypad ENTER key in a **Windows/X application** session, you need to modify your X keymap (for example, `xuniversal.txt`) and add a mapping for the KP\_Enter key, for example:

```
92 KP_Enter KP_Enter NoSymbol NoSymbol 0x801c
```

**Warning!** The X keymap is a global/user resource, so all applications for that user may be affected by this change. If any of these applications do not handle KP\_Enter, then you may need to consult your X/Windows application vendor for assistance.

**Note** The Java™ technology clients are unable to distinguish between RETURN and the keypad ENTER key.

---

## 6375418 - Non-ASCII Characters in Candidate Window and Status Window of Input Method Cannot Be Displayed

### Problem

Users in Chinese (Simplified and Traditional), Japanese, and Korean locales cannot display non-ASCII characters in the candidate and status windows of the input method when running applications on a Solaris OS application server. This affects Solaris 8, 9, 10 and 10u1 OS platforms.

## Cause

Missing font path configuration on the Secure Global Desktop server.

## Solution

Add Chinese, Japanese, and Korean font path information to the font server on the Secure Global Desktop host.

For example, if the Secure Global Desktop Server is installed on a Solaris 10 OS platform and you are using the Simplified Chinese input method:

1. Edit the `/usr/openwin/lib/X11/fontserver.cfg` file and add the Chinese font path information as follows:

```
clone-self = on
use-syslog = off
catalogue = /usr/openwin/lib/locale/zh_CN.GB18030/X11/fonts/75dpi, /usr/
openwin/lib/locale/zh_CN.GB18030/X11/fonts/TrueType,
/usr/openwin/lib/locale/zh.GBK/X11/fonts/75dpi, /usr/openwin/lib/locale/
zh.GBK/X11/fonts/TrueType, /usr/openwin/lib/locale/zh/X11/fonts/75dpi,
/usr/openwin/lib/locale/zh/X11/fonts/TrueType, /usr/openwin/lib/locale/
zh.UTF-8/X11/fonts/misc, /usr/openwin/lib/locale/iso_8859_2/X11/
fonts/75dpi,
/usr/openwin/lib/locale/iso_8859_2/X11/fonts/Type1, /usr/openwin/lib/
locale/iso_8859_2/X11/fonts/TrueType, /usr/openwin/lib/locale/
iso_8859_4/X11/fonts/75dpi,
/usr/openwin/lib/locale/iso_8859_4/X11/fonts/Type1, /usr/openwin/lib/
locale/iso_8859_5/X11/fonts/75dpi, /usr/openwin/lib/locale/iso_8859_5/
X11/fonts/Type1,
/usr/openwin/lib/locale/iso_8859_5/X11/fonts/TrueType, /usr/openwin/lib/
locale/ar/X11/fonts/TrueType, /usr/openwin/lib/locale/iso_8859_7/X11/
fonts/TrueType,
/usr/openwin/lib/locale/iso_8859_7/X11/fonts/75dpi, /usr/openwin/lib/
locale/iso_8859_7/X11/fonts/Type1, /usr/openwin/lib/locale/iso_8859_8/
X11/fonts/Type1,
/usr/openwin/lib/locale/iso_8859_8/X11/fonts/TrueType, /usr/openwin/lib/
locale/iso_8859_9/X11/fonts/75dpi, /usr/openwin/lib/locale/iso_8859_9/
X11/fonts/Type1,
/usr/openwin/lib/locale/iso_8859_9/X11/fonts/TrueType, /usr/openwin/lib/
locale/iso_8859_15/X11/fonts/TrueType
# in decipoints
default-point-size = 120
default-resolutions = 75,75,100,100
```

2. Restart the font server on the Secure Global Desktop host.

```
svcadm restart xfs
```

3. Configure Secure Global Desktop with the location of the font server.

- o In Array Manager, select X Protocol Engine properties.
- o In the Font Path box, type the details of the font server, for example tcp/boston:7000

**Note** Changes to font path information only take effect for new Protocol Engines only. Existing Protocol Engines are not affected.

The Secure Global Desktop Administration Guide has more detailed information on using your own X fonts, see "How do I use my own X fonts?"

Alternatively, on Solaris 10 OS application servers only, upgrading to the latest version of the Internet Intranet Input Method Framework (IIIMF) should also fix the problem.

---

## 6448990 - Backslash and Yen Keys Produce the Same Character in Windows Applications

### Problem

When using Japanese PC 106 or Sun Type 7 Japanese keyboards with Windows applications running through Secure Global Desktop, the Yen and Backslash keys produce the same result.

### Cause

A know issue with key handling.

### Solution

Modify the Xsun keytable or the Xorg keytable on the client device.

For example, change the `/usr/openwin/etc/keytables/Japan7.kt` file as follows:

```
...
#137    RN      XK_backslash  XK_bar  XK_prolongedsound
 137    RN      XK_yen        XK_bar  XK_prolongedsound
...
#39     RN      XK_0          XK_asciitilde  XK_kana_WA      XK_kana_WO
 39     RN      XK_0          XK_0          XK_kana_WA      XK_kana_WO
...
```



For example, change the `/usr/X11/lib/X11/xkb/symbols/sun/jp` file as follows:

```
...
# key <AE13> { [ backslash, bar          ], [ prolongedsound      ]          };
  key <AE13> { [ yen, bar                ], [ prolongedsound      ]          };
...
# key <AE10> { [ 0, asciitilde          ], [ kana_WA, kana_WO      ]          };
  key <AE10> { [ 0, 0], [ kana_WA, kana_WO  ]          };
...
```

After making these changes, you must restart `dtlogin`:

```
/etc/init.d/dtlogin stop
/etc/init.d/dtlogin start
```

---

## 6456278 - Integrated Mode Does Not Work for the Root User on Solaris 10 x86 Platforms

### Problem

On Solaris 10 x86 platforms, enabling Integrated mode when you are logged in as root does not add applications to the desktop Start Menu. You may also see the following warning:

```
gnome-vfs-modules-WARNING **: Error writing vfolder configuration file "//.
gnome2/vfolders/applications.vfolder-info": File not found.
```

### Cause

A known issue with the Gnome Virtual File System (VFS).

### Solution

There is currently no solution.

---

## 6458111 - On SUSE Linux Enterprise Server 10 Client Devices, the Gnome Main Menu Crashes When Using the Integrated Client

### Problem

On client devices running SUSE Linux Enterprise Server 10, the Gnome Main Menu crashes when using the Integrated Client. The crash usually occurs on login or logout.

### **Cause**

A known problem with the Gnome Main Menu applet on SUSE Linux Enterprise Server 10 (Novell bug reference 186555).

### **Solution**

Disabling the Recently Used Applications functionality improves the stability of the Gnome Main Menu.

Run the following commands on the client device:

```
gconftool-2 --set --type=list \  
    --list-type=int /desktop/gnome/applications/main-menu/lock-down/  
showable_file_types [0,2]  
  
pkill main-menu  
  
pkill application-browser
```

---

## **6458548 - Renamed Start Menu Entries for the Sun Secure Global Desktop Client Are Not Honored**

### **Problem**

When configured to operate in Integrated mode, the Sun Secure Global Desktop Client creates entries in the desktop Start Menu. It is possible to rename these entries, but the changes are not honored by the Client.

### **Cause**

Renaming Start Menu entries is not supported.

### **Solution**

Do not rename the Secure Global Desktop Start Menu entries.

---

## 6463946 and 6463949 - Many Keys Do Not Work For Japanese Users in Applications That Display in a Web Browser Window

### Problem

Japanese users working with applications that are configured to display on the webtop or in a new browser window find that many keys do not work. Problems have been noticed with the Windows key, the Applications key, and the Katakana, Zenkaku\_Hankaku, Hiragana and Muhenkan keys.

### Cause

Applications configured to display on the webtop or in a new browser window, use the classic Java technology client. This client has not been internationalized or localized.

### Solution

Change the application's Display Using attribute so that the application displays in either a kiosk, an independent or a seamless window.

---

## 6464809 - System Login Banners Containing Characters Such as "#", "\$" or "=" Cause the Login Scripts to Fail When the Connection Method is SSH

### Problem

When the connection method is SSH, system login banners containing characters such as "#", "\$" or "=" cause the login scripts to fail.

### Cause

The SGD login scripts interpret characters such as "#", "\$" or "=" as a command prompt. When the login scripts detect a command prompt, they stop checking for a password prompt.

### Solution

Do one of the following:

- Edit the `/opt/tarantella/var/serverresources/expect/procs.exp` login script.

Change the following line:

```
set seen_pw_or_ssh_prompt 0  
to
```

```
set seen_pw_or_ssh_prompt 1
```

- Configure SSH on your system to use client keys. This bypasses the password prompt.
  - Remove the characters causing the problem from the system login banner.
- 

## **6466958 - You Cannot Use Shift + Click or Control + Click With the Integrated Client**

### **Problem**

Secure Global Desktop allows users to change the way an application is displayed by holding down the Control key when clicking the link to start an application. Holding down the Shift key allows users to start an application as a different user. Neither of these options work when clicking links in the desktop Start Menu (Integrated Client).

### **Cause**

This functionality is not yet available to the Integrated Client.

### **Solution**

To use this functionality, you must start the application from a webtop. To display a webtop, click the Webtop link in the Start Menu.

---

## **6470197 - Compiling Your Own Apache Modules for Use With the Secure Global Desktop Web Server Fails**

### **Problem**

When you compile your own Apache modules for use with the Secure Global Desktop Web Server, the compilation fails because of a missing `egcc` compiler.

### **Cause**

The configuration file for the Apache eXtenSion tool (`apxs`) that is used to build extension modules for the Secure Global Desktop Web Server uses the `egcc` compiler and this may not be available on your system.

### **Solution**

Either modify the `apxs` configuration file (`/opt/tarantella/webserver/apache/version/bin/apxs`) to use a compiler that is available on your system or create a symlink for `egcc` that links to the compiler on your system.

---

## 6476194 - Shortcuts for the Integrated Client do not Display on the KDE Desktop Menu on SUSE Linux Enterprise Server 10

### Problem

Shortcuts for the Integrated Client do not display on the KDE Desktop Menu on SUSE Linux Enterprise Server 10.

### Cause

SUSE-specific configuration of the KDE menu system means that if a menu contains only one application entry, then that single application is used in the main menu instead of the menu. If menu entry is a sub-menu, the sub-menu does not display at all. This causes the Integrated Client Login menu not to display.

### Solution

The workaround is to add the following line to the `[menus]` section of `$HOME/.kde/share/config/kickerrc`:

```
ReduceMenuDepth=false
```

Then run the following command for the KDE panel to immediately pick up the changes:

```
dcop kicker kicker restart
```

All subsequent KDE sessions will automatically use this setting.

---

## 6476661- Integrated Client Does Not Work as Expected With the Gnome Desktop on Red Hat Enterprise Linux 4

### Problem

After enabling the Automatic Client Login or the Add Applications to Start Menu options in your profile, the Secure Global Desktop Client does not start automatically when you log in to the Gnome Desktop

and/or the Start Menu is not updated with webtop content when you log in to Secure Global Desktop.

### **Cause**

A known bug with Gnome Desktop on Red Hat Enterprise Linux 4 ([https://bugzilla.redhat.com/bugzilla/show\\_bug.cgi?id=151887](https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=151887)). The directories containing the `.menu` files are not monitored and so changes to the Start Menu are not detected.

### **Solution**

The workaround is run the following command to restart the `gnome-panel` and pick up new menu information:

```
pkill gnome-panel
```

---

## **6477187 - Client Drive Mapping Fails if the Client for Microsoft Networks Is Not Enabled on a Microsoft Windows Application Server**

### **Problem**

Client drive mapping fails if the Client for Microsoft Networks is not enabled on a Microsoft Windows application server.

### **Cause**

The Client for Microsoft Networks must be enabled to allow remote access to files and folders.

### **Solution**

Enable the Client for Microsoft Networks, as follows:

1. In Control Panel, double-click Network Connections.
2. Right-mouse click on the network card and select Properties.
3. On the General tab, check the box next to Client for Microsoft Networks.
4. Click OK.

---

## **6477549 - Integrated Client Does Not Work as Expected With the Gnome Desktop on Red Hat Enterprise Linux 3**

## Problem

After enabling the Add Applications to Start Menu option in your profile, the Start Menu is not updated with webtop content when you log in to Secure Global Desktop.

Starting the Secure Global Desktop Client from the command line may also result in the following error:

```
-----  
process:5281): GLib-CRITICAL **: file gtree.c: line 261  
(g_tree_destroy): assertion `tree != NULL' failed  
-----
```

## Cause

Red Hat Enterprise Linux 3 has menu editing disabled by default and so the Gnome Start Menu is not updated.

The error message is not critical.

## Solution

Enable menu editing for the Gnome Desktop, as follows:

1. Log in as root.
2. Change directory to the `/etc/gnome-vfs-2.0/modules` directory.
3. Move the `default-modules.conf` file as follows:

```
mv default-modules.conf default-modules.conf.without-menu-editing
```

4. Copy the `default-modules.conf.with-menu-editing` file as follows:

```
cp default-modules.conf.with-menu-editing default-modules.conf
```

Users must log out of the Gnome Desktop and log back in again for the change to take effect.

---

## 6480880 - Integrated Client Does Not Work With Relocated Webtops

### Problem

If you relocate the browser-based webtop to your own JavaServer Pages (JSP) container, the

Integrated Client refuses to connect to Secure Global Desktop.

### **Cause**

The Integrated Client requires some files from the Axis web application.

### **Solution**

To use the Integrated Client, you must also copy the Axis web application to the remote host. Copy everything in the `/opt/tarantella/webserver/tomcat/5.0.28_axis1.2/webapps/axis` directory to the remote host.

**Note** The `axis` directory contains several symbolic links, ensure these links are followed when you copy the directory.

---

## **6481148 - Localized Text Is Not Used During Installation**

### **Problem**

When you install Secure Global Desktop in a supported locale, the language used during the installation is English.

### **Cause**

To see localized text during installation, the `gettext` package must be installed on the host. If this package is missing, the installation defaults to English.

### **Solution**

Ensure the `gettext` package is installed before installing Secure Global Desktop.

---

## **6482912 - Secure Global Desktop Client Will Not Install Automatically Using Internet Explorer 7 With Microsoft Windows Vista**

### **Problem**

Using Internet Explorer 7 on Microsoft Windows Vista platforms, the Secure Global Desktop Client cannot be automatically downloaded and installed. The Client can be installed manually and it can be installed automatically using another browser, such as Firefox.



## **Cause**

Internet Explorer has a Protected Mode that prevents the Client downloading and installing automatically.

## **Solution**

Add the Secure Global Desktop server to the list of Trusted Sites list in Internet Explorer's Security Settings.

---

## **List of Applications in the Desktop Start Menu Are Not Sorted Alphabetically**

### **Problem**

When using Integrated mode on Microsoft Windows client devices, users may notice that the Start Menu entries are not sorted alphabetically.

### **Cause**

This is caused by a Windows feature that adds new items to end of a menu rather than preserving the alphabetical sorting.

### **Solution**

See [Microsoft KB article 177482](#) for details.

---

## **Start Menu Entries Do Not Display on Sun Java Desktop**

### **Problem**

On Sun Java Desktop Systems, users may find that Start Menus entries are not created for Secure Global Desktop when they enable Integrated mode. The Start menu entries are added when they log out of their desktop and log in again.

### **Cause**

A known issue with the Gnome panel.

## Solution

The solution is to install the following patches:

- 119906-05 for Solaris OS on SPARC platforms
- 119907-05 for Solaris OS on x86 platforms

The workaround is to log out of the desktop and log in again.

---

## Users with Sun Type 7 Japanese Keyboards Cannot Input Characters Correctly Using Secure Global Desktop

### Problem

Users with Sun Type 7 Japanese keyboards cannot input characters correctly using Secure Global Desktop.

### Cause

Missing Solaris OS keytable on the client device.

### Solution

Install the appropriate patch to install the keytable on the client device:

Platform	Required Patch
Solaris 10 OS on SPARC platforms	121868-03
Solaris 9 OS on SPARC platforms	113764-04
Solaris 8 OS on SPARC platforms	111075-05
Solaris 10 OS on x86 platforms	121869-03
Solaris 9 OS on x86 platforms	113765-03
Solaris 8 OS on x86 platforms	114539-02

---

## Documentation Issues

The following are the known documentation issues with this release:

- [Correction to the Integrated Client Documentation](#)
  - [Instructions for Relocating the Webtop to Another Host Do Not Work for the Integrated Client](#)
  - [Correction to Supported Versions of SecurID](#)
- 

### **Correction to the Integrated Client Documentation**

Secure Global Desktop allows users to change the way an application is displayed by holding down the Control key when clicking the link to start an application. Holding down the Shift key allows users to start an application as a different user.

The Secure Global Desktop Administration Guide and User Guide incorrectly state that this functionality is available when using the Integrated Client.

To use this functionality, you must start the application from a webtop. To display a webtop, click the Webtop link in the Start Menu.

---

### **Instructions for Relocating the Webtop to Another Host Do Not Work for the Integrated Client**

The page "Relocating the browser-based webtop to your own JSP container" contains instructions for moving the webtop to another host.

These instructions are valid if you want to work in Webtop mode. To use the Integrated Client, however, you must also copy the Axis web application to the remote host. Copy everything in the `/opt/tarantella/webserver/tomcat/5.0.28_axis1.2/webapps/axis` directory to the remote host.

**Note** The `axis` directory contains several symbolic links, ensure these links are followed when you copy the directory.

---

### **Correction to Supported Versions of SecurID**

The Secure Global Desktop Administration Guide incorrectly states that the SecurID login authority works with versions 4 and 5 of the RSA ACE/Server.

This login authority works with versions 4, 5 **and** 6.

---

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties. Sun, Sun Microsystems, the Sun logo, Java and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries.

UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Copyright © 1997-2006 Sun Microsystems, Inc. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

L'utilisation est soumise aux termes du contrat de licence.

Cette distribution peut comprendre des composants développés par des tierces parties.

Sun, Sun Microsystems, le logo Sun, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays.

UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

# Sun Secure Global Desktop Software 4.3 Installation Guide

Read this page to find out how to install Sun Secure Global Desktop Software version 4.3 on your system.

If you are upgrading, read the upgrade instructions **before** installing the software.

This page uses the term "host" to mean the UNIX/Linux system on which you want to install Sun Secure Global Desktop Software.

Part Number: 819-6254

---

## Contents

- [Before You Install](#)
  - [Installing Sun Secure Global Desktop Software](#)
  - [Upgrading Sun Secure Global Desktop Software](#)
  - [Getting Started with Sun Secure Global Desktop Software](#)
  - [Removing Sun Secure Global Desktop Software](#)
- 

## Before You Install

- [Release Notes](#)
  - [Secure Global Desktop Web Server](#)
  - [The ttaserv and ttasys Users](#)
  - [Application Connection Methods](#)
- 

## Release Notes

Before installing Sun Secure Global Desktop Software, you should read the Secure Global Desktop Release Notes. The Release Notes contain important information about this version of Secure Global Desktop, including:

- The supported installation platforms.
- Required operating system modifications. If you do not make the required modifications, Secure

Global Desktop may not install.

- Known issues and bugs with installation.
- 

## Secure Global Desktop Web Server

When you install Secure Global Desktop, you install the Secure Global Desktop Web Server. The Secure Global Desktop Web Server is an Apache web server that has been pre-configured for use with Secure Global Desktop.

When you install Secure Global Desktop, you will be prompted for the TCP port on which the Secure Global Desktop Web Server listens for HTTP connections. This is usually port 80/tcp, but if another process is listening on that port you will be prompted to choose another.

---

## The `ttaserv` and `ttasys` Users

There must be a `ttaserv` and `ttasys` user on the host before you can install Secure Global Desktop. There must also be a `ttaserv` group.

The `ttasys` user owns all the files and processes used by the Secure Global Desktop server. The `ttaserv` user owns all the files and processes used by the Secure Global Desktop Web Server.

The Secure Global Desktop server does not require the privileges of the root user to run. The server starts as root and then downgrades to the `ttasys` user.

If you try to install the software without these users and group in place, the installation will stop without making any changes to the system and tell you what you need to do. The requirements are:

- The user names must be `ttaserv` and `ttasys`.
- The group name must be `ttaserv`.
- You can use any UID or GID you want. The UID and GID may be different.
- Both users must have `ttaserv` as their primary group.
- Both users must have a valid shell, for example `/bin/sh`.
- These accounts should be locked (`passwd -l`).

One way to create these users is with the `useradd` and `groupadd` commands, for example:

```
groupadd ttaserv
useradd -g ttaserv -s /bin/sh ttaserv
passwd -l ttaserv
```

---

## Application Connection Methods

To be able to run an application (including the default webtop applications), Secure Global Desktop needs to be able to connect to an application server and start the application. Typically this is done using telnet or SSH (Secure Shell). One of these services should be enabled before installing the Secure Global Desktop.

If you are using SSH, you must enable X11 forwarding in your SSH configuration. The Secure Global Desktop Administration Guide has details on using SSH with Secure Global Desktop.

---

## Installing Sun Secure Global Desktop Software

Sun Secure Global Desktop Software contains several installable components.

The component installed on **hosts** provides the main functionality of Secure Global Desktop:

- [Installing Secure Global Desktop on Solaris OS Platforms](#)
- [Installing Secure Global Desktop on Linux Platforms](#)

The components installed on **application servers**, called Enhancement Modules, are used to provide additional functionality for Secure Global Desktop, for example load balancing or client drive mapping:

- [Installing the Secure Global Desktop Enhancement Module for Microsoft Windows](#)
- [Installing the Secure Global Desktop Enhancement Module for UNIX](#)
- [Installing the Secure Global Desktop Enhancement Module for Linux](#)

The components installed on **client devices** allow users to connect to Secure Global Desktop. Usually these components are installed automatically when users connect to Secure Global Desktop. This requires a web browser with Java™ technology enabled. If your organization prefers not to use Java technology, or you want more control over where the Secure Global Desktop Client is installed, you can install the Sun Secure Global Desktop Client manually:

- [Installing the Secure Global Desktop Client on Microsoft Windows Platforms](#)
- [Installing the Secure Global Desktop Client on Solaris OS and Linux Platforms](#)

If you are using the *classic webtop*, you can use a manually installable Native Client instead of the Java technology client:

- [Installing the Native Client for Microsoft Windows](#)

- [Installing the Native Client for UNIX/Linux](#)
  - [Installing the Native Client for Mac OS X](#)
- 

## Installing Secure Global Desktop on Solaris OS Platforms

On the Solaris™ Operating System (Solaris OS), you install Secure Global Desktop with the `pkgadd` command.

If the installation file is compressed, you need to expand it before installing.

If you are upgrading, read the [upgrade instructions](#) **before** installing the software.

By default, the software is installed in `/opt/tarantella`, but the installation program will prompt you for the installation directory when you install the software.

1. Log in as root.
2. Install Secure Global Desktop:

```
pkgadd -d /full_path/ttaarch.pkg
```

where *arch* is `i386` for Solaris OS on x86 platforms and `sps60` is for Solaris OS on SPARC® platforms.

When you install Secure Global Desktop, Setup:

- Asks you to agree to the Software License Agreement.
- Presents a list of recommended settings, which you can accept or change. If a web server is currently running on port 80/tcp, Setup asks you which port to use for the Secure Global Desktop Web Server.
- Installs and configures the software. This includes creating an organizational hierarchy with some sample applications, and making the root user a Secure Global Desktop Administrator.
- Adds files to the appropriate system start-up directory to ensure that the Secure Global Desktop server and the Secure Global Desktop Web Server start when the system reboots. Assuming you install the software in run level 3, these files will be in `/etc/rc.d/rc3.d` and named `*Tarantella` and `*TarantellaWebServer`.
- Modifies root's `crontab` to archive the Secure Global Desktop log files weekly.

When Setup has finished installing, Secure Global Desktop and the Secure Global Desktop Web Server will be running.

If the installation fails with a `pwd: cannot determine current directory!` error message, change to the `/tmp` directory and try again.



After you have installed the software, you should verify that the Secure Global Desktop package has registered in the package database by running the following command:

```
pkginfo | grep -i tta
```

---

## Installing Secure Global Desktop on Linux Platforms

On Linux, you install Secure Global Desktop with the `rpm` command.

If you are upgrading, read the [upgrade instructions](#) **before** installing the software.

By default, the software is installed in `/opt/tarantella`, but you can choose a different installation directory by using the `--prefix` option when you install the software.

1. Log in as root.

2. Install Secure Global Desktop:

```
rpm -Uvh tta-version.i386.rpm
```

3. Start the Secure Global Desktop server by running the following command:

```
/opt/tarantella/bin/tarantella start
```

When you start the Secure Global Desktop server for the first time, the installation program, Secure Global Desktop Setup, automatically starts. Setup:

- Asks you to agree to the Software License Agreement.
- Presents a list of recommended settings, which you can accept or change. If a web server is currently running on port 80/tcp, Setup asks you which port to use for the Secure Global Desktop Web Server.
- Installs and configures the software. This includes creating an organizational hierarchy with some sample applications, and making the root user a Secure Global Desktop Administrator.
- Adds files to the appropriate system start-up directory to ensure that the Secure Global Desktop server and the Secure Global Desktop Web Server start when the system reboots. Assuming you install the software in run level 3, these files will be in `/etc/rc.d/rc3.d` and named `*Tarantella` and `*TarantellaWebServer`.
- Modifies root's `crontab` to archive the Secure Global Desktop log files weekly.
- Adds a Secure Global Desktop PAM configuration file, `/etc/pam.d/tarantella`. This is copied from the existing `/etc/pam.d/passwd` file. If this file does not exist, the PAM configuration file is not created.

When Setup has finished, the Secure Global Desktop server and the Secure Global Desktop Web Server will be running.

After you have installed the software, you should verify that the Secure Global Desktop package has

registered in the package database by running the following command:

```
rpm -qa | grep -i tta
```

---

## Installing the Secure Global Desktop Enhancement Module for Microsoft Windows

The Secure Global Desktop Enhancement Module for Microsoft Windows contains modules for client drive mapping, load balancing and seamless windows.

By default, the Enhancement Module is installed in `C:\Program Files\Tarantella\Enhancement Module`, but the installation program will prompt you for the installation directory.

1. Log in to the Windows host as a user with administrator privileges.
  2. Save the Enhancement Module installation program (`temwin32.exe`) to a temporary directory.
    - o If you are not installing from the CD, you can download the installation program from a Secure Global Desktop server from:  
`http://server.example.com`.
  3. Double-click `temwin32.exe` to install the Enhancement Module.
  4. Follow the instructions on your screen. **Note** You can install an individual module or install all modules.
- 

## Installing the Secure Global Desktop Enhancement Module for UNIX

The Secure Global Desktop Enhancement Module for UNIX contains modules for client drive mapping and load balancing.

You install the Enhancement Module with the `pkgadd` command.

If the installation file for the Enhancement Module is compressed, you need to expand it before installing.

By default, the Enhancement Module is installed in `/opt/tta_tem`, but the installation program will prompt you for the installation directory.

1. Log in as root on the host.
2. Save the Enhancement Module installation program (`temi3so.pkg` for Solaris OS on x86 platforms and `temspso.pkg` for Solaris OS on SPARC platforms) to a temporary directory on the application server.
  - o If you are not installing from the CD, you can download the Enhancement Module from a Secure Global Desktop server from:  
`http://server.example.com`.
3. Install the Enhancement Module:

```
pkgadd -d /full_path/temi3so.pkg for Solaris OS on x86 platforms  
pkgadd -d /full_path/temspso.pkg for Solaris OS on SPARC platforms
```

4. Follow the instructions on your screen.

**Note** The installation program adds a file to the appropriate system start-up directory to ensure that the load balancing service starts when the system reboots. Assuming you install the software in run level 3, this file will be in `/etc/rc.d/rc3.d` and named `*tem`.

---

## Installing the Secure Global Desktop Enhancement Module for Linux

The Secure Global Desktop Enhancement Module for Linux contains modules for client drive mapping and load balancing.

You install the Enhancement Module with the `rpm` command.

By default, the Enhancement Module is installed in `/opt/tda_tem`, but you can choose a different installation directory by using the `--prefix` option when you install.

1. Log in as root on the application server.
2. Save the Enhancement Module installation program (`temversion.i386.rpm`) to a temporary directory on the application server.
  - o If you are not installing from the CD, you can download the program from a Secure Global Desktop server from:  
`http://server.example.com`.

3. Install the Enhancement Module:  

```
rpm -Uvh temversion.i386.rpm
```

**Note** The installation program adds a file to the appropriate system start-up directory to ensure that the load balancing service starts when the system reboots. Assuming you install the software in run level 3, this file will be in `/etc/rc.d/rc3.d` and named `*tem`.

---

## Installing the Secure Global Desktop Client on Microsoft Windows Platforms

The Sun Secure Global Desktop Client is installed automatically when you connect to Secure Global Desktop using a web browser with Java technology enabled. Only follow these instructions if you want to *manually* install the Client.

By default, the Secure Global Desktop Client is installed in `C:\Program Files\Sun\Secure Global Desktop Client`, but you can choose a different installation directory when you install the software. When you install, a shortcut for the Client is added to the Windows Start Menu.

1. Download the Client Setup program (`sgdcwin-lang.exe`) to a temporary directory on your PC.
  - o In a web browser, go to `http://server.example.com`
  - o Select your preferred language by clicking one of the flags at the top of the page.
  - o Click Install the Sun Secure Global Desktop Client.
2. Browse to the temporary directory and double-click `sgdcwin-lang.exe`.
3. Follow the instructions on your screen.

To log in to Secure Global Desktop, you can launch the Secure Global Desktop Client as part of the installation or click on the Secure Global Desktop Login shortcut in the Start Menu.

The first time you start the Secure Global Desktop you are prompted for the following information:

- The Server URL. This is `http://server.example.com/sgd`
- Proxy settings. The settings can be determined from your default web browser (requires Java technology) or you can enter them.

---

## Installing the Secure Global Desktop Client on Solaris OS and Linux Platforms

The Sun Secure Global Desktop Client is installed automatically when you connect to Secure Global Desktop using a web browser with Java technology enabled. Only follow these instructions if you want to *manually* install the Client.

By default, the Secure Global Desktop Client is installed in `$HOME/bin`, but you can choose a different installation directory when you install the software.

1. Download the Client Setup program to a temporary directory on your system.
  - o In a web browser, go to `http://server.example.com`
  - o Click Install the Sun Secure Global Desktop Client.
2. Browse to the temporary directory and extract the tar file by typing one of the following at the command prompt:
  - o `tar xvf sgdc13li.tar` on Linux x86 32-bit platforms
  - o `tar xvf sgdc13so.tar` on Solaris OS on x86 platforms
  - o `tar xvf sgdcspso.tar` on Solaris OS on SPARC platforms
3. Install the Client by typing `sh sgdc/install`.
4. Follow the instructions on your screen.

To log in to Secure Global Desktop, you run the `ttatcc` command.

The first time you start the Secure Global Desktop Client you are prompted for the following information:

- The Server URL. This is `http://server.example.com/sgd`
  - Proxy settings. The settings can be determined from your default web browser (requires Java technology) or you can enter them.
- 

## Installing the Native Client for Microsoft Windows

By default, the Native Client is installed in `C:\Program Files\Tarantella\Sun Secure Global Desktop Native Client`, but you can choose a different installation directory when you install the software.

1. Copy the Client Setup program (`tncwin32.exe`) to a temporary directory on your PC.
    - If you are not installing from the CD, you can download the program from a Secure Global Desktop server from:  
`http://server.example.com`
  2. Browse to the temporary directory and double-click `tncwin32.exe`.
  3. Follow the instructions on your screen.
- 

## Installing the Native Client for UNIX/Linux

By default, the Native Client is installed in `$HOME/bin`, but you can choose a different installation directory when you install the software.

1. Copy the Client tar file to a temporary directory on your system.
    - If you are not installing from the CD, you can download the file from a Secure Global Desktop server from:  
`http://server.example.com`
    - The file is:
      - `tnci3li.tar` for Linux x86 32-bit platforms
      - `tncspso.tar` for Solaris OS on SPARC platforms
      - `tnci3so.tar` for Solaris OS on x86 platforms
  2. At a command prompt, extract the tar file by typing `tar xvf <tar file> .`
  3. Install the Native Client by typing `sh ttwebtop/install.`
- 

## Installing the Native Client for Mac OS X

1. Copy the Client disk image file (`tncppdw.dmg`) to a temporary directory on your Macintosh.
    - o If you are not installing from the CD, you can download the file from a Secure Global Desktop server from:  
`http://server.example.com`
  2. Open (mount) the disk image.
  3. Drag the Secure Global Desktop Client application to your desktop or hard drive.
- 

## Upgrading Sun Secure Global Desktop Software

To upgrade Sun Secure Global Desktop Software you can either uninstall Secure Global Desktop and install the new version or you can perform an "in-place" upgrade. If you perform an "in-place" upgrade, your current configuration is usually preserved when you upgrade. The following instructions apply to "in-place" upgrades.

**Note** the directory paths listed in this section assume the software is installed in the default `/opt/tarantella` directory.

- [Upgrades and Early Access Program \(EAP\) Software](#)
  - [Upgrading an Evaluation Version of Secure Global Desktop](#)
  - [Conditions for Upgrading to Version 4.3](#)
  - [Before You Upgrade on Solaris OS Platforms](#)
  - [Before You Upgrade from 4.2 on Linux Platforms](#)
  - [Upgrading a Fully Licensed Single-server Array](#)
  - [Upgrading a Fully Licensed Multiple-server Array](#)
  - [Upgrading the Secure Global Desktop Web Server](#)
  - [Upgrading the Secure Global Desktop Enhancement Module](#)
  - [Upgrading Secure Global Desktop Clients](#)
  - [The Changes Secure Global Desktop Makes During the Upgrade](#)
  - [Upgrading a Customized Secure Global Desktop Installation](#)
- 

### Upgrades and Early Access Program (EAP) Software

Upgrades to or upgrades from EAP releases of Secure Global Desktop software are not supported. EAP releases must always be "clean" installs.

---

### Upgrading an Evaluation Version of Secure Global Desktop

If a Secure Global Desktop server is in evaluation mode or expired evaluation mode, you upgrade by installing the next version of Secure Global Desktop.

A server that was in expired evaluation mode remains in expired evaluation mode after the upgrade. You cannot log in to a Secure Global Desktop server when it is in expired evaluation mode. To license a server when it is in expired evaluation mode, you must either add a valid license key (using the `tarantella license add` command) or join the server to an array that is already fully licensed.

---

### Conditions for Upgrading to Version 4.3

Upgrades to version 4.3 are only supported from the following versions of Secure Global Desktop:

- Sun Secure Global Desktop Software version 4.2
- Tarantella Secure Global Desktop version 3.42

If you want to upgrade from any other version of Secure Global Desktop, or from Tarantella Enterprise 3 version 3.3 or earlier, contact Support.

You can only upgrade from Secure Global Desktop version 3.42 if **both** of the following are true:

- The server is fully licensed.
- You have a valid maintenance subscription **or** you have bought the right to upgrade.  
A valid maintenance subscription means you have installed sufficient maintenance keys for your product keys before trying to upgrade.  
If you have bought the right to upgrade, you must install the Right to upgrade key before trying to upgrade.

If you upgrade from version 4.1 or earlier, your license keys will be upgraded when you install version 4.3. Use the `tarantella license list` command to list your new license keys. **Make a note of them and keep them somewhere safe.**

---

### Before You upgrade on Solaris OS Platforms

Before you upgrade on Solaris OS platforms, create an installation administration file (for example, `/tmp/pkgadmin`) with the following contents:

```
conflict=nocheck
```

When you install Secure Global Desktop, use the `-a file` option to specify the administration file, for example:

```
pkgadd -a /tmp/pkgadmin -d /full_path/ttaarch.pkg
```

---

## Before You Upgrade from 4.2 on Linux Platforms

On Linux platforms, if you are upgrading from **version 4.2**, you must manually uninstall all optional packs before upgrading.

To list all the packs that have been installed, run the following command:

```
rpm -qa | grep -i tta
```

To remove all optional packs, run the following command:

```
rpm -e pack ...
```

for example `rpm -e ttasecure tta3270` removes the Security Pack and the Mainframe Connectivity Pack.

---

## Upgrading a Fully Licensed Single-server Array

To upgrade a fully licensed array containing a single server:

1. Make sure there are no webtop and emulator sessions running in the array, including suspended sessions.
  2. Upgrade the server by installing Secure Global Desktop.
- 

## Upgrading a Fully Licensed Multiple-server Array

As Secure Global Desktop servers in an array share configuration information, all servers in an array must run on the same major/patch (4.3x) version of Secure Global Desktop. This means that to upgrade a multiple-server array, you must dismantle the array and upgrade each server independently.

To upgrade a fully licensed array containing multiple servers:

1. Make sure there are no webtop and emulator sessions running in the array, including suspended sessions.
2. Dismantle the array.
  - On the **primary server**, use the `tarantella array detach --secondary server` command to detach the secondary servers.
  - Only detach one server at a time.
  - Wait for the array change to be copied to all members of the array before detaching any more servers. You can tell that this has happened when the `tarantella status`



command returns the same result when you run it on each array member.

- When a secondary is detached from an array it loses its license keys.
3. Upgrade the primary server by installing Secure Global Desktop.
  4. Upgrade the secondary servers by installing Secure Global Desktop.
  5. Rebuild the array.
    - On the **primary server**, use the `tarantella array join --secondary server` command to add the secondary servers.
    - Only add one server at a time.
    - Wait for the array change to be copied to all members of the array before adding any more servers. You can tell that this has happened when the `tarantella status` command returns the same result when you run it on each array member.
- 

## Upgrading the Secure Global Desktop Web Server

When you upgrade, you upgrade the Secure Global Desktop Web Server. If you customized any of the files used by the Secure Global Desktop Web Server, these will be preserved when you upgrade:

- For Apache, in `/opt/tarantella/var/webserver/apache/<oldversion>`.
- For Tomcat, in `/opt/tarantella/var/webserver/tomcat/<oldversion>`.

You have to manually copy your customizations to the new Apache/Tomcat directories.

---

## Upgrading the Secure Global Desktop Enhancement Module

To upgrade the Secure Global Desktop Enhancement Module for Windows, you uninstall the previous version and then install the new version.

To upgrade the Secure Global Desktop Enhancement Module for UNIX/Linux, you first [stop all services provided by the Enhancement Module](#) and then install the new version.

---

## Upgrading Secure Global Desktop Clients

All web browser users **must** restart their web browsers before connecting to an upgraded Secure Global Desktop server.

If you are using your own web server instead of the Secure Global Desktop Web Server, you **must** restart your web server to ensure that users receive upgraded Java archives.

Native Client users should download and install the latest version of the Client from `http://server.example.com`.

Version 4.0/4.1 versions and 4.2+ versions of the Native Client for Microsoft Windows are installed in different locations to previous versions. This means that previous versions are not uninstalled when you upgrade and will remain on the Windows Start menu. You may need to keep the previous versions to connect to Secure Global Desktop servers running older version of the software or they can be manually uninstalled.

---

## The Changes Secure Global Desktop Makes During the Upgrade

A complete copy of your ENS database (this is the storage area for all the objects in your Secure Global Desktop organizational hierarchy) is taken from the `var/ens` directory and backed up to the `var/ens.<oldversion>` directory. The backup is not changed and the existing ENS database is only changed if new objects essential to the running of Secure Global Desktop are needed.

The local/global array configuration stored in the `var/serverconfig` directory is only changed if there is a need to insert any new properties files and add new attributes to existing properties. This directory is **not** backed up.

All the server resources files in the `var/serverresources` directory are replaced. These files are not normally edited as they control how Secure Global Desktop works.

The Secure Global Desktop login scripts contained in the `var/serverresources/expect` directory is backed up to `var/serverresources/expect.<oldversion>`.

If you have customized Secure Global Desktop by changing the files found in a standard installation (for example, webtop themes) or by adding your own files (for example, Expect scripts), these are not upgraded. You may have to upgrade these files manually. When you install the new version of Secure Global Desktop, Setup warns you if there are files which may need to be upgraded manually and displays a list of log files to help you identify them. See [Upgrading a Customized Secure Global Desktop Installation](#) for advice on how to upgrade these files.

---

## Upgrading a Customized Secure Global Desktop Installation

When you upgrade your version of Secure Global Desktop, the Setup program will preserve your existing configuration, but it does not upgrade any customized files.

There are two types of customized files that may need attention after you have upgraded:

- **Customized files** - these are files found in a standard Secure Global Desktop installation which have been changed by an Administrator, for example by adapting standard webtop themes or Expect scripts.
- **Bespoke files** - these are files your organization has created and added to a Secure Global Desktop installation, for example your own webtop themes and Expect scripts.

**Note** The following information assumes you have installed Secure Global Desktop in its default location, `/opt/tarantella`.

## What Happens to Customized Files During the Upgrade

During installation, Setup creates a backup of all **customized files**, including login scripts, by moving the standard Secure Global Desktop files in the following directories (and the subdirectories within them):

- `var/docroot`  
moved to `var/docroot.<oldversion>`.
- `var/serverresources/expect`  
moved to `var/serverresources/expect.<oldversion>`.
- `etc/data`  
moved to `etc/data.<oldversion>`.
- `etc/templates`  
moved to `etc/templates.<oldversion>`.

This means that immediately after an upgrade, your customizations will not be active. These customizations need to be manually upgraded.

Secure Global Desktop Setup leaves **bespoke files** in their current location and does not attempt to upgrade them. These files need to be manually upgraded.

## Finding Your Customized and Bespoke Files

During the upgrade, if Setup detects that you have customized and/or bespoke files, you will see a message that says four log files have been produced:

- `var/log/upgraded.files`  
This is a summary of the changes.
- `var/log/customized.list`  
This is a list of any files that the Administrator has edited or added.
- `var/log/customizedchanged.list`  
This is a list of any files that the Administrator has edited which have been changed by the upgrade.
- `var/log/docrootjava.log`  
This is a list of new or modified Java technology files from the original installation that Secure

Global Desktop Setup has saved.

You can use these log files to identify the customized and/or bespoke files that need to be manually upgraded.

## Manually Upgrading Customized Files

The `customizedchanged.list` log file lists the customized files that may have to be manually upgraded.

For each file listed in this log file, there will be three versions of the file held on your system:

- The old, customized version, backed up in the `var/docroot.<oldversion>` directory.
- The old, uncustomized version, in the `etc/templates.<oldversion>` directory.
- The new, uncustomized version, in the `etc/templates` directory.

To upgrade your customized files:

- Create a copy of your customized files from the `var/docroot.<oldversion>` directory.
- Use a utility such as `diff` to compare the file in the `etc/templates.<oldversion>` directory with the file in the `etc/templates` directory. This will highlight the changes that have been made between Secure Global Desktop versions.
- Use a utility such as `patch` to apply the same changes to your copy of your customized files.
- Copy the upgraded customized files into the correct location under `var/docroot`.

## Manually Upgrading Bespoke Files

The `docrootjava.log` and `customized.list` log files list the bespoke files that may have to be manually upgraded.

The only way to upgrade these files is to compare versions of the standard Secure Global Desktop files to identify changes that have taken place and then apply those changes to your bespoke files.

To identify the changes, you need to compare the following files:

- The old version of the standard Secure Global Desktop files in the `etc/templates.<oldversion>` directory.
- The new version of the standard Secure Global Desktop files in the `etc/templates` directory.

Use a utility such as `diff` to compare the files in these directories. This will highlight the changes that have been made between Secure Global Desktop versions. Apply these changes to your bespoke files, for example by using a utility such as `patch`.

---

## Getting Started with Sun Secure Global Desktop Software

- [Logging in](#)
  - [Controlling Secure Global Desktop](#)
  - [Adding License Keys](#)
- 

### Logging in

1. Using a web browser with Java technology enabled, go to the following URL:

`http://server.example.com`

The Secure Global Desktop Web Server Welcome Page displays.

2. If you want, select your preferred language by clicking one of the flags at the top of the page.
3. Click Log in.

You may see a Java security message. Click Run to install the Sun Secure Global Desktop Client.

4. When the Untrusted Initial Connection message displays, check that the hostname is correct and click OK.
5. When the Secure Global Desktop login page displays, log in using the username "Administrator" and the password of the UNIX/Linux root user.

The login page may take a few minutes to display the first time you visit it.

Secure Global Desktop supports several mechanisms for authenticating users. By default, any user with an account on the host can log in to Secure Global Desktop using their UNIX/Linux username and password.

6. When you have logged in, the webtop displays.

The webtop lists the applications you can run and documents you can see. When you first log in, your webtop lists:

- **Array Manager, Configuration Wizard, Object Manager, Profile Editor, and Session Manager.** These are the Secure Global Desktop administration tools. They are only available on the webtops of Secure Global Desktop Administrators. Use Configuration Wizard to add users quickly and give them webtops.
- Some **sample applications** that Secure Global Desktop found on your system so you

can start using the product.

On the webtop, click Help to display the **Secure Global Desktop Administration Guide**. This is the on-line documentation for configuring and running Secure Global Desktop. Read all of the "Getting started" section as this covers all the essential information to help you get started with Secure Global Desktop.

---

## Controlling Secure Global Desktop

You control Secure Global Desktop from the command line using the `tarantella` command. This is a script installed in `/opt/tarantella/bin`. As this script is not on the standard PATH, you must use the full pathname each time you run the command, or change to `/opt/tarantella/bin` before issuing the command. Alternatively:

- Add `/opt/tarantella/bin` to the PATH:  

```
PATH=$PATH:/opt/tarantella/bin ; export PATH
```
- Create an alias:  

```
alias t=/opt/tarantella/bin/tarantella
```

There are restrictions on which users can use which commands in the family of `tarantella` commands:

- Commands which control the Secure Global Desktop Server and Secure Global Desktop Web Server can only be run by root.
- Commands for running Array Manager and Object Manager, and for creating arrays, can only be run Secure Global Desktop Administrators.
- All other commands can be run by any user in the `ttaserv` group.

Use the `usermod -G` command to make a user a member of the `ttaserv` group. The `ttaserv` group does not have to be the user's primary or effective group.

## Controlling the Secure Global Desktop Server

You control the Secure Global Desktop server using a `tarantella` command as follows:

- `tarantella start` - starts Secure Global Desktop services on a host, including printing services.
- `tarantella stop` - stops Secure Global Desktop services on a host, prompting if users are currently connected.
- `tarantella restart` - stops and then restarts Secure Global Desktop services on a host.

## Controlling the Secure Global Desktop Web Server

You control the Secure Global Desktop Web Server using the `tarantella webserver` command as follows:

- `tarantella webserver start` - starts the web server.
- `tarantella webserver stop` - stops the web server.
- `tarantella webserver restart` - stops and then restarts the web server.

### Controlling the Secure Global Desktop Enhancement Module for Windows

When you install the Secure Global Desktop Enhancement Module for Windows, the load balancing service starts immediately. The load balancing service also starts automatically whenever the server is rebooted. You can also manually stop and start the load balancing service, as follows:

1. Log in to the Windows server as a user with administrator privileges.
2. In Control Panel, open Administrative Tools and click Computer Management.
3. In the tree, open Services and Applications and then click Services.
4. Select the Secure Global Desktop Load Balancing Service and right-mouse click.
5. Select Stop or Start.

### Controlling the Secure Global Desktop Enhancement Module for UNIX/Linux

When you install the Secure Global Desktop Enhancement Module for UNIX/Linux, you must manually start the services that it provides. The load balancing service also starts automatically whenever the server is rebooted. The client drive mapping service must always be manually started.

You control the Enhancement Module by running the following commands as root:

- `install_dir/bin/tem start` - starts the load balancing service.
- `install_dir/bin/tem stop` - stops the load balancing service.
- `install_dir/bin/tem startcdm` - starts the client drive mapping service.
- `install_dir/bin/tem stopcdm` - stops the client drive mapping service.

By default, `install_dir` is `/opt/tta_tem`.

The first time you start the load balancing service, you will be asked to confirm the amount of virtual memory the server has.

---

### Adding License Keys

By default, Secure Global Desktop installs in a 30-day evaluation mode. During this trial period:

- The size of an array is limited to 2 Secure Global Desktop servers.
- The number of users that can log in or have running emulator sessions is limited to 5.

After 30 days the Secure Global Desktop server no longer allows users to log in.

To continue using Secure Global Desktop, you must add a license key. You can add license keys:

- On the License Properties panel in Array Manager.
  - On the command line, with the `tarantella license add license_key` command.
- 

## Removing Sun Secure Global Desktop Software

- [Uninstalling Secure Global Desktop](#)
  - [Uninstalling the Secure Global Desktop Enhancement Module for Windows](#)
  - [Uninstalling the Secure Global Desktop Enhancement Module for UNIX/Linux](#)
- 

### Uninstalling Secure Global Desktop

To remove Secure Global Desktop from your system:

1. Log in as root.
2. Run the following command:  

```
tarantella uninstall --purge.
```

**Note** the `tarantella uninstall` command is the only supported method for removing Secure Global Desktop. This command stops all Secure Global Desktop processes before removing the software. Do not use the `rpm` or `pkgrm` commands directly to remove the software.

---

### Uninstalling the Secure Global Desktop Enhancement Module for Windows

You uninstall the Secure Global Desktop Enhancement Module for Windows by selecting Add/Remove programs from Microsoft Windows Control Panel.

You must have Administrator privileges to do this.



**Note** You can also uninstall individual modules.

---

## Uninstalling the Secure Global Desktop Enhancement Module for UNIX/Linux

To uninstall the Secure Global Desktop Enhancement Module on UNIX/Linux platforms:

1. Log in as root.
  2. Uninstall the Enhancement Module by running one of the following commands:
    - o `rpm -e tem` on Linux platforms
    - o `pkgrm tem` on Solaris platforms
- 

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties. Sun, Sun Microsystems, the Sun logo, Java and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries.

UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Copyright © 1997-2006 Sun Microsystems, Inc. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

L'utilisation est soumise aux termes du contrat de licence.

Cette distribution peut comprendre des composants développés par des tierces parties.

Sun, Sun Microsystems, le logo Sun, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays.

UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

## Introducing Sun Secure Global Desktop Software

### Read this topic to...

- Learn what Sun Secure Global Desktop Software can do.

Sun Secure Global Desktop Software provides you with secure, remote access to desktop applications running on application servers. It instantly web-enables existing Windows, UNIX, Linux, Mainframe, and AS/400 applications without the need for rewriting any application code.

Secure Global Desktop uses a [three-tier model](#), in which the Secure Global Desktop server is independent of the clients and the application servers. Users can access Secure Global Desktop from a wide range of client devices across everything from a LAN to a dial-up modem connection. Application servers require little or no configuration to work with Secure Global Desktop.

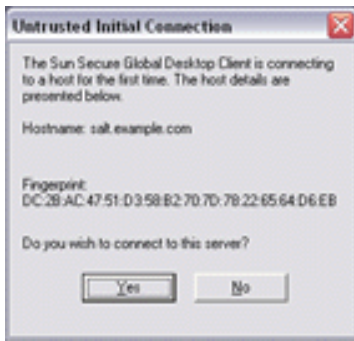
Secure Global Desktop Administrators are in control of security. They control which users can access which applications, using SSL-based secure connections if needed. Each user has their own webtop which provides access to the applications they're authorized to use.

Administration uses the directory services model, with objects representing the people, applications, documents and application servers in your organization. These can be arranged in a hierarchy that mirrors the structure of your organization.

For scalability and load balancing, Secure Global Desktop servers can be grouped into an array. This allows them to share information about users, applications, and usage information. In effect, an array acts as one, larger, server. Secure Global Desktop servers can be administered from any member of the array.

### Logging in to Secure Global Desktop

To log in to Secure Global Desktop, users start a web browser (Java™ technology must be enabled) and go to the `http://server.example.com/sgd` URL. Opening this URL shows a splash screen. If a Java Security Warning dialog displays, users must click Run to allow the Secure Global Desktop Client to be installed and started. When the Secure Global Desktop Client connects to a Secure Global Desktop server for the first time, a security message displays.



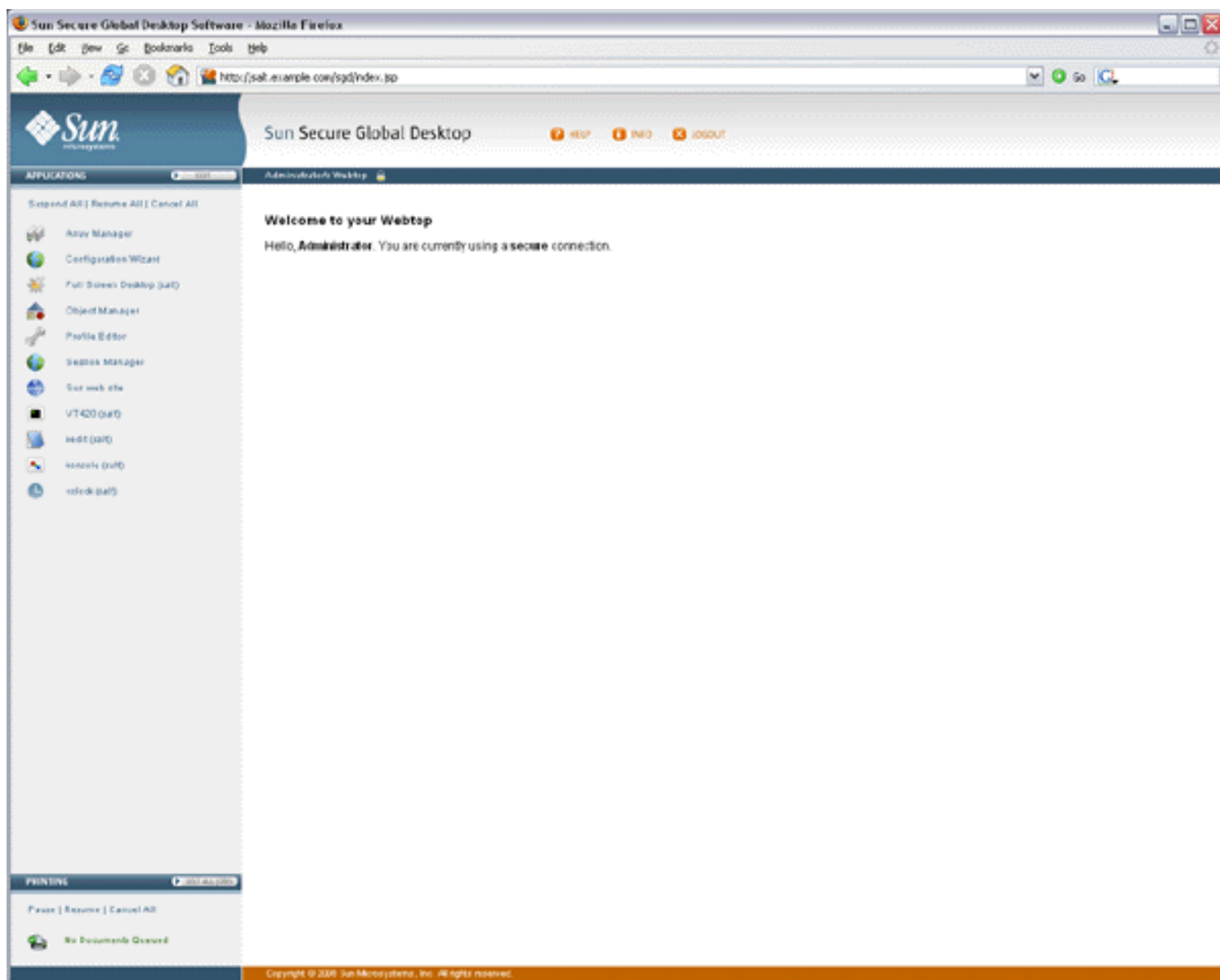
Users should check the hostname and fingerprint details before clicking Yes to agree to the connection. Once they have agreed to the connection, the Secure Global Desktop Client will not prompt when connecting to this host again.

Next the login page displays where users type their username and password for the Secure Global Desktop server.



Secure Global Desktop has a flexible authentication mechanism, allowing different user types to log in to Secure Global Desktop in different ways. By default, Secure Global Desktop is configured to allow users with an account on the UNIX host to log in with their UNIX username and password. All UNIX users see the same webtop. When you install Secure Global Desktop, Setup creates a default Secure Global Desktop Administrator with the username "Administrator". This user authenticates using the password of the UNIX root user on the host.

Once a user is authenticated, their webtop displays:



The Applications area of the webtop lists the applications that the user can run. When Secure Global Desktop is first installed, the Applications area contains a few sample applications. Secure Global Desktop Administrators have extra links for the Secure Global Desktop administration tools: Array Manager, Configuration Wizard, Object Manager, Profile Editor, and Session Manager.

## Running applications

To start an application, click its link on the webtop.



When a user starts an application, they may be asked for a username and password. This is authentication information for the application server which is running the application. These details can be cached securely so the user does not need to enter them more than once for each application server.

Secure Global Desktop Administrators configure how the applications appear. Some may appear on the webtop

and others in a separate window.

When an application is running, a triangle appears in front of the application's name on the webtop and a number appears in brackets after it. The session toolbar also appears below the application name.



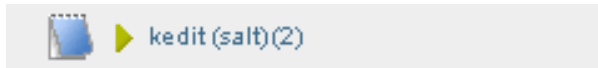
The number in brackets is the number of separate instances of the application the user has started. Secure Global Desktop Administrators configure how many instances of an application users can run.

There is a separate session toolbar for each running instance of the application:

- Click **||** to suspend an application.
- Click **▶** to resume an application.
- Click **✖** to end an application.

**Note** Suspending and resuming applications is explained below.

Click the triangle to hide and show the session toolbars for the application sessions.



You can manage all your application sessions at once:




- Click Suspend All to suspend all running applications.
- Click Resume All to resume all suspended applications.
- Click Cancel All to end all running or suspended applications.

## Suspending and resuming applications

Some applications can be configured to keep running even when they're not displayed. These are "resumable" applications.

Applications can have one of three resumability settings:

Setting	Description
---------	-------------

Not resumable	The application exits when the user logs out of Secure Global Desktop. You cannot suspend or resume, non-resumable applications.
Resumable until log out	The application continues to run until the user logs out of Secure Global Desktop. While they are logged in, the user can suspend and resume these applications.
Always resumable	The application continues to run even after the user has logged out of Secure Global Desktop. When they log in again, they click the resume button  to display the running application again.

To close an application's window without ending the application, you *suspend* the application. To display the window again and start using the application, you *resume* the application.

## Using groups

Only a Secure Global Desktop Administrator can add an application to, or remove an application from, the list of applications that users can run. However, users can "personalize" their webtop by arranging their list of applications into groups. The user decides how and when the groups display. Groups are useful for keeping similar applications together or for hiding applications not used very often.

By clicking the Edit button in the Applications area of the webtop and then clicking the Edit Groups tab, users can add or edit their groups. Users can have as many groups as they like.

## Editing profiles

By clicking the Edit button in the Applications area of the webtop and then clicking the Client Settings tab, users can configure the Secure Global Desktop Client, see [Profiles and the Sun Secure Global Desktop Client](#) for details.

## Printing

Users can manage printing from the [Printing area on the webtop](#).

## Logging out

You should always log out of Secure Global Desktop before closing your web browser. This lets Secure Global Desktop shut down any applications that need not run any more and makes sure nobody can use a user's applications in their name without permission.

If someone closes their web browser without logging out (or if their web browser crashes), they are not logged out of Secure Global Desktop. The user can log in to Secure Global Desktop again and can resume applications configured to be Webtop session resumable or Always resumable.

To log out of Secure Global Desktop, click the Logout button on your webtop and click OK when prompted for confirmation.

## Related topics

- [Users and trusted Secure Global Desktop servers](#)
- [Integrating Secure Global Desktop with the desktop Start Menu](#)
- [Working with the Sun Secure Global Desktop Client](#)
- [Profiles and the Sun Secure Global Desktop Client](#)
- [Securing client connections with Secure Global Desktop security services](#)

## Integrating Secure Global Desktop with the desktop Start Menu

### Read this topic to...

- Understand how to access Secure Global Desktop from the client desktop Start Menu
- Understand the differences between Webtop mode and Integrated mode

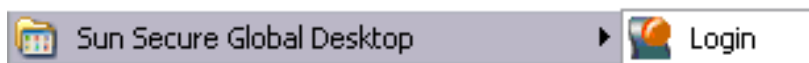
When users first connect to a Secure Global Desktop server, they usually start a web browser and go the `http://server.example.com/sgd` URL. Here they [log in and display a webtop](#). However, once users have logged in, the Sun Secure Global Desktop Client can be [configured to operate in Integrated mode](#).

When the Secure Global Desktop Client operates in Integrated mode, the links for starting applications display in the desktop Start Menu instead of on the webtop so that users can run remote applications in the same way as local applications. Depending on how you configure Start Menu integration, there may be no need to use a web browser.

**Note** Integrated mode is the recommended mode if your organization prefers [not to use Java™ technology on the client device](#). Integrated mode is not available for the *classic* webtop.

### Working in Integrated mode

When the Secure Global Desktop Client is in Integrated mode, the user logs in to Secure Global Desktop by clicking the Login link on their desktop Start Menu.

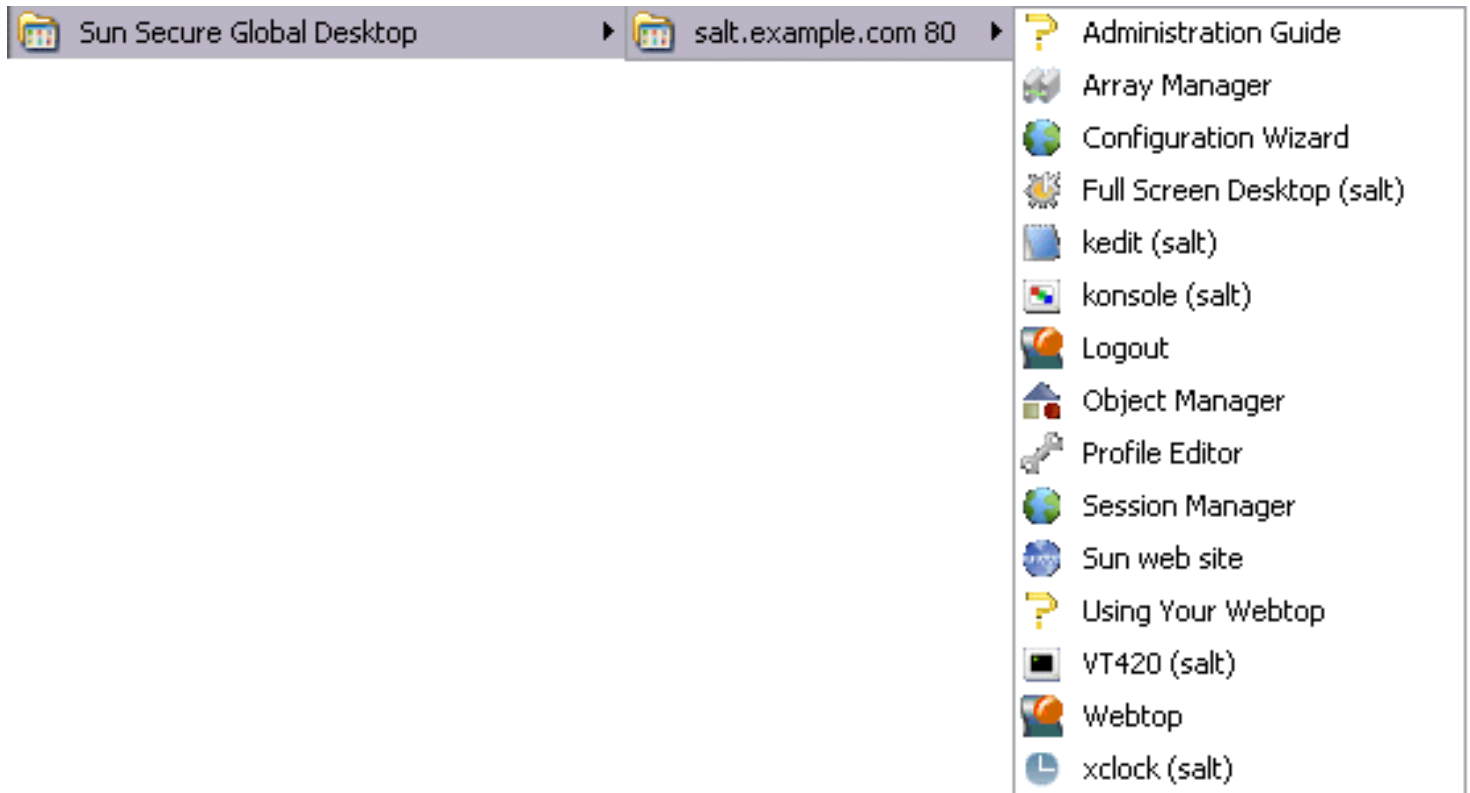


If the user has logged in to more than one Secure Global Desktop server, there is a Login link for each server in the Start Menu. With Integrated mode, you can only be logged in to a single Secure Global Desktop server at any one time. Once the user has logged in, the Login links for other Secure Global Desktop servers are removed from the Start Menu.

**Note** To use Integrated mode, you must log in using the Start Menu. Integrated mode is not available if you start a web browser and log in.



Once the user has logged in to Secure Global Desktop, the Start Menu is updated with the links for the applications they can run through Secure Global Desktop.



To start an application, the user clicks its link on the Start Menu. To start another instance of the application, they click the link again.

Working in integrated mode simplifies session management. Unlike the webtop, there are no controls for suspending and resuming applications. Instead, when the user logs out, the Secure Global Desktop Client automatically suspends or ends all running emulator sessions. When the user logs in again, the Secure Global Desktop Client automatically resumes all suspended sessions.

When launched from the Start Menu, applications that are configured to [Display Using](#) the webtop or a new browser window are displayed in an independent window.

Users can [launch applications with a different username and password](#) by pressing and holding down the SHIFT key when clicking the link to start an application.

Printing is simplified too, printing is always "on" and print jobs go straight to the printer the user selected. Unlike the webtop, print jobs cannot be managed individually.

If the user needs to display a webtop, for example to be able to edit their profile, resume a suspended application or manage printing, they can click the Webtop link on the Start Menu. The user is not prompted to log in as they already have a webtop session. The webtop is displayed in their default web browser.

If the user has arranged any of their webtop content to [display in groups](#), those groups are also used in the Start Menu. If the group is configured to hide webtop content, the content does not display in the Start Menu.

To log out of Secure Global Desktop, the user clicks the Logout link on the Start Menu.

### Related topics

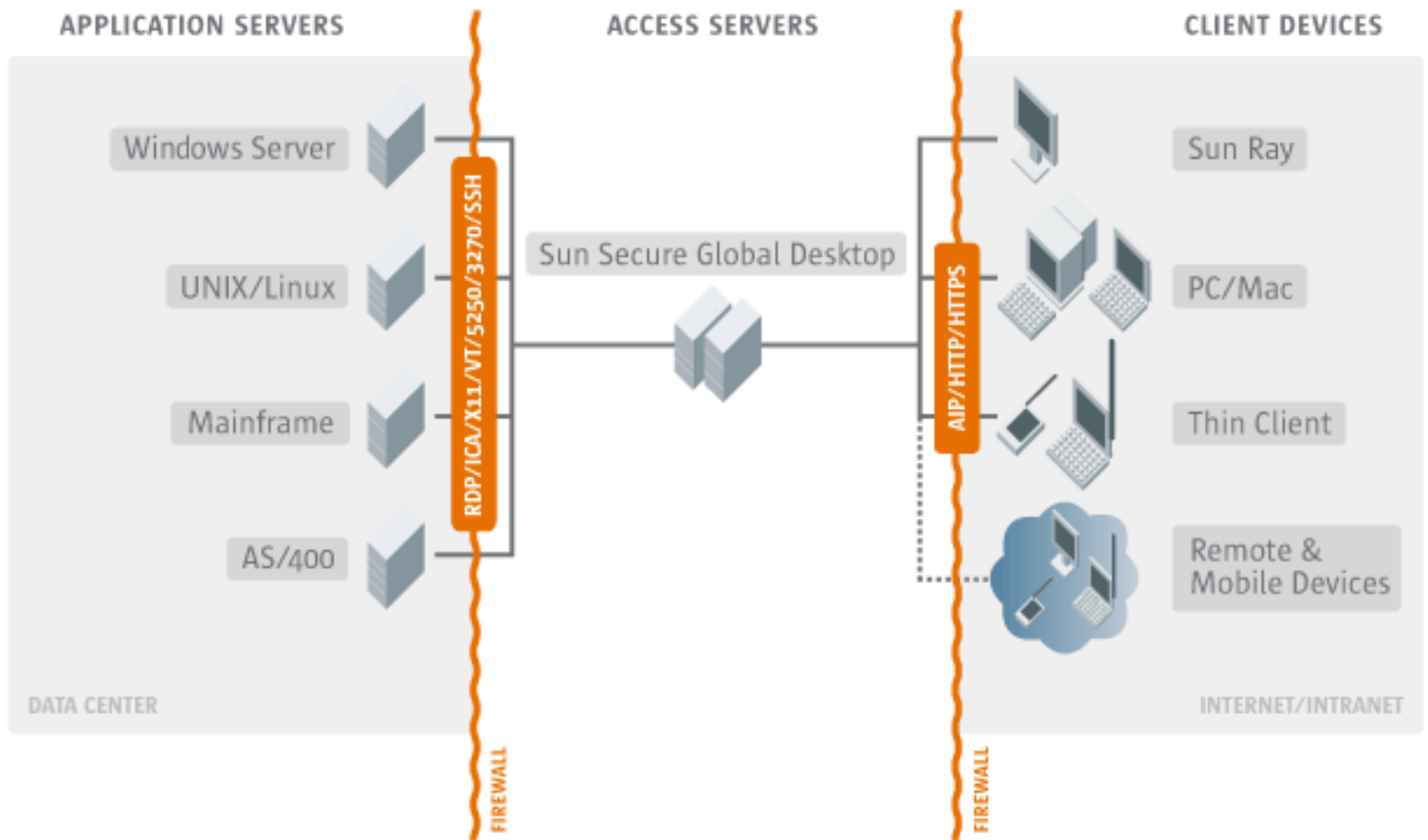
- [Configuring the Sun Secure Global Desktop Client for desktop Start Menu integration](#)
- [Introducing Sun Secure Global Desktop Software](#)
- [Working with the Sun Secure Global Desktop Client](#)
- [Profiles and the Sun Secure Global Desktop Client](#)
- [Using Secure Global Desktop with proxy servers](#)
- [Securing client connections with Secure Global Desktop security services](#)

## Introducing the three-tier architecture

### Read this topic to...

- Understand the three-tier architecture model of Secure Global Desktop.

Secure Global Desktop is built around a three-tier architecture model:



Different tiers can reside on the same host (for example, a single UNIX host can act as both a Secure Global Desktop server and an application server), but the tiers remain logically independent.

### The first tier: client devices

A *client device* is a piece of hardware that can communicate with Secure Global Desktop using a web browser and the Sun Secure Global Desktop Client.

The web browser communicates with the Secure Global Desktop Web Server on the second tier and displays the webtop to users.

The Sun Secure Global Desktop Client communicates with Secure Global Desktop servers on the second tier and displays the applications that users run.

The Adaptive Internet Protocol (AIP) ensures optimal network usage between the first and second tiers.

## The second tier: Secure Global Desktop servers

The second tier may contain a single Secure Global Desktop server, or many Secure Global Desktop servers configured to form an [array](#).

A Secure Global Desktop server is responsible for:

- Authenticating users when they log in to Secure Global Desktop.
- Negotiating with application servers to authenticate users when they run applications, prompting users for passwords when necessary.
- Causing the Sun Secure Global Desktop Client to display applications.
- Keeping track of running applications even after users have logged out, so that they can resume them later.

## The third tier: application servers

An *application server* runs users' applications.

When a user clicks a link on their webtop, Secure Global Desktop starts the application on an appropriate application server. Output from the application is redirected by the Secure Global Desktop server from the application server to the client device.

When you tell Secure Global Desktop about an application, you include information about all the application servers that may run the application. Secure Global Desktop load balances between the application servers.

## Summary

- Secure Global Desktop is based around a three-tier architecture.
- The first tier contains client devices. Web browsers let users access Secure Global Desktop and display webtops. The Sun Secure Global Desktop Client displays applications that users run.
- The second tier contains Secure Global Desktop servers, which act as a gateway between the first and third tiers.
- The third tier contains the application servers that run users' applications.

### Related topics

- [Introducing Sun Secure Global Desktop Software](#)
- [Understanding webtop and emulator sessions](#)
- [Introducing application server load balancing](#)



## Understanding webtop and emulator sessions

### Read this topic to...

- Learn what webtop sessions and emulator sessions are, and how to control them.

You can keep track of what your users are doing by monitoring the webtop sessions and emulator sessions in progress.

- A webtop session begins when a user logs in to Secure Global Desktop, and ends when the user logs out.
- An emulator session begins when a user starts an application by clicking its link on their webtop, and ends when the application exits.

### Webtop sessions

A webtop session begins when a user logs in to Secure Global Desktop. How the user logs in, the username and password they type, determines the [type of user](#) they are. In turn, this determines the behavior of the user's webtop session. There are two cases:

- For [anonymous users](#), and users logged in using a [shared \(guest\) account](#).
- For all other types of user.

Anonymous/shared account	Others
The webtop session <b>ends when a user logs out or closes their web browser.</b>	The webtop session <b>ends when a user logs out.</b>
If the user is already logged in, <b>logging in again creates a new webtop session.</b> No existing webtop sessions are affected.	If the user is already logged in, <b>logging in again will relocate the webtop session:</b> the old webtop session ends.

Webtop sessions are hosted by the Secure Global Desktop [array](#) member the user logs in to.

### Webtop session management

In [Object Manager](#), person objects, [profile objects](#) and host objects have a Sessions tab. This shows all the webtop sessions involving the object: for example, all the webtop sessions involving a particular profile object.

On the Sessions tab you can view details about each webtop session and log a user out of Secure Global Desktop by ending their webtop session.

You can also use the `tarantella webtopsession` command to manipulate webtop sessions from the command line.

## Emulator sessions

An emulator session begins when a user starts an application and usually ends only when the application exits.

As with webtop sessions, the type of user influences the behavior of emulator sessions. For anonymous or shared users, emulator sessions always end when the webtop session ends. For other users, emulator sessions may persist between webtop sessions.

An emulator session is hosted by an [array](#) member. Each emulator session has a corresponding Protocol Engine process, which communicates between the client device and the application server. The Protocol Engine converts the display protocol used by the application to the Adaptive Internet Protocol, AIP, understood by Secure Global Desktop components on the client device.

You can use [emulator session load balancing](#) to spread the load of the Protocol Engines among the Secure Global Desktop servers in the array.

Each emulator session corresponds to an application currently running through Secure Global Desktop.

## Emulator session resumability

Emulator session resumability lets users stop using an application at any time, and resume it later on any client device. The application continues running when it's not displayed, so, for example, you can start a lengthy calculation, shut down your client device, and come back to the application later from any other client device to pick up the results.

Each application object has a [Resumable](#) attribute that determines an application's resumability.

An emulator session can be suspended at any time by user action (such as closing the web browser), or through an unscheduled event such as a communications failure.

Resumable applications are useful for these reasons:

- Applications that take a long time to start can be left running even after users have logged out of Secure Global Desktop.
- Mobile users can leave applications running while they travel.
- Users can easily recover from web browser or other crashes.

## Emulator session management

In [Object Manager](#), application objects, host objects and person objects have a Sessions tab. This shows all the emulator sessions involving the object: for example, all the applications a person is running, or all those running on a particular application server.

On the Sessions tab you can view details about each emulator session, and end or shadow sessions. Shadowing a session lets you and the user see and interact with the application at the same time.

**Note** You can only shadow Windows and X applications.

You can also use the `tarantella emulatorsession` command to manipulate emulator sessions from the command line.

### Related topics

- [Introducing Array Manager](#)
- [Introducing Object Manager](#)
- [The tarantella webtopsession command](#)
- [The tarantella emulatorsession command](#)
- [Using shadowing to troubleshoot a user's problem](#)



## Introducing Array Manager

### Read this topic to...

- Learn what Array Manager is and what it can do.

Use Array Manager to perform these tasks:

- **Set up and manage an array** of Secure Global Desktop servers, for [emulator session load balancing](#).
- Configure **array-wide settings**, and **settings for each array member**.

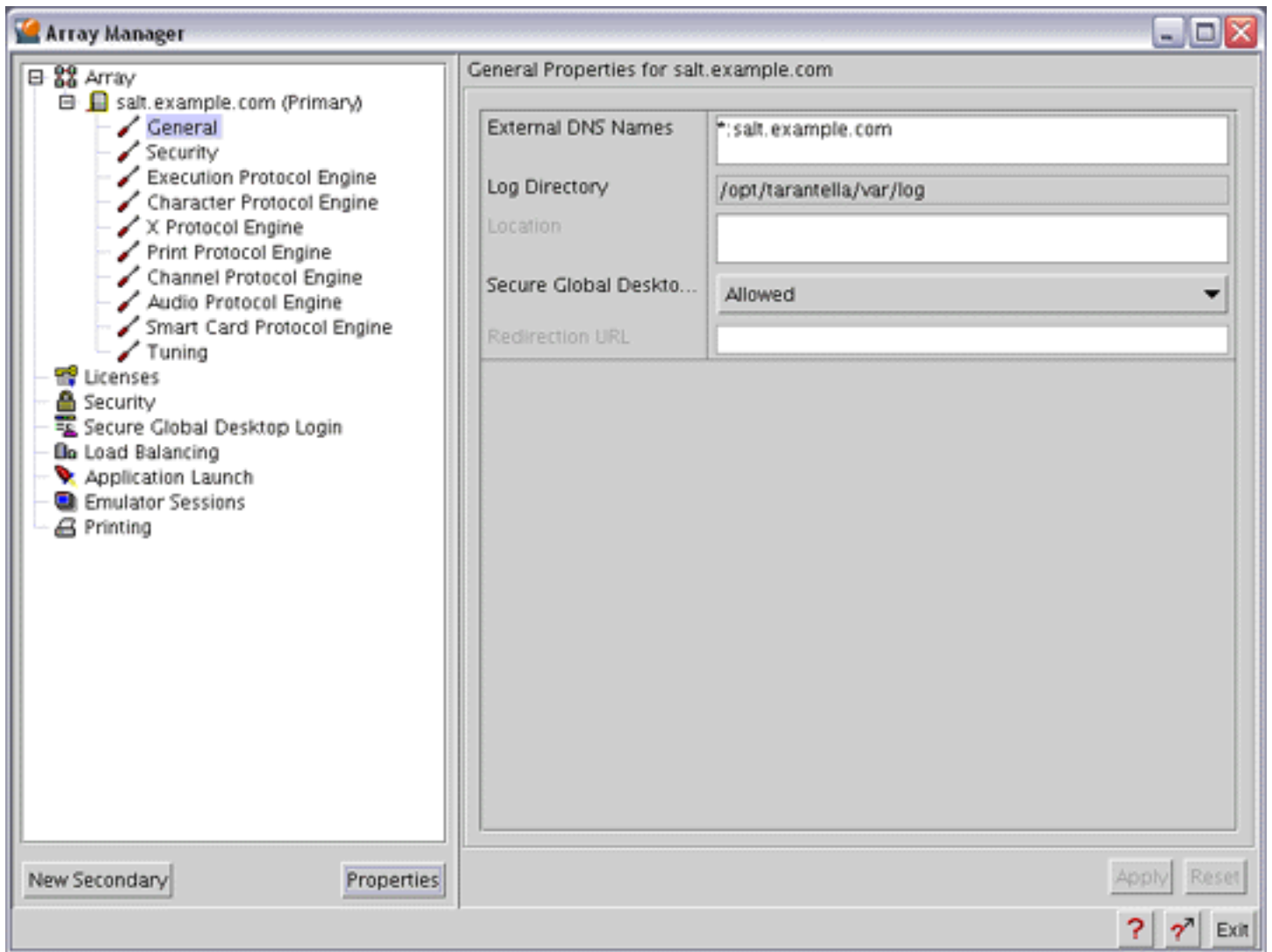
You can use command-line tools for these tasks, if you prefer. See `tarantella array` and `tarantella config` for more information.

Only [Secure Global Desktop Administrators](#) are allowed to run Array Manager.

### What you see

Array Manager has two panes, which you can resize.

- On the left, the Array pane shows the array members and all the areas you can configure.
- On the right, the Properties pane lets you configure those areas.



You can get help on any part of Array Manager: click the context help button at the lower right of the Array Manager window, and then click the part you want help on.

## The Array pane

The Array pane shows all the areas you can configure. It is arranged as a tree:

- **At the top of the tree are the array-wide properties.** Changing attributes for these affects all array members. For example, in [Secure Global Desktop Login](#) properties you can enable login authorities, which affects how users log in whatever array member they log in to.
- **Expand the Array part of the tree to show all the array members.** Choose Properties for an array member to show its current status.
- **Expand the tree for an array member to show the configurable areas for that array member.** Changing an attribute here affects only that array member.

You can also [set up and dismantle an array](#).

## The Properties pane

The Properties pane shows all the attributes you can change either for the array or for a particular Secure Global Desktop server.

For detailed information on array-wide attributes, see:

- [Application Launch properties](#)
- [Array properties](#)
- [Emulator Sessions properties](#)
- [Licenses properties](#)
- [Load Balancing properties](#)
- [Printing properties](#)
- [Security properties](#)
- [Secure Global Desktop Login properties](#)

For detailed information on server-specific attributes, see:

- [Audio Protocol Engine properties](#)
- [Channel Protocol Engine properties](#)
- [Character Protocol Engine properties](#)
- [Execution Protocol Engine properties](#)
- [General properties](#)
- [Print Protocol Engine properties](#)
- [Security properties](#)
- [Smart Card Protocol Engine properties](#)
- [Tuning properties](#)
- [X Protocol Engine properties](#)

### Related topics

- [What is an array?](#)
- [Setting up and dismantling a Secure Global Desktop array](#)
- [The tarantella array command](#)
- [The tarantella config command](#)
- [Introducing Object Manager](#)



## Introducing Object Manager

### Read this topic to...

- Learn what Object Manager is and what it can do.

Use Object Manager to perform these tasks:

- **Create and configure objects** representing the people, hosts, applications and documents within your organization.
- **Define webtops** for all users of Secure Global Desktop, and see whose webtop any object is on.
- Monitor **who's running which applications** on which application servers, and shadow or end those application sessions.
- Find out **who's cached passwords** for which application servers, and delete password cache entries.

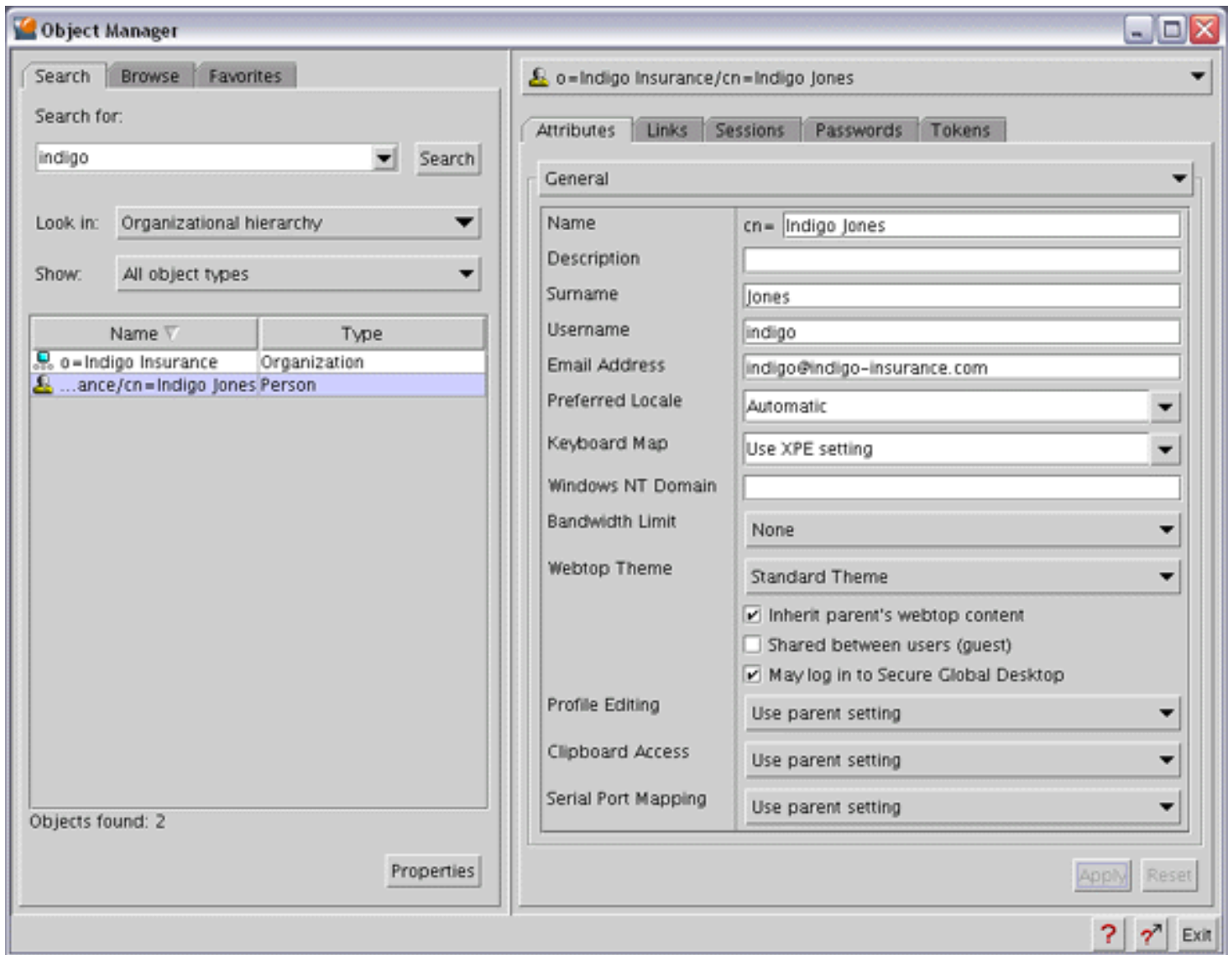
You can also use command-line tools for these tasks, if you prefer. These tools also allow you to [automate the tasks](#).

Only [Secure Global Desktop Administrators](#) are allowed to run Object Manager.

### What you see

Object Manager has two panes, which you can resize.

- On the left, the Finder pane lets you search and browse for objects to work with, and lets you remember commonly accessed objects in a list of Favorites.
- On the right, the Properties pane lets you work with the objects you locate, and lets you easily return to objects you've worked with recently.



You can get help on any part of Object Manager: click the context help button at the lower right of the Object Manager window, and then click the part you want help on.

### The Finder pane

Tab	Description
-----	-------------

Search	<ul style="list-style-type: none"> <li>● Use this tab to search all or part of the organizational hierarchy for objects matching your search criteria.</li> <li>● Type a search term in the box, and then click Search.</li> <li>● An object matches if the search term is a substring of the object's Name, Username or Email Address attribute.</li> <li>● The Search box remembers your previous searches.</li> <li>● You can constrain searches using the Look In list, which restricts the scope of the search, and the Show list, which restricts the types of object to search for.</li> <li>● To find out which <a href="#">login profile</a> could be used by someone, choose All Potential Logins from the Look In list and set the search term to the username that user would type when logging in to Secure Global Desktop.</li> </ul>
Browse	<ul style="list-style-type: none"> <li>● Use this tab to browse through the organizational hierarchy for objects.</li> <li>● You can restrict the types of object displayed, using the Show list.</li> <li>● Create new objects by clicking the organization or organizational unit object that you want the new object to belong to, and then clicking New. Alternatively, right-click an organization or organizational unit object and choose New.</li> </ul>
Favorites	<ul style="list-style-type: none"> <li>● Use this tab to remember the objects you work with often.</li> <li>● Add an object to your Favorites by dragging and dropping, or by right-clicking the object and choosing Add To Favorites.</li> </ul>

## The Properties pane

At the top of the Properties pane is a list of the objects you've viewed properties for since you started Object Manager. You can return to an object's properties by clicking it in this list.

The main part of the Properties pane shows properties for an object. Different object types have different properties, including different tabs.

Tab	Description
Attributes	<ul style="list-style-type: none"> <li>● General settings for an object. The attributes available depend on the type of object.</li> <li>● Related attributes are grouped. Use the list on the Attributes tab to move between sets of attributes.</li> <li>● Click Apply to remember any attribute changes you make.</li> <li>● To get help on an attribute, click the context help button at the lower right of the Object Manager window, and then click the attribute.</li> </ul>

Links	<ul style="list-style-type: none"> <li>• Defines the links that appear on webtops. Person objects, organizational unit objects and organization objects have Links tabs.</li> <li>• Drop objects into the box to add them to the webtop.</li> <li>• Drop a group into the box to include the members of the group on a webtop.</li> <li>• Drop an organizational unit into the box to include the contents of the OU's Links tab on a webtop.</li> <li>• Click the buttons at the bottom of the tab to show the Links tab as a tree or a table. The tree displays the groups and OUs, so you can see why a particular link appears on a webtop. The table just shows the links themselves, hiding groups and OUs.</li> </ul>
Members	<ul style="list-style-type: none"> <li>• Defines the members of a group.</li> <li>• Drop objects into the box to add them to the group.</li> <li>• As groups are often added to Links tabs to include similar webtop content on many different webtops, the Members tab lets you show group members as a tree or a table like a Links tab.</li> </ul>
Hosts	<ul style="list-style-type: none"> <li>• Defines the application servers that can run an application. All application object types have a Hosts tab.</li> <li>• The contents of an application object's Hosts tab are used for <a href="#">application server load balancing</a>.</li> <li>• Drop host objects into the box to include them in application server load balancing for the application.</li> <li>• Drop a group into the box to include the members of the group.</li> <li>• Click the buttons at the bottom of the tab to show the Hosts tab as a tree or a table. The tree displays the groups, so you can see why a particular application server is included. The table just shows the application servers themselves, hiding groups.</li> </ul>
Seen By	<ul style="list-style-type: none"> <li>• Shows, for an object, all the other objects that refer to it. You can think of this as the reverse of the Hosts or Links tab. For example: <ul style="list-style-type: none"> <li>◦ If a person has an application on their webtop, then the person object will appear on the application object's Seen By tab.</li> <li>◦ If an application may run on a particular host, then the application object appears on the host object's Seen By tab.</li> </ul> </li> <li>• Expand the tree to follow the references further. For example, if an application is a member of a group, and the group appears on three people's webtops, then the Seen By tab for the application object shows the group object, which expands to show the three person objects.</li> <li>• You can drop objects on a Seen By tab. For example, if you drop a person object on an application object's Seen By tab, this has the effect of adding the application to the person's webtop. The person object's Links tab shows the application object.</li> </ul>



Sessions	<ul style="list-style-type: none"> <li>• Shows the webtop sessions related to the person, host or <a href="#">profile objects</a> you're viewing properties for.</li> <li>• Shows the emulator sessions related to the person, host or application object you're viewing properties for.</li> <li>• For webtop sessions, the tab shows information such as the Secure Global Desktop server the user is logged in to, the type of connection the user has and the printing status of the client.</li> <li>• For emulator sessions, the tab shows information such as the application server running the application, its start time, whether it's suspended or currently running.</li> <li>• You can use this tab to end an emulator or webtop session.</li> <li>• You can also "shadow" an emulator session: this allows both you and the user to interact with the same application.</li> </ul>
Passwords	<ul style="list-style-type: none"> <li>• Shows the password cache entries related to the person or host object you're viewing properties for.</li> <li>• The table shows information about each password cache entry, including the username the person typed to log in to the application server (which isn't necessarily the same username they typed to log in to Secure Global Desktop).</li> <li>• You can delete password cache entries here.</li> </ul>

## Using Object Manager

In this section we'll show what you can do with Object Manager.

Remember that to use Object Manager you'll need to be logged in to Secure Global Desktop as a Secure Global Desktop Administrator.

### Defining webtops

Secure Global Desktop supports many different types of user, but the principle is the same for all types: **an object in the organizational hierarchy defines the webtop content**. Usually the object is directly associated with the user. For example, the user Indigo Jones might have a person object with [ENS name](#) `o=Indigo Insurance/cn=Indigo Jones`.

In Object Manager, **each person object has a Links tab**. To add applications to a user's webtop, you can drag the application objects and drop them onto the Links tab (you could also use Copy and Paste).

You can also **give users webtop content based on their position within the organizational hierarchy**: each organizational unit object has a Links tab, too. You can decide, for each person object, whether the user "inherits" webtop content from the OU they belong to, just check or clear the [Inherit Parent's Webtop Content](#) box in the person object's attributes.

**OU objects can also inherit webtop content** from their own parent in the organizational hierarchy. So a person object may include webtop content from all its ancestors in the organizational hierarchy, up to and including the organization object.

Another form of inheritance uses group objects. A group is just a collection of other objects, from anywhere in the organizational hierarchy, and an object may appear in many groups. **If you add a group object to a Links tab, the group members appear on the webtop.**

Finally, **you can inherit webtop content from any OU** and not just the parent OU. Just add the OU object to a Links tab.

By inheriting webtop content from parent objects, groups and OUs you can easily give many different users similar webtops and manage them efficiently. The Links tab lets you see where each object on a webtop is inherited from, using a tree. Alternatively you can view the webtop content as a simple table.

### Summary

1. Using the Finder pane, locate the person object or OU you want to define the webtop for.
2. Choose Properties for the object, and then click the Links tab.
3. Use the Finder pane to locate the application objects, group objects or OU objects you want to add to the webtop, and drag them onto the Links tab.
4. If you want to inherit webtop content from the parent object in the organizational hierarchy, click the Attributes tab and make sure the Inherit Parent's Webtop Content box is checked.

### Load balancing application servers

[Application server load balancing](#) lets you **spread the load of a heavily used application across multiple application servers**. Secure Global Desktop can choose an application server to help ensure optimal performance for users and optimal resource usage.

In Object Manager **each application object has a Hosts tab**. To define all the application servers the application can run on, you add host objects to the Hosts tab by dropping them on the tab, or using Copy and Paste. The Secure Global Desktop server performs application server load balancing across all the application servers defined on the application's Hosts tab.

You can **create groups with host objects as members**, and drop the groups onto the Hosts tab as well. Like the Links tab, the Hosts tab lets you see the hosts as a tree or a table.

### Summary

1. Using the Finder pane, locate the application object you want to load balance across multiple application servers.
2. Choose Properties for the object, and then click the Hosts tab.

3. Use the Finder pane to locate the host objects or group objects you want to use for load balancing, and drag them onto the Hosts tab.

## Managing webtop sessions

Person objects, [profile objects](#) and host objects all have a **Sessions tab which display the webtop sessions** involving that object. The tab shows information about the webtop session, such as:

- the name of Secure Global Desktop server the user is logged in to
- the date and time the user logged in
- the type of connection the user has and
- the printing status of the client.

You can **end webtop sessions** by selecting one or more sessions and clicking Log Out User.

You can also **move between Sessions tabs easily**. For example, when viewing the webtop sessions for a host object, you can right-click one of the sessions and choose Properties to view the person object's Sessions tab.

## Summary

1. Using the Finder pane, locate the object you want to view webtop sessions involving.
2. Choose Properties for the object, and then click the Sessions tab.
3. Select a webtop session and choose Log Out User, or right-click one of the objects involved and choose Properties.

## Managing emulator sessions

Each emulator session involves three elements: **an application, the application server** that's running the application, and **the person** who's running the application. Consequently application objects, host objects and person objects all have a **Sessions tab displaying the emulator sessions** involving that object.

The Sessions tab shows the other two elements in the emulator session. For example, the Sessions tab for a person object shows the applications that person is currently running, and the application servers they're running on. The tab also shows other information about each session, including the date and time the session started, and whether the session is suspended or currently active.

On the Sessions tab you can **end a session**, by selecting a session and clicking End Session. You can also **"shadow" a session**, which allows both you and the user to view and interact with the application simultaneously.

**Note** You can only shadow Windows and X applications.

You can also **move between Sessions tabs easily**. For example, when viewing the emulator sessions for a person object, you can right-click one of the applications involved and choose Properties to view the application object's Sessions tab -- and see who else is running the same application.

## Summary

1. Using the Finder pane, locate the object you want to view emulator sessions involving.
2. Choose Properties for the object, and then click the Sessions tab.
3. Select a session and choose End Session or Shadow Session, or right-click one of the objects involved and choose Properties.

## Managing passwords

Each password cache entry involves two elements: **a person**, and **the application server** the password is cached for. Consequently person objects and host objects both have a **Passwords tab displaying the password cache entries** involving that object.

The Passwords tab shows the other element in the password cache entry. For example, the Passwords tab for a person object shows the application servers they have cached passwords for. The tab also shows other information about each entry, including the username on the application server.

On the Passwords tab you can **delete a password cache entry**, by selecting an entry and clicking Remove.

You can also **move between Passwords tabs easily**. For example, when viewing the password cache entries for a person object, you can right-click one of the application servers involved and choose Properties to view the host object's Passwords tab -- and see who else has cached passwords on that application server.

## Summary

1. Using the Finder pane, locate the object you want to view password cache entries for.
2. Choose Properties for the object, and then click the Passwords tab.
3. Select a password cache entry and choose Remove, or right-click one of the objects involved and choose Properties.

## Related topics

- What is ENS?
- Objects and the organizational hierarchy
- Introducing Array Manager
- The tarantella object command
- The tarantella webtopsession command
- The tarantella emulatorsession command
- The tarantella passcache command

## Introducing the Secure Global Desktop Web Server

### Read this topic to...

- Learn about the Secure Global Desktop Web Server.

You must have a web server running on each host on which Secure Global Desktop is installed. When you install Secure Global Desktop, Secure Global Desktop Setup also installs the Secure Global Desktop Web Server. The Secure Global Desktop Web Server is a web server which has been pre-configured for use with Secure Global Desktop. It consists of:

- an [Apache web server](#)
- the [mod\\_ssl](#) module for Apache
- an Apache [Jakarta Tomcat server](#)

**Note** The Apache web server includes all the standard Apache modules as shared objects.

If you have an existing web server on the Secure Global Desktop host, this won't be affected by the Secure Global Desktop Web Server as this will be listening on a different port. You do not have to use the Secure Global Desktop Web Server, but to use your own web server you will have to [configure it for use with Secure Global Desktop](#).

You can configure the Secure Global Desktop Web Server using standard Apache directives, see the [Apache documentation](#) for details.

You control the Secure Global Desktop Web Server independently of the Secure Global Desktop server, using the `tarantella webservice` command.

## Securing the Secure Global Desktop Web Server

The Secure Global Desktop Web Server is also configured to be a secure (HTTPS) web server. You just need to install an appropriate server certificate or [share the server certificate used for Secure Global Desktop security services](#).

Every web server in an array of Secure Global Desktop servers must use the same HTTP (or HTTPS)

port. You must not mix HTTP and HTTPS web servers in the same Secure Global Desktop array.

Once you enable secure connections to a web server, the URL in [the client profile](#) must be re-configured to an HTTPS URL.

### Related topics

- [The tarantella webservice command](#)

## Where is Secure Global Desktop installed?

The standard installation directory for Secure Global Desktop is `/opt/tarantella`.

Secure Global Desktop Setup lets installers choose a different installation directory. To find out your installation directory, type the following:

- on Solaris OS platforms, `pkgparam `pkginfo 'tta.*' | cut -d' ' -f2` INSTDIR`
- on Linux platforms, `rpm -qi tta | grep Relocations`

### Related topics

- [What's in the Secure Global Desktop installation directory?](#)
- [Backing up and restoring a Secure Global Desktop installation](#)



## What's in the Secure Global Desktop installation directory?

The [Secure Global Desktop installation directory](#) contains the following sub-directories:

- `bin`
- `etc`
- `var` and
- `webserver`.

This topic gives a summary of what's in each of these sub-directories and what they are used for.

### bin directory

The `bin` directory contains the scripts, binaries and server-side Java™ technology needed to run Secure Global Desktop.

### etc directory

The `etc` directory contains configuration files that control the behavior of Secure Global Desktop and applications running under Secure Global Desktop. It contains the following subdirectories:

Subdirectory	What it contains
<code>etc/data</code>	<p>The following configuration files:</p> <ul style="list-style-type: none"><li>• application object attribute maps (<code>attrmap.txt</code>)</li><li>• color maps (<code>colormap.txt</code>)</li><li>• host name maps (<code>hostnamemap.txt</code>)</li><li>• Java archive maps used by the classic webtop (<code>archives.txt</code>)</li><li>• mainframe terminal configuration (<code>ttaansi.ti</code>)</li><li>• printer driver maps (<code>default.printerinfo.txt</code>)</li><li>• printer driver to printer type mappings (<code>printertypes.txt</code>)</li><li>• printer to user-friendly name mappings (<code>printernamemap.txt</code>)</li><li>• RGB color names (<code>rgb.txt</code>)</li><li>• timezone configuration (<code>timezone</code>)</li></ul>

<code>etc/data/keymaps</code>	Keyboard map files ( <code>ansikey.txt</code> ).
<code>etc/fonts</code>	X Window System fonts and additional fonts installed with Secure Global Desktop.
<code>etc/pkg</code>	Information about installed Secure Global Desktop packages, for example version compatibility and dependencies.
<code>etc/templates</code>	A complete copy of the standard files that get installed in the <code>etc/data</code> directory and the <code>var/serverresources</code> directory.

## var directory

The `var` directory contains the files that are used by the web server and the files that the Secure Global Desktop server copies to other members of the array. The `var` directory contains many subdirectories and the important ones are listed below:

Subdirectory	What it contains
<code>var/docroot</code>	The Secure Global Desktop login html pages. These are only used by the classic webtop.
<code>var/docroot/cgi-bin</code>	The Secure Global Desktop CGI programs. These are only used by the classic webtop.
<code>var/docroot/native</code>	The Sun Secure Global Desktop Native Client installation files. These can only be used to access the classic webtop.
<code>var/docroot/resources</code>	The files used to display the classic webtop, including login and webtop themes.
<code>var/tsp</code>	X.509 certificates and security keys.
<code>var/ens</code>	The ENS database.
<code>var/log</code>	Server log files.
<code>var/print</code>	The print queue and fifo.
<code>var/serverresources/expect</code>	Secure Global Desktop login scripts.
<code>var/spool</code>	Files on their way to the print queue.

## webserver directory

The `webserver` directory contains the scripts, binaries and server-side Java technology needed to run the Secure Global Desktop Web Server, web services and the browser-based webtop.

Subdirectory	What it contains
<code>apache</code>	All the files needed to configure and run the Secure Global Desktop Web Server.
<code>tomcat</code>	All the files needed to configure and run the Tomcat JavaServer Pages (JSPs)/servlet container.
<code>tomcat/version/webapps/axis</code>	All the files needed to run Secure Global Desktop web services. The browser-based webtop uses web services.
<code>tomcat/version/webapps/sgd</code>	All the files needed to run the browser-based webtop, including the Sun Secure Global Desktop Client.

### Related topics

- [Where is Secure Global Desktop installed?](#)
- [Backing up and restoring a Secure Global Desktop installation](#)

## What X fonts are installed?

Secure Global Desktop Setup installs the standard X Window System fonts in compiled (.pcf) and compressed form, together with some additional fonts required by different UNIX systems. Fonts are installed in the `/opt/tarantella/etc/fonts` directory.

See [Fonts in X11R6.8.2](#) for details.

The following fonts and font directories are available:

Directory	Description
75dpi	Variable-pitch 75 dpi fonts.
100dpi	Variable-pitch 100 dpi fonts.
andrew	Fonts from the Andrew toolkit, required by some IBM applications.
CID	This is a placeholder for CID-keyed fonts. If you want to add your own CID fonts for use with Secure Global Desktop install them in this directory.
cyrillic	Cyrillic fonts.
encodings	Contains a set of encoding files used by the Type1 and TrueType font handlers
hangul	Korean fonts.
hp	Fonts required by some Hewlett-Packard applications.
icl	Fonts required by some ICL applications.
misc	Fixed-pitch fonts, cursor fonts, and fonts for compatibility with older versions of X.
oriental	Kanji and other oriental fonts.
scoterm	Cursor fonts.
TTF	True Type fonts.
Type1	PostScript Type 1 fonts.

## Related topics

- [X Protocol Engine properties \(server-specific\)](#)
- [X application object](#)
- [How do I use my own X fonts?](#)

## Configuring your own web server for use with Secure Global Desktop

A web server on each array member is an essential part of a working Secure Global Desktop installation.

When you install Secure Global Desktop, you install the [Secure Global Desktop Web Server](#). This web server is pre-configured for use with Secure Global Desktop and we recommend you use it.

If you want to use a your own web server with Secure Global Desktop you can do so. However, you must configure the web server for use with Secure Global Desktop. The configuration depends on whether you are using the browser-based webtop or the classic webtop or both.

### Configuring a web server for the browser-based webtop

The browser-based webtop uses the SOAP protocol (over HTTP) to access the services provided by a Secure Global Desktop server. This means, even if you use your own web server, you **must** continue to run the Secure Global Desktop Web Server.

To use your own web server for the browser-based webtop, you need a web server **and** a JavaServer Pages (JSP) container because the webtop is a JSP application. Once you have a working web server/JSP container, follow these instructions for [relocating the browser-based webtop](#).

### Configuring a web server for the classic webtop

To be able to use your own web server with the classic webtop, the web server must support CGI.

If you are using **only** the classic webtop, you do not need to run the Secure Global Desktop Web Server. To prevent the Secure Global Desktop Web Server from running:

1. Stop the Secure Global Desktop Web Server: `tarantella webserver stop`.
2. Change your system boot scripts so that the Secure Global Desktop Web Server does not start when the system boots, and that your own web server does. The Secure Global Desktop Web Server boot script is in the `/etc/rc.d/rc?.d/` directory, where ? depends on the runlevel the host boots in. The boot script name contains "TarantellaWebServer". You must move or delete the script.

**Note** If you are using the browser-based webtop **and** the classic webtop, you must continue to run the Secure Global Desktop Web Server. See above for details.

To configure your own web server for the classic webtop:

1. Add an `Alias` (Document directory) for the Secure Global Desktop document root. For example:

```
Alias /tarantella /opt/tarantella/var/docroot
```

2. Add a `ScriptAlias` (Program or CGI directory) for the Secure Global Desktop CGI programs. For example:

```
ScriptAlias /tarantella/cgi-bin /opt/tarantella/var/docroot/cgi-bin
```

3. Make sure your web server listens on the standard HTTP or HTTPS ports, 80/tcp or 443/tcp.

To ensure that users can download the Native Client and Secure Global Desktop Java™ archives, edit your web server's `mime.types` file and add "exe", "dmg", "jar" and "cab" as file extensions for the "application/octet-stream" mime type, for example:

```
application/octet-stream      bin dms lha lzh class so dll exe dmg jar cab
```

**Note** You may have to remove the "exe" file extension as an extension for the "magnus-internal/cgi" mime type.

### Related topics

- [Introducing the Secure Global Desktop Web Server](#)
- [Relocating the browser-based webtop to your own JSP container](#)

## Licensing and Sun Secure Global Desktop Software

Sun Secure Global Desktop Software has two licensing modes: evaluation mode and fully licensed mode.

License mode	Description
Evaluation mode	<ul style="list-style-type: none"><li>• Applies when no license keys have been installed.</li><li>• Lets you evaluate Secure Global Desktop for <b>30 days</b>.</li><li>• The size of an array is limited to 2 Secure Global Desktop servers</li><li>• The number of users that can log in or have running emulator sessions is limited to 5.</li></ul>
Fully licensed	<ul style="list-style-type: none"><li>• Applies when any license keys have been installed.</li><li>• The size of an array is not limited.</li><li>• The number of users that can log in or have running emulator sessions is limited by the installed license keys.</li></ul>

While you are evaluating Secure Global Desktop, the number of days remaining in the evaluation period is shown whenever a user logs in to Secure Global Desktop using a web browser.

After the 30-day evaluation period, users will be unable to log in to their webtop and unable to start or resume applications. To continue using Secure Global Desktop you must obtain and install a license key.

You add license keys on the [Licenses properties panel](#) in Array Manager or by using the `tarantella license add` command.

### License keys and licenses

When you install a license key, it installs the licenses that unlock the software features. Licenses are either:

- array-based, they make functionality available to the Secure Global Desktop servers in an array or
- user-based, they make functionality available to users.



The following table lists the types of license available, their basis and what they license:

License type	Basis	Software features
Base Component	User	<p>Core functionality such as:</p> <ul style="list-style-type: none"> <li>• the ability to log in</li> <li>• the ability to authenticate users against an LDAP directory server</li> <li>• support for SOCKS v5 proxy servers</li> <li>• support for HTTP and Secure (SSL) proxy servers</li> <li>• the ability to traverse firewalls</li> <li>• webtops, application launches and session management and</li> <li>• support for arrays.</li> </ul>
Security (TSP)	User	The ability to use secure connections and the ability to authenticate users using RSA SecurID®.
Advanced Security (TASP)	User	<p>The ability to use FIPS-compliant secure connections and the ability to authenticate users using RSA SecurID®.</p> <p><b>Note</b> This requires a separate software package.</p>
Windows Connectivity	User	The ability to run Windows applications.
UNIX Connectivity	User	The ability to run UNIX and Linux applications.
AS/400 Connectivity	User	The ability to run 5250 applications.
Mainframe Connectivity	User	The ability to run 3270 applications.
Directory Services Integration	Array	<p>The ability:</p> <ul style="list-style-type: none"> <li>• to use an LDAP version 3 directory instead of ENS for holding user information.</li> <li>• to use the Active Directory login authority.</li> </ul>
Portal Integration	Array	The ability to use Secure Global Desktop with a Sun™ Portal Server.

Advanced Load Management	Array	The ability to load balance application servers based on their true CPU or memory load.
--------------------------	-------	---

## User-based licenses

User-based licenses are enforced by the software on a concurrent user basis. A user is allocated a license as soon as they use a software component. For example, when a user logs in to Secure Global Desktop, they are allocated a Base Component license. If they then run a Windows application, they are allocated a Windows Connectivity license. The license is released when they stop using the component.

A single user is never counted as using more than one of each type of license. However, a user may be counted as using several license types at once. For example, if a user has four UNIX applications running over a secure connection, then that user is counted as using one Base Component license, one Security license and one UNIX Connectivity license.

Note the following:

- Each [guest user](#) and [anonymous user](#) is counted as a separate user.
- When all the Base Component licenses are allocated, additional users may not log in to Secure Global Desktop.
- When all the Security licenses are allocated, additional users may not log in to Secure Global Desktop using secure connections.
- Array Manager and Object Manager are counted as applications.
- If a user suspends an application, they are counted as still using a connectivity component and keep their license, even if they are not logged in to Secure Global Desktop.
- If a user logs out of Secure Global Desktop without closing applications that are configured to be always resumable, the applications continue run (and use a connectivity component) until they time out ([Resumable For](#)). The default timeout period is 8 days.
- It is possible for a user to log in to Secure Global Desktop but not be able to run any applications. This is because there are Base Component licenses available but all the connectivity licenses are being used (users, who are not logged in, have suspended application sessions).

## License administration

Secure Global Desktop automatically allocates and releases licenses to users as they use software components. Secure Global Desktop Administrators cannot manually allocate and release licenses, although they can end a user's webtop and emulator sessions.

The Secure Global Desktop log files record all license usage over time. Secure Global Desktop Administrators can use the `tarantella license query` command to display information on both current and past license usage across the array.

## Related topics

- [The tarantella license command](#)
- [Licenses properties \(array-wide\)](#)

## **Sun Secure Global Desktop Software legal and copyright information**

### **Proprietary Rights Notice**

Copyright © 1997-2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo, Java and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon architecture developed by Sun Microsystems, Inc.

UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Adobe is a registered trademark of Adobe Systems, Incorporated.

Products covered by and information contained in this service manual are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS,

REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright © 1997-2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuels relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

Cette distribution peut comprendre des composants développés par des tierces parties.

Sun, Sun Microsystems, le logo Sun, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Adobe est une marque enregistrée de Adobe Systems, Incorporated.

Les produits qui font l'objet de ce manuel d'entretien et les informations qu'il contient sont régis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes biologiques et chimiques ou du nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers les pays sous embargo américain, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exhaustive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE

UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

## Third-party copyright notices and licenses

Sun Secure Global Desktop Software uses some third-party software. The following copyright notices and licenses apply to the **third-party software** and **not** to Secure Global Desktop software.

If you access terminal server functionality provided by Microsoft operating system products, you need to purchase additional licenses to use such products. Consult the license agreements for the Microsoft operating system products you are using to determine which licenses you must acquire.

%%The following software or portions thereof may be included in this product: SSLava Toolkit. The following applies to such software:

This Software is derived in part from the SSLava(tm) Toolkit which is Copyright (c) 1996-1998 by Phaos Technology Corp. All Rights Reserved.

%%The following software or portions thereof may be included in this product: TeemTalk (TN5250E and/or TN3270E). The following applies to such software:

Some portions of this computer software product are copyright works owned by Neoware UK Ltd.

Copyright (c) Neoware UK Ltd. 1990-2005

Sun Microsystems, Inc. or its subsidiary is acting as a distributor and not as author or developer of this software.

%%The following software may be included in this product: Apache Web Server (HTTP Server). Use of any of this software is governed by the terms of the license below:

Apache License

Version 2.0, January 2004  
<http://www.apache.org/licenses/>

## TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

### 1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control

systems,

and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.
4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without



modifications, and in Source or Object form, provided that You meet the following conditions:

- (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
- (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
- (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
- (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify

the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[ ]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");  
you may not use this file except in compliance with the License.  
You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

%%The following software may be included in this product: Apache Jakarta.  
Use of any of this software is governed by the terms of the license below:  
Apache License

Version 2.0, January 2004  
<http://www.apache.org/licenses/>

## TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

### 1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the

direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.
4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
  - (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
  - (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
  - (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A

PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.
9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[ ]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");  
you may not use this file except in compliance with the License.

You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

%%The following software may be included in this product: Apache XML Soap. Use of any of this software is governed by the terms of the license below:

Apache License

Version 2.0, January 2004  
<http://www.apache.org/licenses/>

#### TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

##### 1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but



not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.
3. Grant of Patent License. Subject to the terms and conditions of

this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:
  - (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and
  - (b) You must cause any modified files to carry prominent notices stating that You changed the files; and
  - (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
  - (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution

notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.
6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.
7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.
8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all

other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. **Accepting Warranty or Additional Liability.** While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[ ]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");  
you may not use this file except in compliance with the License.  
You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

%%The following software may be included in this product: Xerces (XML parser libraries). Use of any of this software is governed by the terms of the licenses below:

XERCES:

```
/*
 * The Apache Software License, Version 1.1
 *
 *
 * Copyright (c) 1999 The Apache Software Foundation. All rights
 * reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in
 * the documentation and/or other materials provided with the
 * distribution.
 *
 * 3. The end-user documentation included with the redistribution,
 * if any, must include the following acknowledgment:
 *     "This product includes software developed by the
 *     Apache Software Foundation (http://www.apache.org/)."
 * Alternately, this acknowledgment may appear in the software itself,
 * if and wherever such third-party acknowledgments normally appear.
 *
 * 4. The names "Xerces" and "Apache Software Foundation" must
 * not be used to endorse or promote products derived from this
 * software without prior written permission. For written
 * permission, please contact apache@apache.org.
 *
 * 5. Products derived from this software may not be called "Apache",
 * nor may "Apache" appear in their name, without prior written
 * permission of the Apache Software Foundation.
 *
 * THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED
 * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
 * DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
 * LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
```

\* USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND  
\* ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,  
\* OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT  
\* OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF  
\* SUCH DAMAGE.

\* =====

\*  
\* This software consists of voluntary contributions made by many  
\* individuals on behalf of the Apache Software Foundation and was  
\* originally based on software copyright (c) 1999, International  
\* Business Machines, Inc., <http://www.ibm.com>. For more  
\* information on the Apache Software Foundation, please see  
\* .

#### W3C SOFTWARE NOTICE AND LICENSE

Copyright 1994-2002 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>

This W3C work (including software, documents, or other related items) is being provided by the copyright holders under the following license. By obtaining, using and/or copying this work, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions:

Permission to use, copy, modify, and distribute this software and its documentation, with or without modification, for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the software and documentation or portions thereof, including modifications, that you make:

- 1.The full text of this NOTICE in a location viewable to users of the redistributed or derivative work.
- 2.Any pre-existing intellectual property disclaimers, notices, or terms and conditions. If none exist, a short notice of the following form (hypertext is preferred, text is permitted) should be used within the body of any redistributed or derivative code: "Copyright [\$date-of-software] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>"
- 3.Notice of any changes or modifications to the W3C files, including the date changes were made. (We recommend you provide URIs to the location from which the code is derived.)

THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE

ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR DOCUMENTATION.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to the software without specific, written prior permission. Title to copyright in this software and any associated documentation will at all times remain with copyright holders.

---

This formulation of W3C's notice and license became active on August 14 1998 so as to improve compatibility with GPL. This version ensures that W3C software licensing terms are no more restrictive than GPL and consequently W3C software may be distributed in GPL packages. See the older formulation for the policy prior to this date. Please see our Copyright FAQ for common questions about using materials from our site, including specific terms and conditions for packages like libwww, Amaya, and Jigsaw. Other questions about this notice can be directed to [site-policy@w3.org](mailto:site-policy@w3.org).

SAX license at:

<http://www.saxproject.org/?selected=pd>

%The following software may be included in this product: mod\_ssl. Use of any of this software is governed by the terms of the license below:

#### LICENSE

The mod\_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

=====  
Copyright (c) 1998-2004 Ralf S. Engelschall. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:  
 "This product includes software developed by Ralf S. Engelschall for use in the mod\_ssl project (<http://www.modssl.org/>)."
4. The names "mod\_ssl" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [rse@engelschall.com](mailto:rse@engelschall.com).
5. Products derived from this software may not be called "mod\_ssl" nor may "mod\_ssl" appear in their names without prior written permission of Ralf S. Engelschall.
6. Redistributions of any form whatsoever must retain the following acknowledgment:  
 "This product includes software developed by Ralf S. Engelschall for use in the mod\_ssl project (<http://www.modssl.org/>)."

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL RALF S. ENGELSCHALL OR HIS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

%The following software may be included in this product: OpenSSL (SSLeay). Use of any of this software is governed by the terms of the license below:

License

This is a copy of the current LICENSE file inside the CVS repository.



=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style

Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

OpenSSL License

-----

```
/* =====
 * Copyright (c) 1998-2005 The OpenSSL Project. All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 * notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in
 * the documentation and/or other materials provided with the
 * distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 * software must display the following acknowledgment:
 * "This product includes software developed by the OpenSSL Project
 * for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 * endorse or promote products derived from this software without
 * prior written permission. For written permission, please contact
 * openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 * nor may "OpenSSL" appear in their names without prior written
 * permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 * acknowledgment:
```

\* "This product includes software developed by the OpenSSL Project  
\* for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"  
\*

\* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY  
\* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE  
\* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR  
\* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR  
\* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,  
\* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT  
\* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;  
\* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)  
\* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,  
\* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)  
\* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED  
\* OF THE POSSIBILITY OF SUCH DAMAGE.

\* =====  
\*

\* This product includes cryptographic software written by Eric Young  
\* (eay@cryptsoft.com). This product includes software written by Tim  
\* Hudson (tjh@cryptsoft.com).

\*  
\*/

Original SSLeay License  
-----

/\* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)  
\* All rights reserved.  
\*  
\* This package is an SSL implementation written  
\* by Eric Young (eay@cryptsoft.com).  
\* The implementation was written so as to conform with Netscapes SSL.  
\*  
\* This library is free for commercial and non-commercial use as long as  
\* the following conditions are aheared to. The following conditions  
\* apply to all code found in this distribution, be it the RC4, RSA,  
\* lhash, DES, etc., code; not just the SSL code. The SSL documentation  
\* included with this distribution is covered by the same copyright terms  
\* except that the holder is Tim Hudson (tjh@cryptsoft.com).  
\*  
\* Copyright remains Eric Young's, and as such any Copyright notices in  
\* the code are not to be removed.  
\* If this package is used in a product, Eric Young should be given  
attribution

```
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright
*   notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*   notice, this list of conditions and the following disclaimer in the
*   documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*   must display the following acknowledgement:
*   "This product includes cryptographic software written by
*     Eric Young (eay@cryptsoft.com)"
*   The word 'cryptographic' can be left out if the routines from the
library
*   being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof)
from
*   the apps directory (application code) you must include an
acknowledgement:
*   "This product includes software written by Tim Hudson (tjh@cryptsoft.
com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version
or
* derivative of this code cannot be changed. i.e. this code cannot simply
```

be

```
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/
```

%%The following software may be included in this product: zlib. Use of any of this software is governed by the terms of the license below:

License

```
/* zlib.h -- interface of the 'zlib' general purpose compression library
   version 1.2.2, October 3rd, 2004
```

Copyright (C) 1995-2004 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org  
Mark Adler madler@alumni.caltech.edu

\*/

%%The following software may be included in this product: gzip. Use of any of this software is governed by the terms of the license below:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.  
675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

## Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them

these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

#### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not

restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

1. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

2. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

3. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License.

(Exception:

if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

1. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

2. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

3. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object



code

or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose

that choice. This section is intended to make thoroughly clear what is believed

to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright

holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such

case, this License incorporates the limitation as if written in the body of this

License.

10. The Free Software Foundation may publish revised and/or new versions of

the General Public License from time to time. Such new versions will be similar

in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If

the Program specifies a version number of this License which applies to it and

"any later version", you have the option of following the terms and conditions

either of that version or of any later version published by the Free Software

Foundation. If the Program does not specify a version number of this License,

you may choose any version ever published by the Free Software Foundation.

11. If you wish to incorporate parts of the Program into other free programs

whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation,

write to the Free Software Foundation; we sometimes make exceptions for this.

Our decision will be guided by the two goals of preserving the free status of

all derivatives of our free software and of promoting the sharing and reuse of

software generally.

#### NO WARRANTY

12. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY

FOR  
THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN  
OTHERWISE  
STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE  
PROGRAM  
"AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED,  
INCLUDING,  
BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS  
FOR A  
PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE  
PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE  
COST OF  
ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

13. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING  
WILL  
ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE  
THE  
PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY  
GENERAL,  
SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR  
INABILITY  
TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING  
RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A  
FAILURE OF  
THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR  
OTHER  
PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Copyright 1992-1993 Jean-loup Gailly, Copyright Mark Adler.

% The following software may be included in this product: X11R6.4. Use  
of any of this software is governed by the terms of the license below:

Copyright (C) 1998 The Open Group

Permission is hereby granted, free of charge, to any person obtaining a  
copy of this software and associated documentation files (the  
"Software"), to deal in the Software without restriction, including  
without limitation the rights to use, copy, modify, merge, publish, dis-  
tribute, sublicense, and/or sell copies of the Software, and to permit  
persons to whom the Software is furnished to do so, subject to the fol-  
lowing conditions:

The above copyright notice and the following permission notice shall be  
included in all copies of the Software:

THE SOFTWARE IS PROVIDED AS IS, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE OPEN GROUP BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF, OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of The Open Group shall not be used in advertising or otherwise to promote the use or other dealings in this Software without prior written authorization from The Open Group.

X Window System is a trademark of The Open Group.

% The following software may be included in this product: X Window System (X11R6.8.2). Use of any of this software is governed by the terms of the licenses below:

<http://xorg.freedesktop.org/releases/X11R6.8.2/doc/LICENSE3.html#3>

XFree86 License:

XFree86 code without an explicit copyright is covered by the following copyright/license:

Copyright (C) 1994-2003 The XFree86 Project, Inc. All Rights Reserved. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE XFREE86 PROJECT BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the XFree86 Project shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from the XFree86 Project.

Portions also covered by other licenses as noted in the above url.

%%The following software may be included in this product: OpenMotif. Use of any of this software is governed by the terms of the license below:

THE OPEN GROUP PUBLIC LICENSE

MOTIF GRAPHICAL USER INTERFACE SOFTWARE

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS THE OPEN GROUP PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

## 1. DEFINITIONS

"Contribution" means:

1. in the case of The Open Group, L.L.C. ("The Open Group"), the Original Program, and

2. in the case of each Contributor,

i.

changes  
to the Program, and

ii.

additions to  
the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which:

- i. are separate modules of software distributed in conjunction with the Program under their own license agreement, even if the separate modules are linked in binary form to the Program, and
- ii. are not derivative works of the Program.

"Contributor" means The Open Group and any other entity that distributes the Program.

"Licensed Patents" mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Open Source" programs mean software for which the source code is available without confidential or trade secret restrictions and for which the source code and object code are available for distribution without license charges.

"Original Program" means the original version of the software accompanying this Agreement as released by The Open Group, including source code, object code

and  
documentation, if any.

"Program" means the Original Program and Contributions.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

## 2. GRANT OF RIGHTS

The rights granted under this license are limited solely to distribution and sublicensing of the Contribution(s) on, with, or for operating systems which are themselves Open Source programs. Contact The Open Group for a license allowing distribution and sublicensing of the Original Program on, with, or for operating systems which are not Open Source programs.

1. Subject to the terms of this Agreement and the limitations of this Section 2, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

2. Subject to the terms of this Agreement and the limitations of



this

Section 2, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

3. Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

4. Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

### 3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a. it complies with the terms and conditions of this Agreement; and

b. its license agreement:

i. effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii. effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii. states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv. states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

- a. it must be made available under this Agreement; and
- b. a copy of this Agreement must be included with each copy of the Program.

Each Contributor must include the following in a conspicuous location in the Program:

Copyright (c) {date here}, The Open Group Ltd. and others. All Rights Reserved.

In addition, each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

#### 4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, subject to the limitations provided in Section 2, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create

potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must:

- a. promptly notify the Commercial Contributor in writing of such claim, and
- b. allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defence and any related settlement negotiations.

The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court

requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

## 5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

## 6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY

OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

## 7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation or other similar official proceedings to enforce patent rights against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, If Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of

such non-compliance. If all Recipient's rights under this Agreement terminate,  
Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

The Open Group may publish new versions (including revisions) of this Agreement from time to time. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. No one other than The Open Group has the right to modify this Agreement. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

%The following software may be included in this product: JAACL/TCL. Use of any of this software is governed by the terms of the license below:

The following terms apply to all versions of the core Tcl/Tk releases, the Tcl/Tk browser plug-in version 2.0, and TclBlend and Jacl version 1.0.

Please

note that the TclPro tools are under a different license agreement. This agreement is part of the standard Tcl/Tk distribution as the file named "license.terms".

#### TCL/TK LICENSE TERMS

This software is copyrighted by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. government, the Government shall have only "Restricted Rights" in the software



and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as "Commercial Computer Software" and the Government shall have only "Restricted Rights" as defined in Clause 252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the authors grant the U.S. Government and others acting in its behalf permission to use and distribute the software in accordance with the terms specified in this license.

%The following software may be included in this product: XML Parser. Use of any of this software is governed by the terms of the license below:

Copyright (c) 1997, 1998 James Clark

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the ``Software''), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED ``AS IS'', WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL JAMES CLARK BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of James Clark shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from James Clark.

%%The following software may be included in this product: Cryptix Libraries (crypto libraries). Use of any of this software is governed by the terms of the license below:

#### Cryptix General License

Copyright (c) 1995-2005 The Cryptix Foundation Limited.  
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE CRYPTIX FOUNDATION LIMITED AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CRYPTIX FOUNDATION LIMITED OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

%%The following software may be included in this product: Unicode Character Table. Use of any of this software is governed by the terms of the license below:

#### UNICODE 2.1 CHARACTER DATABASE

Copyright (c) 1991-1998 Unicode, Inc.  
All Rights reserved.

## DISCLAIMER

The Unicode Character Database "UNIDAT21.TXT" is provided as-is by Unicode, Inc. (The Unicode Consortium). No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

This disclaimer is applicable for all other data files accompanying the Unicode Character Database, some of which have been compiled by the Unicode Consortium, and some of which have been supplied by other vendors.

## LIMITATIONS ON RIGHTS TO REDISTRIBUTE THIS DATA

Recipient is granted the right to make copies in any form for internal distribution and to freely use the information supplied in the creation of products supporting the Unicode (TM) Standard. This file can be redistributed to third parties or other organizations (whether for profit or not) as long as this notice and the disclaimer notice are retained.

## EXPLANATORY INFORMATION

The Unicode Character Database defines the default Unicode character properties, and internal mappings. Particular implementations may choose to override the properties and mappings that are not normative. If that is done, it is up to the implementer to establish a protocol to convey that information. For more information about character properties and mappings, see "The Unicode Standard, Worldwide Character Encoding, Version 2.0", published by Addison-Wesley. For information about other data files accompanying the Unicode Character Database, see the section of the Unicode Standard they were extracted from, or the explanatory readme files and/or header sections with those files.

The Unicode Character Database has been updated to reflect Version 2.1 of the Unicode Standard, with two additional characters added to those published in Version 2.0:

U+20AC EURO SIGN

## U+FFFC OBJECT REPLACEMENT CHARACTER

A number of corrections have also been made to case mappings or other errors in the database noted since the publication of Version 2.0. And a few normative bidirectional properties have been modified to reflect decisions of the Unicode Technical Committee.

The Unicode Character Database is a plain ASCII text file consisting of lines containing fields terminated by semicolons. Each line represents the data for one encoded character in the Unicode Standard, Version 2.1. Every encoded character has a data entry, with the exception of certain special ranges, as detailed below.

There are five special ranges of characters that are represented only by their start and end characters, since the properties in the file are uniform, except for code values (which are all sequential and assigned). The names of CJK ideograph characters and Hangul syllable characters are algorithmically derivable. (See the Unicode Standard for more information). Surrogate characters and private use characters have no names.

The exact ranges represented by start and end characters are:

- The CJK Ideographs Area (U+4E00 - U+9FFF)
- The Hangul Syllables Area (U+AC00 - U+D7A3)
- The Surrogates Area (U+D800 - U+DFFF)
- The Private Use Area (U+E000 - U+F8FF)
- CJK Compatibility Ideographs (U+F900 - U+FAFF)

The following table describes the format and meaning of each field in a data entry in the Unicode Character Database. Fields which contain normative information are so indicated.

Field	Explanation
-----	-----

0	Code value in 4-digit hexadecimal format. This field is normative.
---	---

1	Unicode 2.1 Character Name. These names match exactly the names published in Chapter 7 of the Unicode Standard, Version
---	---

2.0, except for the two additional characters.

This field is normative.

2 General Category. This is a useful breakdown into various "character types" which can be used as a default categorization in implementations.

Some of the values are normative, and some are informative.

See below for a brief explanation.

3 Canonical Combining Classes. The classes used for the Canonical Ordering Algorithm in the Unicode Standard. These classes are also printed in Chapter 4 of the Unicode Standard. This field is normative. See below for a brief explanation.

4 Bidirectional Category. See the list below for an explanation of the abbreviations used in this field. These are the categories required by the Bidirectional Behavior Algorithm in the Unicode Standard. These categories are summarized in Chapter 4 of the Unicode Standard.

This field is normative.

5 Character Decomposition. In the Unicode Standard, not all of the decompositions are full decompositions. Recursive application of look-up for decompositions will, in all cases, lead to

a maximal decomposition. The decompositions match exactly the decompositions published with the character names in Chapter 7 of the Unicode Standard. This field is normative.

6 Decimal digit value. This is a numeric field. If the character has the decimal digit property, as specified in Chapter 4 of the Unicode Standard, the value of that digit is represented with an integer value in this field. This field is normative.

7 Digit value. This is a numeric field. If the character represents a digit, not necessarily a decimal digit, the value is here. This covers digits which do not form decimal radix forms, such as the compatibility superscript digits. This field is informative.

8 Numeric value. This is a numeric field. If the character has the numeric property, as specified in Chapter 4 of the Unicode Standard, the value of that character is represented with an integer or rational number in this field. This includes fractions as,

e.g., "1/5" for U+2155 VULGAR FRACTION ONE FIFTH.

Also included are numerical values for compatibility characters such as circled numbers. This field is normative.

- 9 If the characters has been identified as a "mirrored" character in bidirectional text, this field has the value "Y"; otherwise "N". The list of mirrored characters is also printed in Chapter 4 of the Unicode Standard. This field is normative.
- 10 Unicode 1.0 Name. This is the old name as published in Unicode 1.0. This name is only provided when it is significantly different from the Unicode 2.1 name for the character. This field is informative.
- 11 10646 Comment field. This field is informative.
- 12 Upper case equivalent mapping. If a character is part of an alphabet with case distinctions, and has an upper case equivalent, then the upper case equivalent is in this field. See the explanation below on case distinctions. These mappings are always one-to-one, not one-to-many or many-to-one. This field is informative.
- 13 Lower case equivalent mapping. Similar to 12. This field is informative.
- 14 Title case equivalent mapping. Similar to 12. This field is informative.

#### GENERAL CATEGORY

The values in this field are abbreviations for the following. Some of the values are normative, and some are informative. For more information, see the Unicode Standard. Note: the standard does not assign information to control characters (except for TAB in the Bidirectional Algorithm). Implementations will generally also assign categories to certain control characters, notably CR and LF, according to platform conventions.

#### Normative

Mn = Mark, Non-Spacing

Mc = Mark, Spacing Combining

Me = Mark, Enclosing

Nd = Number, Decimal Digit

Nl = Number, Letter

No = Number, Other

Zs = Separator, Space

Zl = Separator, Line

Zp = Separator, Paragraph

Cc = Other, Control

Cf = Other, Format

Cs = Other, Surrogate

Co = Other, Private Use

Cn = Other, Not Assigned

#### Informative

Lu = Letter, Uppercase

Ll = Letter, Lowercase

Lt = Letter, Titlecase

Lm = Letter, Modifier

Lo = Letter, Other

Pc = Punctuation, Connector

Pd = Punctuation, Dash

Ps = Punctuation, Open

Pe = Punctuation, Close

Po = Punctuation, Other

Sm = Symbol, Math

Sc = Symbol, Currency

Sk = Symbol, Modifier

So = Symbol, Other

#### BIDIRECTIONAL PROPERTIES

Please refer to the Unicode Standard for an explanation of the algorithm for Bidirectional Behavior and an explanation of the significance of these categories.

These values are normative.

#### Strong types:

L Left-Right; Most alphabetic, syllabic, and logographic characters (e.g., CJK ideographs)

R Right-Left; Arabic, Hebrew, and punctuation specific to those scripts

#### Weak types:

EN European Number

ES	European Number Separator
ET	European Number Terminator
AN	Arabic Number
CS	Common Number Separator

Separators:

B	Block Separator
S	Segment Separator

Neutrals:

WS	Whitespace
ON	Other Neutrals ; All other characters: punctuation, symbols

CHARACTER DECOMPOSITION TAGS

The decomposition is a normative property of a character. The tags supplied with certain decompositions generally indicate formatting information. Where no such tag is given, the decomposition is designated as canonical. Conversely, the presence of a formatting tag also indicates that the decomposition is a compatibility decomposition and not a canonical decomposition. In the absence of other formatting information in a compatibility decomposition, the tag is used to distinguish it from canonical decompositions.

In some instances a canonical decomposition or a compatibility decomposition may consist of a single character. For a canonical decomposition, this indicates that the character is a canonical equivalent of another single character. For a compatibility decomposition, this indicates that the character is a compatibility equivalent of another single character.

The compatibility formatting tags used are:

- A font variant (e.g. a blackletter form).
- A no-break version of a space or hyphen.
- An initial presentation form (Arabic).
- A medial presentation form (Arabic).
- A final presentation form (Arabic).
- An isolated presentation form (Arabic).
- An encircled form.
- A superscript form.
- A subscript form.
- A vertical layout presentation form.
- A wide (or zenkaku) compatibility character.
- A narrow (or hankaku) compatibility character.



A small variant form (CNS compatibility).  
A CJK squared font variant.  
A vulgar fraction form.  
Otherwise unspecified compatibility character.

#### CANONICAL COMBINING CLASSES

0: Spacing, enclosing, reordrant, and surrounding  
1: Overlays and interior  
6: Tibetan subjoined Letters  
7: Nuktas  
8: Hiragana/Katakana voiced marks  
9: Viramas  
10: Start of fixed position classes  
199: End of fixed position classes  
200: Below left attached  
202: Below attached  
204: Below right attached  
208: Left attached (reordrant around single base character)  
210: Right attached  
212: Above left attached  
214: Above attached  
216: Above right attached  
218: Below left  
220: Below  
222: Below right  
224: Left (reordrant around single base character)  
226: Right  
228: Above left  
230: Above  
232: Above right  
234: Double above

Note: some of the combining classes in this list do not currently have members but are specified here for completeness.

#### CASE MAPPINGS

In addition to uppercase and lowercase, because of the inclusion of certain composite characters for compatibility, such as "01F1;LATIN CAPITAL LETTER DZ", there is a third case, called titlecase, which is used where the first character of a word is to be capitalized (e.g. UPPERCASE, Titlecase, lowercase). An example of such a character is "01F2;LATIN CAPITAL LETTER D WITH SMALL LETTER Z".

The uppercase, titlecase and lowercase fields are only included for characters that have a single corresponding character of that type. Composite characters (such as "339D;SQUARE CM") that do not have a single corresponding character of that type can be cased by decomposition.

The case mapping is an informative, default mapping. Certain languages, such as Turkish, German, French, or Greek may have small deviations from the default mappings listed in the Unicode Character Database.

#### MODIFICATION HISTORY

Modifications made in updating the Unicode Character Database for the Unicode Standard, Version 2.1 (from Version 2.0) are:

- \* Added two characters (U+20AC and U+FFFC).
- \* Amended bidi properties for U+0026, U+002E, U+0040, U+2007.
- \* Corrected case mappings for U+018E, U+019F, U+01DD, U+0258, U+0275, U+03C2, U+1E9B.
- \* Changed combining order class for U+0F71.
- \* Corrected canonical decompositions for U+0F73, U+1FBE.
- \* Changed decomposition for U+FB1F from compatibility to canonical.
- \* Added compatibility decompositions for U+FBE8, U+FBE9, U+FBF9..U+FBFB.
- \* Corrected compatibility decompositions for U+2469, U+246A, U+3358.

Some of the modifications made in updating the Unicode Character Database for the Unicode Standard, Version 2.0 are:

- \* Fixed decompositions with TONOS to use correct NSM: 030D.
- \* Removed old Hangul Syllables; mapping to new characters are in a separate table.
- \* Marked compability decompositions with additional tags.
- \* Changed old tag names for clarity.
- \* Revision of decompositions to use first-level decomposition, instead of maximal decomposition.
- \* Correction of all known errors in decompositions from earlier versions.
- \* Added control code names (as old Unicode names).
- \* Added Hangul Jamo decompositions.
- \* Added Number category to match properties list in book.
- \* Fixed categories of Koranic Arabic marks.
- \* Fixed categories of precomposed characters to match decomposition where possible.
- \* Added Hebrew cantillation marks and the Tibetan script.

\* Added place holders for ranges such as CJK Ideographic Area and the Private Use Area.

\* Added categories Me, Sk, Pc, Nl, Cs, Cf, and rectified a number of mistakes in the database.

%The following software may be included in this product: Castor. Use of any of this software is governed by the terms of the license below:

Copyright 1999-2004 (C) Intalio Inc., and others. All Rights Reserved.

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "ExoLab" must not be used to endorse or promote products derived from this Software without prior written permission of Intalio Inc. For written permission, please contact [info@exolab.org](mailto:info@exolab.org).
4. Products derived from this Software may not be called "Castor" nor may "Castor" appear in their names without prior written permission of Intalio Inc. Exolab, Castor and Intalio are trademarks of Intalio Inc.
5. Due credit should be given to the ExoLab Project (<http://www.exolab.org/>).

THIS SOFTWARE IS PROVIDED BY INTALIO AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTALIO OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR

PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

%The following software may be included in this product: MIT Kerberos. Use of any of this software is governed by the terms of the license below:

Copyright Notice and Legal Administrivia

-----  
Copyright (C) 1985-2005 by the Massachusetts Institute of Technology.

All rights reserved.

Export of this software from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original MIT software. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Individual source code files are copyright MIT, Cygnus Support, OpenVision, Oracle, Sun Soft, FundsXpress, and others.

Project Athena, Athena, Athena MUSE, Discuss, Hesiod, Kerberos, Moira,

and Zephyr are trademarks of the Massachusetts Institute of Technology (MIT). No commercial use of these trademarks may be made without prior written permission of MIT.

"Commercial use" means use of a name in a product or other for-profit manner. It does NOT prevent a commercial firm from referring to the MIT trademarks in order to convey information (although in doing so, recognition of their trademark status should be given).

----

The following copyright and permission notice applies to the OpenVision Kerberos Administration system located in kadmin/create, kadmin/dbutil, kadmin/passwd, kadmin/server, lib/kadm5, and portions of lib/rpc:

Copyright, OpenVision Technologies, Inc., 1996, All Rights Reserved

WARNING: Retrieving the OpenVision Kerberos Administration system source code, as described below, indicates your acceptance of the following terms. If you do not agree to the following terms, do not retrieve the OpenVision Kerberos administration system.

You may freely use and distribute the Source Code and Object Code compiled from it, with or without modification, but this Source Code is provided to you "AS IS" EXCLUSIVE OF ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY OTHER WARRANTY, WHETHER EXPRESS OR IMPLIED. IN NO EVENT WILL OPENVISION HAVE ANY LIABILITY FOR ANY LOST PROFITS, LOSS OF DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM THE USE OF THE SOURCE CODE, OR THE FAILURE OF THE SOURCE CODE TO PERFORM, OR FOR ANY OTHER REASON.

OpenVision retains all copyrights in the donated Source Code. OpenVision also retains copyright to derivative works of the Source Code, whether created by OpenVision or by a third party. The OpenVision copyright notice must be preserved if derivative works are made based on the donated Source Code.

OpenVision Technologies, Inc. has donated this Kerberos Administration system to MIT for inclusion in the standard

Kerberos 5 distribution. This donation underscores our commitment to continuing Kerberos technology development and our gratitude for the valuable work which has been performed by MIT and the Kerberos community.

----

Portions contributed by Matt Crawford were work performed at Fermi National Accelerator Laboratory, which is operated by Universities Research Association, Inc., under contract DE-AC02-76CH03000 with the U.S. Department of Energy.

---- The implementation of the Yarrow pseudo-random number generator in src/lib/crypto/yarrow has the following copyright:

Copyright 2000 by Zero-Knowledge Systems, Inc.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Zero-Knowledge Systems, Inc. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Zero-Knowledge Systems, Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

ZERO-KNOWLEDGE SYSTEMS, INC. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL ZERO-KNOWLEDGE SYSTEMS, INC. BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTUOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- The implementation of the AES encryption algorithm in src/lib/crypto/aes has the following copyright:

Copyright (c) 2001, Dr Brian Gladman , Worcester, UK.  
All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary form is allowed (with or without changes) provided that:

1. distributions of this source code include the above copyright notice, this list of conditions and the following disclaimer;
2. distributions in binary form include the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other associated materials;
3. the copyright holder's name is not used to endorse products built using this software without specific written permission.

#### DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties in respect of any properties, including, but not limited to, correctness and fitness for purpose.

---- The implementation of the RPCSEC\_GSS authentication flavor in src/lib/rpc has the following copyright:

Copyright (c) 2000 The Regents of the University of Michigan.  
All rights reserved.

Copyright (c) 2000 Dug Song .  
All rights reserved, all wrongs reversed.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE

DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Related topics

- [Do I need to license Windows Terminal Services?](#)



## How do I add new Secure Global Desktop Administrators?

You can use Object Manager or the `tarantella role` command to add new Secure Global Desktop Administrators.

To add a Secure Global Desktop Administrator using Object Manager:

1. On the Browse tab, open the [Secure Global Desktop System Objects](#) organization.
2. Select the Global Administrators role object, and then click Properties.
3. Find the person object for the user you want to be a Secure Global Desktop Administrator, and drop it on the Members tab.

The user's webtop now includes the links shown in the [Links tab](#) of the Global Administrators object. In Object Manager, the Links tab for the user's person object also shows the links.

To remove a Secure Global Desktop Administrator using Object Manager, click the person object in the Global Administrators object's Members tab, and then click Remove.

## What happens if all the Secure Global Desktop Administrators are removed?

If there are no Secure Global Desktop Administrators defined (no users occupy the Global Administrators role) then the user with [TFN name](#) `.../_user/root` (corresponding to the UNIX root user) is given administration privileges. You can log in as this user and run Object Manager to add some Secure Global Desktop Administrators.

### Related topics

- [Roles in Secure Global Desktop](#)
- [What is a role object?](#)
- [The tarantella role command](#)

## What ports does Secure Global Desktop use?

This page lists the ports used by Secure Global Desktop and their purpose. It also lists the direction and protocol information needed to [configure firewalls for use with Secure Global Desktop](#). The ports are divided into ports used for:

- [connections between client devices and Secure Global Desktop servers](#)
- [connections between Secure Global Desktop servers](#)
- [connections between Secure Global Desktop servers and application servers](#) and
- [connections to authentication services and directory services](#).

### Ports used for connections between client devices and Secure Global Desktop servers

Source	Destination	Destination port	Purpose
Client	Web server on the Secure Global Desktop host	80/tcp	Standard, unencrypted HTTP requests and responses used to display webtops.
Client	Web server on the Secure Global Desktop host	443/tcp	Secure, encrypted HTTPS requests and responses used to display webtops.
Client	Secure Global Desktop server	3144/tcp	Standard, unencrypted connections used for control and application display updates.
Client	Secure Global Desktop server	5307/tcp	SSL-based secure, encrypted connections to Secure Global Desktop servers. Used for control and application display updates.

### Notes

- Client devices must be able to access the web server on any host on which Secure Global Desktop is installed.
- If you are using Secure Global Desktop in "[firewall forwarding mode](#)", all the traffic that would normally flow through ports 443 and 5307 flows only through the firewall forwarding port, which is

usually port 443.

- Ports 80 and 443 are registered ports for web servers.
- Ports 3144 and 5307 are ports registered for use only by Secure Global Desktop.

## Ports used for connections between Secure Global Desktop servers

Source	Destination	Destination port	Purpose
Secure Global Desktop server	Another Secure Global Desktop server	515/tcp	Used when moving print jobs from one Secure Global Desktop server to another using the <code>tarantella print move</code> command.
Secure Global Desktop server	Another Secure Global Desktop server	5427/tcp	Used for connections between Secure Global Desktop servers to allow array replication and sharing of both static and dynamic data across the array.

### Notes

- Connections on port 5427 are required to establish and run arrays.
- **All** array members must be able to connect to **any other** member of the array.
- Port 5427 is registered for use only by Secure Global Desktop.

## Ports used for connections between Secure Global Desktop servers and application servers

Source	Destination	Destination port	Purpose
Secure Global Desktop server	Application server	22/tcp	Used to connect to X and character applications using Secure SHell (SSH).
Secure Global Desktop server	Application server	23/tcp	Used to connect to Windows, X and character applications using telnet.

Application server	Secure Global Desktop server	137/udp	Used for WINS services with client drive mapping. The server binds to this port at start-up only if WINS services are currently enabled.
Application server	Secure Global Desktop server	139/tcp	Used for client drive mapping services. The server binds to this port at start-up, whether or not client drive mapping services are currently enabled.
Secure Global Desktop server	Application server	512/tcp	Used to connect to X applications using rexec.
Application server	Secure Global Desktop server	515/tcp	Used to send print jobs from the application server to a Secure Global Desktop server.
Secure Global Desktop server	Application server	3389/tcp	Used to connect to Windows applications configured to use the Microsoft RDP protocol.
Secure Global Desktop server	Application server	3579/tcp	Used for connections between the primary Secure Global Desktop server and the Secure Global Desktop load balancing service running on an application server.
Application server	Secure Global Desktop server	3579/udp	Used for connections between the Secure Global Desktop load balancing service running on an application server and the primary Secure Global Desktop server.

Secure Global Desktop server	Application server	5999/tcp	Used to connect to Windows applications, if the application configured to use the Wincenter protocol <b>and</b> the connection method is telnet. The Wincenter protocol is no longer supported but may be used by legacy Windows application objects,
Application server	Secure Global Desktop server	6010/tcp and above	Used to connect X applications with the protocol engines running on the Secure Global Desktop server.

## Notes

- Ports 22, 23, 512, 3389 and 5999 only need to be opened if they are required to run applications through Secure Global Desktop. The ports actually used depends on the application type, the [connection method](#) used to log in to the application server and (for Windows applications) the [protocol](#) used.
- Ports 137 and 139 may be used by products providing Windows file and print services, such as Samba. You only need to open these ports if you are using [client drive mapping](#).
- Ports 3579 tcp and udp are ports registered for use only by Secure Global Desktop. You only need to open these ports if you are using [Secure Global Desktop Advanced Load Management](#).
- Port 5500 is only required if you are using the SecurID login authority. For the RSA ACE/Agent to authenticate to the Master ACE/Server through a firewall, port 5500/udp must be open from the Agent IP to the Master and Slave IP.
- Ports 6010/tcp and above are not used if the Secure Global Desktop server connects to the application server using SSH and [port forwarding is enabled](#).

## Ports used for connections to authentication services and directory services

Source	Destination	Destination port	Purpose
Secure Global Desktop server	Windows server	88/udp or tcp	Used to authenticate users from a Windows domain.

Secure Global Desktop server	Windows server	137/udp	Used to authenticate users from a Windows domain.
Secure Global Desktop server	Windows server	139/tcp	Used to authenticate users from a Windows domain.
Secure Global Desktop server	LDAP directory server	389/tcp	Used to authenticate users and/or provide webtop content using LDAP.
Secure Global Desktop server	Windows server	464/udp or tcp	Used to allow users to change their password if it has expired.
Secure Global Desktop server	LDAP directory server	636/tcp	Used to authenticate users and/or provide webtop content using SSL-based LDAP (LDAPS).
RSA SecurID/ ACE Server®	Secure Global Desktop server	1024/udp to 65535/udp	Used to authenticate users using SecurID/ ACE.
Secure Global Desktop server	Windows server	3268/tcp	Used to authenticate users from a Windows domain.
Secure Global Desktop server	RSA SecurID/ACE Server	5500/udp	Used to authenticate users using SecurID/ ACE.

## Notes

- Ports 88, 464 and 3268 are only required if you are using the [Active Directory login authority](#). Ports 88 and 464 can be either udp or tcp depending on the packet size and your Kerberos configuration, see [enabling the Active Directory login authority for details](#).
- Ports 137 and 139 may be used by products providing Windows file and print services, such as Samba. You only need to open these ports if you are using the [NT login authority](#).
- Ports 389/636 are only required if you are using the [LDAP login authority](#) or Directory Services Integration.

- Ports 1024 to 65535 are only required if you are using the [SecurID login authority](#). For the RSA ACE/Server® to communicate to the RSA ACE/Agent® through a firewall, all ports from 1024 to 65535/udp must be open from the Master and Slave IPs to the Agent IPs.
- Port 5500 is only required if you are using the SecurID login authority. For the RSA ACE/Agent to authenticate to the Master ACE/Server through a firewall, port 5500/udp must be open from the Agent IP to the Master and Slave IP.

### Related topics

- [Security and Secure Global Desktop](#)
- [Using Secure Global Desktop with firewalls](#)
- [What is an array?](#)
- [Introducing application server load balancing](#)

## What do I need to tell my users?

The following information is essential to help people use Secure Global Desktop:

Information	Description
Which program to use.	<p>If you are using the browser-based webtop:</p> <ul style="list-style-type: none"><li>• Users can log in to Secure Global Desktop using one of the supported web browsers. If Java™ technology is enabled, the Sun Secure Global Desktop Client is automatically installed.</li><li>• Users can manually download and install the Secure Global Desktop Client from <code>http://server.example.com</code> (you may alternatively use https). This adds a shortcut for starting the Secure Global Desktop Client to the desktop Start Menu.</li></ul> <p>If you are using the classic webtop, users can log in:</p> <ul style="list-style-type: none"><li>• Using one of the supported web clients.</li><li>• Using the Sun Secure Global Desktop Native Client. You can download the Native Client from <code>http://server.example.com</code> (you may alternatively use https).</li></ul>
What login URL to use.	<p>Use <code>http://server.example.com/sgd</code> to access the browser-based webtop.</p> <p>Use <code>http://server.example.com/tarantella</code> to access the classic webtop.</p> <p>You can also use https.</p> <p><i>server</i> is the name of a web server configured for Secure Global Desktop.</p>



What username and password to type to log in to Secure Global Desktop.	Secure Global Desktop supports many different <a href="#">types of user</a> , including users with ENS person objects, UNIX users, LDAP users and anonymous users. The usernames and passwords depend on the type of user.
What usernames and passwords to type to log in to application servers.	Applications on users' webtops may run on many different application servers. When a user clicks a link to start an application, Secure Global Desktop may prompt them for a username and password for the application server. By default, users may choose to save the authentication details in the password cache (stored securely on the Secure Global Desktop server) so they don't need to type their details more than once.
How to log out of a web server authenticated Secure Global Desktop session securely.	If you are using web server authentication, users should close their web browser after logging out of Secure Global Desktop.
How to get help.	When Secure Global Desktop is first installed, all users have a link to the User Guide guide on their webtop.

## Related topics

- [How can I make additional Native Clients available?](#)
- [Introducing Secure Global Desktop printing](#)

## What happens when a user's password expires?

Secure Global Desktop normally requires a user to supply passwords for:

- the Secure Global Desktop server they log in to and
- the application server on which they launch an application.

In most circumstances, Secure Global Desktop Administrators can configure what happens when a user supplies an expired password.

## Logging in to Secure Global Desktop

Secure Global Desktop logins are controlled by login authorities. The following table shows which login authorities support aged passwords.

Login authority	Supports aged passwords?
<a href="#">Anonymous user</a>	Not applicable. User logs in without a username or password.
<a href="#">ENS</a>	Yes, see below for details.
<a href="#">NT</a>	No.
<a href="#">LDAP</a>	Yes, see <a href="#">Enabling the LDAP login authority</a> for details.
<a href="#">Active Directory</a>	Yes, see <a href="#">Enabling the Active Directory login authority</a> for details.
<a href="#">UNIX Group</a>	Yes, see below for details.
<a href="#">UNIX User</a>	Yes, see below for details.
<a href="#">SecurID</a>	Yes.

**Note** For [web server/third party authentication](#), the expiry of the user's password is handled by the web server/third party authentication mechanism and is nothing to do with Secure Global Desktop.

If Secure Global Desktop can handle the expiry of the user's password, then when a user attempts to

log in with an expired password, the aged password dialog displays. This dialog:

- confirms that the password has expired and
- allows the user to enter and confirm a new password.

If the new password is accepted, the user is logged in to Secure Global Desktop.

**Note** For SecurID authentication, if the user's PIN has expired, a new PIN dialog displays instead of the aged password dialog.

## ENS/UNIX users and password expiry

If you want Secure Global Desktop to prompt ENS or UNIX users for a new password when they log in to Secure Global Desktop with an expired password, the Pluggable Authentication Module (PAM) interface must be installed on your Secure Global Desktop servers.

If the PAM interface is not installed, Secure Global Desktop will not be able to support aged passwords. An error message is logged in `/opt/tarantella/var/log/pemanagerpid_error.log` on server startup if this is the case.

When you install Secure Global Desktop, Secure Global Desktop Setup automatically creates PAM configuration entries for Secure Global Desktop by copying the current configuration for the `passwd` program.

- On Solaris Operating System platforms, entries are created in the `/etc/pam.conf` file.
- On Linux platforms, the `/etc/pam.d/tarantella` file is created.

## Launching applications

You can use Array Manager to modify the way that Secure Global Desktop deals with expired passwords on all application servers. The [Application Launch](#) panel lets you configure what happens when a user tries to launch an application on an application server for which their password has expired. Secure Global Desktop can:

- Let the user log in manually.
- Prompt the user for authentication, and attempt to launch the application again.
- Treat this as a launch failure.

The Prompt User option may not work on some application servers. In such circumstances, you must customize the appropriate [login script](#).

## Related topics

- [Login authorities](#)
- [Application Launch properties \(array-wide\)](#)

## Working with users in different locales

When you install Secure Global Desktop, the default language used for the browser-based webtop, the Sun Secure Global Desktop Client and for login scripts is English. Secure Global Desktop Administrators can configure Secure Global Desktop to add support for users in different locales.

**Note** The *classic* webtop is only available in English. The **Preferred Locale** attribute for person objects has no effect on the language used for the browser-based webtop.

### Setting the default language for the browser-based webtop

By default, the Secure Global Desktop Web Server Welcome page at `http://server.example.com` displays in English. To change the default language of the Welcome page, amend the symbolic link `/opt/tarantella/webserver/apache/<version>/htdocs/index.html` so that it links to another index page in this directory. For example to make the default Welcome page display in Japanese, link to the `index_ja.html` page.

When users log in using a web browser at the `http://server.example.com/sgd` URL, the default language used for messages displayed by the login dialog and the webtop is controlled by the `m_defaultLang = "en";` line in the following files:

- `/opt/tarantella/webserver/tomcat/<version>/webapps/sgd/resources/jsp/localeutils.jsp`
- `/opt/tarantella/webserver/tomcat/<version>/webapps/sgd/index.jsp`

To change the default language, edit this line and replace "en" with the language identifier for one of the following supported languages:

Language	Identifier
English	en
French	fr
Japanese	ja
Korean	ko

Simplified Chinese	zh_CN
Traditional Chinese	zh_TW

The default language is also controlled by the Preferred Language in the user's [profile](#). Whenever the Secure Global Desktop Client is started from the command line (for example when the Secure Global Desktop Client is in integrated mode), the language specified in the profile is used for messages displayed by the Secure Global Desktop Client, the login dialog, and the webtop. Secure Global Desktop Administrators can set the default language by editing the profiles in their organizational hierarchy.

**Note** To be able to display text for a locale, users must also have appropriate fonts installed on their client device.

## Overriding the default language

Users can override the default language as follows:

- On the Secure Global Desktop Web Server Welcome page (<http://server.example.com>), click one of the "flags" at the top of the page to select a preferred language and then click Log in to access a webtop in that language.
- Specify a different preferred language in the profile.
- Log in to Secure Global Desktop using a URL that specifies the preferred language. The URL is `http://server.example.com/sgd/index.jsp?langSelected=lang` where *lang* is one of the language identifiers listed in the table above. Users can manually type this URL in their web browser, or it can be specified as the Login URL in the profile.
- Run the Secure Global Desktop Client from the command line and use the `preferredlanguage lang` **command line argument** to set the language, where *lang* is one of the language identifiers listed in the table above. This argument can be used in shortcuts and shell scripts.

## Login scripts

By default, the [login scripts supplied with Secure Global Desktop](#), support system prompts in English. Administrators can add support for system prompts in other languages as follows:

- Edit the `vars.exp` login script and add a translation for each of the English prompts defined. You do not need to translate every prompt, only the prompts that are different to the English ones. The file contains examples to help you get started. You can also provide translations for the variables, strings and error message section to match the client/user locale.
- Configure the [Host Locale](#) attribute for your host objects to match a locale defined in `vars.exp`.

## Related topics

- [Working with the Sun Secure Global Desktop Client](#)
- [What are login scripts?](#)

## Working with the Sun Secure Global Desktop Client

The Sun Secure Global Desktop Client is the part of Secure Global Desktop that is installed on client devices and is required to run applications.

The Secure Global Desktop Client can operate in either of the following modes:

- **Webtop mode** - uses a [web browser to display a special web page](#), called a webtop, that lists the applications a user can run through Secure Global Desktop and provides controls for managing application sessions and printing. This is the default mode.
- **Integrated mode** - the list of applications that a user can run through Secure Global Desktop [displays in the desktop Start Menu on the client device](#). This allows users to run remote applications in the same way as local applications. Depending on other configuration factors, there may be no need to use a web browser.

**Note** You cannot use the Secure Global Desktop Client with the classic webtop.

Depending on the client platform, users see an icon in the System tray or Workspace switcher when the Secure Global Desktop Client is running.

The Secure Global Desktop Client performs the following functions:

- Gets information about the client device, such as the operating system, local printers and client drives.
- Manages the display of applications that are **not** configured to display in a web browser window (out-of-place applications).
- Maintains a communication connection (using the AIP protocol) with the Secure Global Desktop server.
- Receives and acts on events from the Secure Global Desktop server, for example the arrival of a print job.

## Installing the Secure Global Desktop Client

The Secure Global Desktop Client can be installed automatically or manually.

### Automatic installation



If you have a web browser with Java™ technology enabled, the Secure Global Desktop Client is installed automatically when you visit the `http://server.example.com/sgd` URL.

With automatic installation, different versions of the Secure Global Desktop Client are installed in separate directories. This means:

- Users only have to log in to an upgraded Secure Global Desktop server in order to upgrade the Secure Global Desktop Client.
- Users who log in to different Secure Global Desktop servers always run the correct Secure Global Desktop Client for the version of Secure Global Desktop.

The Secure Global Desktop Client is installed in the following directories:

- On Microsoft Windows client devices, in a user-specific writeable directory, for example:

```
C:\Documents and Settings\user\Local Settings\Temp\tcc\version
```

The actual location depends on the user's privileges, the operating system and the Java Plug-in being used.

- On UNIX/Linux/Mac OS X client devices, the user's home directory:

```
$HOME/.tarantella/tcc/version
```

If you want to use automatic installation and have more control over where the Secure Global Desktop Client is installed, you can develop your own web application for installing the Secure Global Desktop Client and use Secure Global Desktop web services to specify the installation location.

## Manual installation

With manual installation, you have full control over where the Secure Global Desktop Client is installed. You download and install the Secure Global Desktop Client from the Secure Global Desktop Web Server home page, `http://server.example.com`. Click the Install the Sun Secure Global Desktop Client link. The Sun Secure Global Desktop Client download page has instructions for downloading and installing the Secure Global Desktop Client.

On Microsoft Windows client devices, the default installation directory is: `C:\Program Files\Sun\Secure Global Desktop Client`. A shortcut for the Secure Global Desktop Client is also added to the Windows Start Menu.

**Note** Manual installation is not available for all supported client platforms.

## Configuring the Secure Global Desktop Client

The Secure Global Desktop Client needs to be configured so that it can connect to a Secure Global Desktop server. The connection settings are defined in a [client profile that is stored on the client device](#). The profile controls:

- The URL the Secure Global Desktop Client connects to when it starts, usually this is the URL used to log in to Secure Global Desktop.
- The operating mode of the Secure Global Desktop Client whether the applications a user can run display on a webtop or the user's desktop Start Menu.
- Whether or not the user is logged in automatically when the Secure Global Desktop Client starts.
- Whether or not the Secure Global Desktop Client starts automatically when the user logs in to their desktop system.
- Proxy server configuration, whether the settings are manually configured in the profile or determined from the web browser.

**Note** The Secure Global Desktop Client can only connect to a Secure Global Desktop server if they both have the same major/patch (4.xx) version number.

There is one profile for each Secure Global Desktop server that the user connects to. The profile is downloaded when the user connects to a Secure Global Desktop server. If the Secure Global Desktop Client has been installed manually, the user is prompted for initial connection information the first time the Secure Global Desktop Client is started.

## Running the Secure Global Desktop Client from the command line

Typically users log in to Secure Global Desktop by starting a web browser and visiting the `http://server.example.com/sgd` URL. Connecting to Secure Global Desktop in this way, automatically downloads and starts the Secure Global Desktop Client. However, you can also start the Secure Global Desktop Client from the command line and connect to a Secure Global Desktop server. You can run the Secure Global Desktop Client in either Webtop mode and Integrated mode in this way.

You start the Secure Global Desktop Client with the `tcc` command on Microsoft Windows client platforms or the `ttatcc` command on UNIX/Linux/Mac OS X client platforms, as follows:

```
tcc
  [ -application appname ]
  [ -loginurl url ]
  [ -preferredlanguage lang ]
  [ -profile profile ]
```

Argument	Description
<code>-application <i>appname</i></code>	<p>The name of an application to run. This does not have to be a TFN name.</p> <p><b>Note</b> If the application is not on the user's webtop, they cannot launch the application.</p>
<code>preferredlanguage <i>lang</i></code>	<p>The language to use in any dialogs and messages displayed by the Secure Global Desktop Client. This overrides the language defined in the profile. The following are the supported languages:</p> <ul style="list-style-type: none"> <li>• <code>en</code> for English</li> <li>• <code>fr</code> for French</li> <li>• <code>ja</code> for Japanese</li> <li>• <code>ko</code> for Korean</li> <li>• <code>zh_CN</code> for Simplified Chinese</li> <li>• <code>zh_TW</code> for Traditional Chinese</li> </ul>
<code>-profile <i>profile</i></code>	<p>The name of the profile to use when starting the Secure Global Desktop Client.</p> <p>Currently there is only one profile for each Secure Global Desktop server, called Default.</p> <p>To specify the profile for a particular server, use <code>-profile server.example.com::Default</code></p> <p><b>Note</b> Profile names are case sensitive.</p>
<code>-loginurl <i>URL</i></code>	<p>The login URL. This overrides the URL defined in the profile.</p>

**Note** The arguments are case-sensitive.

The command line does not allow you to supply a username and password. However, the Secure Global Desktop Client can be [configured to log a user in automatically](#).

## Examples

The command line for the Secure Global Desktop Client can be used to create your own shortcuts and

shell scripts. The following are some example commands:

**Note** If either the Connect on System Login or the Add applications to Start Menu options are enabled in a user's profile, the Secure Global Desktop Client automatically adds shortcuts for itself in the user's desktop Start Menu. The Sun Secure Global Desktop Software Release Notes has details of which desktop systems are supported.

### Example 1: Starting without any arguments

```
ttatcc
```

- The Secure Global Desktop Client starts using the settings defined in the Default profile, available from the user's profile cache.
- If there is no profile or it does not contain a login URL, the Secure Global Desktop Client starts but it cannot connect to a Secure Global Desktop server.
- If the user has previously connected to more than one Secure Global Desktop server, the Secure Global Desktop Client connects to the last Secure Global Desktop server the user connected to using the profile for that server.
- Example use: to start the Secure Global Desktop Client when the user always connects to the same Secure Global Desktop server.

### Example 2: Connecting to a particular Secure Global Desktop server

```
ttatcc -profile server.example.com::Default
```

- The Secure Global Desktop Client starts using the settings defined in the profile for `server.example.com`, available from the user's profile cache.
- If there is no profile in the cache for `server.example.com`, the Secure Global Desktop Client starts and connects to the last Secure Global Desktop server the user connected to using the profile for that server.
- Example use: to start the Secure Global Desktop Client when the user may connect to different Secure Global Desktop servers.

### Example 3: Overriding the login URL

```
tcc -loginurl URL
```

- The Secure Global Desktop Client starts using the settings defined in the Default profile, available from the user's profile cache, but connects to the specified URL.
- Depending on the URL, this could be used to launch an application.

- Example use: to start the Secure Global Desktop Client and connect to a single Secure Global Desktop server, but connect to different web applications on that server.

#### Example 4: Running a single application

```
ttatcc -application Write-O-Win
```

- The Secure Global Desktop Client starts using the settings defined in the Default profile and starts the specified application.
- If the Secure Global Desktop Client is in webtop mode or the user does not have an authentication token, the login URL defined in the profile is loaded into the user's default web browser.
- Example use: to start the Secure Global Desktop Client and connect to a single Secure Global Desktop server, but only run a single application.

#### Compatibility with previous versions

The Secure Global Desktop Client also supports the command line arguments available in versions 4.2x or earlier of Secure Global Desktop:

```
ttatcc
  -loginurl url
  -server server
  -port tcp
  -startimmediate
[ -secure ]
[ -baseroute ]
[ -firewalltraversal ]
[ -resource resource ]
[ -connectioncookie cookie ]
[ -ca pem_file ]
```

Argument	Description
<code>-loginurl <i>URL</i></code>	The URL that is to be used to log in to Secure Global Desktop.
<code>-server <i>server</i></code>	The fully-qualified DNS name of the Secure Global Desktop server the Secure Global Desktop Client is to connect to.
<code>-port <i>tcp</i></code>	The port on which the Secure Global Desktop Client is to connect to the Secure Global Desktop server. Usually this is port 5307/tcp when the user has a secure connection to Secure Global Desktop, otherwise port 3144/tcp is used.

<code>-startimmediate</code>	<p>Starts the Secure Global Desktop Client immediately and loads the URL specified by the <code>-loginurl</code> option in the user's default web browser.</p> <p><b>Note</b> From version 4.3, the Secure Global Desktop Client <b>always</b> starts immediately, whether this argument is used or not.</p>
<code>-secure</code>	Create a secure connection to the Secure Global Desktop server.
<code>-baseroute</code>	The base network route the Secure Global Desktop Client is to use to traverse a SOCKS proxy server.
<code>-firewalltraversal</code>	Indicates that the Secure Global Desktop server is using firewall forwarding. Connections to the Secure Global Desktop server and the webtop both use the same port, usually port 443/tcp.
<code>-resource resource</code>	For use by web service developers only, specifies the name of a resource file to use for the Sun Secure Global Desktop Client. The resource file is a DLL containing, for example icons and text. This can only be used on Windows client devices.
<code>connectioncookie cookie</code>	For use by web service developers only, supplies the cookie used by the Secure Global Desktop server to identify the webtop session for which the Sun Secure Global Desktop Client is being used.
<code>-ca pem_file</code>	<p>Specifies the path to the root certificate (<code>ca.pem</code> file) if you are using a custom Certificate Authority.</p> <p><b>Note</b> Because of security changes in version 4.3, you no longer need to use this argument.</p>

**Note** The arguments are case-sensitive.

## The Sun Secure Global Desktop Client Helper

When using a web browser with Java technology enabled, the Secure Global Desktop Client is supported by the Sun Secure Global Desktop Client Helper, which is a Java applet.

The Sun Secure Global Desktop Client Helper performs the following functions:

- Downloads and installs the Secure Global Desktop Client. This only applies if automatic installation is used.
- Obtains proxy server settings from the web browser and sends them to the Secure Global Desktop Client. This depends on the settings in the user's profile.
- Starts the Secure Global Desktop Client. This only happens when a user starts a web browser and goes to the login URL.
- Manages the display of applications that are configured to display on the webtop or in a new browser window (in-place applications).
- Responds to instructions received from the Secure Global Desktop Client, for example prompting the web browser to re-draw the screen.

The Sun Secure Global Desktop Client Helper is optional, see [Can I use the browser-based webtop without Java technology?](#) for details.

### Related topics

- [Introducing Sun Secure Global Desktop Software](#)
- [Integrating Secure Global Desktop with the desktop Start Menu](#)
- [Profiles and the Sun Secure Global Desktop Client](#)
- [Using Secure Global Desktop with proxy servers](#)
- [Securing client connections with Secure Global Desktop security services](#)

## Profiles and the Sun Secure Global Desktop Client

A profile is a group of configuration settings that control the Sun Secure Global Desktop Client. The settings in a profile define:

- How the Secure Global Desktop Client connects to a Secure Global Desktop server, for example the URL to connect to and the proxy server to use.
- The operating mode of the Secure Global Desktop Client, for example whether to display a webtop (Webtop mode) or whether the list of applications that a user can run displays in the desktop Start Menu (Integrated mode).
- How the Secure Global Desktop Client behaves, for example, if it loses a connection to a Secure Global Desktop server.

**Note** Profiles should not be confused with [login profiles](#). Login profiles control webtop content and other Secure Global Desktop-specific settings, such as printing and secure connections.

Every time the Secure Global Desktop Client starts it uses a profile. Users have one profile (one group of settings) for each Secure Global Desktop server they connect to.

### Creating, editing and deleting profiles

Secure Global Desktop Administrators can create, edit and delete profiles. Users can only edit their own profiles.

#### Administrators

Administrators create, edit and delete profiles with the Secure Global Desktop administration tool, Profile Editor. The Profile Editor is only available on an Administrator's webtop.

Administrators can create, edit and delete profiles for:

- Organization objects.
- Organizational unit objects.
- Login profile objects available in the `o=Tarantella System Objects` organization, for example `o=Tarantella System Objects/cn=LDAP Profile`.

Each object can only have one profile. The default system profile on the `o=Tarantella System`



Objects object can be edited but it cannot be deleted.

## Users

Administrators can configure which users can edit their own profiles. This is configured as follows:

1. On the [Array Properties](#) panel of Array Manager, profile editing for the array as a whole can be enabled or disabled. By default, it is enabled.

**Note** If profile editing is disabled in Array Manager, it is disabled for **all** users, including Administrators. However, Secure Global Desktop Administrators can still create and edit profiles using the Profile Editor application.

2. The [Profile Editing](#) attribute on organization, organizational unit or person objects can be used to control which users in the organization are allowed to edit profiles. The setting for this attribute can be inherited from a parent object in the organizational hierarchy so that Administrators can enable or disable profile editing for many users without having to edit each person object. By default, profile editing is enabled for all users.

Users edit their own profiles from their webtop by clicking the Edit button in the Applications area of the webtop and then clicking the Client Settings tab. Users can only edit the profile for the Secure Global Desktop server they are currently connected to.

**Note** [Anonymous users](#) cannot edit profiles. This is because these users are temporary.

## Profile settings

The following table lists the settings available in a profile with a description of what they do.

Setting	Description
Login URL	<ul style="list-style-type: none"><li>• The Secure Global Desktop URL to use for the profile, usually <code>http://server.example.com/sgd</code>.</li><li>• In Webtop mode, the URL is loaded automatically in the user's default web browser so that they can log in and access their webtop.</li><li>• In Integrated mode, the URL is only loaded in the user's default web browser if the user needs to log in to Secure Global Desktop, or if the Secure Global Desktop Client needs to obtain proxy server settings.</li><li>• The URL in a profile can be overridden by a <a href="#">command line argument</a>.</li></ul>

	<ul style="list-style-type: none"><li>• The default Login URL is <code>http://server.example.com:80/sgd/index.jsp</code>.</li></ul>
Connect on System Login	<ul style="list-style-type: none"><li>• If enabled, the Secure Global Desktop Client is started automatically with this profile whenever the user logs in to their client device.</li><li>• The Secure Global Desktop Client creates an application shortcut or symbolic link for itself in the startup folder for the desktop system. The links are created in the following locations:<ul style="list-style-type: none"><li>◦ Microsoft Windows - the Windows startup folder for the current user, usually <code>C:\Documents and Settings\username\Start Menu\Programs\Startup</code>.</li><li>◦ KDE - <code>\$HOME/.kde/autostart</code></li><li>◦ Gnome - <code>\$HOME/.config/autostart</code></li><li>◦ Sun Java Desktop System - <code>\$HOME/.config/autostart</code></li></ul></li><li>• This is disabled by default.</li></ul>
Automatic Client Login	<ul style="list-style-type: none"><li>• If enabled, as soon as the Secure Global Desktop Client starts, it will attempt to log the user in using an <a href="#">authentication token</a>.</li><li>• Only enable this option if the Add applications to Start Menu is enabled.</li><li>• This is disabled by default.</li></ul>
Add applications to Start Menu	<ul style="list-style-type: none"><li>• Controls how users interact with Secure Global Desktop.</li><li>• If enabled, the applications a user can run <a href="#">display in the desktop Start Menu</a> on the client device (Integrated mode). Users do not have any of the controls that are available on a webtop, for example controls for suspending and resuming applications.</li><li>• If disabled, the applications a user can run <a href="#">display on a webtop in a web browser</a> (Webtop mode).</li><li>• This is disabled by default.</li></ul>

Alternative PDF viewer	<ul style="list-style-type: none"><li>• The application command for an alternative PDF viewer to use with <a href="#">PDF printing</a>.</li><li>• If the application is not on the user's <code>PATH</code>, type the full path to the application.</li><li>• This setting only applies to UNIX, Linux and Mac OS X client devices.</li></ul>
Logging	<ul style="list-style-type: none"><li>• Controls the amount of information that is output to the Secure Global Desktop Client log file.</li><li>• The output is logged to a text file in the same directory as the Secure Global Desktop Client.</li><li>• The default is Errors only.</li></ul>
Preferred Language	<ul style="list-style-type: none"><li>• The default language to use when the Secure Global Desktop Client is started from the command line, for example when the Secure Global Desktop Client is in Integrated mode.</li><li>• The language selected is used for messages displayed by the Secure Global Desktop Client, the login dialog, and the webtop.</li><li>• See <a href="#">Working with users in different locales</a> for details.</li><li>• The default is en.</li></ul>
Check for Local X Server	<ul style="list-style-type: none"><li>• If enabled, the Secure Global Desktop Client checks whether there is an X server running on the client device.</li><li>• Enabling this option can improve performance when launching X applications that are configured to display using <a href="#">an X server on the client device</a>. If a local X server is not available, an independent window is used instead.</li><li>• This setting only applies to Windows client devices.</li><li>• This is disabled by default.</li></ul>

Proxy settings	<ul style="list-style-type: none"> <li>• Settings that control how the Secure Global Desktop Client determines what proxy servers to use.</li> <li>• Use default web browser settings means use the proxy server settings configured in the user's default web browser.</li> <li>• Manual proxy settings allows you to define the proxy server settings in the profile. You can specify either an HTTP or a SOCKS proxy server or both.</li> <li>• In Integrated mode, if the proxy settings are determined from a web browser, the Secure Global Desktop Client has to start the web browser at least once in order to detect what the proxy settings are.</li> <li>• If the proxy settings are determined from a web browser, the settings are cached and used the next time the Secure Global Desktop Client starts.</li> <li>• If Establish proxy settings on session start is enabled, every time the Secure Global Desktop Client starts, the default web browser is started so that the proxy settings can be determined. The cached proxy settings are not used.</li> <li>• The default is: Use default web browser settings. Establish proxy settings on session start is disabled.</li> </ul>
Connection Failure	<ul style="list-style-type: none"> <li>• Settings that control what the Secure Global Desktop Client does if the connection to a Secure Global Desktop server is lost, whether to always reconnect, to never reconnect or to ask the user.</li> <li>• If the Secure Global Desktop Client reconnects, these settings control how many attempts are made to reconnect and the time in seconds between each attempt.</li> <li>• If the Secure Global Desktop Client is unable to reconnect, the webtop session ends and any running applications are ended or suspended, depending on the <a href="#">resumability setting of the application</a>.</li> <li>• The default settings are: Always attempt to reconnect, Number of attempts: 6, and Interval: 10.</li> </ul>

## The profile cache

Profiles created by Administrators are stored on the Secure Global Desktop server on which they are created and then copied to all the other members of the array so that they are available for editing on any Secure Global Desktop server.

When a user first logs in to Secure Global Desktop, the Secure Global Desktop Client downloads the profile to a profile cache on the client device. The profile that is downloaded is the first match of the following:

- The profile defined for a system login profile object that is assigned to the user. For example, if the user was authenticated using the UNIX user login authority and a profile has been created for the `.../_ens/o=Tarantella System Objects/cn=UNIX User Profile` object, this is the profile that is downloaded.
- The profile defined by an Administrator for the organizational unit or organization to which the user belongs. If there is no profile for the user's organizational unit, Secure Global Desktop checks any parent object further up the organizational hierarchy to see whether they have a profile.
- The system default profile defined for the `o=Tarantella System Objects` object.

When a user edits and saves a profile, they override the profile defined by an Administrator (or the system default profile) and create a user-specific profile that is only saved in the profile cache on the client device.

**Note** Users must log out of Secure Global Desktop and log in again for changes to their profile to take effect.

The profile cache is specific to each user who logs in to Secure Global Desktop from the client device and is stored in the following locations:

- On UNIX, Linux and Mac OS X client devices - `$HOME/.tarantella/tcc/profile.xml`
- On Microsoft Windows client devices - `C:\Documents and Settings\username\Local Settings\Application Data\Sun\SSGD\profile.xml`

The same profile cache is used by the Secure Global Desktop Client whether it has been installed manually or automatically.

The profile cache is updated each time the user edits a profile or each time the user logs in if they are using the profile defined by an Administrator.

The profile cache contains one profile for each Secure Global Desktop server the user has connected to.

Users can restore a profile to the default settings by editing the profile and clicking the Reset button. This resets the profile to the settings defined for the system default profile on the `o=Tarantella System Objects` object.

## Related topics

- Working with the Sun Secure Global Desktop Client

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Configuring the Sun Secure Global Desktop Client for desktop Start Menu integration

In a default installation, users [log in to Secure Global Desktop and display a webtop](#). Sun Secure Global Desktop Client can also be configured to operate in [Integrated mode](#) so that the list of applications a user can run displays in the desktop Start Menu instead of on the webtop.

To use Secure Global Desktop in this way:

- Integrated mode must be enabled in the user's profile. Other settings in the profile also affect how Integrated mode works.
- Applications may have to be configured to give users the best experience.
- Users have to perform an initial login in webtop mode.

**Note** See the Sun Secure Global Desktop Software Release Notes for details of the desktop systems that are supported for Integrated mode.

### Configuring the profile

Integrated mode must be enabled in the user's profile. Secure Global Desktop Administrators can enable Integrated mode by creating profiles for organization and organizational unit objects. Alternatively, if [profile editing](#) is enabled, users can enable Integrated mode themselves.

The following settings in a profile are applicable to using Integrated mode:

Setting	Description
Add applications to Start Menu	<ul style="list-style-type: none"><li>• Enables Integrated mode.</li><li>• Causes the Secure Global Desktop Client to add icons to the user's desktop Start Menu.</li></ul>

Automatic Client Login	<ul style="list-style-type: none"> <li>• Enables automatic logins to Secure Global Desktop.</li> <li>• If this is disabled, users must log in with a web browser. This means they see a webtop <b>and</b> have applications in their desktop Start Menu.</li> <li>• See <a href="#">Using the authentication token login authority for automatic logins</a> for more details.</li> </ul>
Connect on System Login	<ul style="list-style-type: none"> <li>• If enabled, the Secure Global Desktop Client connects each time the user logs into the desktop system.</li> <li>• If Automatic Client Login is also enabled, this gives users a single sign-on experience.</li> </ul>
Proxy server settings	<ul style="list-style-type: none"> <li>• Proxy server settings can be configured in the profile itself or detected from the default web browser.</li> <li>• Configuring the settings in the profile itself reduces the need for a web browser.</li> <li>• See <a href="#">Using Secure Global Desktop with proxy servers</a> for more details.</li> </ul>

**Note** If a user edits their profile, they must log out of Secure Global Desktop and log in again for the changes to take effect.

## Configuring applications

When launched from a desktop Start Menu, applications that are configured to [Display Using](#) the webtop or a new browser window are displayed in an independent window. You may want to configure these applications to use a different window.

For applications that are configured to [Display Using](#) an independent window, closing the window may end or suspend the emulator session, depending on the object's [Window Close Action](#) attribute.

In Integrated mode, there are no controls for suspending and resuming individual application instances. Applications that are configured to be [always resumable](#) are automatically suspended when you log out and resumed when you log in. While in Integrated mode, you can only resume a suspended session by displaying a webtop and using the session controls for the application.

You may also want to configure the [Max Instances](#) attribute to limit the number of instances users can run.

## Performing the initial login in webtop mode



1. Start a web browser and go the `http://server.example.com/sgd` URL.

**Note** The **Secure Global Desktop Client** can be manually downloaded, installed and started from the command line.

2. Log in and display a webtop.

3. Enable Integrated mode.

- Click the Edit button in the Applications area of the webtop and then click the Client Settings tab.
- Check the Add applications to Start Menu box.
- To log in automatically, check the Automatic Client Login box. This generates an authentication token when the profile is saved.
- To start the Secure Global Desktop Client when you log in to the desktop system, check the Connect on System Login box.
- Configure the proxy server settings.
- Click Save.

4. Log out of Secure Global Desktop.

5. Log in to Secure Global Desktop **using the Login link** on the desktop Start Menu.

After the initial login, and depending on configuration, users do not need to use a web browser to access Secure Global Desktop. However, the Secure Global Desktop Client may start the user's default web browser if the user needs to log in or if it needs to obtain proxy server settings from the browser.

### Generating new authentication tokens

If a user needs to generate a new authentication token, they must edit their profile as follows:

1. Clear the Automatic Client Login box.
2. Click Save.
3. Check the Automatic Client Login box.
4. Click Save.

### Related topics

- Integrating Secure Global Desktop with the desktop Start Menu
- Introducing Sun Secure Global Desktop Software
- Working with the Sun Secure Global Desktop Client
- Profiles and the Sun Secure Global Desktop Client
- Using Secure Global Desktop with proxy servers
- Securing client connections with Secure Global Desktop security services

[Secure Global Desktop Administration Guide](#) > [Applications, documents and hosts](#) > [Launching a single application without displaying a webtop](#)

## Launching a single application without displaying a webtop

With Secure Global Desktop you can launch a single application without displaying webtop. How you do this depends on whether you are using the browser-based webtop or the classic webtop.

**Note** If an application is not on the user's webtop, they cannot launch the application.

### Browser-based webtop

For the browser-based webtop you can launch a single application either by using the Secure Global Desktop Client command line or by using Secure Global Desktop web services.

#### Using the Secure Global Desktop Client command line

You can use the [Secure Global Desktop Client command line](#) to launch a single application. You can use the command line to develop your own shortcuts or shell scripts. This works best if you use [automatic logins](#).

#### Using Secure Global Desktop web services

You can use Secure Global Desktop web services to develop your own "application launcher" to launch a single application from a URL. You can use this method to launch an application from a bookmark or a favorite. Secure Global Desktop provides an example application that shows what is possible with web services.

The URL for using the Secure Global Desktop example application is:

```
http://server.example.com/sgd/launcher.jsp?  
o=application_name&u=username&p=password&e=true|false
```

The URL has the following parameters:

Parameter	Description
<code>o=application_name</code>	The name of the application object. This does not have to be a TFN name.

<code>u=username</code>	The username to use to log in to Secure Global Desktop.
<code>p=password</code>	The password to use to log in to Secure Global Desktop.
<code>e=true false</code>	<code>true</code> means display an edit page where users can override some of the application attributes. <code>false</code> means do not display edit page.

**Note** All of the parameters are optional.

For example, the following URL launches the Write-o-win application using the configuration for the application object defined in Object Manager.

```
http://boston.indigo-insurance.com/sgd/launcher.jsp?o=Write-o-win&u=indigo&p=purple&e=false
```

## Classic webtop

If you are using the Java™ technology clients, you can use [Javascript to launch a single application](#).

If you are using the Native Client, you can use the [Native Client command line](#) to launch a single application. You can use the command line to develop your own shortcuts or shell scripts.

### Related topics

- [Launching applications from JavaScript](#)

[Secure Global Desktop Administration Guide](#) > [Clients and webtops](#) > Does the browser-based webtop use themes?

## Does the browser-based webtop use themes?

No. The browser-based webtop does not use [login themes](#), [webtop themes](#), icon themes or [preferred locales](#) to determine the appearance of the webtop.

However, different *styles* of the browser-based webtop are available by visiting a different URL:

URL	Style	Description
<code>http://server.example.com/sgd</code>	Standard	The "default" browser-based webtop.
<code>http://server.example.com/sgd/hierarchy.jsp</code>	Hierarchical	A webtop that lists webtop content according to the <a href="#">groups</a> the applications and documents belong to.
<code>http://server.example.com/sgd/thin.jsp</code>	Thin	A webtop that does not use Java™ technology to start the Sun Secure Global Desktop Client or display applications.

If you want to use themes to determine the appearance of the webtop you can either use the *classic* webtop (`http://server.example.com/tarantella`) or develop your own webtop application using the Secure Global Desktop web services API.

### Related topics

- [Introducing Sun Secure Global Desktop Software](#)

## Can users access Secure Global Desktop without Java technology?

Yes, with some additional configuration.

### Browser-based webtop

The browser-based webtop uses the Sun Secure Global Desktop Client Helper, which is a Java™ applet, to perform the following functions:

- To download, install and start the Sun Secure Global Desktop Client.
- To obtain proxy server settings from the user's web browser.
- To display applications on the webtop or in a new browser window.

If your organization prefers not to use Java technology, you must manually download and install the Secure Global Desktop Client, and then configure it to connect to Secure Global Desktop.

#### 1. Manually download and install the Secure Global Desktop Client.

- You download the Secure Global Desktop Client from the Secure Global Desktop Web Server at <http://server.example.com>.
- Click the link to Install the Sun Secure Global Desktop Client.
- The download page and Sun Secure Global Desktop Software Installation Guide have details of how to install the Secure Global Desktop Client.

#### 2. Start the Secure Global Desktop Client and connect to Secure Global Desktop.

- If available, start the Secure Global Desktop Client from the shortcut in the desktop Start Menu. Otherwise, start the Secure Global Desktop Client from [the command line](#).
- The first time you start the Secure Global Desktop Client, it prompts you for the URL to connect to (normally <http://server.example.com/sgd>) and for the proxy server settings to use.
- When the Secure Global Desktop Client connects, it starts your default web browser and the login page displays.
- Log in. The webtop displays.

#### 3. Edit the profile for your client device.

- On the webtop, click the Edit button in the Applications area of the webtop. Click the Client Settings tab and [edit the profile](#).
- Configure the operating mode of the Secure Global Desktop Client, whether webtop mode or integrated mode.

- **Integrated mode** gives users the best user experience when Java technology is unavailable, check the Add applications to Start Menu box.
- Use **automatic logins** to minimize the use of a web browser, check the Automatic Client Login box.
- Whenever the Secure Global Desktop Client needs to display a page in a web browser, for example to display a webtop or a login page, it always starts the **default** web browser.
- To update the webtop display, users may have to manually reload the page. Alternatively, change the login URL to use the "thin" style webtop, `http://server.example.com/sgd/thin.jsp`.
  - Configure the **proxy server settings**. You must specify the proxy server settings in the profile because these settings cannot be obtained from the web browser.
  - Click save.

**Note** Secure Global Desktop Administrators can pre-configure many of these settings for users by editing the profile for an organization or organizational unit object.

#### 4. Log out of Secure Global Desktop.

When Java technology is disabled, applications that are configured to **Display Using** the webtop or a new browser window are displayed in an independent window instead.

### Classic webtop

To access Secure Global Desktop and use the classic webtop without Java™ technology, users must use the Sun Secure Global Desktop Native Client.

The Native Client can be downloaded from the Secure Global Desktop Web Server at `http://server.example.com`.

Applications that are configured to **Display Using** the webtop or a new browser window are displayed in an independent window instead.

#### Related topics

- Working with the Sun Secure Global Desktop Client
- Using Secure Global Desktop with proxy servers
- Integrating Secure Global Desktop with the desktop Start Menu



## Relocating the browser-based webtop to your own JSP container

The browser-based webtop is a JavaServer Pages (JSP) application which you can relocate to your own JSP container. The JSP container can be on the same host as Secure Global Desktop or on a different host.

**Note** You can't relocate the *classic* webtop.

To use your own JSP container, the container must support:

- Version 2.2 of the Java Servlet specification.
- Version 1.2 of the JavaServer Pages specification.

**Note** Once you relocate the webtop to your JSP container, you have to manually upgrade the webtop by following the above steps for each new release.

To relocate the browser-based webtop:

1. Re-configure the ports used by the Secure Global Desktop Web Server.
  - If your web server/JSP container is on the **same host** as Secure Global Desktop, you may have to re-configure the ports used by the Secure Global Desktop Web Server.
  - The Secure Global Desktop Web Server may be listening on the standard HTTP or HTTPS ports (80/tcp or 443/tcp), depending on the ports selected when you installed Secure Global Desktop. You need to configure your web server to listen on ports 80/tcp or 443/tcp and configure the Secure Global Desktop Web Server to use different ports (by editing the `/opt/tarantella/webserver/apache/version/conf/httpd.conf` file).
  - The Tomcat component of the Secure Global Desktop Web Server uses port 8005/tcp and 8009/tcp. If these ports are used elsewhere, for example by your JSP container, you must change the Tomcat configuration. Edit the `/opt/tarantella/webserver/tomcat/version/conf/server.xml` file and change the server shutdown port (port 8005/tcp) and the Coyote/JK2 AJP 1.3 Connector port (8009/tcp).
2. Copy the webtop web application to your JSP container.
  - Copy all the files in the `//opt/tarantella/webserver/tomcat/<version>/webapps/sgd` directory into the web applications directory on the new host.
3. Copy the required library and class files.
  - The browser-based webtop requires some additional library and class files, which must be

copied to your container.

- Copy the following Jar files from the `//opt/tarantella/webserver/tomcat/<version>/common/lib` directory to the global library directory on your container:
  - `axis.jar`
  - `commons-discovery.jar`
  - `commons-logging.jar`
  - `jaxrpc.jar`
  - `saaaj.jar`
  - `xerces.jar`
- Copy the following class files from the `//opt/tarantella/webserver/tomcat/<version>/common/classes` directory to the global class directory on your container:
  - `com/tarantella/tta/webservices/client/listener/SSLListener.class`

#### 4. Configure the web services endpoints.

- The browser-based webtop uses the SOAP protocol (over HTTP) to access the services provided by a Secure Global Desktop server. The browser-based webtop uses a `Resources.properties` file to determine which server and port to send the web services requests to. This is currently set to `http://localhost`.
- Edit the `Resources.properties` file in the `sgd/WEB-INF/classes/com/tarantella/tta/webservices/client/apis` directory **on the new host**. Replace `http://localhost:port` with `http://server:port` where *server* is the DNS name of a Secure Global Desktop server and *port* is the port that the Secure Global Desktop Web Server listens on. Do this for each of the web services listed in the properties file.
- If the webtop has been relocated to a different host or you are using Secure Global Desktop security services, we recommend you [secure the SOAP connections to a Secure Global Desktop server](#).

#### 5. Restart your JSP container and the Secure Global Desktop Web Server.

- You must restart your JSP container to apply the global library and class file changes.
- If you made any configuration changes to the Secure Global Desktop Web Server, you must restart it (`tarantella webserver restart`) to apply the changes.

#### 6. Log in to the relocated webtop.

**Note** If you are using third party authentication, you may also want to configure [a new trusted user](#) for the relocated webtop.

#### Related topics

- Configuring your own web server for use with Secure Global Desktop
- Securing the SOAP connections to a Secure Global Desktop server
- Web server/third party authentication

## Secure Global Desktop and Java archives

Secure Global Desktop uses Java™ applets for a variety of purposes. These Java applets must be downloaded from the Secure Global Desktop server to the client device's web browser.

The files that make up each applet can be combined into a Java archive. Java archives are useful because:

- They may be compressed, which makes them faster to download.
- They may include more than one applet.
- They may be digitally signed.
- Web browsers can keep local copies of them, which in some cases means they may only need to be downloaded once.

Web browsers can keep local copies of Java archives either by *caching* them, or *locally installing* them:

- Caching a Java archive means the browser stores the archive in its cache, along with other temporary files. However, when the cache is full, or if an applet isn't used for a while, the browser may delete the archive. Similarly, if a user manually clears their browser's cache, the archive is deleted.
- Installing a Java archive is more permanent. The archive can only be removed by the user.

Web browsers usually prompt the user for permission to cache/install an archive. For the archive to be cached/installed, the user must grant permission.

The Java archives in Secure Global Desktop work correctly with all supported browsers. However, some browsers have settings which can disable support for Java archives. If you have changed a particular browser's configuration, the browser may be unable to cache or install Java archives. You can always re-enable Java archive support by returning the browser to its default configuration.

### If you are using the classic webtop

Secure Global Desktop provides several types of Java archive, as different web browsers support different types of archive. If you are using the classic webtop, Secure Global Desktop uses the mappings in the `/opt/tarantella/etc/data/archives.txt` file to control which archive types are used with which browsers.

The table below shows:

- the setting required in `archives.txt` to use an archive type
- a description of the archive type and
- the features of the archive.

Setting	Archive type	Compression	Local copy	Signed
cab	Microsoft cabinet files	Compressed	Cached	Signed
cab4	Microsoft distribution units	Compressed	Installed	Signed
jpsjar	Archives signed using Sun JDK™ suitable for Sun Java Plug-in	Compressed	Cached	Signed
nsjar	Netscape signed installable Java archives	Compressed	Installed	Signed
sjar	Netscape signed non-installable Java archives	Compressed	Cached	Signed
zip	Zip archives	Uncompressed	Cached	Not signed

**Note** Netscape signed Java archives can be used with non-Netscape browsers.

By default, Secure Global Desktop uses these settings for the following browsers:

Browser/platform	Setting
Microsoft Internet Explorer 5 on Windows	cab4
Microsoft Internet Explorer 6 on Windows using Microsoft Virtual Machine	cab4
Microsoft Internet Explorer 6 on Windows using Sun Java Plug-In	jpsjar
Microsoft Internet Explorer on Apple Mac OS X 10.2+	jpsjar
Netscape 6.x and 7.x	jpsjar

**Note** The cab4 setting used by default for Internet Explorer users on Windows means that the archive is installed locally. However, the ability to install archives locally requires Administrator privileges. If Secure Global Desktop detects that the user does not have these privileges, it will automatically use the cab archive type instead as this is cached rather than installed.

### Customizing which browsers receive which archives

If the archive types used by default are unsuitable, you can edit the `/opt/tarantella/etc/data/archives.txt` file to change which archive types users receive. The file contains comments to help you customize archive delivery.

If you only need to temporarily override the settings in the `archives.txt` file so that you use a different Java archive, you can do this by running the Secure Global Desktop CGI program `ttaarchives.cgi` with a query string. This program sets a cookie which overrides `archives.txt`. For example, using the URL `http://server/tarantella/cgi-bin/ttaarchives.cgi?cab` sets your session to use the Microsoft cabinet archive. The cookie lasts for as long as you have your web browser running. The cookie is deleted when you close the web browser.

You can find full details on the query string settings available for `ttaarchives.cgi` by running:

```
http://server/tarantella/cgi-bin/ttaarchives.cgi?
```

### Related topics

- [How does Secure Global Desktop use applets?](#)

## Running the Native Client from the command line

### Syntax

```
ttwebtop
[ -anonymous ]
[ -application application ]
[ -args arguments ]
[ -cache ]
[ -help ]
[ -login ]
[ -password password ]
[ { -showwebtop | -minimized } | -trayicon ]
[ -url URL ]
[ -username username ]
[ -version ]
```

### Description

Runs the Native Client for UNIX or Windows from the command line. The options are case sensitive.

**Note** The Native Client can only be used to access the *classic* webtop.

Option	Description
<code>-anonymous</code>	Allows the user to log into Secure Global Desktop without supplying a username and password, if <a href="#">anonymous access</a> is enabled on the Secure Global Desktop server.
<code>-application <i>application</i></code>	Launches an instance of an application without displaying the webtop. For <i>application</i> , use the name of the application as it appears in the Name field in Object Manager. If the name contains spaces, enclose it in double quotes, for example "X Claim".

<p><code>-args</code> <i>arguments</i></p>	<p>Used with the <code>-application</code> option to supply command-line arguments/parameters for the application, for example, "<code>-bg red</code>".</p> <p>To be able to use this option you must also enable client overrides on the Secure Global Desktop server. You do this by running the following command:</p> <pre>tarantella config edit --tarantella-config-applaunch-allowclientoverrides true</pre> <p>This option is only available for the Native Client for Microsoft Windows.</p>
<p><code>-cache</code></p>	<p>Use Native Client password caching.</p>
<p><code>-help</code></p>	<p>Displays command-line usage information. This option is only available for the Native Client for UNIX.</p>
<p><code>-login</code></p>	<p>Hides the Native Client Log in dialog and logs the user in to Secure Global Desktop using the password in the password cache. You should use the <code>-cache</code> option with this option.</p>
<p><code>-minimized</code></p>	<p>Forces the webtop to be minimized as soon as it is launched.</p> <p>If you are using the Native Client for Microsoft Windows, this disables the Show in system tray option in the Native Client options.</p>
<p><code>-password</code> <i>password</i></p>	<p>The password the user uses to log in to the Secure Global Desktop server.</p> <p>Only the Native Client for Microsoft Windows allows you to enter a password immediately after the <code>-password</code> option. See examples 3 and 4 below for the differences between UNIX and Windows.</p>



<code>-showwebtop</code>	<p>Forces the webtop to display if its previous state was minimized.</p> <p>If you are using the Native Client for Microsoft Windows, this disables the Show in system tray option in the Native Client options.</p>
<code>-trayicon</code>	<p>Displays Secure Global Desktop as an icon in the Windows system tray instead of displaying a webtop. This option is only available for the Native Client for Microsoft Windows.</p> <p>The Secure Global Desktop icon in the Windows system tray :</p> <ul style="list-style-type: none"><li>• is colored when you are logged in</li><li>• displays a cog when you are launching an application and</li><li>• is grayed out when you are logged out.</li></ul> <p>You click the Secure Global Desktop icon to see the list of applications you can run. You right-mouse click the icon to access the Native Client menu options.</p> <p>This option disables the Always show and Auto hide options in the Native Client options.</p> <p>If you use this option with the <code>-application</code> option, only the Native Client menu options are available from the system tray icon.</p>
<code>-url <i>URL</i></code>	<p>Secure Global Desktop server URL.</p>
<code>-username <i>username</i></code>	<p>The username the user uses to log in to the Secure Global Desktop server.</p> <p>For the Native Client for Microsoft Windows, if you do not supply a username on the command line, the Log in dialog will display even if the <code>-login</code> option is used.</p> <p>For the Native Client for UNIX this is optional. If it is not supplied, the value of the LOGNAME environment variable is used.</p>

`-version`

Displays version information about the Native Client. This option is only available for the Native Client for UNIX.

## Using the Native Client password cache

The Native Client password cache is completely unrelated to the application server password cache and is always specific to the Secure Global Desktop server (as shown by the `-url` option) the user is logging in to. If a user can log in to different Secure Global Desktop servers, they will have to cache passwords for each Secure Global Desktop server they have access to.

The `-cache` option performs two alternative functions:

- It forces the Native Client to prompt the user for their Secure Global Desktop login password and then to store it encrypted on the client.
- When used with the `-login` option, it forces Secure Global Desktop to look up passwords in the password cache.

When password caching is used, the username, the url and password combination is stored as an obfuscated string either in the Window's registry or in a UNIX userinfo file. If you are particularly concerned about security, we recommend you do not cache passwords.

Examples 2, 3 and 6 below show you how to cache passwords.

Whenever you cache a password, the Native Client prompts you to confirm the password. The password confirmation only checks what has been typed, it does not validate the password.

You should use the `-login` option with the `-cache` option, to prevent the Native Client Log in dialog from displaying, as in examples 2 and 6 below. If you use these options together, the Native Client Log in dialog will only display if:

- the URL is incorrect,
- the password has not already been cached,
- the password has expired,
- the cached password is incorrect, or
- the username is incorrect.

To change their own password, a user can either:

- remove the `-login` option (see example 2 below), so that the Native Client Log in dialog displays or
- for Native Client for UNIX only, they can store a new password (see example 3 below).

## Running webtops and single applications

When you run the Native Client without the `-application` option, you get a standard webtop. If you use the `-application` option, that application is launched (or resumed) without displaying the webtop. This option can be used to integrate applications with a desktop application or window manager.

When you run an application, the Native Client establishes a connection to the Secure Global Desktop server. If you launch another application using the same username and URL, the existing connection will be used unless the `-anonymous` option is used. This allows you to run several applications at once from separate shortcuts.

## Examples

### Example 1 - running the Native Client and logging in each time

The user Graham Green wants log in to the Secure Global Desktop server newyork. On the command line he types:

```
ttwebtop -url http://newyork.indigo-insurance.com/tarantella \  
-username green
```

When Graham runs this command, the Log in dialog displays. He enters his password and then the Native Client logs him in to Secure Global Desktop. He sees a Webtop.

With the Native Client for UNIX, if Graham's LOGNAME environment variable is `green`, he can leave out the `-username` option.

### Example 2 - running a webtop with a cached password

The user Emma Rald wants log in to the Secure Global Desktop server newyork with her cached password. On the command line she types:

```
ttwebtop -url http://newyork.indigo-insurance.com/tarantella \  
-username emmarald -login -cache
```

The first time Emma runs this command, the Log in dialog displays. She enters her password (if she uses the Native Client for Microsoft Windows, she also has to confirm the password). The Native Client then caches the password and logs her in to Secure Global Desktop. She sees a Webtop.

The Native Client for UNIX lets you pre-cache a password, see example 3 below.

The next time she runs this command, Emma is logged straight in to Secure Global Desktop and sees her webtop.

With the Native Client for UNIX, if Emma's LOGNAME environment variable is `emmarald`, she can leave out the `-username` option.

### Example 3 - caching a password without logging in (Native Client for UNIX only)

The user Sid Cerise wants to cache his password for the Secure Global Desktop server `newyork` **without** logging in. On the command line he types:

```
ttwebtop -url http://newyork.indigo-insurance.com/tarantella \  
-username cerise -password -cache
```

When he runs this command, he is prompted on the command line for his password and then has to confirm it. The Native Client then caches the password and exits.

If Sid's LOGNAME environment variable is `cerise`, he can leave the `-username` option out.

**Note** You can only cache a password in this way with the Native Client for UNIX.

### Example 4 - bypassing the Log in dialog without using a cached password (Native Client for Microsoft Windows only)

The user Bill Orange wants to log in to the Secure Global Desktop server `newyork` **without** using a cached password and bypassing the Log in dialog. On the command line he types:

```
ttwebtop -url http://newyork.indigo-insurance.com/tarantella -login \  
-username orange -password ldespairN -minimized
```

Bill is logged in to Secure Global Desktop and gets a minimized webtop.

The password displays in clear text on the command line.

**Note** You can only log in in this way with the Native Client for Microsoft Windows. This method of logging in is particularly useful for testing.

### Example 5 - running a single application and logging in each time

The user Ginger Butcher wants to log in to the Secure Global Desktop server `newyork` **without** caching her password and run the Array Manager application. On the command line she types:

```
ttwebtop -url http://newyork.indigo-insurance.com/tarantella \  
-username ginger -application "Array Manager"
```

When Ginger runs this command, the Log in dialog displays. She enters her password and then the Native Client logs her in to Secure Global Desktop. The Array Manager application starts. She does not see a webtop.

With the Native Client for UNIX, if Ginger's LOGNAME environment variable is `ginger`, she can leave out the `-username` option.

**Note** Because the application name Array Manager contains a space, Ginger encloses it in quotes on the command line.

### Example 6 - running a single application using a cached password

The user Violet Carson wants to log in to the Secure Global Desktop server newyork using her cached password and run the XClaim application. On the command line she types:

```
ttwebtop -url http://newyork.indigo-insurance.com/tarantella -login \  
-username violet -cache -application XClaim
```

The first time Violet runs this command, the Log in dialog displays. She enters her password (if she uses the Native Client for Microsoft Windows, she also has to confirm the password). The Native Client then caches the password and logs her in to Secure Global Desktop. The XClaim application starts.

The next time she runs this command, Violet is logged straight in to Secure Global Desktop and the XClaim application starts. She does not see a webtop.

With the Native Client for UNIX, if Violet's LOGNAME environment variable is `violet`, she can leave out the `-username` option.

#### Related topics

- [How can I make additional Native Clients available?](#)

## Native Client preferences files on UNIX, Linux and Mac OS X client devices

The Native Client on UNIX, Linux and Mac OS X client devices uses a preferences file to control how users connect to a Secure Global Desktop server and how they display web documents.

The preferences are stored in the `$HOME/.tarantella/native-preferences` file. Each preference is specified using a line of the form:

```
Preference=value
```

The following preferences can be defined:

Preference	Description
URL	The URL to be used to log in to Secure Global Desktop.  The URL is displayed in the login dialog.
Username	The username to be used to log in to Secure Global Desktop.  The username is displayed in the Native Client login dialog.
Anonymous	Whether to check Log In Anonymously in the login dialog. Use 1 for yes, 0 for no.
DocLaunch	The method of viewing web documents: <ul style="list-style-type: none"><li>• 0 = Automatic.</li><li>• 1 = Run the configured DocBrowser application on the host (see below).</li><li>• 2 = Use the application object configured to display web documents.</li></ul>
CertsFile	The full path to a root certificate file (the <code>ca.pem</code> file) if you are using a <a href="#">custom Certificate Authority</a> . For example:  <pre>CertsFile=/usr/local/global-certs/ca.pem</pre>

UseProxy	Whether to use an HTTP proxy server when connecting to Secure Global Desktop. Use 1 for yes, 0 for no (default).
ProxyHost	The Internet hostname of a host running an HTTP proxy server. This setting is not used unless UseProxy=1.  <pre>ProxyHost=chicago.indigo-insurance.com</pre>
ProxyPort	The port on ProxyHost where the HTTP proxy server listens. This setting is not used unless UseProxy=1. A ProxyHost must also be specified. The default value is 8080.
NoProxyList	A semicolon-separated list of Internet hostnames for which connections are <b>not</b> to be proxied. This setting is not used unless either UseProxy=1 or UseSocks=1.  <pre>NoProxyList=chicago.indigo-insurance.com;detroit.indigo-insurance.com</pre>
DocBrowser	The full path of the application to use for displaying web documents, if DocLaunch=1. For example:  <pre>DocBrowser=/usr/bin/netscape</pre>
UseSocks	Whether to use a Socks proxy server when connecting to Secure Global Desktop. Use 1 for yes, 0 for no (default).
SocksHost	The Internet hostname of a host running a Socks proxy server. This setting is not used unless UseSocks=1.  <pre>ProxyHost=chicago.indigo-insurance.com</pre>
SocksPort	The port on SocksHost where the Socks proxy server listens. This setting is not used unless UseSocks=1. A SocksHost must also be specified. The default value is 1080.

SerialPorts	<p>A list of serial ports to be mapped in a Windows application emulator session.</p> <p>Each serial port in the list is separated with a semi-colon and has the format <code>serial device=<i>com_port_name</i></code>.</p> <pre data-bbox="289 317 1533 373">/dev/ttyS0=COM1;/dev/ttyS4=COM8</pre> <p>The <code>=<i>com_port_name</i></code> is optional, but if it is omitted the serial port will be mapped to COMx in the Windows application session where x is the position of the serial port in the list.</p>
-------------	--

If the user changes these settings in the Native Client dialogs, for example by entering a different login URL, the changes to all values apart from DocBrowser and CertsFile are saved to the preferences file when the user exits the Native Client.

#### Related topics

- [Running the Native Client from the command line](#)
- [Using Secure Global Desktop with proxy servers](#)
- [Configuring access to serial ports](#)



## How can I make additional Native Clients available?

Users can download the Sun Secure Global Desktop Native Client from a Secure Global Desktop server at `http://server` (you can also use https). The following Native Clients are always available to download:

- the Native Client for Microsoft Windows
- the Linux version of the Native Client for UNIX and
- the Native Client for Mac OS X.

**Note** The Native Client can only be used to access the *classic* webtop.

You can make additional Native Clients available for download by copying the Native Client setup files to the `/opt/tarantella/var/docroot/native` directory on the Secure Global Desktop server. All Native Client setup files present in this directory are dynamically published on the Native Client download page.

Additional or newer versions of the Native Client may also be available from:

- the Secure Global Desktop CD or
- the [Sun Secure Global Desktop Software web site](http://www.sun.com/software/products/sgd/) (<http://www.sun.com/software/products/sgd/>).

### Related topics

- [What do I need to tell my users?](#)

## Customizing the Native Client for UNIX

You can configure the Native Client for UNIX to use your own images for the splash screen and the webtop "display" pane.

The images used must be in XPM format. For good results, the splash screen image should be no larger than 300x400 and the webtop image should be no larger than 640x480.

1. Change to the appropriate `app-defaults` directory:
  - o For user class *root*, `/usr/lib/X11/app-defaults`
  - o For user class *user*, `$HOME/.tarantella/app-defaults`
2. Open `Ttwebtop` in a text editor.
3. To add a splash screen image, find the line containing `*splashScreen*Pixmapfile`.
4. Delete the `comment`.
5. Insert the full pathname to the splash screen XPM file.
6. To add a webtop image, find the line containing `*demgrSW*Pixmapfile`.
7. Delete the `comment`.
8. Insert the full pathname to the webtop XPM file.

**Note** The Native Client can only be used to access the *classic* webtop.

### Related topics

- [Native Client preferences files on UNIX, Linux and Mac OS X client devices](#)
- [Running the Native Client from the command line](#)

## What is an array?

In Secure Global Desktop, an array is a **collection of Secure Global Desktop servers that share configuration information**.

Arrays have these benefits:

- Users and emulator sessions are load-balanced across the array. To scale to more users, simply add more Secure Global Desktop servers to the array.
- With more than one server, there's no single point of failure. You can decommission a server temporarily with the minimum of disruption to your users.
- Configuration information, including all the objects in your organizational hierarchy, is replicated to all array members. All array members have access to all information.

You can use [Array Manager](#) to add and remove servers from the array, to change the primary server, and to [configure both array-wide and server-specific settings](#).

## Array structure

An array contains:

- **One primary server.** This is the authoritative source for array-wide information, and maintains the definitive copy of the organizational hierarchy.
- **Any number of secondary servers.** Information is replicated to these servers by the primary server.

A single, "standalone" server is considered to be the primary server in an array with no secondary servers.

Secure Global Desktop servers in an array may run different operating systems. However, all the array members must run the same version of Secure Global Desktop.

### Related topics

- Introducing Array Manager
- Setting up and dismantling a Secure Global Desktop array
- Understanding webtop and emulator sessions
- Introducing webtop and emulator session load balancing
- The tarantella array command
- The tarantella config command

## Setting up and dismantling a Secure Global Desktop array

You set up and dismantle an array of Secure Global Desktop servers:

- by using Array Manager or
- by using the `tarantella array` command.

**Note** After making a change to the structure of an array, it is advisable to wait until Secure Global Desktop has copied the changes to all array members before making any further changes. The changes have been copied when the `tarantella status` command returns the same result for each array member.

Changing the structure of an array will have an effect on the certificates used for [secure intra-array communication](#).

### Adding a server to an array

In Array Manager, you add a Secure Global Desktop server to an array by clicking New Secondary and then typing the server's DNS name.

From the command line, you use the `tarantella array join` command.

If the server you add has been load balancing application servers using [Advanced Load Management](#), we recommend that you do a warm restart (`tarantella restart --warm`) of the new server after it has joined the array. If the array to which the new server is joined is using Advanced Load Management, we recommend you do a warm restart of the whole array after the new server has joined.

### Removing a server from an array

In Array Manager, you remove a Secure Global Desktop server from an array by right-clicking it in the tree and then clicking Detach Server.

From the command line, you use the `tarantella array detach` command.

To remove the primary server from an array, first make another server the primary server and then remove the old primary server.

When you remove a server from an array, it loses its license keys.

## Changing the primary server in an array

In Array Manager, you change the primary server in the array by right-clicking the server you want to become the primary server and then clicking Make Primary.

From the command line, you use the `tarantella array make_primary` command.

**Note** The previous primary server becomes a secondary server.

### Related topics

- [What is an array?](#)
- [Introducing Array Manager](#)
- [The tarantella array command](#)

## Backing up and restoring a Secure Global Desktop installation

This topic describes how you:

- [Make a full backup of a Secure Global Desktop installation.](#)
- [Restore a damaged Secure Global Desktop component.](#)
- [Do a full restore of a Secure Global Desktop installation.](#)

### How to make a full backup of a Secure Global Desktop installation

To be able to restore a Secure Global Desktop installation or to be able to repair some individual Secure Global Desktop components, you will need a full backup.

While making the backup, **do not** run any command-line tools or use Object Manager or Array Manager. It is also best if you shut down the Secure Global Desktop server while making the backup. However, if this is not possible, do it when the server is least loaded.

To back up Secure Global Desktop:

1. Run the `tarantella archive` command.
2. Backup the entire [Secure Global Desktop installation directory](#) on each member of the array.

Secure Global Desktop also uses the following configuration files which only need to be backed up if you are using them and you have modified them:

- `/etc/ttapiprinter.conf` - this contains the lpr defaults.
- `/etc/sdace.txt` and `/var/ace/data` - these contain RSA SecurID® settings.
- web server password and `.htaccess` files if you have created these files for use with the Secure Global Desktop Web Server and they are stored outside the Secure Global Desktop installation directory.

### How to restore a damaged Secure Global Desktop component

For the purposes of restoring a damaged installation, Secure Global Desktop can be divided up into the following components:

- Binaries, scripts and template files
- HTML theme files
- Expect scripts
- Server-specific configuration
- Array-wide configuration
- The enterprise (ENS) database
- Automatic log archives
- Secure Global Desktop printing
- the Secure Global Desktop Web Server, web services and the browser-based webtop

## Binaries, scripts and template files

The binaries, scripts and template files are only modified as part of an installation, patch or custom engineering work. These do not change very often.

You can restore these files from a backup or another installation.

- The binaries are in the following directories:
  - `/opt/tarantella/bin/bin`
  - `/opt/tarantella/var/docroot/java`
  - `/opt/tarantella/var/docroot/mac`
  - `/opt/tarantella/var/docroot/native`
- The scripts are in the `/opt/tarantella/bin/scripts` directory.
- The template files are in the `/opt/tarantella/etc/templates` directory.

## HTML theme files

The HTML theme files control the appearance of the *classic* webtop.

How you recover these files depends on whether or not you are using customized themes:

- If you are not using customized themes, you can restore these files from another installation, a backup, or from the `/opt/tarantella/etc/templates` directory.
- If you are using customized themes, you must only restore these files from a backup.

The theme files are under the `/opt/tarantella/var/docroot/resources` directory.

**Note** The locale-specific template theme files are in directories with names of the form `locale_0x3d_locale/`. These correspond to the `locale=locale/` directories in the `/opt/`



`tarantella/var/docroot/resources` directory.

## Expect scripts

The [Expect scripts](#) control the interaction between Secure Global Desktop and the application servers (for example, by logging a user in).

How you recover these scripts depends on whether or not you are using customized scripts:

- If you are not using customized scripts, you can restore these files from another installation, a backup, or from the `/opt/tarantella/etc/templates` directory.
- If you are using customized scripts, you must only restore these files from a backup.

The scripts are in the `/opt/tarantella/var/serverresources/expect` directory.

## Server-specific configuration

Server-specific configuration covers all the properties for a Secure Global Desktop server that are not shared with the other members of the array, such as the server DNS name and server tuning.

As this configuration is unique to a particular Secure Global Desktop host, it must only be restored from a backup taken from that host.

The server-specific configuration is in the `/opt/tarantella/var/serverconfig/local` directory.

If you are using Secure Global Desktop security services, you should restore the following directories and file:

- `/opt/tarantella/var/tsp`
- `/opt/tarantella/var/info/certs`
- `/opt/tarantella/var/info/key`

## Array-wide configuration

Array-wide configuration covers all the properties that are the same for all the array members, for example the names of the other array members.

To restore global configuration for:

- a primary Secure Global Desktop server, you must only restore from a backup of the primary.
- a secondary Secure Global Desktop server, we recommend you restore from the primary.

The array-wide configuration is in the `/opt/tarantella/var/serverconfig/global` directory.

## The enterprise (ENS) database

The enterprise (ENS) database is shared across the array and contains all the webtop, application and user information. This information changes very regularly.

We recommend you restore the enterprise database from the backup of the primary Secure Global Desktop server.

The enterprise database is in the `/opt/tarantella/var/ens` directory.

## Automatic log archives

By default, Secure Global Desktop archives its log files each week at 4am on Sunday using a cron job.

If the root user's crontab becomes corrupt or the archiving does not take place, use `tarantella setup` to restore the default setting, or change the time and day that the archiving takes place.

The log files are archived under the `/opt/tarantella/var/log/` directory.

## Secure Global Desktop printing

When you install Secure Global Desktop, it configures a Secure Global Desktop print queue.

If the print queue is not present, you can restore it:

- by manually running the print install script (`prtinstall.en.sh`) or
- by running the `tarantella setup` command.

The print queue is in the `/opt/tarantella/var/print` directory.

## The Secure Global Desktop Web Server, web services and the browser-based webtop

The configuration of the Secure Global Desktop Web Server, web services and the browser-based webtop is unique to a particular Secure Global Desktop host and must only be restored from a backup taken from that host.

The configuration for the Secure Global Desktop Web Server is in the `/opt/tarantella/`

`webserver/apache/apache_version` directory. You may also have web server password and `.htaccess` files which may be stored in other locations.

The configuration for Secure Global Desktop web services is in the `/opt/tarantella/webserver/tomcat/tomcat_version` directory.

The files used for the browser-based webtop are in the `/opt/tarantella/webserver/tomcat/tomcat_version/webapps/sgd` directory.

## How to do a full restore of your Secure Global Desktop installation

If you are unable to restore a damaged Secure Global Desktop component or you are unsure about the extent of the damage to your system, you must do a full restore of your Secure Global Desktop installation. To do a full restore, you must have [a full backup](#).

To do a full restore:

1. Stop the Secure Global Desktop server (`tarantella stop`).
2. Uninstall Secure Global Desktop by running the `tarantella uninstall --purge` command.

**Note** If this fails, you may have to manually remove the Secure Global Desktop package. Use `rpm -e tta` on Linux platforms and `pkgrm tta` on Solaris Operating System platforms.

3. Delete the Secure Global Desktop installation directory by running `rm -rf /opt/tarantella`
4. Re-install Secure Global Desktop and any patches (if applicable). This will install the printer, rc scripts and set-up package database.
5. Stop the Secure Global Desktop server (`tarantella stop`).
6. Delete the Secure Global Desktop installation directory by running `rm -rf /opt/tarantella` and reinstate Secure Global Desktop from backup.

**Note** Make sure the server names match.

7. Restart the Secure Global Desktop server (`tarantella start`).

### Related topics

- [Where is Secure Global Desktop installed?](#)
- [What's in the Secure Global Desktop installation directory?](#)



[Secure Global Desktop Administration Guide > Arrays, servers and load balancing > Every server in the array has been disabled and no-one can access Secure Global Desktop](#)

## Every server in the array has been disabled and no-one can access Secure Global Desktop

A Secure Global Desktop Administrator can specify that a Secure Global Desktop server is not available to users (`--server-login disabled`). This prevents users from logging in to that server and starting new emulator sessions.

If an Administrator accidentally denies access to all servers in the array, you can't use Secure Global Desktop to access Array Manager and re-enable logins.

If this happens, you can either:

- run Array Manager from the command line using the `tarantella arraymanager` command and then re-enable Secure Global Desktop logins for a server, or
- re-enable Secure Global Desktop logins for a server by running:

```
tarantella config edit --server server --server-login enabled
```

### Related topics

- [Introducing Array Manager](#)

[Secure Global Desktop Administration Guide](#) > [Security](#) > Users are unable to connect to Secure Global Desktop when it is in firewall forwarding mode

## Users are unable to connect to Secure Global Desktop when it is in firewall forwarding mode

Users may find that they are unable to connect to Secure Global Desktop when it is in [firewall forwarding mode](#). A common cause of this problem is that Secure Global Desktop was started **before** the Secure Global Desktop Web Server.

In firewall forwarding mode, Secure Global Desktop listens on port 443 and forwards any web connections to the Secure Global Desktop Web Server, which is configured to listen on localhost port 443 (127.0.0.1:443). If Secure Global Desktop is started before the Secure Global Desktop Web Server, Secure Global Desktop binds to all the available interfaces and this means that Secure Global Desktop forwards any web connections to itself in an infinite loop.

One solution is to always start the Secure Global Desktop Web Server before Secure Global Desktop.

Another solution is to configure Secure Global Desktop so that it never binds to the localhost interface. To do this, run the following command:

```
tarantella config edit \  
  --tarantella-config-server-bindaddresses-external "!127.0.0.1"
```

**Note** On some shells you cannot use double quotes ("!127.0.0.1") as the !127 may get substituted. Use single quotes instead ('!127.0.0.1').

You can also use this command to specify exactly which interfaces you *do* want Secure Global Desktop to bind to. You do this by entering a comma-separated list of DNS names and/or IP addresses.

### Related topics

- [Using Secure Global Desktop with firewalls](#)
- [Using Secure Global Desktop with the HTTPS port through a firewall](#)

## Managing unauthenticated connections to Secure Global Desktop

Unauthenticated connections to Secure Global Desktop consume server resources. To prevent this happening, Secure Global Desktop uses timeouts.

For the browser-based webtop, the Secure Global Desktop server applies the timeout and breaks the connection. This causes the Sun Secure Global Desktop Client to exit. Two controls are used:

- an **unauthenticated session timeout** which controls how long unauthenticated webtop sessions last before they are expired. This is an array-wide property. The default is 600 seconds.

You can change this by running:

```
tarantella config edit \  
--tarantella-config-array-unauthenticatedsessiontimeout seconds
```

- an **unauthenticated session limit** which controls the number of unauthenticated webtop sessions a Secure Global Desktop Server can have. This is a server-specific property. The default is 100 sessions. You can change this by running:

```
tarantella config edit \  
--tarantella-config-server-maxunauthenticatedsessions sessions
```

For the classic webtop, the Java™ technology client applies the timeout and breaks the connection. This timeout occurs after six AsadKeepAlive packets have been sent by the client. By default, AsadKeepAlive packets are sent every 100 seconds. The interval is configured in the `/opt/tarantella/var/docroot/resources/login/sco/tta/boot/strap.html` file.

### Related topics

- [Understanding webtop and emulator sessions](#)

## Users are unable to relocate their webtop sessions

When a user logs in to a Secure Global Desktop server without logging out of another, normally the user's webtop session is relocated to the new server (this is sometimes called session grabbing). If the clocks on all array members are not synchronized, webtop sessions may not relocate successfully.

The timestamps on the webtop sessions determine which is newer. The newer webtop session is considered to be current. If clocks are not synchronized, the timestamps may give misleading information.

The solution is to make sure that clocks are synchronized between Secure Global Desktop servers in the array. For example, you can use `rdate`.

### Related topics

- [Understanding webtop and emulator sessions](#)



## Application Launch properties (array-wide)

Attributes on the Application Launch Properties panel of Array Manager control the user experience when clicking links to applications on webtops. The attributes apply to all array members.

From the command line, use `tarantella config` to view and edit these settings.

Changes to these attributes take effect immediately.

Array Manager	Command line	Description
Authentication: Save Secure Global Desktop login details in cache	<code>--launch-savettapassword 1   0</code>	<ul style="list-style-type: none"><li>• Whether to save in the password cache the username and password the user types to log in to Secure Global Desktop.</li><li>• If you are using the <a href="#">SecurID login authority</a>, we recommend you don't save the username and password as SecurID passwords can't be re-used.</li></ul>
Authentication: Try Secure Global Desktop password if cached	<code>--launch-trycachedpassword 1   0</code>	<ul style="list-style-type: none"><li>• Whether to try the password the user typed for the Secure Global Desktop server (if it's stored in the password cache) as the password for the application server.</li><li>• Secure Global Desktop server passwords might be stored in the cache if some applications are configured to run on the Secure Global Desktop host, or if Save Secure Global Desktop Login Details In Cache is checked.</li><li>• This setting may be overridden by a <a href="#">host object's Authentication</a> attribute.</li></ul>

<p>Authentication: Allow smart card authentication</p>	<pre>--launch-allowsmartcard 1   0</pre>	<ul style="list-style-type: none"> <li>• Allow users to log in with a smart card.</li> <li>• For details of the conditions for using smart card authentication, see <a href="#">Using smart cards with Windows applications</a>.</li> </ul>
<p>Authentication Dialog</p>	<pre>--launch-showauthdialog user   system   none</pre>	<ul style="list-style-type: none"> <li>• Controls when the application server's authentication dialog displays. This is either: <ul style="list-style-type: none"> <li>◦ If the user holds down the SHIFT key when they click an application's link or if there is a password problem (<code>user</code>)</li> <li>◦ Only when there is a password problem (<code>system</code>)</li> <li>◦ Never (<code>none</code>)</li> </ul> </li> </ul>
<p>If Password Has Expired</p>	<pre>--launch-expiredpassword manual   dialog   none</pre>	<ul style="list-style-type: none"> <li>• The action to take if the user's password has expired on the application server. Some types of application server do not support the Prompt User (<code>dialog</code>) setting.</li> </ul>
<p>"Save password" box</p>	<pre>--launch-savepassword- initial checked   cleared  --launch-savepassword- state enabled   disabled</pre>	<ul style="list-style-type: none"> <li>• Two attributes which control the initial state of the Save password box in the application server authentication dialog and whether users can change it.</li> <li>• If users can't change the setting, the initial state determines whether users may save passwords in the application server password cache.</li> </ul>

<p>"Always use smart card" Box</p>	<pre>--launch- alwayssmartcard-initial checked   cleared  --launch-- alwayssmartcard-state enabled   disabled</pre>	<ul style="list-style-type: none"> <li>• Two attributes which control the initial state of the Always use smart card box in the application server's authentication dialog and whether users can change it.</li> <li>• If users can't change the setting, the initial state determines whether the user's decision to always use smart card authentication is cached.</li> </ul>
<p>Launch Details</p>	<pre>--launch-details- initial shown   hidden  --launch-details-state enabled   disabled</pre>	<ul style="list-style-type: none"> <li>• Two attributes which control the initial display of the Launch Details area of the application launch dialog and whether users can change it.</li> <li>• If users can't change the setting, the initial state determines whether users see the application launch details.</li> </ul>
<p>If Launch Fails</p>	<pre>--launch-details- showonerror 1   0</pre>	<ul style="list-style-type: none"> <li>• Whether to show the launch details area if an application launch fails.</li> </ul>
<p>Launch Dialog</p>	<pre>--launch- showdialogafter <i>seconds</i></pre>	<ul style="list-style-type: none"> <li>• The delay in seconds before showing the application launch dialog to users.</li> </ul>

### Related topics

- [Introducing application server load balancing](#)
- [Introducing Array Manager](#)
- [The tarantella passcache command](#)

## Array properties (array-wide)

Attributes on the Array Properties panel of Array Manager are general settings for the array. The attributes apply to all array members.

From the command line, use `tarantella config` to view and edit these settings.

Array Manager	Command line	Description
Port Numbers (unencrypted connections)	<code>--array-port-unencrypted tcp_port</code>	<ul style="list-style-type: none"> <li>The TCP port number used for <b>unencrypted</b> connections between client devices and Secure Global Desktop servers.</li> <li>Open this port in your firewall to enable connections from users who have standard connections (connections not using SSL).</li> <li>You should restart every Secure Global Desktop server in the array for changes to this attribute to take effect.</li> </ul>
Port Numbers (encrypted connections)	<code>--array-port-encrypted tcp_port</code>	<ul style="list-style-type: none"> <li>The TCP port number used for <b>encrypted</b> connections between client devices and Secure Global Desktop servers.</li> <li>Open this port in your firewall to enable connections from users who have secure (SSL-based) connections to Secure Global Desktop.</li> <li>You should restart every Secure Global Desktop server in the array for changes to this attribute to take effect.</li> </ul>

<p>Port Numbers (connections between array members)</p>	<pre>--array-port-peer tcp_port</pre>	<ul style="list-style-type: none"> <li>• The TCP port number used for connections <b>between Secure Global Desktop array members</b>.</li> <li>• These connections are used to replicate information across the array.</li> <li>• You should restart every Secure Global Desktop server in the array for changes to this attribute to take effect.</li> </ul>
<p>Log Filter</p>	<pre>--array-logfilter filter...</pre>	<ul style="list-style-type: none"> <li>• Which diagnostic messages are logged, and where.</li> <li>• This attribute contains multiple values, each of the form <i>component/subcomponent/severity:destination</i>.</li> <li>• Use the wildcard * to match multiple components, subcomponents and severities. On the command line, remember to quote any filters containing wildcards to stop your shell from expanding them.</li> <li>• Valid destinations are a filename or the <a href="#">TFN name</a> of a plug-in log handler.</li> <li>• On the command line, separate each <i>filter</i> with a space. Remember to quote any filters that contain wildcards *, to stop your shell from expanding them.</li> <li>• File names may include the placeholder %%PID%%, which is substituted with a process ID.</li> <li>• On the command line, separate each <i>filter</i> with a space. In Array Manager, separate each filter with a RETURN.</li> <li>• For detailed information on setting log filters and viewing log output, see <a href="#">Using log filters to troubleshoot problems with the Secure Global Desktop server</a>.</li> <li>• Changes to this attribute take effect immediately.</li> </ul>

<p>Enable billing services</p>	<pre>--array-billingservices 1   0</pre>	<ul style="list-style-type: none"> <li>• Whether to enable billing services across the array.</li> <li>• This may use significant additional disk space on array members.</li> <li>• If enabled, you can use <code>tarantella query billing</code> to analyze the billing logs.</li> <li>• Changes to this attribute take effect on an array member the next time the Secure Global Desktop server starts.</li> </ul>
<p>Enable resource synchronization</p>	<pre>--array-resourcesync 1   0</pre>	<ul style="list-style-type: none"> <li>• Whether to enable replication of resources across the array.</li> <li>• If enabled, synchronization starts at a time determined in <a href="#">Tuning properties</a> for each array member.</li> <li>• Changes to this attribute take effect immediately.</li> </ul>
<p>Client Drive Mapping: Let users access client drives</p>	<pre>--array-cdm 1   0</pre>	<ul style="list-style-type: none"> <li>• Whether to enable client drive mapping (CDM) across the array, see <a href="#">configuring client drive mapping</a> for details.</li> <li>• If you enable drive mapping, CDM services only become available when you restart all Secure Global Desktop servers in the array. To manually start CDM services without restarting the array, run the <code>tarantella start cdm</code> command on all members of the array.</li> <li>• If you disable drive mapping, the CDM processes only stop when you restart all Secure Global Desktop servers in the array. To manually stop CDM services without restarting the array, run the <code>tarantella stop cdm</code> command on all members of the array.</li> <li>• Changes to this attribute only take effect for new webtop sessions.</li> </ul>

<p>Client Drive Mapping: Use WINS for better performance</p>	<pre>--array-cdm-wins 1   0</pre>	<ul style="list-style-type: none"> <li>• Whether to enable WINS to improve performance of client drive access. Without WINS, performance may be limited by known problems with Microsoft Windows networking.</li> <li>• WINS services use <a href="#">port 137/udp</a> on the Secure Global Desktop server.</li> <li>• Only enable WINS if either of the following is true: <ul style="list-style-type: none"> <li>◦ Your Microsoft Windows application servers are on the same subnet as an array member.</li> <li>◦ Your Microsoft Windows application servers list an array member as a WINS server.</li> </ul> </li> <li>• Changes to this attribute take effect on an array member the next time the Secure Global Desktop server starts.</li> </ul>
<p>Client Drive Mapping: Fallback Drive</p>	<pre>--array-cdm-fallbackdrive letter_direction</pre>	<ul style="list-style-type: none"> <li>• For client drives that can't be mapped using the configured drive letter because that drive letter is already in use, which drive letter to start searching from and the direction to search. The first unused drive letter is used to map the client drive.</li> <li>• Allowed values are of the form [a-zA-Z] [+ -], for example v- to start at drive V and search alphabetically backwards, or f+ to search forwards from drive F. Drive letters are case-insensitive.</li> <li>• Changes to this attribute take effect for new webtop sessions.</li> </ul>

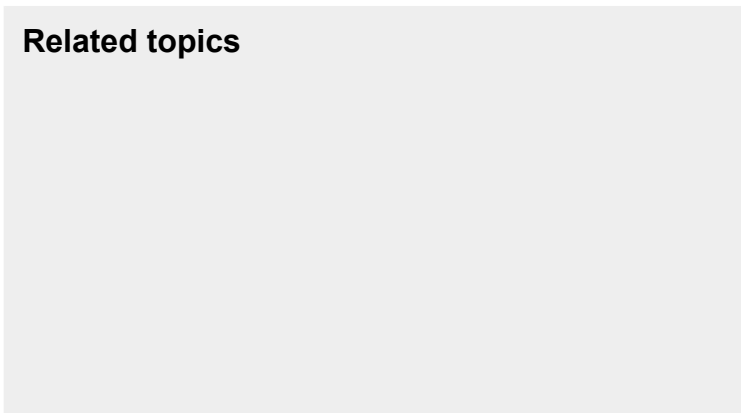
<p>Audio: Enable audio service</p>	<pre>--array-audio 1   0</pre>	<ul style="list-style-type: none"> <li>• Whether to enable audio services across the array.</li> <li>• Audio is only available for applications running on a Microsoft Windows 2003 application server. <a href="#">Audio redirection must also be enabled on the server.</a></li> <li>• Changes to this attribute only take effect for new webtop sessions.</li> </ul>								
<p>Audio: sound quality</p>	<pre>--array-audio-quality low   medium   high</pre>	<ul style="list-style-type: none"> <li>• The sample rate of the audio data.</li> <li>• Adjusting the audio quality increases or decreases the amount of audio data sent.</li> <li>• By default, Secure Global Desktop uses Medium Quality Audio. This should be sufficient in most cases.</li> <li>• The sample rates are: <table border="1" data-bbox="987 930 1531 1503"> <thead> <tr> <th>Setting</th> <th>Sound sample rate</th> </tr> </thead> <tbody> <tr> <td>Low Quality Audio</td> <td>8kHz</td> </tr> <tr> <td>Medium Quality Audio</td> <td>22.05kHz</td> </tr> <tr> <td>High Quality Audio</td> <td>Same as medium (this is a Terminal Services restriction)</td> </tr> </tbody> </table> </li> </ul>	Setting	Sound sample rate	Low Quality Audio	8kHz	Medium Quality Audio	22.05kHz	High Quality Audio	Same as medium (this is a Terminal Services restriction)
Setting	Sound sample rate									
Low Quality Audio	8kHz									
Medium Quality Audio	22.05kHz									
High Quality Audio	Same as medium (this is a Terminal Services restriction)									
<p>Smart card: Enable smart card service</p>	<pre>--array-sccard 1   0</pre>	<ul style="list-style-type: none"> <li>• Whether to enable smart card services across the array.</li> <li>• Support for smart cards is only available for applications running on a Microsoft Windows Server 2003 application server.</li> <li>• Changes to this attribute only take effect for new webtop sessions.</li> </ul>								



<p><b>Profile Editing:</b> Enable user profile editing</p>	<pre>--array-editprofile 1   0</pre>	<ul style="list-style-type: none"><li>• Whether to allow users to create or edit their own <a href="#">profiles</a> for use with the Secure Global Desktop Client.</li><li>• By default, profile editing is enabled.</li><li>• If profile editing is disabled, it is disabled for <b>all</b> users, including Secure Global Desktop Administrators. However, Secure Global Desktop Administrators can still create and edit profiles using the Profile Editor application.</li><li>• Profile editing for individual users can be enabled and disabled using the <a href="#">Profile Editing</a> attribute for organization, organizational unit or person objects in Object Manager</li><li>• Changes to this attribute only take effect for new webtop sessions.</li></ul>
<p><b>Clipboard: Enable copy and paste</b></p>	<pre>--array-clipboard- enabled 1   0</pre>	<ul style="list-style-type: none"><li>• Whether to allow copy and paste operations for Windows and X application emulator sessions across the array.</li><li>• By default, copy and paste is allowed.</li><li>• Copy and paste operations for individual users can be enabled and disabled using the <a href="#">Clipboard Access</a> attribute for organization, organizational unit or person objects in Object Manager</li><li>• Changes to this attribute only take effect for new emulator sessions.</li></ul>

Clipboard: Client security level	<code>--array-clipboard-clientlevel</code>	<ul style="list-style-type: none"> <li>• The security level for Secure Global Desktop clients.</li> <li>• Used to <a href="#">control copy and paste operations</a> between Windows or X application emulator sessions and applications running on the client device.</li> <li>• The security level can be any positive integer. The higher the number, the higher the security level. The default security level is 3.</li> <li>• Use <code>-1</code> on the command line to disable copy and paste operations with applications running on the client.</li> <li>• Changes to this attribute only take effect for new emulator sessions.</li> </ul>
Serial Port: Enable serial port mapping	<code>--array-serialport 1   0</code>	<ul style="list-style-type: none"> <li>• Whether to enable access to serial ports across the array, see <a href="#">configuring access to serial ports</a> for details.</li> <li>• By default, access to serial ports is allowed.</li> <li>• Access to serial ports for individual users can be enabled and disabled using the <a href="#">Serial Port Mapping</a> attribute for organization, organizational unit or person objects in Object Manager</li> <li>• Changes to this attribute only take effect for new webtop sessions.</li> </ul>

## Related topics



- Introducing Array Manager
- What is an array?
- What ports does Secure Global Desktop use?
- Tuning properties (server-specific)
- Using log filters to troubleshoot problems with the Secure Global Desktop server
- How do I enable sound in Windows applications?
- Configuring client drive mapping
- Using smart cards with Windows applications
- Using copy and paste with Secure Global Desktop
- Configuring access to serial ports
- Profiles and the Sun Secure Global Desktop Client

## Audio Protocol Engine properties (server-specific)

Attributes on the Audio Protocol Engine Properties For... panel of Array Manager let you tune Secure Global Desktop audio processes for a particular array member. The attributes apply independently to each Secure Global Desktop server.

From the command line, use `tarantella config` to view and edit these settings.

Changes to these attributes take effect for new Protocol Engines only. Existing Protocol Engines are not affected.

Array Manager	Command line	Description
Compression	<code>--audiope-compression auto   always   never</code>	<ul style="list-style-type: none"><li>• Whether an Audio Protocol Engine uses data compression on a client connection.</li><li>• By default, compression is off. This is to avoid unnecessarily compressing audio data, which may already be compressed.</li><li>• Use <code>auto</code> ("If connection is slow" in Array Manager) to cause the Audio Protocol Engine to compress data if the connection is slow.</li></ul>

### Related topics

- [Introducing Array Manager](#)

## Channel Protocol Engine properties (server-specific)

Attributes on the Channel Protocol Engine Properties For... panel of Array Manager let you tune Secure Global Desktop channel processes for a particular array member. The Secure Global Desktop channel is used to detect information about the client, for example to detect client drives or audio devices.

The attributes apply independently to each Secure Global Desktop server.

From the command line, use `tarantella config` to view and edit these settings.

Changes to these attributes take effect for new Protocol Engines only. Existing Protocol Engines are not affected.

Array Manager	Command line	Description
Compression	<code>--chpe-compression auto   always   never</code>	<ul style="list-style-type: none"><li>• Whether a Channel Protocol Engine uses data compression on a client connection.</li><li>• Use <code>auto</code> ("If connection is slow" in Array Manager) to cause the Channel Protocol Engine to compress data if the connection is slow.</li></ul>
Threshold	<code>--chpe-compressionthreshold bytes</code>	<ul style="list-style-type: none"><li>• The smallest size of network packet that a Channel Protocol Engine will compress.</li></ul>
Process Tuning: Exit after	<code>--chpe-exitafter seconds</code>	<ul style="list-style-type: none"><li>• The length of time a Channel Protocol Engine process will continue running without any active connections.</li></ul>

## Related topics

- [Configuring client drive mapping](#)

## Character Protocol Engine properties (server-specific)

Attributes on the Character Protocol Engine Properties For... panel of Array Manager let you tune terminal emulator processes for a particular array member. The attributes apply independently to each Secure Global Desktop server.

From the command line, use `tarantella config` to view and edit these settings.

Changes to these attributes take effect for new Protocol Engines only. Existing Protocol Engines are not affected.

Array Manager	Command line	Description
Command-line Arguments	<code>--cpe-args args</code>	<ul style="list-style-type: none"><li>Any arguments to the Protocol Engine. For example, the name of a log file.</li><li>You shouldn't need to change this unless asked by Technical Support.</li></ul>
Process Tuning: Maximum sessions per engine	<code>--cpe-maxsessions num</code>	<ul style="list-style-type: none"><li>The maximum number of emulator sessions each Character Protocol Engine handles.</li><li>More Character Protocol Engines are started to meet demand.</li></ul>
Process Tuning: Maximum users per engine	<code>--cpe-maxusers num</code>	<ul style="list-style-type: none"><li>The maximum number of users each Character Protocol Engine handles.</li><li>More Character Protocol Engines are started to meet demand.</li></ul>
Process Tuning: Exit after	<code>--cpe-exitafter num</code>	<ul style="list-style-type: none"><li>The length of time a Character Protocol Engine process will continue running without any active connections.</li></ul>

## Related topics

- [Introducing Array Manager](#)



## Emulator Sessions properties (array-wide)

Attributes on the Emulator Sessions Properties panel of Array Manager control the resumability of applications. The attributes apply to all array members.

From the command line, use `tarantella config` to view and edit these settings.

Changes to these attributes take effect immediately.

Array Manager	Command line	Description
Resumability Timeout: webtop session	<code>--sessions-timeout-session mins</code>	<ul style="list-style-type: none"><li>• For applications configured to be "Webtop session" <b>resumable</b>, the length of time (in minutes) a suspended emulator session is guaranteed to be resumable after the user disconnects. (Note that if the user logs out, these emulator sessions end.)</li><li>• After this period the Secure Global Desktop server will end the session.</li><li>• You can override this setting in an application's properties.</li></ul>
Resumability Timeout: Always	<code>--sessions-timeout-always mins</code>	<ul style="list-style-type: none"><li>• For applications configured to be "Always" <b>resumable</b>, the length of time (in minutes) a suspended emulator session is guaranteed to be resumable after the user disconnects or logs out.</li><li>• After this period the Secure Global Desktop server will end the session.</li><li>• You can override this setting in an application's properties.</li></ul>

AIP Keepalive	<pre>--sessions- aipkeepalive secs</pre>	<ul style="list-style-type: none"><li>• How often a keepalive message is sent to client devices during emulator sessions. The default value is 100 seconds.</li><li>• Some HTTP proxy servers will close a connection if there is no activity on it. Using a keepalive ensures a connection stays open. If you change this value, you may also want to change the corresponding <a href="#">client-side keepalive</a>.</li><li>• Set this to 0 to disable keepalive messages.</li><li>• This is also used keep open connections between the client and the Secure Global Desktop server for client drive mapping.</li></ul>
---------------	--	---

### Related topics

- [Applications disappear after about two minutes](#)
- [Understanding webtop and emulator sessions](#)
- [Resumable \(--resumable\)](#)
- [Introducing Array Manager](#)

## Execution Protocol Engine properties (server-specific)

Attributes on the Execution Protocol Engine Properties For... panel of Array Manager let you tune application launch processes for a particular array member. The attributes apply independently to each Secure Global Desktop server.

From the command line, use `tarantella config` to view and edit these settings.

Changes to these attributes take effect for new Protocol Engines only. Existing Protocol Engines are not affected.

Array Manager	Command line	Description
Command-line Arguments	<code>--execpe-args <i>args</i></code>	<ul style="list-style-type: none"><li>• Any arguments to the Protocol Engine. For example, the name of a log file.</li><li>• You shouldn't need to change this unless asked by Technical Support.</li></ul>
Login Script Directory	<code>--execpe-scriptdir <i>dir</i></code>	<ul style="list-style-type: none"><li>• The directory on the Secure Global Desktop host in which login scripts are stored.</li><li>• Use <code>%%INSTALLDIR%%</code> to mean the Secure Global Desktop <a href="#">installation directory</a>.</li><li>• If an application object's <a href="#">Login Script</a> attribute uses a relative pathname, for example "unix.exp", this directory is assumed.</li><li>• You shouldn't need to change this attribute.</li></ul>
Process Tuning: Maximum sessions per engine	<code>--execpe-maxsessions <i>num</i></code>	<ul style="list-style-type: none"><li>• The maximum number of emulator sessions each Execution Protocol Engine handles.</li><li>• More Execution Protocol Engines are started to meet demand.</li></ul>

Process Tuning: Maximum users per engine	<code>--execpe-maxusers num</code>	<ul style="list-style-type: none"><li>• The maximum number of users each Execution Protocol Engine handles.</li><li>• More Execution Protocol Engines are started to meet demand.</li></ul>
Process Tuning: Exit after	<code>--execpe-exitafter seconds</code>	<ul style="list-style-type: none"><li>• The length of time an Execution Protocol Engine process will continue running without any active connections.</li></ul>

### Related topics

- [Introducing Array Manager](#)
- [Login Script \(--login\)](#)

## General properties (server-specific)

Attributes on the General Properties For... panel of Array Manager are general settings for a particular array member. The attributes apply independently to each Secure Global Desktop server.

From the command line, use `tarantella config` to view and edit these settings.

Changes to these attributes take effect immediately.

Array Manager	Command line	Description
DNS Name	<code>--server-dns-external dns_name</code>	<ul style="list-style-type: none"><li>• The external DNS names of this server.</li><li>• This setting allows you to use different names depending on the IP address of the client.</li><li>• Only change this setting if this server is known by different names on the network, for example, inside and outside a firewall.</li><li>• Each name has the format <code>IP_pattern:DNS name</code>, where <code>IP_pattern</code> is a regular expression matching a client IP address, for example <code>192.168.10.*</code>.</li><li>• If this server only has one name, use one line matching all clients, for example: <code>*:www.indigo-insurance.com</code>.</li><li>• The order of the names is important. The DNS name for the <b>first</b> matching IP pattern is used. For example if the following names are defined: <code>192.168.10.*:boston.indigo-insurance.com</code></li></ul>

		<p>*:www.indigo-insurance.com clients with IP addresses beginning 192.168.10 connect to boston.indigo-insurance.com, and all other clients connect to www.indigo-insurance.com.</p> <ul style="list-style-type: none"> <li>In Array Manager, press the RETURN key after each name definition. On the command line, use a space to separate the names, for example: <pre>--server-dns-external "192.168.10.*:boston. indigo-insurance.com" "*" www.indigo-insurance.com"</pre> </li> </ul> <p><b>Note</b> You must restart this Secure Global Desktop server for a change to this setting to take effect.</p>
Log Directory	<code>--server-logdir <i>dir</i></code>	<ul style="list-style-type: none"> <li>Where diagnostic logs are stored on this host.</li> <li>You can set the Log Filter on the <a href="#">Array properties</a> panel.</li> </ul> <p><b>Note</b> This is a read-only attribute and can't be changed.</p>
Location	<code>--server-location <i>location</i></code>	<ul style="list-style-type: none"> <li>A string identifying the location of the array member, used for intelligent array routing.</li> <li>Leave blank unless your array spans a WAN (or includes slow links) and you use the intelligent array routing load balancing feature.</li> <li>More than one string is allowed, but this slows application launch.</li> <li>This setting constrains emulator session and application server load balancing to ensure optimal bandwidth usage. Secure Global</li> </ul>

		<p>Desktop servers are chosen with the same location as application servers, where possible.</p> <ul style="list-style-type: none"> <li>• If used, you should set this attribute on all array members, and for appropriate host objects in the organizational hierarchy.</li> </ul>
Secure Global Desktop Login	<pre>--server-login enabled   disabled</pre>	<ul style="list-style-type: none"> <li>• Whether to allow users to log in to this Secure Global Desktop server.</li> <li>• Choose Not Allowed (disabled) to "decommission" a Secure Global Desktop server: no users may log in and no new emulator sessions can start. Users currently logged in to this server, or with emulator sessions hosted on this server, are not affected. Users may log in to another array member and resume emulator sessions hosted on this server.</li> <li>• Users are redirected to the web page defined in the Redirection URL. Typically, you would set this to another Secure Global Desktop server in the array.</li> </ul>
Redirection URL	<pre>--server-redirectionurl url</pre>	<ul style="list-style-type: none"> <li>• The URL that client devices are redirected to if this Secure Global Desktop server is not allowing users to log in.</li> <li>• If blank, redirects to a page telling users that they may not log in.</li> </ul>

## Related topics

- Introducing Array Manager
- Introducing webtop and emulator session load balancing
- Introducing application server load balancing
- What are peer DNS names and external DNS names?
- Array properties (array-wide)
- Location (--location)



## Licenses properties (array-wide)

The Licenses Properties panel of Array Manager is in two parts:

- the top part allows you to see and manage your Secure Global Desktop license keys and
- the bottom part shows a summary of what's licensed by the key.

### License management

The license management part of the panel shows all the license keys currently installed in the array. The keys apply to all array members. When you move your mouse pointer over a license key, a tooltip displays which shows a breakdown of what's licensed by the key.

You can add and remove license keys in this area:

- To add a license key, type or paste the key into the empty boxes.  
As you type the last character in the key, the key is validated and becomes active.
- To remove a key, delete the characters in the key.  
When you remove the last character in the key, the key is deleted.

As you add/remove license keys, Secure Global Desktop updates the information in the license summary part of the panel.

If you remove all the license keys, Secure Global Desktop reverts to evaluation mode or expired evaluation mode, depending on how recently you installed the software. You cannot log in to a Secure Global Desktop server when it is in expired evaluation mode. To license a server when it is in expired evaluation mode, you must either add a valid license key (using `tarantella license add`) or join the server to an array that is already fully licensed.

Array Manager displays any invalid license keys with a red background. This may be for example, because the license key was entered incorrectly.

### Licensing summary

The licensing summary part of the panel displays the current licensing status for the array. It shows:

- the Secure Global Desktop product you are licensed to use.

- the current license mode of the array. This is either:
  - [Evaluation mode](#) - the end date of the evaluation period displays in brackets.
  - [Fully licensed](#)
- a breakdown by license type of what's licensed. For details about license types, see [Licensing and Sun Secure Global Desktop Software](#).

### Related topics

- [Licensing and Sun Secure Global Desktop Software](#)
- [The tarantella license command](#)

## Load Balancing properties (array-wide)

Attributes on the Load Balancing Properties panel of Array Manager are used:

- to set the algorithm Secure Global Desktop uses to load balance emulator sessions and
- to set the default algorithm Secure Global Desktop uses to load balance application servers.

The attributes apply to all array members.

From the command line, use `tarantella config` to view and edit these settings.

Changes to these attributes take effect immediately.

Array Manager	Command line	Description
Emulator Sessions: Use array member with	<code>--sessions-loadbalancing-algorithm <i>algorithm</i></code>	<ul style="list-style-type: none"><li>• The algorithm used at application launch time to choose the array member that hosts the emulator session (in other words, the method used to choose where to run the Protocol Engine when a user starts an application).</li><li>• In Array Manager, values are User's webtop session, Least CPU usage and Fewest emulator sessions.</li><li>• On the command line, values are: <code>.../_beans/com.sco.tta.server.loadbalancing.tier2.LocalLoadBalancingPolicy</code> (for User's webtop session) <code>.../_beans/com.sco.tta.server.loadbalancing.tier2.CpuLoadBalancingPolicy</code> (for Least CPU usage) <code>.../_beans/com.sco.tta.server.loadbalancing.tier2.SessionLoadBalancingPolicy</code> (for Fewest emulator sessions).</li><li>• Select User's webtop session to choose the</li></ul>

		array member which is hosting the user's webtop session.
Applications: Use application server with	<code>--launch-loadbalancing-algorithm cpu   memory   sessions</code>	<ul style="list-style-type: none"> <li>• The default algorithm Secure Global Desktop uses to choose the best application server on which to run the application. The server is selected from those defined on the application object's <a href="#">Hosts tab</a>.</li> <li>• This attribute is only used if the value of the application object's <a href="#">Load Balancing Algorithm</a> is <code>Use array-wide setting</code>.</li> <li>• Select one of the following settings: <ul style="list-style-type: none"> <li>◦ Least CPU usage (<code>cpu</code>) - choose the application server with the most CPU idle time.</li> <li>◦ Most free memory (<code>memory</code>) - choose the application server with the most free memory.</li> <li>◦ Fewest application sessions (<code>sessions</code>) - choose the application server that is running the fewest application sessions through Secure Global Desktop. This is the default setting.</li> </ul> </li> </ul> <p><b>Note</b> To use these algorithms, you must also install the Sun Secure Global Desktop Enhancement Module on the application server.</p>

## Related topics

- [Introducing webtop and emulator session load balancing](#)
- [Understanding webtop and emulator sessions](#)
- [Introducing application server load balancing](#)



## Print Protocol Engine properties (server-specific)

Attributes on the Print Protocol Engine Properties For... panel of Array Manager let you tune Secure Global Desktop printing processes for a particular array member. The attributes apply independently to each Secure Global Desktop server.

From the command line, use `tarantella config` to view and edit these settings.

Changes to these attributes take effect for new Protocol Engines only. Existing Protocol Engines are not affected.

Array Manager	Command line	Description
Compression	<code>--ppe-compression auto   always   never</code>	<ul style="list-style-type: none"><li>• Whether a Print Protocol Engine uses data compression on a client connection.</li><li>• Use <code>auto</code> ("If connection is slow" in Array Manager) to cause the Print Protocol Engine to only compress data if the connection is slow.</li></ul>
Threshold	<code>--ppe-compressionthreshold bytes</code>	<ul style="list-style-type: none"><li>• The smallest size of file that a Print Protocol Engine will compress.</li></ul>
Process Tuning: Exit after	<code>--ppe-exitafter seconds</code>	<ul style="list-style-type: none"><li>• The length of time a Print Protocol Engine process will continue running without any active connections.</li></ul>

### Related topics

- Introducing Array Manager
- Introducing Secure Global Desktop printing

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Printing properties (array-wide)

Attributes on the Printing Properties panel of Array Manager control printing from Windows applications that use the Microsoft RDP [Windows Protocol](#). The settings on this panel are the default settings for the array which can be overridden by the [user-specific printing configuration](#) for an organization, organizational unit or person object.

From the command line, use `tarantella config` to view and edit these settings.

Array Manager	Command line	Description								
Printing	<code>--printing-mapprinters 2   1   0</code>	<p>Controls which client printers users can print to from Windows application. By default, users can print to all their client printers.</p> <table border="1"><thead><tr><th>Command line</th><th>Array Manager</th></tr></thead><tbody><tr><td>2</td><td>Let users print to all client printers</td></tr><tr><td>1</td><td>Let users print to client's default printer</td></tr><tr><td>0</td><td>No client printers available.</td></tr></tbody></table> <ul style="list-style-type: none"><li>• If you select No client printers available, you can still use a <a href="#">Secure Global Desktop PDF printer</a>.</li><li>• Changes to this attribute take effect for new webtop sessions.</li><li>• If users can only print to their default printer and they want to print to a different printer, they have to log out of Secure Global Desktop, change the default printer</li></ul>	Command line	Array Manager	2	Let users print to all client printers	1	Let users print to client's default printer	0	No client printers available.
Command line	Array Manager									
2	Let users print to all client printers									
1	Let users print to client's default printer									
0	No client printers available.									



		and then log in again.
Printing: Let users print to a PDF printer	<code>--printing-pdfenabled 1   0</code>	<p>Allows users to print from a Windows application using the Secure Global Desktop "Universal PDF" printer.</p> <ul style="list-style-type: none"> <li>• This is enabled by default.</li> <li>• Changes to this attribute take effect for new webtop sessions.</li> </ul>
PDF Printing: Let users print to a PDF local file	<code>--printing-pdfviewerenabled 1   0</code>	<p>Allows users to print from a Windows application using the Secure Global Desktop "Print to Local PDF File" printer.</p> <ul style="list-style-type: none"> <li>• This is enabled by default.</li> <li>• Changes to this attribute take effect for new webtop sessions.</li> </ul>
PDF Printing: Driver name	<code>--printing-pdfdriver <i>driver_name</i></code>	<p>Type the name of the printer driver to use for Secure Global Desktop PDF printing. This printer driver must be installed on every Windows application server used with Secure Global Desktop.</p> <ul style="list-style-type: none"> <li>• This attribute is only available if Let users print to a PDF printer is enabled.</li> <li>• The printer driver must be a PostScript printer driver.</li> <li>• The default is <code>HP Color LaserJet 8500 PS</code>.</li> <li>• The name of the printer driver must match the name of the printer driver installed on the Windows application server exactly. Pay particular attention to the use of capitals and spaces. The <code>/opt/tarantella/etc/data/default.printerinfo.txt</code> file contains all the common printer driver names ordered by manufacturer. To avoid errors, copy and paste the driver name</li> </ul>

		<p>from this file.</p> <ul style="list-style-type: none"> <li>• Changes to this attribute take effect for new webtop sessions.</li> </ul>
<p>PDF Printing: Make PDF printer the default for Windows 2000/3</p>	<pre>--printing-pdfisdefault 1   0</pre>	<p>Sets the Secure Global Desktop "Universal PDF" printer as the client's default printer when printing from a Windows application.</p> <ul style="list-style-type: none"> <li>• This attribute is only available if Let users print to a PDF printer is enabled.</li> <li>• By default, the Universal PDF printer is not the default (0).</li> <li>• Changes to this attribute take effect for new webtop sessions.</li> </ul>
<p>PDF Printing: Make PDF file printer the default for Windows 2000/3</p>	<pre>--printing-pdfviewerisdefault 1   0</pre>	<p>Sets the Secure Global Desktop "Print to Local PDF File" printer as the client's default printer when printing from a Windows application.</p> <ul style="list-style-type: none"> <li>• This attribute is only available if Let users print to a PDF local file is enabled.</li> <li>• By default, the Print to Local PDF File printer is not the default (0).</li> <li>• Changes to this attribute take effect for new webtop sessions.</li> </ul>

## Related topics

- [Introducing Secure Global Desktop printing](#)
- [Configuring Secure Global Desktop PDF printing](#)
- [User-specific printing configuration \(--userprintingconfig\)](#)
- [Introducing Array Manager](#)
- [What is an array?](#)



## Security properties (array-wide)

Attributes on the Security Properties panel of Array Manager are security settings for the array. The attributes apply to all array members.

From the command line, use `tarantella config` to view and edit these settings.

Array Manager	Command line	Description
Password Cache: Generate new encryption key on restart	<code>--security-newkeyonrestart 1   0</code>	<ul style="list-style-type: none"><li>• Whether to generate a new encryption key for the password cache when the Secure Global Desktop server restarts.</li><li>• If a new encryption key is generated, the existing password cache is preserved and encrypted with the new key.</li></ul>
Print Name Mappings: Expire after	<code>--security-printmappings-timeout seconds</code>	<ul style="list-style-type: none"><li>• How long an entry in the print name mapping table is retained. This table is used to ensure that users can print from an application and then exit the application, without losing the print job.</li><li>• The timer starts counting when the user closes the last application on that application server.</li><li>• We recommend you set this to be greater than the maximum delay between choosing to print from an application and the printer responding.</li><li>• If you change this value, all existing expiry timeouts are reset. Changes take effect immediately.</li></ul>

		<ul style="list-style-type: none"> <li>• To flush the table, set to 0, Apply, and then set to a larger value.</li> <li>• To display the table, use <code>tarantella print status --namemapping</code>.</li> </ul>
<p>Connection Types: Apply when users log in</p>	<pre>--security-applyconnections 1   0</pre>	<ul style="list-style-type: none"> <li>• Whether to take note of the <b>Connections</b> attributes when a user logs in to Secure Global Desktop.</li> <li>• Check the box (set to 1) if you're using the Connections attribute for person, organizational unit or organization objects.</li> <li>• Clear the box if Secure Global Desktop security services are not enabled.</li> <li>• If Secure Global Desktop security services are enabled, connections are secure unless the box is checked <b>and</b> some connections are defined otherwise.</li> <li>• Clearing the box lets users log in more quickly.</li> <li>• Changes to this attribute take effect immediately.</li> </ul>
<p>X Displays: Use X authorization (xauth)</p>	<pre>--security-xsecurity 1   0</pre>	<ul style="list-style-type: none"> <li>• Whether to secure all Secure Global Desktop X displays using X authorization. This prevents users from accessing X displays they're not authorized to access.</li> <li>• We recommend that you use X authorization. It is enabled by default.</li> <li>• To use X authorization, xauth must be installed on the application server.</li> <li>• If X authorization is enabled, Secure Global Desktop checks</li> </ul>

the standard locations for the xauth binary. Extra configuration may be needed if the [binary is in a non-standard location](#).

- Changes to this attribute take effect immediately.

**Note** This setting only secures the X display between the Secure Global Desktop server and the application server.

### Related topics

- [Introducing Array Manager](#)
- [What is an array?](#)
- [The tarantella passcache command](#)
- [Users cannot print from applications displayed through Secure Global Desktop](#)
- [Connections \(--conntype\)](#)
- [When X authorization is enabled, applications fail to start](#)

## Security properties (server-specific)

Attributes on the Security Properties For... panel of Array Manager are security settings for a particular array member. The attributes apply independently to each Secure Global Desktop server.

From the command line, use `tarantella config` to view and edit these settings.

Changes to these attributes take effect immediately.

Array Manager	Command line	Description
Connection Types	<code>--security-connectiontypes types</code>	<ul style="list-style-type: none"><li>• The possible connection types, and their current status.</li><li>• Check the box for each connection type you want to make available to users.</li><li>• From the command line, valid settings are <code>std</code> (standard connections only), <code>ssl</code> (secure connections only) or <code>std,ssl</code> (both standard and secure connections).</li><li>• Disabled types are not installed on this Secure Global Desktop server.</li></ul>
SSL Accelerator Support: Accept plaintext on secure port	<code>--security-acceptplaintext 1   0</code>	<ul style="list-style-type: none"><li>• Check the box to enable support for an external SSL accelerator.</li><li>• Checking this box allows the SSL Daemon to accept plain text traffic and pass it on to Secure Global Desktop server as if it was SSL traffic it had decoded.</li></ul>

<p>If SSL Daemon Doesn't Start</p>	<pre>--security-ssldaemon- failmode reducesecurity   stopserver</pre>	<ul style="list-style-type: none"> <li>• The action to take if the SSL Daemon, fails to start.</li> <li>• Choose Allow Standard Connections Only (reducesecurity) if you want the Secure Global Desktop server to continue running as though security services have been disabled. Users configured for secure connections will receive standard connections.</li> </ul>
<p>Firewall Forwarding URL</p>	<pre>--security-firewallurl server_url</pre>	<ul style="list-style-type: none"> <li>• The absolute URL to forward all web server traffic not related to Secure Global Desktop.</li> <li>• Use this feature if you plan to run Secure Global Desktop on the same port as your web server so that you don't have to open any additional ports in your firewall.</li> </ul>

### Related topics

- [Introducing Array Manager](#)
- [Security properties \(array-wide\)](#)
- [Connections \(--conntype\)](#)
- [What are Secure Global Desktop security services?](#)
- [Using Secure Global Desktop with the HTTPS port through a firewall](#)



## Secure Global Desktop Login properties (array-wide)

Use the attributes on the Array Manager Secure Global Desktop Login Properties panel to control how users log in to Secure Global Desktop. The attributes apply to all array members and take effect immediately.

Use the `tarantella config` command to `list` and `edit` these settings.

Attribute	Command Line	Description
Login Theme	<code>--login-theme <i>theme_name</i></code>	<ul style="list-style-type: none"><li>Choose the login theme to be used across the array.</li><li>The login theme determines the style and appearance of the page users see when logging in to Secure Global Desktop from a web browser.</li></ul> <p><b>Note</b> This attribute is only used with the <i>classic</i> webtop. The browser-based webtop does not use login themes.</p>
Use classic web server authentication	<code>--tarantella-config-components-webloginauthority 1   0</code>	<ul style="list-style-type: none"><li>Check the box to enable web server authentication for the <i>classic</i> webtop.</li></ul>
Use third party authentication	<code>--login-thirdparty 1   0</code>	<ul style="list-style-type: none"><li>Check the box to enable third party authentication for the <i>browser-based</i> webtop.</li><li>Allows you to give webtops to users who have been authenticated by an external mechanism, such as web server authentication.</li></ul>

<p>Search ENS for matching person</p>	<p>For the classic webtop:  <pre>--login-web-ens 1   0</pre></p> <p>For the browser-based webtop:  <pre>--tarantella-config-login-thirdparty-searchens 1   0</pre></p>	<ul style="list-style-type: none"> <li>• Check one or more boxes to select the search methods you want Secure Global Desktop to use to determine the identity and <a href="#">login profile</a> of a user who has been authenticated by an external authentication method.</li> <li>• See <a href="#">web server/third party authentication</a> for details.</li> <li>• If more than one box is checked, the search methods are used in the order shown above. However, neither web server authentication nor third party authentication support ambiguous users and so the first match found is used.</li> <li>• If the searches do not produce a match, the standard login page displays and the user must log in to Secure Global Desktop in the normal way.</li> </ul> <p><b>Note</b> On the command line, there are separate commands for the classic and browser-based webtops. If you use the command line, we recommend you enable/disable the options for <b>both</b> webtops.</p>
<p>Search LDAP and use closest ENS match</p>	<p>For the classic webtop:  <pre>--login-web-ldap-ens 1   0</pre></p> <p>For the browser-based webtop:  <pre>--tarantella-config-ldap-thirdpartyldapcandidate-useens 1   0</pre></p>	
<p>Search LDAP and use LDAP profile</p>	<p>For the classic webtop:  <pre>--login-web-ldap-profile 1   0</pre></p> <p>For the browser-based webtop:  <pre>--tarantella-config-ldap-thirdpartyldapcandidate-useprofile 1   0</pre></p>	
<p>Use default profile</p>	<p>For the classic webtop:  <pre>--login-web-profile 1   0</pre></p> <p>For the browser-based webtop:  <pre>--tarantella-config-login-thirdparty-allownonens 1   0</pre></p>	

Tokens are valid for

```
--login-web-tokenvalidity int
```

- The validity period of the web server authentication token in seconds. The number of seconds must be between 1 and 600. The default value is 180.
- If web server authentication is enabled, when a user goes to the `http://server.example.com/tarantella` URL, the web server generates a token and this is accepted by the Secure Global Desktop server as proof of authentication. Each token is valid only once.
- The token may need to be valid for a few minutes to allow client devices to download the Secure Global Desktop Java™ archive. If all users have the archive already installed, you can reduce the validity period to a few seconds.
- Reducing the token validity period may result in failed logins on slow networks.
- To ensure a token cannot be intercepted and used by a third party while still valid, use secure (HTTPS) web servers.

**Note** This attribute is only used for web server authentication with the *classic* webtop.

Web server username	<code>--login-web-user <i>string</i></code>	<ul style="list-style-type: none"> <li>• The username of the user that owns web server (httpd) processes.</li> <li>• The default is <code>ttaserv</code> as this is the user used by the <a href="#">Secure Global Desktop Web Server</a>.</li> <li>• If you use your own web server, you must change this to the user you use for your web server, typically <code>nobody</code>.</li> <li>• This user is a trusted user for web authentication. We recommend you restrict access to this user and you restrict the processes that run as this user. It is more secure to have a user that is used to run the web server and nothing else.</li> <li>• All web servers used in the array must use the same username.</li> <li>• You must restart all array members for a change to this setting to take effect.</li> </ul> <p><b>Note</b> This attribute is only used for web server authentication with the <i>classic</i> webtop.</p>
Anonymous user login authority	<code>--login-anon 1   0</code>	<ul style="list-style-type: none"> <li>• Check one or more boxes to enable those <a href="#">login authorities</a>.</li> <li>• The login authorities are listed in the order in which they are tried. If one login authority authenticates the user, no more login authorities are tried.</li> <li>• SecurID authentication is not supported on the Solaris Operating System on x86 platforms.</li> <li>• The <a href="#">authentication token login</a></li> </ul>
Authentication token login authority	<code>--login-atla 1   0</code>	
ENS login authority	<code>--login-ens 1   0</code>	
NT login authority	<code>--login-nt 1   0</code>	

LDAP login authority	<code>--login-ldap 1   0</code>	<p><b>authority</b> can only be used when the Secure Global Desktop Client is operating in <b>integrated mode</b>. The Native Client and Java™ technology clients do not support this login authority.</p>
Active Directory login authority	<code>--login-ad 1   0</code>	
UNIX group login authority	<code>--login-unix-group 1   0</code>	
UNIX user login authority	<code>--login-unix-user 1   0</code>	
SecurID login authority	<code>--login-securid 1   0</code>	
Windows NT Domain	<code>--login-nt-domain <i>dom</i></code>	<ul style="list-style-type: none"> <li>• The name of the Windows domain that the <b>NT login authority</b> uses to authenticate users.</li> </ul>
URL	<code>--login-ldap-url <i>url</i></code>	<ul style="list-style-type: none"> <li>• The location of the LDAP directory/Active Directory server (s) used for the LDAP login authority, the Active Directory login authority, third party/web server authentication (the LDAP user identity mapping options) and Directory Services Integration.</li> <li>• For the <b>LDAP login authority</b> and <b>third party/web server authentication</b>, this is a semicolon-separated list of URLs. The URLs are used in the order they are listed. If the first LDAP directory server listed is unavailable, Secure Global Desktop tries the next one in the list. Each URL has the form <code>ldap://<i>server</i>:<i>port</i>/<i>searchroot</i></code> where: <ul style="list-style-type: none"> <li>◦ <b>server</b> is the DNS name of the LDAP directory server.</li> </ul> </li> </ul>

- *port* is the TCP port on which the LDAP directory server listens for connections. You can omit this (and the preceding ".") to use the default port.
- *searchroot* is the position in the LDAP directory structure from which the LDAP login authority should start searching for matching users, for example `dc=indigo-insurance,dc=com`.

**Note** Use an `ldaps://` URL if your LDAP directory server requires or allows SSL connections. Extra configuration is required for SSL connections, see [Securing connections to LDAP directory servers](#) for details.

- For the **Active Directory login authority**, this is the URL of an Active Directory domain and takes the form `ad://domain`, for example `ad://east.indigo-insurance.com`. The URL **must** start `ad://` and **must not** contain a *searchroot*. Only enter **one** domain.

Username/ Password	Use <code>tarantella passcache new --ldap</code> command.	<ul style="list-style-type: none"><li>• The username and password of a user that has privileges to search an LDAP directory server/Active Directory server. This is not required for some LDAP directory servers.</li><li>• For the <b>LDAP login authority</b> or <b>third party/web server authentication</b>, use a full username such as <code>cn=Bill Orange, cn=Users, dc=indigo-insurance, dc=com</code>.</li><li>• For the <b>Active Directory login authority</b>, use a user principal name such as <code>orange@indigo-insurance.com</code></li></ul> <p><b>Note</b> For security reasons, the password is not displayed even if it has been previously set.</p>
Use Certificates	<code>--login-ldap-pki-enabled 1   0</code>	<ul style="list-style-type: none"><li>• Whether to use client certificates to authenticate the connection to an Active Directory server.</li><li>• This is disabled by default.</li><li>• See <a href="#">Securing connections to Active Directory and LDAP directory servers</a> for details</li></ul>

Base Domain	<code>--login-ad-base-domain <i>dom</i></code>	<ul style="list-style-type: none"> <li>• The domain the Active Directory login authority uses if users only supply a partial domain when they log in.</li> <li>• For example, if the root domain is set to "indigo-insurance.com" and a user logs in with the username "rouge west", the Active Directory login authority tries to authenticate "rouge west.indigo-insurance.com".</li> </ul>
Default Domain	<code>--login-ad-default-domain <i>dom</i></code>	<ul style="list-style-type: none"> <li>• The domain the Active Directory login authority uses if users do not supply a domain when they log in.</li> <li>• For example, if the default domain is set to "east.indigo-insurance.com" and a user logs in with the username "rouge", the Active Directory login authority tries to authenticate "rouge east.indigo-insurance.com".</li> </ul>
Generate authentication tokens	<code>--login-autotoken 1   0</code>	<ul style="list-style-type: none"> <li>• Whether to create authentication tokens for users so they can be authenticated with the <a href="#">authentication token login authority</a>.</li> <li>• To ensure an authentication token cannot be intercepted and used by a third party, use secure (HTTPS) web servers and <a href="#">enable Secure Global Desktop security services</a>.</li> </ul>

## Related topics



- Login authorities
- Introducing web server authentication
- Web server/third party authentication

## Smart Card Protocol Engine properties

Attributes on the Smart Card Protocol Engine Properties panel of Array Manager let you tune Secure Global Desktop smart card processes for a particular array member. The attributes apply independently to each Secure Global Desktop server.

From the command line, use `tarantella config` to view and edit these settings.

Changes to these attributes take effect for new Protocol Engines only. Existing Protocol Engines are not affected.

Array Manager	Command line	Description
Compression	<code>--scardpe-compression auto   always   never</code>	<ul style="list-style-type: none"><li>• Whether a Smart Card Protocol Engine uses data compression on a client connection.</li><li>• Use <code>auto</code> ("If connection is slow" in Array Manager) to cause the Protocol Engine to only compress data if the connection is slow.</li></ul>

### Related topics

- [Using smart cards with Windows applications](#)
- [Users are unable to use smart cards with Windows applications](#)

## Tuning properties (server-specific)

Attributes on the Tuning Properties For... panel of Array Manager let you tune the Secure Global Desktop server. The attributes apply independently to each Secure Global Desktop server.

From the command line, use `tarantella config` to view and edit these settings.

Array Manager	Command line	Description
Processing Limits: Maximum simultaneous requests	<code>--tuning-maxrequests num</code>	<ul style="list-style-type: none"><li>• The maximum number of requests the server processes simultaneously.</li><li>• As a rough guide, set this to the number of CPUs multiplied by 4.</li><li>• Too high a setting may degrade performance.</li><li>• Changes to this attribute take effect immediately.</li></ul>
Processing Limits: Maximum simultaneous webtop connections	<code>--tuning-maxconnections num</code>	<ul style="list-style-type: none"><li>• The maximum number of simultaneous webtop connections (connections between Secure Global Desktop clients and the Secure Global Desktop server).</li><li>• Once the limit is reached, connections are refused.</li><li>• Too high a setting may degrade performance.</li><li>• Changes to this attribute take effect immediately.</li></ul>

<p><b>File Descriptors</b></p>	<pre>--tuning- maxfiledescriptors <i>num</i></pre>	<ul style="list-style-type: none"> <li>● The maximum number of open file descriptors to allow.</li> <li>● Increasing this increases the number of simultaneous connections that may be handled.</li> <li>● This value affects all Secure Global Desktop server components.</li> <li>● Too high a setting may degrade performance.</li> <li>● Changes to this attribute take effect when the server restarts.</li> </ul>
<p><b>Server JVM Size</b></p>	<pre>--tuning-jvm-initial <i>MB</i> --tuning-jvm-scale <i>percent</i> --tuning-jvm-max <i>MB</i></pre>	<ul style="list-style-type: none"> <li>● Three attributes controlling the size and expansion rate of the memory allocated to the Secure Global Desktop server's Java™ 2 Platform Standard Edition Runtime Environment (JRE): <ul style="list-style-type: none"> <li>○ The amount of memory, in MB, to allocate initially for the Secure Global Desktop server's Java Virtual Machine (JVM). Set this to no greater than the amount of RAM on the host.</li> <li>○ A scaling factor (expressed as a percentage), used to increase the amount of JVM memory dynamically when needed.</li> <li>○ An absolute maximum size in MB, which is never exceeded.</li> </ul> </li> <li>● Too high settings may degrade performance.</li> <li>● Changes to this attribute take effect when the server or JVM restarts.</li> </ul>

Resource Synchronization	<code>--tuning-resourcesync-time <i>time</i></code>	<ul style="list-style-type: none"><li>• At what time to start resource synchronization each day, if enabled for the <a href="#">array</a>.</li><li>• Use the server's local time zone.</li><li>• Express the time in 24-hour clock format, for example "16:00 for 4pm.</li><li>• Changes to this attribute take effect immediately.</li></ul>
--------------------------	---	---

### Related topics

- [Introducing Array Manager](#)
- [Array properties \(array-wide\)](#)

## X Protocol Engine properties (server-specific)

Attributes on the X Protocol Engine Properties For... panel of Array Manager let you tune graphical emulator processes for a particular array member. The attributes apply independently to each Secure Global Desktop server.

From the command line, use `tarantella config` to view and edit these settings.

Changes to these attributes take effect for new Protocol Engines only. Existing Protocol Engines are not affected.

Array Manager	Command line	Description
Command-line Arguments	<code>--xpe-args <i>args</i></code>	<ul style="list-style-type: none"><li>Any arguments to the Protocol Engine. For example, the name of a log file.</li><li>You shouldn't need to change this unless asked by Technical Support.</li></ul>
Monitor Resolution	<code>--xpe-monitorresolution <i>dpi</i></code>	<ul style="list-style-type: none"><li>The default monitor resolution (in dpi) to assume.</li><li>You can override this value using an application's <a href="#">Monitor Resolution</a> attribute.</li></ul>
Font Path	<code>--xpe-fontpath <i>fontpath</i></code>	<ul style="list-style-type: none"><li>Directories on the Secure Global Desktop host containing the fonts used by the X Protocol Engine.</li><li>Font paths are listed in search order.</li><li>Use <code>%%INSTALLDIR%%</code> to mean the Secure Global Desktop <a href="#">installation directory</a>.</li><li>You can include font servers, for example <code>tcp/</code></li></ul>

		<p>boston:7000.</p> <ul style="list-style-type: none"> <li>On the command line, separate each directory in the font path with a comma ",".</li> </ul>
RGB Database	<code>--xpe-rgbdatabase file</code>	<ul style="list-style-type: none"> <li>Full pathname on the Secure Global Desktop host of the RGB database used by the X Protocol Engine to resolve color names to RGB values.</li> <li>Use <code>%%INSTALLDIR%%</code> to mean the Secure Global Desktop <a href="#">installation directory</a>.</li> </ul>
Keyboard Map	<code>--xpe-keymap lang   client-locale   file</code>	<ul style="list-style-type: none"> <li>The default keyboard map to use for graphical applications.</li> <li>To use a keyboard map based on the locale of: <ul style="list-style-type: none"> <li>the Secure Global Desktop server, select Use lang variable.</li> <li>the client device, select Use client's input locale.</li> </ul> </li> </ul> <p>The actual keymap used is determined using the <code>/opt/tarantella/etc/data/keymaps/xlocales.txt</code> file.</p> <p><b>Note</b> You can use the <code>*</code> and <code>?</code> wildcards in the <code>xlocales.txt</code> file to support a wide range of input locales. See the <code>xlocales.txt</code> file for details.</p> <ul style="list-style-type: none"> <li>Alternatively you can type a filename to always use a particular keyboard map.</li> <li>You can override this for each user with the person object's <a href="#">Keyboard Map</a> attribute.</li> </ul>

Client Window Management	<pre>--xpe-cwm-maxwidth <i>pixels</i> --xpe-cwm-maxheight <i>pixels</i></pre>	<ul style="list-style-type: none"> <li>• Two attributes for tuning this particular value of the <a href="#">Display Using</a> attribute.</li> <li>• The maximum expected horizontal and vertical display resolution for client devices connecting to this server.</li> <li>• Only applies for applications with Display Using set to Client Window Management, to avoid clipping problems.</li> </ul>
Session Start Timeout	<pre>--xpe-sessionstarttimeout <i>seconds</i></pre>	<ul style="list-style-type: none"> <li>• How long the X Protocol Engine waits for X applications to connect.</li> </ul>
Process Tuning: Maximum sessions per engine	<pre>--xpe-maxsessions <i>num</i></pre>	<ul style="list-style-type: none"> <li>• The maximum number of emulator sessions each X Protocol Engine handles.</li> <li>• More X Protocol Engines are started to meet demand.</li> </ul>
Process Tuning: Maximum users per engine	<pre>--xpe-maxusers <i>num</i></pre>	<ul style="list-style-type: none"> <li>• The maximum number of users each X Protocol Engine handles.</li> <li>• More X Protocol Engines are started to meet demand.</li> </ul>
Process Tuning: Exit after	<pre>--xpe-exitafter <i>seconds</i></pre>	<ul style="list-style-type: none"> <li>• The length of time an X Protocol Engine process will continue running without any active connections.</li> </ul>

## Related topics

- [Introducing Array Manager](#)
- [How do I use my own X fonts?](#)
- [Monitor Resolution \(--dpi\)](#)
- [Keyboard Map \(--keymap\)](#)
- [Display Using \(--displayusing\)](#)



Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Introducing webtop and emulator session load balancing

### Read this topic to...

- Understand how you can load balance webtop and emulator sessions.
- Know how to configure load balancing for webtop and emulator sessions.

### Webtop session load balancing

Webtop session load balancing is concerned with choosing a Secure Global Desktop server to log in to.

Users may log in to any Secure Global Desktop server in an [array](#) to see the same webtop, and to start or resume the same applications.

Webtop session load balancing happens before the first connection is made to Secure Global Desktop. You can use a number of mechanisms to choose an appropriate Secure Global Desktop server. For example:

- Round-robin or Dynamic DNS. You give your users one URL to use for Secure Global Desktop (for example, <http://www.indigo-insurance.com/tarantella>), and configure your DNS server to choose a Secure Global Desktop server in the array. Any server may be chosen.
- Allocate different Secure Global Desktop servers to different departments, and give one URL to each department.

**No webtop session load balancing solution is supplied with Secure Global Desktop.** You can use any third-party solution to choose a Secure Global Desktop server.

### Emulator session load balancing

Emulator session load balancing is concerned with choosing an [array](#) member to host an emulator session.

An emulator session requires a protocol engine, which communicates with the user's client device and with the application server running the application. A protocol engine may run on any array member: not necessarily the same array member that hosts the user's webtop session.

Secure Global Desktop can automatically balance emulator sessions across the array. The more array members you have, the less the load on each. You configure the algorithm used for emulator session load balancing on the [Load Balancing Properties](#) panel of Array Manager.

### Related topics

- [Understanding webtop and emulator sessions](#)
- [Introducing application server load balancing](#)

## Introducing application server load balancing

### Read this topic to...

- Understand what application server load balancing is.
- Learn how Administrators manage application server load balancing.
- Learn about Secure Global Desktop Advanced Load Management.
- Learn the main steps for configuring application server load balancing.

## What is application server load balancing?

Application server load balancing is concerned with:

- choosing an application server on which to run an application so that users get the best performance and
- distributing the launch of applications so that the application servers achieve a similar relative workload.

## How Administrators manage application server load balancing

Secure Global Desktop Administrators manage application server load balancing centrally from the array by:

- defining the set of application servers that can run an application by adding host objects to the application object's [Hosts](#) tab.
- making application servers [available or unavailable to run applications](#), for example to allow for maintenance work.
- selecting a load balancing algorithm, which Secure Global Desktop uses to determine the most suitable server for the user. You can set an [array-wide default algorithm](#) which you can then [override for an individual application](#).

By default, Secure Global Desktop uses an algorithm which load balances application servers by

counting the number of application sessions each server is hosting through Secure Global Desktop and then selecting the server with the fewest sessions. You can also use Advanced Load Management, which provides additional algorithms for load balancing application servers based on their **true load when a user launches an application**.

## Using Advanced Load Management

Advanced Load Management provides algorithms for load balancing application servers based on either the amount of free memory or the amount of free CPU when the application is launched. You can only load balance X applications, Windows applications and character applications using these algorithms.

To use this feature, you must install a Sun Secure Global Desktop Enhancement Module on every application server. This installs a load balancing service which provides Secure Global Desktop with 'real time' information about the application server's CPU/memory load. It also helps Secure Global Desktop to detect whether an application server is available, for example because it is being rebooted.

### Overview of how the load balancing service works

The following is an overview of how the load balancing service works:

1. Whenever the primary Secure Global Desktop server is started, it builds a list of application servers that need to be load balanced. The list is updated whenever a host is added to or removed from an application object.
2. The primary Secure Global Desktop server contacts each of the application servers that are to be load balanced and requests initial load information. It does this by contacting the load balancing service which is listening on port 3579/tcp. Establishing contact also confirms that the application server is available to run applications.
3. The primary Secure Global Desktop server sends updates to the other array members with capacity values for each of the algorithms and notifies them which application servers are currently not available.
4. The load balancing service sends regular updates to the primary Secure Global Desktop server. The Secure Global Desktop server listens on port 3579/udp for the updates. The updates take place even if the load does not change. The absence of a regular update helps Secure Global Desktop to detect whether a server is available to run applications.
5. The primary Secure Global Desktop server sends updates to the other array members with capacity values for each of the algorithms and notifies them which application servers are currently not available. The updates take place even if the load does not change.
6. The primary or secondary Secure Global Desktop servers launch applications on the basis of the load information they have received.

**Note** The load balancing service always sends application server load data to the primary Secure Global Desktop server. If the primary is not available, CPU or memory-based load balancing is not available

and so the default session-based load balancing is used instead.

## Configuring application server load balancing

To use application server load balancing, you have to:

- [Configure Secure Global Desktop for load balancing](#)
- Install a Sun Secure Global Desktop Enhancement Module (only if you are using Advanced Load Management) and
- [Tune application server load balancing](#)

If you experience problems with CPU or memory-based load balancing, try the [load balancing troubleshooter](#).

### Related topics

- [Introducing the three-tier architecture](#)
- [Introducing webtop and emulator session load balancing](#)

## Configuring application server load balancing

The purpose of application server load balancing is to select the application server (host object) that will give the user the best performance for a particular application. When launching an application, Secure Global Desktop builds a list of candidate application servers using the application servers listed on the [hosts tab](#) for the application object. Secure Global Desktop then has to determine which of the candidates is the best one for the user. The decision takes into account:

- [the availability of the applications servers](#)
- [intelligent array routing](#)
- [server affinity](#)
- [the relative power of the application servers](#) and
- [the application server with the least load.](#)

This topic describes how these factors and your Secure Global Desktop configuration affect the choice of application server.

### Application server availability

When launching an application, Secure Global Desktop checks its list of candidate application servers to see if any of them are currently unavailable. If an application server is unavailable, it is removed from the list.

Secure Global Desktop Administrators can mark an application server as being unavailable by unchecking the [Available to run applications](#) attribute for the host object in Object Manager. You can do this, for example, to make an application server unavailable during maintenance work.

If you are using Secure Global Desktop Advanced Load Management, the load balancing service sends regular keep alive packets to Secure Global Desktop. If these packets stop, Secure Global Desktop considers the application server to be 'out of contact' and treats the server as unavailable until the load balancing service makes contact again.

### Intelligent array routing

Secure Global Desktop uses intelligent array routing to ensure that connections between Secure Global Desktop servers and application servers take place over high-speed links.

Secure Global Desktop's Protocol Engines convert the native protocol (such as X11), which is used between the application server and the Secure Global Desktop server, into the Adaptive Internet Protocol (AIP), which is used between the Secure Global Desktop server and the client device. AIP is optimized for lower bandwidths and, in general, it's best to use high-speed links between Secure Global Desktop servers and application servers so they're "close" in network terms.

However, if your network includes slow links, you can optimize application usability by identifying the 'location' of each array member and each application server. Intelligent array routing tries to ensure that the Protocol Engine runs on a Secure Global Desktop server in the same location as the application server. You should make sure that all servers configured with the same location are connected by high-speed links.

You define the [location of each array member](#) in Array Manager, and the [location of each application server](#) in Object Manager.

## Server affinity

When launching applications, Secure Global Desktop takes into account whether the user is already running any applications on an application server. This is known as **server affinity**. Server affinity means that, if possible, Secure Global Desktop will launch an application on the same application server as the last application the user launched.

**Note** For server affinity to work efficiently, the applications must be associated with the same set of hosts.

Server affinity is expressed as a percentage and currently only two values are allowed:

- 0 - this means any running applications do not affect the choice of application server.
- 100 - this means any existing application servers must be re-used if they can run the selected application. This is the default value.

You change the server affinity value by running the following command:

```
tarantella config edit --tarantella-config-applaunch-appserveraffinity  
affinity_value
```

**Note** If you are using Windows applications, we recommend that you do not change this value, as using multiple application servers causes problems, especially with roaming profiles. There may also be licensing implications for running different applications in a suite of applications on different servers.

## The relative power of the application servers



Secure Global Desktop allows you to factor the relative power of the application servers in to the decision as to where to launch an application.

The relative power is expressed as a percentage and by default all servers have a value of 100. By [editing the `weighting` load balancing property](#) for your servers, you can increase/decrease these weightings to increase/decrease the likelihood of Secure Global Desktop choosing an application server. You can use this to:

- reduce the number of application sessions that are launched on a particular server, for example, because it is used for other processes outside of Secure Global Desktop, or
- increase the number of application sessions that are launched on a particular server, for example, because, although it has less CPU capacity, it has better IO capabilities.

For more details on how the weighting is used, see the load calculations below.

### Example 1

You have two application servers london and paris, paris has a weighting of 50 and london has a weighting of 100. If all the other application launch conditions are met and the servers currently have the same load, london is more likely to be chosen to launch the application.

### Example 2

You have 100 application servers and you want to make just one of them "more powerful" than the others. Increase the weighting of that server to 200.

## The application server with the least load

Secure Global Desktop uses a load balancing algorithm to select the application server with the least load.

You set an array-wide default algorithm on the [Load Balancing Properties](#) panel of Array Manager. You can override the default by specifying a different algorithm for [the application object](#). This allows you load balance applications in different ways.

Currently three algorithms are supported:

- [Fewest application sessions](#).
- [Least CPU usage](#).
- [Most free memory](#).

To use the CPU/memory-based algorithms, the Sun Secure Global Desktop Enhancement Module must

be installed and running on every application server.

**Note** You can only load balance Windows, X and character applications with the CPU/memory-based algorithms.

### **Fewest application sessions**

The Fewest application sessions algorithm allows Secure Global Desktop to choose the application server which is currently running the fewest number of application sessions. It is based on a simple count of the number of application sessions being hosted through Secure Global Desktop.

This algorithm is the default.

If you use either the CPU or memory-based algorithms, the Fewest application sessions algorithm is used as a fallback whenever there is a problem, for example, if the application server load information is not available to the array when the application is launched. This might happen, for example, if the primary Secure Global Desktop server is being re-started.

The application server load is calculated using the following formula:

```
number of application sessions x 100 /server weighting
```

### **Example calculation**

The application server london is currently hosting 10 application sessions and has a server weighting value of 100.

The application server paris is currently hosting 12 application sessions, and has a server weighting value of 100.

The load value for london is:

```
10 x 100/100 = 10
```

The load value for paris is:

```
12 x 100/100 = 12
```

Assuming the other conditions for launching an application are met, Secure Global Desktop would chose london to launch the next two application sessions. If the server weighting value for london was decreased to 50, Secure Global Desktop would choose paris to launch the next 8 application sessions,

because london's load is now 20 (10 x 100/50).

## Least CPU usage

The Least CPU usage algorithm allows Secure Global Desktop to choose the application server with the most CPU idle and is suitable for applications that require many processor cycles.

The algorithm measures the application server's load in terms of its CPU capabilities (measured in bogomips) and by how much of its CPU is being used. These measurements are taken by the load balancing service.

The spare capacity is calculated using the following formula:

```
(bogomips x cpu idle %) x weighting /100
```

### Example calculation

The application server london has a bogomips measurement of 500, a server weighting value of 75 and has 25% CPU idle.

The application server paris has a bogomips measurement of 100, a server weighting value of 100 and has 50% CPU idle.

The spare capacity for london is:

```
(500 x 25) x 75/100 = 9375
```

The spare capacity for paris is:

```
(100 x 50) x 100/100 = 5000
```

Assuming the other conditions for launching an application are met, london would be the chosen application server, even though paris is using less of its CPU and has a higher server weighting value.

## Most free memory

The Most free memory algorithm allows Secure Global Desktop to choose the application server with most free virtual memory and is suitable for applications that require a lot of memory.

The algorithm measures the application server's load by comparing the application server's actual virtual memory with the amount of memory that is currently being used. These measurements are taken

by the load balancing service.

The spare capacity is calculated using the following formula:

```
virtual memory free x weighting /100
```

### Example calculation

The application server london has a server weighting value of 100 and has 250MB virtual memory free.

The application server paris has a server weighting value of 75 and has 500MB virtual memory free.

The spare capacity value for london is:

```
250 x 100/100 = 250
```

The spare capacity value for paris is:

```
500 x 75/100 = 375
```

Assuming the other conditions for launching an application are met, paris would be the chosen application server.

### Related topics

- [Introducing application server load balancing](#)
- [Troubleshooting CPU/memory-based application server load balancing](#)
- [Tuning application server load balancing](#)
- [Editing application server load balancing properties](#)

## Tuning application server load balancing

Administrators can tune application server load balancing by [editing application server load balancing properties](#). These properties affect:

- how the CPU/memory-based load balancing service operates, and
- how Secure Global Desktop calculates the application server load.

This topic describes how you can tune load balancing and assumes you understand [how Secure Global Desktop load balancing works](#).

### Tuning properties used by all load balancing algorithms

#### The application server's relative power

The `weighting` property allows you to factor the relative power of the application servers in to the decision Secure Global Desktop takes as to where to launch an application. This is discussed in [Configuring load balancing](#).

### Tuning properties used by the CPU/memory-based algorithms

#### Load balancing ports

The primary Secure Global Desktop server in the array contacts the load balancing service on an application server on port 3579/tcp. This is controlled by the `listeningport` property.

The load balancing service sends updates to the primary Secure Global Desktop server on port 3579/udp. This is controlled by the `probe.listeningport` property.

These ports are registered ports and you should only change these properties if Secure Global Desktop Support asks you to. You will need to open these ports if you have a firewall between the primary Secure Global Desktop server and the application servers.

#### Secure Global Desktop server requests updates from an application server

The `connectretries` property is the number of times the primary Secure Global Desktop server tries to connect to an application server to request load updates. The interval between each attempt is

controlled by the `shorttimeout` property. If the attempts to connect fail, the Secure Global Desktop server waits for the period of time controlled by the `longtimeout` property before trying again.

For example, using the defaults for these properties, the Secure Global Desktop server makes 5 attempts (`connectretries`) to contact the application server at 20 second intervals (`shorttimeout`). If all 5 fail, Secure Global Desktop waits 600 seconds (`longtimeout`) before making 5 more attempts at 20 second intervals.

You might want to change the timeout properties, for example, if your application server takes a long time to reboot.

The `scaninterval` property controls the period of time between scans of the Secure Global Desktop server's list of load-balanced application servers. The scan checks for the application servers that need to be contacted to request a load update (`connectretries`).

The `sockettimeout` property controls how long it is before a Secure Global Desktop server gets an error by trying to contact the load balancing service when there is no data available.

### **Frequency of the load calculation**

The `probe.samplerate` and `probe.windowsize` properties control how often the load balancing service measures the application server's average load.

For example, the `probe.samplerate` is 10 seconds and the `probe.windowsize` is 5. After 50 seconds (5 x 10), the 5 measurements needed to calculate the average have been taken. After a further 10 seconds, the load balancing service takes a new measurement, discards the oldest measurement and then calculates a new average load.

You can increase/decrease the frequency of the calculation depending on how often you expect the application server load to change. For example, do users start applications at the start of the day and then close them at the end, or do they repeatedly start and stop applications.

### **Frequency of updates to the primary Secure Global Desktop server**

The `replyfrequency` property controls the interval at which the load balancing service send updates to the primary Secure Global Desktop server.

The `percentagechange` property controls the minimum percentage change in CPU/memory use that must be reported to the primary Secure Global Desktop server. The load balancing service sends these updates as soon as the percentage change occurs. For example if an application server is running at 30% CPU load and the `percentchange` value is 10, an update occurs when the load is either 20% or 40%. The load balancing service takes into account sudden 'spikes' of activity and also makes

adjustments when, for example a server reaches 81% CPU load and the `percentagechange` value is 20%.

The `replyfrequency` updates are sent even if the load does not change and even if there has been a `percentagechange` update. The basis for the `percentagechange` calculation is reset every time there is a `replyfrequency` update.

If there is no update from an application server for `updatelimit x replyfrequency` seconds, Secure Global Desktop considers the application server to be 'out of contact'. This means the application server is marked as unavailable to launch applications until the Secure Global Desktop server can re-establish contact with it.

### Reliability of CPU/memory data

Secure Global Desktop considers the CPU/memory data to be too unreliable if there has been no update from the application server for `maxmissedsamples x replyfrequency` seconds.

**Note** The load balancing service sends updates even if the load does not change.

If the data is unreliable, the data is ignored when making the decision on where to launch an application. The net effect of this is to make the application server the last in the queue so that it will only be used to launch applications if no other server is available or suitable.

### Frequency of updates to array members

The primary Secure Global Desktop server sends CPU/memory load updates to the other members of the array every `maxmissedsamples x replyfrequency/2` seconds. This update takes place even if the load does not change.

If a secondary Secure Global Desktop server misses an update, it considers the load data it has to be unreliable and reverts to the Fewest application sessions method of load balancing. It uses this method until it receives a new update.

#### Related topics

- Introducing application server load balancing
- Configuring application server load balancing
- Troubleshooting CPU/memory-based application server load balancing
- Editing application server load balancing properties



## Editing application server load balancing properties

You can tune Secure Global Desktop load balancing by editing application server load balancing properties. The properties are stored in a properties file, which you can edit with a text editor. There are three properties files:

- a [global properties file](#), which contains the default settings for the array.
- an [application server-specific properties file](#), which allows you to override some of the global settings for a particular application server.
- a [UNIX application server properties file](#), which contains the settings the UNIX load balancing service uses when it is first started or re-started.

This topic describes how you edit the properties files and what properties are available. For detailed information on how to use the properties, see [Tuning application server load balancing](#).

**Only edit these properties if you are sure you know what you're doing.**

### The global load balancing properties file

The file `tier3lb.properties` contains the default load balancing properties for the array. The file is in the `/opt/tarantella/var/serverconfig/global` directory. You should only edit these properties on the primary Secure Global Desktop server in the array. The primary will copy the amended files to the secondaries.

In the `tier3lb.properties` properties file, the properties are prefixed with `tarantella.config.tier3lb`, for example `tarantella.config.tier3lb.weighting`.

The table below:

- lists the properties you can change,
- gives the default value of the property when Secure Global Desktop is first installed,
- explains what each property is used for, and
- indicates whether you can override the property in an application server-specific properties file.

Property	Default value	Purpose	Can be overridden?
----------	---------------	---------	--------------------

<code>connectretries</code>	3	The number of times the Secure Global Desktop server tries to connect to the application server to request CPU/memory updates.	No
<code>listeningport</code>	3579	The UDP port the Secure Global Desktop server uses to listen for data sent by the load balancing service.	No
<code>longtimeout</code>	900	The pause in seconds between groups of attempts by the Secure Global Desktop server to connect to the application server.	No
<code>maxmissedsamples</code>	20	The number of missed samples used to calculate whether the CPU/memory data for the application server is too unreliable to be used.	No
<code>probe.listeningport</code>	3579	The TCP port the load balancing service uses to listen for requests from Secure Global Desktop servers, for example, when to start sending updates.	Yes
<code>probe.percentchange</code>	10	The minimum percentage increase or decrease in CPU/memory use that must be reported to the Secure Global Desktop server.	Yes
<code>probe.replyfrequency</code>	30	The interval in seconds at which the load balancing service sends CPU/memory measurements to the Secure Global Desktop server. The minimum value for this property is 2.	Yes
<code>probe.samplerate</code>	15	The interval in seconds between CPU/memory measurements. The minimum value for this property is 1.	Yes
<code>probe.windowsize</code>	3	The number of CPU/memory measurements used to calculate the CPU/memory average. The minimum value for this property is 1.	Yes

<code>scaninterval</code>	60	The interval in seconds between scans of the Secure Global Desktop server's list of load-balanced application servers.	No
<code>shorttimeout</code>	60	The interval in seconds between attempts by the Secure Global Desktop server to connect to the application server.	No
<code>sockettimeout</code>	5	The socket timeout in seconds.	No
<code>updatelimit</code>	5	The limit used to calculate when the load balancing service has stopped sending updates.	No
<code>weighting</code>	100	The weighting of load measurements relative to the other application servers.	Yes

**Note** The following properties also appear in the `tier3lb.properties` properties file, but they must not be changed:

```
tarantella.config.name=tier3lb
tarantella.config.type=server
```

## The application server load balancing properties file

You can override some of the array default properties by creating a server-specific load balancing properties file. You have to manually create this file in the `/opt/tarantella/var/serverconfig/global/t3hostdata` directory. You should only create a server-specific properties file on the primary Secure Global Desktop server in the array. The primary will copy the file to the secondaries.

The properties you can override are shown in the table above.

In the server-specific properties file, the properties are prefixed with `tarantella.config.tier3hostdata`, for example `tarantella.config.tier3hostdata.weighting`.

To create a server-specific properties file:

1. On the primary Secure Global Desktop server, change to the `/opt/tarantella/var/serverconfig/global/t3hostdata` directory.
2. Copy the `template.properties` file to a file called `hostname.properties` in the same directory, for example, `paris.indigo-insurance.com.properties`.

3. Open the file in a text editor.
4. Find the line containing the `tarantella.config.tier3hostdata.name` property.
5. After the "=", add the ENS name of the application server. The name must be enclosed in quotes and each part of the host name must be escaped using a backslash. For example, to apply the properties to the host `paris.indigo-insurance.com`, type `".../_ens/o\=Indigo Insurance/cn\=paris"`.
6. Uncomment the lines (by deleting the "#") which contain the properties you want to be override. Only uncomment the properties you want to be different from the array defaults.
7. Change the values of the properties you want to override.
8. Save the changes and close the file.
9. Do a warm restart of the primary Secure Global Desktop server (`tarantella restart --warm`).

**Note** The `template.properties` file contains comments to help you create a server-specific file.

## The UNIX application server properties file

The UNIX application server properties file contains the settings that are used when the load balancing service is first started or whenever the service is restarted, for example if the server is rebooted.

The properties file is installed in the same directory as the Sun Secure Global Desktop Enhancement Module on the application server. By default, this is `/opt/tta-tem`.

You should only make changes to these properties:

- if you have been asked to by Secure Global Desktop Support or
- if you change the physical or virtual memory of the application server and you have not re-installed the Sun Secure Global Desktop Enhancement Module.

If you change these properties, you must manually stop and restart the load balancing service.

In the UNIX server properties file, the properties are prefixed with `tarantella.config.tier3loadbalancing`, for example `tarantella.config.tier3loadbalancing.port`.

### Related topics

- Introducing application server load balancing
- Configuring application server load balancing
- Troubleshooting CPU/memory-based application server load balancing
- Editing application server load balancing properties

## Troubleshooting CPU/memory-based application server load balancing

If you experience problems with CPU or memory-based application server load balancing, you can get information from various places to help you understand what is happening:

- **Secure Global Desktop server log files** - add the following filters on the [Array properties panel](#) in Array Manager:

```
server/tier3loadbalancing/*:t3loadbal%%PID%%.log
server/tier3loadbalancing/*:t3loadbal%%PID%%.jsl
```

This provides detailed information about the decision to launch an application and the data being sent by the application server.

- **application server log files** - for UNIX application servers these will be in the same directory as the Sun Secure Global Desktop Enhancement Module, by default this is `/opt/tda-tem`. For Windows application servers, this information displays in the Event Viewer.
- **load balancing service connection cgi program** - visit the following URL:  
`http://application_server_dns_name:3579?get&ttalbinfo`

You can use this information to troubleshoot the following symptoms:

### The load balancing service isn't working

- Has the Sun Secure Global Desktop Enhancement Module been installed on all application servers and is it running?  
Use the load balancing service connection cgi program to check.
- Is the primary Secure Global Desktop server running?  
The load balancing service on the application server sends load information to the primary Secure Global Desktop server. If the primary is not available, Secure Global Desktop uses Fewest application sessions as the method for load balancing application servers.
- Is your firewall blocking the load balancing service?  
For the load balancing service to work, the firewall must allow:
  - a TCP connection on port 3579 between the Secure Global Desktop server and the application server.
  - a UDP connection on port 3579 between the application server and the Secure Global Desktop server.

**Note** These connections do not need to be authenticated.

- What do the Secure Global Desktop server log files show?

## Secure Global Desktop ignores a server-specific load balancing properties file

After creating a server-specific load balancing properties file, you must do a warm restart of the primary Secure Global Desktop server (`tarantella restart --warm`).

## One application server is never picked

- Has the Sun Secure Global Desktop Enhancement Module been installed and is it running?  
Use the load balancing service connection cgi program to check.
- Is the application server available to launch applications?  
Check the host object in Object Manager.

## One application server is always picked regardless of its load

- Is more than one application server configured to run the application?  
Check the hosts tab for the application object.
- Are the other application servers available to launch applications?  
Check the host objects in Object Manager.
- Are you using the correct algorithm?  
Check the array-wide and application object settings.
- Are you using server affinity?  
Server affinity is on by default.
- What do the Secure Global Desktop server log files show?
- What do the application server log files show?
- Has the Sun Secure Global Desktop Enhancement Module has been installed?  
Use the load balancing service connection to check.

## Two identical application servers, but one launches more applications than the other

- Is the server weighting value for the servers the same?

## The server log file shows an update received for an unknown id

If the Secure Global Desktop server log file shows an information message which contains the text 'Got an update for unknown id *id* from machine *application server DNS name*' this can be ignored. It occurs only when the primary Secure Global Desktop server is restarted.

## Related topics

- [Introducing application server load balancing](#)
- [Configuring application server load balancing](#)
- [Tuning application server load balancing](#)
- [Editing application server load balancing properties](#)



## Using log filters to troubleshoot problems with the Secure Global Desktop server

When you first install Secure Global Desktop, the default log filters log all errors on the Secure Global Desktop server. If you want to obtain more detailed information, for example to troubleshoot a problem, you can set additional log filters. You set additional log filters by:

- typing the filter directly into the Log Filter field on the [Array properties](#) panel of Array Manager. Each filter must be separated by a RETURN.
- using the `tarantella config edit --array-logfilter` command. Each filter must be separated by a space.

Each filter has the form:

```
component/sub-component/severity:destination.
```

The options for each part of the filter and how you view the log output are described below.

**Note** Log filters can create large amounts of data. It is good practice to set as specific a filter as possible and then remove the filter when you have finished with it.

### Selecting a component and sub-component

Selecting a component and sub-component allows you to choose the area of information you want to log from the Secure Global Desktop server. The table below shows the available component/sub-component combinations and an explanation of the kind of information this will produce.

Component and sub-component	Information provided
<code>admin/auth</code>	Authentication of Secure Global Desktop Administrators and the UNIX root user. Example use: to find out why an Administrator is unable to run Object Manager.
<code>admin/gui</code>	Using Array Manager and Object Manager. Example use: to find out why you can not create an object in Object Manager.

admin/jndi	The Java Naming and Directory Interface™ (JNDI). Example use: to find out why a naming error with an object in ENS has happened.
admin/misc	Miscellaneous messages from using the administration tools. Example use: to find out why default profile objects are not available.
admin/status	Verbose logging for the <code>tarantella status</code> command. Example use: to find out why the <code>tarantella status</code> command is failing.
admin/webtopsession	Records of webtop sessions. Example use: to find out why a record of user's webtop session can not be found.
audit/glue	Audit of changes made to the Secure Global Desktop server configuration or to your ENS configuration and who made the changes. Example use: to find out who made changes to a person object.
audit/license	License use across an array of Secure Global Desktop servers. Example use: to find out why the use of licenses is not being recorded.
audit/session	Starting and stopping webtop and emulator sessions. Example use: to find out how long a user had an emulator session running.
cdm/audit	Authorization of Secure Global Desktop user for client drive mapping (CDM) purposes. Example use: to find out whether a user's credentials are causing CDM to fail.
cdm/server	Information about CDM services. Example use: to find out whether a client connection error is causing CDM to fail.
common/config	How Secure Global Desktop server configuration is stored and copied across the array. Example use: to find out why an array-wide configuration change is not being applied to a Secure Global Desktop server.

<code>metrics/glue</code>	Memory and timings. Example use: to find out how long it took to run a Secure Global Desktop command.
<code>metrics/soap</code>	The SOAP component of Tomcat's SOAP proxy. Example use: to trace how long it took a SOAP request to finish.
<code>server/billing</code>	Secure Global Desktop billing services. Example use: to find out why billing data is being lost.
<code>server/common</code>	General Secure Global Desktop information. Example use: to troubleshoot DNS errors.
<code>server/config</code>	Changes to Secure Global Desktop server configuration. Example use: to log changes to Secure Global Desktop server configuration or to find out if the configuration has become corrupt.
<code>server/csh</code>	The Secure Global Desktop client session handler. Example use: to find out why a user can not re-start an application session.
<code>server/deviceservice</code>	Mapping of users to accessible device data. Example use: to find out why a user can not access client drives.
<code>server/diskds</code>	Information about the ENS database. Example use: to get information about corrupt objects or inconsistencies in ENS.
<code>server/glue</code>	The Secure Global Desktop ASAD protocol used in requests from Secure Global Desktop clients to log in or launch applications or to communication between Secure Global Desktop servers. Example use: to find out why a user can't launch an application.
<code>server/install</code>	Installation and upgrades. Example use: to investigate problems with an installation.
<code>server/kerberos</code>	Windows Kerberos authentication. Example use: to find out why an Active Directory user can't log in.
<code>server/launch</code>	Launching or resuming applications. Example use: to find out why a user can't launch an application.
<code>server/ldap</code>	Connections to an LDAP server. Example use: to find out why an LDAP user can't log in.

<code>server/loadbalancing</code>	Webtop and emulator session load balancing. Example use: to find out why a Secure Global Desktop host isn't being selected to host emulator sessions.
<code>server/logging</code>	Logging. Example use: to find out why log messages are not being written to a file.
<code>server/login</code>	Log in to Secure Global Desktop. Example use: to find out which login authority authenticated a user and the login profile used.
<code>server/mupp</code>	The Secure Global Desktop MUPP protocol. Example use: Only use this filter if Secure Global Desktop Support asks you to.
<code>server/netlet</code>	Netlet connections. Example use: to find out why Netlet connections are failing.
<code>server/printing</code>	Secure Global Desktop printing services. Example use: to find out why print jobs are failing.
<code>server/replication</code>	Copying data between Secure Global Desktop servers in an array. Example use: to find out why data hasn't been copied between array members.
<code>server/securid</code>	Connections to SecurID ACE/Server®. Example use: to find out why SecurID authentication is not working.
<code>server/security</code>	Secure SSL-based connections. Example use: to find out why the SSL Daemon is not running.
<code>server/server</code>	The Secure Global Desktop JServer component. Example use: to troubleshoot Secure Global Desktop server failures, such as Java runtime exceptions which are not logged elsewhere.
<code>server/services</code>	Internal Secure Global Desktop server services. Example use: to find out why a service is failing.
<code>server/session</code>	Webtop sessions. Example use: to find out why a session failed to suspend.

<code>server/soap</code>	SOAP bean interface Example use: to diagnose problems with the SOAP beans.
<code>server/soapcommands</code>	SOAP requests. Example use: to log the SOAP requests received.
<code>server/tfn</code>	Secure Global Desktop Federated Naming (TFN) namespace. Example use: to find out why Object Manager is running in read-only mode.
<code>server/tier3loadbalancing</code>	Application server load balancing. Example use: to find out why a host is not being selected to launch an application.
<code>server/tokencache</code>	Authentication token cache. Example use: to find out why an authentication token is not being created for a user.
<code>server/tscal</code>	Windows Terminal Services Client Access Licenses (CALs) for non-Windows clients. Example use: to find out why a non-Windows client doesn't have a CAL.
<code>server/webtop</code>	Webtop content. Example use: to find out why an application isn't appearing on a user's webtop.

## Selecting the severity

You can select one of the following levels of severity for each log filter:

Severity	Description
<code>fatalerror</code>	Logs information on fatal errors. Fatal errors stop the Secure Global Desktop server from running. When you first install Secure Global Desktop, all fatal errors are logged by default.
<code>error</code>	Log information on any errors that occur. When you first install Secure Global Desktop, all errors are logged by default.
<code>warningerror</code>	Log information on any warnings that occur, for example if system resources are running low. When you first install Secure Global Desktop, all warnings are logged by default.

<code>info</code>	Informational logging. Useful for problem solving and identifying bugs.
<code>moreinfo</code>	Verbose informational logging.
<code>auditinfo</code>	Logs selected events for auditing purposes, for example changes to Secure Global Desktop server configuration. For details see, <a href="#">Using log filters for auditing</a>

The `fatalerror` severity produces the least amount of information and the `moreinfo` severity produces the most.

Selecting a severity level is not cumulative. For example, selecting `info` does not mean you also see `warning`, `error` or `fatalerror` log messages. To log more than one level of severity, use a wild card (see below).

## Using wildcards

You can use a wildcard ( `*` ) to match multiple components, sub-components and severities. For example, to log all warning, error and fatal error messages for printing, you could use `server/printing/*error`.

**Note** If you use a wildcard on the command line, you must enclose the filter in quotes to stop your shell from expanding them.

## Selecting a destination

When selecting a destination for the logs, you can specify that the output goes to:

- a log file or
- a log handler.

## Using log files

If you are outputting to a file, you can output to two types of file:

- `filename.log` - Secure Global Desktop formats this log output so that it is easy to read. This format is required by the `tarantella query errlog` command.

**Note** This command only searches log files that have names that end `error.log`.

- `filename.jsl` - Secure Global Desktop formats this log output for automated parsing and searching.

This format is required by the `tarantella query audit` command.

The file extension of the destination file controls the format of the file.

You can also create a separate log file for each process ID by including the `%%PID%%` placeholder in the file name.

The log files are output in the log directory specified on the [General Properties](#) pane for each array member. The directory is usually `/opt/tarantella/var/log`. You cannot change the location of the log files, but you can use a symlink to redirect the logs to a different location. Alternatively, you can use the syslog log handler described below.

## Using log handlers

A log handler is a JavaBeans component used as the destination for the log messages. When specifying a log handler, you must use its Secure Global Desktop Federated Name (TFN). Secure Global Desktop provides two standard log handlers:

- ConsoleSink and
- SyslogSink.

The ConsoleSink writes log messages in a easy to read format to standard error. This log handler is enabled by default and logs all errors. The TFN of this log handler is:

```
.../_beans/com.sco.tta.server.log.ConsoleSink
```

The SyslogSink writes log messages to the UNIX/Linux syslog facility. The TFN of this log handler is:

```
.../_beans/com.sco.tta.server.log.SyslogSink
```

## Example log filters

Here are some examples of commonly used log filters:

- to debug user logins:

```
server/login/*:login%%PID%%.log  
server/login/*:login%%PID%%.jsl
```

- to troubleshoot client drive mapping:

```
cdm/*/*:cdm%%PID%%.log  
cdm/*/*:cdm%%PID%%.jsl
```

```
server/deviceservice/*:cdm%%PID%%.log
server/deviceservice/*:cdm%%PID%%.jsl
```

- to troubleshoot printing problems:

```
server/printing/*:print%%PID%%.log
server/printing/*:print%%PID%%.jsl
```

- to get timing measurements for server performance:

```
metrics/*/*info:metrics.log
metrics/*/*info:metrics.jsl
```

- to send all warnings, errors and fatalerrors to syslog:

```
*/**/*error:.../_beans/com.sco.tta.server.log.SyslogSink
```

## Viewing log output

To view the log output, you can either:

- open the `.log` files in an editor or
- use `tarantella query` command.

If you use the `tarantella query` command, use:

- `tarantella query errlog` to see only the errors and fatalerrors for specific Secure Global Desktop server components and
- `tarantella query audit` searches the logs for any messages relating to a person, an application or an application server.

**Note** You can only use these commands to view the log output until the logs are archived. You configure archiving when you install Secure Global Desktop but you can change the settings at any time by running the `tarantella setup` command.

### Related topics



- Using log filters for auditing
- Array properties (array-wide)
- The tarantella query errlog command
- The tarantella query audit command

## Using log filters for auditing

Sun Secure Global Desktop Software allows you to set log filters to provide an audit of the following system events:

- starting up and shutting down the Secure Global Desktop server
- starting up and shutting down Secure Global Desktop security (SSL) services
- changes to your ENS configuration
- changes to your Secure Global Desktop server configuration
- unsuccessful attempts to log in to a Secure Global Desktop server
- logging in to and logging out from a Webtop and
- starting and stopping an application (emulator) session.

To audit these events, you must set a `*/**/auditinfo` log filter. You can use any of the standard destinations as a destination for the output, but you must direct the output to a `.jsl` file if you want to view the audit information from the command line.

**Note** Log output is only created while a Secure Global Desktop server is actually running. If a Secure Global Desktop server is stopped, only the UNIX root user can perform any of the auditable events.

For each of the events, the log filter records:

- the date and time of the event
- the type of event
- the result of the event, whether it was successful or it failed
- the identity of the user responsible for the event and
- any other relevant information about the event, for example what was changed and to what value.

## Viewing audit log information

You can use any of the standard methods for viewing the log output. However, the most useful command to view the log output is:

```
tarantella query audit --format text|csv|xml --filter "filter"
```

If you select the text format, Secure Global Desktop formats the log output so that it is easy to read on screen but it does not show every detail logged. Using the csv format shows every detail logged but it is

only suitable for outputting to a file.

The filter is an [RFC2254](#)-compliant LDAP search filter. The command searches the log fields in the log files for matching entries to display. For auditing purposes, the most useful log fields are:

- log-category
- log-tfn-name
- log-keyword and
- log-event.

For auditing purposes, the log-category is always `*auditinfo`, but this can be any of the standard log filter component/sub-component/severity settings.

The log-tfn-name is the Tarantella Federated Naming (TFN) names associated with the event, for example the TFN name of the application started or the TFN name of the Administrator who changed the configuration of a Secure Global Desktop server.

The log-keyword is an identifier for the auditable events and log-event is the name of the event. The table below shows all the log-keywords along with their corresponding log-event, together with a description of the event.

Log-keyword	Log-event	Description
createFailure	createFailure	A user tried to create an ENS object but failed.
createSuccess	createSuccess	A user created an ENS object.
deleteFailure	deleteFailure	A user tried to delete an ENS object but failed.
deleteSuccess	deleteSuccess	A user deleted an ENS object.
loginFailure	loginResultReconnect	The Secure Global Desktop server requested the client to reconnect on a different port.
loginFailure	loginResultFailed	None of the enabled login authorities authenticated the user.
loginFailure	loginResultRejected	User was denied a login by a login filter. For example, this may be because logins are currently not allowed for that particular server, or because the user is currently not allowed to log in.

loginFailure	loginResultDisabled	The Secure Global Desktop server is not currently accepting connections.
loginFailure	loginResultInvalidWebToken	An invalid web authentication token was presented.
loginFailure	loginResultNoAmbig	An ambiguous login failed because the Secure Global Desktop server does not support ambiguous logins.
loginFailure	loginResultAmbiguous	An ambiguous login failed because the user did not give enough disambiguation information.
loginFailure	loginResultAnonymous	An anonymous login failed because the Secure Global Desktop server does not support anonymous logins.
loginFailure	loginResultNoSecurity	Login failed because the user requires a secure connection, but the connection was made to the standard port.
loginFailure	loginResultUnresolveable	Login failed because the Secure Global Desktop server was unable to resolve which user the login was for.
loginFailure	loginResultUnknown	Login failed because the Secure Global Desktop server was unable to process an unexpected login result.
loginSuccess	webtopSessionStartedDetails	Started a webtop session for a user.
logout	webtopSessionEndedDetails	Stopped a webtop session for a user.
modifyFailure	modifyFailure	A user tried to change an ENS object or the Secure Global Desktop server configuration but failed.
modifySuccess	modifySuccess	A user changed an ENS object or the Secure Global Desktop server configuration.
renameFailure	renameFailure	A user tried to rename an ENS object but failed.
renameSuccess	renameSuccess	A user renamed an ENS object.
serverStart	serverStart	The Secure Global Desktop server was started.
serverStop	serverStop	The Secure Global Desktop server was stopped.

sessionEnded	sessionEndedDetails	Stopped an emulator session for a user.
sessionStarted	sessionStartedDetails	Started emulator session for a user.
sslStart	securitySSLStart	Started Secure Global Desktop security (SSL) services.
sslStop	securitySSLStop	Stopped Secure Global Desktop security (SSL) services.

There are a large number of other log fields which you can use in a filter. For a list of the commonly used ones, see the `tarantella query audit` command.

## Example filters

To search for failed log in attempts:

```
--filter "(&(log-category=*auditinfo)(log-keyword=loginFailure))"
```

To search for changes to made to the Secure Global Desktop server configuration by the Administrator Bill Orange:

```
--filter "(&(log-category=*auditinfo)(log-keyword=modifySuccess)(log-tfn-name=.../ens/o=Indigo Insurance/ou=IT/cn=Bill Orange))"
```

### Related topics

- [Using log filters to troubleshoot problems with the Secure Global Desktop server](#)
- [The tarantella query audit command](#)
- [Array properties \(array-wide\)](#)

## Objects and the organizational hierarchy

### Read this topic to...

- Discover how you can organize your resources in Secure Global Desktop.

Secure Global Desktop is built on the principles of *directory services*:

- People, resources and the structure of your organization are represented by *objects* in a directory.
- Different types of object have different configuration settings, known as *attributes*.
- The *relationships* between objects are important and have meanings.
- Each object is identified using a *unique name*.

### Types of object

Secure Global Desktop includes a number of different object types.

The set of objects available, and the attributes for each object, are collectively called the *schema*. Secure Global Desktop objects are based on the commonly used LDAP v3 schema. We have extended these objects, using the standard method of doing so, to support Secure Global Desktop functionality such as webtops and configurable connection types.

For more information on the LDAP schema, see [RFC 2256](#).

These following objects are available:

- [Organization](#)
- [Organizational unit](#)
- [Group](#)
- [Person](#)
- [Host](#)
- [Character application](#)
- [X application](#)
- [Windows application](#)
- [Document](#)

- Active Directory container
- Domain component
- 3270 application
- 5250 application

Another object type, the *profile object*, helps make managing webtops easier for different types of user. For example, you can define a special webtop for users who log in to Secure Global Desktop *anonymously*.

Finally, *role objects* let you grant certain users special privileges. For example, the Global Administrators role object defines which users are Secure Global Desktop Administrators, who can run the Secure Global Desktop administration tools such as Object Manager.

## Organizing your resources

You use objects to represent the different parts of your organization. Together, the objects form your *organizational hierarchy*.

The top level of the organizational hierarchy contains an object representing your organization. Within that, you create all the objects you need.

You can use *organizational unit (OU)* objects to subdivide your organization. For example, you might want to use an OU for each department in your organization. An OU can contain other OUs, to further subdivide your organization.

It's important to **design your organizational hierarchy**. Here are some tips:

- **Arrange your organizational units to resemble departments.** This way you can take advantage of the *webtop inheritance* of Secure Global Desktop to make managing webtops easy. If everyone in a department needs an application, then add the corresponding application object to the webtop for the organizational unit. By default, everyone belonging to an organizational unit inherits the OU's webtop.
- **Don't nest too much, or too little.** A very "flat" hierarchy makes management of webtops harder -- you can't use webtop inheritance. But a very "deep" hierarchy, with many nested OUs, may introduce other overheads, such as a requirement to move people between OUs much more often. The number of levels you need depends on the size and shape of your organization.
- **Use a naming convention for each object type.**
  - For person objects, we recommend you use the person's full name, for example "Indigo Jones".
  - For application and document objects, the object name is displayed on users' webtops.
- **Use groups.** A *group* is a collection of objects from anywhere in the organizational hierarchy. You

might collect host objects together, for example, to relate all application servers on one site. Objects can be a member of more than one group.

To get started on your organizational hierarchy, [learn about Object Manager](#).

### Related topics

- [Introducing Object Manager](#)
- [What is ENS?](#)
- [What is the Tarantella System Objects organization?](#)



## What is ENS?

ENS, which stands for *Enterprise Naming System*, is the **storage area for all the objects in your Secure Global Desktop organizational hierarchy**.

ENS is arranged in a **directory structure**. At the top are the organization objects. Inside an organization there may be organizational units and other types of object such as person objects, document objects and application objects. Organizational units may themselves contain other objects, including more OUs.

**ENS objects include attributes for Secure Global Desktop-specific behavior.** For example, each person object has a [Webtop Theme](#) attribute that defines the look of the user's Webtop. Also, application objects and host objects combine to let you configure [application server load balancing](#).

**Each object has a unique name within ENS.** The / character in a name separates containers (such as organization objects or organizational unit objects) from their contents. For example, the person object for Indigo Jones, which belongs to the organization object for Indigo Insurance, would have this name:

```
o=Indigo Insurance/cn=Indigo Jones
```

The "o=" ([organization](#)) and "cn=" ([common name](#)) parts of the name identify the attributes whose values distinguish the object from its siblings. In other words, in this example no other objects that belong to the organization object Indigo Insurance have common name Indigo Jones.

**ENS is just one part of the Secure Global Desktop datastore:** one namespace that may be used. To properly name an object, you need to use its [Tarantella Federated Naming \(TFN\) name](#): this includes the namespace. A TFN name is a unique identifier for something in the Secure Global Desktop datastore. The person object for Indigo Jones has this TFN name:

```
.../_ens/o=Indigo Insurance/cn=Indigo Jones
```

Here ... identifies the "root" of TFN, and `_ens` the ENS namespace. Within that namespace, you use the ENS name.

## Why does ENS matter?

ENS is just one namespace, corresponding to the Secure Global Desktop organizational hierarchy.

There are many other namespaces, such as DNS and LDAP. ENS objects define Secure Global Desktop-specific behavior.

The flexibility of Secure Global Desktop allows different namespaces to be used where needed. For example, [login authorities](#) authenticate users in different ways: the ENS login authority searches ENS for matching person objects the LDAP login authority searches the LDAP namespace for matching person objects, and uses an ENS object for Secure Global Desktop-specific behavior.

The integration of these different namespaces is powerful. This makes it important to understand where ENS fits, and what it's used for.

### Related topics

- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)
- [Login authorities](#)

## The Secure Global Desktop datastore and Tarantella Federated Naming

### Read this topic to...

- Understand what Tarantella Federated Naming is and what it's used for.

The Secure Global Desktop datastore is the **sum of all the information used by the various components of Secure Global Desktop**. The datastore includes:

- Information about hosts and users on the network.
- Secure Global Desktop session information.
- Organizational information you provide.

The diverse sources of this information are all accessed in the same way, using TFN (Tarantella Federated Naming) names.

**Each object in the datastore has a unique TFN name.** TFN names include a component identifying the source of the information: the *namespace*. TFN names commonly have this form:

```
.../namespace/name-within-namespace
```

The ... indicates the "root" of TFN. Each namespace may use a different naming scheme. The *namespace* part of the TFN name acts as a "gateway" to that naming scheme.

For example, an object in the **ENS** organizational hierarchy might have this name:

```
.../_ens/o=Indigo Insurance/ou=Marketing/cn=Cust-o-Dat
```

The `_ens` indicates the ENS part of the datastore: the ENS namespace. Within ENS, the object's name is `o=Indigo Insurance/ou=Marketing/cn=Cust-o-Dat`, indicating an object with **common name** Cust-o-Dat, belonging to the organizational unit Marketing, which in turn belongs to the organization Indigo Insurance.

Other namespaces might use a different naming scheme. For example, a similar object stored on an LDAP directory server might have this name:

```
.../_service/sco/tta/ldapcache/cn=Cust-o-Dat,ou=Marketing,o=Indigo  
Insurance
```

Here the order of the hierarchy is reversed, and is comma-separated rather than slash-separated. However, the syntax is different only within the LDAP namespace.

## Why do TFN names matter?

Some command-line tools for configuring Secure Global Desktop require you to name objects to work with. In many cases the flexibility of Secure Global Desktop means you can name objects from many different parts of the datastore.

For example, if you're using `tarantella passcache` to add a new password cache entry, you need to name the resource you're caching the password for. This might be the name of an [ENS host object](#) or a DNS name, for example. In both cases you need to give the name that Secure Global Desktop uses: the TFN name.

## Commonly used namespaces

Namespace	Example	Description
ENS	<code>.../_ens/o=Indigo Insurance/ ou=Marketing/cn=Cust-o-Dat</code>	The <a href="#">ENS</a> namespace, containing objects with Secure Global Desktop-specific behavior.
LDAP	<code>.../_service/sco/tta/ldapcache/ cn=Cust-o-Dat,ou=Marketing,o=Indigo Insurance</code>	Objects in an LDAP directory server.
DNS	<code>.../_dns/verona.indigo-insurance.com</code>	Hosts on the network.

### Related topics

- [The tarantella command](#)
- [What is ENS?](#)



## What is the Tarantella System Objects organization?

The Tarantella System Objects organization contains objects that are essential for smooth running and maintenance of Secure Global Desktop.

For example, Tarantella System Objects contains the Global Administrators [role object](#), which determines who's a Secure Global Desktop Administrator, and application objects for both [Object Manager](#) and [Array Manager](#).

You can edit objects within this organization, but you can't delete, move or rename them, or create new ones.

### Related topics

- [Objects and the organizational hierarchy](#)
- [Organization object](#)

## Naming objects in the organizational hierarchy

In general, when you create an object either in Object Manager or on the command line you can use any characters you want for the name of the object. However, it is best to avoid the backslash ( ) character, the plus (+) character and apostrophes in object names as this can cause problems. If you use a forward slash in an object name, you must backslash protect (escape) it.

On the command line, if the name of an object includes spaces, make sure you enclose the name in quotes, for example ".../\_ens/o=Indigo Insurance".

With the tarantella object command, any name in the ENS namespace is treated as case insensitive. When you create or rename an object, the case used is preserved. However, other tarantella commands, such as the webtopsession and emulatorsession commands, **are** case sensitive.

### Using forward slashes

Secure Global Desktop interprets the forward slash as a part of the organizational hierarchy. For example, if you try to create an object with the relative name `cn=a/b` beneath `o=organization`, Secure Global Desktop will try to create an object called `b` within the `o=organization/cn=a` object. This fails because `o=organization/cn=a` does not exist.

If you must use a forward slash, you must backslash protect (escape) it. For example, to create an object with the relative name `cn=a/b` beneath `o=organization`, type `cn=a\/b`. This will create an object `o=organization/cn=a/b`.

#### Related topics

- [Introducing Object Manager](#)

## What is a role object?

Role objects define **which users occupy particular roles, and what additional links those users see on their webtop**. Role objects are stored in the Secure Global Desktop System Objects organization within the [ENS](#) organizational hierarchy.

**Note** You can't create or delete role objects: there are a fixed number of roles, with predefined privileges.

In Object Manager, choosing Properties for a role object shows two tabs:

- **The Members tab shows all the users who occupy the role:** those users with the privileges granted by the role. Drop person objects or profile objects on this tab to let the appropriate users occupy the role.
- **The Links tab shows the extra webtop links these users have.** Drop objects on this tab to add them to the webtop.

For each object in the Members tab, the tree shown on the object's own Links tab shows the role object, which expands to show the webtop links granted by the role.

From the command line, use `tarantella role` to define which users occupy a role and the extra webtop links they see.

### Related topics

- [Roles in Secure Global Desktop](#)
- [The tarantella role command](#)
- [What is ENS?](#)



## Roles in Secure Global Desktop

Roles are used in Secure Global Desktop to allocate and restrict who can perform certain tasks. Only those users occupying a given role may perform the tasks associated with that role.

Associated with a role are a set of webtop links. These links appear on the webtops of all users occupying that role, in addition to the links those users normally see.

You define who occupies a role, and the extra links they see, using [role objects](#).

### Available roles

There is one role available as standard with Secure Global Desktop: the Global Administrators role.

- Users occupying the Global Administrators role are Secure Global Desktop Administrators, who can configure any part of Secure Global Desktop. They can run both Object Manager and Array Manager, as well as all `tarantella` commands.
- Users without any explicit role have no administration privileges.

#### Related topics

- [The tarantella role command](#)
- [How do I add new Secure Global Desktop Administrators?](#)

## Populating the Secure Global Desktop organizational hierarchy using a batch script

### Problem

You want to populate your organizational hierarchy.

### Solution

Use the batch scripting functionality of the `tarantella object` command to create objects within the organizational hierarchy.

### Alternatives

- Create and manipulate objects in Object Manager. This method is not recommended if you want to populate the organizational hierarchy with a large number of objects.
- Run individual `tarantella object` commands in sequence. This introduces additional processing overhead, and is not recommended.

### Case study

Indigo Insurance needs to create objects -- organizational units (OUs), applications, people and so on -- to reflect the structure of the organization. You want to automate this process.

### Solution

1. Design the structure of your Secure Global Desktop organizational hierarchy, reflecting the structure of Indigo Insurance. Think carefully about how you can use [inheritance](#) to make webtop management more easy.
2. Create a file for each type of object you're using in your organizational hierarchy. Each file contains one line per object, with the correct syntax for creating the object from the appropriate `tarantella object new_object_type` command. For example, with five organizational units you might have a file `orgunits.txt` containing the following:

```
--name ".../_ens/o=Indigo Insurance/ou=IT"
--name ".../_ens/o=Indigo Insurance/ou=Sales" \
  --webtop indigo/sales/standard
```

```
--name ".../_ens/o=Indigo Insurance/ou=Marketing" \  
  --webtop indigo/marketing/standard  
--name ".../_ens/o=Indigo Insurance/ou=Finance" \  
  --webtop indigo/finance/standard \  
  --conntype '*:*:SSL'  
--name ".../_ens/o=Indigo Insurance/ou=Finance/ou=Administration"
```

You must use the full [TFN name](#) for each object. **Do not** include the command name (for example, `object new_windowsapp`) as part of each line.

3. Once all your files are complete, use the `tarantella object script` command to process them all at once, for example like this:

```
#!/bin/sh  
  
tarantella object script << EOF  
new_orgunit --file orgunits.txt  
new_group --file groups.txt  
new_host --file hosts.txt  
new_person --file people.txt  
new_xapp --file xapps.txt  
new_windowsapp --file windowsapps.txt  
new_charapp --file charapps.txt  
EOF
```

`tarantella object script` runs each command in order, which reads and processes the appropriate file.

## Next steps

- You can use any `tarantella object` subcommand with `tarantella object script`, and you don't have to read in object details from other files. For example, you can customize webtops from a batch script by including `add_link` and `remove_link` lines.
- Many other commands, for example `tarantella passcache`, accept `--file` arguments, so you can perform multiple related actions at once.

## Related topics

- [The tarantella object command](#)
- [The tarantella object script command](#)



[Secure Global Desktop Administration Guide](#) > [Organizing your resources](#) > All Administrators have been removed and no-one can use the administration tools

## All Administrators have been removed and no-one can use the administration tools

If all Secure Global Desktop Administrators have been removed, no-one can use Array Manager, Object Manager or the command-line tools.

If there are no Secure Global Desktop Administrators defined (no users have the Global Administrators role) then the user with [TFN name](#) `.../_user/root` (corresponding to the UNIX root user) is given administration privileges and they can create new Administrators. To do this:

1. Log in as root on the host where Secure Global Desktop is installed.
2. Stop the Secure Global Desktop server by running `tarantella stop`.
3. Start Object Manager by running `tarantella objectmanager`.
4. Either create a new user or use an existing user and [add them as a Secure Global Desktop Administrator](#).
5. Make sure the new Administrator is someone who can be authenticated against the login authorities you are using.
6. Exit Object Manager.
7. Restart the Secure Global Desktop server by running `tarantella start`.

The new Administrator can now use the Secure Global Desktop administration tools.

### Related topics

- [Roles in Secure Global Desktop](#)

## Creating and publishing an application object to users

### Problem

You've installed a new application and want to publish it to users on their webtops.

### Solution

In [Object Manager](#), create an application object of the correct type, and add it to users' webtops by dragging it onto their [Links](#) tabs. Drag it to the Links tab of an organizational unit object or an organization object, or the Members tab of a group object, to add it to the webtops of users who inherit content from that object.

**Note** The application will appear on users' webtops after a few moments. If you are using the classic webtop, users have to log out and log in again to see the application on their webtop.

### Alternatives

- Use the `tarantella object` command to create the object and publish it to users from the command line.

### Case study

Indigo Insurance has a new X application, XClaim. The application must appear on the webtops of everyone in the Finance department, as well as the webtop of the President, Indigo Jones. The application is installed on london.indigo-insurance.com, geneva.indigo-insurance.com and prague.indigo-insurance.com, and users must be load-balanced across those application servers.

### Solution

1. Log in to a Secure Global Desktop server as a [Secure Global Desktop Administrator](#). Only Secure Global Desktop Administrators can create objects and publish applications.
2. On your webtop, click Object Manager. If you've used Object Manager before, it appears just how you left it.
3. The new application "belongs to" the Finance department, so the application object should belong in the Finance organizational unit. Use the Search or Browse tabs to locate the Finance OU object. Right-click this object, point to New, and then click X Application.

4. Object Manager opens the Finance OU on the Browse tab, and displays a text box. Type the name of the object in the box, for example XClaim, and press Return. This name is used to uniquely identify the object within the OU, and is also shown on a user's webtop.
5. Properties for the new object appear on the right. On the Attributes tab, choose General from the list. These are the attributes you're most likely to want to change. You can get help on any attribute by clicking the context help button, in the lower-right corner of Object Manager, and then clicking the attribute.
6. For [Application Command](#), type the full pathname of the program on the application servers that may run it (the path must be the same on all of them), for example `/usr/local/bin/xclaim`. You don't put command-line arguments here -- use the [Arguments For Command](#) attribute for those.
7. You should set [Width](#) and [Height](#) to the application size, in pixels. Alternatively you could set [Display Using](#) to Client Window Management: this makes the application look like it's running on the client device.
8. If you like, scroll down the list of attributes, and choose different attribute groupings from the list, to see what other settings you can change. When you've finished changing attributes, click Apply.
9. To define the application servers that can run the application, use the [Hosts](#) tab of the application object. Drag host objects representing the application servers onto the tab: Secure Global Desktop will load-balance users across these application servers. For example, you would add host objects for london.indigo-insurance.com, geneva.indigo-insurance.com and prague.indigo-insurance.com to the Hosts tab to load-balance across these hosts.
10. To add the application to the webtops of everyone in the Finance department, choose Properties for the Finance OU object, and then click the [Links](#) tab. Then simply drag the application object onto the tab. Everyone in the OU sees the new application on their webtop the next time they log in, as long as their person object is configured to [inherit webtop content from their parent](#) (they are by default).
11. To add the application to Indigo Jones's webtop, use the Search or Browse tabs to locate his person object, choose Properties, click the Links tab, and then drag the application onto the tab.

## Next steps

- If you want to add an application to the webtops of all users of a particular type, such as UNIX users or anonymous users, use the Links tab of the appropriate [profile object](#).
- If you want to create multiple objects, or to modify many users' webtops at the same time, use the `tarantella object` command's [batch processing](#) capabilities.

## Related topics

- Introducing Sun Secure Global Desktop Software
- Introducing Object Manager
- Creating and configuring a person object
- Objects and the organizational hierarchy
- Introducing application server load balancing



## Creating and configuring a person object

### Problem

You want to create and configure a new person object for someone in your organization.

### Solution

In [Object Manager](#), create a person object in the appropriate place in the organizational hierarchy, setting the attributes (**especially the Username attribute**) appropriately. Then use the Links tab to add any webtop content for this person.

### Alternatives

- Use the `tarantella object` command to create and configure the object from the command line.
- You can allow [anonymous access](#) -- logging in to Secure Global Desktop without a username or password -- without creating a person object.
- You can allow access by [UNIX users](#) without creating a person object.
- Integrate with an existing LDAP directory server on your network containing the people in your organization.

### Case study

Indigo Insurance has a new recruit, Ginger Butcher. Ginger joins the IT department, and will be a Secure Global Desktop Administrator. She has special responsibility for training, and needs to use the presentation tool Slide-o-Win regularly. You need to create and configure a person object for Ginger.

### Solution

1. Log in to a Secure Global Desktop server as a [Secure Global Desktop Administrator](#). Only Secure Global Desktop Administrators can create person objects.
2. On your webtop, click Object Manager. If you've used Object Manager before, it appears just how you left it.
3. The new recruit "belongs to" the IT department, so the person object should belong in the IT organizational unit. Use the Search or Browse tabs to locate the IT OU object. Right-click this object, point to New, and then click Person.
4. Object Manager opens the IT OU on the Browse tab, and displays a text box. Type the name of

the person in the box, in this case `Ginger Butcher`, and press Return. This name is used to uniquely identify the object within the OU.

5. Properties for the new object appear on the right. On the Attributes tab, choose General from the list. These are the attributes you're most likely to want to change. You can get help on any attribute by clicking the context help button, in the lower-right corner of Object Manager, and then clicking the attribute.
6. For **Surname**, type the person's family name, in this case `Butcher`.
7. For **Username**, type the UNIX username of the person, in this case `ginger`. This attribute may be used for authentication: see [user types](#) for more information.
8. For **Email Address**, type the person's full email address, in this case `ginger@indigo-insurance.com`.
9. If you want Ginger's webtop to include everything that's on the webtop of the IT organizational unit, make sure that **Inherit Parent's Webtop Content** is checked.
10. As this person object is for Ginger only and isn't shared between multiple users, make sure that **Shared Between Users (Guest)** is not checked.
11. To let Ginger log in to Secure Global Desktop, make sure that **May Log In To Secure Global Desktop** is checked.
12. If you like, choose different attribute groupings from the list, to see what other settings you can change. When you've finished changing attributes, click Apply.
13. To define the webtop content that applies only for Ginger Butcher, use the **Links** tab of the person object. Use the Search or Browse tabs to locate application objects you want to add to the webtop (they don't have to be in the same OU as the person object), and just drag them onto the tab. You can also drag group objects onto the tab: Secure Global Desktop shows all the members of the group on Ginger's webtop.
14. Ginger Butcher needs to be a Secure Global Desktop Administrator. On the Browse tab, open the Secure Global Desktop System Objects organization, and then double-click Global Administrators. Drag the person object for Ginger Butcher to the Members tab to make Ginger a Secure Global Desktop Administrator.

## Next steps

- If you want to create multiple objects, or to modify many users' webtops at the same time, use the `tarantella object` command's [batch processing](#) capabilities.

## Related topics

- Introducing Object Manager
- Creating and publishing an application object to users
- Objects and the organizational hierarchy
- Introducing Sun Secure Global Desktop Software

## Mirroring your LDAP organization in ENS

If you have configured Secure Global Desktop to authenticate users with either the LDAP login authority, the Active Directory login authority or web server/third party authentication (using the LDAP search methods), all users have the same webtop content (defined by the default LDAP profile object `o=Tarantella System Objects/cn=LDAP Profile`) and have the same Secure Global Desktop-specific settings.

In order to customize webtop content and/or Secure Global Desktop-specific settings, you have to mirror some of your LDAP organization in ENS by creating the person objects that will be used as login profiles. These login profiles can then be used to control the following:

- Webtop content.
- Access to standard or secure connections to Secure Global Desktop.
- Access to client drives on Microsoft Windows client devices.
- Access to printers on Microsoft Windows client devices.
- Access to serial ports.

**Note** [Directory Services Integration](#) offers a more efficient and flexible way of customizing webtop content.

For details of how the login profiles are determined, see the [LDAP login authority](#), the [Active Directory login authority](#) or [web server/third party authentication](#).

When you create person objects as login profiles:

- You don't need to mirror your entire LDAP organization in ENS, only as much of the structure as you need.
- Inherit as much as possible from other objects in the organizational hierarchy.
- Only create person objects for individual users if you really have to.

### Example

- Indigo Insurance has five departments: IT, Sales, Marketing, Finance, and Administration
- It has a flat organizational hierarchy.
- The Finance and Marketing departments need different webtop content to the other departments.

- Sid Cerise in the Finance department also wants access to the Cust-o-dat application but no-one else in Finance is allowed to access it.

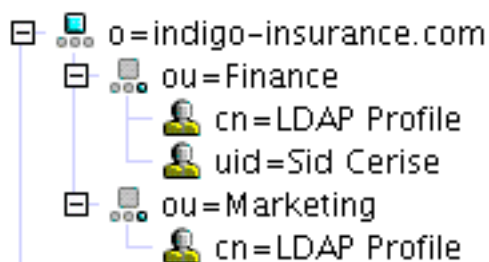
The objects you create, depend on the type of LDAP directory being used.

## Sun ONE Directory Server

If you are using Sun™ ONE Directory Server, the LDAP names are:

- `ou=IT,o=indigo-insurance.com` for IT
- `ou=Sales,o=indigo-insurance.com` for Sales
- `ou=Finance,o=indigo-insurance.com` for Finance
- `ou=Marketing,o=indigo-insurance.com` for Marketing
- `uid=Sid Cerise,ou=Finance,o=indigo-insurance.com` for Sid Cerise

To give users the webtops they need, you could create the following objects in the organizational hierarchy:



**Note** You **must** create the person object using a `uid=` prefix. Use BACKSPACE to delete the Secure Global Desktop default `cn=` prefix for person objects and then type `uid=`. You can only do this when you create the object. Once the object has been created, you cannot amend the `cn=` part of the name.

With this organizational hierarchy:

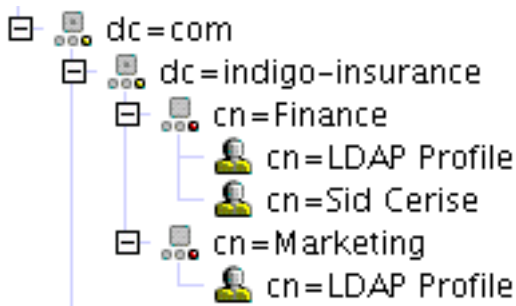
- Sid Cerise receives the webtop defined for his person object. He also **inherits webtop content** and other settings from parent OU objects in the organizational hierarchy.
- Users in the Finance and Marketing departments receive the webtop defined for the Finance and Marketing `cn=LDAP Profile` objects. They also **inherit webtop content** and other settings from parent OU objects in the organizational hierarchy.
- All other users receive the webtop and other settings defined for the `o=tarantella System Objects/cn=LDAP Profile` object.

## Microsoft Active Directory

If you are using Microsoft Active Directory, the LDAP names are:

- `cn=IT,dc=indigo-insurance,dc=com` for IT
- `cn=Sales,dc=indigo-insurance,dc=com` for Sales
- `cn=Finance,dc=indigo-insurance,dc=com` for Finance
- `cn=Marketing,dc=indigo-insurance,dc=com` for Marketing
- `cn=Sid Cerise,cn=Finance,dc=indigo-insurance,dc=com` for Sid Cerise

To give users the webtops they need, you could create the following objects in the organizational hierarchy:



**Note** You **must** use domain component and Active Directory container objects to mirror your LDAP organization.

With this organizational hierarchy:

- Sid Cerise receives the webtop and other settings defined for his person object.
- Users in the Finance and Marketing departments receive the webtop and other settings defined for the Finance and Marketing `cn=LDAP Profile` objects.
- All other users receive the webtop and other settings defined for the `o=tarantella System Objects/cn=LDAP Profile` object.

**Note** It is not possible to inherit webtop content or other settings from domain component and Active Directory container objects.

## Related topics

- The LDAP login authority
- The Active Directory login authority
- Web server/third party authentication
- Using Directory Services Integration
- Can I deny an LDAP user access to Secure Global Desktop?

## Using Directory Services Integration

### Overview

Secure Global Desktop Directory Services Integration (DSI) allows you to use an LDAP version 3 directory instead of ENS for holding user information. With DSI, you do not need any ENS person objects. You can still have ENS person objects if you want, for example for Secure Global Desktop Administrators, but using DSI means you don't need to [mirror your LDAP organization in ENS](#).

When you use DSI, you configure application objects (or group objects) instead of person objects, so that it is an application that defines which LDAP users see it on their webtop.

You can only use DSI for users who have their identity established by an LDAP directory server. In other words, the user must have been authenticated using either:

- the [LDAP login authority](#) or
- the [Active Directory login authority](#) or
- [web server/third party authentication](#) using one of the LDAP identity mapping search methods.

The login profile used depends on which of these methods was used to authenticate the user. However, if you don't mirror your LDAP organization in ENS the default LDAP Profile object (`o=Tarantella System Objects/cn=LDAP Profile`) is used.

If you use DSI, webtop content is aggregated, that is a user can receive applications based on:

- the [links tab](#) of their login profile **plus**
- the application/group objects that specify the user.

### Requirements

Currently DSI is only supported on:

- Sun™ ONE (formerly Netscape or iPlanet) version 4.1+ directory servers.
- Microsoft Active Directory servers.

**Note** It may work on other LDAP directory servers, but it isn't supported.



## Enabling Directory Services Integration

To enable DSI:

1. Enable one of the login authorities that gives users an LDAP identity and test that it works.
2. Configure the login profiles in ENS. If you want more control over settings such as security and printing, you may want to configure person objects as well as the `o=Tarantella System Objects/cn=LDAP Profile` object.
3. Configure the application/document objects and/or group objects to define which LDAP users see each application or group of applications on their webtop.

## Configuring applications for Directory Services Integration

In Object Manager all application, document and group objects have a Directory Services Integration panel. You use the attributes on this panel to configure which LDAP users see an application or document. For group objects, the configuration applies to all applications and documents that are members of the group. The attributes on the Directory Services Integration panel are:

- LDAP Users (`--ldapusers`)
- LDAP Groups (`--ldapgroups`)
- LDAP Searches (`--ldapsearch`)

### The LDAP Users attribute

The LDAP users attribute is a list of Distinguished Names (DNs) of the individual users in the LDAP directory that should see the application on their webtop.

For example, to give Sid Cerise in the Finance department access to the `Cust-o-dat` application, you could:

1. Edit the `Cust-o-dat` application object in Object Manager.
2. Click the Directory Services Integration panel.
3. In the LDAP Users box, type:  
`uid=Sid Cerise,ou=Finance,o=indigo-insurance.com`

**Note** If you assign several individual users to an application or group object, it is more efficient to use the LDAP Search attribute instead.

### The LDAP Groups attribute

The LDAP Groups attribute is a list of DN's of the groups in the LDAP directory that should see the

application on their webtop. All members of the LDAP group receive the application.

For example, to give a set of applications to managers in the Finance and Marketing departments, you could:

1. Create a group object in Object Manager.
2. Click the Links tab for the group.
3. Drop application and document objects onto the Links tab.
4. Click the Directory Services Integration panel.
5. In the LDAP Groups box, type:  
`cn=managers,ou=Finance,o=indigo-insurance.com cn=managers,ou=Marketing,  
o=indigo-insurance.com`

**Note** If you assign several groups to an application or group object, it is more efficient to use the LDAP Search attribute instead.

### The LDAP Searches attribute

The LDAP Searches attribute is a list of [RFC 2254 search filters](#) and/or [RFC 1959 LDAP URLs](#) for specifying which users that should see the application on their webtop.

For example, to give an application to all managers in the Sales department and anyone who has Violet Carson as their manager, you could:

1. Edit the application object in Object Manager.
2. Click the Directory Services Integration panel.
3. In the LDAP Searches box, type:  
`"(&(job=manager)(dept=Sales))" "(manager=Violet Carson)"`

**Note** You can also use an LDAP search URL for the LDAP Search attribute, for example:  
`"ldap:///ou=Sales,dc=indigo-insurance,dc=com??sub?job=manager"`.

### Performance effects of using Directory Services Integration

Using Directory Services Integration requires many round-trips to an LDAP directory server. This can generate a lot of network traffic and degrade performance.

We recommend you use the LDAP Search attribute wherever possible as this is more efficient and flexible. Use the LDAP Users and LDAP Groups attributes very sparingly.

### Refining LDAP Group searches

## Group membership

When Secure Global Desktop searches for members of LDAP groups it searches for users in the `uniquemember`, `member`, and `uniqueMember` attributes on group objects.

If these attributes do not provide enough information to allow Secure Global Desktop to uniquely identify users, for example because the attribute contains only the user's relative distinguished name (RDN), then the group search will fail.

Secure Global Desktop allows you to specify one or more short name attributes which can be used to identify users. Secure Global Desktop considers a user to be a member of a group if the value of their short name attribute also appears in one of the group membership attributes (`uniquemember`, `member`, and `uniqueMember`) for the group. For short name attributes to work, they must contain unique values.

To specify one or more short name attributes:

1. Stop the Secure Global Desktop server: `tarantella stop`.
2. Run the following command:  

```
tarantella config edit \  
--com.sco.jndi.toolkit.utils.LDAPUserCollection.properties-  
userShortAttributes-append attribute
```

You can list more than one attribute. Each attribute must be separated by a space.
3. Start the Secure Global Desktop server: `tarantella start`.
4. Repeat these steps on each member of the array.

To specify additional attributes as group membership attributes:

1. Stop the Secure Global Desktop server: `tarantella stop`.
2. Run the following command:  

```
tarantella config edit \  
--com.sco.jndi.toolkit.utils.LDAPUserCollection.properties-  
directAttributes-append attribute
```

You can list more than one attribute. Each attribute must be separated by a space.
3. Start the Secure Global Desktop server: `tarantella start`.
4. Repeat these steps on each member of the array.

## Nested groups (sub-groups)

By default the LDAP group search searches a single depth of LDAP groups. If your organization uses nested groups (sub-groups), you can increase the depth of the search. To do this:

1. Stop the Secure Global Desktop server: `tarantella stop`.
2. Run the following command:  

```
tarantella config edit \  
--com.sco.jndi.toolkit.utils.LDAPUserCollection.properties-  
maximumGroupDepth depth
```
3. Start the Secure Global Desktop server: `tarantella start`.
4. Repeat these steps on each member of the array.

The default depth is "0" and you should increase the value to match the depth of the nested groups. Increasing the depth will have a negative effect on performance.

## LDAP cache

Secure Global Desktop caches the data it collects from an LDAP directory server. If you find that Secure Global Desktop is not detecting changes, you can manually flush the cached data with the [tarantella cache](#) command.

### Related topics

- [Mirroring your LDAP organization in ENS](#)
- [The LDAP login authority](#)
- [The Active Directory login authority](#)
- [Web server/third party authentication](#)

## Do I need to license Windows Terminal Services?

Yes. If you access terminal server functionality provided by Microsoft operating system products, you need to purchase additional licenses to use such products. Consult the license agreements for the Microsoft operating system products you are using to determine which licenses you must acquire.

Currently, information regarding Terminal Services can be found in:

- [Licensing Terminal Server in Windows Server 2003.](#)
- [Microsoft Windows 2000 Terminal Services Licensing.](#)

### Related topics

- [Licensing and Sun Secure Global Desktop Software](#)

## Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop

To use Microsoft Windows Terminal Services with Secure Global Desktop you may have to configure:

- [Authentication settings](#)
- [Session resumability](#)
- [Windows printer mapping](#)
- [Windows Server 2003 FIPS encryption level](#)
- [Windows Server 2003 session restrictions](#)
- [Windows Server 2003 remote desktop users](#)
- [Windows Server 2003 time zone redirection](#)
- [Windows Server 2003 audio redirection](#)
- [Windows Server 2003 smart card device redirection](#)
- [Windows Server 2003 COM port mapping](#)

**Note** For detailed information on configuring Terminal Services, see the Microsoft sites for [Windows 2000 Server](#) and [Windows Server 2003](#).

### Authentication settings

By default, Windows 2000 Server always prompts for a password when users log in, whether or not Secure Global Desktop supplies the password for the application server from its password cache. By default, Windows Server 2003 does not prompt for passwords.

To configure a Windows Server to stop prompting for passwords for Secure Global Desktop users:

1. In Terminal Services Configuration, click Connections.
2. Double-click RDP-Tcp.
3. Click the Logon Settings tab.
4. Clear the Always Prompt for Password box.

Changes to this setting only apply to new Windows Terminal Server sessions.

### Session resumability

Windows Terminal Services allow users' sessions to continue running following a connection loss. We recommend that you disable this feature on the Windows Server, and let Secure Global Desktop handle [session resumability](#). This prevents unnecessary use of resources on the application server, and ensures that if users share accounts on the application server, they do not resume each other's Windows sessions.

For example, with session resumability enabled on Windows, an application configured in Secure Global Desktop to be [Webtop session resumable](#) **does not** end when the user logs out of Secure Global Desktop. Windows preserves the session so that it may be resumed later.

Resources may be consumed unnecessarily on more than one application server if the application is configured to run on [multiple application servers](#).

To illustrate how shared accounts may lead to "stolen" sessions, consider this example. The Windows resume mechanism is enabled on the application server rome. Secure Global Desktop user Bill Orange starts the Write-o-Win application on rome with the Windows username "guest". Bill then logs out of Secure Global Desktop without closing Write-o-Win. Secure Global Desktop user Rusty Spanner then starts Write-o-Win as "guest" on the same application server. Rusty resumes the copy of Write-o-Win running in Bill's Windows session because of the Windows resume mechanism.

To configure a Windows Server to allow Secure Global Desktop to handle session resumability:

1. In Terminal Services Configuration, click Connections.
2. Double-click RDP-Tcp.
3. Click the Sessions tab.
4. For the When Session Limit Is Reached Or Connection Is Broken option, choose End Session. (If necessary, clear the Override User Settings box to do this.)

Changes to these settings only apply to new Windows Terminal Server sessions.

## Windows printer mapping

To support printing to client printers from a Windows Terminal Server session, Windows printer mapping must be enabled (it is by default). Follow these steps if it has been disabled:

1. In Terminal Services Configuration, click Connections.
2. Double-click RDP-Tcp.
3. Click the Client Settings tab.
4. Clear the Windows printer mapping box.

Changes to these settings only apply to new Windows Terminal Server sessions.

## **Windows Server 2003 FIPS encryption level**

Secure Global Desktop does not support the Federal Information Processing Standards (FIPS) encryption level, available on Windows Server 2003.

If you have enabled FIPS encryption, you must change it as follows:

1. In Terminal Services Configuration, click Connections.
2. Double-click RDP-Tcp.
3. Click the General tab.
4. In the Encryption Level list, choose an encryption level.

Changes to these settings only apply to new Windows Terminal Server sessions.

## **Windows Server 2003 session restrictions**

By default, Windows Server 2003 only allows users one Terminal Services session each. If a user starts another desktop session or another instance of an application (with the same arguments), the second Terminal Services session "grabs" the first session and disconnects it. This means from the webtop it is not possible to launch two desktops or two instances of the same application on the same Windows Server 2003.

To change this behavior:

1. In Terminal Services Configuration, click Server Settings.
2. Double-click Restrict each user to one session.
3. Clear the Restrict each user to one session box.

Changes to this setting only apply to new Windows Terminal Server sessions.

## **Windows Server 2003 remote desktop users**

For Windows Server 2003, users can only use Terminal Services if they are members of the Remote Desktop Users group.

## **Windows 2003 time zone redirection**

Windows Server 2003 allows client computers to redirect their time zone settings to the Terminal Server so that users see the correct time for their time zone in their desktop/application sessions. Terminal Services uses the server base time on the Terminal Server and the client time zone information to calculate the time in the session. This feature may be useful if you have clients in different time zones.



By default, this feature is disabled. To enable the feature on a Windows 2003 Server:

1. Either:
  - start the Microsoft Group Policy Management Console or
  - start an empty Microsoft Management Console and add the Group Policy Object Editor snap-in.
2. Select the group policy object you want to edit.
3. Click Computer configuration, Administrative Templates, Windows Components, Terminal Services, Client/Server Data Redirection.
4. Open Allow Time Zone Redirection.
5. Click Enabled.
6. Click OK.

Changes to this setting only apply to new Windows Terminal Server sessions.

## **Windows Server 2003 audio redirection**

Windows Server 2003 can redirect sound to a Windows Terminal Server session. By default, this feature is disabled. To enable the feature:

1. In Terminal Services Configuration, click Connections.
2. Double-click RDP-Tcp.
3. Click the Client Settings tab.
4. Clear the Audio mapping box.

Changes to this setting only apply to new Windows Terminal Server sessions.

## **Windows Server 2003 smart card device redirection**

Windows Server 2003 can redirect smart card devices to a Windows Terminal Server session. This is enabled by default. Follow these steps if it has been disabled:

1. Either:
  - start the Microsoft Group Policy Management Console or
  - start an empty Microsoft Management Console and add the Group Policy Object Editor snap-in.
2. Select the group policy object you want to edit.
3. Click Computer configuration, Administrative Templates, Windows Components, Terminal Services, Client/Server Data Redirection.
4. Double-click the Do not allow smart card device redirection setting.

5. Click enabled.

Changes to this setting only apply to new Windows Terminal Server sessions.

## Windows Server 2003 COM port mapping

Windows Server 2003 allows users to access the serial ports on the client device from a Windows Terminal Server session. By default, this feature is disabled. To enable the feature:

1. In Terminal Services Configuration, click Connections.
2. Double-click RDP-Tcp.
3. Click the Client Settings tab.
4. Clear the COM port mapping box.

Changes to this setting only apply to new Windows Terminal Server sessions.

### Related topics

- [Windows Protocol \(--winproto\)](#)
- [Do I need to license Windows Terminal Services?](#)

## Running Windows applications on client devices

To let users click a webtop link to run a Windows application on their client device (rather than display it through Secure Global Desktop), make sure the [Try Running From Client First](#) box is checked for the application object.

If you have problems, check the following:

- Make sure the application is installed in the correct location on the client device.
- For web browser users, make sure the web browser supports and uses the signed [Java™ archive](#) supplied with Secure Global Desktop. (Some browsers may be configured to disable support for Java archives. You should reconfigure these browsers to allow users to run applications locally.)

### Related topics

- [Introducing Object Manager](#)

## How do I enable sound in Windows applications?

To enable sound in Windows applications:

1. [Configure audio redirection on the Windows 2003 Server](#).
2. Enable the Secure Global Desktop audio service on the [Array properties](#) panel in Array Manager.

### Notes

- You can only play sound in Windows 2003 Terminal Services sessions.
- Users must log out of Secure Global Desktop and log back in again to enable sound in their current Windows Terminal Server sessions.
- Only the following clients can play sound:
  - the Sun Secure Global Desktop Client running on Windows 2000/XP Professional, Linux, Solaris Sunrays or Mac OS X
  - the Native Client for Linux
  - the Native Client for UNIX running on Solaris
  - the Native Client for Mac OS X.

### Related topics

- [Troubleshooting sound in Windows applications](#)
- [Audio Protocol Engine properties \(server-specific\)](#)

## Using smart cards with Windows applications

Secure Global Desktop allows users to access a smart card reader attached to their client device from applications running on a Windows Server 2003 application server. Users can:

- Log on to a Windows Server 2003 server using a smart card.
- Access the data on a smart card while using an application running on a Windows 2003 Server, for example, to use a certificate for signing or encrypting an e-mail.

**Note** Windows 2000 Server application servers do not support smart card device redirection.

## Supported clients

The following clients support smart cards:

- the Sun Secure Global Desktop Client (the browser-based webtop) on the supported Windows, Linux and Solaris client platforms
- the Native Client for Unix/Linux (the classic webtop) on the supported Linux and Solaris client platforms
- the Native Client for Microsoft Windows (the classic webtop) on the supported Windows client platforms

## Enabling support for smart cards

To enable support for smart cards:

1. Deploy smart cards on the Windows Server 2003 domain.
  - See the [Smart card deployment checklist](#) for the main configuration steps.
  - Check that [smart card device redirection](#) is enabled for Terminal Services on the Windows Server 2003 (it is by default).
  - Ensure that smart cards are working before introducing Secure Global Desktop.
2. Configure the smart card readers on client devices.
3. On the [Array properties](#) panel in Array Manager check that the Secure Global Desktop smart card service is enabled (it is by default).
4. Ensure that the Windows applications that require smart cards use Microsoft RDP as the [Windows Protocol \(--winproto\)](#).

5. On the [Application Launch properties](#) panel in Array Manager, check that the Allow smart card authentication box is checked (it is by default) and, if required, change the settings for the Always use smart card box.

## Application server authentication dialog settings

The [Application Launch properties](#) panel in Array Manager has several attribute which control the behavior of the application server authentication dialog when using the Secure Global Desktop smart card service.

The **Allow smart card authentication** box controls whether users get the choice of logging in with a smart card or only with a username and password.

The **Always use smart card Box** attributes allow you to control whether a user's decision to log in with a smart card is remembered (cached) for the next time they log in to that application server and whether they can change this setting. If the box is checked (by the user or by the system), the decision is cached in the application server password cache.

**Note** Being able to choose an authentication method and/or to cache the smart card decision depends on users having access to the application server authentication dialog. If you [disable users ability to use SHIFT + click](#), this restricts users' access to this dialog.

## Configuring smart card readers on client devices

Secure Global Desktop works with Personal Computer/Smart Card (PC/SC)-compliant cards and readers, see the [PC/SC Workgroup](#) for details.

### Windows clients

On Windows client devices, once the reader (and any required drivers) have been installed on the client, the smart card should be available to Terminal Services sessions running through Secure Global Desktop.

### Linux and Solaris clients

On Linux and Solaris clients, a PCSC-Lite library must be installed in order for Secure Global Desktop to communicate with smart card readers. PCSC-Lite provides an interface to the PC/SC framework on UNIX/Linux.

For **Linux** clients, PCSC-Lite is available from:

- your Linux vendor, for example, for Fedora you can download the package from [the Fedora extras](#)

site

- the MUSCLE project, <http://www.musclecard.com>

PCSC-Lite version 1.2.0 or later is required.

For **Solaris** clients, PCSC-Lite compatible libraries are available in:

- the PC/SC Shim for SCF package
- the Sun Ray PC/SC Bypass package

The PC/SC Shim for SCF package (PCSCshim) allows you to use a PC/SC application with the Solaris Card Framework (SCF) and should work with Sun internal readers and Sun Ray readers. Version 1.1.1 or later is required. The PC/SC Shim is included with Solaris 10. For other Solaris versions, the Shim is available from the MUSCLE project (<http://www.musclecard.com>).

The Sun Ray PC/SC Bypass package (SUNWsrcbp) provides a PCSC-Lite interface for the Sun Ray reader. Make sure you have the latest patches for Sun Ray Server Software and the latest SUNWsrcbp package.

Secure Global Desktop clients require the PCSC-Lite `libpcsclite.so` library file. This is normally installed in `/usr/lib` but it depends on your dynamic linker path. If this file is installed outside of the dynamic linker path or you want to use a different library file, use the `TTA_LIB_PCSCCLITE` environment variable to specify the location. This can be set either in the user's environment or in the login script.

## Logging in to Windows Server 2003 with a smart card

1. Log in to Secure Global Desktop.
2. On the webtop, click the link to start the Windows application/desktop.
3. When the application server authentication dialog displays, click Use smart card.
4. To always use a smart card to log in, click the Always use smart card box.
5. When the Windows security dialog displays, insert your smart card.
6. When prompted enter your PIN.

### Related topics

- Array properties (array-wide)
- Smart Card Protocol Engine properties
- Users are unable to use smart cards with Windows applications
- Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop



## Using seamless windows for Windows applications

With seamless windows, the Windows application server manages the display of the application. This means an application's windows behave in the same way as an application running on a Windows application server, regardless of the user's desktop environment. The window can be resized, stacked, maximized and minimized. The Windows Start Menu and Taskbar do not display.

**Note** seamless windows are not suitable for displaying Windows desktop sessions: use a kiosk or independent window instead.

To use seamless windows:

- The application server must be a Windows 2000/2003 application server.
- The Sun Secure Global Desktop Enhancement Module for Windows must be installed on the application server.
- The Windows application object must be configured to:
  - use Microsoft RDP as the [Windows protocol](#) and
  - [Display Using \(--displayusing\)](#) a seamless window.
- The user must use a client that supports seamless windows.

If any of the above conditions are not met, the Windows application displays in an independent window instead.

You can only use seamless windows with the browser-based webtop.

### Notes

- If an application is launched in a seamless window, you can toggle between a seamless and independent window by pressing the SCROLL LOCK key.
- Applications that have non-rectangular windows, for example a media player with a customized skin, display in a rectangular window.
- On Windows client devices, seamless windows are not affected by the Cascade, Tile Windows Horizontally, or Tile Windows Vertically window commands.
- If a screen saver or the Windows Security dialog displays, the window automatically switches to an independent window. Unlocking the application automatically restores the window to a seamless window.

- If a seamless window application is resumed on a display that is a different size (larger or smaller) to the original session, the application is displayed in an independent window.
- Each application displaying in a seamless window has its own RDP connection.

## Gnome 2.0.0 Desktop issue

Applications configured to display in seamless windows may not display correctly when accessed from a Gnome 2.0.0 Desktop. This is caused by an unpatched version of the Metacity Window Manager. The solution is to install the Gnome 2.0.0 Window Manager patch. Patch ID: 115780-03. Available from the SunSolve web site (<http://sunsolve.sun.com>)

### Related topics

- [Display Using \(--displayusing\)](#)
- [Windows application object](#)

## Configuring access to serial ports

To give users access to client serial port devices from Windows applications running through Secure Global Desktop:

1. [Configure the Windows application for COM port mapping.](#)
2. [Give users access to serial ports.](#)
3. [Configure the serial ports to be mapped.](#)

### Configuring the Windows application for COM port mapping

Users can only access serial ports from a Windows application if:

- The application is running on a Microsoft Windows Server 2003 application server.
- [COM port mapping](#) has been enabled on the application server (it is disabled by default).
- The Windows application is configured to use the Microsoft RDP [Windows Protocol](#).

### Giving users access to serial ports

On the [Array Properties](#) panel of Array Manager, access to serial ports for the array as a whole can be enabled or disabled. By default, access to serial ports is enabled.

In Object Manager, you enable or disable access to serial ports for individual users using the [Serial Port Mapping](#) attribute for organization, organizational unit or person objects. Access to serial ports can be inherited (the Use parent setting) from parent objects in the organizational hierarchy. This allows you to enable or disable access to serial ports for many users without having to edit each person object.

When a user starts a Windows application, Secure Global Desktop checks the person object for the user and then any parent object further up the organizational hierarchy to see whether access to serial ports is enabled or disabled. If all the objects checked are configured to use the parent's setting, then the array-wide default setting is used.

### Configuring the serial ports to be mapped

If a users has permission to access serial ports, Secure Global Desktop then has to determine which serial ports to map in the Windows application session.

On **UNIX and Linux** client platforms, users must have read and write access to any serial device that will be mapped. The *first match* of the following is used:

1. The serial ports listed in the `SUN_MAP_SERIALPORTS` environment variable.

Each serial port in the list is separated with a semi-colon and has the format `serial device=com_port_name`.

```
/dev/ttyS0=COM1;/dev/ttyS4=COM8
```

The `=com_port_name` is optional, but if it is omitted the serial port will be mapped to COMx in the Windows application session where x is the position of the serial port in the list.

2. The serial ports listed in the user's client configuration file.

For the **Native Client**, the `SerialPorts=` entry in the `$HOME/.tarantella/native-preferences` file lists the serial ports to be mapped. The `SerialPorts=` entry has to be added manually.

For the **Secure Global Desktop Client**, the `<serialports>` entry in the `<localsettings>` section of the user's [client profile cache](#) lists the serial ports to be mapped. The `<serialports>` entry has to be added manually.

For both these clients, the serial ports are listed in the same format as above.

3. The serial port listed in the `SUN_DEV_SERIAL` environment variable.

This is a single serial device, for example `/dev/ttyS2`. This is always mapped to COM1 in the Windows application session.

On **Windows** client platforms, the *first match* of the following is used:

1. The serial ports configured for the user's client.

For the **Native Client**, the `HKEY_CURRENT_USER\Software\Tarantella\Tarantella Native Client\Settings\SerialPorts` registry key lists the serial ports to be mapped. This key has to be added manually. The data type for the key is String.

For the **Secure Global Desktop Client**, the `<serialports>` entry in the `<localsettings>` section of the user's [client profile cache](#) lists the serial ports to be mapped. The `<serialports>` entry has to be added manually.

For both these clients, each serial port in the list is separated with a semi-colon and has the format `serial device=com_port_name`.

```
COM1=COM5 ; COM2=COM8
```

The `=com_port_name` is optional, but if it is omitted the serial port will be mapped to COMx in the Windows application session where x is the position of the serial port in the list.

2. Any available COM1 to COM9 ports.

The Secure Global Desktop clients attempt to open ports COM1 to COM9. If a COM port is found, it is mapped to the same COM port number in the Windows application session

### Related topics

- [Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop](#)
- [Windows application object](#)
- [Array properties \(array-wide\)](#)
- [Serial Port Mapping \(--serialport\)](#)
- [Native Client preferences files on UNIX, Linux and Mac OS X client devices](#)

## Using Remote Desktop on Microsoft Windows XP Professional

Microsoft Windows XP Professional includes the Remote Desktop feature that allows you to access a computer using the Remote Desktop Protocol. You can use Secure Global Desktop and Remote Desktop, for example, to give users to access their office PC when they are out of the office.

You should ensure that the Remote Desktop connection on the Windows XP host is working before introducing Secure Global Desktop. See [Get started using Remote Desktop with Windows XP Professional](#) for details.

To configure Secure Global Desktop for use with Remote Desktop:

- Create a [host object](#) for each Windows XP host.
- Create [Windows application objects](#).
  - Only full Windows desktop sessions are supported. You cannot run a specific application on the Windows XP host.
  - Seamless windows are not supported.
  - To ensure users access their own PC, you may have to create separate Windows application objects for each Windows XP host.
- To use client drive mapping, install the Sun Secure Global Desktop Enhancement Module for Windows on the Windows XP host.

### Related topics

- [Windows application object](#)

## Configuring client drive mapping

To give users access to the drives or file systems on their client device from UNIX, Linux or Microsoft Windows applications running through Secure Global Desktop, you have to:

1. Install the Sun Secure Global Desktop Enhancement Module on your application servers and configure the application servers for client drive mapping.
2. Enable client drive mapping.
3. Configure which drives you want users to access from Secure Global Desktop.

## Configuring UNIX and Linux application servers

1. Install the Sun Secure Global Desktop Enhancement Module for UNIX/Linux.

The Secure Global Desktop Installation Guide has details of how to install the Enhancement Module. The Secure Global Desktop Release Notes lists the supported platforms for Enhancement Module.

**Note** By default, the Enhancement Module is installed in `/opt/tta_tem`. If you install it in a different location, you must edit the `/opt/tarantella/var/serverresources/expect/vars.exp` Expect script and amend the `ttatdmclexe` variable with the correct location.

2. Configure the Network File System (NFS) share (export) that will be used for client drive mapping.

You must have an NFS server installed and running on the application server. The NFS server must share (export) a directory that will be used for client drive mapping. By default, the directory is `/smb`. You have to manually create and export this directory. The share must be accessible to localhost and users must have read and write access to it. Consult your system documentation for details of how to configure an NFS server and export a directory.

You can specify an alternative NFS share in the client drive mapping configuration file, `/opt/tta_tem/etc/client.prf`. Edit the `[nfsserver/mount/mountpoint={ (/smb) }]` setting to reflect the name of the share.

3. Start the client drive mapping processes, using the `/opt/tta_tem/bin/tem startcdm` command.

## Configuring how drives are displayed

When client drive mapping is enabled, the user's client drives or file systems are available by default in the `My SGD drives` directory in the user's home directory. The `My SGD drives` directory is a symbolic link to the NFS share that is used for client drive mapping.

You can configure the name and location of the symbolic link by **adding** one or more of the following settings to the client drive mapping configuration file, `/opt/tta_tem/etc/client.prf`:

- `[nfsserver/user/symlinkname={ (symlink) }]`

The name of the symbolic link. Default: `My SGD Drives`

For example, to change the name of the symbolic link to `Client Shares`, add the following line to the configuration file:

```
[nfsserver/user/symlinkname={ (Client Shares) }]
```

- `[nfsserver/user/symlinkdir={ (dir) }]`

The directory where the symbolic link is created. Default: `$HOME`

For example, to create the symbolic link in the `/tmp` directory, add the following line to the configuration file:

```
[nfsserver/user/symlinkdir={ (/tmp) }]
```

The directory can also be specified using environment variables. The variables you can use are controlled by the `nfsserver/user/envvars` setting.

For example, to create the symbolic link in the `/tmp/username` directory, add the following line to the configuration file:

```
[nfsserver/user/symlinkdir={ (/tmp/$USER) }]
```

- `[nfsserver/user/envvars={ (var) ... }]`

The list of environment variables that can be used when specifying the directory where the symbolic link is created. Default: `(USER) (HOME) (LOGNAME)`

Enclose each variable in parentheses. Do not include the dollar sign (\$) before the variable name.

The variables in the list **replace** the default variables.

For example, to be able to use the `$HOME`, `$USER`, `$DISPLAY` and `$TMPDIR` variables, add the



following line to the configuration file:

```
[nfssserver/user/envvars={ (HOME) (USER) (DISPLAY) (TMPDIR) }]
```

**Note** After making any changes to this file, you must restart the client drive mapping processes by running the `/opt/tta_tem/bin/tem stopcdm` and `/opt/tta_tem/bin/tem startcdm` commands.

## Configuring Microsoft Windows application servers

1. Install the Sun Secure Global Desktop Enhancement Module for Windows.

The Secure Global Desktop Installation Guide has details of how to install the Enhancement Module. The Secure Global Desktop Release Notes lists the supported platforms for Enhancement Module.

2. **(Optional)** Reconfigure the application server's drives.

By default, the application server's drives are also listed when users access their client drives from a Windows application. If you want Windows client users to see familiar drive letters, such as drive A for their client's floppy drive, you can configure the application server to [remap its drive letters or hide its drives](#).

**Note** Client drive mapping is only available for Windows application objects that are configured to use the Microsoft RDP [Windows Protocol](#).

## Enabling client drive mapping on the Secure Global Desktop server

1. On the [Array properties](#) panel in Array Manager, check Let Users Access Client Drives.
2. **(Optional)** Check Use WINS for better performance.

Only enable WINS if either of the following is true:

- Your Microsoft Windows application servers are on the same subnet as an array member.
- Your Microsoft Windows application servers list an array member as a WINS server.

3. For Fallback drive, choose a drive letter and a direction.

These settings are used if the desired drive letter is already allocated on a Microsoft Windows application server. When this happens, the first available fallback drive letter is allocated instead. By default, this is drive V, then drive U, then drive T, and so on.

4. Click Apply, and then exit.
5. Either restart all the Secure Global Desktop servers in the array or run the `tarantella start cdm` command on each array member.

After you enable client drive mapping, users must log out and log in again (start a new webtop session)

to be able to access their client drives or file systems.

If you use another Server Message Block (SMB) server, such as Samba, on the same host as the Secure Global Desktop server, you will not be able to start the client drive mapping service as both services use port 139/tcp. To use client drive mapping, you must either disable the other SMB server or [configure the host to allow more than one service to use port 139/tcp](#).

## Configuring the drives available to Unix, Linux and Mac OS X clients

By default, users on Unix, Linux and Mac OS X clients have access to their home directory and this is mapped to a drive called "My Home".

**Note** The Java technology client does not support client drive mapping on UNIX, Linux and Mac OS X client platforms.

Users can configure which part of their client file system they can access from applications by editing the `$HOME/.tarantella/native-cdm-config` configuration file. This file is automatically created when either the Secure Global Desktop Client or the Native Client is installed. The file contains detailed instructions for users on how to create mapped drives.

The configuration file contains entries with the form `<path> <type> <label>` where:

- `<path>` is the absolute path name of the client file system.
- `<type>` is either `unknown`, `fixed`, `floppy`, `cdrom` or `remote`.
- `<label>` is the name that will be used in the application session.

Use a separate line for each drive and separate each of the fields with a space or a tab. If either the `<path>` or the `<label>` fields contains spaces or tabs, enclose the field in quotes.

You can use environment variables in the `<path>` or `<label>` fields. You delimit these with a dollar sign (`$`). To use a literal `$`, escape it with another `$`.

The following is an example configuration file:

```
[cdm]
$HOME$ fixed "My Home"
/tmp/$USER$ fixed Temp
"/mnt/win/My Documents" fixed "My Local Documents"
[/cdm]
```

**Note** Changes to the configuration file only take effect for new webtop sessions.

## Configuring the drives available to Microsoft Windows clients

For Microsoft Windows clients, you configure the drives you want users to access with the [Client Drive Mapping](#) attribute for person objects, organizational unit objects and organization objects. Client drive mapping uses inheritance. You define access to client drives at an organization level, which you can override at an organizational unit level, and override again at a person object level. By default, users have

When a user logs in to a Secure Global Desktop server, information is gathered about the drives on the client device. For each available drive, the Client Drive Mapping attribute on the user's person object is checked. If there is no matching client drive configured, the parent organizational unit's Client Drive Mapping attribute is checked, and so on up the organizational hierarchy to the organization object.

If a match is found, then the associated access rights are granted for that drive, using the configured drive letter. If that drive letter is already in use on the application server, the Fallback Drive configured on the [Array](#) panel of Array Manager is used to determine the drive letter to use.

At each level you configure a number of drive mapping specifications. Each of these states a client drive letter, the access rights to that drive, and the application server drive letter to allocate. For example, you might specify that a user has read-write access to client drive A using application server drive Z. The first matching entry in the list is used, so make sure the most specific settings (for example, A or B) appear before more general settings (for example, All Drives).

**Note** Changes to client drive specifications only take effect for new webtop sessions.

### Example

You want to disable access to all client drives for all users and then give only Ruby Port access to her PC's floppy drive.

To disable access to all client drives:

1. In Object Manager, display the properties for the o=Indigo Insurance object.
2. Click the Attributes tab and choose Client Drive Mapping from the list.
3. Change the row that specifies access for All Drives so that the Access Rights are None.
4. Click Apply.

To give Ruby Port access to her PC's floppy drive:

1. In Object Manager, display the properties for Ruby Port's person object.
2. Click the Attributes tab and choose Client Drive Mapping from the list.

3. Click New.
4. Specify the client drive.
  - For Client Drive, choose A: (the drive letter of Ruby's floppy drive) or R/W Removable (this matches all read-write removable drives, such as floppy drives).
  - For Access Rights, choose Read-write. This lets Ruby have full access the drive, as long as the floppy disk is not write-protected.
  - For Drive Letter, choose Same As Client. With this setting, client drive mapping services attempts to use the same drive letters on the application server as are used on the client device.
5. Click Apply.

### Related topics

- [Client Drive Mapping \(--cdm\)](#)
- [Array properties \(array-wide\)](#)
- [Users are having problems accessing client drives](#)
- [The tarantella start cdm command](#)

## Remapping or hiding Windows 2000/2003 application server drives

### Problem

You want to let users access their client drives using the same drive letters they use on their client device, for example drive A for the first floppy drive. However, even with the Sun Secure Global Desktop Enhancement Module for Windows installed, these drive letters are in use for application server drives.

### Solution

On the Windows 2000/2003 application server, use the Computer Management tools to disable drives A and B, to disable or remap any CD or DVD drives, and to remap hard drives (except the application server boot volume, which can't be remapped).

### Case study

Indigo Insurance uses a Windows 2000 application server [verona.indigo-insurance.com](http://verona.indigo-insurance.com), on which [client drive mapping services](#) are already enabled. Users habitually choose drive A to try to access their floppy drive, but this refers to drive A on the application server, not the client device. You want to make sure that drive A accesses the client drive.

The application server verona currently has the following drives:

Drive Letter	Description
A:	Floppy drive
C:	Fixed drive (boot volume)
D:	Fixed drive
E:	CD drive

### Solution

1. Log in to [verona.indigo-insurance.com](http://verona.indigo-insurance.com) as a user with administrative privileges. To avoid disruption, you should make sure that nobody is currently using this server as an application

server (to check, look at the Sessions tab in Object Manager for the host object representing this application server).

2. In Control Panel, open Administrative Tools and then click Computer Management.
3. In the tree, open Storage and then click Disk Management. Using this tool you can change the drive letters used to access some drives.
4. In the Volume List (usually shown at the top of the panel on the right), right-click drive D and choose Change Drive Letter And Path. Click the drive letter, and then click Edit. In the Assign A Drive Letter list, choose the drive letter you want to use to access this drive, for example X. Click OK, and then click Close.
5. In the same way, change the drive letter of the CD drive from E to Y, for example. You can't change the drive letter of the boot volume, in this example drive C.
6. The Disk Management tool doesn't let you change the drive letters to use for floppy drives. To allow use of drive letters A and B to access client drives, you must disable the floppy drives on the application server. On the left side of the Computer Management window, open System Tools and then click Device Manager. Then on the right, open Floppy Disk Drives. Right-click the drive shown, and choose Disable. (Note that if you prefer, you can disable access to a CD or DVD drive rather than change the drive letter used. However, this means you won't be able to install software from that drive unless you temporarily enable it again.)

## Next steps

- To ensure consistency for users, you should remap or disable drives on all Windows 2000/2003 application servers used for client drive mapping.
- For information on hiding drives so that users can only access a limited set of drives, see the Microsoft article [Using Group Policy Objects to Hide Specified Drives in My Computer for Windows 2000 \(Q231289\)](#)

## Related topics

- [Configuring client drive mapping](#)
- [Client Drive Mapping \(--cdm\)](#)
- [Users are having problems accessing client drives](#)

## Can I run another SMB service with client drive mapping?

Yes, with additional configuration. In a default installation, you can not use client drive mapping and run another SMB server, such as Samba, on the host because they both use port 139/tcp.

To allow more than one service to use port 139/tcp:

1. Configure the Secure Global Desktop host to have more than one IP address by either installing another network interface card (NIC) or using IP aliasing to assign multiple IP addresses to a single NIC.
2. Configure the IP addresses you want the Secure Global Desktop server to bind to for client drive mapping:
  - o Stop the Secure Global Desktop server: `tarantella stop`.
  - o Run the following command:

```
tarantella config edit --tarantella-config-cdm-externalnbtaddress  
ip_address ...
```

The default setting is `*` which means bind to all interfaces. Separate each IP address with a space.

- o Start the Secure Global Desktop server: `tarantella start`.
  - o Repeat these steps on each member of the array.
3. Configure the other service(s) to bind to a different IP address.

### Related topics

- [Configuring client drive mapping](#)
- [Users are having problems accessing client drives](#)

## A Kiosk application isn't appearing full-screen

### Is the application being resumed on a display with a different size?

If an application configured to [Display Using](#) Kiosk mode is resumed on a display that's larger or smaller than the display on which it was started, the application no longer fits the display exactly.

- If the new display size is smaller than the original (fewer pixels), the application is clipped by the edges of the display.
- If the new display size is larger than the original (more pixels), the application won't fill the display.

### Is the application displayed to non-Windows client devices?

Kiosk mode is supported only for Microsoft Windows client devices. On other client devices, the application appears in an independent window, filling the screen.

#### Related topics

- [Introducing Object Manager](#)
- [Display Using \(--displayusing\)](#)



[Secure Global Desktop Administration Guide > Applications, documents and hosts > A session doesn't end when the user exits the application](#)

## A session doesn't end when the user exits the application

### Is the Session Ends When attribute set correctly?

Using Object Manager, or from the command line, choose the appropriate [Session Ends When](#) setting for the application object.

If the Session Ends When attribute text box is disabled, the session ends when there are no visible windows.

### Are processes still running which cause the Windows session not to exit?

When running an application on a Windows 2000/2003 Terminal Server, closing the application does not always result in the session closing. This is because the Sun Secure Global Desktop Enhancement Module for Windows is still running.

The solution is to configure the Sun Secure Global Desktop Enhancement Module to ignore certain system processes so that it closes. To do this, edit the `System processes` value for the `HKEY_LOCAL_MACHINE\Software\Tarantella\Enhancement Module for Windows` key in the registry on the application server. This value is a string which is a comma separated list of exe binaries which the Sun Secure Global Desktop Enhancement Module should ignore. You must amend this value by listing the processes that were running when the session failed to close. To do this, open Task Manager (while you have a session that has failed to close) and click the Processes tab. Make a list of all the exe processes that are running. **Do not include** the following processes:

- clipsrv.exe
- conime.exe
- csrss.exe
- EventLog.exe
- lmsvcs.exe
- lsass.exe
- MsgSvc.exe
- nddeagnt.exe
- netdde.exe
- NETSTRS.EXE
- os2srv.exe

- proquota.exe
- rdpclip.exe
- screg.exe
- smss.exe
- spoolss.exe
- ttaswm.exe
- ttatdm.exe
- wfshell.exe
- win.com
- winlogon.exe

If you are running a single application session, you may find that the session still does not exit even after editing the `System processes` registry setting. To force the session to exit, amend the `Logoff application sessions` setting for the `HKEY_LOCAL_MACHINE\Software\Tarantella\Enhancement Module for Windows` key and change the `DWORD` value to 1.

#### Related topics

- [Session Ends When \(--endswhen\)](#)
- [Introducing Object Manager](#)

[Secure Global Desktop Administration Guide](#) > [Applications, documents and hosts](#) > An application exits immediately after starting

## An application exits immediately after starting

Users may see this problem with Windows applications or X applications.

Using Object Manager, or from the command line, configure the application object to [keep launch connections open](#).

### Related topics

- [Keep launch connection open \(--keepopen\)](#)
- [Introducing Object Manager](#)

## An application requires a richer set of cursors

For the browser-based webtop, applications that do not display on the webtop or in a new browser windows should not have problems with cursors.

Applications that do display on the webtop or in a new browser window, or applications launched from the *classic* webtop, require Java™ technology. This currently supports only a limited set of cursors. If you require more cursors, try any of the following:

- On Microsoft Windows 2000, use Microsoft Internet Explorer. Additional functionality for this browser allows the display of any cursors. This works if you use either Microsoft Virtual Machine or Sun Java Plug-in.
- Use the Native Client instead of a web browser. The Native Client can display any cursors. The Native Client can only be used with the *classic* webtop.

### Related topics

- [What do I need to tell my users?](#)
- [Use Windows cursor \(--wincursor\)](#)
- [Introducing Object Manager](#)

## An application won't start

### Microsoft Windows applications

Using Object Manager, check the following:

- Is the correct [Windows protocol](#) set for the application server?
- Make sure that the [Application Command](#) attribute contains the full pathname of the application's executable, including the correct filename extension.
- Make sure that the pathname **does not** point to a Windows shortcut.
- Make sure that the application is correctly installed and configured on all [application servers that may run it](#). The application servers are defined in the application object's [Hosts](#) tab. The application must be installed in the same location on every application server.
- Make sure that the [connection method](#) is appropriate to the application servers.
- Make sure that the [Windows NT Domain](#) attribute is set correctly.
- If no users can start applications (and no users can log in), try `tarantella restart --warm`.

### X applications

Using Object Manager, check the following:

- Make sure that the [Application Command](#) attribute contains the full pathname of the application's executable.
- Make sure that the application is correctly installed and configured on all [application servers that may run it](#). The application servers are defined in the application object's [Hosts](#) tab. The application must be installed in the same location on every application server.
- Make sure that the [connection method](#) is appropriate to the application servers.
- Make sure that all required [Environment Variables](#) are set correctly.
- Make sure that the [Login Script](#) is set correctly.
- If no users can start applications (and no users can log in), try `tarantella restart --warm`.

### Application server

It may be worth [increasing the launch timeouts](#) on the application server.

## Related topics

- [Creating and publishing an application object to users](#)
- [Introducing Object Manager](#)

## An application's animation appears "jumpy"

The application object's [Allow Delayed Updates](#) and [Command Execution](#) attributes can affect the display of animation.

For animation, we recommend the following:

- Turn off Allow Delayed Updates.
- Set Command Execution to In Order.

### Related topics

- [Command Execution \(--execution\)](#)
- [Allow delayed updates \(--delayed\)](#)
- [Introducing Object Manager](#)

## Applications disappear after about two minutes

If users find that their applications disappear unexpectedly after about two minutes, it may be that your proxy server is timing out the connections. Proxy servers will drop a connection after a short period of time if there is no activity on the connection.

Secure Global Desktop sends keepalive packets to keep the connection open and by default this is every 100 seconds. If applications are disappearing, you may have to increase the frequency at which keepalive packets are sent to keep the connection open.

### The AIP keepalive

The AIP keepalive is used for emulator sessions. It is used with the browser-based webtop and the classic webtop. To change the keepalive:

- On your webtop, click Array Manager.
- Click [Emulator Sessions](#), Properties.
- Change the AIP Keepalive setting, for example to 60.
- Click Apply.

Alternatively, you can run the following command:

```
tarantella config edit --sessions-aipkeepalive secs
```

### The webtop keepalive for the classic webtop

For the *classic webtop* only, you may also have to amend the keepalive used for the webtop connection. To change the keepalive for web browsers:

1. Open `/var/docroot/resources/login/sco/tta/boot/strap.html` **and** `/var/docroot/resources/login/sco/tta/boot/autostrap.html`.
2. Decrease the value for the `AsadKeepAlive` parameter, for example to 60.

If you have created any customized themes which use entry-point HTML files, you will need to modify the `AsadKeepAlive` parameter in those files instead. See [Using Secure Global Desktop with proxy servers](#) for details.



To amend the keepalive for Native Clients:

1. Open `/var/docroot/resources/login/sco/tta/boot/serverinfo.html`.
2. Decrease the `WebtopKeepAlive=100` setting, for example to 60.

### Related topics

- [Using Secure Global Desktop with proxy servers](#)

## Can I access a web application through Secure Global Desktop?

Yes. A web application is simply a web page (in fact, any URL) that requires the user to supply a username and password for access. So to access a web application, you must create a [document object](#) that links to the URL of the web application.

Unlike passwords for application servers, Secure Global Desktop cannot cache the usernames and passwords for accessing web applications. However you can configure [web server authentication](#) so that users can access Secure Global Desktop from a web application without having to log in again. Alternatively, you can authenticate Secure Global Desktop users to the web application.

**Note** The Sun Secure Global Desktop Native Client does not support web server authentication.

We also recommend that you use a secure (HTTPS) web server so that all communications and passwords are encrypted using SSL before transmission.

### Related topics

- [Document object](#)
- [Introducing web server authentication](#)
- [Enabling web server authentication for the browser-based webtop](#)
- [Enabling web server authentication for the classic webtop](#)

## Can I prevent users from launching applications with a different username and password?

Yes. In a standard Secure Global Desktop installation, users can force Secure Global Desktop to prompt them for a username and password by holding down the SHIFT key when they click an application's link on the webtop. To prevent users from being able to do this, you must change the Authentication Dialog attribute on the [Application launch](#) panel in Array Manager. This attribute controls when the application server's authentication dialog displays.

The settings are:

Setting	Description
Never show	Holding down SHIFT has no effect on the application launch. If a user's cached password is incorrect or missing, the authentication dialog <b>never</b> displays and the application launch fails.
Show on password problem only	Holding down SHIFT has no effect on the application launch. If a user's cached password is incorrect or missing, the authentication dialog displays.
Show on Shift-click or password problem	Holding down SHIFT forces the authentication dialog to display. This is the default Secure Global Desktop setting.

### Related topics

- [Application Launch properties \(array-wide\)](#)

## Can I use multiple monitors with Secure Global Desktop?

Yes. However, if any of the applications are set to display using [client window management](#) you may have to amend your application and monitor configuration to be able to use multiple monitors.

To use multiple monitors with client window management, you must:

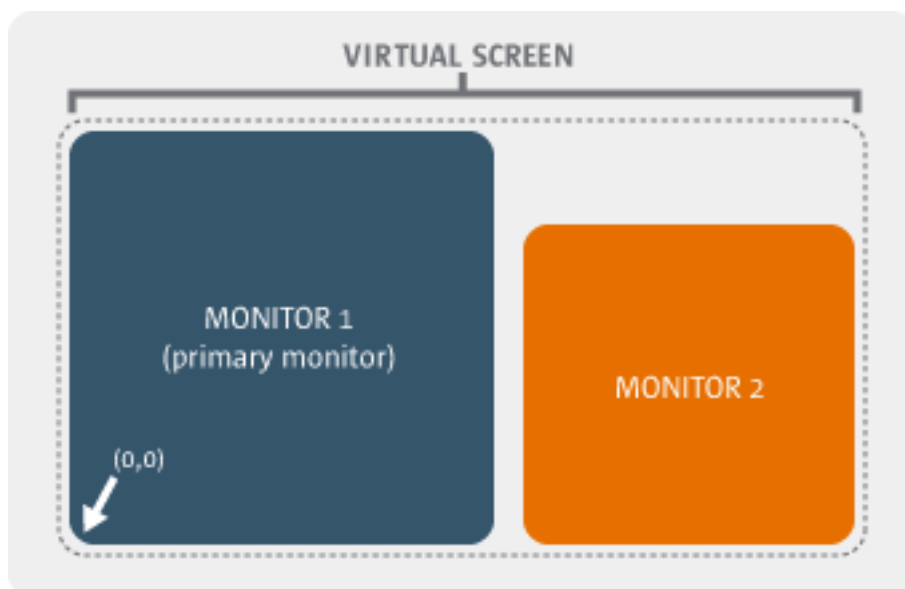
- disable shared resources
- ensure that the Secure Global Desktop server sends the client enough space to display all the monitors on the desktop and
- set up the monitors correctly.

### Disabling shared resources

To disable shared resources, you must edit each application in Object Manager and uncheck the [Share resources between similar sessions](#) checkbox (it's on the Advanced panel). You must do this for **all** client window management applications that will be displayed using multiple monitors.

### Sending the correct desktop size

You must also ensure that the Secure Global Desktop server sends the client the size of the entire desktop area (the "virtual screen" in the diagram below) and not just the size of the primary monitor.



For example, if the dimensions of Monitor 1 in the diagram are 1200 x 768 and the dimension of Monitor 2 are 800 x 600, then the desktop size that needs to be configured is 2000 x 768.

To send the correct desktop size, edit the Client Window Management maximum height and width on the [X Protocol Engine](#) panel in Array Manager so that it matches the size of the virtual screen.

**Note** This will increase the amount of memory used on the client and on the Secure Global Desktop server.

## Setting up the monitors

You must set up the monitors so that all the secondary monitors are to the right of the primary monitor (see the diagram above). You have to do this because the X server cannot handle negative screen coordinates.

### Related topics

- [Display Using \(--displayusing\)](#)
- [Share resources between similar sessions \(--share\)](#)

## Can I use Secure Global Desktop to access VMS applications?

Yes. You can use Secure Global Desktop to access X or character applications on a VMS application server.

To be able to run VMS applications, you must change the [Login Script](#) used by the X or character application object to either `vms.exp` or `vmsrexec.exp`. The script you use depends on the [Connection Method](#) for the application.

By default, the `vms.exp` or `vmsrexec.exp` login scripts set the transport variable to `TCPIP`, which is correct for Digital TCP/IP stacks (including UCX). If you need to change this variable, you can edit the scripts in the `/opt/tarantella/var/serverresources/expect` directory.

To use VMS X applications, you must also disable X security on the [Security](#) properties panel in Array Manager or by running:

```
tarantella config edit --security-xsecurity 0
```

This is because VMS does not support X security.

### Related topics

- [Character application object](#)
- [X application object](#)
- [Login scripts supplied with Secure Global Desktop](#)

## How do I run a Common Desktop Environment (CDE) session?

To run a Common Desktop Environment (CDE) session through Secure Global Desktop, you must create an X application object with the following attribute settings:

Attribute	Value
Application Command (--app)	The full path to the <code>Xsession</code> application, for example <code>/usr/dt/bin/Xsession</code>
Keep launch connection open (--keepopen)	Enabled ( <code>true</code> )
Session Ends When (--endswhen)	Login script exits ( <code>loginscript</code> )

**Note** You **must** use these settings, to allow Secure Global Desktop to shut down the CDE session correctly.

### Running a CDE application directly

To run a CDE application directly rather than from the CDE Front Panel you must create an X application object with the following attribute settings:

Attribute	Value
Application Command (--app)	The full path to the application you want to run
Window Manager (--winmgr)	<code>/usr/dt/bin/dtwm -xrm "Dtwm*useFrontPanel: false" -xrm "Dtwm*ws0*backdrop*image: none"</code>
Session Ends When (--endswhen)	No visible windows ( <code>nowindows</code> )

**Note** This is the default value for this attribute

Keep launch connection open ( <code>--keepopen</code> )	Disabled ( <code>false</code> )  <b>Note</b> This is the default value for this attribute
---	---

### Related topics

- [X application object](#)
- [The tarantella object `new\_xapp` command](#)



[Secure Global Desktop Administration Guide > Applications, documents and hosts >](#) In some X applications, the ALT and ALT GR keys do not work

## In some X applications, the ALT and ALT GR keys do not work

The X keyboard maps used by Secure Global Desktop include support for the META key on a Sun™ keyboard. Some X applications choose to use the META key in preference to the ALT key, when both keys are made available in the X keyboard map.

Edit the keyboard map file being used with the application. Replace the following lines:

```
199 Meta_L NoSymbol NoSymbol NoSymbol
200 Meta_R NoSymbol NoSymbol NoSymbol
```

With the following:

```
199 NoSymbol NoSymbol NoSymbol NoSymbol
200 NoSymbol NoSymbol NoSymbol NoSymbol
```

### Related topics

- [Keyboard Map \(--keymap\)](#)

## Secure Global Desktop uses too much of my network's bandwidth

Using Object Manager, or from the command line, set the [Bandwidth Limit](#) attribute for a person object to reduce the maximum allowable bandwidth the person can use.

**Note** Reducing the available bandwidth may have implications for application usability.

### Related topics

- [Bandwidth Limit \(--bandwidth\)](#)
- [Introducing Object Manager](#)

## Troubleshooting sound in Windows applications

Select the section that best matches the problem:

- [No sound plays at all](#)
- [Sound is muffled or distorted](#)
- [Not all users require sound](#)

### No sound plays at all

If no sound is playing at all in the Windows Terminal Services session, use the following checklist to resolve the problem:

Things to check	Description
Can the Secure Global Desktop client play sound?	<p>Only the following clients can play sound:</p> <ul style="list-style-type: none"><li>• the Sun Secure Global Desktop Client running on Windows 2000/XP Professional, Linux, Solaris Sunrays or Mac OS X</li><li>• the Native Client for Linux</li><li>• the Native Client for UNIX running on Solaris</li><li>• the Native Client for Mac OS X.</li></ul>
Does the client have an audio device?	<p>To be able to play sound, the client must have an audio device. If the client has a device, check that it works.</p> <p>On UNIX/Linux client platforms, the user must also have read and write access to the <code>/dev/audio</code> device.</p> <p><b>Note</b> On Solaris, if the <code>AUDIODEV</code> environment variable has been set to a different device, the Sun Secure Global Desktop Native Client tries to use this device before trying the <code>/dev/audio</code> device.</p>

Has the audio service been enabled on the Secure Global Desktop server?	By default, the audio service is disabled for a Secure Global Desktop array. Check that the audio service has been enabled on the <a href="#">Array properties</a> panel in Array Manager.
Has the sound quality been changed?	By default, Secure Global Desktop uses Medium Quality Audio. Changing the sound quality to Low Quality Audio or High Quality Audio limits the audio formats used in the Terminal Services session and may mean that the client can't play sound.  Reset the sound quality to Medium Quality Audio on the <a href="#">Array properties</a> panel in Array Manager.
Is the application running on a Windows 2003 server?	You can only play sound in Windows 2003 Terminal Services sessions.
Has sound been enabled on the Windows 2003 server?	By default, sound is disabled for Windows Terminal Services sessions. See the <a href="#">instructions for enabling sound</a> .

## Sound is muffled or distorted

If sound is muffled or distorted, adjust the audio quality and compression settings to see if this improves the sound.

You adjust:

- the quality setting on the [Array Properties properties](#) panel in Array Manager.
- the compression setting on the [Audio Protocol Engine properties](#) panel in Array Manager.

**Note** The net gain of compressing audio data, which is pre-compressed, may be limited.

## Not all users require sound

If you enable sound on the Windows 2003 application server and enable the Secure Global Desktop audio service, all users will be able to play sound in their Windows Terminal Services session. However, playing sound increases the amount of network bandwidth used and so you may want to restrict its use. Currently, the only way to do this is to disable sound for groups of users on the Windows 2003 server. To do this:

1. Either:
  - start the Microsoft Group Policy Management Console or

- start an empty Microsoft Management Console (by running mmc.exe from the Start, Run menu) and add the Group Policy Object Editor snap-in.
2. Select the group policy object you want to edit.
3. Click Computer configuration, Administrative Templates, Windows Components, Terminal Services, Client Server Data Redirection.
4. Open Allow audio redirection.
5. Click Disabled.
6. Click OK.

Changes to this setting only apply to new Windows Terminal Server sessions.

### Related topics

- [Audio Protocol Engine properties \(server-specific\)](#)
- [Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop](#)

## Users are having problems accessing client drives

Select the section that best matches the user's symptoms:

- No client drives are mapped within the user's session or there are fewer than drives than expected
- Windows client drives are mapped using unexpected drive letters
- More client drives are mapped than expected
- The Recycle Bin doesn't work as expected
- Laptop/notebook users experience a delay in seeing mapped drives
- Mapped drives have unusual names

Note also the [client limitations](#) and limitations on [shared users](#).

On Microsoft Windows application servers, you can also run the drive mapping application in "diagnostic mode" to help troubleshoot drive mapping problems.

### No client drives are mapped within the user's session or there are fewer drives than expected

Checklist	More information
Is the user logged in to Secure Global Desktop using a suitable client?	The Java™ technology client (classic webtop) only supports client drive mapping on Microsoft Windows client platforms.
Is the Sun Secure Global Desktop Enhancement Module installed on the application server?	<p>To access client drives from applications displayed through Secure Global Desktop, the Sun Secure Global Desktop Enhancement Module must be installed on the application server.</p> <p>The Secure Global Desktop Release Notes has details of the supported platforms for the Sun Secure Global Desktop Enhancement Module.</p>

<p>Is client drive mapping enabled?</p>	<p>In Array Manager, open <a href="#">Array</a> properties. To enable client drive mapping services, make sure that Let Users Access Client Drives is checked.</p> <p>Remember, client drive mapping services only become available when you restart all Secure Global Desktop servers in the array. To manually start CDM services without restarting the array, run the <code>tarantella start cdm</code> command on all members of the array.</p>
<p>Have the user's client drives been configured correctly?</p>	<p>For users on <b>Microsoft Windows</b> client devices, the <a href="#">Client Drive Mapping</a> attribute on person, organizational unit and organization objects determines which client drives each user may access. The user may be configured to have no access to any client drives. Remember to check the ancestor OUs in the organizational hierarchy: client drive mapping settings are inherited, so you can give access to many users with one configuration change.</p> <p>For users on <b>UNIX, Linux or Mac OS X</b> client devices, check that the user's <code>\$HOME/.tarantella/native-cdm-config</code> file is present and has valid entries.</p>
<p>Are client drive mapping services running?</p>	<p>Run the following command on the host where Secure Global Desktop is installed:</p> <pre>ps -ef   grep ttacdmd.</pre> <p>If client drive mapping services are running, there should be at least two processes with the name "ttacdmd".</p> <p>If there are no any drive mapping processes, run the following command:</p> <pre>grep cdm /opt/tarantella/var/log/*.</pre> <p>Check the output for any messages.</p> <p>On UNIX, Linux and Mac OS X application servers, use the following command to check that client drive mapping processes are running:</p> <pre>ps -ef   grep ttatdm</pre> <p>If they are not, run the following command:</p>

	<pre>/opt/tta_tem/bin/tem startcdm</pre> <p>If starting client drive mapping processes produces errors such as "Failed to mount /smb" check that the NFS server is running and that the directory being used for client drive mapping is exported correctly.</p>
<p>Do the version numbers for the Sun Secure Global Desktop Enhancement Module and the Secure Global Desktop server match?</p>	<p>Run the following command on the host where Secure Global Desktop is installed:</p> <pre>tarantella version</pre> <p>Make a note of the version number.</p> <p>On a Windows application server, browse to the C:\Program Files\Tarantella\Enhancement Module directory. Right-mouse click on the <code>ttatdm.exe</code> file and select Properties. On the Version tab, click File Version.</p> <p>On a UNIX/Linux application server, run the following command:</p> <pre>/opt/tta_tem/bin/tem version</pre>
<p>Are other services using ports 139/tcp and 137/udp?</p>	<p>Secure Global Desktop client drive mapping services must bind to port 139/tcp, which is used for Server Message Block (SMB) services. This port may already be in use, for example by a product such as Samba. Port 137/udp is also used if you enable the Use WINS for better performance option on <a href="#">Array properties</a>.</p> <p>To find out whether any other process is using port 139 (137), stop the Secure Global Desktop server and then run the following commands on the host on which Secure Global Desktop is installed:</p> <pre>netstat -an   grep 139 grep 139 /etc/xinetd.conf.</pre> <p>To ensure that client drive mapping services are available, stop any other products that bind to port 139/tcp (and 137/udp, if required), and restart the Secure Global Desktop server.</p> <p>Follow these instructions for using <a href="#">client drive mapping and another SMB service on the same host</a>.</p>



Does logging reveal any errors?

Enable drive mapping logging by adding the following filters on the [Array Properties](#) panel of Array Manager:

```
cdm/*/*:cdm%%PID%%.log
cdm/*/*:cdm%%PID%%.jsl
server/deviceservice/*:cdm%%PID%%.log
server/deviceservice/*:cdm%%PID%%.jsl
```

Check the log files for any errors.

On Windows application servers, check the Windows Event Viewer for any drive mapping errors. See also [running client drive mapping in "diagnostic mode"](#) for logging options.

On UNIX/Linux application servers, check for any drive mapping errors in the `clerr.log` and the `clPID.log` files in the `/opt/tta_tem/var/log` directory.

Does the error log on a Microsoft Windows application server show an `Add device failed with ERROR_INVALID_PASSWORD` error message?

If no client drives are mapped in the Microsoft Windows application session and you see error such as `Add device failed with ERROR_INVALID_PASSWORD` in the [client drive mapping log output](#), this can be caused by either SMB packet signing or the LAN Manager authentication level.

This applies to Microsoft Windows Server 2003 and Microsoft Windows 2000 Server.

### **SMB packet signing**

Microsoft Windows application servers can be configured so that the Server Message Block (SMB) communications between a client and Microsoft Windows server are digitally signed for security.

Secure Global Desktop does not support SMB packet signing. The solution is to disable SMB packet signing.

See this [Microsoft TechNet article](#) for information on disabling SMB packet signing.

## LAN Manager authentication level

The LAN Manager authentication level controls the authentication protocols used for communications between a client and Microsoft Windows server. If the authentication level is set too high, client drive mapping fails.

The solution is to edit the **Security options Network security: LAN Manager authentication level** policy and select Send LM NTLM - Use NTLMv2 session security if negotiated.

See [Microsoft KB article 823659](#) for details.

Have all the client drives been found?

For Windows clients, the Sun Secure Global Desktop Client displays information about the drives it has found. Right-mouse click on the System Tray icon and select Connection info.

You can also debug the classic webtop (Java technology client) as follows:

1. Ensure the Java™ Console is enabled in the web browser.
2. Add the following parameter to the client drive mapping applet in the file `opt.html`:  

```
<param name="DebugMask" value="255">
```
3. Log in to Secure Global Desktop.
4. Check the Java Console for information on why drives have not been mapped.

**Note** `opt.html` is in the directory for the theme you are using in `/opt/tarantella/var/docroot/resources`.

Is the drive mapping connection between the application server and the Secure Global Desktop server working?

To check whether the drive mapping connection between the application server and the Secure Global Desktop server is working, enable drive mapping in "[diagnostic mode](#)" on the application server. When the drive mapping window displays, select Information from the Debug menu. Check the output for information on why the drive connections are failing.

Common reasons why drive connections fail include:

- the application server can't resolve the netbios name of the Secure Global Desktop server. The solution is to configure a WINS server on the application server that points to a WINS server that can resolve the netbios name of the Secure Global Desktop server. Alternatively, edit the `lmhosts` file to include the netbios name and address of the Secure Global Desktop server.
- the `ttacdm` program isn't running because another SMB server is running.

## Windows client drives are mapped using unexpected drive letters

If a drive letter is already in use on the Microsoft Windows application server (for example, drive A is reserved for the application server's floppy drive), the drive can't be remapped automatically. The client drive mapping service uses a [Fallback Drive](#) to ensure the client drive can be accessed using a different drive letter.

To help ensure that the configured drive letter is available, we recommend that you [hide or remap application server drives to use different drive letters](#).

## More client drives are mapped than expected

For users on **Microsoft Windows** client devices, client drives are inherited within the organizational hierarchy, so you can give access to many users with one configuration change. Check the [Client DriveMapping](#) attribute on the organizational unit object the user's person object belongs to. If necessary, check all ancestors of the person object, including the top-level organization object. You can override a setting that's specified in a parent OU or organization object, by configuring the person object's Client Drive Mapping attribute: the first matching drive specification is used.

For users on **UNIX, Linux or Mac OS X** client devices, check that the user's `$HOME/.tarantella/native-cdm-config` file is present and has valid entries.

## The Recycle Bin doesn't work as expected

On Microsoft Windows client devices, client drives accessed through Secure Global Desktop are treated by the application server as network drives. This means that Recycle Bin features are not available for client drives.

- Deleting a file does not send the file to the Recycle Bin.
- The `Recycled` directory, if present, is not shown as the Recycle Bin and its contents are not displayed specially by Windows.

## Laptop/notebook users experience a delay in seeing mapped drives

Laptop/notebook users who have external floppy drives can experience a delay if the floppy drive is not attached when they access client drives. The delay happens because the client times out before it realizes the floppy drive is not available.

The solution is either:

- for the user to attach the floppy drive before accessing client drives, or
- deny the user access to the floppy drive (`--cdm`)

## Mapped drives have unusual names

On Windows client devices, sometimes drives appear with unusual names. This is caused by the drive mapping application timing out.

The solution is to increase the default timeout values in the Windows registry for the client drive mapping application (`ttatdm.exe`) on the application server. To do this:

1. In the Windows Registry Editor (`regedit`), edit the `HKEY_LOCAL_MACHINE\Software\Tarantella, Inc.\Enhancement Module for Windows` key.
2. Double-click `Initial Timeout`. The Edit DWord Value window displays.
3. In the Base part of the screen, click Decimal.
4. In the Value data field increase the value. (The value is in milliseconds and the default is 10000.)
5. Click OK.
6. Double-click `Subsequent Timeout`. The Edit DWord Value window displays.
7. In the Base part of the screen, click Decimal.
8. In the Value data field increase the value to something like 8000. (The value is in milliseconds and the default is 1000.)
9. Click OK.

10. Close the Registry Editor.

11. For the changes to take effect, the user needs to log out of Windows and then log in again.

On UNIX, Linux and Mac OS X client devices, the names of mapped drives are configured in the user's the `$HOME/.tarantella/native-cdm-config` file. Check that it has valid entries.

## Client limitations

Not all functionality is available for users of Netscape browsers when using the classic webtop:

- Users are unable to obtain drive information (for example, free disk space).
- Users are unable to change file permissions.
- Drives with removable media are detected only if the media is present when the emulator session starts.
- Drives identified as A or B are assumed to be read/write removable drives (floppy disk drives).
- Read/write drives identified as C-Z are assumed to be fixed drives.
- Read-only drives identified as C-Z are assumed to be read-only removable drives (CD or DVD drives).

## Shared users

On Unix or Linux application servers, access to client file systems is given to users based on their UNIX user ID and standard NFS file system privileges. If a shared account is used to access applications, client drive mapping will not be available to the shared users. This is because Secure Global Desktop has no way to distinguish between these users as they all have the same user ID.

## Running client drive mapping in "diagnostic mode"

On Microsoft Windows application servers, you can run the drive mapping application in "diagnostic mode" to obtain information for troubleshooting drive mapping problems. To enable "diagnostic mode":

1. Log on to the application server as an Administrator.
2. Double-click the drive mapping program file (`C:\Program Files\Tarantella\Enhancement Module\ttatdm.exe`).
3. When the drive mapping window displays, select the level of information you want by choosing an option from the Debug menu.

The Debug menu has the following options:

- **Errors** - select this option to see any errors that have occurred.  
This also causes errors to be reported to the Windows Event Viewer. This option is selected by

default.

- **Warnings** - select this option to see any errors and warnings that have occurred. This also causes errors and warnings to be reported to the Windows Event Viewer.
- **Information** - select this option to display all drive mapping information.
- **Log to file** - select this option to save the output to a log file in the user's temp directory. The drive mapping window shows you the name and location of the log file it has written.
- **Start visible** - select this option to have the drive mapping window display every time the drive mapping services are started.

The drive mapping window only shows drive mapping information from when the window is displayed. It does not show historical information. If you change the level of information displayed in the drive mapping window, the user needs to log out of Windows and log in again to generate the new information.

The Edit menu allows you to select, copy and clear information from the drive mapping window.

#### Related topics

- [Client Drive Mapping \(--cdm\)](#)
- [Configuring client drive mapping](#)
- [Remapping or hiding Windows 2000/2003 application server drives](#)

## Users are unable to use smart cards with Windows applications

If users find they are unable to use their smart cards with Windows applications, use the following checklist to identify the source of the problem.

Check	Description
Application server configuration	<ul style="list-style-type: none"><li>• Is the application running on a Windows Server 2003 application server? Only Windows Server 2003 supports smart card device redirection.</li><li>• Has <a href="#">smart card device redirection</a> been enabled for Terminal Services on the Windows Server 2003?</li></ul>
Secure Global Desktop configuration	<ul style="list-style-type: none"><li>• Does the Windows application use Microsoft RDP as the <a href="#">Windows Protocol (--winproto)</a>?</li><li>• Is the Secure Global Desktop smart card service enabled on the <a href="#">Array properties</a> panel in Array Manager?</li><li>• Is the Allow smart card authentication box checked on the <a href="#">Application Launch properties</a> panel in Array Manager?</li></ul>
Client configuration	<ul style="list-style-type: none"><li>• Is the user using <a href="#">a supported client</a>?</li><li>• Is the smart card reader working?<ul style="list-style-type: none"><li>○ On Windows clients:<ul style="list-style-type: none"><li>■ Check that the smart card reader listed in the Windows Device Manager.</li><li>■ Check that the smart card service is running on the client (click Start Menu, Programs, Administrative Tools, Services).</li><li>■ Check that the Sun Secure Global Desktop Client has detected the smart card reader and card. Right-mouse click on the Secure Global Desktop icon in the Windows system tray and select Connection info. The Smart card reader property should list the details in the format <i>reader.ATR_string</i> where <i>reader</i> is the manufacturer and model of the smart card reader and <i>ATR_string</i> is the Automatic Terminal Recognition (ATR) string which is a sequence of hexadecimal numbers used to identify</li></ul></li></ul></li></ul>

the card to the system.

- On Linux/Solaris clients, start the Native Client, click Cancel when the log in dialog displays and then select View log from the Webtop menu. Check the message(s) that display and see below for details.

## Native Client for UNIX/Linux smart card messages

### No smart card support ( `lib_name` ): error message

`lib_name` is the PCSC-Lite library file the Native Client tried to load. On Linux and Solaris this is `libpcsclite.so`. Depending on your dynamic linker path, this is normally installed in the `/usr/lib` directory. `<error_message>` is any additional error message from the dynamic linker.

This message only displays if the Native Client can't load a PCSC-Lite library.

Either install a version of the PCSC-Lite library or use the `TTA_LIB_PCSCLITE` environment variable to specify the location.

### Smart card library loaded: `lib_name`

`lib_name` is the name of the PCSC-Lite library loaded by the Native Client.

This message only displays if the Native Client successfully loaded a PCSC-Lite library.

### Failed to find context entry points in `lib_name`

`lib_name` is the name of the PCSC-Lite library loaded by the Native Client.

This message only displays if the PCSC-Lite library loaded by the Native Client does not support a minimum set of API routines.

Either install another version of the PCSC-Lite library or use the `TTA_LIB_PCSCLITE` environment variable to specify a different library.

### Smart card support failed to initialize (0xH)

0xH is a PCSC hexadecimal error code.

The Native Client successfully loaded a PCSC-Lite library, but the smart card system on the client platform is not working.



Check that the smart card system is running on the client platform:

- On Linux:
  - Check that the PCSC daemon (`pcscd`) is running, for example by running `/sbin/service pcscd status`.
  - Try restarting the PCSC daemon with a `--debug stdout` option. Insert the card in the reader and see if the reader and card are detected.
- On Solaris:
  - If you are using the PC/SC Shim for SCF package, check that the OCF server (`ocfserv`) is running. Enable it if it isn't (`svcadm enable svc:/network/rpc/ocfserv`).
  - If you are using the Sun Ray PC/SC Bypass package, check the Sun Ray Server Software configuration.

### Smart card reader: `reader name`

Lists the names of all the smart card readers attached to the client device.

If no smart card reader is listed, check the configuration of the client device.

#### Related topics

- [Array properties \(array-wide\)](#)
- [Smart Card Protocol Engine properties](#)
- [Using smart cards with Windows applications](#)
- [Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop](#)

## Users are unable to copy and paste text or graphics

### Character applications

For character applications displayed through Secure Global Desktop, users should be able to copy and paste text to other applications.

If you are using the *classic webtop*, web browsers must support and use one of the signed [Java™ archives](#) supplied with Secure Global Desktop. Check that the browser has not been configured to disable support for Java archives.

### Windows and X applications

Users can only copy and paste text under certain conditions:

- Copy and paste for the array as a whole must be enabled on the [Array Properties](#) panel of Array Manager. Copy and paste is enabled by default.
- The user must be allowed to copy and paste. If the [Clipboard Access](#) attribute on person objects is enabled, then the user can copy and paste. If this attribute is set to Use parent setting, then the setting of any parent organizational unit or organization object is used. Copy and paste is enabled by default.
- To be able to paste data to another Windows or X application displayed through Secure Global Desktop, the source application (the application the data was copied from) must be configured to have a [Clipboard Security Level](#) that is lower than, or equal to, the target application. The default security level is 3.
- To be able to paste data to an application running on the client device, the source application must be configured to have a [Clipboard Security Level](#) that is lower than, or equal to, the client security level configured on the [Array Properties](#) panel of Array Manager. The default client security level is 3.

If these conditions are not met, users paste the following message instead of the copied data:

```
Sun Secure Global Desktop Software: Copied data not available to this application
```

### Graphics

You can only copy graphics from, or paste graphics to, Microsoft Windows 2000/2003 applications.

If you are using the *classic webtop*, you can only do this if you're using the Native Client for Microsoft Windows.

### Related topics

- [Using copy and paste with Secure Global Desktop](#)
- [Secure Global Desktop and Java archives](#)

## Users complain of poor performance with the Windows desktop

When using Windows Terminal Services, users may complain that the performance of the Windows desktop is poor. This can be caused by using animation effects and other desktop settings in the Windows session. Performance is affected because these features require more screen updates and can greatly increase the bandwidth used. The problem is more severe on slower connections.

The things that can cause these problems include:

- animated mouse cursors
- mouse cursor shadows
- screensavers
- animated icons in the notification area
- animated images in programs
- animated wallpaper and
- images used as wallpaper.

By default, the Secure Global Desktop Terminal Services Client (`ttatsc`) enables these features. You can turn off these features off by using one or more `-perf disable option protocol arguments (--protoargs)` for the Windows application object. The options are:

Option	Description
<code>wallpaper</code>	Disables the desktop wallpaper. Disabling the wallpaper can reduce the amount of data that has to be updated when users move items around the desktop.
<code>fullwindowdrag</code>	Disables the option to show the contents of a window while it is being moved.
<code>menuanimations</code>	Disables transition effects for menus and tooltips.
<code>theming</code>	Disables desktop themes.
<code>cursorshadow</code>	Disables the shadow on the mouse pointer.
<code>cursorsettings</code>	Disables mouse pointer schemes and customizations.

## Related topics

- [Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop](#)

## Users have problems displaying high color X applications

Several problems can occur when displaying high color X applications:

- User receives a "client not capable error"
- The X application fails with "can't allocate enough color planes" error (or similar)
- The colors appear strange
- The X application uses too much bandwidth
- The color quality declines when a session is shadowed
- 8-bit applications exit with a PseudoColor visual error

### User receives a "client not capable error"

If a user receives a "client not capable error", they are using an old version of the Sun Secure Global Desktop Native Client or they are not using the latest Secure Global Desktop Java™ archives. To be able to view 16 and 24-bit applications, they must upgrade to the latest version of the Native Client or make sure they download the latest archives.

### The X application fails with "can't allocate enough color planes" error (or similar).

If an X application fails to run and exits with errors such as "can't allocate enough color planes", the application probably only displays 8-bit color. Check the display specification of the application and adjust the color depth setting.

### The colors appear strange

If there are any problems with appearance in 16-bit or 24-bit color applications, set the quality to full, that is:

- 24 for 24-bit applications, and
- 16 for 16-bit applications.

This should correct any problems.

### The X application uses too much bandwidth

If bandwidth is critical, try quality levels 6 and 9. However there is no guarantee on the bandwidth saving or how badly the appearance will be affected.

## The color quality declines when a session is shadowed

If you shadow a user's session, either you or the user may experience a decline in the color quality.

If you and the user have different color depth settings, the color format will be converted and colors dithered. To avoid this, increase the color depth (`--depth`) of the Object Manager to 16-bit or 24-bit.

For the two sessions to match exactly both the color depth (`--depth`) and color quality (`--quality`) of the two sessions need to match. If the quality settings are `auto` or `best`, you may end up with different color quality levels to that of the user (for example if the user is on a low bandwidth connection and you have a high bandwidth connection).

## 8-bit applications exit with a PseudoColor visual error

If you run an 8-bit application within a 16 or 24-bit high color X application session, for example from a CDE desktop, you may find the application exits with an error such as `"Cannot find a matching 8-bit PseudoColor visual"`.

To fix this, change the color depth (`--depth`) of the X application to 16/8-bit or 24/8-bit so that it supports multiple color depths.

**Note** There are memory and performance effects of using these settings.

If the 8-bit application requires the primary color depth to be 8-bit (rather than 16 or 24-bit), use either the 8/16-bit or the 8/24-bit setting. If the application still exits, the only solution is to run the 8-bit application in a separate Secure Global Desktop session.

### Related topics

- [Color quality \(`--quality`\)](#)
- [Color depth \(`--depth`\)](#)

## Users see font problems

### Is the font size wrong?

Check the values of both the application object's [Monitor Resolution](#) attribute (in Object Manager) and the [X Protocol Engine's](#) Monitor Resolution attribute (in Array Manager).

### Are the wrong fonts displayed?

Using Array Manager, check that the [X Protocol Engine](#) Font Path is correct for every server in the array.

In general, the Font Path should be the same for all servers in an array.

#### Related topics

- [Monitor Resolution \(--dpi\)](#)
- [X Protocol Engine properties \(server-specific\)](#)
- [Introducing Object Manager](#)
- [Introducing Array Manager](#)



## Users see window clipping with Client Window Management applications

This means users are displaying applications on displays with greater resolution than expected.

In Array Manager, set the Client Window Management Maximum Width and Maximum Height attributes to the greatest display resolution you expect to support. You set these attributes in the [X Protocol Engine](#) properties for each server in the array independently.

**Note** Increasing the Maximum Width and Maximum Height attributes increases the memory requirements for Client Window Management applications on both client devices and Secure Global Desktop servers.

### Related topics

- [X Protocol Engine properties \(server-specific\)](#)
- [Display Using \(--displayusing\)](#)
- [Introducing Array Manager](#)

## Using copy and paste with Secure Global Desktop

### Read this topic to...

- Understand what copy and paste operations Secure Global Desktop supports.
- Understand how Secure Global Desktop Administrators can control copy and paste operations in Windows and X applications.

Users can copy and paste **text** between applications displayed through Secure Global Desktop. Users can also copy and paste text between applications running on a client device and applications displayed through Secure Global Desktop. Secure Global Desktop supports the copy and paste of Unicode characters.

Users can only copy and paste **graphics** to or from Microsoft Windows 2000/2003 applications. If you are using the *classic webtop*, users can only copy and paste graphics if they are using the Native Client for Microsoft Windows.

For **Windows and X applications**, you copy and paste by using the normal method for the application you are copying from, and then the normal method for the application you are pasting to.

For **character applications**, click with the right mouse button, and then click Copy or Paste as appropriate. To select a column of text in a character application, hold down the Shift key while selecting the text.

Secure Global Desktop Administrators have full control over copy and paste operations in Windows and X applications.

### Controlling copy and paste in Windows and X applications

Secure Global Desktop Administrators can control copy and paste operations in Windows and X applications displayed through Secure Global Desktop as follows:

1. On the [Array Properties](#) panel of Array Manager, copy and paste for the array as a whole can be enabled or disabled. By default, it is enabled.

2. The [Clipboard Access](#) attribute on organization, organizational unit or person objects can be used to control which users in the organization are allowed to use copy and paste. The setting for this attribute can be inherited from a parent object in the organizational hierarchy so that Administrators can enable or disable copy and paste for many users without having to edit each person object. By default, copy and paste is enabled.
3. Windows and X application objects can be assigned a [Clipboard Security Level](#). Users can only copy and paste data to an application displayed through Secure Global Desktop if it has the same security level or higher as the source application (the application the data was copied from). This allows Administrators to secure the data available through particular applications. The default security level is 3.
4. On the [Array Properties](#) panel of Array Manager, a security level can also be assigned to Secure Global Desktop clients. Data can only be copied from Secure Global Desktop to applications running on the client device if the client has the same security level or higher as the source application. This allows Administrators to secure the flow of data outside of Secure Global Desktop. The default client security level is 3.

When configuring security levels, the higher the number the higher the security level.

**Note** Character applications displayed through Secure Global Desktop are treated the same as applications running on the client. This is because character applications use the local client clipboard for copy and paste operations.

If a user attempts a copy and paste operation that is not permitted, for example because of differing security levels, they paste the following message instead of the copied data:

```
Sun Secure Global Desktop Software: Copied data not available to this
application
```

## Example

Copy and paste has been enabled for all users in the Indigo Insurance organization. In Array Manager, clients have a security level of 3 (the default).

In Object Manager, the following applications have been created with these security levels:

Application	Clipboard Security Level
XFinance	3
XClaim	4
Write-o-Win	4
Slide-o-Win	2

When Emma Rald runs these applications, she can perform the following copy and paste operations:

In this application	Emma can paste data from
XFinance	<ul style="list-style-type: none"><li>• Slide-o-Win (it has a lower security level).</li><li>• Applications running on her client device (client has equal security level).</li></ul>
XClaim	<ul style="list-style-type: none"><li>• XFinance and Slide-o-Win (they have a lower security level).</li><li>• Applications running on her client device (client has lower security level).</li><li>• Write-o-Win (it has an equal security level).</li></ul>
Write-o-Win	<ul style="list-style-type: none"><li>• XFinance and Slide-o-Win (they have a lower security level).</li><li>• Applications running on her client device (client has lower security level).</li><li>• XClaim (it has an equal security level).</li></ul>
Slide-o-Win	<ul style="list-style-type: none"><li>• Copy and paste not allowed (all applications and the client have a higher security level)</li></ul>

### Tips for Administrators

- To disable copy and paste from applications running on the client device to all applications displayed through Secure Global Desktop, the client security level must be **higher than** the highest security level applied to any application in the organizational hierarchy.
- To disable copy and paste from all applications displayed through Secure Global Desktop to applications running on the client device, the client security level must be **lower than** the lowest security level applied to any application in the organizational hierarchy.
- To disable all copy and paste operations for an individual Windows or X application accessed through Secure Global Desktop, disable copy and paste on the application.
- Inherit the copy and paste settings from other objects in the organizational hierarchy as much as possible. Only enable or disable copy and paste for individual users if you really have to. This reduces administration.
- For best results when copying and pasting non-ASCII text, run Secure Global Desktop in a UTF-8 locale.

### Related topics

- Array properties (array-wide)
- Clipboard Access (--clipboard)
- Clipboard Security Level (--clipboardlevel)
- Users are unable to copy and paste text or graphics

## Using shadowing to troubleshoot a user's problem

### Problem

A user is having difficulty with an application and they want you to troubleshoot their problem.

### Solution

Use Object Manager to find the user's session and then shadow it. Shadowing allows the user and a Secure Global Desktop Administrator to see and use the application simultaneously.

### Case study

Graham Green is working from home today and using Microsoft® PowerPoint® through Secure Global Desktop to create a Marketing presentation. He's having trouble with the presentation template and has contacted you for help. To fix the problem, you need to shadow Graham's emulator session.

You're logged in as a Secure Global Desktop Administrator and have Object Manager running. You know two things about the session you want to shadow: who's running it (Graham Green) and what application is involved (Microsoft PowerPoint). You can use either of these to locate the session. In this example, we will use the person. All session information for a user is shown on the Sessions tab for their person object.

### Solution

1. In Object Manager use the Search or Browse tabs to locate the person object for Graham Green and choose Properties.  
Properties for the object appear on the right of Object Manager.
2. Click the Sessions tab.  
The Sessions tab shows all the applications that Graham is currently running.
3. In the Emulator sessions part of the tab, click the session for the PowerPoint application, as this is the session we want to shadow.
4. Click Shadow Session.
5. Graham sees a dialog box, asking whether he wants to allow you to shadow the session.
6. Graham clicks Yes.  
A new window appears on your screen, showing Graham's running PowerPoint application. Both you and Graham can control the mouse pointer and use the application.

7. You fix Graham's problem and then close the shadowing window (don't close the application). Graham sees a dialog box telling him that no-one is currently shadowing the session.

## Next steps

- You could also have found Graham's session by searching or browsing for the PowerPoint application object and showing its Sessions tab. This shows everyone who's currently running PowerPoint.
- The Sessions tab shows other session information such as the date and time the session started, and whether the session is suspended or currently active.
- You can only shadow Windows and X applications.
- If the user has emulator sessions for two or more applications which are using [shared resources](#), all applications that are sharing resources will display when you shadow the session. The button bar on the shadowing window allows you to toggle between the applications.
- You can also shadow a user's session from the command line, see `tarantella emulatorsession shadow`.

## Related topics

- [Using shadowing in the classroom](#)
- [The tarantella emulatorsession shadow command](#)
- [Understanding webtop and emulator sessions](#)

## Using shadowing in the classroom

### Read this topic to...

- Learn how to configure application objects for use in a "virtual classroom".

You can use Secure Global Desktop shadowing to create a "virtual classroom" where the "pupils" in the classroom shadow an application being demonstrated by a "teacher".

To be able to do this, you have to create a teacher's application object and a "classroom" application object.

### Creating the teacher's application object

1. In Object Manager, create a new Windows or an X application object.
2. Configure the object how you want.
3. On the Advanced attributes panel, type one of the following in the [Login Script](#) box:
  - `unixclass.exp` if the application is an X application.
  - `winclass.exp` if the application is a Windows application.
4. Click Apply.
5. Select the application servers that can run the application, by dragging host objects on to the [Hosts tab](#) of the application object.
6. Add the application to the teacher's webtop by dragging the application object on to the [Links tab](#) for the teacher's person object.

### Creating the classroom application

1. In Object Manager, create a new X application object.

**Note** The classroom application is an X application even if the teacher's application is a Windows application.

2. In the [Application Command](#) box type:  
`/opt/tarantella/bin/bin/ttashadow`



3. In the **Arguments For Command** box type:  
`-readonly -silent -pointer $SHADOWDISPLAY`
4. From the **Color Depth** list select 16-bit - thousands of colors.
5. On the Advanced attributes panel, type `pupil.exp` in the **Login Script** box.
6. On the Advanced attributes panel, type the following in the **Environment Variables** box:  
`MYCLASS="TFN_name_of_teacher's_application"`  
for example, `MYCLASS=".../_ens/o=Indigo Insurance/ou=Finance/cn=XClaim"`
7. Configure the application object in any other way you want.
8. Click Apply.
9. Select the application servers that can run the application, by dragging host objects on to the **Hosts tab** of the application object. The `ttashadow` application is only available on hosts where Secure Global Desktop is installed.
10. Add the application to the webtops of all users in the class by dragging the application object on to the **Links tab** for the person/profile object(s).

## Notes

- The teacher must launch their application first, then the pupils launch their classroom application to shadow the teacher.
- The classroom can only shadow Windows or X applications.
- Only one person can use the teacher's application at any one time. If more than one person starts the teacher's application, the classroom will shadow the application that was started last. For this reason, we recommend you only give the teacher's application to one user. If you have several teachers, create separate application objects for each of them.
- The classroom application must have a **color depth** of at least 16-bit.
- The size of the classroom application should be at least the size of the teacher's application. We recommend the classroom displays in an independent window.
- When the teacher starts their application, information is stored on the Secure Global Desktop server about which application can be shadowed by the classroom. This information is **not** copied to the other members of the array. This means that if the classroom application is launched on a different Secure Global Desktop server to the teacher's application, the classroom launch will fail because the information about which application can be shadowed will not be available. You can use locations to guarantee that the teacher and classroom applications are launched on the same Secure Global Desktop server. You must set the location of the **host objects** and the **Secure Global Desktop server**. Otherwise, we recommend you only use classroom shadowing in a single server Secure Global Desktop array.

## Related topics

- Using shadowing to troubleshoot a user's problem
- The tarantella emulatorsession shadow command
- Understanding webtop and emulator sessions

[Secure Global Desktop Administration Guide](#) > [Users and authentication](#) > Using Windows Terminal Services, users are prompted for usernames and passwords too often

## Using Windows Terminal Services, users are prompted for usernames and passwords too often

### Is the wrong username or password cached?

The user may have typed the wrong username or password for the application server or Windows domain when prompted, and checked Save This Password to save the information in the password cache.

To fix, the user should press Shift when clicking the link to start (not resume) the application. This displays the authentication dialog again, and the user can correct their username and password.

### Why does this happen?

Secure Global Desktop sends username and password information to Windows Terminal Services to authenticate the user. If authentication fails, Windows prompts the user again. No information is returned to Secure Global Desktop indicating whether authentication succeeded or failed, and the details remain in the Secure Global Desktop password cache whether correct or incorrect.

### Is Windows 2000/2003 configured to always prompt?

By default, a Windows 2000 Server application server always prompts for a password when users log in, whether or not Secure Global Desktop supplies the password for the application server from its password cache. By default, a Windows 2003 Server does not prompt for passwords.

To fix, see [Configuring Windows Terminal Services for use with Secure Global Desktop](#).

#### Related topics

- [Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop](#)

## When X authorization is enabled, applications fail to start

In a default Secure Global Desktop installation, X authorization is enabled. If there are any problems with X authorization, users will not be able to start applications. If applications are failing to launch because of X authorization, the message "Failed to find xauth" or "Attempt to run xauth failed" will display in the application launch details dialog in the user's browser or Native Client.

Use the following checklist to establish why X authorization is causing application launches to fail:

### Is X authorization installed on the application server?

For Secure Global Desktop to be able to use X authorization, xauth must be installed on every application server.

If xauth is not installed, you must either install it or disable X authorization on the [Security properties](#) panel in Array Manager.

**Note** This disables X security for the entire array.

### Can Secure Global Desktop find the xauth binary?

If the message "Failed to find xauth" displays in the application launch dialog, Secure Global Desktop can't find the xauth binary. By default, Secure Global Desktop searches the following locations for the xauth binary:

- `/usr/bin/X11/xauth`
- `/usr/X/bin/xauth`
- `/usr/X11R6/bin/xauth`
- `/usr/bin/X/xauth`
- `/usr/openwin/bin/xauth`

If the xauth binary is in a different location, you must add its location to the `/opt/tarantella/var/serverresources/expect/vars.exp` [login script](#). Look for the line beginning `set xauthcmds`.

**Note** If the xauth binary is only in one location, you can

## Does the user have a UNIX account on the application server?

speed up application launches by removing the unnecessary locations from the `vars.exp` login script.

When the user starts an application, the Secure Global Desktop X Protocol Engine generates a cookie and stores it in the `.Xauthority` file in the user's home directory on the application server. The cookie is used to validate whether or not the user has permission to connect to the X display.

If the user does not have a home directory, the cookie cannot be stored in the user's `.Xauthority` file and so the user cannot be validated.

You can either:

1. Create a UNIX account for the user on the application server
2. Disable X authorization on the [Security properties](#) panel in Array Manager or
3. Edit the launch script so that the cookie is stored in a temporary directory.

The launch script you need to edit is `/opt/tarantella/var/serverresources/expect/procs.exp`.

Change the following line:

```
execute "[lindex $xauthcmds $i] add
$XDISPLAY . $xauthcookie\n"
```

to something like:

```
execute "[lindex $xauthcmds $i] -f /tmp/.
xauth$username add $XDISPLAY . $xauthcookie
\n"
```

## Further logging

If the checklist above does not help you resolve problems with X authorization, check the log file in `/opt/tarantella var/log`. The log file will be `execpePID_error.log`.

If this does not help, you can increase the amount of information that is logged. To do this, you need to amend the log filter on the Secure Global Desktop and enable debugging in the login script.

You amend the log filter by running the `tarantella config edit --tarantella-config-execpeconfig-logfilter` command. In a default installation, the following filters are set:

```
execpe/*/*error,pem/*/*error,launchhelper/*/*error
```

Change the filters to:

```
execpe/*/*,pem/*/*,launchhelper/*/*error
```

To enable debugging in the login script, edit the `/opt/tarantella/var/serverresources/expect/unix.exp` file and uncomment out the `startdebug` line.

### Related topics

- [Security properties \(array-wide\)](#)

## 3270 application object

- Use a 3270 application object if you want to put a **3270 application** on a webtop.
- To create a 3270 application object, use Object Manager or the `tarantella object new_3270app` command.
- Secure Global Desktop uses the third party TeemTalk® for Unix emulator for 3270 applications. See the [TeemTalk for Unix User's Guide](#) (in PDF format. [Download the Adobe Reader](#)) for details.
- The first time a user runs the emulator, the `tta3270.nv` config file is created in the user's home directory on the Secure Global Desktop host.

## Attributes

### General

- Name
- Description
- Arguments For Command
- Connection Method
- Resumable
- Session Ends When
- Max Instances
- Display Using
- Client's maximum size
- Scale to fit window
- Width
- Height
- Webtop Icon
- Webtop Hints

### 3270

- 3270 Host
- Port Number
- Close Telnet Action
- Keyboard Type

- Soft Button Levels
- Maximize the emulator window
- Enable menu bar
- Enable File and Settings menus
- Foreground Color
- Background Color

## **Appearance**

- Root Window
- Color

## **Adaptive Internet Protocol**

- Command Compression
- Command Execution
- Interlaced Images
- Use graphics acceleration
- Allow delayed updates

## **Directory Services Integration**

- LDAP Users
- LDAP Groups
- LDAP Search

## **Advanced**

- Environment Variables
- Window Manager
- Login Script
- Emulator Applet Page
- Resumable For
- Middle Mouse Timeout
- Window Close Action
- Euro Character
- Monitor Resolution
- Keep launch connection open



- [Lock keymap](#)
- [Share resources between similar sessions](#)

### Related topics

- [The tarantella object new\\_3270app command](#)

## 5250 application object

- Use a 5250 application object if you want to put a **5250 application** on a webtop.
- To create a 5250 application object use Object Manager or the `tarantella object new_5250app` command.
- Secure Global Desktop uses the third party TeemTalk® for Unix emulator for 5250 applications. See the [TeemTalk for Unix User's Guide](#) (in PDF format. [Download the Adobe Reader](#)) for details.
- The first time a user runs the emulator, the `teemx320.nv` config file is created in the user's home directory on the Secure Global Desktop host.

## Attributes

### General

- Name
- Description
- Arguments For Command
- Connection Method
- Resumable
- Session Ends When
- Max Instances
- Display Using
- Client's maximum size
- Scale to fit window
- Width
- Height
- Webtop Icon
- Webtop Hints

### 5250

- AS/400 Host
- Port Number
- Close Telnet Action
- Keyboard Type

- Soft Button Levels
- Maximize the emulator window
- Enable menu bar
- Enable File and Settings menus
- Foreground Color
- Background Color

## **Appearance**

- Root Window
- Color

## **Adaptive Internet Protocol**

- Command Compression
- Command Execution
- Interlaced Images
- Use graphics acceleration
- Allow delayed updates

## **Directory Services Integration**

- LDAP Users
- LDAP Groups
- LDAP Search

## **Advanced**

- Environment Variables
- Window Manager
- Login Script
- Emulator Applet Page
- Resumable For
- Middle Mouse Timeout
- Window Close Action
- Euro Character
- Monitor Resolution
- Keep launch connection open

- [Lock keymap](#)
- [Share resources between similar sessions](#)

### Related topics

- [Introducing Object Manager](#)
- [The tarantella object new\\_5250app command](#)
- [Character application object](#)

## Active Directory container object

- Use an Active Directory container object to replicate your Microsoft Active Directory structure within the Secure Global Desktop organizational hierarchy.
- To create an Active Directory container object use Object Manager or the `tarantella object new_container` command.

### Attributes

- [Name](#)

### Notes

- Use this object if you're using a Microsoft Active Directory server with the LDAP login authority, or you are using the Active Directory login authority, **and** your Active Directory structure uses container objects.
- Active Directory containers are similar to organizational units, but do not include additional Secure Global Desktop-specific attributes. In particular, Active Directory containers have no webtop content.

### Related topics

- [The LDAP login authority](#)
- [The Active Directory login authority](#)
- [Domain component object](#)
- [The tarantella object new\\_container command](#)
- [Mirroring your LDAP organization in ENS](#)
- [Using Directory Services Integration](#)

## Character application object

- Use a character application object if you want to put a **VT420, Wyse 60 or SCO Console character application** on a webtop.
- To create a character application object use Object Manager or the `tarantella object new_charapp` command.

## Attributes

### General

- Name
- Description
- Application Command
- Arguments For Command
- Load Balancing Algorithm
- Connection Method
- Emulation Type
- Terminal Type
- Resumable
- Max Instances
- Display Using
- Client's maximum size
- Width
- Height
- Columns
- Lines
- Webtop Icon
- Webtop Hints

### Appearance

- Font Family
- Font Size
- Fixed font size

- Wrap long lines
- Cursor
- Status Line
- Scroll Style
- Border Style

## **Behavior**

- Answerback Message
- Application key mode
- Keypad
- Cursor Keys
- Escape Sequences
- Code Page

## **Directory Services Integration**

- LDAP Users
- LDAP Groups
- LDAP Search

## **Advanced**

- Command Compression
- Environment Variables
- Login Script
- Keyboard Map
- Attribute Map
- Color Map
- Emulator Applet Page
- Resumable For
- Window Close Action

## **Hosts tab**

- Hosts

## **Notes**

- Character application objects support VT420, Wyse 60 or SCO Console character applications. The [Emulation Type](#) attribute determines the type of application.
- Depending on the Emulation Type setting, some of the other attributes will be ignored. In Object Manager, ignored attributes are disabled.
- To use and display the euro character, the terminal session must be capable of displaying 8-bit characters. To ensure this, enter the command `stty -istrip`. Also, the client device must be capable of entering the euro character.

### Related topics

- [Introducing Object Manager](#)
- [The tarantella object new\\_charapp command](#)



## Document object

- Use a document object if you want to put a **reference to a web page** on a webtop.
- To create a document object use Object Manager or the `tarantella object new_doc` command.

## Attributes

### General

- Name
- Description
- URL
- Open in new browser window
- Webtop icon
- Webtop Hints

### Directory Services Integration

- LDAP Users
- LDAP Groups
- LDAP Search

## Notes

- A document object can **refer to any URL**: not just HTML pages, but Microsoft Word documents, Adobe Acrobat files, or any other document available on the web. A document can also refer to a web application.
- Due to firewalls or other security mechanisms that may be in place, there may be **some restrictions** in the URLs a user can access from a particular location:
  - For users logging in to Secure Global Desktop using a web browser, the user's **current client device** fetches the URL.
  - For users logging in to Secure Global Desktop using the Sun Secure Global Desktop Native Client, **either the user's client device or the Secure Global Desktop server** fetches the URL (users can configure which is used).

## Related topics

- [Introducing Object Manager](#)
- [The tarantella object new\\_doc command](#)
- [Can I access a web application through Secure Global Desktop?](#)

## Domain component object

- Use a domain component object to replicate your Microsoft Active Directory structure within the Secure Global Desktop organizational hierarchy.
- To create a domain component object use Object Manager or the `tarantella object new_dc` command.

### Attributes

- [Name](#)

### Notes

- Use this object if you're using a Microsoft Active Directory server with the LDAP login authority, or you are using the Active Directory login authority, **and** your Active Directory structure uses domain component objects.
- Domain components are similar to organizational units, but do not include additional Secure Global Desktop-specific attributes. In particular, domain components have no webtop content.
- Domain components may only appear at the top of the organizational hierarchy, or within another domain component.

### Related topics

- [The LDAP login authority](#)
- [The Active Directory login authority](#)
- [Active Directory container object](#)
- [The tarantella object new\\_dc command](#)
- [Mirroring your LDAP organization in ENS](#)
- [Using Directory Services Integration](#)

## Group object

- Use a group object if you want to put **the same collection of objects on many unrelated webtops**, or if you want to **associate similar host objects for application server load balancing**.
- To create a group object use Object Manager or the `tarantella object new_group` command.

## Attributes

### General

- [Name](#)
- [Description](#)

### Directory Services Integration

- [LDAP Users](#)
- [LDAP Groups](#)
- [LDAP Search](#)

### Members tab

- [Members](#)

## Notes

- **Groups aren't the same as organizational units.** Objects may belong to only one organizational unit, but may be a member of many different groups.
- A group's members may include **any type of object, including other groups, from anywhere in the organizational hierarchy**.
- Members of a group may be moved or renamed without affecting group membership.
- Group objects can be added to a [Links tab](#) or a [Hosts tab](#) for an object.
  - For group objects added to a Links tab: **the group members are shown on the webtop (recursively) but not the group itself**.
  - For group objects added to a Hosts tab: **group members are used (recursively) for application server load balancing**.

## Related topics

- [Introducing Object Manager](#)
- [The tarantella object new\\_group command](#)
- [Introducing application server load balancing](#)

## Host object

- Use a host object to **represent an application server used with Secure Global Desktop**.
- To create a host object use Object Manager or the `tarantella object new_host` command.

## Attributes

- Name
- Description
- Address
- Windows NT Domain
- Available to run applications
- Authentication
- Location
- Host Locale

## Notes

- **Host objects are used with application server load balancing.** If you associate two or more host objects with one application object (by adding the host objects to the application object's [Hosts tab](#)), the Secure Global Desktop server will choose one of the host objects to use, based on the load across the application servers.
- You can group host objects together, for example by location or by platform, and load balance across all the application servers in the group by associating the [group object](#) with the application object.

### Related topics

- [Introducing Object Manager](#)
- [The tarantella object new\\_host command](#)
- [Introducing application server load balancing](#)



## Organization object

- Use an organization object for things that apply to your organization as a whole.

### Attributes

#### General

- Name
- Description
- Webtop Theme
- Profile Editing
- Clipboard Access
- Serial Port Mapping

#### Connections

- Connections

#### Client Drive Mapping

- Client Drive Mapping

#### Printing

- User-specific printing configuration
- Client printers
- Let users print to a PDF printer
- Let users print to a PDF local file
- Driver name
- Make PDF printer the default for Windows 2000/3
- Make PDF file printer the default for Windows 2000/3

#### Links tab

- Links



## Notes

- Organization objects are always at the top of the organizational hierarchy.
- All objects in your organization should belong to your organization object, or to an organizational unit within the organization.
- By default, objects on the organization's Links tab appear on the webtops of everyone in the organization.
- The organization object Secure Global Desktop System Objects contains objects related to essential Secure Global Desktop functionality. You may not rename, move or delete objects in this organization.

### Related topics

- [Introducing Object Manager](#)
- [Organizational unit object](#)
- [What is the Tarantella System Objects organization?](#)

## Organizational unit object

- Use an organizational unit (OU) object **to distinguish different departments, sites or teams in your organization.**
- To create an organizational unit object use Object Manager or the `tarantella object new_orgunit` command.

## Attributes

### General

- Name
- Description
- Webtop Theme
- Inherit parent's webtop content
- Profile Editing
- Clipboard Access
- Serial Port Mapping

### Connections

- Connections

### Client Drive Mapping

- Client Drive Mapping

### Printing

- User-specific printing configuration
- Client printers
- Let users print to a PDF printer
- Let users print to a PDF local file
- Driver name
- Make PDF printer the default for Windows 2000/3
- Make PDF file printer the default for Windows 2000/3

## Links tab

- [Links](#)

## Notes

- An organizational unit is a subdivision of an organization, such as a site or a department.
- By default, objects on the OU's Links tab appear on the webtops of everyone in the OU.
- You should base your organizational hierarchy around organizational units. It's best to reflect your organization's real structure. This makes it easy to set up appropriate webtop content, and to manage changes when users change job roles.

### Related topics

- [Introducing Object Manager](#)
- [The tarantella object new\\_orgunit command](#)
- [Organization object](#)

## Person object

- Use a person object **to represent a user in your organization, and give that user a webtop.**
- To create a person object use Object Manager or the `tarantella object new_person` command.

## Attributes

### General

- Name
- Description
- Surname
- Username
- Email address
- Preferred Locale
- Keyboard Map
- Windows NT Domain
- Bandwidth Limit
- Webtop Theme
- Inherit parent's webtop content
- Shared between users (guest)
- May log in to Secure Global Desktop
- Profile Editing
- Clipboard Access
- Serial Port Mapping

### Connections

- Connections

### Client Drive Mapping

- Client Drive Mapping

## Printing

- [User-specific printing configuration](#)
- [Client printers](#)
- [Let users print to a PDF printer](#)
- [Let users print to a PDF local file](#)
- [Driver name](#)
- [Make PDF printer the default for Windows 2000/3](#)
- [Make PDF file printer the default for Windows 2000/3](#)

## Links tab

- [Links](#)

## Notes

- Person objects are closely associated with webtops. Each person object has a Links tab in Object Manager, which defines the webtop.
- There are a number of different [user types](#). Some users may be able to log in to Secure Global Desktop even if they don't have a person object.
- You should put person objects in [organizational units](#) that reflect your organization's structure. This lets you define webtops more efficiently by placing department-wide applications on the webtop of the OU representing the department, and letting the person objects in that OU [inherit the OU's webtop](#).

### Related topics

- [Introducing Object Manager](#)
- [Login authorities](#)

## Windows application object

- Use a Windows application object if you want to put a **Microsoft Windows graphical application** on a webtop.
- To create a Windows application object use Object Manager or the `tarantella object new_windowsapp` command.

### Attributes

#### General

- Name
- Description
- Windows Protocol
- Try running from client first
- Windows NT Domain
- Application Command
- Arguments For Command
- Load Balancing Algorithm
- Connection Method
- Resumable
- Session Ends When
- Max Instances
- Display Using
- Client's maximum size
- Scale to fit window
- Width
- Height
- Color Depth
- Webtop Icon
- Webtop Hints
- Clipboard Security Level

#### Appearance

- Root Window
- Color
- Use Windows cursor

## **Adaptive Internet Protocol**

- Command Compression
- Command Execution
- Interlaced Images
- Use graphics acceleration
- Allow delayed updates

## **Directory Services Integration**

- LDAP Users
- LDAP Groups
- LDAP Search

## **Advanced**

- Environment Variables
- Window Manager
- Login Script
- Emulator Applet Page
- Protocol Arguments
- Resumable For
- Middle Mouse Timeout
- Window Close Action
- Euro Character
- Monitor Resolution
- Keep launch connection open
- Lock keymap

## **Hosts tab**

- Hosts

## **Notes**

- Not all attributes apply to all types of Windows application, and some attribute values are not valid for all types. Object Manager disables attributes that don't apply and restricts you to valid settings for the Windows application type.

### Related topics

- [Introducing Object Manager](#)
- [The tarantella object new\\_windowsapp command](#)



## X application object

- Use an X application object if you want to put **an X11 graphical application** on a webtop.
- To create an X application object use Object Manager or the `tarantella object new_xapp` command.

### Attributes

#### General

- Name
- Description
- Application Command
- Arguments For Command
- Load Balancing Algorithm
- Connection Method
- Resumable
- Session Ends When
- Max Instances
- Display Using
- Client's maximum size
- Scale to fit window
- Width
- Height
- Color Depth
- Webtop Icon
- Webtop Hints
- Clipboard Security Level

#### Appearance

- Root Window
- Color

#### Adaptive Internet Protocol

- Command Compression
- Command Execution
- Color Quality
- Interlaced Images
- Use graphics acceleration
- Allow delayed updates

## Directory Services Integration

- LDAP Users
- LDAP Groups
- LDAP Search

## Advanced

- Environment Variables
- Window Manager
- Login Script
- Emulator Applet Page
- Resumable For
- Middle Mouse Timeout
- Application supports 3-button mouse only
- Window Close Action
- Euro Character
- Monitor Resolution
- Keep launch connection open
- Lock keymap
- Share resources between similar sessions
- Enable X Security Extension

## Hosts tab

- Hosts

## Notes

- The following X extensions are supported:
  - BIG-REQUESTS

- BLINK
  - DAMAGE
  - DEC-XTRAP
  - DOUBLE-BUFFER
  - Extended-Visual-Information
  - GLX
  - MIT-SCREEN-SAVER
  - MIT-SHM
  - MIT-SUNDRY-NONSTANDARD
  - NATIVE-WND
  - RDP
  - RECORD
  - RENDER
  - SCO-MISC
  - SECURITY
  - SGI-GLX
  - SHAPE
  - SYNC
  - TOG-CUP
  - X-Resource
  - XC-APPGROUP
  - XC-MISC
  - XFIXES
  - XFree86-Bigfont
  - XTEST
  - XTTDEV
- A number of [X fonts](#) are supplied with Secure Global Desktop, and you may use your own fonts if you want.

## Related topics

- [Introducing Object Manager](#)
- [The tarantella object new\\_xapp command](#)

## 3270 Host (--hostname)

### Objects with this attribute

- [3270 application](#)

### Object Manager

Attribute name	Usage
3270 Host	In the box, type the DNS name (or IP address) of the 3270 (mainframe) host.

### Command line

Command option	Usage
<code>--hostname <i>host</i></code>	Replace <i>host</i> with the DNS name (or IP address) of the 3270 (mainframe) host.

### Description

This attribute names the 3270 (mainframe) host on which to run the application.

We recommend you use a DNS name rather than an IP address.

### Examples

```
--hostname warsaw.indigo-insurance.com
```

Runs the application on the 3270 host warsaw.indigo-insurance.com.

#### Related topics

- [3270 application object](#)
- [The tarantella object new\\_3270app command](#)



## Background Color (--3270bg) 3270

### Objects with this attribute

- [3270 Application](#)

### Object Manager

Attribute name	Usage
Background Color	Type a valid color resource, such as <code>yellow</code> .

### Command line

Command option	Usage
<code>--3270bg color</code>	Replace <i>color</i> with a valid color resource, such as <code>yellow</code> .

### Description

Specifies the background color of the 3270 application's text window.

Color names are resolved to RGB values using the file named in the [X Protocol Engine's RGB Database](#) attribute.

### Examples

```
--3270bg plum4
```

The background color of the text window is set to the color plum4.

### Related topics

- 3270 application object
- The tarantella object new\_3270app command

## Close Telnet Action (--3270tnclose) 3270

### Objects with this attribute

- [3270 Application](#)

### Object Manager

Attribute name	Usage
Close Telnet Action	Choose a telnet close option from the list.

### Command line

Command option	Usage
--3270tnclose 0 1 2 3	Specify one of the valid telnet close options (0=prompt, 1=exit, 2=reconnect, 3=close).

### Description

Specifies the course of action to be taken by the TeemTalk® for Unix emulator when the telnet connection to the 3270 (mainframe) host is closed. Options are:

- Prompt the user to choose one of the three options below.
- Exit TeemTalk for Unix, which means the Secure Global Desktop application session will be terminated.
- Attempt to reconnect to the 3270 host.
- Do nothing, just sit there with the TeemTalk for Unix interface showing.

### Related topics



- 3270 application object
- The tarantella object new\_3270app command

## Enable File and Settings menus (--3270si) 3270

### Objects with this attribute

- [3270 Application](#)

### Object Manager

Attribute name	Usage
Enable File and Settings menus	Check or clear the box.

### Command line

Command option	Usage
--3270si true false	Specify true or false.

### Description

Specifies whether or not the File and Settings menu items are enabled. When disabled, only the window resize buttons are displayed in the menu bar.

#### Related topics

- [3270 application object](#)
- [The tarantella object new\\_3270app command](#)

## Enable menu bar (--3270mb) 3270

### Objects with this attribute

- [3270 Application](#)

### Object Manager

Attribute name	Usage
Enable menu bar	Check or clear the box.

### Command line

Command option	Usage
--3270mb true false	Specify true (on) or false (off).

### Description

Specifies whether the 3270 application's menu bar is displayed or not.

#### Related topics

- [3270 application object](#)
- [The tarantella object new\\_3270app command](#)

## Foreground Color (--3270fg) 3270

### Objects with this attribute

- [3270 Application](#)

### Object Manager

Attribute name	Usage
Foreground Color	Type a valid color resource, such as <code>yellow</code> .

### Command line

Command option	Usage
<code>--3270fg color</code>	Replace <i>color</i> with a valid color resource, such as <code>yellow</code> .

### Description

Specifies the color of the text in the 3270 application's text window.

Color names are resolved to RGB values using the file named in the [X Protocol Engine's RGB Database](#) attribute.

### Examples

```
--3270fg plum4
```

The text in the text window is set to the color plum4.

### Related topics

- 3270 application object
- The tarantella object new\_3270app command

## Keyboard Type (--3270kt) 3270

### Objects with this attribute

- [3270 Application](#)

### Object Manager

Attribute name	Usage
Keyboard Type	Choose the keyboard type from the list.

### Command line

Command option	Usage
--3270kt pc sun4 sun5 hp	Specify one of the valid keyboard types.

### Description

Specifies the layout to use for mapping the keyboard to the terminal being emulated.

#### Related topics

- [3270 application object](#)
- [The tarantella object new\\_3270app command](#)

## Maximize the emulator window (--3270ma) 3270

### Objects with this attribute

- [3270 Application](#)

### Object Manager

Attribute name	Usage
Maximize the emulator window	Check or clear the box.

### Command line

Command option	Usage
--3270ma true false	Specify true or false.

### Description

Specifies whether the emulator window should be maximized.

These commands will cause the window to be displayed at the maximum size possible when the TeemTalk® for Unix emulator is loaded, while retaining the default number of lines and columns and including all window elements (such as the title bar and soft buttons) if enabled.

### Related topics

- [3270 application object](#)
- [The tarantella object new\\_3270app command](#)

## Port Number (--portnumber) 3270

### Objects with this attribute

- [3270 application](#)

### Object Manager

Attribute name	Usage
Port Number	In the box, type the TCP port number on which to connect to the 3270 host.

### Command line

Command option	Usage
<code>--portnumber</code> <code>tcp</code>	Replace <i>tcp</i> with the TCP port number on which to connect to the 3270 (mainframe) host.

### Description

This attribute specifies the TCP port used by the emulator to exchange data with the 3270 host.

By default, port 23/tcp is used.

See the [TeemTalk for Unix User's Guide](#) (in PDF format. [Download the Adobe Reader](#)) for details.

### Examples

```
--portnumber 4567
```

Connects on port 4567/tcp to the 3270 host.



## Related topics

- [3270 Host \(--hostname\)](#)

## Soft Button Levels (--3270bl) 3270

### Objects with this attribute

- [3270 Application](#)

### Object Manager

Attribute name	Usage
Soft Button Levels	Choose a setting from the list.

### Command line

Command option	Usage
--3270bl 0 1 2 3 4	Specify a level between 0 and 4.

### Description

Specifies how many levels of "soft buttons" are displayed.

#### Related topics

- [3270 application object](#)
- [The tarantella object new\\_3270app command](#)

## AS/400 Host (--hostname)

### Objects with this attribute

- [5250 application](#)

### Object Manager

Attribute name	Usage
AS/400 Host	In the box, type the DNS name (or IP address) of the AS/400 (mainframe) host.

### Command line

Command option	Usage
<code>--hostname</code> <code>host</code>	Replace <i>host</i> with the DNS name (or IP address) of the AS/400 host.

### Description

This attribute names the AS/400 host on which to run the application.

We recommend you use a DNS name rather than an IP address.

### Examples

```
--hostname warsaw.indigo-insurance.com
```

Runs the application on the AS/400 host warsaw.indigo-insurance.com.

#### Related topics

- [Port Number \(--portnumber\) 5250](#)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Background Color (--bg) 5250

### Objects with this attribute

- [5250 Application](#)

### Object Manager

Attribute name	Usage
Background Color	Type a valid color resource, such as <code>yellow</code> .

### Command line

Command option	Usage
<code>--bg color</code>	Replace <i>color</i> with a valid color resource, such as <code>yellow</code> .

### Description

Specifies the background color of the 5250 application's text window.

Color names are resolved to RGB values using the file named in the [X Protocol Engine's RGB Database](#) attribute.

### Examples

```
--bg plum4
```

The background color of the text window is set to the color plum4.

### Related topics

- Foreground Color (--fg) 5250
- Color (--rootcolor)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Close Telnet Action (--tnclose) 5250

### Objects with this attribute

- [5250 application](#)

### Object Manager

Attribute name	Usage
Close Telnet Action	Choose a telnet close option from the list.

### Command line

Command option	Usage
<code>--tnclose 0 1 2 3</code>	Specify one of the valid telnet close options (0=prompt, 1=exit, 2=reconnect, 3=close).

### Description

Specifies the course of action to be taken by the TeemTalk® for Unix emulator when the telnet connection to the AS/400 host is closed. Options are:

- Prompt the user to choose one of the three options below.
- Exit TeemTalk for Unix, which means the Secure Global Desktop application session will be terminated.
- Attempt to reconnect to the AS/400 server.
- Do nothing, just sit there with the TeemTalk for Unix interface showing.

### Related topics

- The tarantella object new\_5250app command



## Enable File and Settings menus (--si) 5250

### Objects with this attribute

- [5250 application](#)

### Object Manager

Attribute name	Usage
Enable File and Settings menus	Check or clear the box.

### Command line

Command option	Usage
--si true false	Specify true or false.

### Description

Specifies whether or not the File and Settings menu items are enabled. When disabled, only the window resize buttons are displayed in the menu bar.

### Related topics

- [The tarantella object new\\_5250app command](#)

## Enable menu bar (--mb) 5250

### Objects with this attribute

- [5250 application](#)

### Object Manager

Attribute name	Usage
Enable menu bar	Check or clear the box.

### Command line

Command option	Usage
--mb true false	Specify true (on) or false (off).

### Description

Specifies whether the 5250 application's menu bar is displayed or not.

### Related topics

- [The tarantella object new\\_5250app command](#)

## Foreground Color (--fg) 5250

### Objects with this attribute

- [5250 application](#)

### Object Manager

Attribute name	Usage
Foreground Color	Type a valid color resource, such as yellow.

### Command line

Command option	Usage
<code>--fg color</code>	Replace <i>color</i> with a valid color resource, such as yellow.

### Description

Specifies the color of the text in the 5250 application's text window.

Color names are resolved to RGB values using the file named in the [X Protocol Engine's RGB Database](#) attribute.

### Examples

```
--fg plum4
```

The text in the text window is set to the color plum4.

### Related topics

- Background Color (--bg) 5250
- Color (--rootcolor)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Keyboard Type (--kt) 5250

### Objects with this attribute

- [5250 application](#)

### Object Manager

Attribute name	Usage
Keyboard Type	Choose the keyboard type from the list.

### Command line

Command option	Usage
<code>--kt pc   sun4   sun5   hp</code>	Specify one of the valid keyboard types.

### Description

Specifies the layout to use for mapping the keyboard to the terminal being emulated.

#### Related topics

- [The tarantella object new\\_5250app command](#)
- [Terminal emulator keyboard maps](#)

## Maximize the emulator window (--ma) 5250

### Objects with this attribute

- [5250 application](#)

### Object Manager

Attribute name	Usage
Maximize the emulator window	Check or clear the box.

### Command line

Command option	Usage
--ma true false	Specify true or false.

### Description

Specifies whether the emulator window should be maximized.

These commands will cause the window to be displayed at the maximum size possible when the TeemTalk® for Unix emulator is loaded, while retaining the default number of lines and columns and including all window elements (such as the title bar and soft buttons) if enabled.

### Related topics

- [The tarantella object new\\_5250app command](#)



## Port Number (--portnumber) 5250

### Objects with this attribute

- [5250 application](#)

### Object Manager

Attribute name	Usage
Port Number	In the box, type the TCP port number on which to connect to the AS/400 host.

### Command line

Command option	Usage
<code>--portnumber tcp</code>	Replace <i>tcp</i> with the TCP port number to connect to on the AS/400 host.

### Description

This attribute specifies the TCP port used by the emulator to exchange data with the AS/400 host.

The default port number 23 can be substituted with any valid 16-bit port number.

See the [TeemTalk for Unix User's Guide](#) (in PDF format. [Download the Adobe Reader](#)) for details.

### Examples

```
--portnumber 4567
```

Connects on port 4567/tcp to the AS/400 host.

### Related topics



- AS/400 Host (--hostname)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Soft Button Levels (--bl) 5250

### Objects with this attribute

- [5250 application](#)

### Object Manager

Attribute name	Usage
Soft Button Levels	Choose a setting from the list.

### Command line

Command option	Usage
--bl 0 1 2 3 4	Specify a level between 0 and 4.

### Description

Specifies how many levels of "soft buttons" are displayed.

### Related topics

- [The tarantella object new\\_5250app command](#)

## Allow delayed updates (--delayed)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Allow delayed updates	Check or clear the box.

### Command line

Command option	Usage
<code>--delayed true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

This attribute specifies whether delayed updates of the display are allowed. This accumulates changes and can improve performance.

If your application's display must always be exact, you should clear the box (on the command line, use `--delayed false`). We recommend you turn off delayed updates for animation.

### Related topics

- Bandwidth Limit (--bandwidth)
- Command Compression (--compression)
- Command Execution (--execution)
- Interlaced Images (--interlaced)
- Use graphics acceleration (--accel)

## Color quality (--quality)

### Objects with this attribute

- [X application](#)

### Object Manager

Attribute name	Usage
Color Quality	Choose a setting from the list.

### Command line

Command option	Usage
<code>--quality automatic best 24 21 18 16 15 12 9 6</code>	Specify a valid setting.

### Description

The effective color depth displayed on client devices. Reducing color quality reduces bandwidth usage, but also reduces the number of colors which may be displayed.

**Note** If the [Color Depth](#) has been set to 8-bit, this attribute is not available. If the Color Depth has been set to 16-bit, only the 16-bit, 15-bit, 12-bit, 9-bit and 6-bit settings will be available.

The default setting `best` fixes the color depth at the most appropriate setting according to network conditions at the time the user starts the application. The color depth will not change while the session is running.

Specify `automatic` to allow the quality level to change at any time during the session depending on network conditions. This setting works within the following ranges:

- for 24 bit images - 12 to 24-bit color
- for 16 bit images - 12 to 16-bit color

The following table shows the effect on color quality of using a numeric quality setting:

Color quality setting	Approximate color quality for 16-bit applications	Approximate color quality for 24-bit applications
24	-	100%
21	-	88%
18	-	75%
16	100%	67%
15	94%	63%
12	75%	50%
9	56%	38%
6	38%	25%

The physical color quality of the client device is not forced to match that of the X session. If a 24-bit color session is being displayed on an 8-bit client device, the client will dither the image locally so that the session can be displayed reasonably.

## Examples

```
--quality 12
```

Sets the color quality to 12-bit color. If the Color Depth has been set to 24-bit, this reduces color quality to approximately 50% on client devices.

### Related topics

- [Color depth \(--depth\)](#)

## Command Compression (--compression)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)
- [Character application](#)

### Object Manager

Attribute name	Usage
Command Compression	Choose a setting from the list.

### Command line

Command option	Usage
<code>--compression automatic on off</code>	Specify a valid setting.

### Description

This attribute determines whether the Adaptive Internet Protocol compresses commands for transmission.

Choose Adjust Dynamically (`--compression automatic`) to allow compression to be turned on or off at any stage, according to the network conditions.

With some applications, compression incurs a greater overhead than transmitting commands uncompressed. You should turn off compression for these applications.

## Related topics

- [Bandwidth Limit \(--bandwidth\)](#)
- [Command Execution \(--execution\)](#)
- [Interlaced Images \(--interlaced\)](#)
- [Use graphics acceleration \(--accel\)](#)
- [Allow delayed updates \(--delayed\)](#)



## Command Execution (--execution)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Command Execution	Choose a setting from the list.

### Command line

Command option	Usage
<code>--execution automatic inorder optimized</code>	Specify a valid setting.

### Description

This attribute determines whether the Adaptive Internet Protocol always executes commands in order, or optimizes commands for performance reasons.

Choose Adjust Dynamically (`--execution automatic`) to allow the network conditions to determine the setting.

For some applications, for example those that use animation, the order in which commands are executed is critical.

When listing object attributes on the command line:

- the `inorder` attribute value displays as `on`.

- the `optimized` attribute value displays as `off`.

### Related topics

- [Bandwidth Limit \(--bandwidth\)](#)
- [Command Compression \(--compression\)](#)
- [Interlaced Images \(--interlaced\)](#)
- [Use graphics acceleration \(--accel\)](#)
- [Allow delayed updates \(--delayed\)](#)

## Interlaced Images (--interlaced)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Interlaced Images	Choose a setting from the list.

### Command line

Command option	Usage
<code>--interlaced automatic on off</code>	Specify a valid setting.

### Description

This attribute determines whether images are transmitted and displayed in a series of interlaced passes or in one pass from top to bottom.

Choose Adjust Dynamically (`--interlaced automatic`) to allow interlacing to be turned on or off at any stage, according to the network conditions.

Interlacing is recommended for graphics-intensive applications, particularly over low-bandwidth connections.

## Related topics

- [Bandwidth Limit \(--bandwidth\)](#)
- [Command Compression \(--compression\)](#)
- [Command Execution \(--execution\)](#)
- [Use graphics acceleration \(--accel\)](#)
- [Allow delayed updates \(--delayed\)](#)

## Use graphics acceleration (--accel)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Use graphics acceleration	Check or clear the box.

### Command line

Command option	Usage
<code>--accel true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

This attribute specifies whether acceleration is allowed. Acceleration optimizes how graphics are rendered and improves performance at the expense of smoothness and exactness. For example, colors may not always be exact.

If your application's display must always be exact, you should clear the box (on the command line, use `--accel false`).

### Related topics

- Bandwidth Limit (--bandwidth)
- Command Compression (--compression)
- Command Execution (--execution)
- Interlaced Images (--interlaced)
- Allow delayed updates (--delayed)

## Application supports 3-button mouse only (--force3button)

### Objects with this attribute

- [X application](#)

### Object Manager

Attribute name	Usage
Application supports 3-button mouse only	Check or clear the box.

### Command line

Command option	Usage
<code>--force3button true false</code>	Specify true or false.

### Description

This attribute lets you specify whether the X application only supports a 3-button mouse.

Check the box if the application only supports a 3-button mouse. The box is cleared by default.

### Examples

```
--force3button true
```

The application only supports a 3-button mouse.

Related topics
• <a href="#">Introducing Object Manager</a>





## Attribute Map (--attributemap)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Attribute Map	In the box, type the full pathname of the attribute map to use.

### Command line

Command option	Usage
--attributemap <i>attrmap</i>	Replace <i>attrmap</i> with the full pathname of the attribute map to use.

### Description

This attribute specifies the attribute map to use for the application. This maps attributes such as bold and underline to colors.

To use the default attribute map, leave the setting blank.

An example attribute map is installed in `/opt/tarantella/etc/data/attrmap.txt`.

### Examples

```
--attributemap /opt/tarantella/etc/data/myattrmap.txt
```

Uses the named attribute map.

## Related topics

- [Terminal emulator attribute maps](#)
- [Color Map \(--colormap\)](#)

## Color Map (--colormap)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Color Map	In the box, type the full pathname of the color map to use.

### Command line

Command option	Usage
<code>--colormap</code> <code>colormap</code>	Replace <i>colormap</i> with the full pathname of the color map to use.

### Description

This attribute specifies the color map to use for the application. A color map maps logical colors, Color\_1, Color\_2 and so on, to displayed colors.

To use the default color map, `/opt/tarantella/etc/data/colormap.txt`, leave the setting blank.

### Examples

```
--colormap /usr/local/maps/mycolormap.txt
```

Uses the named color map.

### Related topics

- Attribute Map (--attributemap)
- Terminal emulator color maps

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Enable X Security Extension (--securityextension)

### Objects with this attribute

- [X application](#)

### Object Manager

Attribute name	Usage
Enable X Security Extension	Check or clear the box.

### Command line

Command option	Usage
<code>--securityextension true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

Whether to enable the X Security Extension for the application.

The X Security Extension divides X clients (hosts) into trusted and untrusted clients. Untrusted clients cannot interact with windows and resources owned by trusted clients.

If you need to run an X application from a host that may not be secure, you should enable the X Security Extension and run the application in untrusted mode. This restricts the operations that the X application can perform in the X server and protects the display.

To run an application in untrusted mode:

1. Configure the X application to use SSH as the [connection method](#).
2. Configure [SSH to allow X11 forwarding](#).

**Note** Object Manager and Array Manager do not work correctly in untrusted mode. Do not enable the X Security Extension for these applications.

The X Security Extension only works with versions of SSH that support `-Y` option.

### Related topics

- [X application object](#)
- [Installing and using SSH with Secure Global Desktop](#)

## Environment Variables (--env)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Environment Variables	In the box, set the environment variables you want, one on each line. Press Return to add new entries.

### Command line

Command option	Usage
<code>--env <i>setting...</i></code>	Replace <i>setting</i> with an environment variable setting, of the form <code>VARIABLE=value</code> . To set more than one variable, use multiple <code>--env</code> arguments.

### Description

This attribute specifies any environment variable settings needed to run the application. For example, you may need to set `LD_LIBRARY_PATH` to access shared libraries.

You should quote an environment variable setting with a value containing spaces.

**Do not** set the `DISPLAY` variable: the display is set automatically for each user.

### Examples

```
--env LD_LIBRARY_PATH=/usr/lib "MY_VARIABLE=603 1769"
```

Runs the application with two environment variables set.

### Related topics

- [Arguments For Command \(--args\)](#)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.



## Emulator Applet Page (--empage)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Emulator Applet Page	In the box, type the filename of the emulator applet page to use.

### Command line

Command option	Usage
--empage <i>empage</i>	Replace <i>empage</i> with the filename of the emulator applet page to use.

### Description

This attribute specifies the filename of an emulator applet page: an HTML page containing a Secure Global Desktop emulator applet capable of displaying the application.

By default, graphical applications use `xde.html` and character applications use `tde.html`.

To let Secure Global Desktop choose an emulator applet page automatically, leave the setting blank.

To name your own page, specify either:

- A filename with no directory components, such as `xde.html`. These are considered relative to the [webtop theme](#) of the current user. This means that if you use more than one webtop theme in your organization, you should include the emulator applet page in each theme.
- A full URL, such as `http://www.indigo-insurance.com/empages/fancy.html`. The same page will be used whatever the user's webtop theme.

This attribute is only used by the classic and browser-based webtops if the application is configured to display on the webtop or in a new browser window (the [Display Using](#) attribute). It is ignored by the Sun Secure Global Desktop Native Client and for applications that do not display in a browser window.

## Examples

```
--empage my_xde.html
```

Uses the custom emulator applet page `my_xde.html` to display the application. A file with this name would need to be present in every webtop theme in use.

### Related topics

- [Display Using \(--displayusing\)](#)
- [Webtop Theme \(--webtop\)](#)

## Euro Character (--euro)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Euro Character	Choose a setting from the list.

### Command line

Command option	Usage
<code>--euro unicode iso8859-15</code>	Specify a valid setting.

### Description

This attribute specifies the keycode mapping required by the application to support the euro character. Most euro-compliant applications currently use iso8859-15. If in doubt, you should check your X application's documentation to see which method you should use.

To use the euro character with Secure Global Desktop, the client device must be capable of entering the character.

**Note** With the Sun Secure Global Desktop Native Client, you type the euro character using ALT GR+4. Typing ALT+0128 on the numeric keypad is not supported.

To display the euro character, you must configure your application to use an iso8859-15 font. Add one of the following to the [Arguments For Command](#) attribute:

```
-fn 5x7euro
```

```
-fn 6x10euro  
-fn 6x13euro  
-fn 6x13boldeuro  
-fn 7x13euro  
-fn 7x13boldeuro  
-fn 7x14euro  
-fn 7x14boldeuro  
-fn 8x13euro  
-fn 8x13boldeuro  
-fn 8x16euro  
-fn 9x15euro  
-fn 9x15boldeuro  
-fn 10x20euro  
-fn 12x24euro
```

This ensures the application will use the iso8859-15 fonts supplied with Secure Global Desktop. You can use your own fonts if you wish. However, to display the euro character they must be iso8859-15 compliant.

The application server must also support the euro character.

#### Related topics

- [What X fonts are installed?](#)
- [How do I use my own X fonts?](#)

## Keep launch connection open (`--keepopen`)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Keep launch connection open	Check or clear the box.

### Command line

Command option	Usage
<code>--keepopen true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

This attribute specifies whether to keep open the connection used to launch the application, or to close the connection.

Usually, you should clear the box (`--keepopen false`).

Check the box (`--keepopen true`) if users experience either of these symptoms:

- The application appears to start and then immediately exits.
- The application has problems shutting down (in this case, also set the [Session Ends When](#) attribute to Login Script Exits).

## Related topics

- [Session Ends When \(--endswhen\)](#)
- [Login scripts supplied with Secure Global Desktop](#)

## Keyboard Map (--keymap)

### Objects with this attribute

- [Person](#)
- [Character application](#)

### Object Manager

Attribute name	Usage
Keyboard Map	For person objects, select a setting from the list or type the pathname of a keyboard map file in the box. For Character applications, type the pathname of a keyboard map file in the box.

### Command line

Command option	Usage
<code>--keymap <i>keymap</i> default client-locale</code> <code>--keymap <i>keymap</i></code>	For person objects, use either <code>default</code> or <code>client-locale</code> or replace <i>keymap</i> with the pathname of a keyboard map file. For Character applications, replace <i>keymap</i> with the pathname of a keyboard map file.

### Description

This attribute specifies the pathname of a keyboard map file. You can use a full pathname or a relative pathname. Relative pathnames are relative to the `/opt/tarantella/etc/data/keymaps` directory.

### Person objects

The keyboard map file specified is used for all graphical applications started by this user.

To use a keyboard map based on the locale of the client device, select Use client's input locale. The actual keymap used is determined using the `/opt/tarantella/etc/data/keymaps/xlocales.txt` file.

**Note** You can use the `*` or `?` wildcards in the `xlocales.txt` file to support a range of input locales. See the `xlocales.txt` file for details.

To use the Secure Global Desktop server's [X Protocol Engine settings](#) configured in Array Manager to determine the keyboard map, select Use XPE setting.

Alternatively, to always use a particular keyboard map for this user, type a filename.

## Character application objects

The keyboard map file specified is used for this application.

Leave blank to use the default keyboard map for the application type. These are built-in to the emulators, but are equivalent to the keyboard maps in the files `ansikey.txt`, `vt420key.txt` and `w60key.txt` (all in `/opt/tarantella/etc/data/keymaps`).

## Examples

```
--keymap mykeymap.txt
```

Uses the named keymap, which is stored in `/opt/tarantella/etc/data/keymaps`.

### Related topics

- [X Protocol Engine properties \(server-specific\)](#)
- [Preferred Locale \(--preflocale\)](#)
- [Lock keymap \(--lockkeymap\)](#)
- [Terminal emulator keyboard maps](#)



## Lock keymap (--lockkeymap)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Lock keymap	Check or clear the box.

### Command line

Command option	Usage
<code>--lockkeymap true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

This attribute specifies whether an application is barred from changing the default keyboard mappings. Check the box to ensure the keyboard mappings may not be changed.

#### Related topics

- [Keyboard Map \(--keymap\)](#)

## Login Script (--login)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Login Script	In the box, type the filename of the login script to use.

### Command line

Command option	Usage
<code>--login</code> <code><i>script</i></code>	Replace <i>script</i> with the filename of the login script to use.

### Description

This attribute specifies the [login script](#) that runs to start this application. You should only change this setting if you're having problems with application start-up.

To let Secure Global Desktop choose a login script automatically, leave the setting blank.

You can use a full pathname or a relative pathname. Relative pathnames are considered relative to the value of the [Execution Protocol Engine's Login Script Directory](#) attribute.

The current working directory of the login script is the directory containing the script. If the script sources another script using a relative pathname, it's considered relative to this directory.

Detailed information on login scripts.

## Examples

```
--login my_login.exp
```

Uses the custom login script `my_login.exp` to launch the application.

### Related topics

- [What are login scripts?](#)
- [Login scripts supplied with Secure Global Desktop](#)
- [A login script returns an error](#)
- [Execution Protocol Engine properties \(server-specific\)](#)

## Middle Mouse Timeout (--middlemouse)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Middle Mouse Timeout	In the box, type a timeout in milliseconds.

### Command line

Command option	Usage
--middlemouse <i>ms</i>	Replace <i>ms</i> with a timeout in milliseconds.

### Description

This attribute lets you emulate the middle mouse button on a two-button mouse by clicking the left and right mouse buttons at the same time.

This setting is the maximum time that may elapse between pressing the left and the right mouse buttons for the action to be treated as a middle mouse button operation.

### Examples

```
--middlemouse 300
```

The left and right buttons must be pressed within 0.3 seconds for the operation to be considered as a middle mouse button operation.

### Related topics

- [Introducing Object Manager](#)

## Monitor Resolution (--dpi)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Monitor Resolution	In the box, type a resolution in dots per inch.

### Command line

Command option	Usage
<code>--dpi <i>dpi</i></code>	Replace <i>dpi</i> with a resolution in dots per inch.

### Description

This attribute specifies the monitor resolution (in dots per inch) that Secure Global Desktop reports to X applications asking for this information. Some X applications need this value to determine what font size to use.

If you leave this attribute blank, the value specified in the [X Protocol Engine's Monitor Resolution](#) attribute is reported.

The default resolution may cause the X application to choose a font size larger than it would normally choose. This can cause clipping problems as the X application may need more screen space than it otherwise would. If this happens, try reducing the resolution by typing a smaller value, for example 75.

The X application may also use too large a font if the X Protocol Engine's [Font Path](#) attribute uses a

different order than the console or X terminal.

## Examples

```
--dpi 75
```

Reports a resolution of 75dpi to X applications that need this information.

### Related topics

- [X Protocol Engine properties \(server-specific\)](#)

## Protocol Arguments (--protoargs)

### Objects with this attribute

- [Windows application](#)

### Object Manager

Attribute name	Usage
Protocol Arguments	In the box, type the command-line arguments for the Windows Protocol.

### Command line

Command option	Usage
<code>--protoargs</code> <code>args</code>	Replace <i>args</i> with the command-line arguments for the Windows Protocol.

### Description

This attribute specifies the command-line arguments to use with the [Windows Protocol](#).

The valid settings depend on the Windows Protocol.

### Examples

```
--protoargs "-dir c:\\mydir"
```

Sets the application's working directory to `c:\mydir`. This example applies to the Microsoft RDP protocol.

### Related topics



- Windows Protocol (--winproto)
- Arguments For Command (--args)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Resumable For (--resumetimeout)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Resumable For	In the box, type the number of minutes you want the application to be resumable for.

### Command line

Command option	Usage
<code>--resumetimeout</code> <i>mins</i>	Replace <i>mins</i> with the number of minutes you want the application to be resumable for.

### Description

This attribute lets you be sure that resources on the Secure Global Desktop host are used as efficiently as possible. It's used with the [Resumable](#) attribute to define when the Secure Global Desktop server will end a suspended emulator session.

Resumable attribute value	Resumable For behavior
Never	<i>Ignored</i>

Webtop session	If the user disconnects from the Secure Global Desktop server without logging out -- for example, if they close their web browser or it crashes -- a timer starts. Once the timer reaches the value of the Resumable For attribute, the Secure Global Desktop server will end the emulator session. (If the user logs out of Secure Global Desktop, the emulator session ends.)
Always	If the user disconnects from the Secure Global Desktop server in any way, including by logging out, a timer starts. Once the timer reaches the value of the Resumable For attribute, the Secure Global Desktop server will end the emulator session.

If you leave this setting blank, the default timeout for the Resumable setting is used. You can configure the default timeouts on the [Emulator Sessions](#) panel in Array Manager.

## Examples

```
--resumetimeout 30
```

Configures the application to be resumable for at least 30 minutes. This timeout would be appropriate for an application configured to be Webtop session resumable.

### Related topics

- [Resumable \(--resumable\)](#)
- [Understanding webtop and emulator sessions](#)
- [Emulator Sessions properties \(array-wide\)](#)

## Share resources between similar sessions (--share)

### Objects with this attribute

- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Share resources between similar sessions	Check or clear the box.

### Command line

Command option	Usage
<code>--share true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

This attribute specifies whether emulator sessions for applications configured to [Display Using](#) client window management try to share resources. Sharing sessions reduces the memory overhead on both the Secure Global Desktop server and the client device.

Resources are shared between applications with the same settings for these attributes:

- [Root Window](#)
- [Color](#)
- [Interlaced Images](#)
- [Use graphics acceleration](#)
- [Allow delayed updates](#)

- [Middle Mouse Timeout](#)
- [Monitor Resolution](#)

### Related topics

- [Display Using \(--displayusing\)](#)

## Window Close Action (--windowclose)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Window Close Action	Choose a setting from the list.

### Command line

Command option	Usage
<code>--windowclose notifyapp   killapp   suspendsession   endsession</code>	Specify a valid setting.

### Description

This attribute determines what happens if the user closes the main application window using the Window Manager decoration. This attribute only applies for applications that are configured to [Display Using](#) client window management or an independent window.

Object Manager	Command line	Description
----------------	--------------	-------------

Notify application	<code>notifyapp</code>	<ul style="list-style-type: none"> <li>• The application is notified of a close action in the normal way. If the application ignores the request, Secure Global Desktop kills it.</li> <li>• When listing object attributes on the command line, this attribute value displays as <code>notifyclient</code>.</li> <li>• This setting only applies to X applications that are configured to <a href="#">Display Using</a> client window management.</li> </ul>
Kill application	<code>killapp</code>	<ul style="list-style-type: none"> <li>• Secure Global Desktop kills the application. This is similar to using the program <code>xkill</code> to exit the application. You should use this setting only if your users are having difficulty closing an application.</li> <li>• When listing object attributes on the command line, this attribute value displays as <code>killclient</code>.</li> <li>• This setting only applies to X applications that are configured to <a href="#">Display Using</a> client window management.</li> </ul>
Suspend session	<code>suspendsession</code>	<ul style="list-style-type: none"> <li>• If the application object is <a href="#">resumable</a>, the application's emulator session is suspended. If the application object is not resumable, the emulator session ends. You should use this setting only if the application provides its own mechanism for the user to exit.</li> <li>• If you are using the Secure Global Desktop Client in Integrated mode, there are no controls for resuming a suspended application. Users have to log out and log in again to resume their applications, or display a webtop.</li> </ul>
End session	<code>endsession</code>	<ul style="list-style-type: none"> <li>• Secure Global Desktop ends the application's emulator session.</li> <li>• This is the default setting for Windows and character applications configured to <a href="#">Display Using</a> an independent window.</li> </ul>

**Note** If an emulator session contains several main application windows, for example a CDE session with several applications running, and this attribute is set to either Suspend Session or End Session, then closing any of the applications will result in the entire session being suspended or ended.

## Examples

```
--windowclose suspendsession
```

Closing the application's main window suspends the emulator session, as long as the application object is resumable.

### Related topics

- [Display Using \(--displayusing\)](#)
- [Understanding webtop and emulator sessions](#)



## Window Manager (--winmgr)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Window Manager	In the box, type a full pathname. Press Return to add new entries.

### Command line

Command option	Usage
<code>--winmgr command...</code>	Replace <i>command</i> with a full pathname. Separate each pathname with a space.

### Description

This attribute specifies any Window Manager to use for the application. You can also use this to name any other applications to run alongside the main application.

You can name as many applications as you want.

A Window Manager isn't needed for X applications configured to [Display Using Client Window Management](#), or for Windows applications that use the Microsoft RDP [Windows Protocol](#).

### Examples

```
--winmgr /usr/local/bin/twm
```

Runs the application with the twm Window Manager.

### Related topics

- [Application Command \(--app\)](#)
- [Arguments For Command \(--args\)](#)

## Border Style (--border)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Border Style	Choose a border style from the list.

### Command line

Command option	Usage
<code>--border normal   indented   raised</code>	Specify the border style you want.

### Description

This attribute determines whether the terminal window has a raised, indented or "flat" (normal) appearance.

### Examples

```
--border raised
```

The terminal window has a raised appearance.

### Related topics

- Cursor (--cursor)
- Scroll Style (--scrollstyle)
- Status Line (--statusline)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Color (--rootcolor)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Color	Type a valid color resource, such as <code>yellow</code> .

### Command line

Command option	Usage
<code>--rootcolor color</code>	Replace <i>color</i> with a valid color resource, such as <code>yellow</code> .

### Description

This attribute determines the color of the root window.

Color names are resolved to RGB values using the file named in the [X Protocol Engine's RGB Database](#) attribute.

### Examples

```
--rootcolor plum4
```

The root window uses the color plum4.

## Related topics

- [Root Window \(--roottype\)](#)
- [X Protocol Engine properties \(server-specific\)](#)

## Cursor (--cursor)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Cursor	Choose a cursor style from the list.

### Command line

Command option	Usage
<code>--cursor off   block   underline</code>	Specify the cursor style you want.

### Description

This attribute specifies how you want the cursor to appear within the application.

### Examples

```
--cursor underline
```

Uses an underline for the cursor.

Related topics
----------------

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.



## Fixed font size (--fixedfont)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Fixed font size	Check or clear the box.

### Command line

Command option	Usage
<code>--fixedfont true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

If this attribute is not checked (`--fixedfont false`), the emulator chooses a font size that fits the defined number of [Columns](#) and [Lines](#) into the [Width](#) and [Height](#) defined for the application. The application's [Font Size](#) is used as a minimum value.

If this attribute is checked (`--fixedfont true`), the [Font Size](#) defined is used, and scroll bars appear if necessary.

**Note** If this attribute is checked (`--fixedfont true`), the [Client's maximum size](#) attribute is ignored.

### Related topics

- Font Family (--font)
- Font Size (--fontsize)
- Width (--width)
- Height (--height)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Font Family (--font)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Font Family	Choose the font family from the list.

### Command line

Command option	Usage
<code>--font courier   helvetica   timesroman</code>	Specify a valid font family.

### Description

This attribute determines the font family used within the terminal window for the application.

Only Courier, Helvetica or Times Roman may be used. It is not possible to use any other font family.

### Examples

```
--font timesroman
```

Uses the Times Roman font in the application's terminal window.

### Related topics

- Font Size (--fontsize)
- Fixed font size (--fixedfont)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Font Size (--fontsize)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Font Size	In the box, type font size in points.

### Command line

Command option	Usage
<code>--fontsize</code> <code>points</code>	Replace <i>points</i> with the font size in points.

### Description

This attribute defines the font size in the terminal window, in the range 2-20 points.

### Examples

```
--fontsize 16
```

Uses a 16-point font in the terminal window.

#### Related topics

- [Font Family \(--font\)](#)
- [Fixed font size \(--fixedfont\)](#)



## Root Window (--roottype)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Root Window	Choose a setting from the list.

### Command line

Command option	Usage
<code>--roottype default   custom</code>	Specify a valid setting.

### Description

This attribute determines the appearance of the root window.

Choose Default Appearance (`--roottype default`) to show the standard X "root weave" pattern. Choose Custom Color (`--roottype custom`) and fill in the [Color](#) attribute (`--rootcolor`) to use your own color.

When listing object attributes on the command line, the `custom` attribute value displays as `color`.

### Examples

```
--roottype color
```

Uses a solid color for the root window, specified using `--rootcolor`.

## Related topics

- [Color \(--rootcolor\)](#)



## Scroll Style (--scrollstyle)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Scroll Style	Choose a scroll style from the list.

### Command line

Command option	Usage
<code>--scrollstyle line   multiple   smooth</code>	Specify the scroll style you want.

### Description

This attribute specifies how the terminal window scrolls: line-by-line, several lines at once, or smoothly.

When listing object attributes on the command line:

- the `line` attribute value displays as `normal`.
- the `multiple` attribute value displays as `jump`.

### Examples

```
--scrollstyle smooth
```

Scrolls smoothly.

### Related topics

- Border Style (--border)
- Cursor (--cursor)
- Status Line (--statusline)

## Status Line (--statusline)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Status Line	Choose a type of status line from the list.

### Command line

Command option	Usage
<code>--statusline none   indicator   hostmessages   standard   extended</code>	Specify the type of status line you want. Not all settings are valid for all types of character application.

### Description

This attribute specifies the type of status line to show for the application.

Application type	Types of status line available
VT420	<ul style="list-style-type: none"><li>• None</li><li>• Cursor position and print mode</li><li>• Messages from the host</li></ul>
Wyse 60	<ul style="list-style-type: none"><li>• None</li><li>• Standard</li><li>• Extended</li></ul>
SCO Console	<ul style="list-style-type: none"><li>• <i>Not applicable</i></li></ul>

When listing object attributes on the command line, the attribute value `hostmessages` displays as `host writable`.

## Examples

```
--statusline none
```

Doesn't display a status line.

### Related topics

- [Border Style \(--border\)](#)
- [Scroll Style \(--scrollstyle\)](#)
- [Cursor \(--cursor\)](#)
- [Emulation Type \(--emulator\)](#)

## Use Windows cursor (--wincursor)

### Objects with this attribute

- [Windows application](#)

### Object Manager

Attribute name	Usage
Use Windows cursor	Check or clear the box.

### Command line

Command option	Usage
<code>--wincursor true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

This attribute only applies if you are using the WinCenter [Windows Protocol](#) only. Although the WinCenter protocol is no longer supported, legacy windows application objects can continue to use it.

This attribute causes WinCenter to display the appropriate cursor from the Windows application in addition to the cursor from the client device. This means that the full range of Windows cursors is available to the application. However, the user sees two cursors being displayed: WinCenter shows a cursor, which is whatever the Windows application would show, and the client device displays its own cursor on top.

#### Related topics

- [Windows Protocol \(--winproto\)](#)



## Wrap long lines (--autowrap)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Wrap long lines	Check or clear the box.

### Command line

Command option	Usage
<code>--autowrap true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

This attribute determines the behavior when a user types characters extending beyond the right edge of the terminal window.

Check the box (on the command line, `--autowrap true`) to wrap the characters onto the next line.

Clear the box (on the command line, `--autowrap false`) to not display the characters. The characters **are** placed in the keyboard buffer.

### Related topics

- [Columns \(--cols\)](#)
- [Width \(--width\)](#)





## Answerback Message (--answermsg)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Answerback Message	In the box, type the text string to use.

### Command line

Command option	Usage
--answermsg <i>message</i>	Replace <i>message</i> with the text string to use.

### Description

This attribute defines the message to return when an inquiry is sent from the application server to the emulator.

This attribute applies to VT420 and Wyse 60 character applications only.

### Examples

```
--answermsg "My message"
```

Returns the text "My message" in response to an inquiry from the application server.

### Related topics

- Emulation Type (--emulator)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Application key mode (--appkeymode)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Application key mode	Check or clear the box.

### Command line

Command option	Usage
<code>--appkeymode true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

This attribute determines whether the application may change the codes generated by keys on the keyboard.

This attribute applies to Wyse 60 character applications only.

#### Related topics

- [Cursor Keys \(--cursorkeys\)](#)
- [Keypad \(--keypad\)](#)

## Code Page (--codepage)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Code Page	Choose a setting from the list.

### Command line

Command option	Usage
<code>--codepage 437   850   852   860   863   865   8859-1   8859-2   Multinational   Mazovia   CP852</code>	Specify a valid setting for the type of character application.

### Description

This attribute specifies the code page you want to use for the emulator. Different code pages are available for different types of character application.

Application type	Code pages available
SCO Console	<ul style="list-style-type: none"><li>• 437 - International</li><li>• 850 - Multilingual</li><li>• 852 - Central Europe</li><li>• 860 - Portuguese</li><li>• 863 - Canadian-French</li><li>• 865 - Danish-Norwegian</li></ul>

VT420	<ul style="list-style-type: none"><li>• 8859-1 - ISO Latin 1</li><li>• 8859-2 - ISO Latin 2</li></ul>
Wyse 60	<ul style="list-style-type: none"><li>• Multinational</li><li>• Mazovia</li><li>• CP852</li></ul>

To display the euro character with SCO Console applications, set this attribute to 850 - Multilingual.

## Examples

```
--codepage 8859-1
```

Uses the ISO 8859-1 code page, appropriate for a VT420 application.

### Related topics

- [Emulation Type \(--emulator\)](#)

## Cursor Keys (--cursorkeys)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Cursor Keys	Choose the cursor key behavior from the list.

### Command line

Command option	Usage
<code>--cursorkeys application   cursor</code>	Specify the cursor key behavior you want.

### Description

This attribute specifies the behavior of the cursor keys: whether they always generate cursor movement codes, or whether you want the application to change the codes generated by the cursor keys.

This attribute applies to VT420 character applications only.

### Examples

```
--cursorkeys cursor
```

The cursor keys always generate cursor movement codes.

### Related topics

- Application key mode (--appkeymode)
- Keypad (--keypad)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Escape Sequences (--escape)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Escape Sequences	Choose a setting from the list.

### Command line

Command option	Usage
<code>--escape 7-bit   8-bit</code>	Specify a valid setting.

### Description

This attribute specifies how escape sequences are sent from the emulator to the application server. Escape sequences may be sent as 7-bit or 8-bit control codes.

This attribute applies to VT420 character applications only.

### Examples

```
--escape 8-bit
```

Sends escape sequences using 8-bit control codes.

### Related topics



- Emulation Type (--emulator)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Keypad (--keypad)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Keypad	Choose the keypad behavior from the list.

### Command line

Command option	Usage
<code>--keypad numeric   application</code>	Specify the keypad behavior you want.

### Description

This attribute specifies the behavior of the numeric keypad, whether it always generates numbers or whether you want the application to change the codes generated by the keypad.

This attribute applies to VT420 character applications only.

### Examples

```
--keypad numeric
```

The keypad always generates numbers.

### Related topics

- Cursor Keys (--cursorkeys)
- Application key mode (--appkeymode)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Client Drive Mapping (--cdm)

### Objects with this attribute

- Organization
- Organizational unit
- Person

### Object Manager

Attribute name	Usage
Client Drive Mapping	Create as many client drive mapping specifications as you need, using the New and Delete buttons. Order them using the arrows.

### Command line

Command option	Usage
<code>--cdm drive_spec...</code>	Replace <i>drive_spec</i> with a drive mapping specification of the form <i>clientdrive:access:driveletter</i> . For example, <i>a:rw:z</i> . See below for more information. Separate each <i>drive_spec</i> with the "pipe" character, " ".

### Description

This attribute defines which drives on their Microsoft Windows client device a user may access from applications running on Microsoft Windows, UNIX and Linux application servers, and which drive letters to use on the application server for those drives.

The Client Drive Mapping attribute is an **ordered list** of drive mapping specifications. Each specification names:

- The client drive letter or type.
- The access rights to grant to the client drive.
- The drive letter to use on the application server to map to the client drive.

**Note** The first matching entry in the list is used, so make sure the most specific settings (for example, A or B) appear before more general settings (for example, All Drives).

The following tables show the values displayed in Object Manager for each part of a drive mapping specification, and the corresponding value to use on the command line.

For Client Drive:

Object Manager	Command line
All drives	<code>alldrives</code>
Fixed drives	<code>fixeddrives</code>
R/W removable	<code>rw</code>
R/O removable	<code>ro</code>
Network drives	<code>networkdrives</code>
A:, B: ... Z:	<code>a, b ... z</code>

For Access Rights:

Object Manager	Command line
Read-only	<code>ro</code>
Read-write	<code>rw</code>
None	<code>none</code>

For Drive Letter:

Object Manager	Command line
Same as client	<code>same</code>
A:, B: ... Z:	<code>a, b ... z</code>

## Examples

```
--cdm 'a:rw:z|networkdrives:rw:same'
```

---

For a person object, this means the user is given read-write access to drive A on their client device using drive Z on the application server, and also has read-write access to all network drives defined on their client device using the same drive letter used on the client.

The user might have access to other drives, for example a fixed drive C, depending on the Client Drive Mapping attributes for the person object's ancestors in the organizational hierarchy.

### Related topics

- [Configuring client drive mapping](#)
- [Array properties \(array-wide\)](#)
- [Remapping or hiding Windows 2000/2003 application server drives](#)
- [Users are having problems accessing client drives](#)

## Connections (--conntype)

### Objects with this attribute

- Organization
- Organizational unit
- Person

### Object Manager

Attribute name	Usage
Connections	Create as many connection type specifications as you need, using the New and Delete buttons. Order them using the arrows.

### Command line

Command option	Usage
<code>--conntype</code> <code>type_spec...</code>	Replace <i>type_spec</i> with a connection type specification of the form <i>client:server:type</i> . For example, <code>192.168.5.*:*:STD</code> . Separate each <i>type_spec</i> with the "pipe" character, " ".

### Description

This attribute defines, for ranges of DNS names or IP addresses, the connections that are allowed between the client device and the Secure Global Desktop server.

When a user logs in to a Secure Global Desktop server, the DNS names and IP addresses of the client device and the Secure Global Desktop server are used to determine the type of connection. First, the Connections attribute for that user's person object is checked. If there's no matching entry, the parent organizational unit's Connections attribute is checked, and so on up the organizational hierarchy to the organization object.

If there's no matching entry for the organization object, the user is given the best available connection.

Any connection may be denied if there is doubt over its validity, for example if a problem with a web

browser means the incorrect [TCP port](#) is used for the connection.

Processing of connection types is turned off by default, which lets users log in more quickly. You can turn on processing of connection types on the [Security](#) panel of Array Manager.

The Connections attribute is an **ordered list** of connection type specifications. Each specification names:

- The DNS name or IP address of a client device. Use the wildcards `?` and `*` to match more than one client device.
- The DNS name or IP address of a Secure Global Desktop server. Use the wildcards `?` and `*` to match more than one Secure Global Desktop server.
- The connection type.

In all cases, DNS names or IP addresses are considered **from the perspective of the Secure Global Desktop server** (they are [peer DNS names and IP addresses](#)). If your network is configured to use different names on each side of a firewall, you must use the names on the side of the Secure Global Desktop servers for this attribute.

These connection types are available:

Object Manager	Command line	Notes
Standard	STD	<ul style="list-style-type: none"><li>• Always available.</li></ul>
Secure	SSL	<ul style="list-style-type: none"><li>• Gives users a secure, SSL-based connection between their client device and the Secure Global Desktop server.</li><li>• Only available if Secure Global Desktop security services are enabled. If not, users configured to receive secure connections are given standard connections instead.</li></ul>
Deny	DENY	<ul style="list-style-type: none"><li>• Denies users access to the Secure Global Desktop server.</li><li>• Always available.</li></ul>

**Note** If security services have been enabled on the Secure Global Desktop server, all connections are secure until the user logs in. Once the user is known, the connection may be downgraded or denied.

## Examples

```
--conntype '192.168.5.*:::SSL|*:::STD'
```



For a person object, means the user is given a secure connection to all Secure Global Desktop servers if the client device has an IP address that starts 192.168.5, and a standard connection for all other client devices.

For an organizational unit or an organization object, these connection type specifications would be used only if no match was found for the client device and Secure Global Desktop server in the person object's Connections attribute.

### Related topics

- [Security and Secure Global Desktop](#)
- [What are Secure Global Desktop security services?](#)
- [Security properties \(array-wide\)](#)
- [Security properties \(server-specific\)](#)
- [How do I tell what connection type a user gets?](#)

## LDAP Groups (--ldapgroups)

### Objects with this attribute

- [Character application](#)
- [Document](#)
- [Group](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
LDAP Groups	Enter one or more distinguished names (DNs) of groups in an LDAP directory.

### Command line

Command option	Usage
<code>--ldapgroups</code> <code>group_dn...</code>	Enter one or more DN's of groups in an LDAP directory.

### Description

Allows you to give an application or group of applications to group of users that match the DN's of groups in an LDAP directory.

Use LDAP-style names for the list and use a comma (,) separator instead of a slash (/). See the example below.

If a group matches any of the groups in the LDAP directory server, the members of that group will receive the application or group of applications on their webtop. These applications are **in addition** to

any applications they would have on the webtop for their login profile.

The LDAP directory server used is the one specified on the [Secure Global Desktop Login](#) properties panel in Array Manager.

**Note** You may need to change the depth of the group search, if your organization uses [nested groups](#) (sub-groups).

## Examples

```
--ldapgroups cn=managers,ou=Sales,dc=indigo-insurance,dc=com cn=managers,  
ou=Marketing,dc=indigo-insurance,dc=com
```

Assigns the application or groups of applications to users in the managers group in the Sales and Marketing departments.

### Related topics

- [LDAP Search \(--ldapsearch\)](#)
- [LDAP Users \(--ldapusers\)](#)
- [The LDAP login authority](#)
- [The Active Directory login authority](#)
- [Using Directory Services Integration](#)

## LDAP Search (--ldapsearch)

### Objects with this attribute

- [Character application](#)
- [Document](#)
- [Group](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
LDAP Search	Enter one or more LDAP search strings.

### Command line

Command option	Usage
<code>--ldapsearch</code> <code>search_string...</code>	Enter one or more LDAP search strings.

### Description

Allows you to give an application or group of applications to the users that match the search criteria. The search criteria can be either:

- an [RFC2254](#)-compliant LDAP search filter or
- an [RFC1959](#)-compliant LDAP URL.

If you use an RFC2254 search filter, enclose each search criteria in double quotes and brackets (see the example below).

If you use an LDAP URL, we recommend you use the format `ldap:///search criteria` (see the example below). If you include the host, port and return attribute specification in the URL they will be ignored. This is because the LDAP directory server used is always the one specified on the [Secure Global Desktop Login](#) properties panel in Array Manager.

If a user matches any of the search criteria, they will receive the application or group of applications on their webtop. These applications are **in addition** to any applications they would have on the webtop for their login profile.

## Examples

```
--ldapsearch "(&(job=manager)(dept=Sales))" "(manager=Violet Carson)"
```

Assigns the application or groups of applications to any manager in the Sales department **and** anyone who has Violet Carson as their manager.

```
--ldapsearch "ldap:///ou=Sales,dc=indigo-insurance,dc=com??sub?job=manager"
```

Assigns the application or groups of applications to any manager in the Sales department of indigo-insurance.com.

### Related topics

- [LDAP Users \(--ldapusers\)](#)
- [LDAP Groups \(--ldapgroups\)](#)
- [The LDAP login authority](#)
- [The Active Directory login authority](#)
- [Using Directory Services Integration](#)

## LDAP Users (--ldapusers)

### Objects with this attribute

- [Character application](#)
- [Document](#)
- [Group](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
LDAP Users	Enter one or more distinguished names (DNs) of users in an LDAP directory.

### Command line

Command option	Usage
<code>--ldapusers</code> <code>user_dn...</code>	Enter one or more DN's of users in an LDAP directory.

### Description

Allows you to give an application or group of applications to the users that match the DN's of users in an LDAP directory.

Use LDAP-style names for the list and use a comma (,) separator instead of a slash (/). See the example below.

If a user matches any of the names in the LDAP directory server, they will receive the application or group of applications on their webtop. These applications are **in addition** to any applications they would

have on the webtop for their login profile.

The LDAP directory server used is the one specified on the [Secure Global Desktop Login](#) properties panel in Array Manager.

## Examples

```
--ldapusers uid=violet,ou=Sales,dc=indigo-insurance,dc=com uid=emmarald,  
ou=Marketing,dc=indigo-insurance,dc=com
```

Assigns the application or groups of applications to users with the UID "violet" in the Sales department and the UID "emmarald" in the Marketing department.

### Related topics

- [LDAP Search \(--ldapsearch\)](#)
- [LDAP Groups \(--ldapgroups\)](#)
- [The LDAP login authority](#)
- [The Active Directory login authority](#)
- [Using Directory Services Integration](#)

## Address (--address)

### Objects with this attribute

- [Host](#)

### Object Manager

Attribute name	Usage
Address	In the box, type a DNS name (recommended) or IP address.

### Command line

Command option	Usage
<code>--address</code> <code>address</code>	Replace <i>address</i> with a DNS name (recommended) or IP address.

### Description

This attribute specifies the network address of the application server.

We recommend you use a DNS name rather than an IP address.

### Examples

```
--address naples.indigo-insurance.com
```

Specifies the address of the application server as `naples.indigo-insurance.com`.

### Related topics



- Login scripts supplied with Secure Global Desktop

## Application Command (--app)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)

### Object Manager

Attribute name	Usage
Application Command	In the box, type the full pathname of the application.

### Command line

Command option	Usage
--app <i>pathname</i>	Replace <i>pathname</i> with the full pathname of the application.

### Description

This attribute specifies the application that runs when users click the link on their webtop.

The pathname must be the same on all [hosts that might run the application](#).

Notes:

- For any command-line arguments, use the [Arguments For Command](#) attribute.
- With X applications, use the [Window Manager](#) attribute to start a window manager for the application.
- With Windows applications, you can use a backslash `\` or a forward slash `/` between subdirectories. (On the command line you may need to escape backslashes: for example, `\\`).

- With Windows applications, you can set this attribute to "-" (a single hyphen) to start a full Microsoft Windows session rather than a particular application.
- On the command line, make sure you quote any pathnames containing spaces.

## Examples

```
--app /usr/local/bin/xfinance
```

Names a UNIX X application.

```
--app "c:/Program Files/Indigo Insurance/cash.exe"
```

Names a Windows application.

### Related topics

- [Introducing application server load balancing](#)
- [Arguments For Command \(--args\)](#)
- [Window Manager \(--winmgr\)](#)

## Arguments For Command (--args)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Arguments For Command	In the box, type the command-line arguments for the application.

### Command line

Command option	Usage
<code>--args args</code>	Replace <i>args</i> with the command-line arguments for the application.

### Description

This attribute specifies the command-line arguments to use when starting the application. (The [Application Command](#) attribute specifies the application that runs, without arguments.)

When specifying `--args` on the command line, you should quote the arguments.

For X applications, **do not** include the `-display` argument: the display is set automatically for each user.

### Examples

```
--args "-bg plum4"
```

Runs the application with command-line arguments to set the background color to "plum4".

### Related topics

- [Application Command \(--app\)](#)
- [Window Manager \(--winmgr\)](#)
- [Protocol Arguments \(--protoargs\)](#)
- [Environment Variables \(--env\)](#)

## Authentication (--auth)

### Objects with this attribute

- [Host](#)

### Object Manager

Attribute name	Usage
Authentication	Choose the setting you want from the list.

### Command line

Command option	Usage
<code>--auth trytta nevertrytta default</code>	Specify one of the valid settings.

### Description

This attribute specifies the policy for authenticating users on the application server, **if no password is already cached** for that server.

Object Manager	Command line	Description
Try Secure Global Desktop password if cached	<code>--auth trytta</code>	<p>If the user's password for logging in to Secure Global Desktop is cached, the same password is used to try to log in to the application server. If the attempt fails, the user is prompted for a password.</p> <p>When listing object attributes on the command line, this attribute value displays as <code>true</code>.</p>

<p>Don't try Secure Global Desktop password</p>	<pre>--auth nevertrytta</pre>	<p>The user's password for logging in to Secure Global Desktop is not used. The user is prompted to enter a username and password for the application server.</p> <p>When listing object attributes on the command line, this attribute value displays as <code>false</code>.</p>
<p>Use array-wide Application Launch setting</p>	<pre>--auth default</pre>	<p>The Try Secure Global Desktop Password If Cached setting configured in <a href="#">Application Launch properties</a> (in Array Manager) determines whether to try the user's password or not.</p> <p>When listing object attributes on the command line, this attribute value displays as <code>default</code>.</p>

A user's password for logging in to Secure Global Desktop may be stored in the password cache if a Secure Global Desktop server is also used as an application server, or if Save Secure Global Desktop Login Details In Cache is checked in [Application Launch properties](#) (in Array Manager).

## Examples

```
--auth trytta
```

Tries the password the user typed to log in to Secure Global Desktop, if it has been cached.

### Related topics

- [Application Launch properties \(array-wide\)](#)

## Available to run applications (--available)

### Objects with this attribute

- [Host object](#)

### Object Manager

Attribute name	Usage
Available to run applications	Check or clear the box.

### Command line

Command option	Usage
<code>--available true false</code>	Specify <code>-- available true</code> or <code>false</code> .

### Description

This attribute specifies whether applications can run on this application server.

Checking the box (`--available true`) allows applications to run. The box is checked by default. An application is started on the application server only if:

- the host object appears on the application object's [Hosts tab](#), and
- the application's load balancing algorithm chooses this application server.

Unchecking the box (`--available false`) means that no new applications can be started on the application server. Making an application server unavailable does not affect applications that are already running. If a user has a suspended application session on the application server and the application has been set up to be always resumable, the user will be able to resume their session.

You can use this attribute, for example, to make an application server temporarily unavailable while you



carry out maintenance work.

If the application server is the only server configured to run a particular application, then the application will not be available to users.

### Related topics

- [Introducing application server load balancing](#)
- [Configuring application server load balancing](#)

## Bandwidth Limit (--bandwidth)

### Objects with this attribute

- [Person](#)

### Object Manager

Attribute name	Usage
Bandwidth Limit	Choose the maximum bandwidth from the list.

### Command line

Command option	Usage
--bandwidth <i>bandwidth</i>	Replace <i>bandwidth</i> with the maximum bandwidth, in bits per second.

### Description

This attribute specifies the maximum bandwidth this person may use between the client device and the Secure Global Desktop server for X and Windows applications.

Choose None (on the command line, 0) to specify no limit: the person uses as much of the available bandwidth as possible. This gives the best application usability for the speed of the network connection.

You don't need to change this unless you have particular bandwidth restrictions: in normal use, we recommend you use None.

The table below shows the bandwidth options in Object Manager and the values you must use on the command line:

Object Manager	Command line
2400 bps	2400

4800 bps	4800
9600 bps	9600
14.4 Kbps	14400
19.2 Kbps	19200
28.8 Kbps	28800
33.6 Kbps	33600
38.8 Kbps	38800
57.6 Kbps	57600
64 Kbps	64000
128 Kbps	128000
256 Kbps	256000
512 Kbps	512000
768 Kbps	768000
1 Mbps	1000000
1.5 Mbps	1500000
10 Mbps	10000000
None	0

## Examples

```
--bandwidth 51200
```

Limits the person to a maximum bandwidth of 512 Kbps.

```
--bandwidth 0
```

Allows this person to use as much of the available bandwidth as possible.

## Related topics

- [Command Compression \(--compression\)](#)
- [Command Execution \(--execution\)](#)
- [Interlaced Images \(--interlaced\)](#)
- [Use graphics acceleration \(--accel\)](#)
- [Allow delayed updates \(--delayed\)](#)

## Color depth (--depth)

### Objects with this attribute

- [X application](#)
- [Windows application](#)

### Object Manager

Attribute name	Usage
Color Depth	Choose a setting from the list.

### Command line

Command option	Usage
<code>--depth 8   16   24   16/8   24/8   8/16   8/24</code>	Specify a valid setting.

### Description

The color depth for the application. The greater the number of colors, the more memory is required on the Secure Global Desktop server and on the client device, and the more network bandwidth is used between them.

The 16/8-bit, 24/8-bit, 8/16-bit and 8/24-bit settings are only available to X applications.

**Note** For Windows applications, only applications running on a Windows 2003 Server can be displayed using 16 or 24-bit color. By default, a Windows 2003 Server displays applications using 16-bit color. If the color depth setting of a Windows application object is different from that of the application server, Secure Global Desktop automatically adjusts the color depth to match the server setting.

### Reducing bandwidth usage for X applications

To reduce network bandwidth at greater color depths for X applications, change the [Color Quality](#)

setting.

## Support for X applications with multiple color depths

The 16/8-bit, 24/8-bit, 8/16-bit and 8/24-bit settings allow you to support X applications with multiple color depths. For example, if you need to run an 8-bit application in a 16 or 24-bit high color X application session (such as a CDE desktop), use either the 16/8-bit or the 24/8-bit setting.

These settings:

- will increase the amount of memory used on the Secure Global Desktop server (compared to an application using a single color depth):
  - the 8/16 setting will use 200% more memory
  - the 8/24 setting will use 400% more memory
  - the 16/8 setting will use 50% more memory and
  - the 24/8 setting will use 25% more memory
- will increase the amount of bandwidth used and
- may affect performance, particularly over low bandwidth connections.

## Examples

```
--depth 16
```

Sets the color depth for the application to 16-bit color (thousands of colors).

### Related topics

- [Color quality \(--quality\)](#)
- [Users have problems displaying high color X applications](#)

## Columns (--cols)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Columns	In the box, type the number of columns in the terminal window for the application.

### Command line

Command option	Usage
<code>--cols cols</code>	Replace <i>cols</i> with the number of columns in the terminal window.

### Description

This attribute defines the number of columns in the terminal window, in the range 5-132.

### Examples

```
--cols 80
```

Uses an 80-column window for the application.

Related topics
<ul style="list-style-type: none"><li>• <a href="#">Lines (--lines)</a></li><li>• <a href="#">Width (--width)</a></li><li>• <a href="#">Height (--height)</a></li></ul>

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.



## Client's maximum size (--maximize)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Client's maximum size	Check or clear the box.

### Command line

Command option	Usage
<code>--maximize true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

This attribute affects the initial size of the application.

Check the box (on the command line, `--maximize true`) to ensure the application fills the user's screen when it starts.

The application appears with window decoration. To cause an application to fill the screen completely, without window decoration, set the application object's [Display Using](#) attribute to Kiosk.

Clear the box (on the command line, `--maximize false`) to size the application according to the

object's [Width](#) and [Height](#) attributes

The application size doesn't change during the lifetime of the emulator session. If the user starts an application on one client device, then resumes the same application on a client device with a different screen resolution, the application does not resize to fit the screen.

**Note** If this attribute is checked (`--maximize true`) and the application is a character application, the [Fixed font size](#) attribute **must** be unchecked (`--fixedfont false`).

#### Related topics

- [Width \(--width\)](#)
- [Height \(--height\)](#)
- [Display Using \(--displayusing\)](#)

## Clipboard Access (--clipboard)

### Objects with this attribute

- [Organization](#)
- [Organizational unit](#)
- [Person](#)

### Object Manager

Attribute name	Usage
Clipboard Access	Pick a setting from the list.

### Command line

Command option	Usage
<code>--clipboard 2 1 0</code>	Specify 2 1 0.

### Description

This attribute [controls whether users can use copy and paste](#) in Windows or X application emulator sessions.

For a person object or organizational unit object, choose Use parent setting (on the command line, `--clipboard 2`) to inherit the setting of a parent object in the organizational hierarchy. This allows you to enable or disable copy and paste for many users without having to edit each person object.

For organization objects, the Use parent setting means use the array-wide setting configured on the [Array Properties](#) panel of Array Manager.

When a user starts a application, Secure Global Desktop checks the person object for the user and then any parent object further up the organizational hierarchy to see whether copy and paste is enabled or disabled. If all the objects checked are configured to use the parent's setting, then the array-wide default setting is used.

By default, copy and paste is allowed.

Command line	Array Manager
2	Use parent setting
1	Enabled
0	Disabled

Changes to this attribute only take effect for new emulator sessions.

## Examples

```
--clipboard 0
```

Disables copy and paste for a user's Windows or X application emulator sessions.

### Related topics

- [Using copy and paste with Secure Global Desktop](#)
- [Users are unable to copy and paste text or graphics](#)

## Clipboard Security Level (--clipboardlevel)

### Objects with this attribute

- [Windows application](#)
- [X application](#)

### Object Manager

Attribute name	Usage
Clipboard Security Level	Type a number in the box or pick from the list.

### Command line

Command option	Usage
<code>--clipboardlevel <i>level</i></code>	Replace <i>level</i> with the security level.

### Description

This attribute is used to [control user copy and paste operations](#) in Windows or X application emulator sessions.

Use this attribute to specify a security level. The security level can be any positive integer. The higher the number, the higher the security level.

You can only copy and paste data to an application if it has the same security level or higher as the source application (the application the data was copied from) .

Secure Global Desktop clients also have a security level. You can only copy and paste data to applications running on the client device if the client has the same security level or higher as the source application.

On the command line, specify `-1` to disable copy and paste operations.

The default security level is 3.

Changes to this attribute only take effect for new emulator sessions.

## Examples

```
--clipboardlevel 5
```

Sets the security level for an application to 5. You can only copy and paste data to this application if the source application or client has a security level of 5 or less.

### Related topics

- [Using copy and paste with Secure Global Desktop](#)
- [Users are unable to copy and paste text or graphics](#)

## Connection Method (--method)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Connection Method	Choose the connection method from the list.

### Command line

Command option	Usage
<code>--method rexec   telnet   ssh</code>	Specify one of the valid connection methods. Not all methods are available for all types of application.

### Description

This attribute specifies the mechanism used by the Secure Global Desktop server to access the application server and start the application.

The default connection method is `telnet`.

For character applications, only the connection methods `telnet` and `ssh` are allowed.

### Examples

```
--method telnet
```

Uses the `telnet` connection method to log in to an application server. This is the default if `--method` is not specified.

### Related topics

- [Installing and using SSH with Secure Global Desktop](#)



## Description (--description)

### Objects with this attribute

- [Character application](#)
- [Document](#)
- [Group](#)
- [Host](#)
- [Organization](#)
- [Organizational unit](#)
- [Person](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Description	In the box, type a description of the object.

### Command line

Command option	Usage
<code>--description</code> <code>text</code>	Replace <i>text</i> with a description of the object.

### Description

This attribute describes the object. You can use this for anything you wish as the Secure Global Desktop server ignores it.

Descriptions can include any characters you want. On the command line, make sure you quote any

descriptions containing spaces.

## Examples

```
--description "The intranet for Indigo Insurance"
```

Describes the object. You might use this description with a document object, for example.

### Related topics

- [Name \(--name\) objects with "common name"](#)

## Display Using (--displayusing)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Display Using	Pick a setting from the list.

### Command line

Command option	Usage
<code>--displayusing webtop   clientwm   newbrowser   independent   kiosk   localx   seamless</code>	Specify one of the valid settings. Not all settings are available for all types of application.

### Description

This attribute determines how the application is displayed to the user. Some settings affect other attributes. For example, in Object Manager choosing Client Window Management disables the attributes for configuring the application's size. On the command line you may specify these other attributes, but they have no effect.

Object Manager	Command line	Applies to	Description
----------------	--------------	------------	-------------

Webtop	<code>webtop</code>	All application types	<ul style="list-style-type: none"> <li>• The application appears on the webtop, alongside the links, embedded within the web page defined in the object's <a href="#">Emulator Applet Page</a> attribute.</li> <li>• Pressing the CONTROL key while clicking a webtop link forces the application to display in an independent window instead.</li> <li>• When listing object attributes on the command line, this attribute value displays as <code>mainbrowser</code>.</li> <li>• If the Secure Global Desktop Client is operating in Integrated mode or Java™ technology is not available, an independent window is used instead.</li> </ul>
Client window management	<code>clientwm</code>	X applications	<ul style="list-style-type: none"> <li>• The application's windows behave in the same way as those of applications running on the client device. For example, the windows may be resized, moved, minimized and maximized using the client's normal window management controls.</li> <li>• The object's <a href="#">Window Close Action</a> attribute determines what happens when the user closes the application's last or main window.</li> <li>• Pressing the CONTROL key while clicking a webtop link has no effect on the application display.</li> <li>• When listing object attributes on the command line, this attribute value displays as <code>multiplewindows</code>.</li> <li>• <b>Recommended for</b> applications with many top-level resizable windows.</li> </ul>

New browser window	<code>newbrowser</code>	All application types	<ul style="list-style-type: none"> <li>• The application appears in a new web browser window, embedded within the web page defined in the object's <a href="#">Emulator Applet Page</a> attribute.</li> <li>• Pressing the CONTROL key while clicking a link on a webtop forces the application to display on the webtop instead.</li> <li>• If the Secure Global Desktop Client is operating in Integrated mode or Java™ technology is not available, an independent window is used instead.</li> </ul>
Independent window	<code>independent</code>	All application types	<ul style="list-style-type: none"> <li>• The application appears in a new window, without any web browser toolbars or menus.</li> <li>• This window may be resized, but this does not resize the application: the window will include scrollbars. The object's <a href="#">Width</a> and <a href="#">Height</a> attributes determine the size of the application.</li> <li>• Closing the window may end or suspend the emulator session, depending on the object's <a href="#">Window Close Action</a> attribute.</li> <li>• Pressing the CONTROL key while clicking a link on a webtop forces the application to display on the webtop instead.</li> <li>• When listing object attributes on the command line, this attribute value displays as <code>awtwindow</code>.</li> <li>• <b>Recommended for Windows applications.</b></li> </ul>

Kiosk	<code>kiosk</code>	Character, X and Windows applications	<ul style="list-style-type: none"> <li>• The application appears full-screen, with no window decoration.</li> <li>• Users may not resize or move the window.</li> <li>• Pressing the CONTROL key while clicking a webtop link has no effect on the application display.</li> <li>• <b>Recommended for</b> full-screen desktop sessions.</li> </ul>
Local X server	<code>localx</code>	X and Windows applications	<ul style="list-style-type: none"> <li>• The application is displayed using an X server installed on the client device, if one is available. Otherwise, an independent window is used.</li> <li>• Applications configured with this setting are <b>not resumable</b> (even if an independent window is used).</li> <li>• The client device X server's host access control must grant access to the application server. See your X server's documentation for information about host access control.</li> <li>• Pressing the CONTROL key while clicking a link on a webtop forces the application to display on the webtop instead.</li> </ul>
Seamless window	<code>seamless</code>	Windows applications	<ul style="list-style-type: none"> <li>• The application's windows behave like an application running on a Windows application server, see <a href="#">Using seamless windows for Windows applications</a>.</li> <li>• If an application is launched in a seamless window, you can toggle between a seamless and independent window by pressing the SCROLL LOCK key.</li> <li>• Pressing the CONTROL key while clicking a webtop link has no effect on the application display.</li> </ul>

			<ul style="list-style-type: none"><li>• When listing object attributes on the command line, this attribute value displays as <code>seamlesswindows</code>.</li><li>• <b>Not recommended for full-screen desktop sessions:</b> use a kiosk or independent window instead.</li></ul>
--	--	--	--

## Examples

```
--displayusing newbrowser
```

Displays the application in a new web browser window, within a web page.

```
--displayusing independent
```

Displays the application in an independent window.

### Related topics

- [Open in new browser window \(--newbrowser\)](#)
- [Emulator Applet Page \(--empage\)](#)
- [X Protocol Engine properties \(server-specific\)](#)
- [Understanding webtop and emulator sessions](#)

## Email Address (--email)

### Objects with this attribute

- [Person](#)

### Object Manager

Attribute name	Usage
Email Address	In the box, type the person's email address.

### Command line

Command option	Usage
--email <i>email</i>	Replace <i>email</i> with the person's email address.

### Description

This attribute specifies a person's email address, in the form *name@domain*.

A [login authority](#) may use this attribute for identifying users.

### Examples

```
--email indigo@indigo-insurance.com
```

Defines the email address of the person as `indigo@indigo-insurance.com`.

### Related topics



- Name (--name) objects with "common name"
- Username (--user)
- Login authorities

## Emulation Type (--emulator)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Emulation Type	Choose the emulation type from the list.

### Command line

Command option	Usage
<code>--emulator scoconsole   vt420   wyse60</code>	Specify the correct emulation type.

### Description

This attribute identifies the type of emulation required for the application: SCO Console, VT420 or Wyse 60. You should also set the correct [Terminal Type](#).

Not all character application attributes apply to all emulation types. In Object Manager, choosing an emulation type will enable and disable other attributes for the object.

### Examples

```
--emulator wyse60
```

Uses Wyse 60 terminal emulation for the application.

### Related topics

- Terminal Type (--termtype)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Height (--height)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Height	In the box, type the height of the application in pixels.

### Command line

Command option	Usage
<code>--height <i>pixels</i></code>	Replace <i>pixels</i> with the height of the application, in pixels.

### Description

This attribute defines the height of the application, in pixels. The minimum height is 10 pixels, the maximum 65535 pixels.

On the command line you must specify the height even if this attribute is not required, for example because the application is configured to [Display Using](#) client window management or to display at the [Client's Maximum Size](#).

### Examples

```
--height 600
```

Uses a 600-pixel high window to display the application.

## Related topics

- [Client's maximum size \(--maximize\)](#)
- [Width \(--width\)](#)
- [Display Using \(--displayusing\)](#)

## Host Locale (--hostlocale)

### Objects with this attribute

- [Host](#)

### Object Manager

Attribute name	Usage
Host Locale	In the box, type type a locale.

### Command line

Command option	Usage
--hostlocale <i>ll_tt</i>	Replace <i>ll_tt</i> with a locale.

### Description

This attribute controls the language used in the login scripts when pattern matching login data from a host.

When using the [login scripts supplied with Secure Global Desktop](#), the `vars.exp` script defines variables for matching system prompts. By default, English system prompts are supported. This script can be customized to [support users in other locales](#).

A locale has two parts, a *language* and an **optional territory**, separated by an underscore.

- The language part of a locale is specified using ISO 639 language codes, for example `en` for English or `ja` for Japanese.
- The territory part of a locale is specified using ISO 3166 territory codes, for example `us` for the United States or `jp` for Japan.

By default, the locale is `en_us`.

### Examples

```
--locale fr
```

Sets the default language of the host object to French. French prompts must be configured in the login scripts used with this host.

### Related topics

- [Working with users in different locales](#)
- [What are login scripts?](#)

## Inherit parent's webtop content (--inherit)

### Objects with this attribute

- [Organizational unit](#)
- [Person](#)

### Object Manager

Attribute name	Usage
Inherit parent's webtop content	Check or clear the box.

### Command line

Command option	Usage
<code>--inherit true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

This attribute determines whether the webtop content for the object also includes the webtop content for the object's parent in the organizational hierarchy.

Depending on this attribute's setting in the parent object, the aggregation of webtop content may continue up the hierarchy to the organization object.

#### Related topics

- [Links tab \(--links\)](#)





## Lines (--lines)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Lines	In the box, type the number of lines in the terminal window for the application.

### Command line

Command option	Usage
<code>--lines</code> <code>lines</code>	Replace <i>lines</i> with the number of lines in the terminal window.

### Description

This attribute defines the number of lines in the terminal window, in the range 5-100.

### Examples

```
--lines 25
```

Uses a 25-line window for the application.

#### Related topics

- [Columns \(--cols\)](#)
- [Width \(--width\)](#)
- [Height \(--height\)](#)



## Load Balancing Algorithm (--loadbal)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)

### Object Manager

Attribute name	Usage
Load Balancing Algorithm	Pick a setting from the list.

### Command line

Command option	Usage
<code>--loadbal default   cpu   memory   sessions</code>	Specify a setting.

### Description

When the application is launched, this setting determines the algorithm Secure Global Desktop uses to choose the best application server on which to run the application. The server is selected from those defined on the application object's [Hosts tab](#).

Object Manager	Command line	Description
Use array-wide setting	<code>default</code>	Use the default algorithm defined on the <a href="#">Load Balancing Properties</a> panel of Array Manager
Least CPU usage	<code>cpu</code>	Choose the application server with the most CPU idle time.

Most free memory	<code>memory</code>	Choose the application server with the most free memory.
Fewest application sessions	<code>sessions</code>	Choose the application server that is running the fewest application sessions through Secure Global Desktop.

**Note** To use the Least CPU usage and Most free memory algorithms, you must also install the Sun Secure Global Desktop Enhancement Module on the application server.

## Examples

```
--loadbal memory
```

When launching the application, use the application server with the most free memory.

### Related topics

- [Introducing application server load balancing](#)
- [Configuring application server load balancing](#)

## Location (--location)

### Objects with this attribute

- [Host](#)

### Object Manager

Attribute name	Usage
Location	In the box, type the location of the application server.

### Command line

Command option	Usage
<code>--location</code> <code>location</code>	Replace <i>location</i> with the location of the application server.

### Description

This attribute specifies the location of the application server, for intelligent array routing. The value is used with [application server load balancing](#) to ensure optimal performance for users.

You can use any string, for example "Scandinavia" or "US-East". Application server load balancing tries to choose an application server and Secure Global Desktop array member with the same location, to minimize the "network distance" between them and maximize performance. (The connection between the user's client device and the Secure Global Desktop server uses the Adaptive Internet Protocol, which adapts to the network conditions.)

You should leave this attribute blank unless you use an array spanning a WAN (or one that includes slow links) and you use the intelligent array routing load balancing feature. More than one string is allowed, but this slows application launch.

If used, you should set this attribute on all appropriate host objects, and for all array members (using the server-specific [General](#) panel in Array Manager).

## Examples

```
--location Peckham
```

Locates the application server in Peckham.

### Related topics

- [Introducing application server load balancing](#)
- [General properties \(server-specific\)](#)

## Max Instances (--maxinstances)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Max Instances	Type a number or pick from the list.

### Command line

Command option	Usage
<code>--maxinstances 0   instances</code>	Specify 0 or replace <i>instances</i> with the number of instances.

### Description

This attribute allows you to set the maximum number of instances of an application a user can run simultaneously. The default is 3.

**Note** The ability to launch multiple application instances is only available to the browser-based webtop.

The application's link on the webtop indicates how many instances of the application the user can run. The webtop also provides tools for suspending, resuming or ending each application instance.

On the command line, use 0 to set the maximum number of instances to unlimited.



## Examples

```
--maxinstances 0
```

Sets the maximum number of instances of the application to unlimited.

### Related topics

- [Understanding webtop and emulator sessions](#)

## May log in to Secure Global Desktop (--enabled)

### Objects with this attribute

- [Person](#)

### Object Manager

Attribute name	Usage
May log in to Secure Global Desktop	Check or clear the box.

### Command line

Command option	Usage
<code>--enabled true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

This attribute specifies whether someone may log in using this person object.

Clear the box (on the command line, `--enabled false`) to deny a user access to their webtop temporarily.

This attribute is always checked for [profile objects](#): users may always log in using the profile object, as long as the appropriate [login authority](#) is available (configured in [Secure Global Desktop Login properties](#) in Array Manager).

To deny access to all users of a particular type, turn off the appropriate [login authority](#).

To stop all users from logging in to a particular Secure Global Desktop server, set Secure Global Desktop Login to Not Allowed in the [General properties](#) pane for that server in Array Manager

## Related topics

- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)
- [General properties \(server-specific\)](#)

## Name (--name) objects with "common name"

### Objects with this attribute

- [Active Directory container](#)
- [Character application](#)
- [Document](#)
- [Group](#)
- [Host](#)
- [Person](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Name	In the box, type the name you want to use for the object within its organizational unit. For example, <code>Indigo Jones</code> .

### Command line

Command option	Usage
<code>--name <i>name</i></code>	Replace <i>name</i> with the full <a href="#">TFN name</a> of the object. For example, <code>".../_ens/o=Indigo Insurance/ou=Finance/cn=XClaim"</code> .

### Description

This attribute specifies the common name of the object in the Secure Global Desktop datastore.

Names can include any characters you want. However we recommend that you avoid using the backslash character, the plus + character and apostrophes in object names as this can cause

problems.

If you use a forward slash in an object name, you must backslash protect (escape) it. For example, to create an object with the relative name `cn=a/b` beneath `o=organisation`, type `cn=a\b`. This will create an object `o=organisation/"cn=a/b"`.

On the command line, make sure you quote any names containing spaces.

## Examples

```
--name ".../_ens/o=Indigo Insurance/cn=Indigo Jones"
```

Defines the common name of the object as `Indigo Jones`. The object belongs to the organization object, `Indigo Insurance`.

```
--name '.../_ens/o=Indigo Insurance/cn=Indigo "Digger" Jones'
```

Defines the common name of the object as `Indigo "Digger" Jones`.

### Related topics

- [Name \(--name\) organization object](#)
- [Name \(--name\) organizational unit object](#)
- [Name \(--name\) domain component object](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## Name (--name) domain component object

### Objects with this attribute

- [Domain component](#)

### Object Manager

Attribute name	Usage
Name	In the box, type the name of the domain component. For example, com.

### Command line

Command option	Usage
<code>--name <i>name</i></code>	Replace <i>name</i> with the full TFN name of the object. For example, ".../_ens/dc=com".

### Description

This attribute specifies the name of the domain component in the Secure Global Desktop datastore.

A domain component is a "container" of DNS names. For example, in the DNS name `www.indigo-insurance.com`, the domain components are `indigo-insurance` and `com`, and the domain component for `com` would contain the domain component for `indigo-insurance`.

Names can include any characters you want. However we recommend that you avoid using the backslash character, the plus `+` character and apostrophes in object names as this can cause problems. If you use a forward slash in an object name, you must backslash protect (escape) it.

On the command line, make sure you quote any names containing spaces.

### Examples

---

```
--name ".../_ens/dc=com/dc=indigo-insurance"
```

Names the domain component `indigo-insurance`.

### Related topics

- [Name \(--name\) objects with "common name"](#)
- [Name \(--name\) organization object](#)
- [Name \(--name\) organizational unit object](#)
- [The tarantella object new\\_dc command](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## Name (--name) organization object

### Objects with this attribute

- [Organization](#)

### Object Manager

Attribute name	Usage
Name	In the box, type the name you want to use for the organization object. For example, <code>Indigo Insurance</code> .

### Command line

Command option	Usage
<code>--name <i>name</i></code>	Replace <i>name</i> with the full <a href="#">TFN name</a> of the object. For example, <code>".../_ens/o=Indigo Insurance"</code> .

### Description

This attribute specifies the name of the organization object in the Secure Global Desktop datastore.

Names can include any characters you want. However we recommend that you avoid using the backslash character, the plus + character and apostrophes in object names as this can cause problems.

If you use a forward slash in an object name, you must backslash protect (escape) it. For example, to create an organization object with the name `o=a/b`, type `o=a\b`. This will create an object `"o=a/b"`.

On the command line, make sure you quote any names containing spaces.

### Examples

```
--name ".../_ens/o=Indigo Insurance"
```



Defines the name of the organization object as `Indigo Insurance`.

### Related topics

- [Name \(--name\) objects with "common name"](#)
- [Name \(--name\) organizational unit object](#)
- [Name \(--name\) domain component object](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## Name (--name) organizational unit object

### Objects with this attribute

- [Organizational unit](#)

### Object Manager

Attribute name	Usage
Name	In the box, type the name you want to use for the organizational unit object. For example, <code>Finance</code> .

### Command line

Command option	Usage
<code>--name <i>name</i></code>	Replace <i>name</i> with the full <a href="#">TFN name</a> of the object. For example, <code>".../_ens/o=Indigo Insurance/ou=Finance"</code> .

### Description

This attribute specifies the name of the organizational unit object in the Secure Global Desktop datastore.

Names can include any characters you want. However we recommend that you avoid using the backslash character, the plus + character and apostrophes in object names as this can cause problems.

If you use a forward slash in an object name, you must backslash protect (escape) it. For example, to create an object with the name `ou=a/b` beneath `o=organisation`, type `ou=a\b`. This will create an object `o=organisation/"ou=a/b"`.

### Examples

```
--name ".../_ens/o=Indigo Insurance/ou=Finance"
```

Defines the name of the organizational unit object as `Finance`. The object belongs to the organization object, `Indigo Insurance` (which must already exist).

### Related topics

- [Name \(--name\) objects with "common name"](#)
- [Name \(--name\) organization object](#)
- [Name \(--name\) domain component object](#)
- [The tarantella object `new\_orgunit` command](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## Open in new browser window (--newbrowser)

### Objects with this attribute

- [Document](#)

### Object Manager

Attribute name	Usage
Open in new browser window	Check or clear the box.

### Command line

Command option	Usage
<code>--newbrowser true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

For users logged in to Secure Global Desktop using a web browser, this attribute determines whether a **new web browser window** is opened to display the URL specified for the object, or whether it is displayed **in the frame alongside the webtop links**.

For Sun Secure Global Desktop Native Client users, this attribute has no effect.

#### Related topics

- [URL \(--url\)](#)
- [Display Using \(--displayusing\)](#)



## Preferred Locale (--preflocale)

### Objects with this attribute

- [Person](#)

### Object Manager

Attribute name	Usage
Preferred Locale	Pick a locale from the list, or type your own in the form <i>//-tt</i> .

### Command line

Command option	Usage
<code>--preflocale //-</code> <code>tt</code>	Replace <i>//-tt</i> with the locale, for example <code>en-us</code> .

### Description

The locale in which the user's webtop and Help appear. Not all locales may be available: if the locale is missing, the user sees an error page.

**Note** This attribute is only used with the classic webtop. The browser-based webtop ignores it.

Choose Automatic to use the client device's current locale, if that can be detected.

A locale has two parts, *language* and *territory*, separated by a hyphen –.

- The language part of a locale is specified using ISO 639 language codes, for example `en` for English or `ja` for Japanese.
- The territory part of a locale is specified using ISO 3166 territory codes, for example `us` for the United States or `jp` for Japan.

### Examples

```
--preflocale en-us
```

Specifies the US English locale: the English dialect used in the United States of America.

```
--preflocale ja-jp
```

Specifies the Japanese locale.

### Related topics

- [Webtop Theme \(--webtop\)](#)
- [Keyboard Map \(--keymap\)](#)

## Profile Editing (--editprofile)

### Objects with this attribute

- [Organization](#)
- [Organizational unit](#)
- [Person](#)

### Object Manager

Attribute name	Usage
Profile Editing	Pick a setting from the list.

### Command line

Command option	Usage
<code>--editprofile 2 1 0</code>	Specify 2 1 0.

### Description

This attribute controls whether or not users can create or edit profiles for use with the Sun Secure Global Desktop Client.

**Note** Profile editing must also be enabled on the [Array Properties](#) panel of Array Manager.

Command line	Array Manager
2	Use parent setting
1	Enabled
0	Disabled

For a person object or organizational unit object, choose Use parent setting (on the command line, `--editprofile 2`) to inherit the setting of a parent object in the organizational hierarchy. This allows



you to enable or disable profile editing for many users without having to edit each person object.

For organization objects, the Use parent setting means use the array-wide setting configured on the [Array Properties](#) panel of Array Manager.

Secure Global Desktop checks the person object for the user and then any parent object further up the organizational hierarchy to see whether profile editing is enabled or disabled. If all the objects checked are configured to use the parent's setting, then the array-wide default setting is used.

If profile editing is disabled for a [profile object](#), for example `.../_ens/o=Tarantella System Objects/cn=UNIX User Profile`, this will affect **all** users that are assigned that login profile.

By default, profile editing is enabled.

## Examples

```
--editprofile 0
```

Disables profile editing.

### Related topics

- [Profiles and the Sun Secure Global Desktop Client](#)
- [Working with the Sun Secure Global Desktop Client](#)

## Resumable (--resumable)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Resumable	Pick a setting from the list.

### Command line

Command option	Usage
<code>--resumable never   session   always</code>	Specify one of the valid resumability settings.

### Description

This attribute determines for how long a user will be able to resume an application.

Object Manager	Command line	Description
Never	<code>never</code>	<ul style="list-style-type: none"><li>• The application can never be resumed.</li><li>• Recommended for applications that do not provide a mechanism for the user to exit. For example, a clock application.</li></ul>

Webtop session	<code>session</code>	<ul style="list-style-type: none"> <li>• The application keeps running and is resumable until the user logs out of Secure Global Desktop.</li> <li>• If a user does not log out of Secure Global Desktop cleanly, for example, if they close their web browser or terminate the Secure Global Desktop Client without logging out, then applications that are webtop session resumable keep running for a time (see <a href="#">Resumable For</a>).</li> <li>• This is the default setting.</li> </ul>
Always	<code>always</code>	<ul style="list-style-type: none"> <li>• The application keeps running for a time (see <a href="#">Resumable For</a>) after the user logs out of Secure Global Desktop, and can be resumed when they next log in.</li> <li>• Recommended for applications that need to exit in a controlled way. For example, an email application that may need to remove lock files before it exits.</li> </ul>

**Note** An X application configured to [Display Using](#) a Local X Server is not resumable, whatever the value of the Resumable attribute.

Users can see if an application is resumable or not by pointing to its link on the webtop and looking at the popup window that displays.

The browser-based web webtop has controls for [suspending and resuming individual application sessions](#). If you are using the Secure Global Desktop Client in [Integrated mode](#), applications that are always resumable are automatically suspended when you log out. When you log in again, they are automatically resumed.

## Examples

```
--resumable never
```

The application is never resumable.

```
--resumable session
```

The application is resumable until the user logs out of Secure Global Desktop.

## Related topics

- Resumable For (--resumetimeout)
- Understanding webtop and emulator sessions
- Emulator Sessions properties (array-wide)

## Scale to fit window (--scalable)

### Objects with this attribute

- [3270 application](#)
- [5250 application](#)
- [Windows application](#)
- [X application](#)

### Object Manager

Attribute name	Usage
Scale to fit window	Check or clear the box.

### Command line

Command option	Usage
<code>--scalable true   false</code>	Specify <code>true</code> or <code>false</code> .

### Description

This attribute specifies that the application should be scaled to fit the window in which it is displayed.

This attribute is only available if the application is set to display in an independent window (`--displayusing independent`) or in a kiosk window (`--displayusing kiosk`).

If this attribute is checked (`true`), the application is always scaled to fit the window in which it is displayed. If you re-size the window, Secure Global Desktop rescales the application to fit the new window size and scroll bars will never display.

You can toggle between a scaled and an unscaled application by pressing the SCROLL LOCK key.

## Examples

```
--scalable true
```

### Related topics

- [Display Using \(--displayusing\)](#)

## Serial Port Mapping (--serialport)

### Objects with this attribute

- [Organization](#)
- [Organizational unit](#)
- [Person](#)

### Object Manager

Attribute name	Usage
Serial Port Mapping	Pick a setting from the list.

### Command line

Command option	Usage
<code>--serialport 2 1 0</code>	Specify 2 1 0.

### Description

This attribute controls whether users can access the serial ports on a client device from a Windows application running on a Microsoft Windows Server 2003 application server.

Command line	Array Manager
2	Use parent setting
1	Enabled
0	Disabled

For a person object or organizational unit object, choose Use parent setting (on the command line, `--serialport 2`) to inherit the setting of a parent object in the organizational hierarchy. This allows you to enable or disable access to serial ports for many users without having to edit each person object.

For organization objects, the Use parent setting means use the array-wide setting configured on the [Array Properties](#) panel of Array Manager.

When a user starts a Windows application, Secure Global Desktop checks the person object for the user and then any parent object further up the organizational hierarchy to see whether access to serial ports is enabled or disabled. If all the objects checked are configured to use the parent's setting, then the array-wide default setting is used.

By default, access to serial ports is enabled.

## Examples

```
--serialport 0
```

Disables access to serial ports.

### Related topics

- [Configuring access to serial ports](#)
- [Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop](#)



## Session Ends When (--endswhen)

### Objects with this attribute

- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Session Ends When	Choose a setting from the list.

### Command line

Command option	Usage
<code>--endswhen lastclient   windowmanager   windowmanageralone   loginscript   nowindows   loginscriptnowindows</code>	Specify a valid setting.

### Description

This attribute determines when an emulator session ends.

Object Manager	Command line	Description
Last client exits	<code>lastclient</code>	The server keeps track of the number of X clients running within the session, and ends the session when this reaches zero.

Window Manager exits	<code>windowmanager</code>	The server ends the session when the Window Manager exits, no matter how many X clients may be running.
Only Window Manager remains	<code>windowmanageralone</code>	The server ends the session when the only remaining X client is the Window Manager. Some Window Managers (such as OpenLook) run X clients in the background, which means that this condition is never met. If you encounter this problem, you should use the No Visible Windows setting ( <code>--endswhen nowindows</code> ).
Login script exits	<code>loginscript</code>	The server ends the session when the <a href="#">login script</a> completes. Use this in conjunction with <a href="#">Keep Launch Connection Open</a> if an application has problems shutting down.
No visible windows	<code>nowindows</code>	The server ends the session when no windows are visible. This is useful for window managers (such as OpenLook) that run X clients in the background.
Script exits or no windows	<code>loginscriptnowindows</code>	The server ends the session when either the <a href="#">login script</a> completes or no windows are visible. Use this for applications that are <a href="#">always resumable</a> and that use X clients as this forces a session to close if an application server is re-booted or disconnected from the network. Use this in conjunction with <a href="#">Keep Launch Connection Open</a> if an application has problems shutting down.

## Examples

```
--endswhen nowindows
```

The emulator session ends when no windows are visible.

### Related topics

- [Keep launch connection open \(--keepopen\)](#)
- [Understanding webtop and emulator sessions](#)

## Shared between users (guest) (--shared)

### Objects with this attribute

- [Person](#)

### Object Manager

Attribute name	Usage
Shared between users (guest)	Check or clear the box.

### Command line

Command option	Usage
<code>--shared true false</code>	Specify <code>true</code> or <code>false</code> .

### Description

This attribute specifies whether the person object will be used by a single user, or will be shared by multiple users in the form of a "guest" account.

The table shows the similarities and differences between person objects with the attribute cleared and with the attribute checked.

Account is not shared	Account is shared
Should be used by <b>one user</b> .	May be used by <b>more than one user</b> .
Each user has their own emulator sessions.	Each user has their own emulator sessions.
Emulator sessions <b>may continue between webtop sessions</b> .	Emulator sessions <b>end when a user logs out or closes their web browser</b> .

One set of password cache and web cache entries.	One set of password cache and web cache entries <b>(which is shared between all users)</b> .
The user <b>may save entries in the password cache</b> .	Users <b>may not save entries in the password cache</b> .
If the user is already logged in, <b>logging in again from a different client device will relocate the webtop session</b> : the old webtop session will end.	<b>Logging in again creates a new webtop session</b> . No existing webtop sessions are affected.

### Related topics

- [Using shared accounts for "guest" users](#)
- [Understanding webtop and emulator sessions](#)

## Surname (--surname)

### Objects with this attribute

- [Person](#)

### Object Manager

Attribute name	Usage
Surname	In the box, type the person's surname.

### Command line

Command option	Usage
<code>--surname</code> <code><i>name</i></code>	Replace <i>name</i> with the surname of the person.

### Description

This attribute specifies the surname (family name) of the person.

Names can include any characters you want. On the command line, make sure you quote any names containing spaces.

### Examples

```
--surname Jones
```

Defines the surname of the person as `Jones`.

### Related topics

- Name (--name) objects with "common name"

## Terminal Type (--termtyp)

### Objects with this attribute

- [Character application](#)

### Object Manager

Attribute name	Usage
Terminal Type	Pick a terminal type from the list or type your own.

### Command line

Command option	Usage
--termtyp <i>type</i>	Replace <i>type</i> with a terminal type, for example <i>ansi</i> .

### Description

This attribute specifies the terminal type required for the application, which you should set appropriately for the [Emulation Type](#).

For UnixWare 7 application servers, we recommend you use `scoansi` rather than `ansi` with applications configured to use SCO Console emulation.

### Examples

```
--termtyp ansi
```

Uses the `ansi` terminal type.

```
--termtyp wyse60
```



Uses the `wyse60` terminal type.

### Related topics

- [Emulation Type \(--emulator\)](#)

## Try running from client first (--trylocal)

### Objects with this attribute

- [Windows application](#)

### Object Manager

Attribute name	Usage
Try running from client first	Check or clear the box.

### Command line

Command option	Usage
--trylocal true false	Specify true or false.

### Description

This attribute specifies whether to try starting the application from the user's client device.

If this is checked and the application isn't installed on the client device, the [Windows Protocol](#) is used. **If this is checked the application will not be resumable -- even if the Windows Protocol is used.**

**Note** A web browser with the signed Secure Global Desktop [Java™ archive](#) (or the Sun Secure Global Desktop Native Client) is needed to allow Secure Global Desktop to start applications on the client device.

#### Related topics

- [Windows Protocol \(--winproto\)](#)



## URL (--url)

### Objects with this attribute

- [Document](#)

### Object Manager

Attribute name	Usage
URL	In the box, type a URL.

### Command line

Command option	Usage
<code>--url <i>url</i></code>	Replace <i>url</i> with a URL.

### Description

The URL associated with the object. This is displayed when users click the link on their webtop.

You can use absolute or relative URLs. Relative URLs are considered relative to the Secure Global Desktop document root (usually `/tarantella`).

On the command line, make sure you quote any values containing spaces or other characters that may be interpreted by your shell.

### Examples

```
--url http://www.indigo-insurance.com
```

Makes the object display the Indigo Insurance home page when clicked.

```
--url ../my_docs/index.html
```

---

Displays that URL, considered relative to the Secure Global Desktop document root.

### Related topics

- [Open in new browser window \(--newbrowser\)](#)

## Username (--user)

### Objects with this attribute

- [Person](#)

### Object Manager

Attribute name	Usage
Username	In the box, type the person's username.

### Command line

Command option	Usage
<code>--user <i>username</i></code>	Replace <i>username</i> with the person's username.

### Description

This attribute specifies the username of a person. This is typically their UNIX username.

A [login authority](#) may use this attribute for identifying and authenticating users.

### Examples

```
--user indigo
```

Defines the Username of the person as `indigo`.

### Related topics

- Name (--name) objects with "common name"
- Login authorities

## Webtop Hints (--hints)

### Objects with this attribute

- [Character application](#)
- [Document](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Webtop Hints	In the box, type the webtop hints. Separate each hint with a semi-colon.

### Command line

Command option	Usage
<code>--hint <i>hint</i>...</code>	Replace <i>hint</i> with the webtop hint. Separate each hint with a semi-colon.

### Description

This attribute allows you to define one or more strings which can be used to provide finer control over the publishing and display of objects on the browser-based webtop.

You can use any number of strings and the strings can be anything. Separate each hint with a semi-colon. We recommend you adopt a name=value naming convention for webtop hints.

This attribute is blank by default.

This attribute is for developers who are using the Secure Global Desktop web services to develop custom webtops.



**Note** currently you can only set this attribute on the command line with the `tarantella object edit` command.

## Examples

```
--hint "preferredsize=16;"
```

Sets a webtop hint that could be used to specify the size of the webtop icon for the application.

### Related topics

- [Introducing Sun Secure Global Desktop Software](#)

## Webtop Icon (--icon)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [Document](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Webtop Icon	Choose an icon from the list.

### Command line

Command option	Usage
<code>--icon</code> <code>icon_name</code>	Replace <i>icon_name</i> with a filename: either a basename (to use an icon within an icon theme) or a URL.

### Description

This attribute specifies the icon that users see on their webtops.

Users accessing Secure Global Desktop using a web browser may have webtops of different shapes and sizes. The look of their webtop is defined by their [Webtop Theme](#) attribute. The webtop theme also determines the icon size and style (the **icon theme**). For instance, a webtop designed for smaller screens might use an icon theme with smaller icons.

**Note** The browser-based webtop does not use webtop or icon themes.

Generally, the Webtop Icon attribute names an icon **within** an icon theme (allowing it to vary depending on the user's webtop theme), rather than naming a particular icon to be used whatever the user's webtop theme.

In Object Manager, the Webtop Icon list shows icons from the sco/tta/standard icon theme. However, the user's icon theme (found from the webtop theme) will be used on the webtop.

On the command line, to name an icon within an icon theme just give the basename including extension (for example, `spreadsheet.gif`). To name an icon to be used whatever a user's icon theme, give an absolute or relative URL. Relative URLs are considered relative to the Secure Global Desktop `java` subdirectory (usually `/tarantella/java`).

## Examples

```
--icon spreadsheet.gif
```

Uses the `spreadsheet.gif` icon in the user's current icon theme.

```
--url http://www.indigo-insurance.com/icons/xclaim.gif
```

Uses the specified icon, whatever the user's current icon theme.

### Related topics

- [Webtop Theme \(--webtop\)](#)

## Webtop Theme (--webtop)

### Objects with this attribute

- Organization
- Organizational unit
- Person

### Object Manager

Attribute name	Usage
Webtop Theme	Pick a webtop theme from the list.

### Command line

Command option	Usage
<code>--webtop <i>theme_name</i></code>	Replace <i>theme_name</i> with the name of a webtop theme, for example <code>sco/tta/standard</code> .

### Description

This attribute defines the webtop theme for an object. A webtop theme defines everything about the appearance and behavior of a webtop for web browser users.

**Note** This attribute is only used with the classic webtop. The browser-based webtop does not use themes.

For a person object or organizational unit object (but not for an organization object), choose Use Parent's Theme (on the command line, `--webtop . .`) to "inherit" the webtop theme of the parent object in the organizational hierarchy. This lets you change the webtop theme of many objects at once without editing each object. This is the default value for new person objects and new organizational unit objects.

Webtop themes are defined in the `/opt/tarantella/var/docroot/resources/webtops` directory. Theme names have three levels, for example `sco/tta/standard`. Each theme directory contains

a file `theme.properties`, describing the theme.

- On the command line, replace *theme\_name* with the value of the `name` property found in the `theme.properties` file. For example, `sco/tta/standard`.
- In Object Manager, the webtop theme names displayed in the list are obtained from the `name-ll-tt` properties in each `theme.properties` file, where *ll-tt* defines a locale. For instance, if you're using the US English version of Object Manager, it will display the values of the `name-en-us` properties in the list of webtop themes.

The attribute is ignored for users of the Native Client.

When listing object attributes on the command line, an attribute value of `..` means use parent's theme.

## Examples

```
--webtop sco/tta/standard
```

Uses the `sco/tta/standard` webtop theme, which all users see by default.

```
--webtop ..
```

Uses the webtop theme of the parent in the organizational hierarchy.

### Related topics

- [Webtop Icon \(--icon\)](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)

## Width (--width)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)
- [3270 application](#)
- [5250 application](#)

### Object Manager

Attribute name	Usage
Width	In the box, type the width of the application in pixels.

### Command line

Command option	Usage
<code>--width <i>pixels</i></code>	Replace <i>pixels</i> with the width of the application, in pixels.

### Description

This attribute defines the width of the application, in pixels. The minimum width is 10 pixels, the maximum 65535 pixels.

On the command line you must specify the width even if this attribute is not required, for example because the application is configured to [Display Using](#) client window management or to display at the [Client's Maximum Size](#).

### Examples

```
--width 300
```

Uses a 300-pixel wide window to display the application.

## Related topics

- [Client's maximum size \(--maximize\)](#)
- [Height \(--height\)](#)
- [Display Using \(--displayusing\)](#)

## Windows NT Domain (--ntdomain)

### Objects with this attribute

- [Host object](#)
- [Windows application object](#)
- [Person object](#)

### Object Manager

Attribute name	Usage
Windows NT Domain	In the box, type the Windows domain to use for authentication.

### Command line

Command option	Usage
<code>--ntdomain <i>dom</i></code>	Replace <i>dom</i> with the Windows domain to use for authentication.

### Description

This attribute specifies the Windows domain to use for the application server authentication process.

**Note** This attribute plays no part in the Secure Global Desktop login.

### Caching passwords

If a user's Secure Global Desktop password is also their Windows domain password, then it is possible to cache this password by setting the Windows NT Domain attribute on the appropriate person or profile object from ENS. As long as saving Secure Global Desktop passwords is enabled, the domain name and password are then stored in the password cache. (If necessary, the Administrator can configure the Authentication dialog to disable password caching.)

See also [Managing passwords](#).



**Note** When using Active Directory, the Windows NT domain attribute does not need to be set on the person or profile object.

## The authentication process

When a Windows application is launched, Secure Global Desktop goes through the following authentication process:

1. Check if the host object has a Windows NT domain set for it. If it does, find the username and password in the application server password cache. If password caching is disabled, prompt for the username and password. Otherwise,
2. Check if the application object has an Windows NT domain set for it. If it does, find the username and password in the password cache. If password caching is disabled, prompt for the username and password. Otherwise,
3. Check the domain stored during login. If the user was logged in using an Active Directory server, the domain name can be inferred from this. Use the domain to find the username and password in the password cache.

## User-specified domains

If you want to allow users to specify their own domains, make sure that the value of this attribute is blank for the host, the application and the person object.

When starting Windows applications, the user can change the domain using the NT Domain field on the Authentication dialog. This field is automatically completed if the NT domain is set for the host or application object or cached, but **not** if the NT domain is set for the person object.

**Note** A user can override the NT Domain attribute by typing a username in the format domain name, for example *indigo\rusty*.

## Examples

```
--ntdomain indigo
```

Authenticates using the domain indigo.

### Related topics

- [The tarantella passcache command](#)
- [Introducing Object Manager](#)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Windows Protocol (--winproto)

### Objects with this attribute

- [Windows application](#)

### Object Manager

Attribute name	Usage
Windows Protocol	Pick a protocol from the list.

### Command line

Command option	Usage
<code>--winproto wts   winframe   none</code>	Specify a valid setting.

### Description

This attribute identifies the protocol used to connect to the server hosting the Windows application.

Object Manager	Command line
Microsoft RDP	<code>wts</code>
Citrix ICA	<code>winframe</code>
None	<code>none</code>

Use Microsoft RDP to run an applications using Microsoft Terminal Services.

Choose None (which checks [Try Running From Client First](#)) if you only want to run a Windows application installed on the client device.

Use the [Protocol Arguments](#) attribute for any command-line options that apply to the defined Windows

Protocol.

## Examples

```
--winproto wts
```

Connects to a Windows server using Microsoft RDP.

### Related topics

- [Try running from client first \(--trylocal\)](#)
- [Protocol Arguments \(--protoargs\)](#)

## Hosts tab (--appserv)

### Objects with this attribute

- [Character application](#)
- [Windows application](#)
- [X application](#)

### Object Manager

Attribute name	Usage
Hosts tab	Drop objects into the box.

### Command line

Command option	Usage
<code>--appserv</code> <code>object...</code>	Replace <i>object</i> with the full <a href="#">TFN name</a> of an object. For example, " <code>.../_ens/o=Indigo Insurance/ou=IT/cn=london</code> ".

### Description

This attribute defines the application servers that can run the application. The Secure Global Desktop server uses [application server load balancing](#) to determine which application server to use. Each application server is stored as **a reference to the object**, so a particular object may appear on many Hosts tabs. (If an object is moved or renamed later, all references to it are automatically updated.)

If a group is added to a Hosts tab, the group's members (and not the group) are used for application server load balancing.

If you don't specify any hosts, the application may run on any Secure Global Desktop server in the array that supports that type of application.

On the command line, make sure you quote any object names containing spaces.

## Examples

```
--appserv ".../_ens/o=Indigo Insurance/ou=IT/cn=geneva "  
          ".../_ens/o=Indigo Insurance/cn=prague "
```

Adds `geneva` and `prague` as application servers for an application.

### Related topics

- [Introducing application server load balancing](#)
- [Host object](#)
- [Group object](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## Links tab (--links)

### Objects with this attribute

- [Organization](#)
- [Organizational unit](#)
- [Person](#)

### Object Manager

Attribute name	Usage
Links tab	Drop objects into the box.

### Command line

Command option	Usage
<code>--links object...</code>	Replace <i>object</i> with the full TFN name of the object. For example, " <code>.../_ens/o=Indigo Insurance/ou=Finance/cn=XClaim</code> ".

### Description

This attribute defines the content of a webtop. Each link is stored as **a reference to the object**, so a particular object may appear on many webtops. (If an object is moved or renamed later, all references to it are automatically updated.)

- If a group is added to a Links tab, the group's members (and not the group) appear on the webtop.
- If an organizational unit is added to a Links tab, the webtop content for that organizational unit (and not the organizational unit) appears on the webtop.

Person objects and organizational unit objects may [inherit webtop content from their parent](#) in the organizational hierarchy.

On the command line, make sure you quote any object names containing spaces.

## Examples

```
--links ".../_ens/o=Indigo Insurance/cn=Pers-o-dat" \  
        ".../_ens/o=Indigo Insurance/cn=Slide-o-win"
```

Adds `Pers-o-dat` and `Slide-o-win` as links on a webtop.

### Related topics

- [Inherit parent's webtop content \(--inherit\)](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)



## Members tab (--member)

### Objects with this attribute

- [Group](#)

### Object Manager

Attribute name	Usage
Members tab	Drop objects into the box.

### Command line

Command option	Usage
<code>--member object...</code>	Replace <i>object</i> with the full <a href="#">TFN name</a> of the object. For example, " <code>.../_ens/o=Indigo Insurance/ou=Finance/cn=XClaim</code> ".

### Description

A group may have many members, including other groups. Each member is stored as **a reference to the object**, so a particular object may be a member of many groups. (If an object is moved or renamed later, all references to it are automatically updated.)

On the command line, make sure you quote any object names containing spaces.

### Examples

```
--member ".../_ens/o=Indigo Insurance/cn=Indigo Jones" \  
        ".../_ens/o=Indigo Insurance/ou=Marketing/cn=Emma Rald"
```

Names `Indigo Jones` and `Emma Rald` as members.

```
--member '.../_ens/o=Indigo Insurance/cn=Indigo "Digger" Jones'
```

Names Indigo "Digger" Jones as a member.

### Related topics

- [Links tab \(--links\)](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## Client printers (--mapprinters)

### Objects with this attribute

- [Organization](#)
- [Organizational unit](#)
- [Person](#)

### Object Manager

Attribute name	Usage
Client printers	Pick a setting from the list.

### Command line

Command option	Usage
<code>--mapprinters 2 1 0</code>	Specify 2 1 0.

### Description

Controls which client printers users can print to when printing from Windows applications that use the Microsoft RDP [Windows Protocol](#).

This attribute is only available if [User-specific printing configuration](#) has been enabled for the object.

The setting for this attribute overrides either of the following:

- The setting for a parent object in the organizational hierarchy.
- The array-wide default setting configured on the [Printing Properties](#) panel in Array Manager, if there is no parent object configuration.

Changes to this attribute only take effect for new webtop sessions.

When you enable user-specific printing configuration, users can print to all their client printers by

default. If you select No client printers available, you can still use a [Secure Global Desktop PDF printer](#).

Command line	Array Manager
2	Let users print to all client printers
1	Let users print to client's default printer
0	No client printers available.

Changes to this attribute only take effect for new webtop sessions.

If users can only print to their default printer and they want to print to a different printer, they have to log out of Secure Global Desktop, change the default printer and then log in again.

## Examples

```
--mapprinters 1
```

Allows users to print only to their default client printer.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [Configuring Secure Global Desktop PDF printing](#)
- [Printing properties \(array-wide\)](#)

## Driver name (--pdfdriver)

### Objects with this attribute

- [Organization](#)
- [Organizational unit](#)
- [Person](#)

### Object Manager

Attribute name	Usage
Driver name	Type the name of the printer driver to use for PDF printing.

### Command line

Command option	Usage
<code>--pdfdriver</code> <code>driver_name</code>	Replace <code>driver_name</code> with the name of the printer driver to use for PDF printing.

### Description

The name of the printer driver to use for Secure Global Desktop [PDF printing](#) when printing from Windows applications that use the Microsoft RDP [Windows Protocol](#).

This printer driver must be installed on every Windows application server used with Secure Global Desktop.

The printer driver must be a PostScript printer driver. The default is `HP Color LaserJet 8500 PS`.

The name you type must match the name of the printer driver installed on your Windows application servers **exactly**. Pay particular attention to the use of capitals and spaces. Use quotes on the command line if the name includes spaces. The `/opt/tarantella/etc/data/default.printerinfo.txt` file contains all the common printer driver names ordered by manufacturer. To avoid errors, copy and paste the driver name from this file.

This attribute is only available if [Let users print to a PDF printer](#) is enabled.

The setting for this attribute overrides either of the following:

- The setting for a parent object in the organizational hierarchy.
- The array-wide default setting configured on the [Printing Properties](#) panel in Array Manager, if there is no parent object configuration.

Changes to this attribute only take effect for new webtop sessions.

## Examples

```
--pdfdriver "HP LaserJet 8000 Series PS"
```

Configures the HP LaserJet 8000 Series PS printer driver as the driver to use for PDF printing.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [Configuring Secure Global Desktop PDF printing](#)
- [Printing properties \(array-wide\)](#)

## Let users print to a PDF local file (--pdfviewerenabled)

### Objects with this attribute

- [Organization](#)
- [Organizational unit](#)
- [Person](#)

### Object Manager

Attribute name	Usage
Let users print to a PDF local file	Check or clear the box.

### Command line

Command option	Usage
<code>--pdfviewerenabled 1 0</code>	Specify 1 (true) or 0 (false).

### Description

Allows users to print using the Secure Global Desktop "Print to Local PDF File" printer when printing from Windows applications that use the Microsoft RDP [Windows Protocol](#).

This attribute is only available if [User-specific printing configuration](#) has been enabled for the object.

The setting for this attribute overrides either of the following:

- The setting for a parent object in the organizational hierarchy.
- The array-wide default setting configured on the [Printing Properties](#) panel in Array Manager, if there is no parent object configuration.

Changes to this attribute only take effect for new webtop sessions.

## Examples

```
--pdfviewerenabled true
```

Allows users to print using the Print to Local PDF File printer.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [Configuring Secure Global Desktop PDF printing](#)
- [Printing properties \(array-wide\)](#)



## Let users print to a PDF printer (--pdfenabled)

### Objects with this attribute

- [Organization](#)
- [Organizational unit](#)
- [Person](#)

### Object Manager

Attribute name	Usage
Let users print to a PDF printer	Check or clear the box.

### Command line

Command option	Usage
<code>--pdfenabled 1 0</code>	Specify 1 (true) or 0 (false).

### Description

Allows users to print using the Secure Global Desktop "Universal PDF" printer when printing from Windows applications that use the Microsoft RDP [Windows Protocol](#).

This attribute is only available if [User-specific printing configuration](#) has been enabled for the object.

The setting for this attribute overrides either of the following:

- The setting for a parent object in the organizational hierarchy.
- The array-wide default setting configured on the [Printing Properties](#) panel in Array Manager, if there is no parent object configuration.

Changes to this attribute only take effect for new webtop sessions.

### Examples

Allows users to print using the Universal PDF printer.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [Configuring Secure Global Desktop PDF printing](#)
- [Printing properties \(array-wide\)](#)

## Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)

### Objects with this attribute

- [Organization](#)
- [Organizational unit](#)
- [Person](#)

### Object Manager

Attribute name	Usage
Make PDF file printer the default for Windows 2000/3	Check or clear the box.

### Command line

Command option	Usage
<code>--pdfviewerisdefault 1   0</code>	Specify 1 (true) or 0 (false).

### Description

Sets the Secure Global Desktop "Print to Local PDF File" printer as the client's default printer when printing from Windows applications that use the Microsoft RDP [Windows Protocol](#).

This attribute is only available if [Let users print to a PDF local file](#) is enabled.

By default, the Print to Local PDF File printer is not the default (false).

The setting for this attribute overrides either of the following:

- The setting for a parent object in the organizational hierarchy.
- The array-wide default setting configured on the [Printing Properties](#) panel in Array Manager, if there is no parent object configuration.

Changes to this attribute only take effect for new webtop sessions.

## Examples

```
--pdfviewerisdefault true
```

Makes the Print to Local PDF File printer the default printer when printing from Windows 2000/2003.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [Configuring Secure Global Desktop PDF printing](#)
- [Printing properties \(array-wide\)](#)

## Make PDF printer the default for Windows 2000/3 (--pdfisdefault)

### Objects with this attribute

- [Organization](#)
- [Organizational unit](#)
- [Person](#)

### Object Manager

Attribute name	Usage
Make PDF printer the default for Windows 2000/3	Check or clear the box.

### Command line

Command option	Usage
<code>--pdfisdefault 1 0</code>	Specify 1 (true) or 0 (false).

### Description

Sets the Secure Global Desktop "[Universal PDF](#)" printer as the client's default printer when printing from Windows applications that use the Microsoft RDP [Windows Protocol](#).

This attribute is only available if [Let users print to a PDF printer](#) is enabled.

By default, the Universal PDF printer is not the default (false).

The setting for this attribute overrides either of the following:

- The setting for a parent object in the organizational hierarchy.
- The array-wide default setting configured on the [Printing Properties](#) panel in Array Manager, if there is no parent object configuration.

Changes to this attribute only take effect for new webtop sessions.

## Examples

```
--pdfisdefault true
```

Makes the Universal PDF printer the default printer when printing from a Windows application.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [Configuring Secure Global Desktop PDF printing](#)
- [Printing properties \(array-wide\)](#)

## User-specific printing configuration (--userprintingconfig)

### Objects with this attribute

- [Organization](#)
- [Organizational unit](#)
- [Person](#)

### Object Manager

Attribute name	Usage
User-specific printing configuration	Check or clear the box.

### Command line

Command option	Usage
<code>--userprintingconfig 1 0</code>	Specify 1 (true) or 0 (false).

### Description

Enables user-specific printing configuration. This configuration is used when printing from Windows applications that use the Microsoft RDP [Windows Protocol](#).

If user-specific printing is enabled, the printing settings for this object override:

- The printing settings for a parent object in the organizational hierarchy.
- The array-wide default printing settings configured on the [Printing Properties](#) panel in Array Manager, if there is no parent object printing configuration.

Printing settings are **not** inherited from parent objects.

Changes to this attribute only take effect for new webtop sessions.

### Examples

```
--userprintingconfig true
```

Enables user-specific printing configuration.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [Configuring Secure Global Desktop PDF printing](#)
- [Printing properties \(array-wide\)](#)



## Secure Global Desktop and user authentication

### Read this topic to...

- Understand the authentication stages involved in using Secure Global Desktop.

Because Sun Secure Global Desktop Software has a [three-tier architecture](#), there are two stages to user authentication:

1. Users authenticate to a Secure Global Desktop server in order to log in to their webtop.
2. Users authenticate to a application server in order to run an application.

### Authenticating to a Secure Global Desktop server

The Secure Global Desktop server supports two mechanisms for authenticating users:

- [web server/third party authentication](#) in which an external mechanism (typically a web server) authenticates the user and the Secure Global Desktop server trusts that the authentication is correct.
- [login authorities](#) in which Secure Global Desktop tries to authenticate the users credentials against one or more external authentication services, for example an LDAP directory.

These mechanisms allow you to integrate Secure Global Desktop with your existing authentication architecture.

The main results of a successful authentication are:

- a user identity, which is the Secure Global Desktop idea of who a user is and
- a login profile, which determines the user's Secure Global Desktop-related settings including webtop content.

Sometimes, but not always, the user's identity and their login profile are the same thing.

### Authenticating to an application server

Secure Global Desktop uses [login scripts](#) to handle the connection to an application server, the authentication process and to start the application.

Secure Global Desktop can store the user's credentials for an application server in a secure password cache so they don't need to type them more than once.

### Related topics

- [Login authorities](#)
- [Web server/third party authentication](#)
- [Introducing web server authentication](#)
- [What are login scripts?](#)
- [Login scripts supplied with Secure Global Desktop](#)
- [The tarantella passcache command](#)
- [Application Launch properties \(array-wide\)](#)

## Denying users access to Secure Global Desktop after failed login attempts

By enabling a login failure handler, Administrators can deny users access to Secure Global Desktop after three failed login attempts. This additional security measure only works if users have ENS person objects.

To enable the login failure handler:

1. On the command line, type:

```
tarantella config edit --tarantella-config-components-  
loginfailurehandler 1
```

2. Then type:

```
tarantella config edit --tarantella-config-components-loginfailurefilter  
1
```

### Notes on enabling the login failure handler

- If you enable this functionality and a user does not have an ENS person object, they will still be able to log in to Secure Global Desktop.
- The number of login attempts is local to each Secure Global Desktop server and is not copied across the array. Only when the login limit is reached on a server, is the user denied access across the array. For example, a user could try to log in on each Secure Global Desktop server two times, but only when they fail for the third time on a server will they be denied access to the other members of the array.
- If a user is denied access, they are only denied access to Secure Global Desktop. They are not denied access to the host on which Secure Global Desktop is installed.
- When a user is denied access, Secure Global Desktop unchecks the [May log in to Secure Global Desktop](#) (`--enabled false`) checkbox for the user's person object in Object Manager. To give a user access again, you only need to re-check this check box (`--enabled true`).
- For security reasons, users are not given any indication that their account has been disabled. They see the same message as if they'd typed an incorrect password.

### Can I change the number of login attempts users get?

Yes, the number of login attempts users get is configurable. To change the number of login attempts:

1. Log in to the primary Secure Global Desktop server.
2. Stop the primary Secure Global Desktop server. On the command line, type:  
`tarantella stop.`
3. Set the number of login attempts. On the command line, type:  
`tarantella config edit --com.sco.tta.server.login.LoginFailureHandler.  
properties-attemptsallowed number.`
4. Start the primary Secure Global Desktop server. On the command line, type:  
`tarantella start.`
5. Do a warm restart of all secondary Secure Global Desktop servers (`tarantella restart --  
warm`).

### Related topics

- [What is ENS?](#)

## All login authorities are disabled and no-one can access Secure Global Desktop

If a Secure Global Desktop Administrator has accidentally disabled all login authorities, no-one will be able to log in to Secure Global Desktop, even the UNIX root user. You can't run Array Manager or Object Manager from the command line because this requires an administrator to log in.

To solve this problem:

1. Log in as root on the host where Secure Global Desktop is installed.
2. Stop the Secure Global Desktop server by running `tarantella stop`.
3. Enable either the UNIX user or the UNIX group login authority by running one of the following commands:

```
tarantella config edit --login-unix-user 1
tarantella config edit --login-unix-group 1
```

4. Restart the Secure Global Desktop server by running `tarantella start`.

The root user can now use Array Manager to turn on other login authorities as required.

### Related topics

- [Login authorities](#)

## Using shared accounts for "guest" users

Normally, users have their own person objects and person objects are not shared between users. However, you may want to allow more than one user to log in using the same username and password, for example to share an account for "guest" users.

You can only share accounts if you are using one or more [login authorities](#) that use an ENS person object as the login profile.

**Note** [Anonymous users](#) are always treated as using a shared account.

To share a person object in this way:

1. In Object Manager, create the person object that will be shared.
2. Check the box next to [Shared Between Users \(Guest\)](#).

Guest users are never prompted for application server passwords. This means guest users can't add or change password cache entries. Use the `tarantella passcache` command to manage application server passwords for guest users.

### Related topics

- [Login authorities](#)
- [Shared between users \(guest\) \(--shared\)](#)

[Secure Global Desktop Administration Guide](#) > [Users and authentication](#) > An "Ambiguous username" dialog is displayed when a user tries to log in

## An "Ambiguous username" dialog is displayed when a user tries to log in

This dialog is displayed only for users who **share person object attributes and also have the same password**.

To prevent the ambiguous username dialog being displayed:

- **Either** prevent users from having identical passwords (recommended).
- **Or** use [Object Manager](#) to change the shared attributes for the affected person objects. For example, clear the [May Log In To Secure Global Desktop](#) box to deny access to all but one of the users sharing the person object attributes and password.

### Cause

A user logs in by typing either their name, username or email address into the username box, followed by their password. For example, user Indigo Jones might type Indigo Jones, indigo or indigo indigo-insurance.com into the username box.

The [ENS login authority](#), or [LDAP login authority](#), then searches the ENS, or LDAP, database for a person object with a name attribute matching the text the user typed. If the search is unsuccessful, the database is searched for a person object with a username attribute matching the text the user entered. If this search is unsuccessful, a matching email address attribute is looked for.

If only one matching person object is found and the correct password has been entered, the user is logged in.

If more than one person object matches, there is the possibility of an ambiguous login. Secure Global Desktop then checks the password against the person objects sharing the entered attribute.

If the password matches only one person object, the user is logged in.

If the password matches more than one person object, the ambiguous username dialog is displayed. The user is then asked to provide one of the two attributes not originally entered, to help resolve the ambiguity.

If this information fails to resolve the ambiguity, that is, two attributes and the password are shared by

more than one person object, the user is asked for the remaining attribute.

If this fails to resolve the ambiguity the login fails.

#### **Related topics**

- [Login authorities](#)
- [What is ENS?](#)
- [Person object](#)



## Solaris OS users are unable to log in when Secure Global Desktop security services are running

If users on the Solaris™ Operating System (Solaris OS) are unable to log in to a Secure Global Desktop server when Secure Global Desktop security services are running, check that the `/dev/random` device is present on the client.

Secure Global Desktop security services require the `/dev/random` device. If it is missing, install the Solaris OS patch that contains this device.

### Related topics

- [Securing client connections with Secure Global Desktop security services](#)

## Using SecurID for application server authentication

As well as using SecurID to authenticate users to Secure Global Desktop, you can use SecurID for application server authentication when launching X and character applications.

To use SecurID authentication, you should first ensure that users can log in to the application server using SecurID before introducing Secure Global Desktop. When you are ready to use SecurID authentication, configure the application to use the `securid/unix.exp` [Login script](#).

When users log in to an application server that uses SecurID authentication, they should enter a username but leave the password field blank. When they click OK, they will be prompted for a passcode.

You should also disable the Save Secure Global Desktop login details in cache attribute on the [Application Launch](#) Properties panel of Array Manager. This is because SecurID passcodes cannot be re-used.

### Related topics

- [The SecurID login authority](#)
- [Enabling the SecurID login authority](#)
- [Login scripts supplied with Secure Global Desktop](#)

## Web server/third party authentication

### Overview

Web server/third party authentication allows users to log in to Secure Global Desktop if they have been authenticated by an external mechanism, such as web server authentication.

If you are using either the classic or browser-based webtop, you can only use [web server authentication](#) with these webtops. If you develop your own webtop applications using the Secure Global Desktop web services, you can use any external/third party authentication mechanism.

Web server authentication for the classic webtop is enabled by default.

Third party authentication for the browser-based webtop is disabled by default.

### Logging in

The user types in a username and password directly to the external mechanism, typically using their web browser's authentication dialog.

### Authentication

Web server/third party authentication is based on trust. Secure Global Desktop trusts that the web server/third party mechanism has authenticated the user correctly and so they are authenticated to Secure Global Desktop.

### User identity and login profile

Once a user has been authenticated, Secure Global Desktop performs a search to establish the user's identity and login profile (see below).

To perform the search, one or more of the identity mapping search methods must be enabled on the [Secure Global Desktop Login properties panel](#) in Array Manager. The methods are tried in the order they are listed (see below).

If the searches do not produce a match, Secure Global Desktop can't establish an identity for the user and so the standard Secure Global Desktop login page displays. The user must log in to Secure Global Desktop so that a login authority can be tried.

Web server/third party authentication does not support **ambiguous users** and so the first match found is used.

### **Search ENS for matching person**

Searches ENS for a **person object** with a **Name**, **Username** or **Email Address** attribute that matches the user's web/third party username.

#### **User identity**

The matching person object in ENS.

#### **Login profile**

The matching person object in ENS.

### **Search LDAP and use closest ENS match**

Searches the LDAP directory for a person object with a **cn** (common name) attribute that matches the user's web/third party username. If there's no match, the search is repeated on the **uid** (username) attribute, and finally on the **mail** (email address) attribute.

#### **User identity**

The identity is the LDAP person object and has the form `.../_service/sco/tta/ldapcache/LDAP-person`.

#### **Login profile**

The first match of the following is used:

1. A person object in ENS with the same name as the LDAP person object, allowing for differences in the naming system. For example, if the LDAP object `cn=Indigo Jones, ou=Administration, o=Indigo Insurance` is found, this login authority would search ENS for `o=Indigo Insurance/ou=Administration/cn=Indigo Jones`.
2. A person object in ENS, with the name `cn=LDAP Profile`, in the same OU as the LDAP person object. For example, `o=Indigo Insurance/ou=Administration/cn=LDAP Profile`.
3. A person object in ENS, with the name `cn=LDAP Profile`, in any parent OU for the LDAP person object. For example, `o=Indigo Insurance/cn=LDAP Profile`.
4. The default LDAP profile object `o=Tarantella System Objects/cn=LDAP Profile`.

## Search LDAP and use LDAP User Profile

Searches the LDAP directory for a person object with a `cn` (common name) attribute that matches the user's web/third party username. If there's no match, the search is repeated on the `uid` (username) attribute, and finally on the `mail` (email address) attribute.

### User identity

The identity is the LDAP person object and has the form `.../_service/sco/tta/ldapcache/LDAP-person`.

### Login profile

The profile object `o=Tarantella System Objects/cn=LDAP Profile` is always used for the login profile.

### Use default profile

No search is performed.

### User identity

For classic web server authentication, the user's identity is always `.../_service/sco/tta/webauth/web-username`.

For third party authentication, the user's identity is always `.../_service/sco/tta/thirdparty/thirdparty-username`.

### Login profile

For classic web server authentication, the profile object `o=Tarantella System Objects/cn=Web User Profile` is always used for the login profile.

For third party authentication, the profile object `o=Tarantella System Objects/cn=Third Party Profile` is always used for the login profile.

## Emulator sessions and password cache entries

Emulator sessions and password cache entries belong to the identity established by the identity mapping search methods.

## Related topics

- [Introducing web server authentication](#)
- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)
- [Trusted users and third party authentication](#)

## Introducing web server authentication

### Read this topic to...

- Learn about web server authentication.

Web server authentication is different to the Secure Global Desktop login authority system because the authentication is actually performed externally by a web server. You configure Secure Global Desktop to trust this authentication and it then determines the user's identity and their login profile.

When users log in, they see their browser's authentication dialog instead of the Secure Global Desktop login page. Once they have typed their username and password, users go directly to their webtop.

### How web server authentication works

Web server authentication (or HTTP authentication) is supported by all web servers and web browsers.

With HTTP authentication:

- A web server administrator protects a section of a web site.
- When a web browser first tries to access a URL within the protected section, the web server responds by requesting authentication.
- The web browser displays an authentication dialog to the user.
- The user types a username and password, which the browser sends to the web server.
- The web server authenticates the user's credentials and allows access to the requested URL.

The web browser caches the credentials, either temporarily (until the user closes the browser) or permanently (if the user checks the box on the browser's authentication dialog). It does this because, with HTTP authentication, the credentials must be sent with every request to a protected URL. The browser sends the credentials automatically.

### Determining the user's identity and login profile

Once the web server has authenticated the user, Secure Global Desktop then obtains the user's identity from the `REMOTE_USER` environment variable. The web server sets this variable after it has authenticated the user. Secure Global Desktop uses this identity to search for a matching login profile.

You can use web server authentication and login authorities together. If Secure Global Desktop can't find a matching login profile, the standard Secure Global Desktop login page displays. The user must log in to Secure Global Desktop and be authenticated by a login authority before they can access their webtop.

Web server authentication does not support [ambiguous users](#). This means users get the webtop of the first matching login profile.

## Points to note about web server authentication

- The way you enable web server authentication depends on whether you are using the [browser-based webtop](#) or the [classic webtop](#). You can enable web authentication in both webtops at the same time.
- The Sun Secure Global Desktop Native Client does not support web server authentication.
- You can use any web server authentication plug-in as long as it sets the `REMOTE_USER` variable. If the plug-in you use doesn't set that variable you can [export the variable your plug-in uses](#).

### Related topics

- [Enabling web server authentication for the browser-based webtop](#)
- [Enabling web server authentication for the classic webtop](#)
- [Users experience problems with web server authentication](#)
- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)



## Enabling web server authentication for the browser-based webtop

To enable web server authentication for the browser-based webtop:

1. On each array member, configure the web server to protect access to the `/sgd` URL.
2. In Array Manager, click Secure Global Desktop Login, Properties.
3. Check the box next to Use third party authentication.
4. Check one or more boxes in User identity mapping.
5. Configure the Tomcat component of the Secure Global Desktop Web Server to trust the web server authentication. On each array member, edit the `/opt/tarantella/webserver/tomcat/version/conf/server.xml` file. Add the following attribute to the connector element (`<Connector>`) for the Coyote/JK2 AJP 1.3 Connector:

```
tomcatAuthentication="false"
```

### Notes

- How you protect the `/sgd` URL depends on your web server, see your web server documentation for details. For the Secure Global Desktop Web Server, see the Apache documentation.
- The boxes you select in User identity mapping are the search methods Secure Global Desktop uses to determine a web user's identity and login profile. For details on how the search methods work, see [third party authentication](#).
- If you select more than one search method, the methods are processed in the order they are shown. As web server authentication does not support [ambiguous users](#) users will get the webtop of the first match found.
- If you are using the either of the LDAP User identity mapping search methods, you may also want to configure [secure connections to the LDAP directory server](#).
- If you are using the Secure Global Desktop Web Server, you can protect the `/sgd` URL in either the Apache or the Tomcat components. We recommend you use Apache.
- By default, for security reasons, Secure Global Desktop Administrators can't log in to the browser-based webtop with web server authentication. The standard login page always displays for these users even if they have been authenticated by the web server. To change this behavior, run the following command:

```
tarantella config edit --tarantella-config-login-thirdparty-allowadmins 1
```

### Example of how to configure the Secure Global Desktop Web Server

The following is an example of how you might configure the Secure Global Desktop Web Server for web server authentication:

1. Use the `/opt/tarantella/webserver/apache/version/bin/htpasswd` binary to create a web server password file.
2. Edit the `/opt/tarantella/webserver/apache/version/conf/httpd.conf` file and insert the following directory directives:

```
SetEnvIf Request_URI "\.(cab|jar|gif|der)$" sgd_noauth_ok

<LocationMatch /sgd>
    Order Allow,Deny
    Allow from env=sgd_noauth_ok
    AuthUserFile file-path
    AuthName auth-domain
    AuthType Basic
    Require valid-user
    Satisfy any
</LocationMatch>
```

where *file-path* is the full path to the web server password file  
and *auth-domain* is the name of authorization realm that appears in the web browser's authentication dialog.

3. Restart the Secure Global Desktop Web Server (`tarantella webserver restart` ) for the configuration changes to take effect.

## Notes

- This example uses a `SetEnvIf` directive as a workaround to the problem where some versions of Sun Java™ Plug-in fail to "remember" the user's credentials (see [http://bugs.sun.com/bugdatabase/view\\_bug.do?bug\\_id=4943729](http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=4943729)).
- This example uses a `LocationMatch` directive rather than a `Directory` directive because the management of the `/sgd` URL is delegated to Tomcat in the standard `httpd.conf` file for the Secure Global Desktop Web Server. This also means you can't use an `.htaccess` file to protect the `/sgd` URL.

## Related topics

- Enabling web server authentication for the classic webtop
- Introducing web server authentication
- Users experience problems with web server authentication
- Login authorities
- Secure Global Desktop Login properties (array-wide)
- Configuring your own web server for use with Secure Global Desktop

## Enabling web server authentication for the classic webtop

To enable web server authentication for the classic webtop:

1. On each array member, configure the web server to protect access to the `/opt/tarantella/var/docroot/cgi-bin/secure` directory.
2. In Array Manager, click Secure Global Desktop Login, Properties.
3. Check the box next to Use classic web server authentication.
4. Check one or more boxes in User identity mapping.
5. If necessary, change the Tokens are valid for and Web server username attributes.

### Notes

- How you protect the `/opt/tarantella/var/docroot/cgi-bin/secure` directory depends on your web server, see your web server documentation for details. For the Secure Global Desktop Web Server, see the Apache documentation.
- The boxes you select in User identity mapping are the search methods Secure Global Desktop uses to determine a web user's identity and login profile. For details on how the search methods work, see [web server authentication](#).
- If you select more than one search method, the methods are processed in the order they are shown. As web server authentication does not support [ambiguous users](#) users will get the webtop of the first match found.
- If you are using either of the LDAP User identity mapping search methods, you may also want to configure [secure connections to the LDAP directory server](#).
- You shouldn't need to change the value in the Tokens are valid for box. Reducing the token validity period may result in failed logins on slow networks.
- For new installations of Secure Global Desktop, the Web server username is set to the correct username (`ttaserv`) for use with the Secure Global Desktop Web Server.

### Example of how to configure the Secure Global Desktop Web Server

The following is an example of how you might configure the Secure Global Desktop Web Server for web server authentication:

1. Use the `/opt/tarantella/webserver/apache/version/bin/htpasswd` binary to create a web server password file.

2. Edit the `/opt/tarantella/webserver/apache/version/conf/httpd.conf` file and insert the following directory directive:

```
<Directory /opt/tarantella/var/docroot/cgi-bin/secure>
AuthUserFile  file-path
AuthName      auth-domain
AuthType      Basic
Require       valid-user
</Directory>
```

where *file-path* is the full path to the web server password file and *auth-domain* is the name of authorization realm that appears in the web browser's authentication dialog.

3. Restart the Secure Global Desktop Web Server (using `tarantella webserver restart` ) for the configuration changes to take effect.

## Notes

- Alternatively, you could protect `/opt/tarantella/var/docroot/cgi-bin/secure` by using an `.htaccess` file. If you do this, you must also set the `AllowOverride` in order for the directives to be applied. To apply the `Auth` directives, you must also include `AuthConfig` (or `All`) in your `AllowOverride` directive.

## Related topics

- [Enabling web server authentication for the browser-based webtop](#)
- [Introducing web server authentication](#)
- [Users experience problems with web server authentication](#)
- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)
- [Configuring your own web server for use with Secure Global Desktop](#)

## Security considerations of using web server authentication

### Username and passwords

Using web server authentication (HTTP authentication) means that the browser has to cache the user's credentials and, in effect, the user's authentication to Secure Global Desktop. To minimize the risk of cached credentials being used by someone else, users:

- must not check the save password box in their browser's authentication dialog. This permanently saves the user's credentials.
- must close their browser after logging out. This clears the user's credentials from the temporary cache. Logging out of Secure Global Desktop does not clear the HTTP authentication details.

**Note** We recommend you use a secure (HTTPS) web server to protect user's credentials.

### Web server authentication and the browser-based webtop

The browser-based webtop uses Secure Global Desktop web services. The `ITarantellaExternalAuth` web service is the web service that is used to set the identity of a user who has been authenticated by an external means, such as web server authentication. For security, the client (the webtop web application) and Secure Global Desktop server (the `ITarantellaExternalAuth` web service) have a shared secret, which is the username and password of a trusted user. This is, in effect, another layer of web server authentication.

In a standard installation, the browser-based webtop is pre-configured with the credentials of a single trusted user. See [Trusted users and third party authentication](#) for details of how to change these credentials or to add a new trusted user.

### Web server authentication and the classic webtop

For the classic webtop, once the web server has authenticated the user, it allows them access to the Secure Global Desktop program `ttawlogin.cgi` and passes the name of the authenticated user (the web username) to this program. The `ttawlogin.cgi` program:

- Checks that it is running as the user that owns the web server processes configured on the Secure Global Desktop Login properties in Array Manager. If it isn't, the web username isn't passed on to the Secure Global Desktop server.

- Uses a secret key to generate a token which contains an encrypted form of the web username and a timestamp. The client device presents this token to the Secure Global Desktop server as proof of authentication.

When the Secure Global Desktop server receives the token, it validates it by:

- using the secret key to decrypt the token and extract the web username.
- checking the timestamp on the token. If it's too old (that is it is outside the token validity period configured on the Secure Global Desktop Login properties in Array Manager), the login fails.
- checking its record of tokens to see whether it has seen the token before. If it has, the login fails.

This means the three main areas of risk when using web server authentication with the classic webtop concern:

- the token
- the secret key and
- the web server username.

To prevent a token from being intercepted and used while still valid, we recommend you secure the connections to the Secure Global Desktop server and to the Secure Global Desktop Web Server (HTTPS).

The secret key shared by the Secure Global Desktop server and the `ttawlogin.cgi` program is generated every time the Secure Global Desktop starts. The secret key is only accessible by someone with root permission on the Secure Global Desktop server. However, a new key is not generated for a warm restart (`tarantella restart -warm`). This behavior can be changed by running the following command:

```
tarantella config edit --tarantella-config-login-webauth-  
refreshkeyonwarmrestart 1
```

The web server username is the name of the user that owns the web server processes. If you are using your own web server, the default user is often `nobody` or `apache`. If you are particularly concerned about security, we recommend that you do not use these defaults.

## Related topics

- Introducing web server authentication
- Enabling web server authentication for the browser-based webtop
- Enabling web server authentication for the classic webtop
- Users experience problems with web server authentication
- Secure Global Desktop Login properties (array-wide)



## Users experience problems with web server authentication

Common problems users experience when they log in to Secure Global Desktop using web server authentication include:

- [Web server authentication fails](#)
- [Users keep getting the standard Secure Global Desktop login page](#)
- [The Java™ Plug-in keeps prompting for passwords](#)
- [Users get the wrong webtop](#)

To help diagnose and resolve some of these problem, add the following log filters on the Array Properties panel in Array Manager:

```
server/login/*error:log_file_name%%PID%%_error.jsl  
server/login/*error:log_file_name%%PID%%_error.log  
server/login/*info:log_file_name%%PID%%_error.jsl  
server/login/*info:log_file_name%%PID%%_error.log
```

### Web server authentication fails

If a user fails to authenticate to the web server, they may see a message such as "401 Authorization Required". This indicates that either there is a problem with the username/password the user is typing or there is a problem with the web server configuration.

Check:

- does the user have an entry in the web server password file?
- is the web server configured to use the correct password file?
- if you are using the Secure Global Desktop Web Server, is the password file accessible by the `ttaserv` user? If this user can't read the password file, web authentication will fail.

### Users keep getting the standard Secure Global Desktop login page

If web server authentication is not set up correctly or it fails for any reason, Secure Global Desktop displays the standard login page. The following table lists the things you may need to check.

What to check	More information
Is the right Secure Global Desktop directory/URL protected?	<p>You must set up your web server to protect:</p> <ul style="list-style-type: none"> <li>• the <code>tarantella/cgi-bin/secure</code> directory for the classic webtop.</li> <li>• the <code>/sgd</code> URL for the browser-based webtop.</li> </ul>
Is Tomcat configured to "trust" the web server authentication?	<p>For the browser-based webtop, the Tomcat component has to be configured to trust the web server authentication.</p> <p>On each array member, edit the <code>/opt/tarantella/webserver/tomcat/version/conf/server.xml</code> file. Add the following attribute to the connector element (<code>&lt;Connector&gt;</code>) for the Coyote/JK2 AJP 1.3 Connector:</p> <pre>tomcatAuthentication="false"</pre>
Does the user have an ENS person object?	<p>If your configuration of Secure Global Desktop relies on users having ENS person objects and you have not enabled one of the fallback profile objects, users may not be able to log in. If this happens and you have enabled the additional logging, search the log file for messages that indicate that Secure Global Desktop could not match the authenticated user to an ENS object.</p> <p>Either create an ENS person object for the user or enable one of the fallback profile objects, see <a href="#">web server/third party authentication</a> for more details.</p>
Is the user a Secure Global Desktop Administrator?	<p>By default, the browser-based webtop will not allow Secure Global Desktop Administrators access if they have been authenticated by a web server. To change this behavior, run the following command:</p> <pre>tarantella config edit --tarantella-config-login-thirdparty-allowadmins 1</pre>
Have you changed the trusted user?	<p>For the browser-based webtop only, if you have changed the username and password of the trusted user, have you verified that the new user works? See <a href="#">security considerations of using web server authentication</a> for details.</p>

Are the tokens timing out?	<p>For the classic webtop only, check that the tokens are not timing out.</p> <p>If you have enabled the additional logging, search the log file for messages beginning <code>invalidToken</code>.</p> <p>Increase the <a href="#">web token validity period</a> and try logging in again.</p>
Is the web server username correct?	<p>For the classic webtop only, check that the web server username configured in Secure Global Desktop matches the user that owns the web server processes. For the Secure Global Desktop Web Server this is <code>ttaserv</code>. This user is required to validate web server authentication tokens.</p>

## The Java Plug-in keeps prompting for passwords

For classic web server authentication to work, the `tarantella/cgi-bin/secure` directory must be protected on your web server. If you protect any other Secure Global Desktop directories (for example `/tarantella` or `/tarantella/cgi-bin`, browsers that use a plug-in virtual machine for the Java™ platform ('Java virtual machine' or 'JVM') will prompt users for their username and password. This happens because the JVM and the browser do not share authentication information.

Make sure you only protect the `tarantella/cgi-bin/secure` directory.

For the browser-based webtop, you may need to upgrade your plug-in version or arrange a workaround, see [http://bugs.sun.com/bugdatabase/view\\_bug.do?bug\\_id=4943729](http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=4943729).

## Users get the wrong webtop

Web server authentication does not support [ambiguous users](#). This means users get the webtop of the first matching login profile.

If you have enabled the additional logging, search the log file for messages that indicate an ambiguous user.

To resolve the situation, you can either:

- accept the first match
- attempt to manually resolve the ambiguity, for example by creating or amending person objects or
- disallow ambiguous logins (classic web server authentication only).

To disallow ambiguous logins for classic web server authentication, run the following command:

```
tarantella config edit --com.sco.tta.server.login.webauth.WebLoginAuthority.  
properties-takeFirstMatch false
```

You must restart the Secure Global Desktop server after making this change.

### Related topics

- [Introducing web server authentication](#)
- [Enabling web server authentication for the browser-based webtop](#)
- [Enabling web server authentication for the classic webtop](#)
- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)

## Can I use PKI client certificates with web server authentication?

Yes. You can strengthen the security of web server authentication by allowing a user to be authenticated if they have valid Public Key Infrastructure (PKI) certificate installed on the client device.

Secure Global Desktop web server authentication relies on the web server setting the `REMOTE_USER` variable to identify the user. However, when users are authenticated using client certificates this variable is not set. The following configuration allows you to export the `SSL_CLIENT_S_DN_CN` variable (which is specific to Apache web servers) to the `REMOTE_USER` variable. If your web server sets a different variable when using client certificates, see how you can [use other web authentication schemes with Secure Global Desktop](#).

To enable client certificates, configure each member of the array as follows:

1. On the web server, configure web authentication so that to access the `/tarantella/cgi-bin/secure/` directory (classic webtop) or the `/sgd` URL (browser-based webtop) you need a client certificate. How you do this depends on your web server. The Secure Global Desktop Web Server includes the Apache `mod_ssl` module.
2. Test that the web server authenticates users who have client certificates.
3. For the classic webtop, enable support for client certificates by running the following command:

```
tarantella config edit --tarantella-config-server-cgibin-bootscrip  
tsecure/ttaauthclientcert.cgi
```

4. For the browser-based webtop, configure the web server to export the `SSL_CLIENT_S_DN_CN` variable so that the Tomcat component of the Secure Global Desktop Web Server can access them. To do this for Apache component of the Secure Global Desktop Web Server:
  1. Edit the `/opt/tarantella/webserver/apache/version/conf/httpd.conf` file.
  2. Uncomment out the line:  
`JkEnvVar SSL_CLIENT_S_DN_CN " "`
  3. Uncomment out the lines:  
`<Location "/sgd">`  
`SSLOptions +StdEnvVars +ExportCertData`  
`</Location>`
5. Restart the Secure Global Desktop Web Server and the Secure Global Desktop server.

When this configuration is complete, enable web server authentication in Array Manager.

### Related topics

- [Enabling web server authentication for the browser-based webtop](#)
- [Enabling web server authentication for the classic webtop](#)
- [Can I use other web authentication schemes with Secure Global Desktop web server authentication?](#)

## Can I use SafeWord PremierAccess with web server authentication?

Yes. You can configure web server authentication to use the third-party SafeWord® PremierAccess™. See <http://www.securecomputing.com> for more information.

Secure Global Desktop web server authentication relies on the web server setting the `REMOTE_USER` variable to identify the user. However, when users are authenticated using SafeWord PremierAccess this variable is not set. The following configuration allows you to export the `HTTP_SAFEWORD_USER` variable to the `REMOTE_USER` variable.

To enable support for SafeWord PremierAccess, configure each member of the array as follows:

1. On the web server, configure SafeWord authentication to protect the `/tarantella/cgi-bin/secure/` directory (classic webtop) or the `/sgd` URL (browser-based webtop).
2. Test that the web server authenticates using SafeWord.
3. For the classic webtop, enable support for SafeWord by running the following command:

```
tarantella config edit --tarantella-config-server-cgibin-bootscrip  
secure/ttaauthsafeword.cgi
```

4. For the browser-based webtop, configure the web server to export the `HTTP_SAFEWORD_USER` variable so that the Tomcat component of the Secure Global Desktop Web Server can access it. To do this for Apache component of the Secure Global Desktop Web Server:
  1. Edit the `/opt/tarantella/webserver/apache/version/conf/httpd.conf` file.
  2. Uncomment out the line:  
`JkEnvVar HTTP_SAFEWORD_USER " "`
  3. Uncomment out the lines:  
`<Location "/sgd">`  
`SSLOptions +StdEnvVars +ExportCertData`  
`</Location>`
5. Restart the Secure Global Desktop Web Server and the Secure Global Desktop server.

When this configuration is complete, enable web server authentication in Array Manager.

- Enabling web server authentication for the browser-based webtop
- Enabling web server authentication for the classic webtop
- Can I use other web authentication schemes with Secure Global Desktop web server authentication?



## Can I use other web authentication schemes with Secure Global Desktop web server authentication?

Yes. However Secure Global Desktop web server authentication relies on the web server setting the `REMOTE_USER` variable to identify the user. However, when users are authenticated using another web authentication scheme, it is likely that another variable is used to identify the user and this means they can't be authenticated to Secure Global Desktop. The solution is to export the value of your variable to `REMOTE_USER`. How you do this depends on whether you are using the classic webtop or the browser-based webtop.

### The classic webtop

If you are using the classic webtop and your web authentication scheme uses another variable, you can export that variable using a wrapper script. For example:

```
#!/bin/sh
REMOTE_USER=$your_variable_name
export REMOTE_USER
exec ./ttawlogin.cgi $*
```

Save the script to a sub-directory in the `/opt/tarantella/var/docroot/cgi-bin/secure` directory. The script must have the same file permissions as the other scripts in this directory.

To implement the wrapper script, follow this process on each array member:

1. Configure your web authentication scheme to protect the `/tarantella/cgi-bin/secure/` directory.
2. Test that your web authentication scheme works.
3. Run the following command:

```
tarantella config edit --tarantella-config-server-cgibin-bootscrip
secure/wrapper_script_name
```

**Note** This command sets the path to the wrapper script and is relative to the `/opt/tarantella/var/docroot/cgi-bin` directory.

4. Restart the Secure Global Desktop server.

When this configuration is complete, enable web server authentication in Array Manager.

In a standard installation, Secure Global Desktop provides two such wrapper scripts:

- `ttaclientcert.cgi` for use with [PKI client certificates](#). This exports the `SSL_CLIENT_S_DN_CN` variable.
- `ttauthsafeword.cgi` for use with [SafeWord® PremierAccess™](#). This exports the `HTTP_SAFEWORD_USER` variable.

## The browser-based webtop

If you are using the browser-based webtop and your web authentication scheme uses another variable, you must configure the webtop web application to export your variable to `remote_user`. For example:

1. On the web server, configure your web authentication scheme to protect the `/sgd` URL.
2. Test that your web authentication scheme works.
3. Configure the web server to export *your\_variable\_name* so that the Tomcat component of the Secure Global Desktop Web Server can access it. To do this for Apache component of the Secure Global Desktop Web Server:
  1. Edit the `/opt/tarantella/webserver/apache/version/conf/httpd.conf` file.
  2. Add a line:

```
JkEnvVar your_variable_name " "
```
  3. Uncomment out the lines:

```
<Location "/sgd">
SSLOptions +StdEnvVars +ExportCertData
</Location>
```
  4. In the `//opt/tarantella/webserver/tomcat/version/webapps/sgd/resources/jsp` directory, edit the `sessionmanager.jsp` and `webtopsession.jsp` files so that they export *your\_variable\_name* to `remote_user`. Use the code for the `HTTP_SAFEWORD_USER` and `SSL_CLIENT_S_DN_CN` variables as examples of how to do this.
4. Restart the Secure Global Desktop Web Server and the Secure Global Desktop server.

When this configuration is complete, enable web server authentication in Array Manager.

By default, the `sessionmanager.jsp` and `webtopsession.jsp` files export:

- the `SSL_CLIENT_S_DN_CN` variable for use with [PKI client certificates](#).
- the `HTTP_SAFEWORD_USER` variable for use with [SafeWord® PremierAccess™](#).

## Related topics

- [Can I use PKI client certificates with web server authentication?](#)
- [Can I use SafeWord PremierAccess with web server authentication?](#)
- [Enabling web server authentication for the browser-based webtop](#)
- [Enabling web server authentication for the classic webtop](#)

## Trusted users and third party authentication

Third party authentication gives users access to Secure Global Desktop **without** having to authenticate to a Secure Global Desktop server. Secure Global Desktop is able to trust the third party authentication mechanism because client applications (such as the browser-based webtop) and the Secure Global Desktop server have a shared secret: the username and password of a trusted user.

In a standard installation, there is just one trusted user. However, you might want to create additional trusted users if you:

- relocate the browser-based webtop to a different JavaServer Pages (JSP) container on a different host.
- develop your own client applications, using the Secure Global Desktop `com.tarantella.tta.webservices.client.views` package, either on the same host as Secure Global Desktop or on a different host.
- have concerns about the security of the default trusted user.

You create and maintain the "database" of trusted users on the Secure Global Desktop server. Usually client applications only use the credentials of a single trusted user to access Secure Global Desktop services.

To create a new trusted user:

1. Stop the Secure Global Desktop Web Server: `tarantella webserver stop`.
2. Add the new trusted user to the "database" of trusted users on the Secure Global Desktop server.
  - Think of a username and password for the trusted user.
  - Use `tarantella webserver add_trusted_user username` to create the trusted user. When prompted, type the password.
  - Use `tarantella webserver list_trusted_users` to check the user has been created.
  - Check that the trusted user works by visiting `http://server/axis/services/rpc/externalauth`. When prompted, log in as the trusted user.
3. Add the new trusted user to the webtop web application.
  - Change to the `/opt/tarantella/webserver/tomcat/version/webapps/sgd/WEB-INF/classes` directory.
  - Run the following command to encode the username/password of the trusted user:

```
/opt/tarantella/bin/jre/bin/java \  
  com.tarantella.tta.webservices.client.views.SgdPasswd \  
  --encode trusted_username:password
```

- Copy the output.
- Edit the `/opt/tarantella/webserver/tomcat/version/webapps/sgd/WEB-INF/classes/com/tarantella/tta/webservices/client/views/Resources.properties` file.
- Replace the text after `sgdaccess=` with the output obtained above.
- Save the changes.

**Note** If you have relocated the webtop, you must perform this step on the remote host.

4. Start the Secure Global Desktop Web Server: `tarantella webserver start`.
5. Repeat these steps on each member of the array.

To change the password of an existing trusted user, you must first delete the user (`tarantella webserver delete_trusted_user`) and then follow the above steps to create the user again.

## Information for application developers

If you are using Secure Global Desktop web services to develop your own applications, the `ITarantellaExternalAuth` web service is used for third party authentication. This web service is protected with Basic web server authentication so that you can only access it using the credentials of a trusted user:

- The `http://server/axis/services/rpc/externalauth` URL is protected in the configuration file for the Axis web application: `/opt/tarantella/webserver/tomcat/version/webapps/axis/WEB-INF/web.xml`
- The Tomcat component of the Secure Global Desktop Web Server is configured to support Basic web server authentication using Tomcat's MemoryRealm and SHA digested passwords. This is in the Tomcat configuration file: `/opt/tarantella/webserver/tomcat/version/conf/server.xml`.
- The list of trusted users is stored in the Tomcat users configuration file: `/opt/tarantella/webserver/tomcat/version/conf/tomcat-users.xml`

The `tarantella webserver add_trusted_user` command is the only supported way to store trusted users on the Secure Global Desktop server.

If you have developed your own client applications using the `com.tarantella.tta.webservices.client.views` package, you can store the trusted user credentials for the application in the same way as the browser-based webtop (see step 3 above). Otherwise, you need to develop your own methods for storing the credentials.

Every time you make a change to a trusted user, you must restart the Secure Global Desktop Web Server.

### Related topics

- [Relocating the browser-based webtop to your own JSP container](#)
- [Web server/third party authentication](#)
- [The tarantella webserver `add\_trusted\_user` command](#)

## Login authorities

### Read this topic to...

- Learn what login authorities are and what they do.
- Learn what login authorities are available.
- Learn what login profiles are.

A login authority provides two services:

- It determines a user's identity by presenting user-supplied credentials to an authentication service.
- It determines a user's login profile, which also defines their webtop content.

Each login authority has its own rules for determining the identity and the login profile.

Secure Global Desktop has the following login authorities:

Login authority	Description
<a href="#">Anonymous user</a>	<ul style="list-style-type: none"><li>• Allows users to log in to Secure Global Desktop without using a username and password.</li><li>• All anonymous users have the same webtop content.</li></ul>
<a href="#">Authentication token</a>	<ul style="list-style-type: none"><li>• Allows users to log in to Secure Global Desktop if the Sun Secure Global Desktop Client supplies a valid authentication token.</li><li>• Users may have their own webtop content, depending on configuration.</li></ul> <p><b>Note</b> This login authority cannot be used with the <i>classic</i> webtop.</p>
<a href="#">ENS</a>	<ul style="list-style-type: none"><li>• Allows users to log in to Secure Global Desktop if they have person objects in ENS and UNIX/Linux accounts on the Secure Global Desktop host.</li><li>• Users have their own webtop content.</li></ul>

NT	<ul style="list-style-type: none"> <li>• Allows users to log in to Secure Global Desktop if they belong to a specified Windows domain.</li> <li>• Users may have their own webtop content, depending on configuration.</li> </ul>
LDAP	<ul style="list-style-type: none"> <li>• Allows users to log in to Secure Global Desktop if they have an entry in an LDAP directory.</li> <li>• Users may have their own webtop content, depending on configuration.</li> </ul>
Active Directory	<ul style="list-style-type: none"> <li>• Allows users to log in to Secure Global Desktop if they have an account in an Active Directory domain.</li> <li>• Users may have their own webtop content, depending on configuration.</li> </ul>
UNIX Group	<ul style="list-style-type: none"> <li>• Allows users to log in to Secure Global Desktop if they have UNIX/Linux accounts on the Secure Global Desktop host.</li> <li>• All UNIX users in the same UNIX group have the same webtop content.</li> </ul>
UNIX User	<ul style="list-style-type: none"> <li>• Allows users to log in to Secure Global Desktop if they have UNIX/Linux accounts on the Secure Global Desktop host.</li> <li>• All UNIX users have the same webtop content.</li> </ul>
SecurID	<ul style="list-style-type: none"> <li>• Allows users with RSA SecurID tokens to log in to Secure Global Desktop.</li> <li>• Users may have their own webtop content, depending on configuration.</li> </ul>

When a user logs in, the enabled login authorities are tried in the order they are listed in Array Manager (the same as the table above). The first login authority that authenticates a user "wins" and no further login authorities are tried.

Secure Global Desktop Administrators can enable and disable each login authority independently. You can configure login authorities either in Array Manager using the Secure Global Desktop Login panel or by using the tarantella `config` command. Secure Global Desktop server authentication is configured array-wide.

## User identities

A successful authentication by a login authority results in an identity or fully qualified name. An identity is a TFN name assigned by a login authority and is the Secure Global Desktop idea of who a user is. The identity is associated with the user's webtop session, their emulator sessions and their entries in the application server password cache.

The identity is not necessarily the name of a person object in ENS. For example, the UNIX User login authority assigns identities in the `.../_user` namespace. This is because it authenticates against the



UNIX/Linux user database.

## Login profiles

A user's webtop content and other Secure Global Desktop-specific settings are controlled by a login profile. Each login authority has its own set of rules for determining the login profile. Login profiles are **always** objects in ENS (this is why they are sometimes called ENS equivalents). A login profile can be a standard person object or a profile object stored in the Tarantella System Objects organization.

For example, although the UNIX Group login authority assigns identities in the `.../_user` namespace, the login profile is always the profile object `.../_ens/o=Tarantella System Objects/cn=UNIX User Profile`.

To allow you to monitor sessions from Object Manager, all webtop and emulator sessions are shown on the Sessions tab for login profiles, not for identities. This is because Object Manager only lets you search and browse ENS and many identities are in other namespaces.

### Related topics

- [Secure Global Desktop Login properties \(array-wide\)](#)
- [Introducing web server authentication](#)
- [Web server/third party authentication](#)

## The Anonymous user login authority

### Overview

The Anonymous user login authority allows users to log in without using a username and password.

As users are anonymous, Secure Global Desktop assigns each anonymous user a temporary identity. The identity is only effective while the user is logged in.

This login authority is disabled by default.

### Logging in

Web browser users log in by clicking the Log in button on the Secure Global Desktop login page, leaving the username and password blank.

If you are using the classic webtop, you can also log in by visiting the following URL:

```
http://server/tarantella/kiosk.html
```

If you are using the Sun Secure Global Desktop Native Client to access the classic webtop, there is a checkbox on the login dialog that allows you to log in anonymously.

### Authentication

1. This login authority authenticates users if the username and password are both blank.
2. If either a username or a password is supplied, the next login authority is tried.
3. If both the username and the password are blank, then the user may log in.

### User identity

As the user does not supply a username or password when they log in, Secure Global Desktop assigns a temporary identity which has the form `.../_dns/server/_anon/number`.

### Login profile

The profile object `o=Tarantella System Objects/cn=Anonymous Profile` is always used for the login profile.

This means all anonymous users receive the same webtop content.

## Emulator sessions and password cache entries

Each user logged in anonymously has independent emulator sessions. These emulator sessions end automatically when the user logs out (or closes the web browser) **even if** the application is configured to be always resumable.

All password cache entries belong to the `o=Tarantella System Objects/cn=Anonymous User Profile` object in ENS. This means that all anonymous users share the same application server passwords. Anonymous users aren't allowed to add or change password cache entries. Use the `tarantella passcache` command to manage application server passwords for anonymous users.

### Related topics

- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)

## The authentication token login authority

### Overview

The authentication token login authority allows users to log in to Secure Global Desktop if the Sun Secure Global Desktop Client submits a valid authentication token.

This login authority is disabled by default.

To use this login authority:

1. The user must log in and be authenticated by another login authority or third party authentication.
2. The user must generate an authentication token.
3. The Secure Global Desktop Client must be configured to operate in [integrated mode](#).

See [Using the authentication token login authority for automatic logins](#) for details of how to configure this login authority.

**Note** The authentication token login authority can only be used with the Secure Global Desktop Client. The Native Client and Java™ technology clients do not support this login authority.

### Logging in

When the Secure Global Desktop Client starts, it submits the authentication token to Secure Global Desktop. The user does not enter a username or password.

### Authentication

1. This login authority authenticates a user if the Secure Global Desktop Client submits a valid authentication token.
2. If the authentication token is valid, the user is logged in.
3. If the authentication token is invalid or the Secure Global Desktop Client does not submit a token, the Secure Global Desktop login dialog is displayed in a web browser so that the user can log in and be authenticated with another login authority or authentication method.

### User identity and login profile

The Secure Global Desktop server stores the authentication token against the identity of the user when they generated their authentication token. This means the identity and login profile used are those of the login authority that originally authenticated the user, for example:

Original authentication	Identity	Login Profile
UNIX user	.../_user/indigo	.../_ens/o=Tarantella System Objects/ cn=UNIX User Profile
ENS	.../_ens/o=Indigo Insurance/ cn=Indigo Jones	.../_ens/o=Indigo Insurance/cn=Indigo Jones
LDAP	.../_service/sco/tta/ldapcache/ dc=com/dc=Indigo Insurance/ cn=Indigo Jones	.../_ens/o=Tarantella System Objects/ cn=LDAP Profile
Third party	.../_service/sco/tta/thirdparty/ indigo	.../_ens/o=Tarantella System Objects/ cn=Third Party Profile

## Emulator sessions and password cache entries

Emulator sessions and password cache entries belong to the identity of the original authentication.

### Related topics

- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)
- [Using the authentication token login authority for automatic logins](#)

## Using the authentication token login authority for automatic logins

The [authentication token login authority](#) allows users to log in automatically to Secure Global Desktop if the Sun Secure Global Desktop Client submits a valid authentication token to the Secure Global Desktop server. Authentication tokens can only be used when the Secure Global Desktop Client is operating in [integrated mode](#).

To enable automatic logins:

1. Secure Global Desktop Administrators must enable the authentication token login authority.
2. Users must enable integrated mode and generate an authentication token.

**Note** The authentication token login authority can only be used with the Secure Global Desktop Client. The Native Client and Java™ technology clients do not support this login authority.

The Secure Global Desktop Release Notes has details of which client desktop systems support running the Secure Global Desktop Client in integrated mode.

### Enabling the authentication token login authority

To be able to use the authentication token login authority, at least one other authentication mechanism must also be enabled. This is because the user must log in at least once and display a webtop in order to generate an authentication token. You can use [third party authentication](#) or any of the other [login authorities](#), apart from the anonymous user login authority.

To enable the authentication token login authority:

1. In Array Manager, display Secure Global Desktop Login properties.
2. Check the Authentication token login authority box.
3. Check the Generate authentication tokens box.
4. Click Apply.

### Enabling integrated mode and generating authentication tokens

To use automatic logins, integrated mode and automatic logins must be enabled in the user's profile. Secure Global Desktop Administrators can configure this for users by creating profiles for organization and organizational unit objects. However, users have to manually generate an authentication token by

editing their profile. This means [profile editing](#) must be enabled for users.

To generate an authentication token, users:

1. Log in to Secure Global Desktop and display a webtop.
2. Click the Edit button on the Applications area of the webtop.
3. Click the Client Settings tab.
4. Check the Automatic Client Login box.
5. Check the Add applications to Start Menu box.
6. Click Save.

Users must generate an authentication token for **each** Secure Global Desktop server they log in to.

**Note** Users must log out of Secure Global Desktop and log in again for changes to their profile to take effect.

If users need to generate a new authentication token, they must edit their profile as follows:

1. Clear the Automatic Client Login box.
2. Click Save.
3. Check the Automatic Client Login box.
4. Click Save.

## **Administering the authentication token login authority**

When a user saves their profile, the Secure Global Desktop server sends the authentication token to the Secure Global Desktop Client. The Secure Global Desktop Client stores the token in the [profile cache](#) on the client device.

To ensure an authentication token cannot be intercepted and used by a third party, use [secure \(HTTPS\) web servers](#) and [enable Secure Global Desktop security services](#).

When a user generates an authentication token, Secure Global Desktop server maintains a record of the tokens issued in a token cache. Secure Global Desktop stores the authentication tokens using the current identity of the user when the token was generated. When a user logs in with an authentication token, the authentication token allows Secure Global Desktop to "remember" the user's original identity and login profile. All webtop sessions and emulator sessions are managed using the original identity and profile. If the original login becomes invalid, for example because the UNIX account is disabled or the password has expired, the user can still log in automatically if they have a valid token. However they will not be able to launch any applications using the invalid login.

Administrators use the `tarantella tokencache` command to list the tokens in the token cache and delete them. Deleting a token from the token cache makes the token stored on a client device invalid. If the Secure Global Desktop Client presents an invalid token, the user is prompted to log in with a username and password. The user must then generate another authentication token if they want to log in automatically.

Administrators can disable the ability to generate new tokens by clearing the Generate authentication tokens box on the Secure Global Desktop Login properties panel in Array Manager. Clearing this box disables the Automatic Client Login option when users edit their profile. If the authentication token login authority is still enabled, users with existing authentication tokens can still log in.

To troubleshoot problems with automatic logins, set a `server/login/*` and a `server/tokencache/*` **log filter**. The `server/login/*` filter allows you see when authentication tokens are being used for authentication and when they fail. The `server/tokencache/*` filter allows you to see errors with operations on the token cache, for example to see why a token has not been added to the cache.

#### Related topics

- [The authentication token login authority](#)
- [The tarantella tokencache command](#)



## The ENS login authority

### Overview

The ENS login authority allows users to log in to Secure Global Desktop if they have person objects in ENS and UNIX/Linux accounts on the Secure Global Desktop host.

This login authority is enabled by default.

### Logging in

The user types either a common name (for example "Indigo Jones"), a username (for example "indigo") or an email address (for example "indigo@indigo-insurance.com").

### Authentication

1. This login authority searches ENS for a [person object](#) with a [Name](#) attribute that matches what the user typed. If there's no match, the search is repeated on the [Username](#) attribute, and finally on the [Email Address](#) attribute.
2. If no person object is found, the next login authority is tried.
3. If a person object is found, the [Username](#) attribute of that object is treated as a UNIX/Linux username. This username, and the password typed by the user, are checked against the UNIX/Linux user database.
4. If the authentication fails, the next login authority is tried.
5. If the authentication succeeds, then the user may log in if the [May Log In To Secure Global Desktop](#) attribute for their person object is checked. If this attribute is cleared, the user may not log in and no further login authorities are tried.

### User identity

The matching person object in ENS is used for the user identity.

### Login profile

The matching person object in ENS is used for the user identity.

### Emulator sessions and password cache entries

Emulator sessions and password cache entries belong to the person object.

## Secure Global Desktop and PAM

Secure Global Desktop supports Pluggable Authentication Modules (PAM). The ENS login authority uses PAM for user authentication, account operations and password operations.

When you install Secure Global Desktop, Secure Global Desktop Setup automatically creates PAM configuration entries for Secure Global Desktop by copying the current configuration for the `passwd` program.

- On Solaris Operating System platforms, entries are created in the `/etc/pam.conf` file.
- On Linux platforms, the `/etc/pam.d/tarantella` file is created.

### Related topics

- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)

## The NT login authority

### Overview

The NT login authority allows users to log in to Secure Global Desktop if they belong to a specified Windows domain.

This login authority is disabled by default.

### Logging in

The user types either a common name (for example "Indigo Jones"), a username (for example "indigo") or an email address (for example "indigo@indigo-insurance.com").

### Authentication

1. This login authority searches ENS for a [person object](#) with a [Name](#) attribute matching what the user typed. If there's no match, the search is repeated on the [Username](#) attribute, and finally on the [Email Address](#) attribute.
2. If a person object is found, the Username attribute of the object is treated as the NT username.
3. If no person object is found, the name the user typed is used as the NT username.
4. The NT username and the password typed by the user are checked against the domain controller.
5. If the authentication fails, the next login authority is tried.
6. If the authentication succeeds, the user may log in **unless**:
  - there was a matching person object **and**
  - the [May Log In To Secure Global Desktop](#) attribute for that person object is cleared.

### User identity

If a person object was found in ENS, that object is used as the identity.

If no person object was found in ENS, the identity is `.../_service/sco/tta/ntauth/NT-username`.

### Login profile

If a person object was found in ENS, that object is used as the login profile.

If no person object was found in ENS, the profile object `o=Tarantella System Objects/cn=NT User Profile` is used.

## Emulator sessions and password cache entries

Emulator sessions and password cache entries belong to the NT user.

### Related topics

- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)

## Enabling the NT login authority

To enable the NT login authority:

1. In Array Manager, click Secure Global Desktop Login, Properties.
2. Check the Login Authorities, NT login authority box.
3. In the Windows NT Domain field, type the name of the domain to authenticate NT users against.

## Authenticating users from more than one domain

If you need to authenticate users from more than one domain, you must have one domain that is trusted by all the other domains. You must use the trusted domain as the Windows domain setting in Array Manager.

When a user in another domain logs in to Secure Global Desktop, they must use the format `domain\username` for their username. If they do not use this format, Secure Global Desktop will try to authenticate the user using the authentication domain and fail.

**Note** The [Windows NT domain \(--ntdomain\)](#) attribute for person objects plays no part in the Secure Global Desktop login.

## If the Secure Global Desktop server is on a different subnet

If the Secure Global Desktop server is on a different subnet to the domain controller, you must hard code the authentication machine by running the following commands:

```
tarantella stop

tarantella config edit \
  --com.sco.tta.server.login.ntauth.NTAuthService.properties-authConfig
authnbt=NTNAME

tarantella config edit \
  --com.sco.tta.server.login.ntauth.NTAuthService.properties-authConfig-
append authserver=my.domain.name

tarantella start
```

where *NTNAME* is the NetBIOS name of the domain controller and *my.domain.name* is the DNS name or IP address of the domain controller.

## About NT usernames and passwords

The NT login authority supports 8-bit case-sensitive NT passwords. The NT username can contain any characters.

### Related topics

- [The NT login authority](#)
- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)

## The LDAP login authority

### Overview

The LDAP login authority allows users to log in to Secure Global Desktop if they have an entry in an LDAP directory.

This login authority is disabled by default.

### Logging in

The user types either a common name (for example "Indigo Jones"), a username (for example "indigo") or an email address (for example "indigo indigo-insurance.com").

### Authentication

1. This login authority searches the LDAP directory for a person object with a `cn` (common name) attribute that matches what the user typed. If there's no match, the search is repeated on the `uid` (username) attribute, and finally on the `mail` (email address) attribute.
2. If a person object is not found, the next login authority is tried.
3. If a person object is found, the password typed by the user is checked against the LDAP person object.
4. If the authentication fails, the next login authority is tried.
5. If the authentication succeeds, the login authority searches ENS for an object to use as the login profile (see below). If the [May Log In To Secure Global Desktop](#) attribute for the login profile is cleared, the user may not log in and no further login authorities are tried.

### User identity

The identity is the LDAP person object and has the form `.../_service/sco/tta/ldapcache/LDAP-person`.

### Login profile

The first match of the following is used:

1. A person object in ENS with the same name as the LDAP person object, allowing for differences in the naming system. For example, if the LDAP object `cn=Indigo Jones`,

`ou=Administration,o=Indigo Insurance` is found, this login authority would search ENS for `o=Indigo Insurance/ou=Administration/cn=Indigo Jones`.

2. A person object in ENS, with the name `cn=LDAP Profile`, in the same OU as the LDAP person object. For example, `o=Indigo Insurance/ou=Administration/cn=LDAP Profile`.
3. A person object in ENS, with the name `cn=LDAP Profile`, in any parent OU for the LDAP person object. For example, `o=Indigo Insurance/cn=LDAP Profile`.
4. The default LDAP profile object `o=Tarantella System Objects/cn=LDAP Profile`.

## Emulator sessions and password cache entries

Emulator sessions and password cache entries belong to the LDAP person object.

### Related topics

- [Enabling the LDAP login authority](#)
- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)



## Enabling the LDAP login authority

To use LDAP directory servers to authenticate users to Secure Global Desktop, you need to enable the LDAP login authority. To do this:

1. Make sure **all** the Secure Global Desktop servers in the array can contact each LDAP directory server you will be using for authentication.
2. In Array Manager, open Secure Global Desktop Login properties.
3. Check the LDAP login authority box.
4. In the URL field, type the URL of one or more LDAP directory servers, for example `ldap://melbourne.indigo-insurance.com`.
  - To secure the connections to LDAP directory servers with SSL/TLS, [follow these instructions](#).
  - Separate each URL with a semicolon.
  - If you enter more than one URL, the URLs are used in the order they are listed. If the first LDAP directory server listed is unavailable, Secure Global Desktop tries the next one in the list.
  - The standard port used for connections to LDAP directory servers is 389/tcp. If the LDAP directory server uses a different port, you must specify the port number as part of the URL, for example `ldap://melbourne.indigo-insurance.com:5678`.
  - Normally, the LDAP login authority searches the entire LDAP directory. You can restrict the search to part of the LDAP directory by adding a search root to the end of the URL, for example `ldap://melbourne.indigo-insurance.com/dc=indigo-insurance,dc=com`
5. Enter the details of an LDAP user in the Username and Password fields.
  - The username must be the distinguished name of the user, for example `cn=tarantella-ldap,cn=Users,dc=indigo-insurance,dc=com`.
  - Some LDAP directory servers support anonymous logins, so you don't need to supply a username or password. Others, including Microsoft Active Directory, require the username and password of a user that has sufficient privileges to search the LDAP directory.
  - You might want to create a special LDAP user reserved for the Secure Global Desktop LDAP login authority.
  - As you can only enter one username and password, this user must be able to search all LDAP directory servers listed in the URL box.
6. Click Apply.

Once the LDAP login authority is enabled, users can log in to Secure Global Desktop using either:

- their full name (common name or `cn`)
- their uid
- their e-mail address or
- their SAM account name.

Users then receive the webtop that has been configured for them using:

- [LDAP user login profile objects](#) and
- [Directory Services Integration](#).

## Password expiry

Secure Global Desktop can prompt a user for a new password if their password has expired on the LDAP directory server. When a user attempts to log in with an expired password, the aged password dialog displays. This dialog:

- confirms that the password has expired and
- allows the user to enter and confirm a new password.

If the new password is accepted, the user is logged in to Secure Global Desktop.

## Sun One Directory Server

For Sun One Directory Servers:

- do not use the "User must change password after reset" option either in the global password policy or for an individual password policy. This causes the password change to fail.
- The LDAP user entered in the Username and Password fields on the Secure Global Desktop properties panel in Array Manager must have administrative privileges.

## Microsoft Active Directory

With Microsoft Active Directory, password expiry (including forcing the user to change their password at next logon) can only be handled if there is a secure (SSL) connection between the Secure Global Desktop server and the Active Directory server. See [Securing connections to LDAP directory servers](#) for details.

## LDAP timeouts

Secure Global Desktop uses two timeouts to control what happens in the event of an LDAP failure.

The LDAP discovery timeout controls how long Secure Global Desktop waits for an LDAP directory server to respond to the initial contact request. The default is 30 seconds. To change this timeout, run the following command:

```
tarantella config edit --tarantella-config-ldap-discovery-timeout secs
```

The LDAP timeout controls how long Secure Global Desktop waits for an LDAP directory server to respond to LDAP operations, such as requests for data. The default is 30 seconds. To change this timeout, run the following command:

```
tarantella config edit --tarantella-config-ldap-timeout secs
```

With both timeouts, Secure Global Desktop makes two attempts to contact the LDAP directory server. If there is no response, Secure Global Desktop tries the next LDAP directory server listed in the URL field on the Secure Global Desktop Login properties panel in Array Manager. If all LDAP directory servers time out, users can't be authenticated with the LDAP login authority and webtop content can't be generated.

### Related topics

- [The LDAP login authority](#)
- [Securing connections to Active Directory and LDAP directory servers](#)
- [Mirroring your LDAP organization in ENS](#)
- [Using Directory Services Integration](#)
- [LDAP users can't log in to Secure Global Desktop](#)
- [Can I deny an LDAP user access to Secure Global Desktop?](#)
- [The tarantella passcache new command](#)

## LDAP users can't log in to Secure Global Desktop

If you are using the LDAP login authority to authenticate users and you find that LDAP users are not able to log in to Secure Global Desktop, use the following checklist to identify the source of the problem.

You may also find it helpful to turn on extra logging in Array Manager. Select the [Array properties](#) panel and add a `server/login/*` and a `server/ldap/*` filter in the Log Filter box.

Things to check	Notes
Is the LDAP login authority enabled?	<p>You cannot use an LDAP directory server with Secure Global Desktop unless the LDAP login authority is enabled.</p> <p>Use the <a href="#">Secure Global Desktop Login</a> properties in Array Manager (or use the <code>tarantella config edit --login-ldap 1</code> command) to enable the LDAP login authority.</p>
Are the URLs of the LDAP directory servers correct?	<p>To be able to use the LDAP login authority, each Secure Global Desktop server must be able to contact the LDAP directory servers at the specified URLs.</p> <p>Use the <a href="#">Secure Global Desktop Login</a> properties in Array Manager (or use the <code>tarantella config view --login-ldap-url</code> command) to check the URLs of the LDAP directory servers. Check:</p> <ul style="list-style-type: none"><li>• Does each URL refer to a valid LDAP directory server?</li><li>• Is each URL separated by a semicolon?</li><li>• Does the URL use the fully qualified name of the LDAP directory server?</li><li>• If the LDAP directory server listens on a non-standard port, is the port number the LDAP directory server listens on included in the URL?</li><li>• Can <b>all</b> Secure Global Desktop servers in the array contact the LDAP directory server at this URL? Can you <code>telnet</code> from the Secure Global Desktop server to the LDAP directory server?</li><li>• If you have used a search root to restrict the start point of the search of the LDAP database, check that the search root is correct.</li><li>• Do the log files indicate that the connection to the LDAP directory</li></ul>

server is timing out? Try increasing the [LDAP timeouts](#).

For Sun™ ONE (formerly Netscape or iPlanet) Directory Server, you may also need to do some extra configuration to map ENS names to LDAP names correctly. For example, the LDAP directory server has a `c=country,o=org,ou=office` structure and is configured to only allow searches under `o=org,c=country`. If ENS has an `o=org,ou=office` structure, then Secure Global Desktop will attempt to search the LDAP database using `o=org` which will fail. To correct this:

1. Use the `tarantella stop` command to stop the Secure Global Desktop server.
2. Run the following command:  

```
tarantella config edit --com.sco.tta.server.login.ens.LdapProfileCandidateAuthority.properties-ensMapping search_root
```

where, for example, `search_root` is `c=country`.
3. Use the [Secure Global Desktop Login](#) properties in Array Manager (or use the `tarantella config edit --login-ldap-url` command) to change the search root for the LDAP server, for example `ldap://server_URL/o=org,c=country`.
4. Use the `tarantella start` command to start the Secure Global Desktop server.
5. Repeat these steps on each member of the array.

Is the LDAP directory server username and password correct?

Some LDAP directory servers support anonymous logins, so you don't need to supply a username or password. Others, including Microsoft Active Directory, require the username and password of a user that has sufficient privileges to search the LDAP database.

Use the [Secure Global Desktop Login](#) properties in Array Manager (or use the `tarantella passcache list --ldap username` command) to check the username and password.

If you are you using secure connections to the LDAP directory server, has this been configured correctly?

Check:

- Does the URL of the LDAP directory server begin `ldaps://`?
- Are Secure Global Desktop security services running?  
Use the `tarantella status` command to check.
- Has the root certificate for each LDAP directory server been imported into the `cacerts` keystore on each Secure Global Desktop server?
- If you are using Microsoft Active Directory, does each Secure Global Desktop server have a valid client certificate?

See [Securing connections to LDAP directory servers](#) for details.

Is Secure Global Desktop providing the right information for locating the user?

When Secure Global Desktop searches an LDAP database for a user it uses the following attributes:

- their full name (common name or `cn`)
- their `uid`
- their e-mail address or
- their SAM account name.

If these attributes are not sufficient for identifying users, you can add extra attributes:

1. Use the `tarantella stop` command to stop the Secure Global Desktop server.
2. Run the following command:  

```
tarantella config edit --searchldapla.properties-  
searchAttributes-append attributes
```

You can list more than one attribute. Each attribute must be separated by a space. The default attributes are `cn uid mail sAMAccountName`.
3. Use the `tarantella start` command to start the Secure Global Desktop server.
4. Repeat these steps on each member of the array.

**Note** These steps require caution as any mistakes can result in all users being unable to log in.

Have recent LDAP configuration changes taken effect?

After making changes to your LDAP database, it is advisable to wait for a period of time for the changes to take effect.

Secure Global Desktop caches the data it collects from an LDAP directory server. If you find that Secure Global Desktop is not detecting changes, you can manually flush the cached data with the [tarantella cache](#) command.

### Related topics

- [The LDAP login authority](#)
- [Enabling the LDAP login authority](#)
- [Using Directory Services Integration](#)
- [Can I deny an LDAP user access to Secure Global Desktop?](#)

## Can I deny an LDAP user access to Secure Global Desktop?

Once you have [enabled the LDAP login authority](#), any LDAP user who can access a Secure Global Desktop server can log in to Secure Global Desktop. However, you may not want all LDAP users to have access to Secure Global Desktop.

The solution is to configure a search filter on the Secure Global Desktop server so that only users, who have a required attribute value on their LDAP user object, can log in to Secure Global Desktop. This requires extra configuration on the LDAP directory server and on the Secure Global Desktop server.

**Note** You can't use this method to deny access to a user authenticated with the [Active Directory login authority](#). This is because the Active Directory server is not used for authentication.

### Configuring the attribute on the LDAP user object

For Secure Global Desktop to be able to apply a filter, it must be able to test for an attribute value on the user object in your LDAP directory server. You could use an attribute that already exists in your LDAP database or create a new attribute, for example an attribute called `allowttallogin`. This attribute must be set for all users in your organization.

### Configuring an LDAP search filter on the Secure Global Desktop server

Once you have configured the LDAP user object attribute, you need to configure a search filter on the Secure Global Desktop server. The filter needs to test the LDAP attribute, to allow users to log in if they meet the condition(s).

To set a search filter:

1. Use the `tarantella stop` command to stop the Secure Global Desktop server.
2. Run the following command:  

```
tarantella config edit --searchldapla.properties-searchFilter (&({0}={1})  
(attribute_test))
```

For example:

```
tarantella config edit --searchldapla.properties-searchFilter (&({0}={1})  
(allowttallogin=true))
```
3. Use the `tarantella start` command to start the Secure Global Desktop server.



After you have re-started Secure Global Desktop, only users who match the search filter will be able to log in to Secure Global Desktop.

### Related topics

- [The LDAP login authority](#)
- [Enabling the LDAP login authority](#)
- [LDAP users can't log in to Secure Global Desktop](#)

## The Active Directory login authority

### Overview

The Active Directory login authority allows users to log in to Secure Global Desktop if they have an account in an Active Directory domain.

This login authority uses a combination of Kerberos authentication and LDAP searches of Active Directory servers, which makes it faster and more secure than the [LDAP login authority](#). It is also more scalable and flexible as users can be authenticated against any domain in a forest and Active Directory is used to provide information about users instead of ENS.

This login authority is disabled by default.

### Logging in

The user types a user principal name (an account logon name and a domain name joined by the " " sign, for example "indigo indigo-insurance.com") and password.

### Authentication

1. This login authority uses the Kerberos protocol to authenticate the user principal name and password against a Key Distribution Center (KDC) for a domain.
2. If the authentication fails, the next login authority is tried.
3. If the authentication succeeds, the user may log in.

### User identity

Once a user has been authenticated, Secure Global Desktop searches an Active Directory server in the domain for an LDAP person object for the user.

The identity is the LDAP person object and has the form `.../_service/sco/tta/ldapcache/LDAP-person`.

### Login profile

The first match of the following is used:

1. A person object in ENS with the same name as the LDAP person object, allowing for differences in the naming system. For example, if the LDAP object `cn=Indigo Jones, cn=Administration, dc=Indigo Insurance, dc=com` is found, this login authority would search ENS for `dc=com/dc=Indigo Insurance/cn=Administration/cn=Indigo Jones`.
2. A person object in ENS, with the name `cn=LDAP Profile`, in the same OU as the LDAP person object. For example, `dc=com/dc=Indigo Insurance/cn=Administration/cn=LDAP Profile`.
3. A person object in ENS, with the name `cn=LDAP Profile`, in any parent OU for the LDAP person object. For example, `dc=com/dc=Indigo Insurance/cn=LDAP Profile`.
4. The default LDAP profile object `o=Tarantella System Objects/cn=LDAP Profile`.

## Emulator sessions and password cache entries

Emulator sessions and password cache entries belong to the LDAP person object.

### Related topics

- [Enabling the Active Directory login authority](#)
- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)

## Enabling the Active Directory login authority

The Active Directory login authority works by authenticating users against a Key Distribution Center (KDC) for a domain and then generating users' webtops using LDAP searches of an Active Directory server. To enable the Active Directory login authority, you need to:

1. Configure Kerberos authentication.
2. Configure the LDAP search and default domain details.

Once the Active Directory login authority is enabled, users can log in to Secure Global Desktop using their user principal name. They then receive the webtop that has been configured for them using:

- [LDAP user login profile objects](#) and
- [Directory Services Integration](#).

## Configuring Kerberos authentication

To configure Kerberos authentication, follow this process for each Secure Global Desktop server in the array:

1. Ensure the time on the Secure Global Desktop server is synchronized with the KDC servers in the domains.
2. Stop the Secure Global Desktop server, `tarantella stop`.
3. Create or edit the Kerberos configuration file.
4. Start the Secure Global Desktop server, `tarantella start`.

## Synchronizing time

The synchronized time between the KDC and the Secure Global Desktop server must be within the Maximum tolerance for computer clock synchronization defined for the Kerberos security policy and the Default domain security policy on the Windows 2000/2003 server.

## Kerberos configuration file

The Kerberos configuration file (`krb5.conf`) specifies which KDC servers Secure Global Desktop authenticates against for a particular domain.

You can either:

- edit your system default configuration file, usually found in either the `/etc` directory (on Linux) or the `/etc/krb5` directory (on Solaris) or
- create a configuration file for use only with Secure Global Desktop. Put the file in the `/opt/tarantella/bin/jre/lib/security` directory.

The configuration file contains several [sections which control Kerberos authentication](#). As a minimum, the file must contain the following sections:

- `[libdefaults]` this sets defaults for Kerberos authentication. You must set the `default_realm` and `default_checksum`.
- `[realms]` this sets the KDCs for each Kerberos realm. A realm can have more than one KDC. The entry for each KDC has the form `hostname:port`. The port can omitted if port 88 (the default) is being used.
- `[domain_realm]` this maps Active Directory domains to Kerberos realms.

For example:

```
[libdefaults]
default_realm = INDIGO-INSURANCE.COM
default_checksum = rsa-md5

[realms]
INDIGO-INSURANCE.COM = {
    kdc = melbourne.indigo-insurance.com
}
EAST.INDIGO-INSURANCE.COM = {
    kdc = ad01.east.indigo-insurance.com
    kdc = ad02.east.indigo-insurance.com
}
WEST.INDIGO-INSURANCE.COM = {
    kdc = ad01.west.indigo-insurance.com
}

[domain_realm]
indigo-insurance.com = INDIGO-INSURANCE.COM
.east.indigo-insurance.com = EAST.INDIGO-INSURANCE.COM
east.indigo-insurance.com = EAST.INDIGO-INSURANCE.COM
.west.indigo-insurance.com = WEST.INDIGO-INSURANCE.COM
west.indigo-insurance.com = WEST.INDIGO-INSURANCE.COM
```

## Password expiry

Secure Global Desktop can be configured to prompt a user for a new password if their password has expired. To be able to do this the Kerberos configuration file must be configured with the details of the server that handles the password change.

On **each member of the array**, edit the Kerberos configuration file and for **each realm** add:

- a `kpasswd_server = hostname:port` and/or an `admin_server = hostname:port` line. This identifies the Kerberos administration server that will handle the password change. If `kpasswd_server` is omitted, the `admin_server` is used instead. The port can be omitted if port 464 (the default) is being used.
- a `kpasswd_protocol = protocol` line. This sets the protocol to be used when communicating with the `admin_server` or `kpasswd_server`. For Active Directory, this must be `SET_CHANGE`.

For example:

```
EAST.INDIGO-INSURANCE.COM = {  
  kdc = ad01.east.indigo-insurance.com  
  kdc = ad02.east.indigo-insurance.com  
  admin_server = ad01.east.indigo-insurance.com  
  kpasswd_protocol = SET_CHANGE  
}
```

## TCP/UDP preference configuration

When sending messages to the KDC or the Kerberos administration server, Secure Global Desktop uses either the UDP or TCP protocols. The protocol used is determined by the `udp_preference_limit` line in the `[libdefaults]` section of the Kerberos configuration file. This line sets the maximum size (in bytes) for packets that can be sent using UDP. If the message is larger than this size, TCP is used. If the KDC or administration server indicates that the package is too big, TCP is used instead. To always use TCP, use `udp_preference_limit = 1`.

## KDC timeout

You can configure a KDC timeout in the event of a failure in the authentication process. The KDC timeout controls how long Secure Global Desktop waits for a reply from a KDC and how many times it tries to contact each KDC.

To set the KDC timeout, add the following lines to the `[libdefaults]` section of the Kerberos configuration file:

```
kdc_timeout = time
max_retries = number
```

The `kdc_timeout` sets the maximum number milliseconds to wait for a reply from a KDC. The `max_retries` is the maximum number of times each KDC is tried. The KDCs for each realm are tried in the order they are listed in the `[realms]` section of the Kerberos configuration file.

If Secure Global Desktop can't contact any KDCs for the user's realm, the authentication phase will fail.

## Configuring the LDAP search and default domain details

1. In Array Manager, open Secure Global Desktop Login properties.
2. Check the Active Directory login authority box.
3. In the URL field, enter the name of an Active Directory domain, for example `ad://east.indigo-insurance.com`.
  - o The URL **must** start with `ad://`.
  - o Only enter one URL.
  - o Secure Global Desktop uses the domain name to perform a DNS lookup to obtain a list of Global Catalog servers. The Global Catalog is used to determine which Active Directory servers Secure Global Desktop can search to determine the user's login profile.
4. Configure whether Secure Global Desktop connects to Active Directory using a secure or a standard connection.
  - o **secure connections** - check the Use Certificates box and [follow these instructions](#).
  - o **standard connections** - in the Username and Password fields, enter the details of a user that has privileges to search Active Directory. The username must be the user principal name, for example `tarantella-ldap@indigo-insurance.com`. You might want to create a special user reserved for the Active Directory login authority.
5. In the Base Domain and Default Domain fields, enter the domains you want Secure Global Desktop to use when users enter incomplete domain information when they log in.
  - o The base domain is used when users only supply a partial domain when they log in. For example, if the root domain is set to "indigo-insurance.com" and a user logs in with the username "rouge west", the Active Directory login authority tries to authenticate "rouge west.indigo-insurance.com".
  - o The default domain is used when users do not supply a domain when they log in. For example, if the default domain is set to "east.indigo-insurance.com" and a user logs in with the username "rouge", the Active Directory login authority tries to authenticate "rouge east.indigo-insurance.com".
6. Click Apply.

## LDAP timeouts

You can configure two LDAP timeouts in the event that the LDAP searches of an Active Directory server fail.

The **LDAP discovery timeout** controls how long Secure Global Desktop waits for an Active Directory server to respond to the initial contact request. The default is 30 seconds. To change this timeout, run the following command:

```
tarantella config edit --tarantella-config-ldap-discovery-timeout secs
```

The **LDAP timeout** controls how long Secure Global Desktop waits for an Active Directory server to respond to LDAP operations, such as requests for data. The default is 30 seconds. To change this timeout, run the following command:

```
tarantella config edit --tarantella-config-ldap-timeout secs
```

With both timeouts, Secure Global Desktop makes two attempts to contact the Active Directory server. If there is no response, Secure Global Desktop tries another Active Directory server. The list of Active Directory servers for a domain is obtained from the Global Catalog. If all Active Directory servers time out, webtop content can't be generated.

## LDAP cache

Secure Global Desktop caches the LDAP data it collects from Active Directory. If you find that Secure Global Desktop is not detecting changes, you can manually flush the cached data with the [tarantella cache](#) command.

### Related topics

- [The Active Directory login authority](#)
- [Mirroring your LDAP organization in ENS](#)
- [Using Directory Services Integration](#)



## The UNIX group login authority

### Overview

The UNIX group login authority allows users to log in to Secure Global Desktop if they have UNIX/Linux accounts on the Secure Global Desktop host. All users in the same UNIX/Linux group have the same webtop content.

This login authority is enabled by default.

### Logging in

The user types a UNIX/Linux username and password.

### Authentication

1. This login authority checks the username and password against the UNIX/Linux user database.
2. If the authentication fails, the next login authority is tried.
3. If the authentication succeeds, the user may log in if the [May Log In To Secure Global Desktop](#) attribute for the login profile is checked. If this attribute is cleared, the user may not log in and no further login authorities are tried.

### User identity

The identity is always `.../_user/UNIX-username`.

### Login profile

The login authority searches ENS for a person object `cn=gid`, where `gid` is the UNIX group ID. If found, this is used as the login profile. If the user belongs to more than one group, the user's primary or effective group is used.

If no person object is found in ENS, the profile object `o=Secure Global Desktop System Objects/cn=UNIX User Profile` is used.

### Emulator sessions and password cache entries

Emulator sessions and password cache entries belong to the UNIX user.

## Secure Global Desktop and PAM

Secure Global Desktop supports Pluggable Authentication Modules (PAM). The UNIX group login authority uses PAM for user authentication, account operations and password operations.

When you install Secure Global Desktop, Secure Global Desktop Setup automatically creates PAM configuration entries for Secure Global Desktop by copying the current configuration for the `passwd` program.

- On Solaris Operating System platforms, entries are created in the `/etc/pam.conf` file.
- On Linux platforms, the `/etc/pam.d/tarantella` file is created.

### Related topics

- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)

## The UNIX user login authority

### Overview

The UNIX group login authority allows users to log in to Secure Global Desktop if they have UNIX/Linux accounts on the Secure Global Desktop host. All users have the same webtop content.

This login authority is disabled by default.

### Logging in

The user types a UNIX/Linux username and password.

### Authentication

1. This login authority checks the username and password against the UNIX/Linux user database.
2. If the authentication fails, the next login authority is tried.
3. If the authentication succeeds, the user may log in.

### User identity

The identity is always `.../_user/UNIX-username`.

### Login profile

The profile object `o=Secure Global Desktop System Objects/cn=UNIX User Profile` is always used for the login profile.

This means all UNIX users receive the same webtop content.

### Emulator sessions and password cache entries

Emulator sessions and password cache entries belong to the UNIX user.

### Secure Global Desktop and PAM

Secure Global Desktop supports Pluggable Authentication Modules (PAM). The UNIX user login authority uses PAM for user authentication, account operations and password operations.

When you install Secure Global Desktop, Secure Global Desktop Setup automatically creates PAM configuration entries for Secure Global Desktop by copying the current configuration for the `passwd` program.

- On Solaris Operating System platforms, entries are created in the `/etc/pam.conf` file.
- On Linux platforms, the `/etc/pam.d/tarantella` file is created.

### Related topics

- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)

## The SecurID login authority

### Overview

The SecurID login authority allows users with RSA SecurID tokens to log in to Secure Global Desktop. This login authority authenticates against an RSA ACE/Server®.

RSA SecurID is a product from RSA Security, Inc., that uses two-factor authentication based on something you *know* (a PIN) and something you *have* (a tokencode supplied by a separate "token" such as a PIN pad, standard card or software token). The PIN and tokencode are combined to form a passcode which is used as the password when you log in to Secure Global Desktop.

This login authority does not support [ambiguous users](#) and so ambiguous login requests are denied.

This login authority is disabled by default.

**Note** SecurID authentication is not supported on the Solaris Operating System on x86 platforms.

### Logging in

The user types their RSA SecurID username, for example "indigo" and their passcode.

### Authentication

1. This login authority searches ENS for a [person object](#) with a [Name](#) attribute matching what the user typed. If there's no match, the search is repeated on the [Username](#) attribute, and finally on the [Email Address](#) attribute.
2. If a person object is found, the Username attribute of that object is used as the RSA SecurID username.
3. If no person object is found, the name the user typed is used as the RSA SecurID username.
4. The RSA SecurID username and the passcode typed by the user are checked against the RSA ACE/Server.
5. If the authentication fails, the user can't log in because there are no further login authorities to try.
6. If the authentication succeeds, the user may log in **unless**:
  - there was a matching person object **and**
  - the [May Log In To Secure Global Desktop](#) attribute for that person object is cleared.

## User identity

If a person object was found in ENS, that object is used as the identity.

If no person object was found in ENS, the identity is `.../_service/sco/tta/securid/SecurID-username`.

## Login profile

If a person object was found in ENS, that object is used as the login profile.

If no person object was found in ENS, the profile object `o=Secure Global Desktop System Objects/cn=SecurID User Profile` is used.

## Emulator sessions and password cache entries

Emulator sessions and password cache entries belong to either the Person object or SecurID User Profile object, depending on which is used.

### Related topics

- [Enabling the SecurID login authority](#)
- [Using SecurID for application server authentication](#)
- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)

## Enabling the SecurID login authority

To enable SecurID authentication and give SecurID users access to a Webtop, you need to:

1. Configure the Secure Global Desktop server as an RSA ACE/Agent®.
2. Switch SecurID authentication on in Array Manager.

Your RSA ACE/Server® should be up to date with the patches released by RSA.

**Note** SecurID authentication is not supported on the Solaris Operating System on x86 platforms.

## Configuring the Secure Global Desktop server as an RSA ACE/Agent

The Secure Global Desktop host must be able to contact the RSA SecurID (ACE) server on the network.

Secure Global Desktop works with versions 4 and 5 of the RSA ACE/Server. The references below are to the RSA ACE/Server v 4.1 Administration Manual.

1. On the Secure Global Desktop server, create a file `/etc/sdace.txt` containing the line:

```
VAR_ACE=/opt/ace/data
```

2. Create a directory `/opt/ace/data` and copy the RSA ACE server's `sdconf.rec` file to it. See the "RSA ACE/Agent Software" section of *Appendix C for UNIX* for details.
3. Set the file permissions so that Secure Global Desktop can read and write the configuration files.

```
chmod 444 /etc/sdace.txt
chown -R ttasys:ttaserv /opt/ace
chmod -R 775 /opt/ace
```

4. Add the Secure Global Desktop server `server.domain.com` as a client machine (type: UNIX) to the ACE database. See Chapter 4 *Clients and Activation on Clients* for details.
5. Add user access to client (sdadmin or GUI) e.g. `user1` can access resource `server.domain.com`. Alternatively, set the **Open to All Locally Known Users** option. See Chapter 4 *Clients and Activation on Clients* for details.

## Switching SecurID authentication on in Array Manager

1. In Array Manager, click Secure Global Desktop Login, Properties.
2. Check the SecurID login authority box.

Or type the following from a command line:

```
tarantella config edit --login-securid 1
```

### Related topics

- [The SecurID login authority](#)
- [Using SecurID for application server authentication](#)
- [Login authorities](#)
- [Secure Global Desktop Login properties \(array-wide\)](#)



## Security and Secure Global Desktop

### Read this topic to...

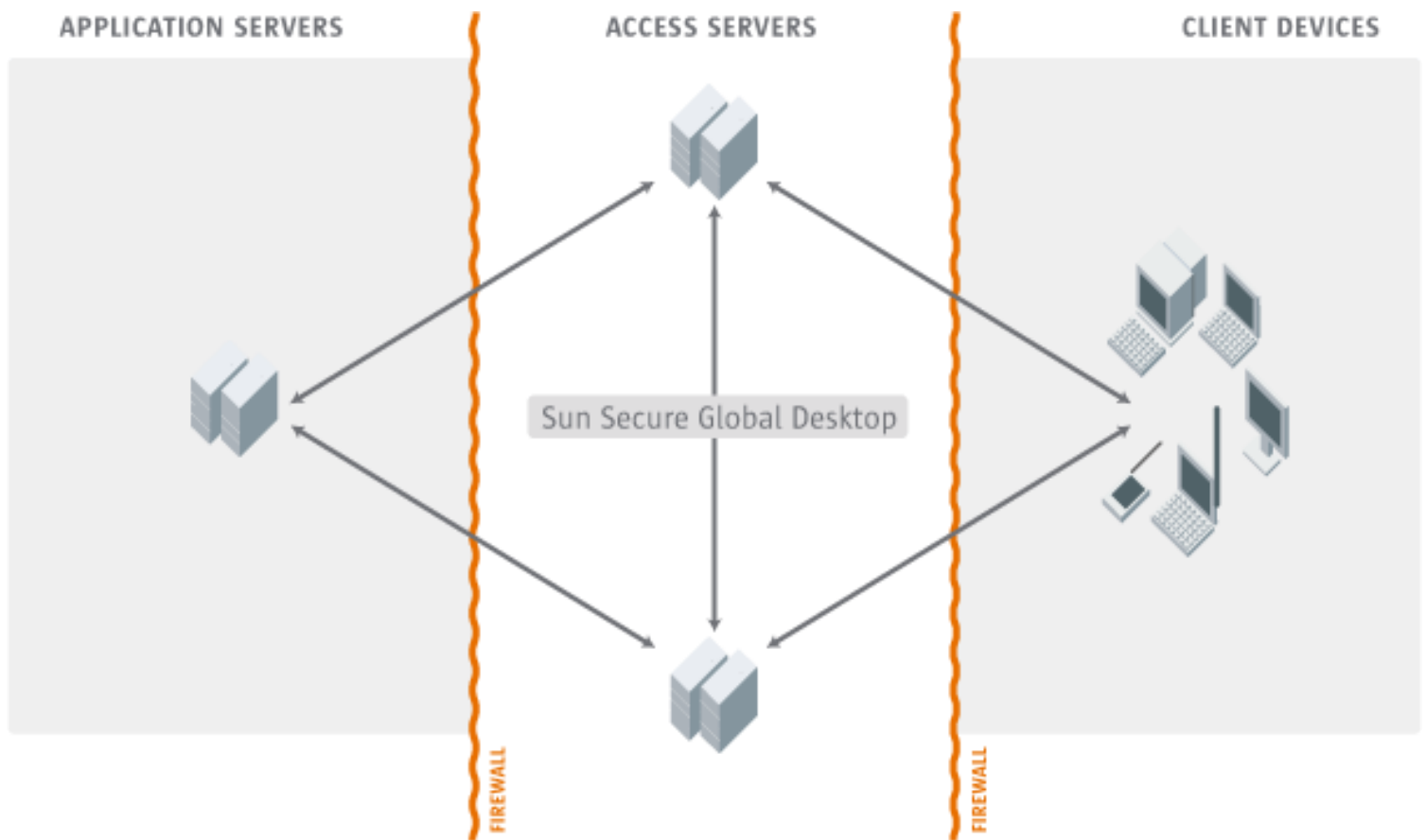
- Understand the security issues when using Secure Global Desktop.

Secure Global Desktop is only one of many components on your network. The information here is related to Secure Global Desktop, and can only help raise security levels as part of an ongoing security strategy.

### Network connections

Secure Global Desktop connects client devices to application servers, acting as a go-between. Also, Secure Global Desktop servers can join together as an array. This means there are three types of connection involved:

Type	Description
Connections between client devices and Secure Global Desktop servers	These may be web server connections (for example, opening the web page that lets you log in to Secure Global Desktop) or Secure Global Desktop-related connections (used by the Secure Global Desktop components running on the client device to connect to the Secure Global Desktop server for example, to send key presses or receive display updates within emulators).
Connections between Secure Global Desktop servers and application servers	These are used to start applications on the application server, and to send and receive data from the application, such as key presses and display updates.
Connections between Secure Global Desktop servers in an array	These are used to update secondary Secure Global Desktop servers with changes made on the primary Secure Global Desktop server.



In a default Secure Global Desktop installation, all standard connections are unencrypted (in the clear). This is as secure as using the telnet program to communicate between two UNIX hosts.

You can raise security levels in these ways:

- Improving security between client devices and Secure Global Desktop servers
- Improving security between Secure Global Desktop servers and application servers
- Using secure connections between the Secure Global Desktop servers in an array
- Configuring Secure Global Desktop to work with a firewall

## Passwords

When a user has a standard connection to Secure Global Desktop, passwords are encoded between the client device and the Secure Global Desktop server to deter casual eavesdroppers. When they have a secure connection, this information is always encrypted.

Secure Global Desktop encrypts all passwords stored in the password cache.

By default, the encryption key used for the password cache never changes. You can force the key to change whenever Secure Global Desktop servers start by checking the Generate New Encryption Key On Restart box on the [Security](#) panel of [Array Manager](#).

## Related topics

- [Improving security between client devices and Secure Global Desktop servers](#)
- [Improving security between Secure Global Desktop servers and application servers](#)
- [What ports does Secure Global Desktop use?](#)
- [Using Secure Global Desktop with firewalls](#)

## What are Secure Global Desktop security services?

Secure Global Desktop security services lets Secure Global Desktop use SSL (the Secure Sockets Layer) to provide secure connections, for example between client devices and Secure Global Desktop servers.

### Related topics

- [Security and Secure Global Desktop](#)
- [Improving security between client devices and Secure Global Desktop servers](#)

## Securing client connections with Secure Global Desktop security services

### Read this topic to...

- Learn the essentials of Secure Global Desktop security services.
- Understand how to enable secure connections.

Secure Global Desktop security services allow you to secure the connections between Secure Global Desktop client and a Secure Global Desktop server. The connections are secured using the Secure Sockets Layer (SSL).

Secure connections have these benefits:

Benefit	Description
No eavesdropping	SSL encrypts all information before transmission.
No tampering	SSL can check that a message has not changed between the client and the Secure Global Desktop server.
No message forgery	SSL requires that the server prove its identity to the client before communications can take place, and also guards against replay attacks.

Internet transactions are open to many forms of attack, for example packet-sniffing, DNS spoofing, and man-in-the-middle attacks. **It is critical to recognize that even when SSL is used, a connection is only secure if SSL is configured correctly.**

Secure Global Desktop security services can only help raise security levels as part of an ongoing security strategy. They can not transform your intranet into a high-security installation by itself.

When Secure Global Desktop is first installed, the initial connection between a Secure Global Desktop client and a Secure Global Desktop server is secured with SSL. However, after the user has logged in, the connection is downgraded to a standard connection. To be able to use SSL permanently for connections to Secure Global Desktop, you must enable Secure Global Desktop security services.

## Enabling Secure Global Desktop security services

To enable Secure Global Desktop security services:

1. [Obtain and install an X.509 certificate](#) for the Secure Global Desktop server to use. An X.509 certificate enables the Secure Global Desktop server to identify itself to a client device. (There are [important security considerations](#) regarding the types of X.509 certificate you can use.)
2. Enable security services for that server, using `tarantella security start`. This enables secure connections for the users you have configured to have them.

Secure connections between the client and Secure Global Desktop server use [port 5307/tcp](#). You may have to configure your firewall to allow network traffic on this port. Alternatively, you may want to use [firewall forwarding](#).

### Security services and secure (HTTPS) web servers

Secure Global Desktop security services only secure the connections between a Secure Global Desktop client and a Secure Global Desktop server. It does not secure any other type of connection, including the connections made to the Secure Global Desktop Web Server. To secure the connections to the Secure Global Desktop Web Server, [follow these steps](#).

If you are using the browser-based webtop or you have developed your own web applications, you may also have to [secure the SOAP connections to a Secure Global Desktop server](#).

### Giving users different types of connection

You can decide which users receive secure (SSL-based) connections, and which users receive standard (unencrypted) connections. To do so, you configure the [Connections](#) attribute for a person object, organizational unit object, or organization object.

You can configure the type of connection based on these factors:

- Who the user is. Perhaps only members of the Accounts department need secure connections.
- The DNS name (or IP address) of the user's client device. Perhaps users only need secure connections when accessing Secure Global Desktop over the Internet.
- The Secure Global Desktop server's DNS name (or IP address). Perhaps users only need secure connections when accessing one particular Secure Global Desktop server.

The initial connection to a Secure Global Desktop server, before users type their username and password, is always secure. This means that usernames and passwords are always sent securely. Once the user is identified, the connection may be downgraded to a standard connection according to

your configuration.

Here are some examples for customizing connection types:

- If you only want the members of one department to have secure connections.
- If your users only need secure connections when accessing Secure Global Desktop over the Internet.
- If your users only need a secure connection to one particular Secure Global Desktop server.

### Related topics

- [Security and Secure Global Desktop](#)
- [Obtaining and installing an X.509 certificate](#)
- [What are X.509 certificates and why do I need one?](#)
- [The tarantella security start command](#)
- [Securing the SOAP connections to a Secure Global Desktop server](#)
- [Connections \(--conntype\)](#)
- [Sharing web server and Secure Global Desktop server certificates](#)
- [What ports does Secure Global Desktop use?](#)
- [Using Secure Global Desktop with firewalls](#)

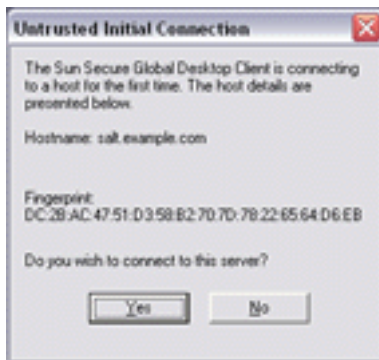
## Users and trusted Secure Global Desktop servers

### Read this topic to...

- Understand the security implications of connecting to a Secure Global Desktop server

When Secure Global Desktop is first installed, the initial connection between a Secure Global Desktop client and a Secure Global Desktop server is secured with SSL. However, after the user has logged in, the connection is downgraded to a standard connection. To be able to use SSL permanently for connections to Secure Global Desktop, you must enable [Secure Global Desktop security services](#).

In addition to using SSL, Secure Global Desktop also requires users to authorize their connections to Secure Global Desktop so that they only connect to trusted servers. The first time a user connects to a Secure Global Desktop server, they see an Untrusted Initial Connection message advising that they are connecting to a server for the first time.

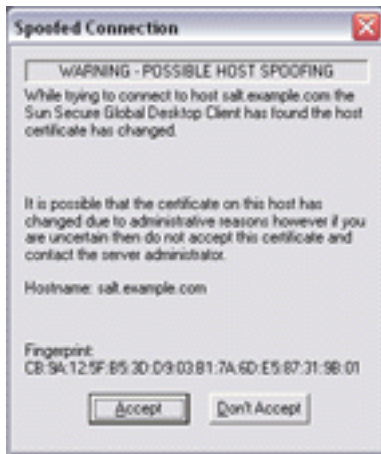


**Note** If there is a problem with the server's security certificate, [a security warning displays](#) before the Untrusted Initial Connection message.

The message displays the hostname and fingerprint of the security certificate for the server they are connecting to. Users should check these details **before** clicking Yes. Once a user has agreed to the connection, the hostname and the fingerprint of the certificate are added to the `hostsvisited` file on the client device. The `hostsvisited` file is stored in the same location as the user's [profile cache](#).

The user is not prompted again about the connection unless there is a problem. If there is a problem, a Spoofed Connection message displays.





To ensure that users only connect to Secure Global Desktop servers that are trusted, Secure Global Desktop Administrators should:

- Provide users with a list of hostnames and fingerprints for the servers that are trusted. Use the `tarantella security fingerprint` command on each member of the array to obtain a list of fingerprints.
- Explain to users the security implications of agreeing to connect to server.

## Classic webtop

If you are using the classic webtop, the Java™ technology client prompts users **every time** it connects to a Secure Global Desktop server. The Native Client **never** prompts users.

### Related topics

- [Securing client connections with Secure Global Desktop security services](#)
- [User prompts and X.509 certificates](#)

## Improving security between client devices and Secure Global Desktop servers

### Read this topic to...

- Learn how to raise security levels between client devices and Secure Global Desktop.

In minimal Secure Global Desktop installations, information is not encrypted when transmitted between a client device and Secure Global Desktop server. Passwords are encoded to deter casual eavesdroppers. These connections are called *standard connections*.

Where higher security is required (for example, if you want to access Secure Global Desktop from outside a firewall) we recommend you use Secure Global Desktop security services to provide *secure connections* (which are based on SSL, the Secure Sockets Layer), in addition to standard connections. Secure connections have these benefits:

Benefit	Description
No eavesdropping	SSL encrypts all information before transmission.
No tampering	SSL can check that a message hasn't changed between the client device and the Secure Global Desktop server.
No message forgery	SSL requires that the server prove its identity to client devices before communication can take place, and also guards against replay attacks.

We also recommend that you use a secure (HTTPS) web server on all Secure Global Desktop hosts. This ensures all web pages that users see are encrypted. **Using a secure web server does not encrypt Secure Global Desktop-related information, such as key presses or display updates.**

For best results, you should use both a secure web server and Secure Global Desktop security services.

### Related topics

- Security and Secure Global Desktop
- Sharing web server and Secure Global Desktop server certificates
- Improving security between Secure Global Desktop servers and application servers

## Improving security between Secure Global Desktop servers and application servers

### Read this topic to...

- Learn how to raise security levels between Secure Global Desktop and your application servers.

The level of security between Secure Global Desktop and your application servers varies depending on the types of application server and the protocols they use.

### UNIX application servers

Normally all communications and passwords are transmitted unencrypted (in the clear) when using protocols such as telnet or rexec, for example. You can download and install SSH (Secure Shell), which provides a more secure alternative. SSH encrypts all communications between hosts and encrypts passwords before they are transmitted. See [Installing and using SSH with Secure Global Desktop](#) for more information.

### Windows application servers

- Using the Microsoft RDP protocol: all communication is encrypted as standard.
- Using the Citrix ICA protocol: all communication uses the telnet protocol and is in the clear.

### Web application servers

The level of security depends on the type of web server you are using to host the web application:

- HTTP web servers: all communications and passwords are transmitted in the clear.
- HTTPS (secure) web servers: all communications and passwords are encrypted before transmission using SSL.

For secure connections to your web application servers we recommend using HTTPS.

## Related topics

- [Security and Secure Global Desktop](#)
- [Improving security between client devices and Secure Global Desktop servers](#)
- [Installing and using SSH with Secure Global Desktop](#)
- [Sharing web server and Secure Global Desktop server certificates](#)

## Giving secure connections across the Internet

### Problem

You want to give secure connections to all users accessing Secure Global Desktop across the Internet.

### Solution

In Array Manager, ensure that processing of Connections settings is enabled, by checking the appropriate box on the [Security](#) panel. Then use Object Manager to configure the organization object so that client devices within a particular DNS domain receive standard connections, and all others receive secure connections.

### Case study

Indigo Insurance exposes a Secure Global Desktop server through a firewall. Users logging in to Secure Global Desktop within the corporate intranet must receive standard connections, but those connecting from the Internet must receive secure connections. All client devices within the intranet are in the domain indigo-insurance.com.

### Solution

1. In Array Manager, display Security properties. For Connection Types, make sure that Apply When Users Log In is checked. Click Apply.
2. In Object Manager, display properties for the organization object.
3. On the Attributes tab, choose [Connections](#) from the list.
4. Click New, and fill in the details for the connection:
  - For Client Device, type `*.indigo-insurance.com`. This matches all client devices within the domain indigo-insurance.com.
  - For Secure Global Desktop server, type `*`. This matches all Secure Global Desktop servers.
  - For Connection, choose Standard.
5. Click New again, using these details:
  - For Client Device, type `*`. This matches all client devices.
  - For Secure Global Desktop server, type `*`. This matches all Secure Global Desktop servers.
  - For Connection, choose Secure.
6. Use the arrow buttons to ensure that the first connection type specification is above the second. The first match is used, so the more-specific pattern should appear before the less-specific

pattern.

7. Click Apply.

## Next steps

- You can override the connection type for everyone in an organizational unit, or for individual users, using the [Connections](#) attribute for OU objects or person objects.
- To define the connection type for some types of user, you configure the Connections attribute for a [profile object](#). For example, the connection type for all UNIX users is configured using the `o=Tarantella System Objects/cn=UNIX User Profile` profile object.

## Related topics

- [Improving security between client devices and Secure Global Desktop servers](#)
- [What ports does Secure Global Desktop use?](#)
- [Using Secure Global Desktop with firewalls](#)
- [Securing client connections with Secure Global Desktop security services](#)
- [Giving secure connections to all users in a department](#)
- [Giving secure connections to a Secure Global Desktop server](#)

## Giving secure connections to a Secure Global Desktop server

### Problem

You want to give all users secure connections to one Secure Global Desktop server in an array.

### Solution

In Array Manager, ensure that processing of Connections settings is enabled, by checking the appropriate box on the [Security](#) panel. Then use Object Manager to configure the organization object so that all client devices will receive a secure connection when connecting to the specified Secure Global Desktop server.

### Case study

Indigo Insurance has an array of Secure Global Desktop servers but only one, `newyork.indigo-insurance.com`, is exposed through the firewall. You want to ensure all users get secure connections when connecting to this server.

### Solution

1. In Array Manager, display Security properties. For Connection Types, make sure that Apply When Users Log In is checked. Click Apply.
2. In Object Manager, display properties for the organization object.
3. On the Attributes tab, choose [Connections](#) from the list.
4. Click New, and fill in the details for the connection:
  - For Client Device, type `*`. This matches all client devices.
  - For Secure Global Desktop server, type the [peer DNS name](#) of the Secure Global Desktop server you want your users to connect to securely, for example `newyork.indigo-insurance.com`.
  - For Connection, choose Secure.
5. Use the arrow buttons to put your new connection type specification first in the list.
6. Click Apply.

### Next steps



- You can override the connection type for everyone in an organizational unit, or for individual users, using the [Connections](#) attribute for OU objects or person objects.
- To define the connection type for some types of user, you configure the Connections attribute for a [profile object](#). For example, the connection type for all UNIX users is configured using the `o=Tarantella System Objects/cn=UNIX User Profile` profile object.

## Related topics

- [Improving security between client devices and Secure Global Desktop servers](#)
- [Securing client connections with Secure Global Desktop security services](#)
- [Giving secure connections to all users in a department](#)
- [Giving secure connections across the Internet](#)

## Giving secure connections to all users in a department

### Problem

You want to give secure connections to the members of one department in your organization.

### Solution

In Array Manager, ensure that processing of Connections settings is enabled, by checking the appropriate box on the [Security](#) panel. Then use Object Manager to configure the organizational unit object to which the users belong, so that all users in that OU receive a secure connection.

### Case study

The Indigo Insurance Finance department requires secure connections for all its users, who may log in to Secure Global Desktop from anywhere.

### Solution

1. In Array Manager, display Security properties. For Connection Types, make sure that Apply When Users Log In is checked. Click Apply.
2. In Object Manager, display properties for the organizational unit object, in this case `o=Indigo Insurance/ou=Finance`.
3. On the Attributes tab, choose [Connections](#) from the list.
4. Click New, and fill in the details for the connection:
  - For Client Device, type `*`. This matches all client devices.
  - For Secure Global Desktop server, type `*`. This matches all Secure Global Desktop servers.
  - For Connection, choose Secure.
5. Use the arrow buttons to put your new connection type specification first in the list. This means that all users without more specific connection types (configured on their own person objects) will match your new connection type specification, and receive a secure connection.
6. Click Apply.

### Next steps

- You can override the connection type for an individual user using the person object's [Connections](#) attribute.

- To define the connection type for some types of user, you configure the Connections attribute for a [profile object](#). For example, the connection type for all UNIX users is configured using the `o=Tarantella System Objects/cn=UNIX User Profile` [profile object](#).

## Related topics

- [Improving security between client devices and Secure Global Desktop servers](#)
- [Securing client connections with Secure Global Desktop security services](#)
- [Giving secure connections across the Internet](#)
- [Giving secure connections to a Secure Global Desktop server](#)

## How do I tell what connection type a user gets?

There are three possible connection types:

Type	Description
Standard connection	Connections between the client device and Secure Global Desktop server are <b>not encrypted</b> .
Secure (SSL) connection	Connections between the client device and Secure Global Desktop server are <b>encrypted</b> . This connection type is only available when Secure Global Desktop security services are enabled.
Denied	The user is denied a connection.

A user's connection type depends on these factors:

- The address of the user's client device.
- The Secure Global Desktop server the user logs in to (the Secure Global Desktop security services may not be enabled, which means that secure connections are not available).
- The username and password the user types to log in (which, in conjunction with the [login authorities](#) available, determines the [login profile](#) associated with the user).
- The Connections setting for the person object and for its ancestors in the organizational hierarchy (as long as [processing of Connections settings](#) is enabled).

### Example

User Mulan Rouge logs in to Secure Global Desktop from her usual client device, fez.indigo-insurance.com. She logs in to a server. Processing of Connections settings is enabled.

Mulan types her usual username and password, which correspond to the person object with TFN name `.../_ens/o=Indigo Insurance/ou=Finance/cn=Mulan Rouge`.

To determine her connection type, Secure Global Desktop checks the person object's [Connections](#) attribute. In this example, assume this has two values:

Client device	Secure Global Desktop server	Connection
---------------	------------------------------	------------

.indigo-insurance.com	Standard
	Secure

**The order of these values is significant:** the first match found determines the connection type. In this case the first entry matches, so Mulan receives a standard connection.

If Mulan instead connects from a client device that's not part of indigo-insurance.com, the first entry doesn't match -- but the second one does. In this case Mulan would receive a secure connection.

If Mulan's Connections attribute had no values, the connection type would be determined by the Connections attribute of the parent in the organizational hierarchy: in this case, the organizational unit Finance.

If necessary, Secure Global Desktop continues to check parent OUs, and finally the top-level organization, until a match is found.

If there's no matching entry for the organization object, the user is given the best available connection.

Any connection may be denied if there is doubt over its validity, for example if a problem with a web browser means the incorrect [TCP port](#) is used for the connection.

### Related topics

- [Login authorities](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)
- [Connections \(--conntype\)](#)
- [Security properties \(array-wide\)](#)

## Tuning the SSL Daemon process

When you start Secure Global Desktop security services (`tarantella security start`), the Secure Global Desktop server starts the SSL Daemon. The SSL Daemon is the Secure Global Desktop component that handles secure connections between clients and the Secure Global Desktop server. The SSL Daemon displays as the `ttassl` process on your system.

By default, the SSL Daemon listens on port 5307 for AIP traffic that has been encrypted with SSL. However, if you are running Secure Global Desktop in [firewall forwarding mode](#), the SSL Daemon listens on port 443 and accepts SSL/AIP *and* HTTPS traffic. In this situation, the Daemon handles the SSL/AIP traffic but forwards the HTTPS traffic on to the web server.

Sometimes when the load on the SSL Daemon is heavy it can fail to handle connections. To avoid this happening, you can tune the SSL Daemon process so that it starts new processes to handle the increased connection load.

You may also want to tune the SSL Daemon process if you have a multi-processor server. By tuning the number of SSL Daemon processes to the number of processors, you may improve the connection performance.

You tune the SSL Daemon process with the `tarantella config edit` command and the following command options:

Option	Description
<code>--tarantella-config-ssldaemon-minprocesses</code>	The number of SSL Daemon processes that start when security services are started. The default is 1.
<code>--tarantella-config-ssldaemon-maxprocesses</code>	The maximum number of SSL Daemon processes that can be started. The default is 1.
<code>--tarantella-config-ssldaemon-maxrestarts</code>	If the SSL Daemon unexpectedly exits, the maximum number of times it tries to restart before failing completely. The default is 10.

```
--tarantella-config-ssldaemon-logfilter
```

A comma separated list of filters used to filter the log output from the SSL Daemon. The default is `ssldaemon/*/*error, multi/daemon/*error:sslmulti%%PID %% .log`.

#### Note:

- This tuning is server-specific you have to tune each server individually.
- You must restart the Secure Global Desktop server (`tarantella restart`) for any changes to take effect.

## How the tuning works

In a default installation, only one SSL Daemon process starts when security services are started and, as the load increases, no further processes are started.

Increasing the `maxprocesses` allows the SSL Daemon to start new processes when it gets overloaded.

Once started, all SSL Daemon processes continue to run, **even if** the load reduces.

If you find you regularly need multiple SSL Daemon processes, it may be worth increasing the `minprocesses`.

If the SSL Daemon fails, either the connections are downgraded to standard connections or the Secure Global Desktop server stops. This is configured on the server's [Security properties panel](#) in Array Manager (the If SSL Daemon Doesn't Start attribute).

## Logging

The filters you use for the log output have the same format as the ones [used for the Secure Global Desktop server](#). The same severity and destination file options can be used.

By default, all errors are logged to the `/opt/tarantella/var/log` directory.

### Related topics

- Securing client connections with Secure Global Desktop security services
- Security properties (server-specific)
- Using Secure Global Desktop with the HTTPS port through a firewall
- Using log filters to troubleshoot problems with the Secure Global Desktop server



## Selecting a cipher suite for secure connections

Sun Secure Global Desktop Software allows you to specify the cipher suite used to secure connections with the the Secure Sockets Layer (SSL). The following cipher suites are supported:

Cipher suite	Client preference	OpenSSL name	JSSE name
RSA_WITH_AES_256_CBC_SHA	1	AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
RSA_WITH_AES_128_CBC_SHA	2	AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
RSA_WITH_3DES_EDE_CBC_SHA	3	DES-CBC3-SHA	SSL_RSA_WITH_3DES_EDE_CBC_SHA
RSA_WITH_RC4_128_SHA	4	RC4-SHA	SSL_RSA_WITH_RC4_128_SHA
RSA_WITH_RC4_128_MD5	5	RC4-MD5	SSL_RSA_WITH_RC4_128_MD5
RSA_WITH_DES_CBC_SHA	6	DES-CBC-SHA	SSL_RSA_WITH_DES_CBC_SHA

## Connections between clients and Secure Global Desktop servers

To specify the cipher suites used for connections between clients and Secure Global Desktop servers, run the following command:

```
tarantella config edit --tarantella-config-security-ciphers cipher_list
```

- You must stop the Secure Global Desktop server before running this command.
- The *cipher\_list* is a colon separated list of cipher suites. You must use the **OpenSSL name** from the table above.
- The order of the cipher suites does not matter, as it is the client that determines which suite will be used, based on the client preference order shown in the table above.
- The default setting is `AES256-SHA:RC4-MD5`.
- The default setting means that the Sun Secure Global Desktop Client and the Native Client will use AES (Advanced Encryption Standard) with a 256-bit key. The Java™ technology client will use RC4 with a 128-bit key. You must include the `RC4-MD5` cipher suite if you are using the Java technology client,

because it does not support AES.

## Connections between Secure Global Desktop servers

To specify the cipher suites used for [secure intra-array communication](#), run the following command:

```
tarantella config edit --tarantella-config-security-peerssl-ciphers cipher_list
```

- You must stop all Secure Global Desktop servers in the array before running this command.
- The *cipher\_list* is a colon separated list of cipher suites. You must use the **JSSE (Java Secure Socket Extension) name** from the table above.
- Although you can specify a list, this is an array-wide setting and so the first cipher in the list will always be used.
- The default setting is `AES256-SHA`.
- The cipher suite is only used if you have enabled secure connections between Secure Global Desktop servers.

## About cipher suites

A cipher suite is a set of cryptographic algorithms used to:

- protect information required to create shared keys (key exchange)
- encrypt messages exchanged between clients and servers (bulk encryption) and
- generate message hashes and signatures to ensure the integrity of a message (message authentication).

A cipher suite specifies one algorithm for each of these tasks. For example, the `RSA_WITH_RC4_128_MD5` cipher suite uses RSA for key exchange, RC4 with a 128-bit key for bulk encryption, and MD5 for message authentication.

### Related topics

- [Securing connections between Secure Global Desktop servers](#)
- [Securing client connections with Secure Global Desktop security services](#)

## Securing connections between Secure Global Desktop servers

In a standard installation, the data transmitted between Secure Global Desktop servers in an array (including data sent from the Secure Global Desktop administration tools) is not encrypted. Secure Global Desktop Administrators can secure the connections between array members with SSL/TLS. Using SSL/TLS for these connections ensures that communication only takes place between servers that have authenticated to each other and ensures the integrity of the data.

### How secure intra-array communication works

Using SSL/TLS to secure intra-array communication means that each member of the array has to have a valid server peer certificate that has been signed by a trusted certificate authority (CA).

As the server peer certificates are only used internally by Secure Global Desktop, the primary server in the array acts as the CA. The primary has a self-signed CA certificate and a private key. All servers in the array have a copy of the primary's CA certificate in a trusted certificate store (the truststore).

All servers in the array (including the primary) have a server peer certificate and a private key. The server peer certificate is signed with the primary's CA certificate and contains a common name (CN) which is the peer DNS name of the Secure Global Desktop server.

When one member of the array connects to another (or an administration tool connects to an array member), the Secure Global Desktop server being connected to presents its server peer certificate as part of the SSL negotiation. The connecting server evaluates the certificate and checks:

- the CN of the certificate matches the peer DNS name of the connecting server
- the expiry date of the certificate and
- the issuer of the certificate, which must be the CA certificate of the primary.

If the certificate is valid, the SSL/TLS connection is established.

### Managing CA and server peer certificates

When you enable secure intra-array communication, Secure Global Desktop automatically generates and distributes the CA and server peer certificates to the members of the array. Whenever there is a change in the array structure, Secure Global Desktop automatically updates the CA and server peer certificates as needed:

- **server joins the array** - the primary CA certificate is installed on the new server and the new server obtains a new server peer certificate signed with the primary CA certificate.
- **server leaves the array** - the detached server becomes the primary server in an array containing one server. The detached server creates a new CA certificate and a new server peer certificate for itself.
- **new primary server** - the primary generates a new CA certificate and installs it on all array members. All secondary servers obtain a new server peer certificate signed with the new primary CA certificate.

Administrators can use the `tarantella security peerca --show` command to view certificates in the truststore. The truststore contains the primary CA certificate.

## Enabling secure intra-array communication

1. Make sure there are no webtop and emulator sessions running in the array, including suspended sessions.
2. Dismantle the array.
  - On the **primary server**, use the `tarantella array detach --secondary server` command (or use Array Manager) to detach the secondary servers.
  - Only detach one server at a time.
  - Wait for the array change to be copied to all members of the array before detaching any more servers. You can tell that this has happened when the `tarantella status` command returns the same result when you run it on each array member.
3. Use the `tarantella stop` command to stop all servers.
4. Enable secure intra-array communication by running the following command on **each server**:

```
tarantella config edit --tarantella-config-security-peerssl-enabled 1
```

5. Use the `tarantella start` command to start all servers.
6. Rebuild the array.
  - Only add one server at a time.
  - On the **server joining the array**, use the `tarantella array join --primary primary_server` command to add the server.
  - You will be prompted to trust the primary server's CA certificate and the fingerprint of the certificate displays.
  - On the **primary server**, use the `tarantella security peerca --show` command to display the fingerprint for the primary server's CA certificate.
  - Check that the certificate fingerprints match. This is important as it verifies that the secondary is communicating with the genuine primary server.
  - If the fingerprints match, complete the array join by accepting the primary server's CA

certificate.

- Wait for the array change to be copied to all members of the array before adding any more servers. You can tell that this has happened when the `tarantella status` command returns the same result when you run it on each array member.

### Related topics

- [Security and Secure Global Desktop](#)
- [Securing client connections with Secure Global Desktop security services](#)
- [The tarantella security peerca command](#)
- [What are peer DNS names and external DNS names?](#)

## Securing the SOAP connections to a Secure Global Desktop server

Client applications, such as the browser-based webtop, use the SOAP protocol (over HTTP) to access the web services provided by a Secure Global Desktop server. You should use HTTPS to secure these SOAP connections if you:

- Use Secure Global Desktop with the HTTPS port through a firewall (firewall forwarding).
- Relocate the browser-based webtop to a different JavaServer Pages (JSP) container on a different host.
- Develop your own applications, using the Secure Global Desktop `com.tarantella.tta.webservices.client.views` package, either on the same host as Secure Global Desktop or on a different host.

**Note** If you develop your own client, for example because you want to use a different programming language, you need to develop your own methods for securing the SOAP connections. This page gives the general principles you need to implement.

## Configuring the client to use HTTPS and trust Secure Global Desktop server certificates

To secure the SOAP connections, the client must be configured to use HTTPS and to trust the X.509 certificates for any Secure Global Desktop servers it connects to. Follow these steps:

1. Add the X.509 certificates to the certificate store.

You install server certificates with the `keytool` application, see the [Java 2 SDK Tools and Utilities documentation](#) for details.

You store the certificates in the certificate store for the Java™ 2 Runtime Environment (JRE) used by the Secure Global Desktop server, `/opt/tarantella/bin/jre/lib/security/cacerts`.

You must add the X.509 certificate for each each member of the array. The certificate for each server is stored in `/opt/tarantella/var/tsp/cert.pem`.

Run the following command:

```
/opt/tarantella/bin/jre/bin/keytool -import \
```

```
-file /opt/tarantella/var/tsp/cert.pem \  
-keystore /opt/tarantella/bin/jre/lib/security/cacerts \  
-storepass changeit \  
-alias hostname
```

2. Change to the `webapps/sgd/WEB-INF/classes/com/tarantella/tta/webservices/client/apis` directory.
3. Edit the `Resources.properties` file.
4. For **each** of the web services listed in the properties file, change the URL to an HTTPS URL.
  - o The URLs have the format `http://server:port/service` (the default is `http://localhost:80/service`).
  - o Use `localhost` for the `server` if the webtop/application is on the same host as Secure Global Desktop. Otherwise, use the fully qualified DNS name of a Secure Global Desktop server.
  - o The `port` is the port that the Secure Global Desktop Web Server listens on.
  - o You can only specify one URL for each web service, for example, `https://boston.indigo-insurance.com:443/axis/services/rpc/print`.
5. Save the changes to the `Resources.properties` file.
6. Restart the web server and JSP container.
  - o If you are using the Secure Global Desktop Web Server, use `tarantella webserver restart --ssl`.
  - o If you are using your own JSP container and/or web server, you must restart your JSP container after making any changes to the `Resources.properties` file. You must also make sure the web server is configured to accept HTTPS connections and restart it.
7. Repeat these steps on each member of the array.

## Remote hosts

If you have relocated the browser-based webtop to another host, or if you have developed your own applications *on another host* using the `com.tarantella.tta.webservices.client.views` package, you must edit **both** the relocated `Resources.properties` file and the one on the Secure Global Desktop server.

## Web services URLs

In the **relocated** `Resources.properties` file, the URLs must be for the Secure Global Desktop server the client application will connect to, for example `https://boston.indigo-insurance.com:443/axis/services/rpc/print`.

In the `Resources.properties` file on the Secure Global Desktop host, amend the URLs to `https://localhost:443`.

## Keystores

You have to create **two keystores**:

- one for the HTTPS connections from the client application (webtop) to the Secure Global Desktop server
- one for the HTTPS connections from the Secure Global Desktop server to the remote host (this is used to send events from the server)

For the HTTPS connections to the Secure Global Desktop server, you must create your own keystore on the **remote host**, using your own JDK. This keystore must contain the Secure Global Desktop server certificate. Add the details of this keystore to the **relocated** `Resources.properties` file, by editing the following lines:

```
keystore=keystore
keystorepass=password
```

For the HTTPS connections from the Secure Global Desktop server to the remote host, you must install the root certificate for the remote host into the keystore (the `cacerts` file) for the JRE used by the Secure Global Desktop server. You do this using the `keytool` application:

```
/opt/tarantella/bin/jre/bin/keytool -import \  
-keystore /opt/tarantella/bin/jre/lib/security/cacerts \  
-storepass changeit \  
-file certificate_path \  
-alias remote_hostname
```

### Related topics

- [Relocating the browser-based webtop to your own JSP container](#)
- [Using Secure Global Desktop with the HTTPS port through a firewall](#)
- [Securing client connections with Secure Global Desktop security services](#)



## Securing connections to Active Directory and LDAP directory servers

You can use Secure Global Desktop security services to secure the connections to an LDAP directory server, including Microsoft Active Directory. LDAP connections are used with the following authentication mechanisms:

- [Active Directory login authority](#).
- [LDAP login authority](#).
- [Web server/third party authentication](#), only if the LDAP user identity mapping search methods are used.

To secure these connections:

1. [Enable Secure Global Desktop security services](#).
2. In Array Manager, configure secure connections to LDAP or Active Directory.
3. Import the root certificates for your directory servers.
4. For Microsoft Active Directory, create and install client certificates for each Secure Global Desktop server in the array.
5. For the Active Directory login authority, enable LDAP signing requirements for the domain.
6. Restart each Secure Global Desktop server in the array, using `tarantella restart`.

The configuration required for steps 2 to 5 is described below.

### Configuring secure connections to LDAP and Active Directory in Array Manager

The configuration needed depends on the authentication mechanisms that have been enabled in Array Manager

#### Active Directory login authority

1. In Array Manager, select Secure Global Desktop Login properties
2. In the URL field, type the name of an Active Directory domain, for example `ad://east.indigo-insurance.com`.  
Only enter one URL. The URL **must** start with `ad://`.
3. Check the Use Certificates box.
4. Click Apply.

## LDAP login authority and web server/third party authentication

1. In Array Manager, select Secure Global Desktop Login properties
2. In the URL field, type the URL of one or more LDAP directory servers, for example `ldaps://melbourne.indigo-insurance.com`.
  - The URLs **must** start with `ldaps://`.
  - Separate each URL with a semicolon.
  - If you enter more than one URL, the URLs are used in the order they are listed. If the first LDAP directory server listed is unavailable, Secure Global Desktop tries the next one in the list.
  - The standard port used for secure connections to an LDAP directory server is 636/tcp. If an LDAP directory server uses a different port, you must specify the port number as part of the URL, for example `ldaps://melbourne.indigo-insurance.com:5678`.
  - Normally, the LDAP login authority searches the entire LDAP directory. You can restrict the search to part of the LDAP directory by adding a search root to the end of the URL, for example `ldaps://melbourne.indigo-insurance.com/dc=indigo-insurance,dc=com`
3. Click Apply.

## Importing root certificates

To be able to use secure connections, Secure Global Desktop must be able to validate the certificate presented by an LDAP directory server or Active Directory. To do this you must import the root certificate (the Certificate Authority's certificate) into the keystore (the `cacerts` file) for the Java™ 2 Runtime Environment (JRE) used by the Secure Global Desktop server.

Run the following command:

```
/opt/tarantella/bin/jre/bin/keytool -import \  
-keystore /opt/tarantella/bin/jre/lib/security/cacerts \  
-storepass changeit \  
-file root_certificate_path \  
-alias alias
```

Notes:

- See the [Java 2 SDK Tools and Utilities documentation](#) for details on how to use the `keytool` application.
- Use the `-alias` option to uniquely identify the certificate.
- Import the root certificate for **every** Active Directory or LDAP directory server you are using with

Secure Global Desktop.

- Import the root certificates into the `cacerts` file on **every** member of the array.

## Creating client certificates for use with Microsoft Active Directory

Microsoft Active Directory will only accept secure connections from servers that have a valid client certificate that has been signed using the Certificate Services on a Windows 2000/2003 Server. You must create and install a client certificate **for each member of the array**.

You create and install server client certificates with the `keytool` application, see the [Java 2 SDK Tools and Utilities documentation](#) for details.

Server client certificates are stored in the Secure Global Desktop certificate store `/opt/tarantella/var/info/certs/sslkeystore`.

You must provide a password when adding or removing certificates from the certificate store. The password for the `sslkeystore` is unique to each Secure Global Desktop server and can be found in the `/opt/tarantella/var/info/key` file. Use this password for both the `-storepass` and `-keypass` options.

To create and install client certificates:

1. Generate the key pair for the client certificate.
2. Generate a Certificate Signing Request for the client certificate.
3. Create the client certificate.
4. Install the client certificate.

### Generating the key pair for the client certificate

Run the following command to generate the key pair for the client certificate:

```
/opt/tarantella/bin/jre/bin/keytool -genkey \  
-keyalg rsa \  
-keystore /opt/tarantella/var/info/certs/sslkeystore \  
-storepass password \  
-alias alias \  
-keypass password
```

### Generating the Certificate Signing Request for the client certificate

Run the following command to generate the Certificate Signing Request (CSR) for the client certificate:

```
/opt/tarantella/bin/jre/bin/keytool -certreq \  
-keystore /opt/tarantella/var/info/certs/sslkeystore \  
-storepass server_password \  
-alias alias \  
-keypass server_password \  
-file path_to_CSR
```

The alias must be the same as the alias used when generating the key pair. Aliases are case-insensitive.

## Creating the client certificate

1. Using Internet Explorer, go to [http://Windows\\_server/certsrv](http://Windows_server/certsrv).
2. Log in.
3. On the Microsoft Certificate Services page, click Request a certificate.
4. On the Request a Certificate page, click advanced certificate request.
5. On the Advanced Certificate Request page, click Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
6. On the Submit a Certificate Request or Renewal Request page, paste the contents of the CSR into the Saved Request text box or browse to the CSR file.
7. Select an appropriate template from the Certificate Templates list.
8. Click Submit.
9. On the Certificate Issued page, ensure DER is selected and click Download certificate chain.
10. Save the certificate file.

## Installing the client certificate

Run the following command to install the client certificate for a Secure Global Desktop server:

```
/opt/tarantella/bin/jre/bin/keytool -import \  
-file certificate_path \  
-keystore /opt/tarantella/var/info/certs/sslkeystore \  
-storepass server_password \  
-alias alias \  
-keypass server_password
```

## Enabling LDAP signing for the domain

For the Active Directory login authority, you must enable LDAP signing on your domain controllers. For

example:

1. Log in to the domain controller as a user with administrative privileges.
2. In Group Policy Object Editor, select Domain Security Policy Local Policies Security options.
3. Edit the **Domain controller: LDAP server signing requirements** policy, select Require signing.
4. Edit the **Network security: LDAP client signing requirements** policy, select Require signing.

### Related topics

- [The LDAP login authority](#)
- [Enabling the LDAP login authority](#)
- [Web server/third party authentication](#)
- [Securing client connections with Secure Global Desktop security services](#)

## Installing and using SSH with Secure Global Desktop

SSH (Secure SHell) is a package that lets you securely execute commands on network hosts. It offers a more secure alternative to the standard UNIX commands for this purpose.

SSH provides the following benefits over the standard UNIX commands:

- All communication between hosts using SSH is encrypted, including the X protocol if you're running X applications.
- Usernames and passwords are always encrypted before being transmitted over the network.

Secure Global Desktop can use SSH to provide secure communications [between Secure Global Desktop servers and application servers](#).

Secure Global Desktop works with SSH version 2.x or later.

Secure Global Desktop automatically detects that SSH is installed if SSH is installed in one of the following directories:

- `/usr/local/bin`
- `/usr/bin`
- `/usr/sbin`
- `/usr/lbin`
- `/bin`
- `/sbin`

## Installing SSH

If SSH isn't already installed, download and install it in one of the directories listed above:

1. Download SSH from the [OpenSSH Home Page](#). Secure Global Desktop works with SSH version 2.x or later.
2. Install SSH on every UNIX application server you want to provide secure access to, and on every Secure Global Desktop host.

**Note** Because of SSH version compatibility problems, we recommend that you use the same major version of SSH (either version 2 or version 3) on all Secure Global Desktop hosts and

application servers for them to communicate securely.

3. Restart your Secure Global Desktop servers using `tarantella restart`.

## Running SSH from a non-standard location

If SSH is not installed in one of the locations listed above or you want to use an SSH command-line argument, you have to set an environment variable to handle this:

1. Stop the Secure Global Desktop server:

```
tarantella stop
```

2. Set the environment variable `TTASSHCLIENT` to the full pathname of the SSH program and any required command-line arguments, for example:

```
TTASSHCLIENT="/usr/local/bin/ssh -q -X"; export TTASSHCLIENT
```

**Note** If you just want to set command-line arguments, you have to include the pathname to the SSH program, even if the SSH program is in a location where Secure Global Desktop can detect it.

3. Edit the file `/etc/services` and add the following line:

```
ssh 22/tcp
```

**Note** This assumes you've configured the SSH daemon on the application server to use the default port (22/tcp).

4. Restart the Secure Global Desktop server:

```
tarantella start
```

## Enabling X11 forwarding

To support X applications through OpenSSH, enable X11 forwarding in the OpenSSH configuration file. On each Secure Global Desktop host:

1. Edit the `sshd_config` file and include the following:

```
X11Forwarding yes
```

2. Edit the `ssh_config` file and include the following:

```
ForwardAgent yes
ForwardX11 yes
```

3. Restart the SSH daemon.

## SSH and the X Security extension

Secure Global Desktop supports the X Security extension. The X Security extension only works with versions of SSH that support `-Y` option. For OpenSSH, this is version 3.8 or later.

You enable support for X Security for an application using the [Enable X Security Extension](#) attribute.

## Using SSH and X authorization

If SSH connections fail when X authorization is enabled, you may have to run the SSH daemon in ipv4-only mode because Secure Global Desktop may not support the xsecurity extension used on your server. You enable ipv4-only mode by editing your system SSH configuration file. For example:

- On SUSE Linux, edit the `/etc/sysconfig/ssh` file and add a `SSHD_OPTS="-4"` line.
- On Red Hat Enterprise Linux, edit the `/etc/sysconfig/sshd` file and add a `OPTIONS="-4"` line.

**Note** If the SSH configuration file does not exist on your system, you can create it.

You must restart the SSH daemon after making this change.

## Advanced SSH usage

Certain SSH functionality, such as client keys, requires that the SSH client process runs as a specific user. In previous releases of Secure Global Desktop, the server process ran as the UNIX root user and had unlimited access to the server. However, from version 4.0 the Secure Global Desktop server processes and the SSH client process run as a non-privileged user. This is for security reasons. To restore the previous behavior, you must make the Secure Global Desktop `ttasshhelper` application a `setuid` root process:

1. Log in as root on the Secure Global Desktop host.
2. Run the following commands:



```
chmod 4510 /opt/tarantella/bin/bin/ttasshhelper
chown root /opt/tarantella/bin/bin/ttasshhelper
```

If you make these changes, you must take particular care to protect your Secure Global Desktop servers from unauthorized access.

## Configuring applications to use SSH

Configure your applications to use the SSH protocol. Using Object Manager, set the [Connection Method](#) attribute to SSH for each character or X application object that requires a secure connection.

### Related topics

- [Improving security between Secure Global Desktop servers and application servers](#)
- [Connection Method \(--method\)](#)
- [Enable X Security Extension \(--securityextension\)](#)

## Using Secure Global Desktop with proxy servers

To use a proxy server with Secure Global Desktop, clients need to be configured with the address and port number of the proxy servers that should be used when connecting to Secure Global Desktop. You may also need to configure Secure Global Desktop to give clients information about traversing server-side proxy servers.

This topic covers:

- [Supported proxy servers](#)
- [Client proxy settings for the browser-based webtop](#)
- [Client proxy settings for the classic webtop](#)
- [Using proxy server automatic configuration scripts](#)
- [Proxy server exception lists](#)
- [Multiple client proxy server configurations and connections to Secure Global Desktop](#)
- [Proxy server timeouts](#)
- [Server-side proxy server configuration](#)

### Supported proxy servers

To use Secure Global Desktop with a proxy server, the proxy server must support [tunneling](#).

For the **browser-based webtop**, you can use HTTP, Secure (SSL) or SOCKS version 5 proxy servers.

For the **classic webtop**, the Java™ technology clients can use HTTP, Secure (SSL) or SOCKS version 5 proxy servers. For the Native Clients, you can only use HTTP and SOCKS version 5 proxy servers.

For SOCKS version 5 proxy servers, Secure Global Desktop supports the Basic and No authentication required authentication methods. No server-side configuration is required.

### Client proxy settings for the browser-based webtop

For the browser-based webtop, there are two connections to consider:

- Connections between the web browser and the Secure Global Desktop Web Server.
- Connections between the Sun Secure Global Desktop Client and Secure Global Desktop.

Connections between the web browser and the Secure Global Desktop Web Server for example to display a webtop, always use the proxy server settings configured for the web browser.

For the Secure Global Desktop Client connections, the [settings in the profile](#) whether the Secure Global Desktop Client determines the proxy server settings from a web browser or from the profile itself. The Secure Global Desktop Client always stores the last proxy settings it used [in the profile cache](#).

If the profile has **Use default web browser settings** enabled, this means that the proxy server settings are determined from the user's web browser. If the Secure Global Desktop Client is Integrated mode, it either uses the last used proxy settings from the profile cache (if available) or starts the user's default web browser to obtain the proxy settings. In Integrated mode, if **Establish proxy settings on session start** is enabled in the profile and the Secure Global Desktop Client starts the user's default web browser every time.

To be able to determine the proxy server settings from a web browser, the web browser must have Java technology enabled. If Java technology is not available or it is disabled in the web browser, the proxy settings must be manually specified in the profile.

**Note** If proxy server settings are defined in the Java Control Panel for the Sun Java Plug-in, these settings are used instead of the web browser settings.

If the profile has **Manual proxy settings** enabled, this allows you to configure the proxy server settings in the profile itself. You can specify either an HTTP or a SOCKS proxy server or both.

## Client proxy settings for the classic webtop

For the classic webtop, the client proxy server settings are configured as follows:

- Java technology clients, the proxy server settings come from the web browser, using the Sun Java Plug-in.
- the Native Client for Microsoft Windows, the proxy server settings have to be manually configured in the client. Click Options in the Webtop menu.
- the Native Client on UNIX, Linux or Mac OS X client devices, the proxy server settings are configured in the [user preferences file](#). This file can be automatically configured using a shell script.

## Sun Java Plug -in version 1.5.0

If you are using the Sun Java Plug-in version 1.5.0 with the classic webtop, the Plug-in does not make the browser's proxy server settings available to the client. Currently the only solution is to use an earlier version of the Plug-in.

## Customized themes for the Java technology client

If you have created a customized webtop theme, it may contain HTML files which are used as "entry points" to Secure Global Desktop. An HTML file counts as an entry point if it is the first HTML page to be loaded which contains Secure Global Desktop applets. In order for Secure Global Desktop to detect and use the proxy server configured in the browser, each applet in an entry-point HTML file must include the [ProxyServer](#) and [ProxyFrame](#) proxy parameters.

## Using the proxy server diagnostic application for the Java technology client

The Java technology client has a diagnostic application, `proxyinfo`, which can be used to investigate any problems Secure Global Desktop encounters when it acquires proxy information.

To access the application, users must type the following URL in their web client:

```
http://server.com/tarantella/cgi-bin/ttawebtop.cgi/tarantella/resources/info/sco/tta/proxyinfo.html
```

You must always run this application through the `ttawebtop.cgi` program.

When you run the application, the Proxy server information page displays and processes the proxy server configuration. The results are output on screen.

The information displayed shows what the application has detected about the user's web client settings and what tests the application has carried out.

The key piece of information shown is the name and port numbers of the candidate proxy servers. These are the proxy servers that Secure Global Desktop can connect to.

You can configure the level of detail shown by the application by adding a parameter to the applet, as follows:

1. Open the `/opt/tarantella/var/docroot/resources/info/sco/tta/proxyinfo.html` file in an editor.
2. Look for the `TTAAPPLET` tag.
3. Insert the following parameter tag between the opening and closing `TTAAPPLET` tags:

```
<param name="LOG_MASK" value="bit mask">
```

The bit mask values for this parameter are:

Value	Setting	Details shown
1	General	The web client settings the <code>proxyinfo</code> application detected
2	Details	The tests the <code>proxyinfo</code> application has carried out
4	Overrides	The domains which have been manually excluded
8	Registry	Windows registry details

The default value is 7, which shows General, Details and Overrides, but not Registry.

4. Close the file and save the changes.

## Using proxy server automatic configuration scripts

Whenever client proxy server configuration is determined from a web browser, you can use an automatic configuration script to automatically configure the proxy settings.

You specify the URL of the configuration script in the connection settings for the web browser. The automatic configuration script must be written in JavaScript and have either a `.pac` file extension or **no file extension**. See the [Netscape Proxy Auto-Config File Format](#) page for details.

**Note** Use this format for all web browsers supported by Secure Global Desktop.

## Proxy server exception lists

You can use proxy server exception lists to control which connections should not be proxied. Exception lists can be configured as follows:

- Secure Global Desktop Client - proxy exception lists can only be used if the proxy settings are determined from a web browser. The exception list is configured in the web browser or Sun Java Plug-in.
- Native Client on UNIX, Linux or Mac OS X client devices - proxy exception lists are configured in the [user preferences file](#).
- Java technology client - the exception list is configured in the web browser or in the Java Control Panel for the Sun Java Plug-in.

An exception list is a semicolon-separated list of DNS host names:

```
chicago.indigo-insurance.com;detroit.indigo-insurance.com;london.indigo-insurance.com
```

**Note** On Mozilla-based browsers, the list is a comma-separated list.

Exception lists may include the wildcard:

```
*.indigo-insurance.com
```

There is no translation between DNS hostnames and IP addresses in exception lists. For example, with an exception list of ".indigo-insurance.com", connections to "chicago.indigo-insurance.com" and "detroit.indigo-insurance.com" would not use the proxy server, but connections to "192.168.5.20" and "192.168.5.30" (their IP addresses) would.

For the browser-based webtop, users must include the following entries in their exception lists:

```
localhost; 127.0.0.1
```

## Multiple client proxy server configurations and connections to Secure Global Desktop

If only **one** proxy server has been configured on the client, Secure Global Desktop uses this proxy server for all HTTP, HTTPS and Secure Global Desktop connections.

**Note** If this is a Secure (SSL) proxy server, the Secure Global Desktop traffic is only encrypted if the user has a [secure connection to the Secure Global Desktop server](#).

If an HTTP **and** a SOCKS proxy server have been configured on the client, and you are using Secure Global Desktop in firewall forwarding mode, Secure Global Desktop uses the HTTP proxy server for all HTTP, HTTPS and Secure Global Desktop connections.

If an HTTP **and** a SOCKS proxy server have been configured on the client, and you are **not** using Secure Global Desktop in firewall forwarding mode, the proxy server Secure Global Desktop uses depends on the client. If the client is:

- the Secure Global Desktop Client, Secure Global Desktop uses:
  - the HTTP proxy server for the HTTP and HTTPS connections and
  - the SOCKS proxy server for all Secure Global Desktop connections.
- the Java technology client, Secure Global Desktop uses:
  - the HTTP proxy server for the HTTP and HTTPS connections and
  - the HTTP proxy server for all Secure Global Desktop connections but the connections go via the SOCKS proxy server first.
- the Native Client, Secure Global Desktop uses:

- the HTTP proxy server for the HTTP and HTTPS connections and
- the SOCKS proxy server for all Secure Global Desktop connections.

## Proxy server timeouts

Proxy servers will drop a connection after a short period of time if there is no activity on the connection. By default, Secure Global Desktop sends keepalive packets every 100 seconds to keep the connection open.

If you find that applications disappear after a short while, you may have to [increase the frequency at which keepalive packets are sent](#).

## Server-side proxy server configuration

When a Secure Global Desktop client connects to the Secure Global Desktop Web Server, Secure Global Desktop can be configured to "instruct" the client to connect using a different DNS name and an array route. An array route is the address of a server-side SOCKS proxy server. The DNS name and array route are determined using the IP address of the client.

### Configuring multiple DNS names

If a Secure Global Desktop server is known by different names on the network, for example inside and outside a firewall, you can configure Secure Global Desktop to connect.

You configure multiple DNS names for a Secure Global Desktop server on the [General Properties](#) panel in Array Manager or with the following command:

```
tarantella config edit --server-dns-external dns_name ...
```

Each *dns\_name* has the format *client IP pattern:external DNS name*, where *IP\_pattern* is a regular expression matching a client IP address, for example `192.168.10.*`.

In Array Manager, press the RETURN key after each name definition. On the command line, use a space to separate the names, for example:

```
tarantella config edit --server-dns-external "192.168.10.*:boston.indigo-insurance.com" "*:www.indigo-insurance.com"
```

The order of the names is important. The **first** matching IP pattern is used. For example if the following names are defined:

```
192.168.10.*:boston.indigo-insurance.com
*:www.indigo-insurance.com
```

Clients with IP addresses beginning 192.168.10 connect to boston.indigo-insurance.com, and all other clients connect to www.indigo-insurance.com. If the order of the names was reversed, all clients would connect to www.indigo-insurance.com.

**Note** You must restart the Secure Global Desktop server for multiple DNS names to take effect.

## Configuring array routes

You configure the routes for an array with the following command:

```
tarantella config edit --tarantella-config-array-netservice-proxy-routes
route ...
```

Each *route* has the format *IP\_pattern:type:host:port*, where:

- *IP\_pattern* is a regular expression matching a client IP address, for example 192.168.10.\*.
- *type* is a connection type. Use `CTSOCKS` for a SOCKS version 5 connection.
- *host* is the DNS name or IP address of the proxy server to connect to.
- *port* is the port to connect to on the *host*.

Enclose each route in quotes and separate the routes with a space.

The order of the routes is important. The **first** matching client IP pattern is used.

The *route* can also be appended with `:ssl` which means that the client should use SSL on that connection before continuing with the SOCKS connection.

For example:

```
"192.168.10.*:CTSOCKS:taurus.indigo-insurance.com:8080" "*:CTSOCKS:draco.
indigo-insurance.com:8080:ssl"
```

Clients with IP addresses beginning 192.168.10 connect via the SOCKS proxy server taurus.indigo-insurance.com on port 8080. All other clients connect via the SOCKS proxy server draco.indigo-insurance.com on port 8080. These clients also connect using SSL before continuing with the SOCKS connection.

**Note** You must restart every server in the array for array routes to take effect.



## Related topics

- [Applications disappear after about two minutes](#)

## Using Secure Global Desktop with firewalls

### Problem

You have a number of firewalls protecting various parts of your network and you want to use Secure Global Desktop.

### Solution

Configure your firewalls to allow packets to be sent between client devices used for Secure Global Desktop and your Secure Global Desktop servers, and between your Secure Global Desktop servers and your application servers. Ensure that the DNS names of web servers and Secure Global Desktop servers are configured correctly for the clients you want to use to log in to Secure Global Desktop.

Using Secure Global Desktop security allows you to [securely traverse firewalls](#).

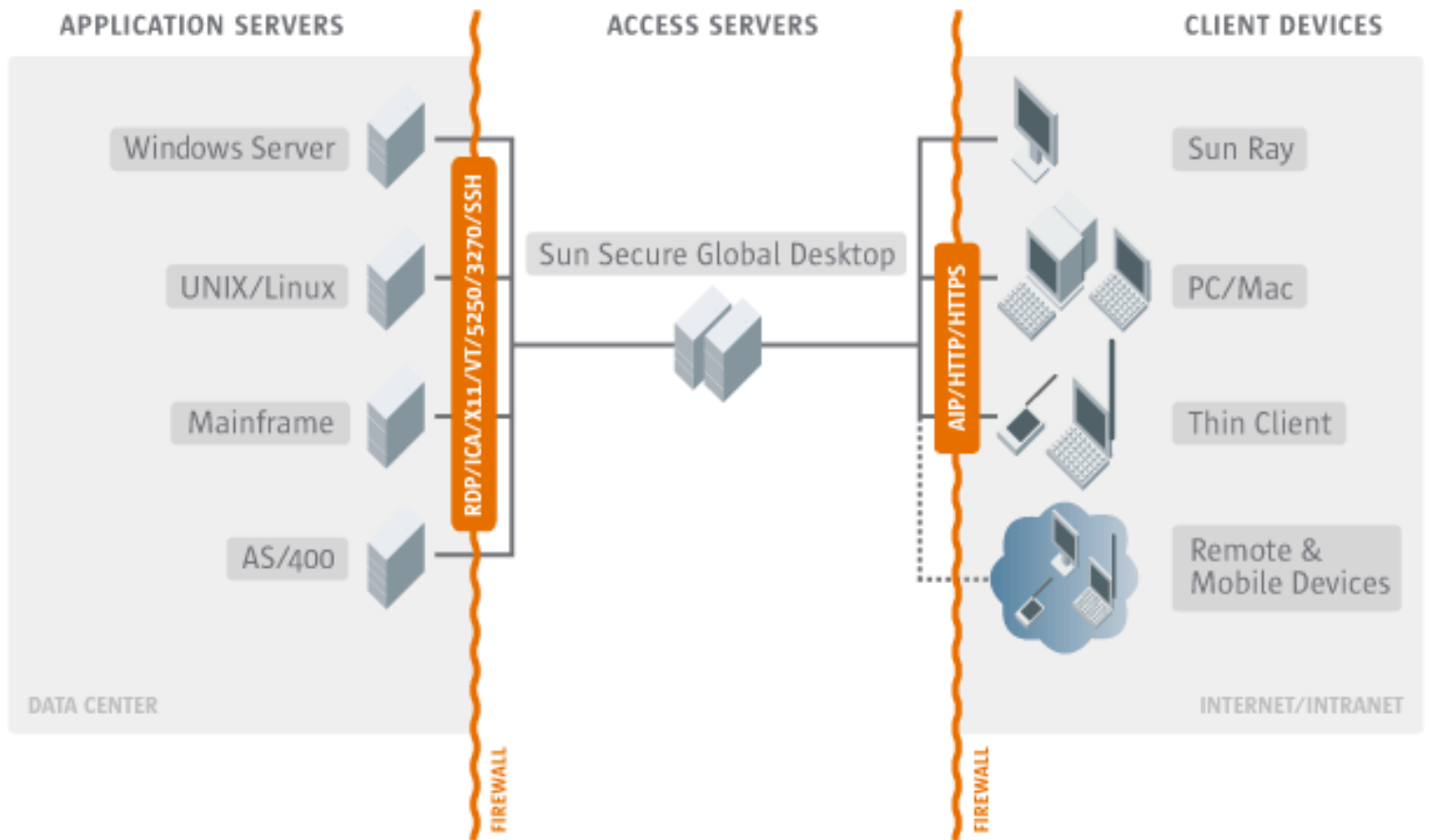
### Case study

Indigo Insurance currently uses two firewalls:

- An application server firewall surrounding all application servers.
- An external firewall between the Internet and the intranet.

Indigo Insurance is installing an array of Secure Global Desktop servers and wants to configure the firewalls to ensure access by client devices, both inside and outside the external firewall, to any application server, using Secure Global Desktop. Also, Indigo Insurance wants to protect the Secure Global Desktop servers behind their own firewall. Each host on which a Secure Global Desktop server is installed has a single network card.

Here's a diagram of the intended network structure:



## Solution

1. The external firewall and the Secure Global Desktop firewall must both allow network traffic for the web server and Secure Global Desktop server for **all array members**.
  - o For the web server:
    - **80/tcp** if you use an HTTP web server.
    - **443/tcp** if you use a secure (HTTPS) web server.
  - o For the Secure Global Desktop server:
    - **3144/tcp** if standard connections are available.
    - **5307/tcp** if secure connections are available.

Typically, you would open **either** ports 80/tcp and 3144/tcp **or** ports 443/tcp and 5307/tcp.

You should close port 5427/tcp. This is used for essential network traffic between Secure Global Desktop servers only.

You can expose only a subset of Secure Global Desktop array members on the Internet. However, if users typically log in to Secure Global Desktop from both inside and outside the external firewall then they may be unable to resume some applications when logging in from the Internet.

2. The application server firewall must allow network traffic between the Secure Global Desktop server and the application server for **all array members**. The ports you need to open depend on the types of application you're using.
  - o **22/tcp** for X and character applications using SSH.

- **23/tcp** for Windows, X and character applications using telnet.
  - **512/tcp** for X applications using rexec.
  - **3389/tcp** for Windows applications configured to use Windows Terminal Services.
  - **6010/tcp and above** for X applications (the number of ports to open depends on the number of simultaneous emulator sessions the Secure Global Desktop server will support).
3. To support printing, the application server firewall must allow network traffic between all array members and the application server on port **515/tcp**.
  4. The application server firewall should deny connections to ports 3144/tcp, 5307/tcp and 5427/tcp: these are not used for network traffic to and from application servers.
  5. Systems may be known by different names inside and outside firewalls. For each Secure Global Desktop array member:
    1. Find out the DNS name to use inside the Secure Global Desktop firewall for the Secure Global Desktop host, and the DNS name to use outside the Secure Global Desktop firewall for the Secure Global Desktop host. (The names may be the same.)
    2. Configure the web server to bind to the DNS name used **inside** the Secure Global Desktop firewall (this is the DNS name the web server binds to when it starts). Consult your web server documentation for help.
    3. Configure the Secure Global Desktop server with the name used **outside** the Secure Global Desktop firewall (this is the DNS name the client device uses to contact the web server). You configure this name in Array Manager, in the array member's [General](#) properties.

## Next steps

- You may also need to [use Secure Global Desktop with a proxy server](#).

### Related topics

- [Using Secure Global Desktop with the HTTPS port through a firewall](#)
- [What is an array?](#)
- [What ports does Secure Global Desktop use?](#)
- [Using Secure Global Desktop with proxy servers](#)

## Using Secure Global Desktop with the HTTPS port through a firewall

### Problem

Your firewall only allows web access from the Internet via port 443. You need Secure Global Desktop to use this port as well.

### Solution

Reconfigure Secure Global Desktop to listen on port 443. Then use the Firewall Forwarding facility to allow Secure Global Desktop to forward any traffic not related to Secure Global Desktop to your web server.

### Case study

Indigo Insurance, has their firewall configured to only allow HTTPS access (on port 443) from the Internet. They do not want to open any additional ports so their array of Secure Global Desktop servers must use the same port as well.

### Solution

1. In Array Manager, select Array and click the Properties button.
2. Change Port Numbers, Encrypted connections from 5307 to 443.
3. For each Secure Global Desktop server in the array, use `tarantella config list --array-port-encrypted` to check that the change to the port number has taken effect.
4. Reconfigure each web server in the array to listen on localhost port 443. For the Secure Global Desktop Web Server, edit the `<IfDefine SSL>` section in the `httpd.conf` file and change Listen 443 to Listen 127.0.0.1:443.
5. For each Secure Global Desktop server in the array, select Security properties and set Firewall Forwarding URL to `https://127.0.0.1:443`. (Alternatively, type `tarantella config edit --security-firewallurl https://127.0.0.1:443` from a command line.)
6. If you are using the browser-based webtop or you have developed your own web applications, you **must also secure the SOAP connections to a Secure Global Desktop server**.
7. Restart each Secure Global Desktop Web Server in the array, `tarantella webserver restart --ssl`.
8. Restart each Secure Global Desktop server in the array, `tarantella restart` command.

## Next steps

- You may need some additional configuration if you are using [Secure Global Desktop with proxy servers](#).

## Related topics

- [How can I support users with a client-side firewall that only allows connections on the HTTPS port?](#)
- [Securing the SOAP connections to a Secure Global Desktop server](#)
- [Security properties \(server-specific\)](#)
- [The tarantella security start command](#)
- [The tarantella security stop command](#)

[Secure Global Desktop Administration Guide](#) > [Security](#) > How can I support users with a client-side firewall that only allows connections on the HTTPS port?

## How can I support users with a client-side firewall that only allows connections on the HTTPS port?

If you have users with a client-side firewall that only allows connections on the HTTPS port (usually port 443/tcp), you can give them access to Secure Global Desktop by using [firewall forwarding](#).

With firewall forwarding, all connections to Secure Global Desktop are made over a single port (the port number is configurable). The Secure Global Desktop server listens on this port for any Adaptive Internet Protocol (AIP) traffic and forwards all other traffic to the web server on the same host.

### Related topics

- [Using Secure Global Desktop with the HTTPS port through a firewall](#)

## What are peer DNS names and external DNS names?

Each computer on the network may have a number of DNS names. For example, the web server `www.indigo-insurance.com` may also be known as `boston.indigo-insurance.com`.

In a network containing a firewall, you can ensure that some names are usable outside the firewall, for example across the Internet, and others are usable inside the firewall. For example, users outside the firewall might be able to use `www.indigo-insurance.com`, but not `boston.indigo-insurance.com`. Users inside the firewall might be able to use either name.

The Secure Global Desktop three-tier architecture can straddle firewalls, allowing access from client devices across the Internet.

- An **external DNS name** is the DNS name that the client devices use. For example, `www.indigo-insurance.com`.
- A **peer DNS name** is the DNS name that the Secure Global Desktop servers in the array use to identify themselves and each other. For example, `boston.indigo-insurance.com`.

These two DNS names may be associated with the same network card (NIC) on the Secure Global Desktop host, or they may each use a different network card.

### Related topics

- [General properties \(server-specific\)](#)
- [Using Secure Global Desktop with firewalls](#)



## What certificates does Secure Global Desktop support?

The Secure Global Desktop supports Base 64-encoded PEM-format X.509 server certificates for use with Secure Global Desktop security services. These have the following structure:

```
-----BEGIN CERTIFICATE-----  
...  
certificate  
...  
-----END CERTIFICATE-----
```

Secure Global Desktop supports X.509 certificates that have been signed with any of the following Certificate Authority (CA) certificates (root certificates):

- Baltimore CyberTrust Code Signing Root
- Baltimore CyberTrust Root
- Entrust.net CA
- Entrust.net Client CA 1
- Entrust.net Client CA 2
- Entrust.net Server CA 1
- Entrust.net Server CA 2
- Equifax Secure CA
- Equifax Secure eBusiness CA 1
- Equifax Secure eBusiness CA 2
- Equifax Secure Global eBusiness CA
- GeoTrust Global CA
- The Go Daddy Group, Inc. Class 2 CA
- GTE CyberTrust Root
- GTE CyberTrust Global Root
- GTE CyberTrust Root 5
- Starfield Technologies, Inc. Class 2 CA
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium CA
- Thawte Server CA

- <http://www.valicert.com>
- VeriSign Class 1 Public Primary CA - G1
- VeriSign Class 1 Public Primary CA - G2
- VeriSign Class 1 Public Primary CA - G3
- VeriSign Class 2 Public Primary CA - G1
- VeriSign Class 2 Public Primary CA - G2
- VeriSign Class 2 Public Primary CA - G3
- VeriSign Class 3 Public Primary CA - G1
- VeriSign Class 3 Public Primary CA - G2
- VeriSign Class 3 Public Primary CA - G3
- VeriSign Class 4 Public Primary CA - G2
- VeriSign Class 4 Public Primary CA - G3
- VeriSign/RSA Secure Server

You can use an X.509 certificate from any other CA. However, by default all users are prompted to accept or decline these certificates because they cannot be validated by Secure Global Desktop. With additional configuration you can [add support for a new CA](#), so that users are not prompted and certificates are validated.

**Note** The CAs supported by the Java™ technology client depends on the configuration of the Java Plug-in. By default, the Plug-in is configured to use the certificates in the browser keystore. If the Plug-in is not configured to do this, you may have to import the CA certificate (root certificate) using the Java Control Panel.

### Related topics

- [Obtaining and installing an X.509 certificate](#)
- [How do I support additional Certificate Authorities?](#)
- [User prompts and X.509 certificates](#)
- [Can I use an X.509 certificate for another product with Secure Global Desktop?](#)
- [Sharing web server and Secure Global Desktop server certificates](#)

## User prompts and X.509 certificates

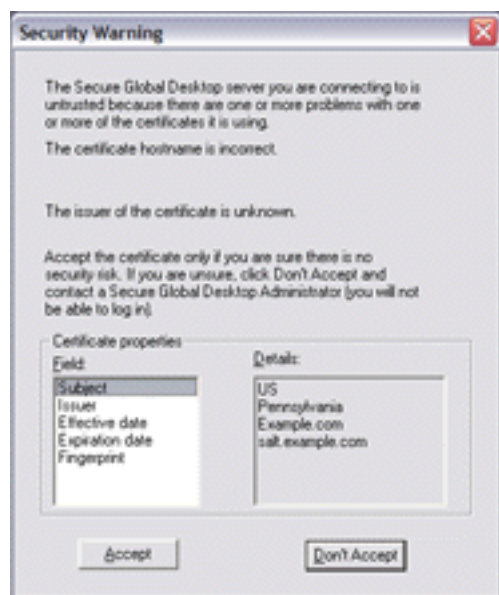
When users log in to a Secure Global Desktop server that has an X.509 certificate, their client validates the certificate before proceeding. If the certificate is valid and users have [agreed to the initial connection to Secure Global Desktop](#), the hostname and the fingerprint of the certificate are added to the `hostsvisited` file on the client device. The `hostsvisited` file is stored in the same location as the user's [profile cache](#).

However, if there are problems with the certificate, for example because the issuer of the certificate is unknown or the certificate has expired, users see a certificate warning message and they are prompted to accept or reject the certificate. **This is a potential security risk.** How certificate warnings are handled depends on whether or not Secure Global Desktop security services are enabled.

**Note** Users see prompts about security certificates **before** agreeing to trust the initial connection to Secure Global Desktop.

### Certificate warnings when security services are disabled

When Secure Global Desktop security services are disabled and users see a security warning message about a certificate, the warning message allows users to accept or reject the certificate.



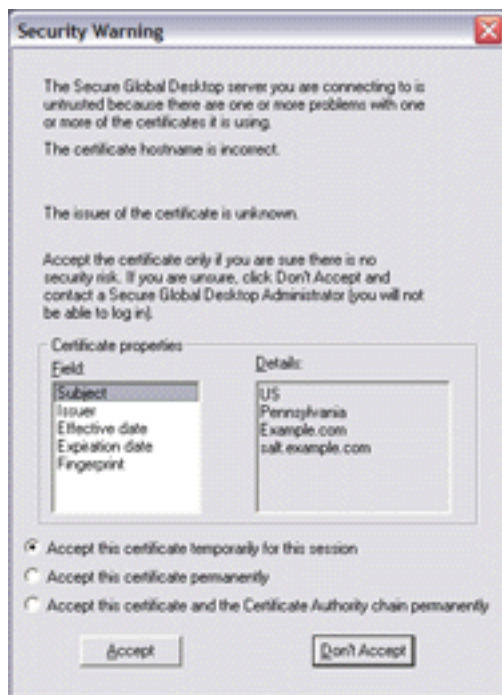
If users accept the certificate and they agree to the connection to the server, the hostname and fingerprint of the certificate are added to the `hostsvisited` file on the client device. The certificate is cached for the lifetime of the webtop session. When users next log in, they **are not prompted** about the certificate.

If users reject the certificate, the connection to Secure Global Desktop is terminated and the certificate details are not added to the `hostsvisited` file. When users next log in, they **are prompted** about the certificate.

If users have previously accepted a certificate, or if the only error with the certificate is that the issuer is unknown, then users **are not prompted** about the certificate.

## Certificate warnings when security services are enabled

When Secure Global Desktop security services are enabled and users see a security warning message about a certificate, the warning message allows users to accept the certificate permanently or temporarily, or to reject the certificate.



If users accept the certificate temporarily and they agree to the connection to the server, the hostname and fingerprint of the certificate are added to the `hostsvisited` file on the client device. The certificate is cached for the lifetime of the webtop session. When users next log in, they **are prompted** about the certificate.

If users accept the certificate permanently and they agree to the connection to the server, the hostname and fingerprint of the certificate are added to the `hostsvisited` file on the client device. The certificate is also added to the `certstore.pem` file on the client device. The `certstore.pem` file is stored in the same location as the user's [profile cache](#). Users can choose to accept just the certificate or [the certificate and its chain](#). When users next log in, they **are not prompted** about the certificate.

If users reject the certificate, the connection to Secure Global Desktop is terminated and no certificate

details are added to the `hostsvisited` file. When users next log in, they **are prompted** about the certificate.

## Avoiding issuer unknown errors

In a default installation, Secure Global Desktop supports [X.509 certificates that have been signed by a number of Certificate Authorities](#).

You can use any other type of Base 64-encoded PEM-format X.509 certificate. However, these certificates cannot be validated unless you [install the Certificate Authority \(CA\) certificate \(or root certificate\)](#) that was used to sign that certificate. If you do not install the CA certificate, users see an issuer unknown error and are prompted to accept or reject the certificate.

### Related topics

- [What certificates does Secure Global Desktop support?](#)
- [How do I support additional Certificate Authorities?](#)
- [The `tarantella security customca` command](#)

## What are X.509 certificates and why do I need one?

An X.509 certificate is an encoded file that a secure service, such as a web server, uses to identify itself to a client. A Secure Global Desktop server with security services enabled also requires a certificate in the same way.

Certificates are generated by Certificate Authorities (CAs) -- trusted third parties that sign a certificate for a particular server. To obtain a certificate for a server you must send a Certificate Signing Request (CSR) to one of these CAs. When a CA receives a CSR they check the validity of the request and return an X.509 certificate. You then install the certificate using the `tarantella security certuse` command.

By default, Secure Global Desktop [supports a number of Certificate Authorities](#).

In some cases, you can [share a certificate](#) between a web server and the Secure Global Desktop server on the same host.

### Related topics

- [Obtaining and installing an X.509 certificate](#)
- [What certificates does Secure Global Desktop support?](#)
- [How do I support additional Certificate Authorities?](#)

## Obtaining and installing an X.509 certificate

### Problem

You want to obtain and install an X.509 certificate for use with Secure Global Desktop security services.

### Solution

Use the `tarantella security certrequest` command to generate a Certificate Signing Request (CSR) for the Secure Global Desktop host. Then send the CSR to a [supported Certificate Authority](#), which will return a certificate for you to install on that host.

### Alternatives

- If you already have a certificate for another application, such as a web server, you may be able to [share that certificate with the Secure Global Desktop server](#).

### Case study

Indigo Insurance, based in Massachusetts, USA, wants to obtain an X.509 certificate for a Secure Global Desktop server.

### Solution

1. On the Secure Global Desktop host, use `tarantella security certrequest` to generate a Certificate Signing Request (CSR):

```
tarantella security certrequest \  
  --country US \  
  --state Massachusetts \  
  --orgname "Indigo Insurance"
```

2. Send the CSR to a [supported Certificate Authority](#).
3. Copy the returned certificate to a temporary file (for example, `/tmp/cert`), then type the following command to install it:

```
tarantella security certuse < /tmp/cert
```

## Next steps

- Once you've installed the X.509 certificate, you can enable secure connections with the `tarantella security start` command.
- There are [important security considerations](#) regarding X.509 certificates and user prompts.

## Related topics

- [Securing client connections with Secure Global Desktop security services](#)
- [Improving security between client devices and Secure Global Desktop servers](#)
- [Sharing web server and Secure Global Desktop server certificates](#)



## Can I use an X.509 certificate for another product with Secure Global Desktop?

To use an X.509 certificate originally obtained for another product (for example, a web server) with Secure Global Desktop, you need to decrypt the private key for that certificate. You can only decrypt private keys that were originally encrypted by a product that uses SSLeay or OpenSSL certificate libraries.

See [Sharing web server and Secure Global Desktop server certificates](#) for more information.

### Related topics

- [Obtaining and installing an X.509 certificate](#)

## Sharing web server and Secure Global Desktop server certificates

### Read this topic to...

- Learn how to share an X.509 certificate between a web server and a Secure Global Desktop server on the same host.

How you share an X.509 certificate between a web server and Secure Global Desktop, depends on whether or not you are using the Secure Global Desktop Web Server.

### Sharing a Secure Global Desktop server certificate with the Secure Global Desktop Web Server

The configuration file (`/opt/tarantella/webserver/apache/apache_version/conf/httpd.conf`) for the Secure Global Desktop Web Server is pre-configured to use the same certificates as the Secure Global Desktop server. These are installed in the `/opt/tarantella/var/tsp` directory. So to share a Secure Global Desktop server certificate with the Secure Global Desktop Web Server:

1. [Obtain and install an X.509 certificate](#) for use with Secure Global Desktop security services.
2. Enable secure (HTTPS) connections to the Secure Global Desktop Web Server with the `tarantella webserver restart --ssl` command.
3. Enable secure connections to the Secure Global Desktop server with the `tarantella security start` command.

### Sharing a certificate for your own web server with a Secure Global Desktop server

If you are using your own web server instead of the Secure Global Desktop Web Server and you want to share its certificate with a Secure Global Desktop server, you have to decrypt the certificate's key and then install it on the Secure Global Desktop server.

**Note** If your web server doesn't let you access the key or the key was not originally encrypted by a product that uses SSLeay or OpenSSL certificate libraries, you must [obtain and install a separate X.509 certificate](#).

To share a certificate:

1. Copy the web server certificate and key file to a safe place that can only be accessed by root, for example:

```
cp /usr/local/apache/certs/boston.indigo-insurance.com.pem /opt/tarantella/var/tsp/
cp /usr/local/apache/certs/boston.indigo-insurance.com.key.pem /opt/tarantella/var/tsp/
```

2. Use the `tarantella security decryptkey` command to decrypt the certificate's key, for example:

```
tarantella security decryptkey \
  --enckey /opt/tarantella/var/tsp/boston.indigo-insurance.com.key.pem \
  --deckey /opt/tarantella/var/tsp/boston.indigo-insurance.com.key.out \
  --format PEM
```

3. Use the `tarantella security certuse` command to install the X.509 certificate using the decrypted key file, for example:

```
tarantella security certuse
  --certfile /opt/tarantella/var/tsp/boston.indigo-insurance.com.pem
  --keyfile /opt/tarantella/var/tsp/boston.indigo-insurance.com.key.out
```

4. Enable secure connections to the Secure Global Desktop server with the `tarantella security start` command.

## Profile configuration

Once you enable secure connections to a web server, the URL in [the client profile](#) must be re-configured to an HTTPS URL.

### Related topics

- What are X.509 certificates and why do I need one?
- Can I use an X.509 certificate for another product with Secure Global Desktop?
- Securing the SOAP connections to a Secure Global Desktop server

## Can I chain Certificate Authority certificates?

Chaining allows the use of intermediate Certificate Authorities. For example, an X.509 server certificate could be signed by an intermediate Certificate Authority, whose own certificate is issued by a different Certificate Authority.

You can use X.509 server certificates that are signed in this way with Secure Global Desktop. However, **certificates for all the links in the chain must be installed** as a Secure Global Desktop custom Certificate Authority.

To do this, combine all the certificates as input to the `tarantella security customca` command. The certificate of the CA used to sign the X.509 server certificate **must appear first**.

For the example above, you could create a file `mychainedcerts.pem` containing:

```
-----BEGIN CERTIFICATE-----  
...  
Intermediate CA's certificate  
...  
-----END CERTIFICATE-----  
  
-----BEGIN CERTIFICATE-----  
...  
CA root certificate  
...  
-----END CERTIFICATE-----
```

You would install this with the command:

```
tarantella security customca --rootfile mychainedcerts.pem
```

If any certificate in the chain is corrupt or invalid, users will see "Certificate Authority not recognized" when they try to log in to Secure Global Desktop, and will be denied access.

### Related topics

- What certificates does Secure Global Desktop support?
- The tarantella security customca command
- Obtaining and installing an X.509 certificate
- User prompts and X.509 certificates
- How do I support additional Certificate Authorities?

## How do I support additional Certificate Authorities?

By default, the Secure Global Desktop [supports a number of Certificate Authorities](#). You can use a Base 64-encoded PEM-format X.509 certificate from an unsupported Certificate Authority (CA) without extra configuration, but certificates are not validated and [users are prompted to accept or decline the certificate](#). This is a potential security risk.

To support additional CAs and allow certificates to be validated, you must install the CA's certificate, or root certificate, for that CA. On the Secure Global Desktop host, type:

```
tarantella security customca
```

Then paste your root certificate in PEM format to standard input.

If your X.509 certificate was signed by an Intermediate CA, you must [install the certificate chain](#).

### Sun Secure Global Desktop Client

If the X.509 certificate is issued by an unsupported CA, the Sun Secure Global Desktop Client always [prompts users about the certificate](#) the first time they connect to the server. If users accept the certificate permanently, they are not prompted about the certificate again. The only way to prevent users from being prompted about the certificate is to:

- Add the server certificate to the `certstore.pem` file on the client device. The certificate is in the `/opt/tarantella/var/tsp/cert.pem` file on each host.
- Add the hostname and fingerprint of the certificate to the `hostnames` file on the client device. Run the `tarantella security fingerprint` command on each host to obtain these details.

### Sun Secure Global Desktop Native Client

Users of the Native Client must download and install the root certificate as follows:

- Download the root certificate from the Sun Secure Global Desktop Native Client download page, available from `http://server.example.com`.
- On Windows client devices, import the root certificate using Internet Options in the Windows Control Panel.
- On UNIX/Linux/Mac OS X client devices, the Sun Secure Global Desktop Native Client searches

the following locations for the root certificate file (`ca.pem`):

- The `/etc/tarantella` directory.
- The location specified in the [user preferences file](#).

## Secure (HTTPS) web servers

If you are using a secure (HTTPS) web server, users are prompted to accept the web server's certificate if the root certificate has not been imported into the web browser's keystore. To allow the web server certificate to be validated without prompting the user, import the root certificate into the user's web browser using the browser's tools for doing this.

If you are using Java™ technology with a secure web server, the Java Plug-in may also prompt users to accept the web server's certificate. This depends on the configuration in the Java Control Panel. By default, the Plug-in is configured to use the certificates in the browser keystore. If the Plug-in is not configured to do this, you may have to import the root certificate using the Java Control Panel.

If you are [sharing Secure Global Desktop server certificates with a web server](#), you can download the root certificate from the Sun Secure Global Desktop Native Client download page, available from <http://server.example.com>.

### Related topics

- [What certificates does Secure Global Desktop support?](#)
- [The tarantella security customca command](#)
- [Obtaining and installing an X.509 certificate](#)
- [User prompts and X.509 certificates](#)
- [Can I chain Certificate Authority certificates?](#)



## Introducing Secure Global Desktop printing

### Read this topic to...

- Understand how Secure Global Desktop printing works.
- Find out how users and administrators control Secure Global Desktop print jobs.
- Learn the main steps for configuring Secure Global Desktop printing.

Secure Global Desktop allows users to print from Windows, X and character applications to a printer attached to their client device. Secure Global Desktop does this by co-operating with the `lp` or `lpr` printing system on the Secure Global Desktop host and the native printing system on the application server.

When a user prints, the print job is sent from the application server to Secure Global Desktop server. The Secure Global Desktop server then sends the print job to the client, which sends it to the user's printer.

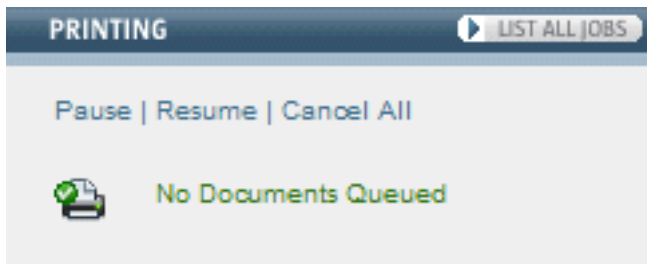
Secure Global Desktop uses **distributed printing**. Print jobs are always sent to the Secure Global Desktop server hosting the emulator session for the application. This means that a user's print jobs are distributed across the array, and there are no bottlenecks or single points of failure.

If the format of the print job used by the application server is different to the format needed by the client printer, Secure Global Desktop converts the print job before sending it to the client.

With **PDF printing**, users print from a Windows, UNIX or Linux application using a Secure Global Desktop PDF printer. The print job is sent from the application server to Secure Global Desktop where it is converted into a portable document format (PDF) file. Secure Global Desktop then sends the PDF file to a PDF viewer on the user's client device where the file can be viewed, saved and printed. PDF printing can be used to avoid issues with printer drivers and print job formats.

### Users manage their own print jobs



Users manage their own print jobs from the Printing area on the webtop:



When documents are printing, the webtop tells a user how many print jobs they have in the queue. Users can click Cancel All to delete all pending print jobs.

Users can also click Pause to temporarily stop printing. When printing is paused, any print jobs that are pending are held in a queue until the user either cancels them or resumes printing. Click Resume to start printing again. The printer icon changes to show you when printing is paused.



To manage print jobs individually, click List all jobs. The webtop displays a list of all the print jobs the user has in the queue, along with information about the job, for example the number of copies and the printer that will be used. If you have paused printing, click  to print just that one print job. To cancel a print job, click .

When printing from a Windows 2000 Server, Windows Server 2003, UNIX or Linux application server, users can choose which printer they print to. If the user does not select a printer, the output will go to their default printer. For all other application servers, the output always goes to the client device's default printer.

Users can see which printer is their default printer by pointing with the mouse at the printer icon on their webtop. A popup displays the name of the default printer.

If a user wants to change their default printer, they must log out of Secure Global Desktop, change the default printer and then log in to again.

## Secure Global Desktop Administrators control printing services

Secure Global Desktop Administrators control printing services with the `tarantella print` command. This command lets you:

- List spooled print jobs and identify the Secure Global Desktop users they belong to. You can use this to check that print jobs from the application server printing system have reached the Secure Global Desktop print queue.
- Remove print jobs from the Secure Global Desktop print queue.
- Pause and restart Secure Global Desktop printing services.
- Move print jobs from one Secure Global Desktop server to another.

## Configuring Secure Global Desktop printing

To be able to print with Secure Global Desktop, you may have to do the following::

1. Configure your application servers.
  - o [UNIX and Linux application servers](#)
  - o [Microsoft Windows 2000/2003 application server](#)
  - o [Microsoft Windows NT 4 application server](#)
  - o [Microsoft Windows NT 3.51 application server](#)
2. [Configure the Secure Global Desktop server to accept remote print requests.](#)
3. [Configure printing if you use the Common UNIX Printing System \(CUPS\).](#)
4. [Configure printing for UNIX clients.](#)
5. [Configure Secure Global Desktop PDF printing.](#)
6. [Configure Secure Global Desktop print job conversion.](#)

If you have trouble printing, follow the steps in the [printing troubleshooter](#).

### Related topics

- [The tarantella print command](#)

## Printing from a Microsoft Windows 2000/2003 application server

When users start or resume a Windows application that uses the Microsoft RDP [Windows Protocol](#), information about the client's printers is sent to Secure Global Desktop. Secure Global Desktop supplies this information to the application server and the application server then creates (or maps) the printers in the Windows Terminal Services session.

When accessing an application on a Microsoft Windows 2000 Server or Microsoft Windows Server 2003, a user sees the printers that are attached to the client and also the printers that are attached directly to the application server.

For users with Windows clients, Secure Global Desktop Administrators can use the settings on the [Printing properties](#) panel in Array Manager to control whether users see all their client printers, just their default client printer, or no client printers. The settings on this panel can be overridden by the settings on the Printing panel for [organization](#), [organizational unit](#) or [person](#) objects in Object Manager.

For users on other client platforms, the client printer users can see depends on the [printers that have been configured](#).

In the application server's Printers folder, the names of the client printers display as follows:

- in a Windows 2000 session, "*printer\_name/Tarantella/Session number*", for example:  
HP LaserJet 8000 Series PS/Tarantella/Session 1
- in a Windows 2003 session, "*printer\_name (from Tarantella) in session number*", for example:  
HP LaserJet 8000 Series PS (from Tarantella) in session 1

To be able to create a printer on the application server:

- [Printer mapping](#) must be enabled on the application server.
- The client must determine the name of the printer driver for the client printer and send it to application server.
- The printer driver for the client printer must be installed on the application server.

For Windows clients, the printer driver name is determined automatically from the client device using the standard Windows printing API. For all other client types, the printer driver must be configured in a printing configuration file, see [configuring printing for UNIX, Linux and Mac OS X clients](#) for details.

When printing from a Windows application, the large number and variety of client printers available can cause problems. The majority of the problems are caused by not having the correct printer drivers installed on the application server. One solution is to use [Secure Global Desktop PDF printing](#). Another solution, for Windows clients only, is to use printer driver mapping.

## Printer driver mapping

For Windows clients, you can use printer driver mapping to map one printer driver name to another. You do this by editing the `[Previous Names]` section of the `/opt/tarantella/etc/data/default.printerinfo.txt` file.

For example, if the file contains the following entry:

```
[Previous Names]
"HP LaserJet 5" = "my HP driver", "my other HP driver"
```

This means that if you have any client printers that use either the "my HP driver" or "my other HP driver" printer driver, Secure Global Desktop will use the "HP LaserJet 5" printer driver when creating the printer.

You can also use wild-card characters ( `*` and `?` ) on the right hand side of the `=` sign. Use `*` to mean any string of characters including an empty string and `?` to mean any single character. This is useful, for example, to create generic printer mappings where you have a wide variety of client devices.

For example, if the file contains the following entry:

```
[Previous Names]
"HP LaserJet 5" = "hp*laserjet 5*"
```

All printer driver names like "HP LaserJet 5", "HP LaserJet 5M", and "HP Color LaserJet 5" would be mapped to the printer driver "HP LaserJet 5".

The `default.printerinfo.txt` file contains more detailed instructions on how to create the mappings.

### Related topics

- Introducing Secure Global Desktop printing
- The tarantella print command
- Configuring Secure Global Desktop PDF printing
- Users cannot print from applications displayed through Secure Global Desktop
- Windows Protocol (--winproto)

## Printing from a UNIX or Linux application server

To print from a UNIX or Linux application server, you have to manually configure at least one Secure Global Desktop printer on the application server. This printer redirects all print jobs to a Secure Global Desktop server. If your array contains more than one Secure Global Desktop server, you need to create a printer for each member of the array.

You configure printers with the Secure Global Desktop printer installation script. This script also installs replacement `lp` or `lpr` scripts. These are used instead of the standard scripts to ensure that print jobs contain enough information for Secure Global Desktop to be able to identify the user who printed them.

If you use the Common UNIX Printing System (CUPS), follow these [additional configuration steps](#).

### Configuring a Secure Global Desktop printer on the application server

You configure a printer on the application server using the `prtinstall.en.sh` script. This script creates a printer, called `tta_printer` by default. This printer redirects print jobs from the application server to the printer on the Secure Global Desktop server (this is also named `tta_printer`).

**Note** If you use the Secure Global Desktop server as an application server, a printer is automatically created when you install the software.

You configure printers as follows:

1. Copy `/opt/tarantella/bin/scripts/prtinstall.en.sh` from a Secure Global Desktop server to a temporary directory on the application server.
2. Log in to the application server as root.
3. Change to the temporary directory.
4. Run the script.

If the array consists of a single Secure Global Desktop server, type:

```
sh prtinstall.en.sh
```

When prompted, type the full DNS name of the Secure Global Desktop server.

If the array contains more than one Secure Global Desktop server, create a printer **for each**

**member of the array.** Type:

```
sh prtinstall.en.sh --ttahost DNS_name --appprinter printer name
```

The *DNS\_name* is the full DNS name of a Secure Global Desktop server. The name of each printer (as specified by the `--appprinter` argument) can be anything you like but it **must** be unique.

## Using the Secure Global Desktop lp or lpr scripts

The `prtinstall.en.sh` script also installs the Secure Global Desktop `lp` or `lpr` replacement scripts. Users must use these scripts when they print from the application server to ensure that print jobs contain enough information for Secure Global Desktop to be able to identify the user who printed them.

The Secure Global Desktop [login scripts](#) set the user's `PATH` to ensure that the replacement scripts take precedence over the system scripts. However, if the application uses a full pathname, for example `/usr/bin/lp`, or modifies `PATH` itself, you should reconfigure the application to use `/opt/tarantella/bin/lp` or `/opt/tarantella/bin/lpr`.

Users print with the replacement scripts as follows:

```
lp -d printer file  
lpr -P printer file
```

If the `-d` or `-P` argument is omitted, the output goes to the client's default printer.

How you specify the *printer* depends on whether the user is printing to a Windows or a UNIX, Linux or Mac OS X client.

**Note** An alternative to the configuration described below is to use [Secure Global Desktop PDF printing](#).

### Printing to a Windows client

When printing to a Windows client, users specify the printer by using any of the following:

- The universal naming convention (UNC) name of a network printer accessible to the client, for example:

```
lp -d '\\\\PRTSERVER\\HPLJ5' filename
```

- A "friendly" name, for example:



```
lpr -P label-printer filename
```

- A port on the client, for example:

```
lpr -P LPT1: filename
```

To use a UNC name, you must enclose the printer name in quotes and escape every backslash with an extra backslash (see the example above). As different shells process backslashes differently, you may need to experiment with the number of backslashes. Users can also use underscores instead of backslashes, for example:

```
lp -d __PRTSERVER_HPLJ5 filename
```

**Note** Using underscores only works if the first two characters of the printer name are underscores.

You can avoid problems with UNC names by using a "friendly" name. You configure "friendly" names in the `/opt/tarantella/etc/data/printernamemap.txt` file. The entries in this file map "friendly" names to UNC names, for example:

```
"label-printer"="\PRTSERVER\HPLJ5"
```

**Note** You do not have to escape any backslashes.

## Printing to a UNIX, Linux or Mac OS X client

When printing to a UNIX, Linux or Mac OS X client, users can specify any printer listed in the `[UNIX]` section of either the global `/opt/tarantella/etc/data/default.printerinfo.txt` file or the user-specific `$HOME/.tarantella/printerinfo.txt` file, for example:

```
lp -d A4-printer filename
lpr -P color-printer filename
```

See [configuring printing for UNIX, Linux and Mac OS X clients](#) for details of how to configure printer names.

## Related topics

- Introducing Secure Global Desktop printing
- The tarantella print command
- The prtinstall.en.sh script
- Users cannot print from applications displayed through Secure Global Desktop

## Printing from a Microsoft Windows NT 4 application server

The configuration needed to allow users to print from a Microsoft Windows NT 4 application server depends on whether the application uses the Microsoft RDP or the Citrix ICA [Windows protocol](#).

### Configuring printing for applications that use the Microsoft RDP protocol

To print from an application that uses the Microsoft RDP protocol, you have to have to configure an LPR-compatible TCP/IP printer on the application server as follows:

1. Log in to the application server as a Windows administrator or a member of the Administration group.
2. In Windows Control Panel, double-click Network.
3. In the Services tab, click Add to install the Microsoft TCP/IP service.
4. Run the Add Printer Wizard on the application server to configure the new printer.
5. When prompted, click Local Printer. Clear the Automatically Detect My Printer box.
6. Click Create A New Port and then click LPR Port.
7. In Name Or Address Of Server Providing lpd, type the full DNS name of the primary Secure Global Desktop server in the array.
8. In Name Of Printer Or Print Queue On That Server, type `ttta_printer`.
9. When prompted, choose the printer model and manufacturer that most closely matches the client device's default printer. If there's no close match, choose a PostScript printer.
10. When prompted as to whether the printer will be shared with other network users, click Do Not Share This Printer.

**Note** This configuration is necessary because the version of Microsoft RDP supported by Windows NT 4 is not the same as the version supported by Windows 2000/2003.

### Configuring printing for applications that use the Citrix ICA protocol

To print from an application that uses the Citrix ICA protocol, you have to configure a Secure Global Desktop printer on the UNIX server running the ICA client **and** on the Windows application server. You do this as follows:

1. [Configure a Secure Global Desktop printer on the UNIX application server](#) that runs the ICA client.
2. Use Secure Global Desktop to log in to the Windows application server. Use the Citrix ICA

protocol.

3. Start the Add Printer Wizard.
4. When prompted how the printer should be managed, click Network Printer Server.
5. In the Connect to Printer box, double-click the Client icon.
6. In the Shared Printer list, double-click the printer you want to configure. The name of the printer you need to select has the format *ip\_address:#printer\_name*, where *ip\_address* is the IP address of the primary Secure Global Desktop server in the array and *printer\_name* is the name of the printer you configured on the UNIX application server.
7. When prompted, choose the printer model and manufacturer that most closely matches the client device's default printer. If there's no close match, choose a PostScript printer.

## Limitations

Printing from a Windows NT 4 application server has the following limitations:

- **No multiple printer support** - you can only print to the client device's default printer. It is not possible for users to select a printer. If a user needs to print to a different printer, they have to log out of Secure Global Desktop, change their default printer and then log in again.
- **Print jobs may be deleted** - when a print job is transferred from the application server to a Secure Global Desktop server, the user's Secure Global Desktop name is needed to identify which client device to sent the print job to. With Windows NT 4 there is no direct way to associate print jobs with Secure Global Desktop users. If Secure Global Desktop cannot identify which user has printed a particular job, the print job is deleted. This might happen, for example, if two users log in to the application server with the same name.
- **Distributed printing is not available** - all print jobs are directed through the primary server in a Secure Global Desktop array.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [The tarantella print command](#)

## Printing from a Microsoft Windows NT 3.51 application server

You can only print from a Microsoft Windows NT 3.51 application server if the application is configured to use the Citrix ICA [Windows Protocol](#). You also have to configure an LPR-compatible TCP/IP printer on the application server as follows:

1. Log in to the application server as a Windows administrator or a member of the Administration group.
2. In Windows Control Panel, double-click Network.
3. Click Add Software.
4. In the Network Software list, click TCP/IP Protocol and Related Components.
5. In Components, select the TCP/IP Network Printing Support box.
6. Run Printer Manager on the application server to configure the new printer.
7. On the Printer Menu, click Create Printer.
8. In the Driver box, click the printer model and manufacturer that most closely matches the client device's default printer. If there's no close match, choose a PostScript printer.
9. Clear the Share This Printer On The Network box.
10. In the Print To box, click Other.
11. In the Available Print Monitors list, double-click LPR Port.
12. In Name Or Address Of Server Providing lpd, type the full DNS name of the primary Secure Global Desktop server in the array.
13. In Name Of Printer Or Print Queue On That Server, type `tta_printer`.

## Limitations

Printing from a Windows NT 3.51 application server has the following limitations:

- **No multiple printer support** - you can only print to the client device's default printer. It is not possible for users to select a printer. If a user needs to print to a different printer, they have to log out of Secure Global Desktop, change their default printer and then log in again.
- **Print jobs may be deleted** - when a print job is transferred from the application server to a Secure Global Desktop server, the user's Secure Global Desktop name is needed to identify which client device to sent the print job to. With Windows NT 3.51 there is no direct way to associate print jobs with Secure Global Desktop users. If Secure Global Desktop cannot identify which user has printed a particular job, the print job is deleted. This might happen, for example, if two users log in to the application server with the same name.

- **Distributed printing is not available** - all print jobs are directed through the primary server in a Secure Global Desktop array.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [The tarantella print command](#)

## Configuring the Secure Global Desktop server to accept remote print requests

To be able to direct print jobs from an application server to a client device, the Secure Global Desktop server must be configured to accept remote print requests. How you do this varies for each platform. Check your System Administration documentation for information about this.

For example, if you are using `lpd` on Linux platforms, you must add an entry in the `/etc/hosts.equiv` or `/etc/hosts.lpd` file (if available) for each application server that may send a print request. After making these changes, remember to restart the LPD daemon.

**Note** For Windows applications that use the Citrix ICA Windows protocol, the entry in `/etc/hosts.equiv` is for the UNIX server running the ICA client.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [The tarantella print command](#)
- [Users cannot print from applications displayed through Secure Global Desktop](#)

## Configuring printing if you use the Common UNIX Printing System (CUPS)

To be able to print using the Common UNIX Printing System (CUPS):

- Users must use the `/opt/tarantella/bin/lp` script for printing.
- CUPS version 1.1.19 or later must be installed.
- CUPS LPD compatibility mode must be enabled for any LPD clients.

If you have any LPD clients on your application server, you must enable the CUPS LPD compatibility mode so that CUPS will accept remote print jobs from LPD clients. The [CUPS Software Administrators Manual](#) explains how you enable LPD compatibility mode.

- CUPS 'raw printing' must be enabled.

On the host on which Secure Global Desktop is installed, enable 'raw printing' in CUPS by editing the `/etc/cups/mime.convs` and `/etc/cups/mime.types` files. These files contain comments explaining how to do this (search for 'raw').

- When you run the `prtinstall.en.sh` script to install a printer on the application server, you may have to use the `--cups` option to indicate that you are using CUPS.

**Note** After making changes to your CUPS configuration, you may have to restart the CUPS daemon.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [The tarantella print command](#)
- [The prtinstall.en.sh script](#)



## Configuring printing for UNIX, Linux and Mac OS X clients

To allow users to print to printers attached to UNIX, Linux or Mac OS X client devices, the printers must be configured in one of the following printer configuration files:

- The global printer configuration file `/opt/tarantella/etc/data/default.printerinfo.txt`.

This file sets the defaults for **all** users printing through that Secure Global Desktop server. As this file is not replicated across the array, you have to manually copy it to the other array members.

- The user-specific printer configuration file `~/.tarantella/printerinfo.txt`.

This file is optional and has to be manually created on client devices. Users can create their own file or you can use the global configuration file as a template and distribute it to users. This file contains the settings for an individual user regardless of which Secure Global Desktop server they print through. The settings in this file take precedence over the settings in the global configuration file.

**Note** An alternative to the configuration described below is to use [Secure Global Desktop PDF printing](#).

The format of the global and user-specific printer configuration file is the same:

```
[UNIX]
"printer_name" = "windows_driver" printer_type
"printer_name" = "windows_driver" printer_type
...
```

**printer\_name** is the name of the printer as it is known to the `lp` or `lpr` system on the client. The printer name must be enclosed in double quotes and be followed by an equals sign. This is the name that users can specify when [printing from a UNIX or Linux application server](#). It is also the name that displays in the Print dialog when users [print from a Windows 2000/2003 application server](#).

**windows\_driver** is the name of the printer driver to use when printing from a Windows 2000/2003 application server. The printer driver name must be enclosed in double quotes. The name of the printer driver must match the name of the printer driver installed on the Windows application server exactly. Pay particular attention to the use of capitals and spaces. The `default.printerinfo.txt` file

contains all the common printer driver names ordered by manufacturer. To avoid errors, copy and paste the driver name from this file.

***printer\_type*** is the format to be used for the print job. The values can be `PostScript`, `PCL` or `Text`. This information is optional, but if it is missing, `PostScript` is used by default. This information is used to determine whether Secure Global Desktop needs to [convert the print job](#) from the format used by the application server to the format used by the printer.

The first printer listed in the `[UNIX]` section is the client's default printer.

When Secure Global Desktop is first installed, the `default.printerinfo.txt` file contains the following entry:

```
[UNIX]
"_Default" = "QMS 1060 Print System" PostScript
```

With this configuration, when users print from a Windows 2003 application server, they see a printer called `_Default (from Tarantella) Session number`. This printer prints to the default printer on the client using a basic PostScript printer driver, "QMS 1060 Print System".

**Note** This also means that a printer will be available in the Windows application even if there is no printer connected to the client.

## Example

Graham Green's `$HOME/.tarantella/printerinfo.txt` file contains the following entries:

```
[UNIX]
"drafts" = "HP DeskJet 970Cxi" PCL
"salesprinter" = "HP LaserJet 5/5M" PostScript
```

When he prints from a Windows 2000 application server to a UNIX client, he has two printers called:

- `drafts/Tarantella/Session number`
- `salesprinter/Tarantella/Session number`

His default printer is `drafts/Tarantella/Session number`, which in this example has been defined as a PCL printer.

## Related topics

- [Introducing Secure Global Desktop printing](#)
- [The tarantella print command](#)
- [Users cannot print from applications displayed through Secure Global Desktop](#)

## Configuring Secure Global Desktop print job conversion

With Secure Global Desktop printing, print jobs are sent from an application server to a Secure Global Desktop server. The Secure Global Desktop server then sends the print job to the client, which sends it to the user's printer. When print jobs arrive at the Secure Global Desktop server, they may need to be converted to a format suitable for the client printer.

To decide whether a print job needs to be converted, the Secure Global Desktop server checks a printer type configuration file to see whether the format used by the client printer matches the format used by the application server. If the format matches, the print job is forwarded to the client device printer without any conversion. If the formats do not match, the Secure Global Desktop server converts the print job to the right format using the `tta_print_converter` script.

**Note** A print job from a Windows 2000/2003 application that uses the the Microsoft RDP [Windows Protocol](#) is **never** converted because it is assumed to be correctly formatted.

To ensure that print jobs are formatted correctly, you may have to edit a printer type configuration file and the `tta_print_converter` script.

### Editing a printer type configuration file

Secure Global Desktop uses the following configuration files to determine the printer type:

- **UNIX and Linux clients** - either `/opt/tarantella/etc/data/default.printerinfo.txt` or `~/tarantella/printerinfo.txt`
- **Windows and Apple Macintosh clients** - `/opt/tarantella/etc/data/printertypes.txt`

You should edit these files if you want to support particular printers or add new types of printer.

**Note** If you add a new printer type, you may also have to edit the `tta_print_converter` script.

If there is insufficient detail or inaccurate mappings in these files, Secure Global Desktop may convert print jobs unnecessarily or not at all.

### Editing the printer configuration file for UNIX Linux and Mac OS X clients

See [configuring printing for UNIX, Linux and Mac OS X clients](#) for details of how to configure printers, including setting the printer type.

## Editing the printer configuration file for Windows clients

For Windows client devices, the `printertypes.txt` file maps printer drivers, for example, `pscript.dll`, to printer types, for example PostScript.

The `printertypes.txt` file includes comments to help you customize it. By default, the file includes mappings for PostScript, PCL and text-only printers.

**Note** The `printertypes.txt` file used for Windows clients also contains entries for UNIX and Apple Macintosh. This is used only as a fallback. For UNIX, it maps UNIX types to printer types. For Apple Macintosh, it maps printer names to printer types.

**Note** You must be logged on as root to edit this file.

On Microsoft Windows systems, to find out the name of the printer driver used by a client device, print a test page and check the Driver Name field.

To add support for a new printer type, add lines following the same pattern. For example:

```
MyNewType=mydriver.drv
```

### Example

Rusty Spanner's client device, `cairo`, runs Windows 2000 and its default printer is PCL. The printer driver in use is `unidrv.dll`.

The Windows 2000 section in `printertypes.txt` has the following:

```
[Windows2000]
PostScript=pscript5.dll;pscript.dll
PCL=rasdd.dll
PostScript=*
```

As there is no specific match for `unidrv.dll`, the final entry applies: PostScript. This means that when Rusty prints, print jobs are incorrectly converted to PostScript before being sent to `cairo`.

To fix this, edit `printertypes.txt` as root to add a specific match for `unidrv.dll`:

```
PCL=rasdd.dll;unidrv.dll
```

Now Secure Global Desktop correctly identifies the printer configured on cairo, and print jobs are converted to PCL for that client device.

## Editing the `tta_print_converter` script

The `tta_print_converter` script converts print jobs from the format used by the application server to the format required by the client device and is determined by the printer type. By default, the script recognizes PostScript and non-PostScript formats. The script uses Ghostscript, available separately, to convert print jobs from PostScript to PCL.

You can edit the `tta_print_converter` script to recognize and convert between different print job formats or to add support for a new printer type.

The shell function `GetDataType` determines the print job format from the first 128 bytes of the print job. The data is URL-encoded: for example, the % character is encoded as %25.

The client printer type is passed to this script in upper case, for example `POSTSCRIPT` or `MYNEWTTYPE`.

The `tta_print_converter` script can be found in the `/opt/tarantella/bin/scripts` directory and it includes comments to help you customize it.

If you experience problems printing to a PCL printer, the `tta_print_converter` script contains some code which has been commented out. You can use this code to see if this solves the problem.

**Note** You must be logged on as root to edit this script.

## Ghostscript

The `tta_print_converter` script uses [Ghostscript](#) to convert print jobs from PostScript to PCL. For best results we recommend you download and install the additional fonts.

When you install Secure Global Desktop, Secure Global Desktop Setup automatically detects Ghostscript if it is installed in one of the following locations:

- `/usr/local/bin`
- `/usr/bin`
- `/opt/sfw/bin`
- `/bin`
- `/usr/sbin`
- `/sbin`
- `/usr/lbin`

If Ghostscript is installed elsewhere, you must run the `prtinstall.en.sh` script with the `--gsbindir` option to tell Secure Global Desktop where to find Ghostscript.

If Ghostscript is not installed, you must install it and then run the `prtinstall.en.sh` script.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [The tarantella print command](#)

## Configuring Secure Global Desktop PDF printing

With Secure Global Desktop PDF printing, users print from a Windows, UNIX or Linux application using a Secure Global Desktop PDF printer. The print job is sent from the application server to Secure Global Desktop where it is converted into a portable document format (PDF) file. Secure Global Desktop then sends the PDF file to a PDF viewer on the user's client device where the file can be viewed, saved and printed.

You configure PDF printing as follows:

1. [Enable the Secure Global Desktop PDF printers.](#)
2. [Check the Ghostscript installation on the Secure Global Desktop host.](#)
3. [Configure PDF viewers on client devices.](#)

Once you have configured PDF printing, you should tell users [how to use PDF printing](#).

### Enabling the Secure Global Desktop PDF printers

Secure Global Desktop has two PDF printers: Universal PDF and Print to Local PDF File.

On Windows client devices, the Universal PDF printer displays the print job as a PDF file in the Adobe Reader, which then prints the PDF file to the user's default printer. The Print to Local PDF File printer displays the print job as a PDF file in the Adobe Reader, which the user can then decide whether to print or save.

On UNIX, Linux and Mac OS X client devices, there is no difference between the Universal PDF and Print to Local PDF File printers as the print job is always displayed as a PDF file in a PDF viewer. The user can then decide whether to print or save the PDF file.

The following configuration is needed to enable the Secure Global Desktop PDF printers.

#### Configuring PDF printers on UNIX and Linux application servers

To use PDF printing, you must [install a Secure Global Desktop printer on the application server](#) using the [Secure Global Desktop printer installation script](#).

#### Configuring PDF printers on Windows application servers



To use PDF printing, you must first choose and install the PostScript printer driver that will be used for PDF printing. Make sure the printer driver has sufficient features for your users. Install this printer driver on **every** Windows application server. By default, Secure Global Desktop is configured to use the `HP Color LaserJet 8500 PS` printer driver.

You enable the PDF printers for the whole array on the [Printing properties](#) panel in Array Manager. The settings on this panel can be overridden by the settings on the Printing panel for [organization](#), [organizational unit](#) or [person](#) objects in Object Manager. You configure PDF printers as follows:

- **Let users print to a PDF printer** - check the box to enable the Universal PDF printer.
- **Let users print to a PDF local file** - check the box to enable the Print to Local PDF File printer.
- **Driver name** - type the name of the PostScript printer driver to use for PDF printing. The name must match the name of the printer driver installed on the Windows application server **exactly**. Pay particular attention to the use of capitals and spaces. The `/opt/tarantella/etc/data/default.printerinfo.txt` file contains all the common printer driver names ordered by manufacturer. To avoid errors, copy and paste the driver name from this file.
- (Optional) To make a PDF printer the default printer for Windows applications, check the box for **Make PDF printer the default for Windows 2000/3** (the Universal PDF printer) or **Make PDF file printer the default for Windows 2000/3** (the Print to Local PDF File printer).

## Notes

- If you make a PDF printer the default printer for Windows applications and you have also configured Secure Global Desktop to only allow users to print to their default printer, users will see two printers in their Windows application: their default client printer and the PDF printer.
- If a PDF viewer is not [configured on client devices](#), the PDF printers will not be available in the Windows application session even if a PDF printer has been enabled.

## Changing the names of the PDF printers

The names of Secure Global Desktop PDF printers are configurable. You can amend these names:

- For the entire array by running the following commands:  
`tarantella config edit --printing-pdfprinter name (for Universal PDF)`  
`tarantella config edit --printing-pdfviewer name (for Print to Local PDF File)`
- For an organization, organizational unit or person object ([user-specific printing configuration](#) must be enabled) by running the following commands:  
`tarantella object edit --name object --pdfprinter name (for Universal PDF)`  
`tarantella object edit --name object --pdfviewer name (for Print to Local PDF File)`

## Checking the Ghostscript installation on the Secure Global Desktop host

Secure Global Desktop uses [Ghostscript](#) to convert print jobs into PDF files. To use PDF printing, Ghostscript **version 6.52 or later** must be installed on the Secure Global Desktop host. Your Ghostscript distribution must include the `ps2pdf` program.

When you install Secure Global Desktop, Setup automatically detects Ghostscript if it is installed in one of the following locations:

- `/usr/local/bin`
- `/usr/bin`
- `/opt/sfw/bin`
- `/bin`
- `/usr/sbin`
- `/sbin`
- `/usr/lbin`

If Ghostscript is installed in a different location, you must run the Secure Global Desktop printer installation script (`prtinstall.en.sh`) with the `--gsbindir` option to tell Secure Global Desktop where to find Ghostscript.

If Ghostscript is not installed on the Secure Global Desktop host, or your Ghostscript distribution does not include the `ps2pdf` program, you must install it and then run the Secure Global Desktop printer installation script.

## Configuring PDF viewers on client devices

To be able to use PDF printing, a PDF viewer must be installed on the client device.

### Windows client devices

On Windows client devices, Secure Global Desktop supports the [Adobe Reader](#) version 4.0 or later.

### UNIX, Linux and Mac OS X client devices

On UNIX, Linux and Mac OS X client devices, Secure Global Desktop supports the following PDF viewers by default:

Client Platform	Default PDF Viewer
Solaris OS on SPARC platforms	Adobe Reader ( <code>acroread</code> )

Solaris OS on x86 platforms	GNOME PDF Viewer ( <code>gpdf</code> )
Linux	GNOME PDF Viewer ( <code>gpdf</code> )
Mac OS X	Preview.app

To be able to use a default PDF viewer, the application must be on the user's `PATH`.

If an alternative PDF viewer is preferred, the command for the alternative viewer application can be configured in the user's [client profile](#). In the profile you enter either the command or the full path to the command, depending on whether the application is on the user's `PATH`.

## How to use PDF printing

From a Windows application, you print in the normal way and select either the Universal PDF or the Print to Local PDF File printer in the application's Print dialog.

From an application running on a UNIX or Linux application server, you print in the normal way using the Secure Global Desktop replacement `lp` or `lpr` scripts. You select a PDF printer as part of the print command, for example:

```
/opt/tarantella/bin/lp -d "Universal PDF" filename  
/opt/tarantella/bin/lpr -P "Print to Local PDF File" filename
```

**Note** The *filename* **must** be a PostScript file, so the application must be able to output PostScript.

On Windows client devices, the PDF file is displayed in the Adobe Reader.

- If the Universal PDF printer was selected, the PDF file is printed automatically to the user's default printer. The Adobe Reader runs minimized and does not exit when the print job has finished.
- If the Print to Local PDF File printer was selected, the PDF file is displayed in the Adobe Reader window. The user can then decide whether to print or save the file.

On UNIX, Linux and Mac OS X client devices, the PDF file is displayed either in the default PDF viewer or in the PDF viewer configured in the client profile. The user can then decide whether to print or save the PDF file. There is no difference between the Universal PDF and the Print to Local PDF File printers as the print job is always displayed in a PDF viewer.

### Related topics

- Printing properties (array-wide)
- Introducing Secure Global Desktop printing
- Printing from a Microsoft Windows 2000/2003 application server
- Printing from a UNIX or Linux application server
- The prtinstall.en.sh script
- Users cannot print from applications displayed through Secure Global Desktop

## The prtinstall.en.sh script

### Syntax

```
sh prtinstall.en.sh [--appprinter printer_name]  
                    [--cups y | n | auto]  
                    [--gsbindir gs_bin_dir]  
                    [--help]  
                    [--nocheck]  
                    [--ttahost host_name]  
                    [--ttaprinter printer_name]  
                    [--uninstall [printer_name]]  
                    [--xrlp_protocol]
```

### Description

Installs a Secure Global Desktop printer on the host on which it is run. It also installs the Secure Global Desktop replacement `lp` or `lpr` scripts.

Location: `/opt/tarantella/bin/scripts`

You must be root to run this script.

Option	Description
<code>--appprinter <i>printer_name</i></code>	Use this option to specify a name for the printer you are installing on the application server. If you do not use this option, the printer will be created with the default name of <code>tta_printer</code> .

<code>--cups y   n   auto</code>	<p>Indicates that you are using the Common UNIX Printing System (CUPS).</p> <p>If you do not use this option, a default of <code>auto</code> is assumed and this means Secure Global Desktop tries to detect whether CUPS is being used. If CUPS is incorrectly detected, use this option to tell Secure Global Desktop whether CUPS is being used (<code>y</code>) or not (<code>n</code>).</p>
<code>--gsbindir gs_bin_dir</code>	<p>Use this option to specify the directory where the Ghostscript is installed.</p> <p>When you run the <code>prtinstall.en.sh</code> script, it checks for the Ghostscript executables in the following locations:</p> <ul style="list-style-type: none"><li>• <code>/usr/local/bin</code></li><li>• <code>/usr/bin</code></li><li>• <code>/opt/sfw/bin</code></li><li>• <code>/bin</code></li><li>• <code>/usr/sbin</code></li><li>• <code>/sbin</code></li><li>• <code>/usr/lbin</code></li></ul> <p>If Ghostscript is not installed in one of these locations, use this option to specify where it is installed.</p> <p>Ghostscript is used for <a href="#">PDF printing</a> and for <a href="#">converting the format of print jobs</a>.</p>
<code>--help</code>	<p>Shows the list of <code>prtinstall.en.sh</code> commands.</p>
<code>--nocheck</code>	<p>Installs the printer without checking the status of the Secure Global Desktop print administration commands.</p>
<code>--ttahost host_name</code>	<p>Fully qualified DNS name of a Secure Global Desktop server</p>
<code>--ttaprinter printer_name</code>	<p>Use this option to specify a name for the printer you are installing on the Secure Global Desktop host. If you do not use this option, the printer will be created with the default name of <code>tta_printer</code>.</p>

```
--uninstall [printer_name]
```

Uninstalls a Secure Global Desktop printer. If you do not specify a printer, you will be prompted for the name of the printer you want to uninstall.

## Examples

```
sh prtinstall.en.sh --appprinter tta_london
```

Installs a Secure Global Desktop printer called `tta_london` on an application server.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [The tarantella print command](#)
- [Printing from a UNIX or Linux application server](#)

## Users cannot print from applications displayed through Secure Global Desktop

Follow the checklists for the:

- [client device](#),
- [application server](#), and
- [Secure Global Desktop server](#).

If these do not resolve the problem, follow the steps in [Diagnosing other problems](#) below.

There is a separate troubleshooter for problems with Windows 2000/2003 [printer preferences and settings](#).

### Client devices

What to check	Description
Does Secure Global Desktop support printing for the client device or printer type?	<p>Check the Printing bar on the webtop, does the printer icon contain a red cross and does the message "No Client Printer Available" display. This means that Secure Global Desktop does not support printing for this client device or printer type or that there was an error creating client printers.</p> <p>Classic webtop users:</p> <ul style="list-style-type: none"><li>• If web browser users see a printer icon containing a red X, they should check the Java™ console for more information.</li><li>• If Sun Secure Global Desktop Native Client users do not see the "Ready to print" message in the status bar, they should select View log from the Webtop menu for more information.</li></ul>



<p>Is printing paused on the client device?</p>	<p>Make sure the user has not paused printing. Check the printer paused icon is not displayed.</p> <p>In <a href="#">Object Manager</a>, you can also use the Sessions tab on person objects, <a href="#">profile objects</a> or host objects to see whether the user has paused printing. Alternatively, use the <a href="#">tarantella webtopsession list</a> command.</p> <p>Classic webtop users:</p> <ul style="list-style-type: none"><li>• Web browser users should check they have not pressed the Pause button.</li><li>• Native Client users should check the status bar.</li></ul>
<p>Is the printer configured correctly?</p>	<p>Make sure that the printer is correctly configured, for example by printing a web page to the printer from a web browser on the client device. Depending on the application server, some print jobs can only go to the client device's default printer.</p> <p>If printing to a UNIX, Linux or Mac OS X client device, check that you have <a href="#">configured printing for these client types</a>.</p>
<p>If you are using PDF printing, is the PDF viewer installed on the client?</p>	<p>To be able to use Secure Global Desktop <a href="#">PDF printing</a>, a PDF viewer must be installed on the client device.</p> <p>Check that the <a href="#">supported viewer or the user's preferred viewer is installed on the client</a>.</p> <p>If it is not installed, the Secure Global Desktop PDF printers will not be available to the user even if PDF printing has been enabled.</p>
<p>Does the user have the necessary registry permissions?</p>	<p>On Windows client devices, users must have write access to the <code>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG\Seed</code> registry key and read access to the rest of the registry.</p> <p>This access is required by several of the Windows APIs for printing.</p>

## Application servers

What to check	Description
Is a printer configured on the application server?	<p>Before users can print, you may need to configure a Secure Global Desktop printer on your application servers:</p> <ul style="list-style-type: none"><li>• <a href="#">UNIX or Linux application server</a></li><li>• <a href="#">Windows 2000/2003 application server</a></li><li>• <a href="#">Windows NT 4 applications server</a></li><li>• <a href="#">Windows NT 3.51 applications server</a></li></ul>
Is the printer being created on the Windows 2000/2003 application server?	<p>If the user is trying to <a href="#">print from a Windows 2000/2003 application server</a> (accessed using Windows Terminal Services) and the user's printers should be configured automatically. If they are not, check the System event log on the application server for the following errors:</p> <ul style="list-style-type: none"><li>• Event ID: 1111 Description: Driver <i>drivertype</i> required for printer <i>printertype</i> is unknown. Contact the administrator to install the driver before you log in again.</li><li>• Event ID: 1105 Description: Printer security information for the <i>printername / clientcomputername /Session number</i> could not be set</li><li>• Event ID: 1106 Description: The printer could not be installed.</li></ul> <p>These errors indicate that the printer driver may not be supported by the application server. Either install the printer driver on the application server or see <a href="#">Printing from a Windows 2000/2003 application server</a> for details on how to support other printer drivers, including using wildcards to support a wide range of printer driver names.</p> <p>It is also worth checking that the name of the printer driver in the <code>default.printerinfo.txt</code> (or the user's <code>\$HOME/.tarantella/printerinfo.txt</code>) matches the name of the driver on the application server.</p> <p>If this does not resolve the problem, see the <a href="#">Microsoft Knowledge Base</a></p>

	<p><a href="#">article Q239088</a> for more details.</p>
Is the application printing to the correct printer?	<ul style="list-style-type: none"><li>• The application must print to the printer you've defined. On UNIX/Linux, the <code>prtinstall.en.sh</code> script creates a printer named <code>tta_printer</code> by default.</li><li>• On UNIX/Linux, the application should print using the replacement <code>lp</code> or <code>lpr</code> scripts installed by <code>prtinstall.en.sh</code>. The Secure Global Desktop <a href="#">login scripts</a> set <code>PATH</code> to ensure that the replacement scripts take precedence over the system scripts. If the application uses a full pathname, for example <code>/usr/bin/lp</code>, or modifies <code>PATH</code> itself, you should reconfigure the application to use <code>/opt/tarantella/bin/lp</code> or <code>/opt/tarantella/bin/lpr</code>.</li></ul>
Are accounts shared on the application server?	<p>If more than one user is simultaneously logged in to the same application server with the same username, Secure Global Desktop may be unable to distinguish which user owns the print jobs, and discards them (logging that it has done so). This occurs with UNIX/Linux application servers on which the <code>prtinstall.en.sh</code> script <b>has not</b> been run. To fix, run the <code>prtinstall.en.sh</code> script to configure a printer.</p> <p>Use the <code>tarantella print</code> command to check that print jobs from the application server printing system have reached the Secure Global Desktop print queue.</p>
Is the Windows name of the server the same as the DNS name?	<p>If you have a Windows NT server with a DNS name of <code>naples.indigo-insurance.com</code> and a NetBIOS name of <code>VESUVIUS</code>, print jobs from this server will fail because they contain the host identifier <code>VESUVIUS</code> instead of <code>naples</code>.</p> <p>You can avoid this problem by editing the file <code>hostnamemap.txt</code> in the <code>/opt/tarantella/etc/data</code> directory. This file allows you to map host names to DNS names. The file contains instructions on how to create the mappings.</p>

<p>If you're using Secure Global Desktop PDF printing, has the same PostScript printer driver been installed on every Windows 2000/2003 application server?</p>	<p>To be able to use Secure Global Desktop <a href="#">PDF printing</a>, you must install the same PostScript printer driver on every Windows 2000/2003 application server. Check that the name of the driver matches the name you typed in the Driver name field on the <a href="#">Array properties</a> panel. The System event log on the application server will show an error if the names do not match.</p>
---	---

## Secure Global Desktop servers

What to check	Description
<p>Is printing paused or disabled across the array?</p>	<p>Use the <code>tarantella print status</code> command to check whether printing is paused or disabled for the array. If necessary, enable printing using <code>tarantella print start</code> or <code>tarantella print resume</code>.</p>
<p>Has the array configuration changed?</p>	<p>Printers are not re-configured when you:</p> <ul style="list-style-type: none"> <li>• You create an array.</li> <li>• You add a new secondary server to the array.</li> <li>• You change the primary server in the array.</li> </ul> <p>If the array has changed you may to re-configure your printers so that print jobs are sent to the correct printer. Whether you have to re-configure or not, depends on <a href="#">the application server and the change made</a>.</p>
<p>Is Ghostscript available on the Secure Global Desktop host?</p>	<p>Secure Global Desktop <a href="#">PDF printing</a> uses Ghostscript to convert print jobs into PDF files. Secure Global Desktop also uses Ghostscript to convert print jobs from PostScript to PCL.</p> <p>If the <code>/opt/tarantella/var/log/print.log</code> contains a message like "can't find ps2pdf" or "Consider obtaining Ghostscript from <a href="http://www.ghostscript.com">http://www.ghostscript.com</a>", either Ghostscript is not installed or it is installed in a non-standard location.</p> <p>When you install Secure Global Desktop, Secure Global Desktop Setup automatically detects Ghostscript if it is</p>

installed in one of the following locations:

- `/usr/local/bin`
- `/usr/bin`
- `/opt/sfw/bin`
- `/bin`
- `/usr/sbin`
- `/sbin`
- `/usr/sbin`

If Ghostscript is installed elsewhere, you must run the `prtinstall.en.sh` script with the `--gsbindir` option to tell Secure Global Desktop where to find Ghostscript.

If Ghostscript is not installed, you must install it and then run the `prtinstall.en.sh` script.

## Diagnosing other problems

If the checklists above do not solve the problem, follow these steps.

### 1. Can you print from the Secure Global Desktop server?

Configure an X or character application to run on the Secure Global Desktop server and display a shell window (for example `xterm`), and start it from your webtop. Try printing a test page, by running `/opt/tarantella/bin/scripts/printtestpage.en.sh`. If the page does not print, try `/opt/tarantella/bin/scripts/printtestpage.en.sh --direct` instead, which bypasses the UNIX/Linux spooler.

What to check	Description
If the first test page prints	The problem is related to the movement of print jobs from the application server to the Secure Global Desktop server. For UNIX/Linux application servers, go to step 3. For Windows Terminal Services, go to step 5.

If the second test page prints	The problem is related to the UNIX/Linux printing system on the host on which Secure Global Desktop is installed. Investigate and fix any problems, using your UNIX/Linux system documentation for help. Then try printing again.
If neither test page prints	The problem is related to the Secure Global Desktop server. Go to step 2.

## 2. Is the Secure Global Desktop printer installed on the Secure Global Desktop server?

In the list of printers on the host, you should see an entry for `tta_printer`. Consult your UNIX/Linux documentation to find out how to display the list of printers. On some systems, this is `lpstat -t`. If your system has a file `/etc/printcap`, this contains a list of printers in plain text format.

What to check	Description
If <code>tta_printer</code> is present	The problem is related to the movement of print jobs from the Secure Global Desktop server to the client device. Go to step 7.
If <code>tta_printer</code> is not present	Run the <code>prtinstall.en.sh</code> script on the Secure Global Desktop server. Then try printing again.

## 3. Is the print job leaving the UNIX/Linux application server?

Using an application object configured to display a shell window on the UNIX/Linux application server, try printing a small text file to the Secure Global Desktop printer. For example, type `lp -d tta_printer /etc/hosts`.

What to check	Description
If the <code>lp</code> command returns an error message	Check that the UNIX/Linux server is configured to print through Secure Global Desktop. You may need to run the <code>prtinstall.en.sh</code> script.
If the <code>lp</code> command returns a print job ID	This suggests that Secure Global Desktop printing is correctly configured, but the problem may lie in the UNIX/Linux system. Go to step 4.

## 4. Is the print job present in the UNIX/Linux spool directory?

The print spool directory varies between different UNIX/Linux systems. Consult your UNIX/Linux system

documentation for assistance.

What to check	Description
If the job is present	There may be a network problem between the application server and Secure Global Desktop server. Go to step 6.
If the job is not present	Check your UNIX/Linux LPD printing configuration. For example, ensure that there are suitable entries in <code>/etc/hosts.equiv</code> or <code>/etc/hosts.lpd</code> , and that there are no deny files, such as <code>/etc/hosts.equiv.deny</code> . Check that the <code>lpd</code> daemon is running ( <code>ps -ef   grep lpd</code> on most systems -- check your system documentation for the correct arguments to the <code>ps</code> command) and listening ( <code>netstat -a   grep printer</code> ). Then try printing again.

## 5. Is the print job leaving the Windows Terminal Services application server?

Check the print queue on the application server. Consult your system documentation if you need help.

What to check	Description
If the print job is leaving the application server	There may be a network problem between the application server and Secure Global Desktop server. Go to step 6.
If the print job is not leaving the application server	<ul style="list-style-type: none"><li>• Check the configuration of the Secure Global Desktop printer.</li><li>• Check that you can ping and telnet to the Secure Global Desktop server from the application server.</li><li>• Look for errors in the Event Log.</li><li>• From a command prompt, try typing <code>lpr -s server -p tta_printer filename</code> to print. If this works, this suggests the printer driver on the application server is not installed or configured correctly.</li></ul>

## 6. Is the print job reaching the Secure Global Desktop server?

Check the Secure Global Desktop print spool directories on the Secure Global Desktop server: `/opt/tarantella/var/spool` and `/opt/tarantella/var/print/queue`.

What to check	Description
---------------	-------------

If the print job is present	<ul style="list-style-type: none"> <li>• Check that you're using fully qualified DNS names in the application object, and that name resolution is working correctly.</li> <li>• Examine the printing log files for more information. Go to step 7.</li> </ul>
If the print job is not present	<ul style="list-style-type: none"> <li>• Check your UNIX/Linux LPD printing configuration. For example, ensure that there are suitable entries in <code>/etc/hosts.equiv</code> or <code>/etc/hosts.lpd</code>, and that there are no deny files, such as <code>/etc/hosts.equiv.deny</code>.</li> <li>• Check that the lpd daemon is running (<code>ps -ef   grep lpd</code>) and listening (<code>netstat -t   grep lpd</code>).</li> <li>• Check that you can ping and telnet to the Secure Global Desktop server from the application server.</li> <li>• Windows Terminal Services: From a command prompt, try typing <code>lpr -s server -p tta_printer filename</code> to print. If this works, this suggests the printer driver on the application server is not installed or configured correctly.</li> </ul>

## 7. Examine the print log files

You can use the `tarantella query` command to examine the logs across the array. Log files are stored in `/opt/tarantella/var/log` on each array member.

If the print log files are empty, you need to edit the Log Filter to log printing messages. In Array Manager, display the Array properties panel and add the following log filters:

```
server/printing/*:print%%PID%%.log
server/printing/*:print%%PID%%.jsl
```

If the log contains messages indicating problems with username mappings, this suggests you may be using shared accounts on the application server. See [Are accounts shared on the application server?](#) above.

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [The tarantella print command](#)





## Troubleshooting printer preferences and settings

When printing from a Windows application that uses the Microsoft RDP [Windows Protocol](#), users can set preferences for the printers they use. Use this page to help resolve problems with printer preferences.

Select the section that best matches the user's symptoms:

- [Current client printer preferences ignored.](#)
- [Changes to printer preferences are not remembered.](#)
- [Printer preferences get lost when a user changes printers.](#)
- [Local printer settings are not set in a remote Windows session.](#)
- [Printer settings are ignored when using PDF printing.](#)

### Current client printer preferences ignored

The first time a client printer is defined for a user, the printer preferences (for example, the paper size and orientation) are the application server's defaults for the printer driver and not the client printer's current preferences.

Users can change the printer preferences on the application server, and these modified preferences are used when they next connect using a client device with the same printer.

### Changes to printer preferences are not remembered

When a user changes their printer preferences, for example by changing the default paper size, sometimes the change is not remembered when they next run a Windows application.

There is a delay between changing the preferences and the new preferences being sent to the client. When changing printer preferences, it is advisable to wait a few minutes before logging out of the Windows application.

### Printer preferences get lost when a user changes printers

Printer preferences are linked directly to the driver name. So if a user changes the printer they use and the new printer uses a different driver name, they have to set the printer preferences again.

### Local printer settings are not set in a remote Windows application

The printer settings of a local printer are not set on the printer in the remote Windows application when you use Secure Global Desktop. However, they are set when you use the Microsoft Terminal Services Client.

Secure Global Desktop does not support this capability.

## **Printer settings are ignored when using PDF printing**

If you are using [Secure Global Desktop PDF printing](#) on a Windows client, some printer settings may be ignored by the Adobe Reader.

This may be because the printer driver used for PDF printing has settings which are not available on the client printer.

Some settings, such as page orientation, have to be set in the Adobe Reader print dialog as well as on the printer in the Windows application session. Once you have set up the Reader, the settings are remembered.

### **Related topics**

- [Introducing Secure Global Desktop printing](#)
- [Users cannot print from applications displayed through Secure Global Desktop](#)

## With Secure Global Desktop PDF printing, fonts don't print as expected

When using Secure Global Desktop PDF printing, users may find that the fonts on the printed output are not what they expected. As PDF printing relies on a combination of Windows printer drivers (when printing from Windows applications), Ghostscript and a PDF viewer to deliver its output, you may have to experiment with the font settings for each of these components to see if this produces a better result.

### TrueType fonts and Windows applications

When printing from a Windows application and the document contains TrueType fonts, users may find that the printer is using its own fonts (device fonts) instead of the TrueType fonts and this can result in some characters being printed as "empty boxes" ( ). The solution to this is to force the printer download the TrueType fonts for printing. To do this:

1. In the Print dialog in the Windows application, click Properties.
2. Click Advanced.
3. Under Graphic settings, change the TrueType Font option to Download as Softfont.
4. Click OK and print.

#### Related topics

- [Configuring Secure Global Desktop PDF printing](#)
- [Users cannot print from applications displayed through Secure Global Desktop](#)
- [Troubleshooting printer preferences and settings](#)

## Can I set a time limit for print jobs?

Yes. Secure Global Desktop Administrators can set a time limit on how long a print request can remain on the Secure Global Desktop server before it gets deleted. This is useful if you have to manage a high volume of printing.

To specify the number of hours that print jobs remain on the server, run the following command:

```
tarantella config edit --tarantella-config-array-printjoblifetime hours
```

To return Secure Global Desktop to its default behavior so that print jobs remain on the server indefinitely, run the following command:

```
tarantella config edit --tarantella-config-array-printjoblifetime 0
```

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [The tarantella print move command](#)
- [The tarantella print cancel command](#)

[Secure Global Desktop Administration Guide](#) > [Printing](#) > Why do users see a printer called `_Default` in their Windows application?

## Why do users see a printer called `Default` in their Windows application?

Users, who access Windows applications using a UNIX, Linux or Mac OS X client, may see a printer called `_Default` created in their Windows application session. This can be confusing to users if their client printer has a different name or they have no client printer.

This is caused by the default setting in [the `printerinfo.txt` file](#) which is used to associate the printer driver name with a print job when printing from a Windows application.

### Correcting the printer name

To change the printer so that it shows the name of the printer the user actually has, you need to either of the following:

- Edit the global `/opt/tarantella/etc/data/default.printerinfo.txt` file (affects all users).
- Edit the user's `$HOME/.tarantella/printerinfo.txt` file (affects just this user).

**Note** The user's `printerinfo.txt` takes precedence over the settings in the `default.printerinfo.txt`.

Edit the `[UNIX]` section of this file so that it shows the correct printer name, Windows printer driver name and printer type, for example:

```
"salesprinter" = "HP LaserJet 5/5M" PostScript
```

**Note** To ensure you have the correct driver name, search for it in the `default.printerinfo.txt` file. This file contains all the common driver names. To avoid errors, such as incorrect capitalization, copy and paste the driver name from this file.

### Removing the `Default` printer completely

If users have no printers attached to their client device, you can prevent the `_Default` printer from appearing in the Windows application by removing the `[UNIX]` section from:

- The global `/opt/tarantella/etc/data/default.printerinfo.txt` file (affects all users).
- The user's `$HOME/.tarantella/printerinfo.txt` file (affects just this user).

## Related topics

- [Configuring printing for UNIX, Linux and Mac OS X clients](#)
- [Printing from a Microsoft Windows 2000/2003 application server](#)

## Do I have to use distributed printing?

No. You can direct all your print jobs through the primary Secure Global Desktop server in the array.

**Note** This is not recommended because if the primary fails, printing services fail.

How you configure printing through only the primary Secure Global Desktop server depends on the application server type.

### UNIX and Linux application servers

To set up printing through the primary Secure Global Desktop server, you must [install](#) a single printer on the application server, using the `--ttahost` option to specify the DNS name of the primary server. If you have installed printers for the other members of the array, you must [uninstall](#) them.

### Windows application servers

To set up printing through only the primary server, you must edit the `wcpwts.exp` [login script](#) so that it sets the following for the `ttatssc` program:

- A `-printcommand lp` or a `-printcommand lpr` argument.
- An `LPDEST` environment variable which sets the name of the Secure Global Desktop printer on the primary Secure Global Desktop server (by default, this is `tta_printer`).

For example:

```
if [catch {exec -- echo $TTATSC1 | env LPDEST=tta_printer $ProtocolCmd "-
stdin" "-printcommand" "lp"
```

### Related topics

- [Introducing Secure Global Desktop printing](#)
- [Users cannot print from applications displayed through Secure Global Desktop](#)





## If the array changes, do I have to re-configure printing?

When you make changes to an array of Secure Global Desktop servers, printers are not reconfigured and so print jobs may be wrongly directed. When you make an array change, a warning message displays advising you that you may have re-configure your printers manually. The warning displays when:

- You create an array.
- You add a new secondary server to the array.
- You change the primary server in the array.

Whether you have to re-configure or not, depends on the application server and the change made:

<b>Application server type</b>	<b>New array</b>	<b>New primary</b>	<b>New secondary</b>
UNIX	No	No	Yes
Windows 2000/2003	No	No	No
Windows NT 4	Yes	Yes	No
Windows NT 3.51	Yes	Yes	No

If you add a new secondary Secure Global Desktop server, you must install a new printer on your UNIX/Linux application servers for the new secondary.

If you create an array or change the primary Secure Global Desktop server in an array, you must re-configure the printers on your Windows NT 4 and NT 3.51 application servers so that they 'point to' the new primary server.

To re-configure a printer, see:

- [UNIX application server](#)
- [Windows NT 4 application server](#)
- [Windows NT 3.51 application server](#)

## Related topics

- [Introducing Secure Global Desktop printing](#)
- [Users cannot print from applications displayed through Secure Global Desktop](#)

## Can I change the name of the printer in the Windows 2000/2003 application session?

Yes and no. When printers are created in a:

- Windows 2000 session they have the format "*printer\_name*/Tarantella/Session *number*", for example:  
`HP LaserJet 8000 Series PS/Tarantella/Session 1`
- Windows 2003 session they have the format "*printer\_name* (from Tarantella) in session *number*", for example:  
`HP LaserJet 8000 Series PS (from Tarantella) in session 1`

For Unix, Linux and Mac OS X clients, the *printer\_name* comes from the [printer configuration file for these clients](#). For Windows clients, the name comes from the printer driver.

You can change the "Tarantella" part of the printer name by editing the `/opt/tarantella/var/serverresources/expect/wcpwts.exp` [login script](#). By adding a `-netbiosname "name"` argument for the `ttatsc` command, for example `-netbiosname "IndigoInsurance"`, you can change the name the printer name in the example above to:  
`HP LaserJet 8000 Series/PS/IndigoInsurance/Session 1`

**Note** The name can only be 15 characters long. If you use more than 15 characters, the name will be truncated.

If you are using Secure Global Desktop PDF printing, you can [amend the names of the PDF printers](#).

### Related topics

- [Printing from a Microsoft Windows 2000/2003 application server](#)

## Can I force users to print only to their default client printer?

Yes. Secure Global Desktop allows users to select which printer they print to. This may not always be desirable.

To force users on **Windows platforms** to print only to their default client printer:

1. Either:
  - In Array Manager, click [Printing properties](#).
  - In Object Manager, select the Printing panel for an [organization](#), an [organizational unit](#) or a [person](#) object.

**Note** The settings in Array Manager affect all users. The settings in Object Manager affect individual users.

2. From the Printing list, select Let users print to client's default printer.
3. Click Apply. The change only takes effect for new webtop sessions.

To force users on **UNIX, Linux and Mac OS X platforms** to print only to their default client printer, there must only be one entry in the [UNIX] section of either the global `/opt/tarantella/etc/data/default.printerinfo.txt` file or the user-specific `$HOME/.tarantella/printerinfo.txt` file. The default printer is the first printer listed in these files.

If users want to change their default printer so they can print to a different printer, they have to log out of Secure Global Desktop, change the default printer and then log in to Secure Global Desktop again.

### Related topics

- [Array properties \(array-wide\)](#)
- [Printing from a UNIX or Linux application server](#)
- [Printing from a Microsoft Windows 2000/2003 application server](#)
- [Users cannot print from applications displayed through Secure Global Desktop](#)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

[Secure Global Desktop Administration Guide](#) > [Printing](#) > When Secure Global Desktop printing has been disabled, print jobs can still be queued

## When Secure Global Desktop printing has been disabled, print jobs can still be queued

After disabling the Secure Global Desktop print system by running `tarantella print stop`, it is still possible to spool print jobs on application servers. These jobs will remain queued until Secure Global Desktop printing is restarted.

To prevent these print jobs from being submitted, the Secure Global Desktop print queue on the application servers must be manually disabled.

### Related topics

- [The tarantella print stop command](#)

## Windows 2000 users are unable to print a file from a mapped network drive

Users running applications on a Windows 2000 Server may find that they are unable to print a file if the document that is being printed is opened from a mapped network drive.

Windows 2000 SP3 introduced a fault that causes printing from a mapped network drive to fail when using Windows Terminal Services. See the [Knowledge Base Article Q328020](#) for details.

The solution is one of the following:

- Copy the file on to the application server and print it from there.
- Obtain the fix from Microsoft.
- Install the latest service pack(s) on the Windows 2000 Server.

### Related topics

- [Users cannot print from applications displayed through Secure Global Desktop](#)



## How do I use my own X fonts?

There are two ways to make your own X fonts available through Secure Global Desktop:

- Copy your fonts in `.pcf` format to a directory on each [array member](#), including a `fonts.dir` file mapping filenames to X logical font descriptions, and then [modify the X Protocol Engine's Font Path](#) on each array member to include that directory. Fonts may be compressed or gzipped.
- Configure a [font server](#) on your network, and [modify the X Protocol Engine's Font Path](#) on each array member to include the location of the font server.

Each array member's X Protocol Engine may use a different font path. However, to avoid inconsistent display of applications, you should ensure the same fonts (in the same order) are available to all X Protocol Engines.

For a new font path to take effect, restart the Secure Global Desktop server on each array member.

After restarting a Secure Global Desktop server, you can check the validity of a font path by starting an xterm (or other graphical terminal) through Secure Global Desktop and then using the command `xset q`.

### The `fonts.dir` file

A font directory must include a `fonts.dir` file, mapping font filenames to X logical font descriptions. An example line from a `fonts.dir` file is:

```
COURBO10.pcf -Adobe-Courier-Bold-0-Normal-10-100-75-75-M-60-ISO8859-1
```

If your font directory doesn't include a `fonts.dir` file, you can use a program such as `mkfontdir` (available for most UNIX systems) to create one.

You may also include a `fonts.alias` file, which specifies aliases for the fonts in the directory. This file maps aliases to X logical font descriptions. For example:

```
variable *-helvetica-bold-r-normal-*-*-140-*
```

### Font servers

A font server is a program that makes fonts on a host available on the network. Font servers make font administration easier by centralizing fonts, reducing duplication.

To name a font server in a font path, you need to know the name of the font server and the port on which fonts are being served. For example, if the font server boston uses port 7000/tcp, add the font path entry `tcp/boston:7000`.

### Related topics

- [X Protocol Engine properties \(server-specific\)](#)
- [The tarantella config command](#)
- [What X fonts are installed?](#)
- [Euro Character \(--euro\)](#)

## Terminal emulator attribute maps

Terminal emulator attribute maps let you change how character attributes such as bold or underline are displayed in the Secure Global Desktop terminal emulators. For example, you can specify that text that normally appears bold and underlined appears red in the Secure Global Desktop terminal emulators (but not red *and* bold and underlined).

Secure Global Desktop provides a default attribute map `/opt/tarantella/etc/data/attrmap.txt`. This maps character attributes to the logical color `Color_15` (white). You can also create your own attribute map.

### Creating your own attribute map

To create your own attribute map:

- As root, create a copy of `/opt/tarantella/etc/data/attrmap.txt` to work on.
- Edit the new file so that character attributes map to your chosen colors.
- Type the name of the file in the application object's **Attribute Map** attribute.

### How you edit character attributes

The Secure Global Desktop attribute maps let you map the following attributes:

- Normal
- Bold
- Dim
- Blinking
- Underline
- Inverse

To map combinations of attributes, separate the attributes with the plus sign `+`, for example `Bold+Underline`.

To display colors in the terminal emulators, Secure Global Desktop maps logical colors to RGB values. For example, the logical color `Color_9` maps to the RGB value `128 0 0` (red).

When mapping attributes to colors in your attribute map, specify the logical color name. For example, to change:

- bold underlined text to red text:

```
Bold+Underline=Color_9
```

- inverse blinking text to light red text:

```
Inverse+Blinking=Color_1
```

For a complete list of logical color to RGB value mappings, refer to the comments in `attrmap.txt`.

You can change the default color mappings by editing the [color map](#) used by the terminal emulators.

**Note** Wyse 60 terminals are black and white. However, you can use the Secure Global Desktop Wyse 60 terminal emulator to display colors in your Wyse 60 applications. You can do this by using the attribute map to map character attributes in the Wyse 60 application to colors.

### Related topics

- [Terminal emulator color maps](#)
- [Terminal emulator keyboard maps](#)
- [Attribute Map \(--attributemap\)](#)

## Terminal emulator color maps

SCO Console (ANSI) and VT420 terminals support 16 colors. The Secure Global Desktop terminal emulator uses a color map to determine how these colors are presented in an emulator session.

**Note** Wyse 60 terminals are monochrome. You can only switch the background and foreground colors (black and white) using the color map. However, you can map [character attributes](#) such as bold or underline to any of the 16 logical colors supported by the terminal emulator.

The color map maps the logical colors `Color_0` through to `Color_15` (inclusive) to colors and the RGB values that Secure Global Desktop uses to represent those colors. The default mappings are as follows:

Logical color	Terminal color	RGB value used by Secure Global Desktop
Color_0	Black	0 0 0
Color_1	Light red	255 0 0
Color_2	Light green	0 255 0
Color_3	Yellow	255 255 0
Color_4	Light blue	0 0 255
Color_5	Light magenta	255 0 255
Color_6	Light cyan	0 255 255
Color_7	High white	255 255 255
Color_8	Gray	128 128 128
Color_9	Red	128 0 0
Color_10	Green	0 128 0
Color_11	Brown	128 128 0
Color_12	Blue	0 0 128

Color_13	Magenta	128 0 128
Color_14	Cyan	0 128 128
Color_15	White	192 192 192

To alter the defaults for a particular application, create your own color map and specify it in the application object's [Color Map](#) attribute.

A default text-format color map `/opt/tarantella/etc/data/colormap.txt` is provided.

## Examples

For example, you might want to make the color red brighter. To do this, you would change the RGB setting of `Color_9` to `192 0 0`.

Or, if you wanted items that appear in light green to appear yellow, you would change the RGB setting of `Color_2` to `255 255 0` (the RGB value of yellow).

One common color change is to switch the foreground and background colors between black and white. When you do this, you are not changing the foreground or background color as such -- you're changing the way black (`Color_0`) and white (`Color_15`) are displayed. Therefore, if your application has a white background and you want to change it to a black background, you would change the value of `Color_15` to `0 0 0` (the RGB value of black).

### Related topics

- [Terminal emulator attribute maps](#)
- [Terminal emulator keyboard maps](#)
- [Color Map \(--colormap\)](#)

## Terminal emulator keyboard maps

The Secure Global Desktop terminal emulators associate keys on the user's client keyboard with keys found on a real terminal. For each type of terminal emulator (SCO Console, Wyse 60 and VT420) there is a default keyboard mapping.

To change the default mappings or define additional mappings for a particular application, you can specify your own keyboard map file using an object's [Keyboard Map](#) attribute.

### Default mappings

The emulators have built-in keyboard maps, which are equivalent to those found in the sample keymap files in `/opt/tarantella/etc/data/keymaps`.

- `anskey.txt` for the SCO Console emulator.
- `vt420key.txt` for the VT420 emulator.
- `w60key.txt` for the Wyse 60 emulator.

**Note** Modifying these keyboard maps does not alter the default mappings used by Secure Global Desktop. The only way to do this is to specify a keyboard map in an application object's [Keyboard Map](#) attribute.

### Creating a keyboard map

To create your own keyboard map, you should make a copy of the relevant default keyboard map and modify it to suit your application. You can modify a keyboard map in any text editor.

The format of a mapping is:

```
ClientKeys=Translation
```

Where *ClientKeys* is the key(s) that the user presses on the client device, and *Translation* is the keystroke(s) sent to the application on the application server. For example:

```
PageDown=Next
```

With this mapping, when the user presses **Page Down** the emulator sends the keystroke **Next** to the application server.

If a particular key has a user-defined mapping, the default settings will be overridden. If no user-defined mapping is present, the default mapping is sent.

You can send complete strings on a single keypress by surrounding the string in double-quotes. For example:

```
F1="hello world"
```

To enter non-printable characters when mapping strings, use the code shown in the table below:

Code	Meaning
r	Carriage return
n	Line feed
"	Double-quote
e	Escape
t	Tab
<i>nnn</i>	The character with octal value <i>nnn</i>
<i>xHH</i>	The character with hex value <i>HH</i>

To specify modifier keys (Shift, Control and Alt) in a mapping, separate the keys with the plus sign, +. For example:

```
Shift+NUMLOCK=INSLINE  
Shift+F1="\0330a"  
Alt+Shift+Control+DELETE="\003[33~"
```

## Key names

The following tables contain lists of key names that are valid in Secure Global Desktop keyboard maps. The first table shows the key names that represent keys on the user's client device. These are the keys that can be mapped to the emulator key names given in the subsequent tables, which are the keystrokes ultimately sent to the application on the application server.



**Note** The default mappings between these key names are as found in the keyboard maps supplied with Secure Global Desktop. If a key is not in a keyboard map, then it is not mapped.

### **Client device keys**

- CURSOR\_DOWN
- CURSOR\_LEFT
- CURSOR\_RIGHT
- CURSOR\_UP
- DELETE
- END
- F1 to F12
- HOME
- INSERT
- KP0 to KP9
- KPADD
- KPDELETE
- KPDIVIDE
- KPENTER
- KPMULTIPLY
- KPSUBSTRACT
- NUMLOCK
- PAGEDOWN
- PAGEUP

### **Application server keystrokes**

SCO Console:

- CURSOR\_DOWN
- CURSOR\_LEFT
- CURSOR\_RIGHT
- CURSOR\_UP
- DELETE
- END
- F1 to F12
- HOME
- INSERT
- KP0 to KP9

- KPADD
- KPDIVIDE
- KPDOT
- KPMULTIPLY
- KPSUBSTRACT
- NUMLOCK
- PAGEDOWN
- PAGEUP

VT420:

- CURSOR\_DOWN
- CURSOR\_LEFT
- CURSOR\_RIGHT
- CURSOR\_UP
- F1 to F20
- FIND
- INSERT
- KP0 to KP9
- KPCOMMA
- KPDOT
- KPENTER
- KPMINUS
- NEXT
- PF1 to PF4
- PREV
- REMOVE
- SELECT

Wyse 60:

- CLRLINE
- CLRSCR
- CURSOR\_DOWN
- CURSOR\_LEFT
- CURSOR\_RIGHT
- CURSOR\_UP
- DELCHAR

- DELETE
- DELLINE
- F1 to F16
- HOME
- INSCCHAR
- INSERT
- INSLINE
- KP0 to KP9
- KPCOMMA
- KPDELETE
- KPENTER
- KPMINUS
- NEXT
- PREV
- PRINT
- REPLACE
- SEND
- SHIFTHOME

#### Related topics

- [Terminal emulator attribute maps](#)
- [Terminal emulator color maps](#)
- [Keyboard Map \(--keymap\)](#)

## What are login scripts?

When a user clicks an application object on their webtop, a *login script* connects to the application server and runs the application. The login script also configures the environment and starts any additional programs (such as a window manager).

Login scripts perform a number of tasks and can handle a number of scenarios. For example, when a user clicks a link to an X application object on their webtop, the login script does the following:

- Logs into the application server, prompting the user for a password if necessary.
- Sets any environment variables specified by the application object's [Environment Variables](#) attribute.
- Starts any extra programs specified by the application object's [Window Manager](#) attribute.
- Launches the X application.

The login script also allows for differences between application servers and checks for any errors that might occur during the login process. If an error is encountered that can't be handled, control is passed back to the user.

Login scripts are designed to be as universal and robust as possible. However, you may need to cope with an unusual scenario. For example, if you have a system prompt that isn't catered for, you can add it to the list of prompts recognized by the script. You shouldn't modify the scripts supplied: instead, work on a copy.

To define the login script used for an application, you use the application object's [Login Script](#) attribute.

Secure Global Desktop login scripts are written in Tcl (version 7.5) and Expect (version 5.25). Expect (developed by Don Libes) extends Tcl (developed by John Ousterhout) and provides additional commands for interacting with programs.

- For more information about Tcl, see [TCL Developer Xchange](#).
- For more information about Expect, see [The Expect Home Page](#).

### Related topics

- Login scripts supplied with Secure Global Desktop
- Login Script (--login)

## Increasing launch timeouts

If you're running applications on a particularly sluggish application server, Secure Global Desktop may fail to start applications, reporting an `ErrApplicationServerTimeout` error.

You can fix this by increasing the launch timeouts in the `vars.exp` [login script](#).

For a slow machine, we recommend that `timeouts(loggedin)` is increased. If the launch fails with `ErrApplicationServerTimeout`, one of the clienttimers is too short. If the launch is particularly slow, it may be better to increase all the clienttimers.

**Note** Changing the launch timeouts will slow down application start times, so only do this if you're experiencing problems, and tune the timeouts to the capabilities of the application server.

**Note** With the exception of the Execution Protocol Engine timeout, none of the timers discussed here is used when launching a Microsoft Windows application.

Launch timeout	Default value (seconds)
<code>timeouts(prelogin)</code>	40
<code>timeouts(loggedin)</code>	20
<code>timers(login)</code>	<code>timeouts(prelogin) + 10</code>
<code>timers(env)</code>	40
<code>timers(runmain)</code>	40
<code>timers(build)</code>	25
<code>timers(total)</code>	5

## Expect timeouts

If an expect timeout expires, the script will attempt to guess the prompt, then continue with the launch.

```
timeouts(prelogin)
```

The time allowed for each expect command to match a required string during the login phase.

For example, after the connection is made to the application server, the script has *prelogin* seconds to match the login prompt before it times out. Every successful match resets the timer. During a login, the prelogin timer will usually be reset for the login, password and shell prompts.

Increasing the prelogin timer will increase the time allowed for each phase of the login. It should be large enough so that the longest phase can be completed.

If the timeout expires, the script assumes that it is logged in and has failed to match the shell prompt and sends "echo SYNC" to the application server to guess the promptstring. If the user was not logged in when the timer fired, the launch will fail. Otherwise, the shell prompt will be set to whatever the application server sent immediately after the "echo SYNC" and the launch continues.

**Note** If you can see "echo SYNC" and the shell prompt ends in the normal way with \$ % # or >, the prelogin timer is too short.

`timeouts (loggedin)`

The time allowed for each expect command to match a required string once the user is logged in.

If the timeout expires, the script moves onto the next command, which may cause commands to be sent before the prompt has returned. The most common occurrence of this timeout is if the script incorrectly sets the shell prompt. This causes each command to wait *loggedin* seconds before moving to the next command and can trigger one of the clienttimers.

## clienttimers

clienttimers are set using the `clienttimer` command. If a clienttimer expires, the launch is aborted with a fatal `ErrApplicationServerTimeout` error.

`timers (login)`

The total time for the complete login phase, from making the connection to receiving the first shell prompt.

The login timer must be large enough to cover all of the login phases. Each individual phase (login prompt, password prompt, shell prompt) may last up to *prelogin* seconds, so *login* should always be greater than *prelogin*.

**Note** If you increase the prelogin timer, you should increase the login timer as well so that the difference between them is never less than 10.

`timers(env)`

The total time from receiving the first shell prompt until all of the application server environment variables have been exported.

`timers(runmain)`

The total time from setting the last environment variable to launching the main application.

`timers(build)`

The total time taken to build the command line to be executed. This timer is only used when launching Merge applications.

`timers(total)`

The total number of clienttimers. You should only change this setting if you add or remove a clienttimer.

## Other timeouts

The `procs.exp login script` includes a 3-second timeout when issuing commands (in `proc wait_for_prompt`).

A timeout of 3 minutes is hard-coded into the Execution Protocol Engine. This is started when the launch request is received and removed when the launch has successfully completed. If it expires, the launch is aborted.

### Related topics

- [An application won't start](#)
- [What are login scripts?](#)
- [Login scripts supplied with Secure Global Desktop](#)



## Login script Tcl commands

As well as using Expect, the login scripts supplied with Secure Global Desktop make use of several Tcl commands. For example, the [tarantella](#) command connects to the application server instead of Expect and provides greater control over the connection. In addition, other Tcl commands are used, described here.

You can use these Tcl commands in your own login scripts.

### authrequest

#### Syntax

```
authrequest [ -normal | -changed ]
```

#### Description

Displays a dialog box that indicates a problem with the username or password.

Argument	Description
-normal	Specifies that the password is incorrect.
-changed	Specifies that the password has expired.

#### Example

```
authrequest -normal
```

### setbuffer

#### Syntax

```
setbuffer [ -buffer num ] [ -output 0|1 ]
```

#### Description

Defines the number of bytes to read from the application server.

Argument	Description
<code>-buffer <i>num</i></code>	Specifies the number of bytes. Default is 1.
<code>-output 0 1</code>	Turns output on (1) or off (0). Default is 1.

### Example

```
setbuffer -buffer 1000
```

## clienttimer

### Syntax

```
clienttimer [ time ] [ message ] [ timers ]
```

### Description

Displays *message* in the progress dialog box for the specified *time*. The progress bar has *timers* sections in total.

### Example

```
clienttimer 10 "Launching the application" 4
```

## canceltimer

### Syntax

```
canceltimer
```

### Description

Cancels the `clienttimer` command. Takes no arguments.

## progress

### Syntax

```
progress [ message ]
```

## Description

Displays *message* in the progress dialog box.

## Example

```
progress "Initializing..."
```

## locallaunch

### Syntax

```
locallaunch [ -start ] [ -abort ] [ -user launchspec -root launchspec ]
```

## Description

Optimizes launch in the situation where the application server is also the Secure Global Desktop server.

Argument	Description								
<code>-start</code>	Starts an optimized launch.								
<code>-abort</code>	Aborts the optimized launch and reverts to the standard connection method.								
<code>-user <i>launchspec</i></code>	Defines the connection methods to use for launching applications on the Secure Global Desktop server when the user <b>is not</b> root. You can specify different behavior for applications that are detached on launch (background applications) and those that aren't (foreground applications). <table border="1"><thead><tr><th><i>launchspec</i></th><th>Description</th></tr></thead><tbody><tr><td>0</td><td>Launches all applications using the Connection Method defined for the application object.</td></tr><tr><td>1</td><td>Background applications use <code>/bin/su</code>. Foreground applications use the application object's Connection Method.</td></tr><tr><td>2</td><td>Background applications use the application object's Connection Method. Foreground applications use <code>/bin/su</code>.</td></tr></tbody></table>	<i>launchspec</i>	Description	0	Launches all applications using the Connection Method defined for the application object.	1	Background applications use <code>/bin/su</code> . Foreground applications use the application object's Connection Method.	2	Background applications use the application object's Connection Method. Foreground applications use <code>/bin/su</code> .
<i>launchspec</i>	Description								
0	Launches all applications using the Connection Method defined for the application object.								
1	Background applications use <code>/bin/su</code> . Foreground applications use the application object's Connection Method.								
2	Background applications use the application object's Connection Method. Foreground applications use <code>/bin/su</code> .								

	3	Launches all applications using /bin/su.																		
<code>-root launchspec</code>	<p>Defines the connection methods to use for launching applications on the Secure Global Desktop server when the user <b>is</b> root. You can specify different behavior for applications that are detached on launch (background applications) and those that aren't (foreground applications).</p> <table border="1"> <thead> <tr> <th><i>launchspec</i></th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>Launches all applications using the Connection Method defined for the application object.</td> </tr> <tr> <td>1</td> <td>Background applications use /bin/su. Foreground applications use the application object's Connection Method.</td> </tr> <tr> <td>2</td> <td>Background applications use the application object's Connection Method. Foreground applications use /bin/su.</td> </tr> <tr> <td>3</td> <td>Launches all applications using /bin/su.</td> </tr> <tr> <td>4</td> <td>Launches all applications using the Connection Method defined for the application object.</td> </tr> <tr> <td>5</td> <td>Background applications use /bin/sh. Foreground applications use the application object's Connection Method.</td> </tr> <tr> <td>6</td> <td>Background applications use the application object's Connection Method. Foreground applications use /bin/sh.</td> </tr> <tr> <td>7</td> <td>Launches all applications using /bin/sh.</td> </tr> </tbody> </table>		<i>launchspec</i>	Description	0	Launches all applications using the Connection Method defined for the application object.	1	Background applications use /bin/su. Foreground applications use the application object's Connection Method.	2	Background applications use the application object's Connection Method. Foreground applications use /bin/su.	3	Launches all applications using /bin/su.	4	Launches all applications using the Connection Method defined for the application object.	5	Background applications use /bin/sh. Foreground applications use the application object's Connection Method.	6	Background applications use the application object's Connection Method. Foreground applications use /bin/sh.	7	Launches all applications using /bin/sh.
<i>launchspec</i>	Description																			
0	Launches all applications using the Connection Method defined for the application object.																			
1	Background applications use /bin/su. Foreground applications use the application object's Connection Method.																			
2	Background applications use the application object's Connection Method. Foreground applications use /bin/su.																			
3	Launches all applications using /bin/su.																			
4	Launches all applications using the Connection Method defined for the application object.																			
5	Background applications use /bin/sh. Foreground applications use the application object's Connection Method.																			
6	Background applications use the application object's Connection Method. Foreground applications use /bin/sh.																			
7	Launches all applications using /bin/sh.																			

The default is `-user 1 -root 3`.

## Example

```
locallaunch -abort
```

## Related topics

- What are login scripts?
- Login scripts supplied with Secure Global Desktop
- The tarantella Tcl command

## The tarantella Tcl command

### Syntax

```
tarantella
[ -hostname app_server ]
[ -middleTierUser username ]
[ -nobackground ]
[ -nosocket ]
[ -portnumber num ]
[ -socket open_socket ]
```

### Description

The login scripts supplied with Secure Global Desktop mainly use Expect for communication with the application server. However, they also use the `tarantella` Tcl command.

The `tarantella` command connects to the application server instead of Expect and provides greater control over the connection.

You can use the `tarantella` Tcl command in your own login scripts. The options that can be used are listed below.

**Note** If invoked, it is the `tarantella` command and not Expect that makes the connection to the application server. You should ensure that the `tarantella` command can only be called once in your scripts. Some options are mutually exclusive. For example, you cannot override the hostname if you've provided a socket connection.

Argument	Description
<code>-nobackground</code>	Specifies that the application server can't run additional commands on the same connection.

<code>-nosocket</code>	Specifies that the application is to be started by some other means, which must be implemented by whoever is creating the script (perhaps by using Expect's <code>spawn</code> command). This can only be done with applications that don't require a permanent connection, such as X applications. This command may prove useful if you have an unusual application server, or if you need to integrate with an existing launch mechanism.
<code>-portnumber <i>num</i></code>	Overrides the port used to make the connection to the application server. If you use this option, you must execute the <code>tarantella</code> command before the first <code>expect</code> command. If you don't, the <code>expect</code> command will be ignored.
<code>-socket <i>open_socket</i></code>	Makes a connection to the application server using the specified open socket.
<code>-middleTierUser <i>username</i></code>	Overrides the Secure Global Desktop username used in protocol negotiations.
<code>-hostname <i>app_server</i></code>	Specifies the application server to connect to, overriding the script's <code>TTA_HOSTNAME</code> variable.

## Examples

```
tarantella -portnumber 5999
```

Connect to the application server on TCP port 5999.

### Related topics

- [What are login scripts?](#)
- [Login scripts supplied with Secure Global Desktop](#)
- [Login script Tcl commands](#)

## Login script variables

Secure Global Desktop login scripts use and support a number of variables. Two types of variable are supported:

- **Guaranteed variables** store the names of commands to run, the application server to log in to, and the connection method to use. All login scripts use at least some of these variables. Guaranteed variables always exist, though they may have a null value.
- **Optional variables** store additional information about the application, the user and their session. These variables are often used to test conditions and modify the login script's behavior accordingly. Optional variables only exist if they have a specified value (for example, the `TTA_ResumeTimeOut` variable only exists if you've specified a value for the application object's [Resumable For](#) attribute).

## Guaranteed variables

Variable	Description
<code>ALTDISPLAY</code>	The fully qualified DNS name of the user's client device and the display number being used.
<code>DISPLAY</code>	The IP address of the user's client device and the display number being used.
<code>TTA_AUXCOMMANDS</code>	Any auxiliary commands to run on the application server. This corresponds to the application object's <a href="#">Window Manager</a> attribute.
<code>TTA_COMMAND</code>	The command to run on the application server. This corresponds to the application object's <a href="#">Application Command</a> attribute.
<code>TTA_CONNECTIONSERVICE</code>	The transport used to connect to the application server. This corresponds to the application object's <a href="#">Connection Method</a> attribute.
<code>TTA_ENVIRONMENT</code>	Any environment variable settings required on the application server. This corresponds to the application object's <a href="#">Environment Variables</a> attribute.



TTA_HOSTNAME	The application server that the login script connects to. This is chosen by application server load balancing, from those shown in the <a href="#">Hosts tab</a> .
TTA_IPADDRESS	The application server's IP address.
TTA_LOGFILE	<p>The name of a file in which error and diagnostic messages are logged. By default, this is of the form <i>scriptID.log</i>, where <i>script</i> is the name of the login script and <i>ID</i> is its process ID on the Secure Global Desktop server.</p> <p>If set to null, messages aren't stored.</p> <p>To log messages in this file, include the code <code>log_file \$env (TTA_LOGFILE)</code> in your login script.</p>
TTA_PRIMARY_DNSNAME	The primary Secure Global Desktop server's fully qualified DNS name. This lets the login script choose the correct <a href="#">Secure Global Desktop printer</a> when setting the default printer value. It's used to differentiate between multiple entries in the <code>/etc/ttaprinter.conf</code> file.
TTA_WILLDISCONNECT	Whether the connection will be broken once the command has been executed.
TTA_AGEDPASSWORD	Whether to use the manual or dialog method of dealing with aged passwords.
TTA_ALLOWTHIRDTIERDIALOG	Whether to allow a dialog box on the third tier if the user's password is aged.
TTA_THIRD_TIER_VARS	The list of variables to export to the environment on the application server.
TTA_STDERR	A temporary error file.

## Optional variables

Most optional variables contain the values of object attributes. The application being started has its application object's attributes made available as optional variables. Similarly, the user's person object's attributes are also available in this way.

The remaining optional variables contain additional information about the user's session.

Variable	Description
TTA_Appearance	Corresponds to the application object's <a href="#">Border Style</a> attribute.
TTA_AppletHeight	Corresponds to the application object's <a href="#">Application Height</a> attribute.
TTA_AppletWidth	Corresponds to the application object's <a href="#">Application Width</a> attribute.
TTA_ApplicationName	The application object's <a href="#">TFN name</a> .
TTA_ApplicationPlacement	Corresponds to the application object's <a href="#">Display Using</a> attribute. This variable can have the values <code>mainbrowser</code> (means webtop), <code>multiplewindows</code> (means client window management), <code>newbrowser</code> (means new browser window), <code>awtwindow</code> (means independent window), <code>kiosk</code> (means kiosk), <code>localx</code> (means local X server) and <code>seamlesswindows</code> (means seamless window).
TTA_Arguments	Corresponds to the application object's <a href="#">Arguments For Command</a> attribute.
TTA_Autowrap	Corresponds to the application object's <a href="#">Wrap Long Lines</a> attribute.
TTA_CachePassword	Whether the Save This Password box was checked if the user supplied their username and password for the application server.
TTA_CLIENT_IPADDR	The IP address of the user's client device.
TTA_CodePage	Corresponds to the application object's <a href="#">Code Page</a> attribute. This variable can have the value <code>437</code> , <code>850</code> , <code>852</code> , <code>860</code> , <code>863</code> , <code>865</code> , <code>8859-1</code> , <code>8859-2</code> , <code>Multinational</code> , <code>Mazovia</code> or <code>CP852</code> .
TTA_ColorMap	Corresponds to the application object's <a href="#">Color Map</a> attribute.
TTA_Columns	Corresponds to the application object's <a href="#">Columns</a> attribute.
TTA_Compression	Corresponds to the application object's <a href="#">Command Compression</a> attribute. This variable can have the value <code>automatic</code> , <code>on</code> or <code>off</code> .

TTA_ContinuousMode	Corresponds to the application object's <b>Command Execution</b> attribute. This variable can have the value <code>automatic</code> , <code>on</code> or <code>off</code> .
TTA_ControlCode	Corresponds to the application object's <b>Escape Sequences</b> attribute. This variable can have the value <code>7-bit</code> or <code>8-bit</code> .
TTA_Cursor	Corresponds to the application object's <b>Cursor</b> attribute. This variable can have the value <code>off</code> , <code>block</code> or <code>underline</code> .
TTA_CursorKeyMode	Corresponds to the application object's <b>Cursor Keys</b> attribute. This variable can have the value <code>application</code> or <code>cursor</code> .
TTA_DelayedUpdate	Corresponds to the application object's <b>Allow Delayed Updates</b> attribute.
TTA_DisplayEnginePage	Corresponds to the application object's <b>Emulator Applet Page</b> attribute.
TTA_DisplayName	Corresponds to the person object's <b>Name</b> attribute.
TTA_Domain	Corresponds to the application object's <b>Windows NT Domain</b> attribute.
TTA_EuroMapping	Corresponds to the application object's <b>Euro Character</b> attribute. This variable can have the value <code>iso8859-15</code> or <code>unicode</code> .
TTA_FilePath	Corresponds to the application object's <b>Application Command</b> attribute.
TTA_FixedFontSize	Corresponds to the application object's <b>Fixed Font Size</b> attribute.
TTA_FontFamily	Corresponds to the application object's <b>Font Family</b> attribute. This variable can have the value <code>courier</code> , <code>helvetica</code> or <code>timesroman</code> .
TTA_FontSize	Corresponds to the application object's <b>Font Size</b> attribute.
TTA_GraphicsAcceleration	Corresponds to the application object's <b>Use Graphics Acceleration</b> attribute.

TTA_Height	<p>Corresponds to the application object's <a href="#">Application Height</a> attribute.</p> <p>This variable provides the same information as <code>TTA_AppletHeight</code>.</p>
TTA_HostName	<p>The application server that the login script connects to. This is chosen by application server load balancing, from those shown in the <a href="#">Hosts tab</a>.</p>
TTA_Icon	<p>Corresponds to the application object's <a href="#">Webtop Icon</a> attribute.</p>
TTA_InstanceName	<p>The emulator session ID.</p>
TTA_InterlacedImages	<p>Corresponds to the application object's <a href="#">Interlaced Images</a> attribute. This variable can have the value <code>automatic</code>, <code>on</code> or <code>off</code>.</p>
TTA_KeymapLock	<p>Corresponds to the application object's <a href="#">Lock Keymap</a> attribute.</p>
TTA_KeypadMode	<p>Corresponds to the application object's <a href="#">Keypad</a> attribute. This variable can have the value <code>application</code> or <code>numeric</code>.</p>
TTA_Lines	<p>Corresponds to the application object's <a href="#">Lines</a> attribute.</p>
TTA_LocalAddr	<p>The IP address of the Secure Global Desktop host.</p>
TTA_LoginScript	<p>Corresponds to the application object's <a href="#">Login Script</a> attribute.</p>
TTA_MiddleMouseTimeout	<p>Corresponds to the application object's <a href="#">Middle Mouse Timeout</a> attribute.</p>
TTA_ParentName	<p>The application object's <a href="#">TFN name</a>.</p> <p>This variable provides the same information as <code>TTA_ApplicationName</code>.</p>
TTA_PortNumber	<p>Corresponds to the 3270 application object's <a href="#">Port Number</a> attribute.</p>

TTA_ProtocolArguments	Corresponds to the application object's <a href="#">Protocol Arguments</a> attribute.
TTA_RemoteAddr	The IP address of the application server which is to run the application.
TTA_RequiresDisplayEngine	Whether or not the application requires a display engine.
TTA_ResumeTimeOut	Corresponds to the application object's <a href="#">Resumable For</a> attribute.
TTA_RootColor	Corresponds to the application object's <a href="#">Color</a> attribute.
TTA_RootType	Corresponds to the application object's <a href="#">Root Window</a> attribute. This variable can have the value <code>default</code> or <code>color</code> .
TTA_ScrollStyle	Corresponds to the application object's <a href="#">Scroll Style</a> attribute. This variable can have the value <code>normal</code> , <code>jump</code> or <code>smooth</code> .
TTA_SecureConnection	Corresponds to the person object's <a href="#">Connections</a> attribute.
TTA_SessionExit	Corresponds to the application object's <a href="#">Session Ends When</a> attribute. This variable can have the value <code>lastclient</code> (means Last Client Exits), <code>windowmanager</code> (means Window Manager Exits), <code>windowmanageralone</code> (means Only Window Manager Remains), <code>loginscript</code> (means Login Script Exits) and <code>nowindows</code> (means No Visible Windows).
TTA_StatusLine	Corresponds to the application object's <a href="#">Status Line</a> attribute. This variable can have the value <code>none</code> , <code>indicator</code> and <code>host writable</code> , <code>standard</code> or <code>extended</code> .
TTA_Suspend	Corresponds to the application object's <a href="#">Resumable</a> attribute. This variable can have the value <code>never</code> , <code>session</code> (means Webtop Session) and <code>forever</code> (means Always).
TTA_TerminalClass	Corresponds to the application object's <a href="#">Emulation Type</a> attribute. This variable can have the value <code>scoconsole</code> , <code>vt420</code> or <code>wyse60</code> .

TTA_TerminalType	Corresponds to the application object's <b>Terminal Type</b> attribute.
TTA_Transport	<p>Corresponds to the application object's <b>Connection Method</b> attribute. This variable can have the value <code>rexec</code>, <code>telnet</code> or <code>ssh</code>.</p> <p>The guaranteed variable <code>TTA_CONNECTIONSERVICE</code> also provides this information.</p>
TTA_UserName	The <b>TFN name</b> of the user this emulator session is for.
TTA_UserSecurityEquivalent	Corresponds to the person object's <b>Username</b> attribute.
TTA_ViewHostReply	Corresponds to the application object's <b>Keep Launch Connection Open</b> attribute.
TTA_WebTop	Corresponds to the person object's <b>Webtop Theme</b> attribute.
TTA_Width	<p>Corresponds to the application object's <b>Application Width</b> attribute.</p> <p>This variable provides the same information as <code>TTA_AppletWidth</code>.</p>
TTA_WinCursor	Corresponds to the application object's <b>Use Windows Cursor</b> attribute.
TTA_WindowsApplicationServer	Corresponds to the application object's <b>Windows Protocol</b> attribute. This variable can have the value <code>wincenter</code> , <code>wincentermf</code> (means Citrix UNIX Integration Services), <code>merge</code> (means SCO Merge), <code>winframe</code> (means Citrix ICA), <code>wcpwts</code> (means Microsoft RDP) or <code>none</code> . Only Citrix ICA and Microsoft RDP are supported. The other protocols can only be used with legacy windows application objects.
TTA_WindowsApplicationSupport	Corresponds to the application object's <b>Try Running From Client First</b> attribute.

## Related topics

- [What are login scripts?](#)
- [Login scripts supplied with Secure Global Desktop](#)
- [Introducing application server load balancing](#)

## Login scripts supplied with Secure Global Desktop

All login scripts supplied with Secure Global Desktop are stored in the `/opt/tarantella/var/serverresources/expect` directory. Each script is fully commented.

To use a particular login script for an application, configure the application object's [Login Script](#) attribute.

Script name	Description
<code>runsubscript.exp</code>	<ul style="list-style-type: none"><li>• The standard wrapper login script used to call all the other Secure Global Desktop login scripts and set the environment variables they are allowed to use.</li></ul>
<code>unix.exp</code>	<ul style="list-style-type: none"><li>• The standard login script for <a href="#">character application</a> and <a href="#">X application</a> objects, used if the <a href="#">Login Script</a> attribute is blank.</li><li>• Can be used with all <a href="#">Connection Methods</a>.</li></ul>
<code>windows.exp</code>	<ul style="list-style-type: none"><li>• The standard login script for <a href="#">Windows application</a> objects, used if the <a href="#">Login Script</a> attribute is blank.</li><li>• Calls other login scripts depending on the <a href="#">Windows Protocol</a> attribute.</li></ul>
<code>wincenter.exp</code>	<ul style="list-style-type: none"><li>• Called by <code>windows.exp</code> for Windows application objects configured to use the WinCenter or Citrix UNIX Integration Services <a href="#">Windows Protocol</a>.</li><li>• Although the WinCenter and Citrix UNIX Integration Services protocols are no longer supported, legacy windows application objects can continue to use them.</li></ul>
<code>unixwin.exp</code>	<ul style="list-style-type: none"><li>• Called by <code>windows.exp</code> for Windows application objects configured to use the SCO Merge or Citrix ICA <a href="#">Windows Protocol</a>.</li><li>• This script assumes that the user's <code>PATH</code> includes the directory in which the Merge or ICA UNIX client software is installed.</li><li>• Although the SCO Merge protocol is no longer supported, legacy windows application objects can continue to use it.</li></ul>



wcpwts.exp	<ul style="list-style-type: none"> <li>Called by <code>windows.exp</code> for Windows application objects configured to use the Microsoft RDP <a href="#">Windows Protocol</a>.</li> </ul>
3270.exp	<ul style="list-style-type: none"> <li>The standard login script for <a href="#">3270 application</a> objects, used if the <a href="#">Login Script</a> attribute is blank.</li> <li>Can be used with all <a href="#">Connection Methods</a>.</li> <li>The script builds a command to run the TeemTalk® for UNIX terminal emulation software.</li> </ul>
5250.exp	<ul style="list-style-type: none"> <li>The standard login script for <a href="#">5250 application</a> objects, used if the <a href="#">Login Script</a> attribute is blank.</li> <li>Can be used with all <a href="#">Connection Methods</a>.</li> <li>The script builds a command to run the TeemTalk® for UNIX terminal emulation software.</li> </ul>
vms.exp	<ul style="list-style-type: none"> <li>The standard login script for <a href="#">VMS X</a> or character application objects for all <a href="#">Connection Methods</a> <b>except</b> <code>rexec</code>.</li> </ul>
vmsrexec.exp	<ul style="list-style-type: none"> <li>The standard login script for <a href="#">VMS X</a> or character application objects if the <a href="#">Connection Method</a> is <code>rexec</code>.</li> </ul>
unixclass.exp	<ul style="list-style-type: none"> <li>Script used to create a shadowable UNIX session, for use in a "<a href="#">virtual classroom</a>" situation.</li> </ul>
winclass.exp	<ul style="list-style-type: none"> <li>Script used to create a shadowable Windows session, for use in a "<a href="#">virtual classroom</a>" situation.</li> </ul>
pupil.exp	<ul style="list-style-type: none"> <li>Script used by the "pupils" when shadowing a "teacher" in a "<a href="#">virtual classroom</a>" situation.</li> </ul>
classroom.exp	<ul style="list-style-type: none"> <li>Convenience script, called by the <code>unixclass.exp</code>, <code>winclass.exp</code> and <code>pupil.exp</code> scripts.</li> <li>Defines common procedures for retrieving the X display to shadow and setting the Xauth permissions for shadowing.</li> </ul>
procs.exp	<ul style="list-style-type: none"> <li>Convenience script, called by other scripts.</li> <li>Defines common procedures.</li> </ul>
securid/procs.exp securid/vars.exp securid/unix.exp	<ul style="list-style-type: none"> <li>Replacements for the standard scripts if you are using <a href="#">SecurID for application server authentication</a>.</li> </ul>

## Related topics

- [What are login scripts?](#)
- [Login Script \(--login\)](#)
- [A login script returns an error](#)

## A login script returns an error

Use the information in this topic to help diagnose why the login script is failing.

- Error Codes are displayed in the Launch Details area of the application launch dialog, in the form "Script *process\_id* exited with code *error\_code* and signal *signal*".
- The Error Name is displayed in the Launch Details area and also appears in log files.

Code	Error Name and description
0	<p>OK</p> <p>The login script has successfully connected to the application server and launched the application.</p>
1	<p><code>ApplicationServerResourceFailure</code></p> <p>The login script failed due to a lack of system resources on the application server. Ensure that the application server is capable of running the required application.</p>
2	<p><code>ApplicationServerNoLicenseAvailable</code></p> <p>No licenses were available on the application server. Ensure that the application server has sufficient licenses for the number of connections you expect to make.</p>
3	<p><code>FaultInExecutionScript</code></p> <p>Your login script contains a syntax error. Review your script.</p>

4	<code>ApplicationServerLoginFailed</code> <p>The login script failed to log into the application server. Check that you can manually log into the application server. If you can, check that the application server's system prompt is recognized by the login script. The login script may also be timing out, try increasing the timeout value (prelogin) in <code>vars.exp</code>.</p>
5	<code>ApplicationServerLoginIncorrect</code> <p>The username and password supplied to the application server were not accepted. Check that the username and password are valid on that application server.</p>
6	<code>ApplicationServerPasswordAged</code> <p>The user's password on the application server has expired. Ensure that the user has a valid password on the application server. To avoid seeing this error, turn the Secure Global Desktop handling of aged passwords on. See <a href="#">What happens when a user's password expires?</a> for details.</p>
7	<code>CommandExecutionFailed</code> <p>The login script successfully logged in to the application server but could not run the command specified in the object's Application attribute. Ensure that the command is valid.</p>
8	<code>ApplicationServerConnectionFailed</code> <p>The login script failed to log in to the application server. Check that you can manually log into the application server.</p>
9	<code>ApplicationServerEndOfFileOnConnection</code> <p>The login script encountered EOF on connection to the application server. Investigate why EOF is being returned.</p>

10	<code>ApplicationServerTimeout</code>  The login script timed out when trying to connect to the application server. Investigate why the login script timed out on the application server.
12	<code>InvalidDesktopSize</code>  The width and height defined for a Windows application is not valid. Check the Application Width and Application Height attributes.
14	<code>CouldNotPipe</code>  The login script was unable to create a pipe between the parent and child processes in the Execution Protocol Engine (ExecPE). This may indicate that there is not enough memory on the application server. Check the number of other applications running on the server and/or increase size of memory.
15	<code>CouldNotFork</code>  The login script was unable to fork a child process in the Execution Protocol Engine (ExecPE). This may indicate that there is not enough memory on the application server. Check the number of other applications running on the server and/or increase size of memory.
16	<code>ScriptRead</code>  The login script produced an error when trying to read from the script process in the Execution Protocol Engine (ExecPE). Try launching the application again. If the error persists, contact Support.
17	<code>ScriptWrite</code>  The login script produced an error when trying to write to the script process in the Execution Protocol Engine (ExecPE). Try launching the application again. If the error persists, contact Support.

18	<code>ThirdTierWrite</code>  The login script produced an error when trying to write to the application server in the Execution Protocol Engine (ExecPE). This usually means the connection to the application server has been lost. Check the application server is available and try launching again.
19	<code>ThirdTierRead</code>  The login script produced an error when trying to read from the application server in the Execution Protocol Engine (ExecPE). This usually means the connection to the application server has been lost. Check the application server is available and try launching again.
21	<code>TransportNotAvailable</code>  The login script was unable to connect to the application server using the requested transport method. Check that the application server supports the transport method. Check that the application server is available.
22	<code>LogFileError</code>  This is not a launch error. Secure Global Desktop was unable to create a log file for the Protocol Engine Manager. This error should never occur, contact Support.
27	<code>ThirdTierFailure</code>  Something has gone wrong on the application server. Check that the server is available and that you can run the application manually.
31	<code>RequestNotSupported</code>  The login script cannot execute the requested auxiliary commands. Check that the application server supports the auxiliary commands and that the ability to execute commands has not been disabled in the script ( <code>tarantella -nobackground</code> ).

32	<code>RequestNotImplemented</code>  The login script cannot execute the requested operation because it has not been implemented. This error should never occur, contact Support.
33	<code>Unknown</code>  Something went wrong in the Execution Protocol Engine (ExecPE). Check the log file and try launching the application again.
34	<code>InternalError</code>  Something went wrong in the Protocol Engine Manager. Check the log file and try launching the application again.
37	<code>ProtocolEngineDied</code>  The Protocol Engine process failed. Check the log file for the PID of the protocol engine and try running the application again. If the problem persists, contact Support.
43	<code>ExpectInitialisationFailed</code>  Secure Global Desktop was unable to initialize the Expect interpreter and so the script was not run. Try running the application again. If the problem persists, contact Support.
44	<code>EvalFileFailed</code>  The login script file does not exist or contains a syntax error which is causing the Expect interpreter to fail. Check that the login script is in the specified directory (all login scripts supplied by Secure Global Desktop are stored in the <code>/opt/tarantella/var/serverresources/expect</code> directory). Check the the Execution Protocol Engine (ExecPE) error log file for details of any errors with the script.

45	<code>CreateInterpreterFailed</code>  Secure Global Desktop was unable to initialize the Tcl interpreter and so the script was not run. Try running the application again. If the problem persists, contact Support.
46	<code>ChdirFailed</code>  The login script failed to change to the directory containing the script. Check the path to the script.
47	<code>ReadError</code>  The login script produced an error when trying reading from the protocol connection between the parent and child processes in the Execution Protocol Engine (ExecPE). Try launching the application again. If the error persists, contact Support.
49	<code>EndOfFile</code>  The login script read an unexpected end of file on a connection. Try launching the application again. If the error persists, contact Support.
51	<code>BadMessage</code>  The login script received an invalid message, probably due to a corruption of the data packet. Try launching the application again. If the error persists, contact Support.
52	<code>StaleCookie</code>  The client connected to the application but the cookie needed for the launch of the application has expired. Try launching the application again. If this fails, try increasing the lifetime of the cookie by editing the <code>/opt/tarantella/var/serverconfig/global/applaunch.properties</code> file. Amend the value of the <code>tarantella.config.applaunch.reconnecttimeout=seconds</code> line. The default value is 600 (10 minutes). If the error persists, contact Support.



53	<code>EatenCookie</code> <p>The client connected to the application but the cookie needed for the launch of the application has already been used (probably by the user running multiple sessions). Try launching the application again. If the error persists, contact Support.</p>
54	<code>DifferentCookie</code> <p>The client connected to the application but the cookie supplied does not match the one required for the launch. Try launching the application again. If the error persists, contact Support.</p>
55	<code>LaunchPolicyNotFound</code> <p>Secure Global Desktop was unable to find the launch policy for this session. This error should never occur. Try launching the application again. If this fails, stop the Secure Global Desktop server, start it again and then launch the application again. If the error persists, contact Support.</p>
56	<code>BadLength</code> <p>The login script received a message that was not the correct length, probably due to a corruption of the data packet. Try launching the application again. If the error persists, contact Support.</p>
57	<code>InvalidConfigObject</code> <p>The configuration data provided by Secure Global Desktop did not contain all the required information. This error should never occur. Try launching the application again. If this fails, stop the Secure Global Desktop server, start it again and then launch the application. If the error persists, contact Support.</p>

58	<code>SessionCircuitNotFound</code>  The connection between the protocol engine and the Protocol Engine Manager has been lost. Try launching the application again. If this fails, stop the Secure Global Desktop server, start it again and then launch the application. If the error persists, contact Support.
59	<code>ExecutionCircuitNotFound</code>  The connection between the Protocol Engine Manager and the Execution Protocol Engine (ExecPE) has been lost. Try launching the application again. If this fails, stop the Secure Global Desktop server, start it again and then launch the application. If the error persists, contact Support.
61	<code>CircuitNotFound</code>  The Protocol Engine Manager can't find a circuit (connection). Try launching the application again. If this fails, stop the Secure Global Desktop server, start it again and then launch the application. If the error persists, contact Support.
62	<code>CreateFailed</code>  The create request to the protocol engine failed and Secure Global Desktop was unable to launch the application. The definition of the application is missing some attributes. Check the log file for details of the missing attributes and correct these errors before trying to launch the application again.
63	<code>Complete</code>  This is not an error. It is a message from Execution Protocol Engine (ExecPE) to the Protocol Engine Manager to indicate the launch process was completed.
65	<code>NonZeroConnectresult</code>  When Secure Global Desktop connected to the web browser, the browser produced an error. Close the browser and try again.

66	<code>UserAbort</code>  This is not an error. The user canceled the application launch.
67	<code>ClientEndOfFileOnConnection</code>  The connection to the client was lost. Close the browser and try again.
68	<code>NothingToDo</code>  This is not an error. It indicates that the launch request sent to the Protocol Engine Manager does not require any protocol engines.
71	<code>IoError</code>  The login script was unable to write to <code>stderr</code> . Try launching the application again. If the error persists, contact Support.
73	<code>TscLicenseor</code>  There are not enough Windows Terminal Services licenses available to be able to launch the application. Increase the number of licenses.

### Related topics

- [What are login scripts?](#)
- [Login scripts supplied with Secure Global Desktop](#)

## The tarantella command

### Syntax

```
tarantella option [ option-specific-arguments ]
```

### Description

You control Secure Global Desktop from the command line using the `/opt/tarantella/bin/tarantella` command.

Don't try to control the Secure Global Desktop server by running binaries directly, or by using `kill`. Using the `tarantella` command is the only supported way of controlling the Secure Global Desktop server.

The options let you control the Secure Global Desktop server in different ways, or produce information about the Secure Global Desktop server. The `tarantella` command can be used in your own shell scripts to help automate your administration of Secure Global Desktop.

If the Secure Global Desktop server is running, most `tarantella` options can be run by root or **any user** in the `ttaserv` group. The `ttaserv` group does not have to be the user's primary or effective group. See the table below for details of which user can use the command options.

If the Secure Global Desktop server is stopped, only root can use the `tarantella` command.

Option	Description	Can be run by ...
<code>archive</code>	Archives the Secure Global Desktop server's log files.	root
<code>array</code>	Creates and manages arrays of Secure Global Desktop servers.	Secure Global Desktop Administrators
<code>arraymanager</code>	Starts Array Manager.	Secure Global Desktop Administrators
<code>cache</code>	Manages the cache of LDAP data.	Secure Global Desktop Administrators

config	Edits array-wide and server-specific configuration.	root or ttaserv group
emulatorsession	Lists and controls emulator sessions.	root or ttaserv group
license	Adds, lists and removes Secure Global Desktop license keys.	root or ttaserv group
object	Manipulates objects in the organizational hierarchy.	root or ttaserv group
objectmanager	Starts Object Manager.	Secure Global Desktop Administrators
passcache	Manipulates the password cache.	root or ttaserv group
print	Controls Secure Global Desktop printing services.	root or ttaserv group
query	Examines the Secure Global Desktop server's log files.	root
restart	Restarts Secure Global Desktop services.	root
role	Give people specific roles, and gives them webtop links specific to that role.	root or ttaserv group
security	Controls security services, manages certificates.	root
setup	Changes Setup options, restores original objects.	root
start	Starts Secure Global Desktop services.	root
start_cdm	Starts client drive mapping services.	root
status	Shows the current status of Secure Global Desktop array members.	root or ttaserv group
stop	Stops Secure Global Desktop services.	root
stop_cdm	Stops client drive mapping services.	root
tokencache	Manipulates the token cache.	root or ttaserv group

<code>tscal</code>	Manages Microsoft Windows Terminal Services Client Access Licenses (CALs) for non-Windows clients.	root or ttaserv group
<code>uninstall</code>	Uninstalls Secure Global Desktop.	root
<code>version</code>	Displays versions of installed Secure Global Desktop packages.	root or ttaserv group
<code>webserver</code>	Controls the Secure Global Desktop Web Server.	root
<code>webtopsession</code>	Lists and controls webtop sessions.	root or ttaserv group

**Note** All commands allow the `--help` option: you can use `tarantella command --help` to get help on a specific command.

## Examples

```
tarantella restart --quiet
```

Stops and then restarts the Secure Global Desktop server, without displaying any messages.

```
tarantella role add_link --role global \
  --link ".../_ens/o=Indigo Insurance/cn=Write-o-Win"
```

Adds a link for the Write-o-Win application to the webtops of members of the Global Administrators role.

### Related topics

- [Introducing Sun Secure Global Desktop Software](#)
- [Roles in Secure Global Desktop](#)

## The tarantella archive command

### Syntax

```
tarantella archive
```

### Description

Archives the Secure Global Desktop server's log files.

Archiving the logs compresses the files and moves them to a numbered subdirectory of the `/opt/tarantella/log` directory. A file `summary.txt` in this directory contains the results of performing the `tarantella query` command at the time of the archive.

### Examples

```
tarantella archive
```

Archives the Secure Global Desktop server's log files.

#### Related topics

- [The tarantella query command](#)
- [Array properties \(array-wide\)](#)
- [General properties \(server-specific\)](#)

## The tarantella array command

### Syntax

```
tarantella array join | detach | make_primary | list
```

### Description

This command allows Secure Global Desktop Administrators to set up and dismantle arrays of Secure Global Desktop servers.

The command may be run on any array member.

Subcommand	Description
<code>join</code>	Adds a server to an array.
<code>detach</code>	Removes secondary servers from an array.
<code>make_primary</code>	Makes a secondary server the primary server for the array that it's currently a member of.
<code>list</code>	Lists the members of the array, identifying the primary server.

**Note** All commands allow the `--help` option: you can use `tarantella array command --help` to get help on a specific command.

### Examples

```
tarantella array join \  
  --primary newyork.indigo-insurance.com \  
  --secondary boston.indigo-insurance.com
```

Adds the server `boston` to the array with primary server `newyork`.

```
tarantella array make_primary \  
  --secondary boston.indigo-insurance.com
```



Makes the secondary server become the primary server in the array. The previous primary server becomes a secondary server.

### Related topics

- [Setting up and dismantling a Secure Global Desktop array](#)
- [What is an array?](#)
- [Introducing Array Manager](#)

## The tarantella array detach command

### Syntax

```
tarantella array detach --secondary serv
```

### Description

Removes a secondary server from the array of Secure Global Desktop servers it belongs to.

Option	Description
<code>--secondary <i>serv</i></code>	<p>Specifies the peer DNS name of a secondary server to remove. The <i>serv</i> must be the name of a secondary server in the same array.</p> <p>You can only remove one server at a time.</p>

To remove the primary server from an array, first [make another server the primary server](#) and then detach the old primary server.

When you remove a server from an array, it loses its license keys.

**Note** After running this command, it is advisable to wait until Secure Global Desktop has copied the changes to all array members before running any further `tarantella array` commands. This is complete when the `tarantella status` command returns the same result for each array member.

If you are using [secure intra-array communication](#), the secondary server generates its own CA certificate and its own server peer certificate when it is detached.

### Examples

```
tarantella array detach --secondary boston.indigo-insurance.com
```

Removes the secondary server boston from the array.

## Related topics

- [The tarantella array command](#)
- [Setting up and dismantling a Secure Global Desktop array](#)
- [What is an array?](#)
- [Introducing Array Manager](#)

## The tarantella array join command

### Syntax

```
tarantella array join [ --primary pserv ]  
                    [ --secondary sserv ]
```

### Description

Adds a server to an array of Secure Global Desktop servers, either as a primary or a secondary server.

Option	Description
<code>--primary <i>pserv</i></code>	Specifies the peer DNS name of the primary server in the array. Defaults to the server on which the command is run.
<code>--secondary <i>sserv</i></code>	Specifies the peer DNS name of the server to add. The <i>sserv</i> must be the only member of an array (a "standalone" server). Defaults to the server on which the command is run.  You can only add one secondary server at a time.

**Note** After running this command, it is advisable to wait until Secure Global Desktop has copied the changes to all array members before running any further `tarantella array` commands. This is complete when the `tarantella status` command returns the same result for each array member.

If the server you add has been load balancing application servers using [Advanced Load Management](#), we recommend that you do a warm restart (`tarantella restart --warm`) of the new server after it has joined the array. If the array to which the new server is joined is using Advanced Load Management, we recommend you do a warm restart of the whole array after the new server has joined.

If you are using [secure intra-array communication](#), you will be prompted to accept the CA certificate of either the primary server or the secondary server depending on where you ran the command.

### Examples

```
tarantella array join \  
--primary newyork.indigo-insurance.com \  
--secondary boston.indigo-insurance.com
```

Adds the server boston to the array with newyork as its primary server.

```
tarantella array join \  
--primary newyork.indigo-insurance.com
```

Adds the server on which the command is run to the array with newyork as its primary server.

### Related topics

- [The tarantella array command](#)
- [Setting up and dismantling a Secure Global Desktop array](#)
- [What is an array?](#)
- [Introducing Array Manager](#)

## The tarantella array list command

### Syntax

```
tarantella array list
```

### Description

Lists each member of the array of Secure Global Desktop servers, identifying the primary server.

**Note** You must be root to run this command.

### Examples

```
tarantella array list
```

Lists all array members.

#### Related topics

- [The tarantella array command](#)
- [Setting up and dismantling a Secure Global Desktop array](#)
- [What is an array?](#)
- [Introducing Array Manager](#)

## The tarantella array make\_primary command

### Syntax

```
tarantella array make_primary --secondary serv
```

### Description

Makes a secondary server the primary server for the array that it's currently a member of. The previous primary server becomes a secondary server.

Subcommand	Description
<code>--secondary serv</code>	Specifies the peer DNS name of the secondary server to be made the primary server.

**Note** After running this command, it is advisable to wait until Secure Global Desktop has copied the changes to all array members before running any further `tarantella array` commands. This is complete when the `tarantella status` command returns the same result for each array member.

If you are using [secure intra-array communication](#), the new primary becomes the certificate authority for the array and issues new server peer certificates to all members of the array.

### Examples

```
tarantella array make_primary \  
  --secondary boston.indigo-insurance.com
```

Makes the secondary server boston the primary server in the array.

### Related topics

- The tarantella array command
- Setting up and dismantling a Secure Global Desktop array
- What is an array?
- Introducing Array Manager



## The tarantella arraymanager command

### Syntax

```
tarantella arraymanager
```

### Description

Runs Array Manager, which lets you add and remove array members, and configure both array-wide and server-specific settings.

### Examples

```
tarantella arraymanager
```

Runs Array Manager.

#### Related topics

- [Introducing Array Manager](#)
- [Introducing webtop and emulator session load balancing](#)
- [The tarantella array command](#)
- [The tarantella config command](#)
- [What is an array?](#)
- [The tarantella objectmanager command](#)

## The tarantella cache command

### Syntax

```
tarantella cache --flush ldapgroups|ldapconn|ldapconn-lookups|all
```

### Description

This command flushes the cache of data obtained from an LDAP directory server. This data is only obtained if you are using:

- the [LDAP login authority](#)
- the [Active Directory login authority](#)
- [Directory Services Integration](#)

**Note** It only flushes the cache on the Secure Global Desktop server on which the command is run.

Argument	Description
<code>--flush ldapgroups ldapconn ldapconn-lookups all</code>	<ul style="list-style-type: none"><li>• <code>ldapgroups</code> - flushes the cache of all LDAP group data, used for Directory Services Integration</li><li>• <code>ldapconn</code> - flushes the cache of all the IP address, domain and attribute data.</li><li>• <code>ldapconn-lookups</code> - flushes the cache of all LDAP search data, used for Directory Services Integration.</li><li>• <code>all</code> - flushes all LDAP data.</li></ul>

### Examples

```
tarantella cache --flush all
```

Flushes the cache of all LDAP data.

## Related topics

- [LDAP users can't log in to Secure Global Desktop](#)

## The tarantella config command

### Syntax

```
tarantella config list | edit
```

### Description

The `tarantella config` command lists and configures array-wide settings, and also server-specific settings for any Secure Global Desktop server in the array.

Subcommand	Description
<code>list</code>	Lists array-wide and server-specific attributes and their current values.
<code>edit</code>	Edits array-wide and server-specific attributes.

**Note** All commands allow the `--help` option: you can use `tarantella config subcommand --help` to get help on a specific command.

### Examples

```
tarantella config list --server newyork.indigo-insurance.com
```

Lists server-specific attributes from the server `newyork.indigo-insurance.com`.

```
tarantella config edit --cpe-maxsessions 10
```

Sets the `cpe-maxsessions` attribute to 10 for the server on which the command is run.

### Related topics

- The tarantella arraymanager command
- The tarantella array command
- Introducing Array Manager
- What is an array?

## The tarantella config edit command

### Syntax

```
tarantella config edit { { --setting value... }...  
                        [ --array | --server serv... ]  
                        } | --file file
```

### Description

Edits array-wide and server-specific attributes.

Option	Description
<code>--setting value...</code>	Names an attribute you want to edit, and its new value(s).
<code>--array</code>	When configuring a server-specific attribute, applies the change to all array members.
<code>--server serv...</code>	When configuring a server-specific attribute, applies the change to each named <i>serv</i> in the array. Use a peer DNS name or IP address for each <i>serv</i> .
<code>--file file</code>	Specifies a file containing a batch of commands to edit attributes.

If neither `--array` nor `--server` is specified, the command sets server-specific attributes for the host on which the command is run.

Use `tarantella config list` to see a list of *settings* you can change.

For detailed information on array-wide attributes, see:

- [Application Launch properties](#)
- [Array properties](#)
- [Emulator Sessions properties](#)
- [Licenses properties](#)
- [Load Balancing properties](#)

- [Printing properties](#)
- [Security properties](#)
- [Secure Global Desktop Login properties](#)

For detailed information on server-specific attributes, see:

- [Audio Protocol Engine properties](#)
- [Channel Protocol Engine properties](#)
- [Character Protocol Engine properties](#)
- [Execution Protocol Engine properties](#)
- [General properties](#)
- [Print Protocol Engine properties](#)
- [Security properties](#)
- [Smart Card Protocol Engine properties](#)
- [Tuning properties](#)
- [X Protocol Engine properties](#)

## Examples

```
tarantella config edit \  
  --cpe-exitafter 50 \  
  --server newyork.indigo-insurance.com \  
           boston.indigo-insurance.com
```

Sets the `cpe-exitafter` attribute to 50 on array members `newyork.indigo-insurance.com` and `boston.indigo-insurance.com`.

```
tarantella config edit \  
  --cpe-maxsessions 10
```

Sets the `cpe-maxsessions` attribute to 10 for the server on which the command is run.

### Related topics

- [The tarantella config list command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.



## The tarantella config list command

### Syntax

```
tarantella config list { [ --setting... ]
                        [ --server serv ]
                        } | --file file
```

### Description

Lists array-wide and server-specific attributes and their current values.

Option	Description
<code>--setting</code>	Names an attribute you want to list the value of. If no <code>--setting</code> is specified, all Array Manager attributes are listed.
<code>--server serv</code>	Lists server-specific attributes for the array member <code>serv</code> (use a peer DNS name or IP address). If omitted, lists server-specific attributes for the host on which the command is run.
<code>--file file</code>	Specifies a file containing a batch of commands to list attributes.

For detailed information on array-wide attributes, see:

- [Application Launch properties](#)
- [Array properties](#)
- [Emulator Sessions properties](#)
- [Licenses properties](#)
- [Load Balancing properties](#)
- [Printing properties](#)
- [Security properties](#)
- [Secure Global Desktop Login properties](#)

For detailed information on server-specific attributes, see:

- [Audio Protocol Engine properties](#)

- [Channel Protocol Engine properties](#)
- [Character Protocol Engine properties](#)
- [Execution Protocol Engine properties](#)
- [General properties](#)
- [Print Protocol Engine properties](#)
- [Security properties](#)
- [Smart Card Protocol Engine properties](#)
- [Tuning properties](#)
- [X Protocol Engine properties](#)

## Examples

```
tarantella config list --server newyork.indigo-insurance.com
```

Lists array-wide attributes, and server-specific attributes for the server `newyork.indigo-insurance.com`.

```
tarantella config list --array-port-unencrypted
```

Lists the value of the `array-port-unencrypted` attribute.

### Related topics

- [The tarantella config edit command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)

## The tarantella emulatorsession command

### Syntax

```
tarantella emulatorsession list | info | shadow | suspend | end
```

### Description

This command allows Secure Global Desktop Administrators to list and manipulate emulator sessions.

Subcommand	Description
list	Lists emulator sessions.
info	Displays detailed information about emulator sessions.
shadow	Shadows an emulator session.
suspend	Suspends emulator sessions.
end	Ends emulator sessions.

**Note** All commands allow the `--help` option: you can use `tarantella emulatorsession subcommand --help` to get help on a specific command.

### Examples

```
tarantella emulatorsession list \  
  --person ".../_ens/o=Indigo Insurance/cn=Emma Rald"
```

Lists Emma Rald's emulator sessions.

```
tarantella emulatorsession shadow \  
  "paris.indigo-insurance.com:965127448604:...%2f_ens%2fo=Indigo Insurance%  
  2fcn=Emma Rald"
```

Shadows the emulator session with the specified session ID.

## Related topics

- [Understanding webtop and emulator sessions](#)
- [The tarantella status command](#)
- [The tarantella webtopsession command](#)

## The tarantella emulatorsession end command

### Syntax

```
tarantella emulatorsession end sessid...
                                [--format text|quiet]
```

### Description

Ends emulator sessions. The applications will exit immediately, which may result in loss of data for users.

Option	Description
<i>sessid...</i>	Specifies the session IDs of the emulator sessions to end. Use <code>tarantella emulatorsession list</code> to find out session IDs.
--format text   quiet	Specifies the output format (default: text). With <code>--format quiet</code> , no messages are displayed.

The exit code of the command is 0 if all sessions were successfully ended, or 1 if some *sessids* didn't exist.

### Examples

```
tarantella emulatorsession end \  
  "paris.indigo-insurance.com:965127448604:...%2f_ens%2fo=Indigo Insurance%  
  2fcn=Emma Rald"
```

Ends the specified emulator session.

### Related topics

- Understanding webtop and emulator sessions
- The tarantella emulatorsession list command

## The tarantella emulatorsession info command

### Syntax

```
tarantella emulatorsession info [ --sessid sessid... ]  
                                [ --peid peid... ]  
                                [--format text|xml|quiet]
```

### Description

Displays detailed information about emulator sessions.

Option	Description
<code>--sessid <i>sessid...</i></code>	Displays detailed information on emulator sessions matching the session IDs listed. Use <code>tarantella emulatorsession list</code> to find out session IDs.
<code>--peid <i>peid...</i></code>	Displays detailed information on emulator sessions matching the Protocol Engine process IDs listed. Valid <i>peids</i> : <ul style="list-style-type: none"><li>• A number, such as 3456, representing the process ID on the host on which the command is run</li><li>• A combination of peer DNS name and process ID, for example <code>boston.indigo-insurance.com:3456</code>, representing the process ID on the array member named.</li></ul>
<code>--format text   xml   quiet</code>	Specifies the output format (default: text). With <code>--format quiet</code> , no messages are displayed.

The exit code indicates the number of *sessids* and *peids* named that do not exist.

### Examples

```
tarantella emulatorsession info --peid 3456 4567
```

Displays detailed information on emulator sessions matching the Protocol Engine process IDs "3456"

and "4567" on the host on which the command is run.

### Related topics

- [Understanding webtop and emulator sessions](#)
- [The tarantella emulatorsession list command](#)



## The tarantella emulatorsession list command

### Syntax

```
tarantella emulatorsession list
    [--person pobj]
    [--application appobj]
    [--appserver hobj]
    [--server serv]
    [--format text|count|xml]
```

### Description

Lists emulator sessions matching the criteria specified. Information shown includes session IDs, which are used with other `tarantella emulatorsession` commands.

An example session ID is `paris.indigo-insurance.com:965127448604:...%2f_ens%2fo=Indigo Insurance%2fcn=Emma Rald`. Session IDs may contain spaces, so make sure you quote them.

Option	Description
<code>--person <i>pobj</i></code>	Lists emulator sessions matching the person specified. Use a <a href="#">TFN</a> name for <i>pobj</i> .
<code>--application <i>appobj</i></code>	Lists emulator sessions matching the application specified. Use a <a href="#">TFN</a> name for <i>appobj</i> .
<code>--appserver <i>hobj</i></code>	Lists emulator sessions matching the application server specified. Use a <a href="#">TFN</a> name for <i>hobj</i> .
<code>--server <i>serv</i></code>	Lists emulator sessions hosted by the Secure Global Desktop array member specified. Use a <a href="#">TFN</a> name or a peer DNS name for <i>serv</i> .
<code>--full</code>	Includes the current IP address of the client and the status of the emulator session in the output. It takes longer to display this information.

```
--format text | count | xml
```

Specifies the output format (default: text). Use `count` to display only the number of matching sessions.

If `--person`, `--application`, `--appserver` and `--server` are all omitted, all emulator sessions are listed.

## Examples

```
tarantella emulatorsession list \  
  --person ".../_ens/o=Indigo Insurance/cn=Emma Rald"
```

Lists Emma Rald's emulator sessions.

```
tarantella emulatorsession list \  
  --server boston.indigo-insurance.com
```

Lists all emulator sessions hosted by the Secure Global Desktop array member `boston.indigo-insurance.com`. (This is the server on which the Protocol Engines run.)

### Related topics

- [Understanding webtop and emulator sessions](#)
- [The tarantella emulatorsession info command](#)

## The tarantella emulatorshadow command

### Syntax

```
tarantella emulatorshadow shadow sessid
                                [--read-only]
                                [--silent]
                                [--format text|quiet]
```

### Description

Shadows an emulator session, allowing you and the user to interact with the application simultaneously. Only Secure Global Desktop Administrators may shadow emulator sessions. You can only shadow Windows and X applications.

**Note** You can also shadow a session from the Sessions tab in Object Manager. You select the session from either the person object or the application object. However, Object Manager does not allow you to shadow a session in read-only mode or silent mode.

If `--silent` is not used, the user is notified that an Administrator wants to shadow their session and they can refuse permission. The user is also notified when shadowing ends.

Option	Description
<code><i>sessid</i></code>	Shadows the emulator session with the specified session ID. Use <code>tarantella emulatorshadow list</code> to find out session IDs.
<code>--read-only</code>	Allows an Administrator to shadow a session without being able to interact with the application.

<code>--silent</code>	<p>Allows an Administrator to shadow a session and interact with the application. The user is <b>not notified</b> that an Administrator wants to shadow their session and they can't refuse permission.</p> <p>If this is used with <code>--read-only</code>, the user does not know they are being shadowed and the Administrator can't interact with the application.</p> <p><b>Note</b> In some countries, it is illegal to shadow a user without their knowledge. It is your responsibility to comply with the law.</p>
<code>--format text   quiet</code>	<p>Specifies the output format (default: text). With <code>--format quiet</code>, no messages are displayed.</p>

The exit code is 0 for success, 1 if the session doesn't exist, 2 if the session isn't shadowable, or 3 if the session is suspended.

## Examples

```
tarantella emulatorsession shadow \  
  "paris.indigo-insurance.com:965127448604:...%2f_ens%2fo=Indigo Insurance%  
2fcn=Emma Rald"
```

Shadows the emulator session with the specified session ID.

```
tarantella emulatorsession shadow \  
  "paris.indigo-insurance.com:965127448604:...%2f_ens%2fo=Indigo Insurance%  
2fcn=Emma Rald" \  
  --read-only --silent
```

Shadows the emulator session with the specified session ID without the user knowing that they are being shadowed. The Administrator is unable to interact with the application.

## Related topics

- Using shadowing to troubleshoot a user's problem
- Using shadowing in the classroom
- Understanding webtop and emulator sessions
- The tarantella emulatorsession list command

## The tarantella emulatorsession suspend command

### Syntax

```
tarantella emulatorsession suspend sessid...
                                [--format text|quiet]
```

### Description

Suspends emulator sessions.

Option	Description
<i>sessid...</i>	Suspends the emulator sessions with the specified session IDs. Use <code>tarantella emulatorsession list</code> to find out session IDs.
<code>--format text   quiet</code>	Specifies the output format (default: text). With <code>--format quiet</code> , no messages are displayed.

The exit code is 0 for success, 1 if some sessions don't exist, 2 if some sessions are already suspended, or 3 if there's a mixture of non-existent and suspended sessions.

### Examples

```
tarantella emulatorsession suspend \  
  "paris.indigo-insurance.com:965127448604:...%2f_ens%2fo=Indigo Insurance%  
  2fcn=Emma Rald"
```

Suspends the emulator session with the specified session ID.

#### Related topics

- [Understanding webtop and emulator sessions](#)
- [The tarantella emulatorsession list command](#)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## The tarantella help command

### Syntax

```
tarantella help
```

### Description

Shows the list of Secure Global Desktop commands.

To get help on a particular command, use `tarantella command --help`.

### Examples

```
tarantella help
```

Shows the list of Secure Global Desktop commands.

#### Related topics

- [The tarantella command](#)
- [Where is Secure Global Desktop installed?](#)



## The tarantella license command

### Syntax

```
tarantella license add | remove | list | status | query | info
```

### Description

This command adds and removes Secure Global Desktop license keys, and displays license information.

Subcommand	Description
add	Adds license keys for the array.
remove	Removes license keys from the array.
list	Lists license keys currently installed.
status	Displays current licensing status.
query	Displays information on license usage across the array, including infringements.
info	Generates signed license key information.

**Note** All commands allow the `--help` option: you can use `tarantella license command --help` to get help on a specific command.

### Examples

```
tarantella license list
```

Displays currently installed license keys for the array.

```
tarantella license add XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

Adds the license key `XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX` (which is not a valid Secure Global Desktop license key).

### Related topics

- [Licensing and Sun Secure Global Desktop Software](#)

## The tarantella license add command

### Syntax

```
tarantella license add key...
```

### Description

Adds license keys to the Secure Global Desktop array.

Argument	Description
<i>key...</i>	Valid Secure Global Desktop license keys. These are of the form <code>AAAAA-AAAAA-AAAAA-AAAAA-AAAAA</code> (five blocks of five case-insensitive characters in the range A-Z, with blocks separated by hyphens).

### Examples

```
tarantella license add XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

Adds the license key `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX` (which is not a valid Secure Global Desktop license key).

#### Related topics

- [The tarantella license command](#)
- [Licensing and Sun Secure Global Desktop Software](#)

## The tarantella license info command

### Syntax

```
tarantella license info
```

### Description

Generates signed license key information.

The output contains:

- a list of your license keys
- information about your array
- the date and time
- the version of Secure Global Desktop and
- a digital signature.

**Note** If you copy the output, make sure you include the BEGIN and END lines.

You must run this command on the primary Secure Global Desktop server.

### Examples

```
tarantella license info
```

Generates signed license key information.

#### Related topics

- [The tarantella license command](#)
- [Licensing and Sun Secure Global Desktop Software](#)



## The tarantella license list command

### Syntax

```
tarantella license list
```

### Description

Lists the license keys currently installed for the array. For details about license keys and licenses, see [Licensing and Sun Secure Global Desktop Software](#).

For summary information, use `tarantella license status`.

### Examples

```
tarantella license list
```

Displays currently installed license keys for the array.

#### Related topics

- [The tarantella license command](#)
- [Licensing and Sun Secure Global Desktop Software](#)

## The tarantella license query command

### Syntax

```
tarantella license query [ --now  
                        | --history [--format text|csv|xml]  
                        | --maxusers [--format text|xml] ]
```

### Description

Displays information on license usage across the array, including license infringements.

To avoid inconsistencies arising from the replication of data across the array, you must run this command on the primary server in the array.

**Note** This command only shows the license usage for the software components that are licensed on a per-user basis.

Secure Global Desktop maintains a history of license usage for 30 samples. A sample is created every day, whenever the server is restarted (warm or cold), and whenever your license keys change (licenses added or removed).

Argument	Description
<code>--now</code>	Displays information on the current license usage across the array. This is the default if no arguments are specified.
<code>--history [--format text   csv   xml]</code>	<p>Displays recent historical information on license usage across the array.</p> <p>The license usage information is broken down by sample and software component. For each component, the command displays:</p> <ul style="list-style-type: none"><li>• the number of licenses used</li><li>• the number of licenses available and</li><li>• the maximum number of users using a component during the sample period (the peak).</li></ul>

	Use <code>--format</code> to specify the output format (by default, "text").
<code>--maxusers [--format text   xml]</code>	<p>Use this option to display the number and the full TFN names of users who were consuming a license when license usage peaked in the history (30 samples) kept by Secure Global Desktop.</p> <p>A user consumes licenses if:</p> <ul style="list-style-type: none"> <li>• they are logged in to Secure Global Desktop or</li> <li>• they have a suspended emulator session or</li> <li>• they are within the lease period for a named-user license.</li> </ul> <p><b>Note</b> Anonymous or guest users will only be listed once.</p> <p>The output distinguishes between standard and secure connections.</p> <p>Use <code>--format</code> to specify the output format (by default, "text").</p>

Information on recent license infringements is also shown whenever a Secure Global Desktop Administrator logs in to Secure Global Desktop.

## Examples

```
$ tarantella license query --now
License usage at: Thu Nov 07 11:31:23 GMT 2002
Type           In use / Total
Base           6      / 10
UNIX           6      / 10
TSP            6      / 10
```

Displays information on the current license usage across the array.

```
$ tarantella license query --history
2002/11/07 11:23:42:
- Base         in use:      6 / 10         peak: 6
- UNIX         in use:      6 / 10         peak: 6
```



```
- Mainframe   in use:      0 / 0           peak: 0
- Windows    in use:      0 / 0           peak: 0
- AS/400     in use:      0 / 0           peak: 0
- TSP        in use:      6 / 10          peak: 6
2002/11/07 11:25:39:
- Base       in use:      4 / 10          peak: 6
- UNIX       in use:      4 / 10          peak: 6
- Mainframe  in use:      0 / 0           peak: 0
- Windows    in use:      0 / 0           peak: 0
- AS/400     in use:      0 / 0           peak: 0
- TSP        in use:      4 / 10          peak: 6
```

Displays recent historical information on license usage across the array.

```
$ tarantella license query --maxusers
Maximum number of users logged in: 3
.../_ens/o=Indigo Insurance/ou=IT/cn=Bill Orange
.../_ens/o=Indigo Insurance/ou=IT/cn=Ginger Butcher
.../_ens/o=Indigo Insurance/ou=IT/cn=Rusty Spanner
Number of TSP users: 0
```

Displays the numbers and names of users who were logged in when license usage last peaked.

### Related topics

- [The tarantella license command](#)
- [Licensing and Sun Secure Global Desktop Software](#)

## The tarantella license remove command

### Syntax

```
tarantella license remove key...
```

### Description

Removes license keys from the Secure Global Desktop array.

If you remove all the license keys, Secure Global Desktop reverts to evaluation mode or expired evaluation mode, depending on how recently you installed Secure Global Desktop. You cannot log in to a Secure Global Desktop server when it is in expired evaluation mode. To license a server when it is in expired evaluation mode, you must either add a valid license key (using `tarantella license add`) or join the server to an array that is already fully licensed.

Argument	Description
<i>key...</i>	The license keys to remove.

### Examples

```
tarantella license remove XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

Removes the license key `XXXXX-XXXXX-XXXXX-XXXXX-XXXXX` (which is not a valid Secure Global Desktop license key).

### Related topics

- [The tarantella license command](#)
- [Licensing and Sun Secure Global Desktop Software](#)



## The tarantella license status command

### Syntax

```
tarantella license status
```

### Description

Displays a summary of the current licensing status for the array. It shows:

- the Secure Global Desktop product you are licensed to use.
- the current license mode of the array. This is either:
  - [Evaluation mode](#) - the end date of the evaluation period displays in brackets.
  - [Fully licensed](#)
- a breakdown by license type of what's licensed. For details about license types, see [Licensing and Sun Secure Global Desktop Software](#).

### Examples

```
tarantella license status
```

Displays a summary of the current licensing status for the array.

#### Related topics

- [The tarantella license command](#)
- [Licensing and Sun Secure Global Desktop Software](#)

## The tarantella object command

### Syntax

```
tarantella object add_host | add_link | add_member | delete | edit |
                    list_attributes | list_contents | new_3270app |
new_5250app |
                    new_charapp | new_container | new_dc | new_doc |
new_group |
                    new_host | new_orgunit | new_person | new_windowsapp |
                    new_xapp | remove_host | remove_link | remove_member |
                    rename | script
```

### Description

The `tarantella object` command lets you create, list, edit and delete objects in the organizational hierarchy. You can also add and remove webtop links, configure application server load balancing for each application, and add and remove group members.

Subcommand	Description
<code>add_host</code>	Adds hosts to the list of those that can run an application.
<code>add_link</code>	Adds links to webtops.
<code>add_member</code>	Adds members to a group.
<code>delete</code>	Permanently deletes objects from the organizational hierarchy.
<code>edit</code>	Edits attributes for an object.
<code>list_attributes</code>	Lists attributes of an object.
<code>list_contents</code>	Lists the contents of an OU or an organization.
<code>new_3270app</code>	Creates 3270 application objects.
<code>new_5250app</code>	Creates 5250 application objects.

<code>new_charapp</code>	Creates character application objects.
<code>new_container</code>	Creates Active Directory container objects.
<code>new_dc</code>	Creates domain component objects.
<code>new_doc</code>	Creates document objects.
<code>new_group</code>	Creates group objects.
<code>new_host</code>	Creates host objects.
<code>new_orgunit</code>	Creates organizational unit objects.
<code>new_person</code>	Creates person objects.
<code>new_windowsapp</code>	Creates Windows application objects.
<code>new_xapp</code>	Creates X application objects.
<code>remove_host</code>	Removes hosts from those that can run an application.
<code>remove_link</code>	Removes links from webtops.
<code>remove_member</code>	Removes members from groups.
<code>rename</code>	Renames or moves an object.
<code>script</code>	Runs a batch script of object commands.

**Note** All commands allow the `--help` option: you can use `tarantella object subcommand --help` to get help on a specific command.

## Examples

```
tarantella object list_contents --name ".../_ens/o=Indigo Insurance"
```

Lists the objects that belong to the organization object in the organizational hierarchy.

```
tarantella object add_link \
  --name ".../_ens/o=Indigo Insurance" \
  --link ".../_ens/o=Indigo Insurance/cn=Write-o-Win"
```

Adds a link to the Write-o-Win application to the organization's webtop. Objects may inherit webtop

content from the organization, so Write-o-Win may appear on the webtops of many different users -- up to the entire organization.

### Related topics

- [Objects and the organizational hierarchy](#)
- [Introducing Object Manager](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)

## The tarantella object add host command

### Syntax

```
tarantella object add_host { --name obj...
                             --host hobj...
                             } | --file file
```

### Description

Adds hosts to the list of those that can run an application, for [application server load balancing](#).

Argument	Description
<code>--name obj...</code>	Specifies the TFN names of application objects you want to configure load balancing for.
<code>--host hobj...</code>	Specifies the TFN names of objects you want to add to the load balancing pool.
<code>--file file</code>	Specifies a file containing a batch of commands to configure application server load balancing.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella object add_host \  
  --name ".../_ens/o=Indigo Insurance/cn=Slide-o-Win" \  
  --host ".../_ens/o=Indigo Insurance/ou=Sales/cn=rome"
```

Adds the host rome to the load balancing pool for the application Slide-o-Win.

```
tarantella object add_host \  
  --name ".../_ens/o=Indigo Insurance/cn=Write-o-Win" \  
  ".../_ens/o=Indigo Insurance/cn=Slide-o-Win" \  
  --host ".../_ens/o=Indigo Insurance/cn=WinHosts"
```



---

Adds the group WinHosts to the load balancing pool for the applications Write-o-Win and Slide-o-Win. Load balancing is performed across all the hosts in WinHosts.

### Related topics

- [The tarantella object command](#)
- [Introducing application server load balancing](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## The tarantella object add link command

### Syntax

```
tarantella object add_link { --name obj...
                             --link lobj...
                             } | --file file
```

### Description

Adds links to webtops.

Argument	Description
<code>--name obj...</code>	Specifies the TFN names of objects you want to add webtop links for.
<code>--link lobj...</code>	Specifies the TFN names of objects you want to add to the webtop.
<code>--file file</code>	Specifies a file containing a batch of commands to add links to webtops.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella object add_link \  
  --name ".../_ens/o=Indigo Insurance/ou=Sales/cn=Violet Carson" \  
  --link ".../_ens/o=Indigo Insurance/cn=Write-o-Win"
```

Adds the Write-o-Win application to Violet Carson's webtop.

```
tarantella object add_link \  
  --name ".../_ens/o=Indigo Insurance/ou=Sales" \  
         ".../_ens/o=Indigo Insurance/ou=Marketing" \  
  --link ".../_ens/o=Indigo Insurance/cn=Applications"
```

Adds the group Applications to the webtops of the organizational units Sales and Marketing. Everyone who inherits webtop content from one of these OUs (for example, they belong to that OU and [Inherit Parent's Webtop Content](#) is checked for their person object) sees all the applications in the group on their webtop.

### Related topics

- [The tarantella object command](#)
- [The tarantella object remove\\_link command](#)
- [The tarantella object list\\_attributes command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## The tarantella object add member command

### Syntax

```
tarantella object add_member { --name obj...
                               --member mobj...
                               } | --file file
```

### Description

Adds objects to groups.

Argument	Description
<code>--name obj...</code>	Specifies the TFN names of group objects you want to add members for.
<code>--member mobj...</code>	Specifies the TFN names of objects you want to add to the groups.
<code>--file file</code>	Specifies a file containing a batch of commands to add group members.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella object add_member \  
  --name ".../_ens/o=Indigo Insurance/cn=Applications" \  
  --member ".../_ens/o=Indigo Insurance/cn=Write-o-Win"
```

Adds the Write-o-Win application to the group Applications.

```
tarantella object add_member \  
  --name ".../_ens/o=Indigo Insurance/cn=WinHosts" \  
  --member ".../_ens/o=Indigo Insurance/ou=Sales/cn=rome" \  
           ".../_ens/o=Indigo Insurance/cn=brussels" \  
           ".../_ens/o=Indigo Insurance/ou=Marketing/cn=berlin"
```

---

Adds the three host objects rome, brussels and berlin to the group WinHosts. This group might be added to an application's [Hosts tab](#) (from the command line: `tarantella object add_host`) to perform [application server load balancing](#) between the hosts.

### Related topics

- [The tarantella object command](#)
- [The tarantella object remove\\_member command](#)
- [The tarantella object list\\_attributes command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## The tarantella object delete command

### Syntax

```
tarantella object delete { --name obj
                          [--children]
                          } | --file file
```

### Description

Permanently deletes objects from the organizational hierarchy.

Argument	Description
<code>--name <i>obj</i></code>	Specifies the <a href="#">TFN</a> name of the object you want to delete.
<code>--children</code>	When deleting organizational units, Active Directory containers or domain components, confirms that you want to delete the object and all objects that belong to it, recursively. As a safeguard, it is impossible to delete an organizational unit, Active Directory container or domain component without specifying <code>--children</code> .
<code>--file <i>file</i></code>	Specifies a file containing a batch of commands to delete objects.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella object delete \  
  --name ".../_ens/o=Indigo Insurance/ou=Sales/cn=Violet Carson"
```

Removes the person object for Violet Carson.

```
tarantella object delete \  
  --name ".../_ens/o=Indigo Insurance/ou=Sales" \  
  --children
```

Deletes the organizational unit Sales.

### Related topics

- [The tarantella object command](#)
- [The tarantella object rename command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## The tarantella object edit command

### Syntax

```
tarantella object edit { --name obj
                        {--attribute [value]}...
                        } | --file file
```

### Description

Edits the attributes of an object in the organizational hierarchy.

Argument	Description
<code>--name <i>obj</i></code>	Specifies the <a href="#">TFN</a> name of the object you want to edit the attributes of.
<code>{--attribute [<i>value</i>]}...</code>	Specifies the attribute names you want to edit, and their new values. The valid <i>attributes</i> depend on the type of object: see the <code>tarantella object new_object_type</code> documentation for the appropriate list. For example, when editing attributes for an application object you can specify <code>--displayusing</code> to edit the <a href="#">Display Using</a> attribute. If you omit <i>value</i> for an attribute, it is deleted from the object.
<code>--file <i>file</i></code>	Specifies a file containing a batch of commands to edit attributes.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella object edit \
  --name ".../_ens/o=Indigo Insurance/ou=Sales" \
  --inherit false
```

Changes the [Inherit Parent's Webtop Content](#) attribute for the organizational unit Sales.



## Related topics

- [The tarantella object command](#)
- [The tarantella object list\\_attributes command](#)
- [The tarantella object rename command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## The tarantella object list attributes command

### Syntax

```
tarantella object list_attributes { --name obj
                                   [--attribute...]
                                   } | --file file
```

### Description

Lists the attributes of an object in the organizational hierarchy.

Argument	Description
<code>--name <i>obj</i></code>	Specifies the <a href="#">TFN</a> name of the object you want to list the attributes of.
<code>-- <i>attribute...</i></code>	Specifies the attribute names you want to list. The valid <i>attributes</i> depend on the type of object: see the <code>tarantella object new_object_type</code> documentation for the appropriate list. For example, when listing attributes for an application object you can specify <code>--displayusing</code> to list the <a href="#">Display Using</a> attribute.
<code>--file <i>file</i></code>	Specifies a file containing a batch of commands to list attributes.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella object list_attributes \  
  --name ".../_ens/o=Indigo Insurance/ou=Sales"
```

Lists all attributes for the Sales organizational unit.

```
tarantella object list_attributes \  
  --name ".../_ens/o=Indigo Insurance/ou=IT/cn=Rusty Spanner" \  
  --email --enabled
```

Lists the [Email Address](#) and [May Log In To Secure Global Desktop](#) attributes for the person object for Rusty Spanner.

### Related topics

- [The tarantella object command](#)
- [The tarantella object list\\_contents command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## The tarantella object list\_contents command

### Syntax

```
tarantella object list_contents { --name obj
                                } | --file file
```

### Description

Lists the objects that belong to a particular object in the organizational hierarchy.

Argument	Description
<code>--name <i>obj</i></code>	Specifies the <a href="#">TFN</a> name of the object you want to list the contents of.
<code>--file <i>file</i></code>	Specifies a file containing a batch of commands to list object contents.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella object list_contents \  
  --name ".../_ens/o=Indigo Insurance/ou=Sales"
```

Lists all the objects within the organizational unit Sales.

### Related topics

- The tarantella object command
- The tarantella object list\_attributes command
- Populating the Secure Global Desktop organizational hierarchy using a batch script
- The Secure Global Desktop datastore and Tarantella Federated Naming

## The tarantella object new 3270app command

### Syntax

```
tarantella object new_3270app {
  --name obj
  --width pixels
  --height pixels
  [ --description text ]
  [ --args args ]
  [ --method rexec|telnet|ssh ]
  [ --resumable never|session|always ]
  [ --endswhen lastclient|windowmanager|windowmanageralone|nowindows|
loginscript|loginscriptnowindows ]
  [ --maxinstances 0|instances ]
  [ --displayusing webtop|clientwm|newbrowser|independent|kiosk|localx ]
  [ --maximize true|false ]
  [ --scalable true|false ]
  [ --icon icon_name ]
  [ --hostname host ]
  [ --portnumber tcp ]
  [ --3270tnclose 0|1|2|3 ]
  [ --3270kt pc|sun4|sun5|hp ]
  [ --3270bl 0|1|2|3|4 ]
  [ --3270ma true|false ]
  [ --3270mb true|false ]
  [ --3270si true|false ]
  [ --3270fg color ]
  [ --3270bg color ]
  [ --roottype default|custom ]
  [ --rootcolor color ]
  [ --compression automatic|on|off ]
  [ --execution automatic|inorder|optimized ]
  [ --interlaced automatic|on|off ]
  [ --accel true|false ]
  [ --delayed true|false ]
  [ --ldapusers user_dn... ]
  [ --ldapgroups group_dn... ]
  [ --ldapsearch search_string... ]
```

```
[ --env setting... ]
[ --login script ]
[ --winmgr command... ]
[ --empage empage ]
[ --resumetimeout mins ]
[ --middlemouse ms ]
[ --windowclose notifyapp|killapp|suspendsession|endsession ]
[ --euro unicode|iso8859-15 ]
[ --dpi monitordpi ]
[ --keepopen true|false ]
[ --lockkeymap true|false ]
[ --share true|false ]
} | --file file
```

## Description

Creates one or more [3270 application objects](#).

Secure Global Desktop uses the third party TeemTalk® for Unix emulator for 3270 applications. See the [TeemTalk for Unix User's Guide](#) (in PDF format. [Download the Adobe Reader](#)) for details.

To [batch-create multiple objects](#), use the `--file` option. Use the other options to create a single object.

## Examples

```
tarantella object new_3270app \  
  --name ".../_ens/o=Indigo Insurance/ou=Finance/cn=3270cat" \  
  --width 1000 --height 800 \  
  --app /3270cat \  
  --hostname warsaw.indigo-insurance.com
```

Creates a new 3270 application object for the application 3270cat. The emulator connects to the 3270 host warsaw.indigo-insurance.com.

## Related topics

- 3270 application object
- Populating the Secure Global Desktop organizational hierarchy using a batch script



## The tarantella object new 5250app command

### Syntax

```
tarantella object new_5250app {
  --name obj
  [ --description text ]
  [ --args args ]
  --width pixels
  --height pixels
  [ --method telnet|ssh ]
  [ --resumable never|session|always ]
  [ --endswhen lastclient|windowmanager|windowmanageralone|nowindows|
loginscript|loginscriptnowindows ]
  [ --maxinstances 0|instances ]
  [ --displayusing webtop|newbrowser|independent ]
  [ --maximize true|false ]
  [ --scalable true|false ]
  [ --icon icon_name ]
  [ --roottype default|custom ]
  [ --rootcolor color ]
  [ --compression automatic|on|off ]
  [ --execution automatic|inorder|optimized ]
  [ --interlaced automatic|on|off ]
  [ --accel true|false ]
  [ --delayed true|false ]
  [ --ldapusers user_dn... ]
  [ --ldapgroups group_dn... ]
  [ --ldapsearch search_string... ]
  [ --env setting... ]
  [ --winmgr command... ]
  [ --login script ]
  [ --empage empage ]
  [ --resumetimeout mins ]
  [ --middlemouse ms ]
  [ --windowclose notifyapp|killapp|suspendsession|endsession ]
  [ --euro unicode|iso8859-15 ]
  [ --dpi monitordpi ]
  [ --keepopen true|false ]
```

```
[ --lockkeymap true|false ]
[ --share true|false ]
[ --hostname host ]
[ --portnumber tcp ]
[ --tnclose 0|1|2|3 ]
[ --ma true|false ]
[ --mb true|false ]
[ --si true|false ]
[ --fg color ]
[ --bg color ]
[ --bl 0|1|2|3|4 ]
[ --kt pc|sun4|sun5|hp ]
} | --file file
```

## Description

Creates one or more [5250 application objects](#).

The Secure Global Desktop uses the third party TeemTalk® for Unix emulator for 5250 applications. See the [TeemTalk for Unix User's Guide](#) (in PDF format. [Download the Adobe Reader](#)) for details.

To [batch-create multiple objects](#), use the `--file` option. Use the other options to create a single object.

## Examples

```
tarantella object new_5250app \  
  --name ".../_ens/o=Indigo Insurance/ou=Finance/cn=5250cat" \  
  --width 400 \  
  --height 300 \  
  --app /5250cat \  
  --appserv ".../_ens/o=Indigo Insurance/cn=prague" \  
  --hostname warsaw.indigo-insurance.com
```

Creates a 5250 application object for the application 5250cat. The emulator runs on the host prague, and connects to the AS/400 host warsaw.indigo-insurance.com.

## Related topics

- 5250 application object
- Populating the Secure Global Desktop organizational hierarchy using a batch script

## The tarantella object new charapp command

### Syntax

```
tarantella object new_charapp {
  --name obj
  --emulator scocon|vt420|wyse60
  --termtype type
  --width pixels
  --height pixels
  [ --description text ]
  [ --app pathname ]
  [ --args args ]
  [ --appserv obj... ]
  [ --method telnet|ssh ]
  [ --resumable never|session|always ]
  [ --maxinstances 0|instances ]
  [ --displayusing webtop|newbrowser|independent|kiosk ]
  [ --maximize true|false ]
  [ --cols cols ]
  [ --lines lines ]
  [ --icon icon_name ]
  [ --font courier|helvetica|timesroman ]
  [ --fontsize points ]
  [ --fixedfont true|false ]
  [ --autowrap true|false ]
  [ --cursor off|block|underline ]
  [ --statusline none|indicator|hostmessages|standard|extended ]
  [ --scrollstyle line|multiple|smooth ]
  [ --border normal|indented|raised ]
  [ --answermsg message ]
  [ --appkeymode true|false ]
  [ --keypad numeric|application ]
  [ --cursorkeys application|cursor ]
  [ --escape 7-bit|8-bit ]
  [ --codepage 437|850|852|860|863|865|8859-1|8859-2|Multinational|Mazovia|
CP852 ]
  [ --ldapusers user_dn... ]
  [ --ldapgroups group_dn... ]
```

```
[ --ldapsearch search_string... ]
[ --loadbal default|cpu|memory|sessions ]
[ --compression automatic|on|off ]
[ --env setting... ]
[ --login script ]
[ --keymap keymap ]
[ --attributemap attrmap ]
[ --colormap colormap ]
[ --empage empage ]
[ --resumetimeout mins ]
[ --windowclose suspendsession|endsession ]
} | --file file
```

## Description

Creates one or more [character application objects](#).

To [batch-create multiple objects](#), use the `--file` option. Use the other options to create a single object.

## Examples

```
tarantella object new_charapp \  
  --name ".../_ens/o=Indigo Insurance/cn=Pers-o-dat" \  
  --emulator vt420 \  
  --termttype vt220 \  
  --width 400 \  
  --height 300 \  
  --app /bin/persodat \  
  --appserv ".../_ens/o=Indigo Insurance/cn=prague" \  
            ".../_ens/o=Indigo Insurance/ou=IT/cn=london"
```

Creates a character application object for the application Pers-o-dat. The application may run on the hosts prague and london ([application server load balancing](#) decides which one to use).

### Related topics

- [Character application object](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)

---

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## The tarantella object new\_container command

### Syntax

```
tarantella object new_container { --name obj
                                } | --file file
```

### Description

Creates one or more [Active Directory container objects](#).

To [batch-create multiple objects](#), use the `--file` option. Use the other options to create a single object.

### Examples

```
tarantella object new_container \  
  --name ".../_ens/dc=com/dc=indigo-insurance/cn=Users"
```

Creates a new Active Directory container object with name `Users`, within the `indigo-insurance.com` domain components.

```
tarantella object new_container --file - <<EOF  
  --name ".../_ens/dc=com/dc=indigo-insurance/cn=Users"  
  --name ".../_ens/dc=com/dc=indigo-insurance/cn=Applications"  
EOF
```

Creates two Active Directory container objects using a batch script defined as a "here-document". You could alternatively store the batch script in a file, and reference it using `--file filename`.

### Related topics

- Active Directory container object
- Domain component object
- Populating the Secure Global Desktop organizational hierarchy using a batch script



## The tarantella object new\_dc command

### Syntax

```
tarantella object new_dc { --name obj
                          } | --file file
```

### Description

Creates one or more [domain component objects](#).

To [batch-create multiple objects](#), use the `--file` option. Use the other options to create a single object.

### Examples

```
tarantella object new_dc \  
  --name ".../_ens/dc=com"
```

Creates a new domain component object with name `com`, at the top level of the organizational hierarchy.

```
tarantella object new_orgunit --file - <<EOF  
  --name ".../_ens/dc=com"  
  --name ".../_ens/dc=com/dc=indigo-insurance"  
EOF
```

Creates two domain component objects using a batch script defined as a "here-document". You could alternatively store the batch script in a file, and reference it using `--file filename`.

### Related topics

- [Domain component object](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## The tarantella object new\_doc command

### Syntax

```
tarantella object new_doc {  
  --name obj  
  --url url  
  [ --description text ]  
  [ --newbrowser true|false ]  
  [ --icon icon_name ]  
  [ --ldapusers user_dn... ]  
  [ --ldapgroups group_dn... ]  
  [ --ldapsearch search_string... ]  
  
} | --file file
```

### Description

Creates one or more [document objects](#).

To [batch-create multiple objects](#), use the `--file` option. Use the other options to create a single object.

### Examples

```
tarantella object new_doc \  
  --name ".../_ens/o=Indigo Insurance/ou=Finance/ou=Administration/cn=Phone  
List" \  
  --url http://newyork.indigo-insurance.com \  
  --newbrowser false
```

Creates a new document object with common name `PhoneList`, belonging to the organizational unit `Administration` (which must already exist).

```
tarantella object new_doc --file - <<EOF  
  --name ".../_ens/o=Indigo Insurance/ou=Finance/ou=Administration/cn=Phone  
List" \  
  --url http://newyork.indigo-insurance.com \  
  --newbrowser false
```

```
--newbrowser false
--name ".../_ens/o=Indigo Insurance/cn=Indigo Insurance web site" \
--url http://www.indigo-insurance.com \
--newbrowser true
EOF
```

Creates two document objects using a batch script defined as a "here-document". You could alternatively store the batch script in a file, and reference it using `--file filename`.

### Related topics

- [Document object](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)

## The tarantella object new\_group command

### Syntax

```
tarantella object new_group {
  --name obj
  [ --description text ]
  [ --member obj... ]
  [ --ldapusers user_dn... ]
  [ --ldapgroups group_dn... ]
  [ --ldapsearch search_string... ]
} | --file file
```

### Description

Creates one or more [group objects](#).

To [batch-create multiple objects](#), use the `--file` option. Use the other options to create a single object.

### Examples

```
tarantella object new_group \  
  --name ".../_ens/o=Indigo Insurance/cn=WinHosts" \  
  --member ".../_ens/o=Indigo Insurance/ou=Sales/cn=rome" \  
  ".../_ens/o=Indigo Insurance/cn=brussels" \  
  ".../_ens/o=Indigo Insurance/ou=Marketing/cn=berlin"
```

Creates a new group object with common name `WinHosts`, belonging to the organization object `Indigo Insurance` (which must already exist). The group's members are the three [host objects](#) for the application servers `rome`, `brussels` and `berlin`.

```
tarantella object new_group --file - <<EOF  
  --name ".../_ens/o=Indigo Insurance/cn=WinHosts"  
  --name ".../_ens/o=Indigo Insurance/cn=UNIXHosts"  
  --name ".../_ens/o=Indigo Insurance/cn=Applications"  
EOF
```

Creates three group objects using a batch script defined as a "here-document". The groups have no members (use `tarantella object add_member` to add members later from the command line). You could alternatively store the batch script in a file, and reference it using `--file filename`.

## Related topics

- [Group object](#)
- [The tarantella object add\\_member command](#)
- [The tarantella object remove\\_member command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)

## The tarantella object new\_host command

### Syntax

```
tarantella object new_host {
  --name obj
  --address address
  [ --description text ]
  [ --ntdomain dom ]
  [ --available true|false ]
  [ --auth trytta|nevertrytta|default ]
  [ --location location ]
  [ --hostlocale ll_tt ]
} | --file file
```

### Description

Creates one or more [host objects](#).

To [batch-create multiple objects](#), use the `--file` option. Use the other options to create a single object.

### Examples

```
tarantella object new_host \  
  --name ".../_ens/o=Indigo Insurance/ou=Finance/cn=paris" \  
  --address paris.indigo-insurance.com \  
  --auth default \  
  --location Europe-north
```

Creates a new host object with common name `paris`, belonging to the organizational unit object `Finance` (which must already exist).

```
tarantella object new_host --file - <<EOF  
  --name ".../_ens/o=Indigo Insurance/ou=Finance/cn=paris" \  
  --address paris.indigo-insurance.com  
  --name ".../_ens/o=Indigo Insurance/cn=brussels" \  
  --address brussels.indigo-insurance.com
```

```
--name ".../_ens/o=Indigo Insurance/ou=IT/cn=london" \  
--address london.indigo-insurance.com  
EOF
```

Creates three host objects using a batch script defined as a "here-document". You could alternatively store the batch script in a file, and reference it using `--file filename`.

## Related topics

- [Host object](#)
- [The tarantella object `add\_host` command](#)
- [The tarantella object `remove\_host` command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)



## The tarantella object new\_org command

### Syntax

```
tarantella object new_org {
  --name obj
  --webtop theme_name
  [ --description text ]
  [ --conntype type_spec... ]
  [ --cdm drive_spec... ]
  [ --userprintingconfig true|false ]
  [ --mapprinters 2|1|0 ]
  [ --pdfenabled 1|0 ]
  [ --pdfviewerenabled 1|0 ]
  [ --pdfdriver driver_name ]
  [ --pdfisdefault 1|0 ]
  [ --pdfviewerisdefault 1|0 ]
  [ --links obj... ]
  [ --editprofile 2|1|0 ]
  [ --clipboard 2|1|0 ]
  [ --serialport 2|1|0 ]
} | --file file
```

### Description

Creates one or more organization (O) objects.

To [batch-create multiple objects](#), use the `--file` option. Use the other options to create a single object.

### Examples

```
tarantella object new_org \  
  --name ".../_ens/o=Indigo Insurance" \  
  --webtop "sco/tta/standard" \  
  --conntype '*:*:SSL'
```

Creates a new organization object with name `Indigo Insurance`. All users in the organization use

the `sco/tta/standard` webtop theme unless the OU or person objects are configured to use a different theme. Connections for all users in the organization will be secure (SSL-based) unless the OU or person objects are configured to give a different type of connection.

```
tarantella object new_org --file - <<EOF
--name ".../_ens/o=Indigo Insurance"
--name ".../_ens/o=Indigo Insurance Services"
EOF
```

Creates two organization objects using a batch script defined as a "here-document". You could alternatively store the batch script in a file, and reference it using `--file filename`.

### Related topics

- [Organization object](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)

## The tarantella object new orgunit command

### Syntax

```
tarantella object new_orgunit {
  --name obj
  [ --description text ]
  [ --webtop theme_name ]
  [ --inherit true|false ]
  [ --conntype type_spec... ]
  [ --cdm drive_spec... ]
  [ --userprintingconfig 1|0 ]
  [ --mapprinters 2|1|0 ]
  [ --pdfenabled 1|0 ]
  [ --pdfviewerenabled 1|0 ]
  [ --pdfdriver driver_name ]
  [ --pdfisdefault 1|0 ]
  [ --pdfviewerisdefault 1|0 ]
  [ --links obj... ]
  [ --editprofile 2|1|0 ]
  [ --clipboard 2|1|0 ]
  [ --serialport 2|1|0 ]
} | --file file
```

### Description

Creates one or more organizational unit (OU) objects.

To batch-create multiple objects, use the `--file` option. Use the other options to create a single object.

### Examples

```
tarantella object new_orgunit \  
  --name ".../_ens/o=Indigo Insurance/ou=IT" \  
  --inherit true \  
  --conntype '*:*:SSL'
```

Creates a new OU object with name `IT`, belonging to the organization object `Indigo Insurance` (which must already exist). This OU inherits webtop content from its parent (the organization object). Connections for all users in the OU will be secure (SSL-based) unless their person objects are configured to give a different type of connection.

```
tarantella object new_orgunit --file - <<EOF
  --name ".../_ens/o=Indigo Insurance/ou=IT"
  --name ".../_ens/o=Indigo Insurance/ou=Finance"
  --name ".../_ens/o=Indigo Insurance/ou=Finance/ou=Administration"
EOF
```

Creates three OU objects using a batch script defined as a "here-document". The OU `Administration` belongs to the OU `Finance`, just created. You could alternatively store the batch script in a file, and reference it using `--file filename`.

### Related topics

- [Organizational unit object](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)

## The tarantella object new person command

### Syntax

```
tarantella object new_person {
  --name obj
  --surname surname
  [ --description text ]
  [ --user user ]
  [ --email name@domain ]
  [ --preflocale ll-tt ]
  [ --ntdomain dom ]
  [ --webtop theme_name ]
  [ --inherit true|false ]
  [ --shared true|false ]
  [ --enabled true|false ]
  [ --conntype type_spec... ]
  [ --cdm drive_spec... ]
  [ --keymap keymap ]
  [ --bandwidth limit ]
  [ --links obj... ]
  [ --userprintingconfig 1|0 ]
  [ --mapprinters 2|1|0 ]
  [ --pdfenabled 1|0 ]
  [ --pdfviewerenabled 1|0 ]
  [ --pdfdriver driver_name ]
  [ --pdfisdefault 1|0 ]
  [ --pdfviewerisdefault 1|0 ]
  [ --editprofile 2|1|0 ]
  [ --clipboard 2|1|0 ]
  [ --serialport 2|1|0 ]
} | --file file
```

### Description

Creates one or more [person objects](#).

To [batch-create multiple objects](#), use the `--file` option. Use the other options to create a single

object.

## Examples

```
tarantella object new_person \  
  --name ".../_ens/o=Indigo Insurance/cn=Indigo Jones" \  
  --surname Jones \  
  --user indigo \  
  --email indigo@indigo-insurance.com \  
  --inherit true \  
  --conntype '*:*:SSL'
```

Creates a new person object for Indigo Jones. Indigo inherits webtop content from the organization object, and is given a secure (SSL-based) connection.

```
tarantella object new_person --file - <<EOF  
  --name ".../_ens/o=Indigo Insurance/cn=Indigo Jones" --surname Jones  
  --name ".../_ens/o=Indigo Insurance/ou=IT/cn=Bill Orange" --surname Orange  
  --name ".../_ens/o=Indigo Insurance/ou=Finance/cn=Mulan Rouge" --surname  
Rouge  
EOF
```

Creates three person objects using a batch script defined as a "here-document". You could alternatively store the batch script in a file, and reference it using `--file filename`.

### Related topics

- [Person object](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)

## The tarantella object new\_windowsapp command

### Syntax

```
tarantella object new_windowsapp {
  --name obj
  --width pixels
  --height pixels
  [ --description text ]
  [ --winproto wts|winframe|none ]
  [ --trylocal true|false ]
  [ --ntdomain dom ]
  [ --app pathname ]
  [ --args args ]
  [ --appserv obj... ]
  [ --method rexec|telnet|ssh ]
  [ --resumable never|session|always ]
  [ --endswhen lastclient|windowmanager|windowmanageralone|nowindows|loginscript|loginscriptnowindows ]
  [ --maxinstances 0|instances ]
  [ --displayusing webtop|newbrowser|independent|kiosk|localx|seamless ]
  [ --maximize true|false ]
  [ --scalable true|false ]
  [ --depth 8|16|24 ]
  [ --icon icon_name ]
  [ --clipboardlevel level ]
  [ --roottype default|custom ]
  [ --rootcolor color ]
  [ --wincursor true|false ]
  [ --compression automatic|on|off ]
  [ --execution automatic|inorder|optimized ]
  [ --interlaced automatic|on|off ]
  [ --accel true|false ]
  [ --delayed true|false ]
  [ --ldapusers user_dn... ]
  [ --ldapgroups group_dn... ]
  [ --ldapsearch search_string... ]
  [ --loadbal default|cpu|memory|sessions ]
  [ --env setting... ]
```

```
[ --login script ]
[ --winmgr command... ]
[ --empage empage ]
[ --protoargs args ]
[ --resumetimeout mins ]
[ --middlemouse ms ]
[ --windowclose suspendsession|endsession ]
[ --euro unicode|iso8859-15 ]
[ --dpi monitordpi ]
[ --keepopen true|false ]
[ --lockkeymap true|false ]
} | --file file
```

## Description

Creates one or more Windows application objects.

To [batch-create multiple objects](#), use the `--file` option. Use the other options to create a single object.

## Examples

```
tarantella object new_windowsapp \  
  --name ".../_ens/o=Indigo Insurance/cn=Write-o-Win" \  
  --width 1000 --height 800 \  
  --app c:\\programs\\apps\\write.exe \  
  --appserv ".../_ens/o=Indigo Insurance/ou=Sales/cn=rome"
```

Creates a new Windows application object for the application Write-o-Win. The application runs on the application server rome.

### Related topics

- [X application object](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)





## The tarantella object new\_xapp command

### Syntax

```
tarantella object new_xapp {
  --name obj
  --width pixels
  --height pixels
  [ --description text ]
  [ --app pathname ]
  [ --args args ]
  [ --appserv obj... ]
  [ --method rexec|telnet|ssh ]
  [ --resumable never|session|always ]
  [ --endswhen lastclient|windowmanager|windowmanageralone|nowindows|loginscript|loginscriptnowindows ]
  [ --maxinstances 0|instances ]
  [ --displayusing webtop|clientwm|newbrowser|independent|kiosk|localx ]
  [ --maximize true|false ]
  [ --scalable true|false ]
  [ --depth 8|16|24|16/8|24/8|8/16|8/24 ]
  [ --icon icon_name ]
  [ --clipboardlevel level ]
  [ --roottype default|custom ]
  [ --rootcolor color ]
  [ --compression automatic|on|off ]
  [ --execution automatic|inorder|optimized ]
  [ --quality automatic|best|24|21|18|16|15|12|9|6 ]
  [ --interlaced automatic|on|off ]
  [ --accel true|false ]
  [ --delayed true|false ]
  [ --ldapusers user_dn... ]
  [ --ldapgroups group_dn... ]
  [ --ldapsearch search_string... ]
  [ --loadbal default|cpu|memory|sessions ]
  [ --env setting... ]
  [ --login script ]
  [ --winmgr command... ]
  [ --empage empage ]
```

```
[ --resumetimeout mins ]
[ --middlemouse ms ]
[ --force3button true|false ]
[ --windowclose notifyapp|killapp|suspendsession|endsession ]
[ --euro unicode|iso8859-15 ]
[ --dpi monitordpi ]
[ --keepopen true|false ]
[ --lockkeymap true|false ]
[ --share true|false ]
[ --securityextension true|false ]
} | --file file
```

## Description

Creates one or more X application objects.

To [batch-create multiple objects](#), use the `--file` option. Use the other options to create a single object.

## Examples

```
tarantella object new_xapp \  
  --name ".../_ens/o=Indigo Insurance/ou=Finance/cn=XFinance" \  
  --width 1000 --height 800 \  
  --app /usr/local/bin/xfinance \  
  --appserv ".../_ens/o=Indigo Insurance/ou=Finance/cn=paris" \  
            ".../_ens/o=Indigo Insurance/ou=Finance/cn=bonn" \  
            ".../_ens/o=Indigo Insurance/cn=lisbon"
```

Creates a new X application object for the application XFinance. The application may run on the hosts paris, bonn or lisbon ([application server load balancing](#) decides which one to use).

### Related topics

- [X application object](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)



## The tarantella object remove\_host command

### Syntax

```
tarantella object remove_host { --name obj...
                                --host hobj...
                                } | --file file
```

### Description

Removes hosts from the list of those that can run an application, for [application server load balancing](#).

Argument	Description
<code>--name obj...</code>	Specifies the TFN names of application objects you want to configure load balancing for.
<code>--host hobj...</code>	Specifies the TFN names of objects you want to remove from the load balancing pool.
<code>--file file</code>	Specifies a file containing a batch of commands to configure application server load balancing.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella object remove_host \  
  --name ".../_ens/o=Indigo Insurance/cn=Slide-o-Win" \  
  --host ".../_ens/o=Indigo Insurance/ou=Sales/cn=rome"
```

Removes the host rome from the load balancing pool for the application Slide-o-Win.

```
tarantella object remove_host \  
  --name ".../_ens/o=Indigo Insurance/cn=Write-o-Win" \  
  ".../_ens/o=Indigo Insurance/cn=Slide-o-Win" \  
  --host ".../_ens/o=Indigo Insurance/cn=WinHosts"
```

---

Removes the group WinHosts from the load balancing pool for the applications Write-o-Win and Slide-o-Win. Load balancing is no longer performed across all the hosts in WinHosts.

### Related topics

- [The tarantella object command](#)
- [Introducing application server load balancing](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## The tarantella object remove link command

### Syntax

```
tarantella object remove_link { --name obj...
                                --link lobj...
                                } | --file file
```

### Description

Removes links from webtops.

Argument	Description
<code>--name <i>obj...</i></code>	Specifies the TFN names of objects you want to remove webtop links for.
<code>--link <i>lobj...</i></code>	Specifies the TFN names of objects you want to remove from the webtop.
<code>--file <i>file</i></code>	Specifies a file containing a batch of commands to remove links from webtops.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella object remove_link \  
  --name ".../_ens/o=Indigo Insurance/ou=Sales/cn=Violet Carson" \  
  --link ".../_ens/o=Indigo Insurance/cn=Write-o-Win"
```

Removes the Write-o-Win application from Violet Carson's webtop.

```
tarantella object remove_link \  
  --name ".../_ens/o=Indigo Insurance/ou=Sales" \  
         ".../_ens/o=Indigo Insurance/ou=Marketing" \  
  --link ".../_ens/o=Indigo Insurance/cn=Applications"
```

Removes the group Applications from the webtops of the organizational units Sales and Marketing. Everyone who inherits webtop content from one of these OUs (for example, they belong to that OU and [Inherit Parent's Webtop Content](#) is checked for their person object) no longer sees all the applications in the group on their webtop. (However, they might still see an application if it is inherited from elsewhere.)

### Related topics

- [The tarantella object command](#)
- [The tarantella object add\\_link command](#)
- [The tarantella object list\\_attributes command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)



## The tarantella object remove member command

### Syntax

```
tarantella object remove_member { --name obj...
                                --member mobj...
                                } | --file file
```

### Description

Removes objects from groups.

Argument	Description
<code>--name obj...</code>	Specifies the TFN names of group objects you want to remove members from.
<code>--member mobj...</code>	Specifies the TFN names of objects you want to remove from the groups.
<code>--file file</code>	Specifies a file containing a batch of commands to remove group members.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella object remove_member \  
  --name ".../_ens/o=Indigo Insurance/cn=Applications" \  
  --member ".../_ens/o=Indigo Insurance/cn=Write-o-Win"
```

Removes the Write-o-Win application from the group Applications.

```
tarantella object remove_member \  
  --name ".../_ens/o=Indigo Insurance/cn=WinHosts" \  
  --member ".../_ens/o=Indigo Insurance/ou=Sales/cn=rome" \  
           ".../_ens/o=Indigo Insurance/cn=brussels" \  
           ".../_ens/o=Indigo Insurance/ou=Marketing/cn=berlin"
```

---

Removes the three host objects rome, brussels and berlin from the group WinHosts.

### Related topics

- [The tarantella object command](#)
- [The tarantella object add\\_member command](#)
- [The tarantella object list\\_attributes command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## The tarantella object rename command

### Syntax

```
tarantella object rename { --name obj
                          --newname newobj
                          } | --file file
```

### Description

Renames or moves an object in the organizational hierarchy.

Argument	Description
<code>--name <i>obj</i></code>	Specifies the <a href="#">TFN</a> name of the object you want to rename or move.
<code>--newname <i>newobj</i></code>	Specifies the new <a href="#">TFN</a> name of the object.
<code>--file <i>file</i></code>	Specifies a file containing a batch of commands to rename or move objects.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella object rename \  
  --name ".../_ens/o=Indigo Insurance/ou=Sales/cn=Elizabeth Blue" \  
  --newname ".../_ens/o=Indigo Insurance/ou=Sales/cn=Liz Blue"
```

Renames the person object for Elizabeth Blue to Liz Blue.

```
tarantella object rename \  
  --name ".../_ens/o=Indigo Insurance/ou=IT/cn=Ginger Butcher" \  
  --newname ".../_ens/o=Indigo Insurance/ou=Sales/cn=Ginger Butcher"
```

Moves Ginger Butcher between the organizational units IT and Sales.

## Related topics

- [The tarantella object command](#)
- [The tarantella object delete command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## The tarantella object script command

### Syntax

```
tarantella object script
```

### Description

Runs a batch script of `tarantella object` commands, or allows commands to be run interactively.

The batch script consists of standard `tarantella object` commands, one per line, **without** the `tarantella object` prefix. For example, you would use `edit` rather than `tarantella object edit`.

The batch script may use `\` to break commands across multiple lines. Lines beginning `#` are treated as comments and ignored.

If you need to include quotes (") or a backslash ( ) character in any of the values for the commands, you must backslash protect them. For example, to use "c: Program Files" as a value for the `--args` option, you must type `--args "\"c:\\Program Files\""`

The command reads from standard input. For example, you can use a "here-document" to run a batch script:

```
$ tarantella object script <<EOF
commands
EOF
```

If standard input is empty, you can run `tarantella object` commands interactively.

### Examples

```
tarantella object script <<EOF
add_link \
  --name ".../_ens/o=Indigo Insurance/ou=Sales" \
  ".../_ens/o=Indigo Insurance/ou=Marketing" \
  --link ".../_ens/o=Indigo Insurance/cn=Applications"
edit \
```

```
--name ".../_ens/o=Indigo Insurance/ou=Sales" \  
--inherit false  
EOF
```

Adds the group Applications to the organizational units Sales and Marketing, and sets the Sales OU's [Inherit Parent's Webtop Content](#) attribute to false.

**Related topics**

- [The tarantella object command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## The tarantella objectmanager command

### Syntax

```
tarantella objectmanager
```

### Description

Runs Object Manager, which lets you configure your organizational hierarchy, define webtops, and monitor and control emulator sessions and the password cache.

### Examples

```
tarantella objectmanager
```

Runs Object Manager.

#### Related topics

- [Introducing Object Manager](#)
- [The tarantella object command](#)
- [The tarantella arraymanager command](#)

## The tarantella passcache command

### Syntax

```
tarantella passcache new | edit | list | delete
```

### Description

This command manipulates the application server password cache. Secure Global Desktop Administrators can create, modify, delete and examine entries.

Subcommand	Description
<code>new</code>	Creates entries in the password cache.
<code>edit</code>	Modifies existing entries in the password cache.
<code>list</code>	Lists the contents of the password cache.
<code>delete</code>	Deletes entries from the password cache.

**Note** All commands allow the `--help` option: you can use `tarantella passcache command --help` to get help on a specific command.

### Examples

```
tarantella passcache new \  
  --person ".../_ens/o=Indigo Insurance/cn=Indigo Jones" \  
  --resource ".../_ens/o=Indigo Insurance/cn=prague" \  
  --resuser indigo \  
  --respass rainbow
```

Creates a password cache entry for the Secure Global Desktop user Indigo Jones, on the application server represented by the host object prague.

```
tarantella passcache list \  
  --person ".../_ens/o=Indigo Insurance/cn=Indigo Jones"
```



Lists entries in the password cache for the Secure Global Desktop user Indigo Jones.

### Related topics

- [Introducing Object Manager](#)

## The tarantella passcache delete command

### Syntax

```
tarantella passcache delete { [ --person pobj | --anon | --ldap ]
                             [ --resource resource ]
                             } | --file file
```

### Description

Deletes entries in the application server password cache.

**Note** You can also use this command to delete the decision to [always use a smart card](#) to authenticate to an application server.

Option	Description
<code>--person <i>pobj</i></code>	Specifies the <a href="#">TFN</a> name of the person object to delete the password cache entry for.
<code>--anon</code>	Removes the password cache entry for all <a href="#">anonymous users</a> .
<code>--ldap</code>	<p>Deletes the password cache entry for LDAP integration. This special entry is only used with the <a href="#">LDAP login authority</a>. This is the username and password for the LDAP directory server that you can enter on the <a href="#">Secure Global Desktop Login</a> panel of Array Manager.</p> <p>Use a full username such as <code>cn=Bill Orange,cn=Users,dc=indigo-insurance,dc=com</code>.</p> <p>If you specify <code>--ldap</code>, the <code>--resource</code> option is ignored.</p>

<code>--resource resource</code>	<p>Specifies the application server or Microsoft Windows domain the password cache entry applies to. For <i>resource</i>, you use a TFN name. This can be:</p> <ul style="list-style-type: none"> <li>• A host object, for example ".../_ens/o=Indigo Insurance/cn=paris".</li> <li>• A DNS name, for example ".../_dns/paris.indigo-insurance.com".</li> <li>• A Windows domain, for example ".../_wns/indigo.dom".</li> <li>• ".../_array" to mean the array. This is used when <a href="#">caching the password used to log in to Secure Global Desktop</a>.</li> </ul>
<code>--file file</code>	Specifies a file containing password cache entries to delete.

If neither `--person`, `--anon` nor `--ldap` is specified, all password cache entries for *resource* are deleted.

If `--resource` is not specified, all the password cache entries for the person (or anonymous user) are deleted.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

## Examples

```
tarantella passcache delete \  
  --person "o=Indigo Insurance/cn=Indigo Jones"
```

Deletes all password cache entries for the user Indigo Jones.

```
tarantella passcache delete \  
  --anon \  
  --resource .../_dns/prague.indigo-insurance.com
```

Deletes all password cache entries for anonymous users on the application server prague.indigo-insurance.com.

## Related topics

- The tarantella passcache command
- The tarantella passcache new command
- The tarantella passcache edit command
- Populating the Secure Global Desktop organizational hierarchy using a batch script

## The tarantella passcache edit command

### Syntax

```
tarantella passcache edit { { --person pobj | --anon | --ldap }  
                          --resource resource  
                          --resuser resuser  
                          [ --respass respass ]  
                          } | --file file
```

### Description

Edits entries in the application server password cache.

Option	Description
<code>--person <i>pobj</i></code>	Specifies the <a href="#">TFN name</a> of the person object to edit the password cache entry for.
<code>--anon</code>	Edits a password cache entry for <a href="#">anonymous users</a> .
<code>--ldap</code>	<p>Edits the password cache entry for LDAP integration. This special entry is only used with the <a href="#">LDAP login authority</a>. This is the username and password for the LDAP directory server that you can enter on the <a href="#">Secure Global Desktop Login</a> panel of Array Manager.</p> <p>Use a full username such as <code>cn=Bill Orange,cn=Users,dc=indigo-insurance,dc=com</code>.</p> <p>If you specify <code>--ldap</code>, the <code>--resource</code> option is ignored.</p>

<code>--resource resource</code>	<p>Specifies the application server or Microsoft Windows domain the password cache entry applies to. For <i>resource</i>, you use a TFN name. This can be:</p> <ul style="list-style-type: none"> <li>• A host object, for example ".../_ens/o=Indigo Insurance/cn=paris".</li> <li>• A DNS name, for example ".../_dns/paris.indigo-insurance.com.dom".</li> <li>• A Windows domain, for example ".../_wns/indigo".</li> <li>• ".../_array" to mean the array. This is used when <a href="#">caching the password used to log in to Secure Global Desktop</a>.</li> </ul>
<code>--resuser resuser</code>	Identifies the username appropriate to the resource. Set this to the text the user would type in the authentication box for this resource.
<code>--respass respass</code>	<p>Specifies the password associated with <i>resuser</i>.</p> <p>If you omit this option, you are prompted for the password.</p>
<code>--file file</code>	Specifies a file containing password cache entries to edit.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

## Examples

```
tarantella passcache edit \
  --person ".../_ens/o=Indigo Insurance/cn=Indigo Jones" \
  --resource ".../_ens/o=Indigo Insurance/cn=prague" \
  --resuser indigo \
  --respass rainbow
```

Edits the password cache entry for the Secure Global Desktop user Indigo Jones, on the application server represented by the host object prague.

```
tarantella passcache edit \
  --anon \
  --resource .../_dns/paris.indigo-insurance.com
```

Edits the password cache entry for anonymous users on the application server paris.indigo-insurance.com.

## Related topics

- [The tarantella passcache command](#)
- [The tarantella passcache new command](#)
- [The tarantella passcache delete command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)

## The tarantella passcache list command

### Syntax

```
tarantella passcache list { [ --person pobj | --anon | --ldap ]
                           [ --resource resource ]
                           [ --resuser resuser ]
                           [ --format text | xml ]
                           } | --file file
```

### Description

Lists entries in the application server password cache.

Option	Description
<code>--person <i>pobj</i></code>	Specifies the <a href="#">TFN</a> name of the person object to list password cache entries for.
<code>--anon</code>	Lists password cache entries for <a href="#">anonymous users</a> .
<code>--ldap</code>	<p>Lists the password cache entry for LDAP integration. This special entry is only used with the <a href="#">LDAP login authority</a>. This is the username and password for the LDAP directory server that you can enter on the <a href="#">Secure Global Desktop Login</a> panel of Array Manager.</p> <p>Use a full username such as <code>cn=Bill Orange,cn=Users,dc=indigo-insurance,dc=com</code>.</p> <p>If you specify <code>--ldap</code>, the <code>--resource</code> option is ignored.</p>



<code>--resource resource</code>	<p>Lists password cache entries for an application server or Microsoft Windows domain. For <i>resource</i>, you use a TFN name. This can be:</p> <ul style="list-style-type: none"> <li>• A host object, for example ".../_ens/o=Indigo Insurance/cn=paris".</li> <li>• A DNS name, for example ".../_dns/paris.indigo-insurance.com".</li> <li>• A Windows domain, for example ".../_wns/indigo.dom".</li> <li>• ".../_array" to mean the array. This is used when <a href="#">caching the password used to log in to Secure Global Desktop</a>.</li> </ul>
<code>--resuser resuser</code>	Lists password cache entries for a particular application server username.
<code>--format text   xml</code>	Specifies the output format (default: text).
<code>--file file</code>	Specifies a file containing password cache entries to list.

If you omit all arguments, or just specify `--format`, all entries in the password cache are displayed.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

## Examples

```
tarantella passcache list \
  --person ".../_ens/o=Indigo Insurance/cn=Indigo Jones"
```

Lists entries in the password cache for the Secure Global Desktop user Indigo Jones.

```
tarantella passcache list
```

Lists all entries in the password cache.

### Related topics

- [The tarantella passcache command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)



## The tarantella passcache new command

### Syntax

```
tarantella passcache new { { --person pobj | --anon | --ldap }  
                        --resource resource  
                        --resuser resuser  
                        [ --respass respass ]  
                        } | --file file
```

### Description

Adds entries to the application server password cache.

Option	Description
<code>--person <i>pobj</i></code>	Specifies the <a href="#">TFN name</a> of the person object to create a password cache entry for.
<code>--anon</code>	Creates a password cache entry for <a href="#">anonymous users</a> .
<code>--ldap</code>	<p>Creates a password cache entry for LDAP integration. This special entry is only used with the <a href="#">LDAP login authority</a>. This is the username and password for the LDAP directory server that you can enter on the <a href="#">Secure Global Desktop Login</a> panel of Array Manager.</p> <p>Use a full username such as <code>cn=Bill Orange,cn=Users,dc=indigo-insurance,dc=com</code>.</p> <p>If you specify <code>--ldap</code>, the <code>--resource</code> option is ignored.</p>

<code>--resource resource</code>	<p>Specifies the application server or Microsoft Windows domain the password cache entry applies to. For <i>resource</i>, you use a TFN name. This can be:</p> <ul style="list-style-type: none"> <li>• A host object, for example ".../_ens/o=Indigo Insurance/cn=paris".</li> <li>• A DNS name, for example ".../_dns/paris.indigo-insurance.com".</li> <li>• A Windows domain, for example ".../_wns/indigo.dom".</li> <li>• ".../_array" to mean the array. This is used when <a href="#">caching the password used to log in to Secure Global Desktop</a>.</li> </ul>
<code>--resuser resuser</code>	Identifies the username appropriate to the resource. Set this to the text the user would type in the authentication box for this resource.
<code>--respass respass</code>	<p>Specifies the password associated with <i>resuser</i>.</p> <p>If you omit this option, you are prompted for the password.</p>
<code>--file file</code>	Specifies a file containing entries to add to the password cache.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

## Examples

```
tarantella passcache new \
  --person ".../_ens/o=Indigo Insurance/cn=Indigo Jones" \
  --resource ".../_ens/o=Indigo Insurance/cn=prague" \
  --resuser indigo \
  --respass rainbow
```

Creates a password cache entry for the Secure Global Desktop user Indigo Jones, on the application server represented by the host object prague.

```
tarantella passcache new \
  --anon \
  --resuser \
  --resource .../_dns/paris.indigo-insurance.com
```

Creates a password cache entry for anonymous users on the application server paris.indigo-insurance.com, prompting for the password.

## Related topics

- [The tarantella passcache command](#)
- [The tarantella passcache edit command](#)
- [The tarantella passcache delete command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)

## The tarantella print command

### Syntax

```
tarantella print start | stop | status | pause | resume | list | cancel |  
move
```

### Description

This command lets you administer Secure Global Desktop printing services across the array.

Subcommand	Description
cancel	Cancels print jobs.
list	Lists print jobs.
move	Moves queued print jobs from one Secure Global Desktop server to another.
pause	Pauses printing temporarily.
resume	Resumes printing.
start	Starts printing services for the array.
status	Displays information about printing services.
stop	Stops printing services for the array.

**Note** All commands allow the `--help` option. You can use `tarantella print command --help` to get help on a specific command.

### Examples

```
tarantella print start
```

Starts Secure Global Desktop printing services for the array.

---

```
tarantella print list --person ".../_ens/o=Indigo Insurance/ou=IT/cn=Bill  
Orange"
```

Lists all print jobs for Bill Orange.

### Related topics

- [Introducing Secure Global Desktop printing](#)

## The tarantella print cancel command

### Syntax

```
tarantella print cancel {--all
                        | --jobid id...
                        | --person pobj... [--server serv]
                        | --server serv}
```

### Description

Cancels Secure Global Desktop print jobs currently spooled.

You can run this command on any array member.

Argument	Description
<code>--all</code>	Cancels all print jobs spooled across the array.
<code>--jobid <i>id...</i></code>	Cancels jobs with the specified <i>ids</i> .
<code>--person <i>pobj...</i></code>	Cancels jobs belonging to each <i>pobj</i> , which must be a <a href="#">TFN</a> name.  If this is used without <code>--server</code> , Secure Global Desktop cancels all print jobs for each <i>pobj</i> .
<code>--server <i>serv...</i></code>	Cancels jobs on each Secure Global Desktop server listed. Use the peer DNS name for each <i>serv</i> .  If this is used with <code>--person</code> , Secure Global Desktop only cancels the print jobs for each <i>pobj</i> on each <i>serv</i> .

### Examples

```
tarantella print cancel --person ".../_ens/o=Indigo Insurance/ou=IT/cn=Bill Orange"
```



Cancels print jobs for Bill Orange.

```
tarantella print cancel --server "detroit.indigo-insurance.com"
```

Cancels all print jobs on the Secure Global Desktop server detroit.

### Related topics

- [The tarantella print command](#)
- [The tarantella print list command](#)
- [The tarantella print status command](#)
- [The tarantella print move command](#)
- [Can I set a time limit for print jobs?](#)
- [What is an array?](#)

## The tarantella print list command

### Syntax

```
tarantella print list { --jobid id...
                       | [ --person pobj... ] [ --server serv... ] }
                       [ --format text|brief ]
```

### Description

Lists print jobs currently spooled.

If you omit `--jobid`, `--person` or `--server` are used, all print jobs across the array are listed.

You can run this command on any array member.

Argument	Description
<code>--jobid <i>id...</i></code>	Lists jobs with the specified <i>ids</i> .
<code>--person <i>pobj...</i></code>	Lists jobs belonging to each <i>pobj</i> , which must be a <a href="#">TFN</a> name.
<code>--server <i>serv...</i></code>	Lists jobs on each Secure Global Desktop server listed. Use the peer DNS name for each <i>serv</i> .  If this is used with <code>--person</code> , Secure Global Desktop only lists the spooled print jobs for that <i>pobj</i> on that <i>serv</i> .
<code>--format <i>text</i>   <i>brief</i></code>	Specifies the output format. <ul style="list-style-type: none"> <li>The "text" format displays a block of text for each print job, showing each print job attribute (for example, the job ID and job owner) on a new line. A blank line separates each job. This is the default.</li> <li>The "brief" format shows print job attributes on one line.</li> </ul>

### Examples

```
tarantella print list --person ".../_ens/o=Indigo Insurance/ou=IT/cn=Bill  
Orange"
```

Lists print jobs for Bill Orange, in "text" format.

```
tarantella print list --person ".../_ens/o=Indigo Insurance/ou=IT/cn=Bill  
Orange" \  
".../_ens/o=Indigo Insurance/ou=IT/cn=Rusty Spanner" \  
--server "detroit.indigo-insurance.com" "chicago.indigo-insurance.com"
```

Lists print jobs in "text" format for Bill Orange and Rusty Spanner on the Secure Global Desktop servers detroit and chicago.

### Related topics

- [The tarantella print command](#)
- [The tarantella print cancel command](#)
- [The tarantella print status command](#)
- [What is an array?](#)

## The tarantella print move command

### Syntax

```
tarantella print move --server serv
                        [ --printer printer_name ]
                        [ --cups {y | n | auto} ]
                        [ --preserve ]
```

### Description

Moves queued print jobs from one Secure Global Desktop server to another.

If a Secure Global Desktop server was temporarily unavailable, you could, for example, use this command to move the print jobs that had become 'stranded' on that server.

**Note** This command only moves the print jobs that are currently in the Secure Global Desktop print queue (`/opt/tarantella/var/print/queue`).

Argument	Description
<code>--cups <i>y</i>   <i>n</i>   <i>auto</i></code>	<p>Indicates that the host from which you are moving print jobs uses the Common UNIX Printing System™ (CUPS).</p> <p>If you do not use this option, a default of <code>auto</code> is assumed and this means Secure Global Desktop tries to detect whether CUPS is being used. If CUPS is incorrectly detected, use this option to tell Secure Global Desktop whether CUPS is being used (<code>y</code>) or not (<code>n</code>).</p>
<code>--preserve</code>	<p>Forces Secure Global Desktop to copy rather than move the print jobs to the target Secure Global Desktop server. The original print jobs are kept in the Secure Global Desktop print queue.</p> <p><b>Note</b> If Secure Global Desktop printing services are re-started on the original Secure Global Desktop server and the print jobs have not been deleted, they will be printed.</p>

<code>--printer</code> <i>printer_name</i>	The name of the printer on the Secure Global Desktop server to which you are moving the print jobs. If you leave out this argument, a default of <code>tta_printer</code> is used.
<code>--server</code> <i>serv</i>	The fully qualified peer DNS name of the Secure Global Desktop server to which you are moving the print jobs.

## Examples

```
tarantella print move --server boston.indigo-insurance.com --printer  
tta_boston
```

Moves print jobs from the host on which the command is run to the printer called `tta_boston` on the host `boston.indigo-insurance.com`.

### Related topics

- [The tarantella print command](#)
- [What is an array?](#)

## The tarantella print pause command

### Syntax

```
tarantella print pause [ --server serv... ]
```

### Description

Pauses Secure Global Desktop printing services. New print jobs continue to spool, but do not print until printing is resumed using `tarantella print resume`. If `--server` is not used, this command pauses printing services across the array.

You can run this command on any array member.

Argument	Description
<code>--server serv...</code>	Pauses printing services on each Secure Global Desktop server listed. Use the peer DNS name for each <code>serv</code> .

**Note** Pausing printing services on individual array members can cause users problems. We recommend that whenever you pause printing services, you do it for the whole array.

### Examples

```
tarantella print pause
```

Pauses printing services across the array.

```
tarantella print pause --server "detroit.indigo-insurance.com" "chicago.  
indigo-insurance.com"
```

Pauses printing services on the Secure Global Desktop servers detroit and chicago.

### Related topics

- The tarantella print command
- The tarantella print resume command
- The tarantella print status command
- What is an array?

## The tarantella print resume command

### Syntax

```
tarantella print resume [ --server serv... ]
```

### Description

Resumes Secure Global Desktop printing services, previously suspended with `tarantella print pause`. Any spooled jobs begin to print. If `--server` is not used, this command resumes printing services across the array.

You can run this command on any array member.

Argument	Description
<code>--server serv...</code>	Resumes printing services on each Secure Global Desktop server listed. Use the peer DNS name for each <code>serv</code> .

**Note** Resuming printing services on individual array members can cause users problems. We recommend that whenever you resume printing services, you do it for the whole array.

### Examples

```
tarantella print resume
```

Resumes printing services across the array.

```
tarantella print resume --server "detroit.indigo-insurance.com" "chicago.  
indigo-insurance.com"
```

Resumes printing services on the Secure Global Desktop servers detroit and chicago.

### Related topics



- The tarantella print command
- The tarantella print pause command
- The tarantella print status command
- What is an array?

## The tarantella print start command

### Syntax

```
tarantella print start [ --server serv... ]
```

### Description

Starts Secure Global Desktop printing services. If `--server` is not used, this command starts printing services across the array.

You can run this command on any array member.

Argument	Description
<code>--server serv...</code>	Starts printing services on each Secure Global Desktop server listed. Use the peer DNS name for each <code>serv</code> .

**Note** Starting printing services on individual array members can cause users problems. We recommend that whenever you start printing services, you do it for the whole array.

### Examples

```
tarantella print start
```

Starts printing services across the array.

```
tarantella print start --server "detroit.indigo-insurance.com"
```

Starts printing services on the Secure Global Desktop server detroit.

### Related topics

- The tarantella print command
- The tarantella print stop command
- The tarantella print status command
- What is an array?

## The tarantella print status command

### Syntax

```
tarantella print status [ --summary  
                        | --server serv  
                        | --namemapping ]
```

### Description

Displays information about Secure Global Desktop printing services, including:

- Whether printing services are available, not available, or paused.
- The number of print jobs spooled.

You can run this command on any array member.

Argument	Description
<code>--summary</code>	Shows information for the array.
<code>--server <i>serv</i></code>	Shows information for the Secure Global Desktop server listed. Use the peer DNS name for the <i>serv</i> .
<code>-- namemapping</code>	<p>Lists all the current name mappings used for printing. The print name mapping table ensures that users can print from an application and then exit the application, without losing the print job.</p> <p>These name mappings expire in time. You can set the expiry timeout in the array-wide <a href="#">Security</a> properties in Array Manager.</p>

### Examples

```
tarantella print status --summary
```

Displays information about Secure Global Desktop printing services for the array.

## Related topics

- [The tarantella print command](#)
- [The tarantella print start command](#)
- [The tarantella print stop command](#)
- [What is an array?](#)

## The tarantella print stop command

### Syntax

```
tarantella print stop [ --server serv... ]  
                    [ --purge ]
```

### Description

Stops Secure Global Desktop printing services. Print jobs won't be accepted and won't spool. If `--server` is not used, this command stops printing services across the array.

You can run this command on any array member.

Argument	Description
<code>--purge</code>	Removes all pending print jobs. If you omit this, print jobs currently spooled are printed.
<code>--server serv...</code>	Stops printing services on each Secure Global Desktop server listed. Use the peer DNS name for each <code>serv</code> .

**Note** Stopping printing services on individual array members can cause users problems. We recommend that whenever you stop printing services, you do it for the whole array.

### Examples

```
tarantella print stop --purge
```

Stops printing services across the array, removing all pending print jobs.

```
tarantella print stop --server "detroit.indigo-insurance.com"
```

Stops printing services on the Secure Global Desktop server detroit.

## Related topics

- [The tarantella print command](#)
- [The tarantella print start command](#)
- [The tarantella print status command](#)
- [What is an array?](#)

## The tarantella query command

### Syntax

```
tarantella query audit | billing | errlog | uptime
```

### Description

Examines the server's log files.

Subcommand	Description
audit	Displays log entries matching some criteria.
billing	Queries billing log files.
errlog	Displays the error log of Secure Global Desktop components.
uptime	Displays how long array members have been available for

**Note** All commands allow the `--help` option: you can use `tarantella query command --help` to get help on a specific command.

### Examples

```
tarantella query errlog
```

Displays all error logs.

```
tarantella query uptime --server newyork.indigo-insurance.com
```

Displays how long the array member `newyork.indigo-insurance.com` has been available.

### Related topics



- The tarantella status command
- Array properties (array-wide)

## The tarantella query audit command

### Syntax

```
tarantella query audit { --app app | --person person | --host host | --
filter filter }
                        [ --server arrayhost ]
                        [ --format text|csv|xml ]
```

### Description

Displays all log entries matching some criteria.

**Note** The output that you see depends on the Log Filter settings for the array. To produce log entries for processing by this command, make sure the Log Filter attribute on the [Array properties](#) panel of Array Manager includes at least one filter that outputs to a `.json` file.

Option	Description
<code>--app <i>app</i></code>	Displays log entries referring to a specific application. Use a <a href="#">TFN</a> name for <i>app</i> .
<code>--person <i>person</i></code>	Displays log entries referring to a specific person. Use a <a href="#">TFN</a> name for <i>person</i> .
<code>--host <i>host</i></code>	Displays log entries referring to a specific host. Use a <a href="#">TFN</a> name or a peer DNS name for <i>host</i> .
<code>--filter <i>filter</i></code>	An <a href="#">RFC2254</a> -compliant LDAP search filter to find matching entries to display. Enclose the filter in quotes. You can use the "=", " =", " =" and ">=" matching rules in the filter.
<code>--server <i>arrayhost</i></code>	Only show log entries from the array member <i>arrayhost</i> (use a peer DNS name). If you omit <code>--server</code> , log entries across the entire array are displayed.

```
--format text | csv | xml
```

Specifies the output format (default: text). If you select the text format, Secure Global Desktop formats the log output so that it is easy to read on screen but it does not show every detail logged. Using the csv format shows every detail logged but it is only suitable for outputting to a file.

## Using a filter

The attributes you use in the filter are the log fields used in the `.jsl` log files. The table below lists the commonly used attributes.

Field name	Description
log-category	This is the logging component/sub-component/severity setting used in the log filters. For example to find entries for a server/printing/ log filter, you could use a "(log-category= printing )" filter
log-date	The system date and time when the event took place. The format is <code>yyyy/MM/dd HH:mm:ss.SSS</code> .
log-ip-address	The IP address of a client or server associated with an event.
log-keyword	The keyword for auditable events, see <a href="#">Using log filters for auditing</a> for details.
log-localhost	The peer DNS name of the Secure Global Desktop server where the event took place.
log-pid	The process ID of the event.
log-security-type	The type of security used on a connection, <code>std</code> or <code>ssl</code> .
log-systime	The system time in milliseconds (UTC time) when the event took place.
log-tfn-name	The TFN name of an object associated with an event. For example starting an application (emulator) session may record the TFN name of the user, the application and the host.

**Note** A complete list of all the log fields is available in the `/opt/tarantella/var/serverresources/schema/log.at.conf` schema file.

## Examples

```
tarantella query audit \
```

```
--person ../_user/indigo \  
--server boston.indigo-insurance.com
```

Displays all log entries for the UNIX user indigo that were logged on the Secure Global Desktop array member boston.indigo-insurance.com.

```
tarantella query audit \  
  --app "..._ens/o=Indigo Insurance/cn=Write-o-win" \  
  --format csv
```

Outputs all log entries that refer to the Write-o-Win application, in CSV (comma-separated values) format.

```
tarantella query audit \  
  --filter "(&(log-category=*error*)(log-tfn-name=..._ens/o=Indigo  
Insurance/cn=Write-o-win) \  
          (log-date>=2003/10/23 00:00:00.0))" \  
  --format text
```

Outputs all log errors that occurred on or after 23 October 2003 for the Write-o-Win application, in human-readable text format.

## Related topics

- [The tarantella query uptime command](#)
- [The tarantella query errlog command](#)
- [Using log filters to troubleshoot problems with the Secure Global Desktop server](#)
- [Using log filters for auditing](#)
- [Array properties \(array-wide\)](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## The tarantella query billing command

### Syntax

```
tarantella query billing { --full | --sessions | --summary }
                        --start date
                        --days days
                        --end date
                        [ --servers arrayhost... ]
```

### Description

Outputs billing information for the array, or for a subset of the array, over a time period. Information is displayed on screen in Comma Separated Values format.

The billing files are written at midnight **local time** each day.

You must run this command on the primary server in the array.

**Note** You must [enable billing services](#) and restart all array members before any data is logged.

Option	Description
<code>--full</code>	Displays detailed information for all <a href="#">webtop sessions</a> and <a href="#">emulator sessions</a> .
<code>--sessions</code>	Displays information for all emulator sessions.
<code>--summary</code>	Displays a short summary of billing information, and an emulator session summary.
<code>--start <i>date</i></code>	Specifies the start of the billing period. The format is <code>YYYY/MM/DD</code> , for example "2000/05/01".
<code>--days <i>days</i></code>	Specifies the number of days from <i>date</i> for which to display billing information.

<code>--end date</code>	Specifies the end of the billing period. The format is <code>YYYY/MM/DD</code> , for example <code>"2000/05/02"</code> . The end date is <b>exclusive</b> . This means, for example, that <code>--start 2001/01/19 --end 2001/01/23</code> is the same as <code>--start 2001/01/19 --days 4</code> and both will query data covering the 19th, 20th, 21st and 22nd.
<code>--servers arrayhost...</code>	Only reports billing information from the named array members (use peer DNS names). If you omit <code>--servers</code> , billing information across the array is reported.

## Examples

```
tarantella query billing \
  --full \
  --start "2000/05/01" \
  --days 30
```

Displays billing information for the entire array, for the 30 days from May 1, 2000.

```
tarantella query billing \
  --summary \
  --start "2000/01/01" \
  --days 30 \
  --servers prague.indigo-insurance.com \
           paris.indigo-insurance.com
```

Displays a short summary of billing information for the servers `prague` and `paris`, for the 30 days from January 1 2000.

```
tarantella query billing \
  --sessions \
  --start "2000/01/19" \
  --end "2000/01/23" \
  > sessions.csv
```

Displays billing information for all emulator sessions for the entire array for the period January 19 2001 to January 22 2001 and outputs the results to a file called `Sessions.csv`.

## Related topics

- The tarantella query uptime command
- The tarantella query errlog command
- The Secure Global Desktop datastore and Tarantella Federated Naming

## The tarantella query errlog command

### Syntax

```
tarantella query errlog [ all|xpe|tpe|print|jserver|pemanager|proxy|wm ]  
                        [ --server arrayhost ]
```

### Description

Displays the error logs of Secure Global Desktop components.

**Note** To display error log information from the JServer component, make sure the Log Filter attribute on the [Array properties](#) panel of Array Manager includes at least one filter that outputs to an `error.log` file. It does, by default.

Option	Description
<code>all   xpe   tpe   print   jserver   pemanager   proxy   wm</code>	Specifies the component error log to display. Use "all" (the default) to display all error logs.
<code>--server arrayhost</code>	Displays error logs from the named array member (use a peer DNS name). If you omit <code>--server</code> , displays error logs from all array members.

### Examples

```
tarantella query errlog
```

Displays all error logs.

```
tarantella query errlog xpe --server newyork.indigo-insurance.com
```

Displays the X Protocol Engine error log on the array member `newyork.indigo-insurance.com`.



## Related topics

- [The tarantella query audit command](#)
- [The tarantella query uptime command](#)
- [Using log filters to troubleshoot problems with the Secure Global Desktop server](#)

## The tarantella query uptime command

### Syntax

```
tarantella query uptime [ --server arrayhost ]
```

### Description

Displays how long array members have been available for.

Option	Description
<code>--server <i>arrayhost</i></code>	Display information for the array member <i>arrayhost</i> (use a peer DNS name). If you omit <code>--server</code> , displays information for all array members.

### Examples

```
tarantella query uptime
```

Displays how long all array members have been available for.

#### Related topics

- [The tarantella query audit command](#)
- [The tarantella query errlog command](#)

## The tarantella restart command

### Syntax

```
tarantella restart [ --warm | --force | --kill ] [ --quiet ]
```

### Description

Stops and then restarts Secure Global Desktop services on the host, prompting if users are currently connected.

This command does not restart the Secure Global Desktop Web Server or Secure Global Desktop web services. Use the `tarantella webserver restart` command to restart these services.

Option	Description
<code>--quiet</code>	Does not prompt: stops Secure Global Desktop services even if users are connected.
<code>--warm</code>	<p>Tries a "warm restart" of the Secure Global Desktop server, which restarts the JServer component without affecting other components.</p> <p>This has no effect on webtop or emulator sessions.</p> <p>Only use this option if no users can log in to Secure Global Desktop or launch applications and no specific reason is found.</p>
<code>--force</code>	Tries harder to stop Secure Global Desktop services.
<code>--kill</code>	<p>Kills the process IDs used by Secure Global Desktop services.</p> <p>Only use this option if you are having difficulty stopping the Secure Global Desktop server by other means.</p>

Stopping Secure Global Desktop services causes all emulator sessions (including suspended emulator sessions) to be terminated.

## Examples

```
tarantella restart --quiet
```

Stops and then restarts Secure Global Desktop services without displaying a confirmation message if users are currently connected.

### Related topics

- [The tarantella stop command](#)
- [The tarantella start command](#)

## The tarantella role command

### Syntax

```
tarantella role add_link | add_member | list | list_links | list_members |  
remove_link | remove_member
```

### Description

The `tarantella role` command gives users specific roles, and to give them webtop links that apply to that role.

Subcommand	Description
<code>add_link</code>	Adds links to the webtops of occupants of particular roles.
<code>add_member</code>	Adds occupants to particular roles.
<code>list</code>	Lists and describes all available roles.
<code>list_links</code>	Lists the webtop links for occupants of particular roles.
<code>list_members</code>	Lists the occupants of particular roles.
<code>remove_link</code>	Removes links from the webtops of users occupying particular roles.
<code>remove_member</code>	Removes occupants from particular roles.

**Note** All commands allow the `--help` option: you can use `tarantella role subcommand --help` to get help on a specific command.

### Examples

```
tarantella role list
```

Lists all available roles.

```
tarantella role add_link \  

```

```
--role global \  
--link ".../_ens/o=Indigo Insurance/cn=Indigo Time"
```

Adds a link for the application Indigo Time to the webtops of users occupying the Global Administrators role.

### Related topics

- [Roles in Secure Global Desktop](#)
- [What is a role object?](#)

## The tarantella role add link command

### Syntax

```
tarantella role add_link { --role rolename
                          --link lobj...
                          } | --file file
```

### Description

Adds links to the webtops of users occupying particular roles.

Argument	Description
<code>--role rolename</code>	Specifies the name of a role, for example <code>global</code> . Use <code>tarantella role list</code> to find out the available roles.
<code>--link lobj...</code>	Specifies the TFN names of objects to add to the webtops of users occupying the role. For example, <code>.../_ens/o=Indigo Insurance/cn=Indigo Time</code> .
<code>--file file</code>	Specifies a file containing a batch of commands to add links to webtops of users with a particular role.

**Note** Make sure you quote any object names containing spaces, for example `".../_ens/o=Indigo Insurance"`.

### Examples

```
tarantella role add_link \  
  --role global \  
  --link ".../_ens/o=Indigo Insurance/cn=Indigo Time"
```

Adds a link for the application Indigo Time to the webtops of users occupying the Global Administrators role.

## Related topics

- [The tarantella role command](#)
- [The tarantella role remove\\_link command](#)
- [The tarantella role list\\_links command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)



## The tarantella role add member command

### Syntax

```
tarantella role add_member { --role rolename
                             --member mobj...
                             } | --file file
```

### Description

Adds occupants to particular roles.

Argument	Description
<code>--role <i>rolename</i></code>	Specifies the name of a role, for example <code>global</code> . Use <code>tarantella role list</code> to find out the available roles.
<code>--member <i>mobj...</i></code>	Specifies the <a href="#">TFN</a> names of person objects or profile objects for the users you want to occupy the role.
<code>--file <i>file</i></code>	Specifies a file containing a batch of commands to add occupants to particular roles.

**Note** Make sure you quote any object names containing spaces, for example `".../_ens/o=Indigo Insurance"`.

### Examples

```
tarantella role add_member \  
  --role global \  
  --member ".../_ens/o=Indigo Insurance/ou=Finance/cn=Sid Cerise"
```

Adds Sid Cerise to the Global Administrators role.

### Related topics

- The tarantella role command
- The tarantella role remove\_member command
- The tarantella role list\_members command
- Populating the Secure Global Desktop organizational hierarchy using a batch script

## The tarantella role list command

### Syntax

```
tarantella role list
```

### Description

Lists and describes all available roles, including the [TFN name](#) of the role object applicable to each role.

Use the short name (for example, "global") with other `tarantella role` commands.

### Examples

```
tarantella role list
```

Lists all available roles.

#### Related topics

- [The tarantella role command](#)
- [The tarantella role list\\_links command](#)
- [The tarantella role list\\_members command](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## The tarantella role list\_links command

### Syntax

```
tarantella role list_links --role rolename
                        | --file file
```

### Description

Lists the webtop links for occupants of particular roles. The [TFN name](#) for each link is shown.

Argument	Description
<code>--role <i>rolename</i></code>	Specifies the name of a role, for example <code>global</code> . Use <code>tarantella role list</code> to find out the available roles.
<code>--file <i>file</i></code>	Specifies a file containing a batch of commands to list role occupants' webtop links.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella role list_links --role global
```

Lists the TFN names of all webtop links for occupants of the Global Administrators role.

### Related topics

- The tarantella role command
- The tarantella role add\_link command
- The tarantella role remove\_link command
- The Secure Global Desktop datastore and Tarantella Federated Naming
- Populating the Secure Global Desktop organizational hierarchy using a batch script

## The tarantella role list\_members command

### Syntax

```
tarantella role list_members --role rolename
                             | --file file
```

### Description

Lists the occupants of particular roles. The [TFN name](#) for each member is shown.

Argument	Description
<code>--role <i>rolename</i></code>	Specifies the name of a role, for example <code>global</code> . Use <code>tarantella role list</code> to find out the available roles.
<code>--file <i>file</i></code>	Specifies a file containing a batch of commands to list the occupants of a particular role.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella role list_members --role global
```

Lists the TFN names of all occupants of the Global Administrators role.

### Related topics

- The tarantella role command
- The tarantella role add\_member command
- The tarantella role remove\_member command
- The Secure Global Desktop datastore and Tarantella Federated Naming
- Populating the Secure Global Desktop organizational hierarchy using a batch script

## The tarantella role remove link command

### Syntax

```
tarantella role remove_link { --role rolename
                             --link lobj...
                             } | --file file
```

### Description

Removes links from the webtops of users occupying particular roles.

Argument	Description
<code>--role rolename</code>	Specifies the name of a role, for example <code>global</code> . Use <code>tarantella role list</code> to find out the available roles.
<code>--link lobj...</code>	Specifies the TFN names of objects to remove from the webtops of users occupying the role. For example, <code>.../_ens/o=Indigo Insurance/cn=Indigo Time</code> .
<code>--file file</code>	Specifies a file containing a batch of commands to remove links from webtops of users with a particular role.

**Note** Make sure you quote any object names containing spaces, for example `".../_ens/o=Indigo Insurance"`.

### Examples

```
tarantella role remove_link \  
  --role global \  
  --link ".../_ens/o=Indigo Insurance/cn=Write-o-Win"
```

Removes a link for the Write-o-Win application from the webtops of members of the Global Administrators role.



## Related topics

- [The tarantella role command](#)
- [The tarantella role add\\_link command](#)
- [The tarantella role list\\_links command](#)
- [Populating the Secure Global Desktop organizational hierarchy using a batch script](#)

## The tarantella role remove member command

### Syntax

```
tarantella role remove_member { --role rolename
                                --member mobj...
                                } | --file file
```

### Description

Removes occupants from particular roles.

Argument	Description
<code>--role <i>rolename</i></code>	Specifies the name of a role, for example <code>global</code> . Use <code>tarantella role list</code> to find out the available roles.
<code>--member <i>mobj...</i></code>	Specifies the TFN names of objects for the users you don't want to occupy the role.
<code>--file <i>file</i></code>	Specifies a file containing a batch of commands to remove occupants from a particular role.

**Note** Make sure you quote any object names containing spaces, for example ".../\_ens/o=Indigo Insurance".

### Examples

```
tarantella role remove_member \  
  --role global \  
  --member ".../_ens/o=Indigo Insurance/ou=Finance/cn=Sid Cerise"
```

Removes Sid Cerise from the Global Administrators role.

### Related topics

- The tarantella role command
- The tarantella role add\_member command
- The tarantella role list\_members command
- Populating the Secure Global Desktop organizational hierarchy using a batch script

## The tarantella security command

### Syntax

```
tarantella security certinfo | certrequest | certuse |  
                        customca | decryptkey | fingerprint | peerca | start |  
stop
```

### Description

Controls Secure Global Desktop security services and manages X.509 certificates.

Option	Description
<code>certinfo</code>	Displays information about an X.509 certificate or Certificate Signing Request (CSR), and optionally checks whether a specified private key matches the public key contained in a particular certificate.
<code>certrequest</code>	Creates a Certificate Signing Request (CSR) (and a corresponding key pair) which you use to obtain an X.509 certificate for use with Secure Global Desktop security services.
<code>certuse</code>	Installs an X.509 certificate (or specifies the location of an installed certificate) for use with Secure Global Desktop security services.
<code>customca</code>	Installs a root certificate for a custom Certificate Authority for use with Secure Global Desktop security services.
<code>decryptkey</code>	Decrypts an encrypted private key so that you can use it with Secure Global Desktop.
<code>fingerprint</code>	Displays the fingerprint of the X.509 certificate installed on this host.
<code>peerca</code>	Shows, imports or exports the primary server's CA certificate used for <a href="#">secure intra-array communication</a> .
<code>start</code>	Enables secure (SSL) connections. Users who require secure connections are given them.

stop	Disables secure (SSL) connections. Users configured for secure connections are given standard connections instead.
------	--

**Note** All commands allow the `--help` option: you can use `tarantella security subcommand --help` to get help on a specific command.

## Examples

```
tarantella security certinfo \  
--csrfile /tmp/boston.csr
```

Displays information about the CSR in `/tmp/boston.csr`.

```
tarantella security decryptkey \  
--enckey /opt/keys/key1 \  
--deckey /opt/keys/key2 \  
--format DER
```

Decrypts the key `/opt/keys/key1` (which is stored in DER format), placing the decrypted key in `/opt/keys/key2`.

### Related topics

- [Securing client connections with Secure Global Desktop security services](#)
- [Security and Secure Global Desktop](#)
- [Improving security between client devices and Secure Global Desktop servers](#)

## The tarantella security certinfo command

### Syntax

```
tarantella security certinfo [ --certfile certfile [ --keyfile keyfile ] ]  
                             [ --checkkey ] [ --full ]  
  
tarantella security certinfo --csrfile csrfile [ --full ]
```

### Description

Displays information about an installed X.509 certificate (first form) or a Certificate Signing Request (second form).

This command can also check whether a specified private key matches the public key (that is, the public key can decrypt text encrypted with the private key) in a particular certificate.

Use the first form of this command without specifying a *certfile* and *keyfile* to check keys and certificates you've already installed using the `tarantella security certuse` command.

Argument	Description
<code>--certfile <i>certfile</i></code>	Specifies the location of a file containing an X.509 certificate. The command displays information about this certificate, including: <ul style="list-style-type: none"><li>• Information about the server and your organization.</li><li>• Credentials of the Certificate Authority (CA) that validated the certificate.</li><li>• Dates for which the certificate is valid.</li></ul>
<code>--keyfile <i>keyfile</i></code>	Specifies the location of a private key.

<pre>--checkkey</pre>	<p>Checks whether a particular private key matches the public key contained in the X.509 certificate specified in <i>certfile</i>.</p> <ul style="list-style-type: none"> <li>• If you specify both <code>--certfile</code> and <code>--keyfile</code>, the command checks that the specified private key in <i>keyfile</i> matches the public key in the <i>certfile</i>.</li> <li>• If you only specify <code>--certfile</code>, the command assumes that <i>certfile</i> contains both a certificate and a private key, and checks that that private key matches the public key in the certificate.</li> <li>• If you omit both <code>--certfile</code> and <code>--keyfile</code>, the command checks the certificate and private key installed in the <code>/opt/tarantella/var/tsp</code> directory.</li> </ul>
<pre>--csrfile <i>csrfile</i></pre>	<p>Specifies the location of a file containing a Certificate Signing Request. The command displays information about this CSR, including:</p> <ul style="list-style-type: none"> <li>• The DNS name (or chosen common name) of the server the CSR is for.</li> <li>• Your organization's name and location.</li> </ul>
<pre>--full</pre>	<p>Displays more detailed information about the specified certificate or CSR -- the contents of the public keys they contain, for example.</p>

## Examples

```
tarantella security certinfo \
  --certfile /opt/certs/newyork.cert \
  --full
```

Displays detailed information about the certificate in `/opt/certs/newyork.cert`.

```
tarantella security certinfo \
  --certfile /opt/certs/boston.cert \
  --keyfile /opt/keys/boston.key \
  --checkkey
```

Displays information about the certificate in `/opt/certs/boston.cert`, and checks that the private key `/opt/keys/boston.key` matches the public key contained in that certificate.

```
tarantella security certinfo \
  --csrfile /tmp/boston.csr
```

---

Displays information about the CSR in `/tmp/boston.csr`.

### Related topics

- [Obtaining and installing an X.509 certificate](#)
- [What are X.509 certificates and why do I need one?](#)



## The tarantella security certrequest command

### Syntax

```
tarantella security certrequest --country country
                                --state state
                                --orgname org
                                [ --ouname ou ]
                                [ --email email ]
                                [ --locality locality ]
                                [ --keylength length ]
```

### Description

Generates a Certificate Signing Request (CSR), and a public and private key pair.

You should send the generated CSR to a [supported Certificate Authority \(CA\)](#) to obtain a certificate for use with Secure Global Desktop security services.

Important notes:

- If your CA lets you change the hostname stored in the certificate, make sure the certificate contains a fully qualified DNS name (for example, boston.indigo-insurance.com, not boston).
- You should make a copy of the private key and CSR generated by this command and keep them in a safe, secure location (on a floppy disk in a safe, for example). Key information is stored in the `/opt/tarantella/var/tsp` directory. **If your private key is lost or damaged, you will be unable to use any certificate you obtain using the CSR.**
- This command generates a new key pair each time you run it. If you generate a CSR with this command and use it to obtain a certificate, running this command again means you won't be able to use the old certificate.

You can use the `tarantella security certinfo` command to display information about certificates and CSRs.

If you don't specify `--ouname`, `--email` or `--locality` Secure Global Desktop simply omits that information from the CSR -- there are no default values.

The options that can be used are as follows:

Argument	Description
<code>--country <i>country</i></code>	Specifies the country in which your organization is located. Use <a href="#">ISO 3166 country codes</a> here. For example, use US for the United States or DE for Germany.
<code>--state <i>state</i></code>	Specifies the state or province in which your organization is located. Don't use abbreviations here (for example, use Massachusetts rather than Mass. or MA).
<code>--orgname <i>org</i></code>	Specifies the official, legal name of your organization.
<code>[ --ouname <i>ou</i> ]</code>	<p>Specifies the name of a subdivision (organizational unit) within your organization, if required.</p> <p>If you don't need to specify an OU, you can use this setting to specify a less formal organization name, if you want.</p>
<code>[ --email <i>email</i> ]</code>	Specifies your business email address. This address will be used for correspondence between you and the Certificate Authority you send the CSR to.
<code>[ --locality <i>locality</i> ]</code>	Specifies the city or principality where your organization is located, if needed.
<code>[ --keylength <i>length</i> ]</code>	Specifies the length of the key pair. The default is 1024. We recommend you use 512-bit or 1024-bit keys.

**Note** Make sure you quote any value containing spaces, for example "Indigo Insurance".

## Examples

```
tarantella security certrequest \
  --country US \
  --state MA \
  --orgname "Indigo Insurance" \
  --email "orange@indigo-insurance.com"
```

Generates a CSR for Indigo Insurance, located in Massachusetts, with contact Bill Orange.

## Related topics

- [What are X.509 certificates and why do I need one?](#)
- [What certificates does Secure Global Desktop support?](#)
- [Obtaining and installing an X.509 certificate](#)

## The tarantella security certuse command

### Syntax

```
tarantella security certuse

tarantella security certuse --certfile cfile
                             [ --keyfile kfile ]
```

### Description

Installs an X.509 certificate (or specifies the location of a previously installed certificate) to be used by Secure Global Desktop security services.

Certificates must be Base 64-encoded PEM-format, with a header line including "BEGIN CERTIFICATE", as used by OpenSSL.

If no arguments are specified, this command reads the certificate from standard input and installs it in `/opt/tarantella/var/tsp`.

Argument	Description
<code>--certfile <i>cfile</i></code>	<p>Specifies the location of a file containing the certificate. If no <code>--keyfile</code> argument is specified, Secure Global Desktop assumes that <i>cfile</i> contains both the certificate and the corresponding private key.</p> <p>You can use this option in two ways:</p> <ul style="list-style-type: none"><li>• To tell Secure Global Desktop about a certificate you've already <a href="#">installed for use with another product (such as a web server)</a>. In this case, Secure Global Desktop <b>makes symbolic links to (not copies of)</b> the <i>cfile</i> (and <i>kfile</i>, if specified).</li><li>• To install a certificate received from a Certificate Authority after generating a Certificate Signing Request using <code>tarantella security certrequest</code>. In this case, Secure Global Desktop installs the certificate in <code>/opt/tarantella/var/tsp</code> for use with Secure Global Desktop security services .</li></ul>

<pre>--keyfile <i>kfile</i></pre>	<p>Specifies the location of a file containing the private key required to decrypt the certificate in <i>cfile</i>.</p> <p>Use this option to tell Secure Global Desktop about a private key you've already installed. If you used the <code>tarantella security certrequest</code> command to generate a CSR and obtain a certificate, you won't need to use this option.</p>
-----------------------------------	--

## Examples

Your circumstances are...	Type this...
<p>You used <code>tarantella security certrequest</code> to generate a CSR, which you sent to a <a href="#">Certificate Authority</a>. The CA returned a certificate to you, which you saved in a temporary file <code>/tmp/cert</code>.</p>	<pre>tarantella security certuse &lt; /tmp/cert</pre>
<p>You already have a certificate (you didn't use <code>tarantella security certrequest</code>). The certificate is installed in <code>/opt/certs/cert</code> and the key needed to decode it is installed in <code>/opt/keys/key</code>.</p>	<pre>tarantella security certuse --certfile /opt/certs/cert --keyfile /opt/keys/key</pre>
<p>You already have a certificate (you didn't use <code>tarantella security certrequest</code>). A single file <code>/opt/certs/cert</code> contains both the certificate and the key needed to decode it.</p>	<pre>tarantella security certuse --certfile /opt/certs/cert</pre>

## Related topics

- Obtaining and installing an X.509 certificate
- What are X.509 certificates and why do I need one?
- What certificates does Secure Global Desktop support?
- Can I use an X.509 certificate for another product with Secure Global Desktop?
- Sharing web server and Secure Global Desktop server certificates

## The tarantella security customca command

### Syntax

```
tarantella security customca

tarantella security customca --rootfile carootfile
                             | --remove
```

### Description

Installs or removes a root certificate for a custom Certificate Authority for use with Secure Global Desktop security services.

Certificates must be Base 64-encoded PEM-format, with a header line including "BEGIN CERTIFICATE", as used by OpenSSL.

If no arguments are specified, this command reads the root certificate from standard input.

Argument	Description
<code>--rootfile <i>carootfile</i></code>	Specifies the location of a file containing the Certificate Authority's root certificate. Details are copied to <code>/opt/tarantella/var/tsp</code> for use by Secure Global Desktop security services.
<code>--remove</code>	Removes any custom Certificate Authority's root certificate currently installed for use with Secure Global Desktop security services.

### Examples

```
tarantella security customca \  
  --rootfile /tmp/rootcert
```

Installs a CA's root certificate from the file `/tmp/rootcert`, which you can then delete.

### Related topics

- Obtaining and installing an X.509 certificate
- What are X.509 certificates and why do I need one?
- What certificates does Secure Global Desktop support?
- Can I use an X.509 certificate for another product with Secure Global Desktop?



## The tarantella security decryptkey command

### Syntax

```
tarantella security decryptkey --enckey enckeyfile
                               --deckey deckeyfile
                               [ --format PEM|DER ]
```

### Description

Decrypts an encrypted private key so that you can use it with Secure Global Desktop. This lets you use an X.509 certificate that you're already using with another product (a web server, for example) rather than obtaining a separate certificate for use exclusively with Secure Global Desktop.

**Note** You can only decrypt private keys that were originally encrypted by a product that uses SSLeay or OpenSSL certificate libraries.

See the `tarantella security certuse` command for information about how to share certificates in this way.

Argument	Description
<code>--enckey <i>enckeyfile</i></code>	Specifies the location of the encrypted private key that you want to decrypt. Only keys encrypted by a product that uses SSLeay or OpenSSL certificate libraries can be decrypted.
<code>--deckey <i>deckeyfile</i></code>	Specifies a file where the decrypted key will be stored.  <b>Note</b> For security reasons, it is very important to restrict access to private keys, especially when stored in an unencrypted form. Access to private keys by unauthorized users can result in a serious security breach. Store private keys accordingly.
<code>--format PEM   DER</code>	Specifies the format in which the encrypted key is stored. Defaults to PEM.

### Examples

```
tarantella security decryptkey \  
--enckey /opt/keys/key1 \  
--deckey /opt/keys/key2 \  
--format DER
```

Decrypts the key `/opt/keys/key1` (which is stored in DER format), placing the decrypted key in `/opt/keys/key2`.

### Related topics

- [Obtaining and installing an X.509 certificate](#)
- [What are X.509 certificates and why do I need one?](#)
- [What certificates does Secure Global Desktop support?](#)
- [Can I use an X.509 certificate for another product with Secure Global Desktop?](#)
- [Sharing web server and Secure Global Desktop server certificates](#)

## The tarantella security fingerprint command

### Syntax

```
tarantella security fingerprint
```

### Description

Displays the fingerprint of the [X.509 certificate](#) installed on this host.

Use this command to obtain the finger and distribute it to users so that can be sure that the Secure Global Desktop server they are connecting to is a trusted server. See [Securing client connections with Secure Global Desktop security services](#) for details.

### Examples

#### Related topics

- [Securing client connections with Secure Global Desktop security services](#)
- [Security and Secure Global Desktop](#)
- [The tarantella security command](#)

## The tarantella security peerca command

### Syntax

```
tarantella security peerca [ --show | --import hostname | --export ]
```

### Description

Shows, imports or exports the primary server's CA certificate used for [secure intra-array communication](#).

Argument	Description
<code>--show</code>	Displays the primary server's CA certificate for the array.
<code>--import</code> <code><i>hostname</i></code>	Import the CA certificate from server <i>hostname</i> .
<code>--export</code>	Export the CA certificate from this server.

### Examples

```
tarantella security peerca --show
```

Shows the primary server's CA certificate for the array.

#### Related topics

- [Securing connections between Secure Global Desktop servers](#)
- [The tarantella security command](#)

## The tarantella security start command

### Syntax

```
tarantella security start [ --array | --server serv... ]
```

### Description

Enables secure (SSL-based) connections for all or part of an array. Secure Global Desktop will give secure connections to those users configured to require them.

To enable secure connections to a particular Secure Global Desktop server you must already have [installed an X.509 certificate](#) for that server.

If you omit both arguments, secure connections are enabled for the host on which the command is run.

Argument	Description
<code>--array</code>	Enables secure connections on all servers in the array that have a suitable X.509 certificate.
<code>--server <i>serv...</i></code>	Enables secure connections for each server named. Each <i>serv</i> is the peer DNS name of a Secure Global Desktop server in the array.

### Examples

```
tarantella security start --array
```

Enables secure connections across the array.

#### Related topics

- [Security and Secure Global Desktop](#)
- [The tarantella security stop command](#)
- [Using Secure Global Desktop with the HTTPS port through a firewall](#)

---

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## The tarantella security stop command

### Syntax

```
tarantella security stop [ --array | --server serv... ]  
                        [ --keep ]
```

### Description

Disables secure (SSL-based) connections for all or part of an array. Users configured to require secure connections are given standard connections instead, if available.

If you omit both arguments, secure connections are disabled for the host on which the command is run.

Argument	Description
<code>--array</code>	Disables secure connections on all servers in the array.
<code>--server <i>serv...</i></code>	Disables secure connections for each server named. Each <i>serv</i> is the peer DNS name of a Secure Global Desktop server in the array.
<code>--keep</code>	Specifies that any existing secure connections are preserved. If omitted, all secure connections are closed.

### Examples

```
tarantella security stop --array --keep
```

Disables security across the array, but preserves any existing secure connections.

#### Related topics

- [Security and Secure Global Desktop](#)
- [The tarantella security start command](#)
- [Using Secure Global Desktop with the HTTPS port through a firewall](#)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.



## The tarantella setup command

### Syntax

```
tarantella setup
```

### Description

Lets you change Setup options. Follow the instructions on your screen.

You can turn weekly archiving on or off. If archiving is on, you can schedule the time at which the log is created.

You can also choose to recreate the default objects and webtop links originally created at installation time. This doesn't remove any objects you've created, but it does replace any objects with the same names as the originals.

### Examples

```
tarantella setup
```

Lets you change Setup options.

#### Related topics

- [The tarantella uninstall command](#)

## The tarantella start command

### Syntax

```
tarantella start
```

### Description

Starts Secure Global Desktop services on the host, including Secure Global Desktop printing services.

This command does not start the Secure Global Desktop Web Server or Secure Global Desktop web services. Use the `tarantella webserver start` command to start these services.

### Examples

```
tarantella start
```

Starts Secure Global Desktop services.

#### Related topics

- [The tarantella stop command](#)
- [The tarantella restart command](#)

## The tarantella start cdm command

### Syntax

```
tarantella start cdm
```

### Description

Starts client drive mapping services on the Secure Global Desktop server on which the command is run.

### Examples

```
tarantella start cdm
```

Starts drive mapping services on the Secure Global Desktop server.

#### Related topics

- [Configuring client drive mapping](#)
- [Users are having problems accessing client drives](#)
- [Array properties \(array-wide\)](#)
- [The tarantella stop cdm command](#)

## The tarantella status command

### Syntax

```
tarantella status [ --summary | --byserver | --server serv | --ping [serv] ]  
                  [ --format text|xml ] [ --verbose ]
```

### Description

Reports Secure Global Desktop server information: array details, the number of webtop and emulator sessions running or suspended across the array, and how those sessions are distributed.

Subcommand	Description
<code>--summary</code>	Summarizes the information array-wide. This is the default.
<code>--byserver</code>	Displays detailed information for each server in the array.
<code>--server <i>serv</i></code>	Displays detailed information for the server <i>serv</i> (use a peer DNS name).
<code>--format text   xml</code>	Specifies the output format. The default is text.
<code>--ping [<i>serv</i>]</code>	Performs a quick health check of all array members or just one server if you specify a server.
<code>--verbose</code>	Displays the server health check and lists servers being contacted, before the command output.

### Examples

```
tarantella status
```

Summarizes information about sessions across the array.

```
tarantella status --server boston.indigo-insurance.com
```

Reports detailed status information for the Secure Global Desktop server boston.indigo-insurance.com.

## Related topics

- [The tarantella emulatorsession command](#)
- [The tarantella webtopsession command](#)
- [The tarantella query command](#)
- [What is an array?](#)

## The tarantella stop command

### Syntax

```
tarantella stop [ --force | --kill ] [ --quiet ]
```

### Description

Stops Secure Global Desktop services on the host, prompting if users are currently connected. This includes Secure Global Desktop printing services.

This command does not stop the Secure Global Desktop Web Server or Secure Global Desktop web services. Use the `tarantella webserver stop` command to stop these services.

**Note** You should never use the UNIX `kill` command to stop Secure Global Desktop services.

Option	Description
<code>--quiet</code>	Does not prompt: stops Secure Global Desktop services even if users are connected.
<code>--force</code>	Tries harder to stop Secure Global Desktop services.
<code>--kill</code>	Kills the process IDs used by Secure Global Desktop services. Only use this option if you are having difficulty stopping the Secure Global Desktop server by other means.

Stopping Secure Global Desktop services causes all emulator sessions (including suspended emulator sessions) to be terminated.

### Examples

```
tarantella stop --quiet
```

Stops Secure Global Desktop services without displaying a confirmation message if users are currently connected.

### Related topics

- The tarantella restart command
- The tarantella start command

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## The tarantella stop cdm command

### Syntax

```
tarantella stop cdm
```

### Description

Stops client drive mapping services on the Secure Global Desktop server on which the command is run.

### Examples

```
tarantella stop cdm
```

Stops drive mapping services on the Secure Global Desktop server.

### Related topics

- [Configuring client drive mapping](#)
- [Users are having problems accessing client drives](#)
- [Array properties \(array-wide\)](#)
- [The tarantella start cdm command](#)



## The tarantella tokencache command

### Syntax

```
tarantella tokencache delete | list
```

### Description

This command manipulates the token cache used by the [authentication token login authority](#). Secure Global Desktop Administrators can list and delete entries.

Subcommand	Description
<code>delete</code>	Deletes entries from the token cache.
<code>list</code>	Lists the contents of the token cache.

**Note** All commands allow the `--help` option: you can use `tarantella tokencache command --help` to get help on a specific command.

### Examples

```
tarantella tokencache delete --all
```

Deletes all entries in the token cache.

```
tarantella tokencache list --creationtime
```

Lists all entries in the token cache and the time the tokens were created.

#### Related topics

- [The authentication token login authority](#)
- [Using the authentication token login authority for automatic logins](#)



## The tarantella tokencache delete command

### Syntax

```
tarantella tokencache delete { [ --username username | --all ] [ --format  
text | xml ] }  
                               | --file file
```

### Description

Deletes entries in the token cache. The token cache is used by the [authentication token login authority](#).

Option	Description
<code>--username <i>username</i></code>	Specifies the <a href="#">TFN</a> name of the entry to be deleted.
<code>--all</code>	Deletes all entries in the cache.
<code>--format text   xml</code>	Output format (default: text).
<code>--file <i>file</i></code>	Specifies a batch file to process. The file contains one line per set of settings, each line using the above options. Use <code>--file -</code> to read from <code>stdin</code> .

### Examples

```
tarantella tokencache delete --all
```

Deletes all entries in the token cache.

#### Related topics

- [The tarantella tokencache command](#)
- [The authentication token login authority](#)
- [Using the authentication token login authority for automatic logins](#)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## The tarantella tokencache list command

### Syntax

```
tarantella tokencache list [ --creationtime ] [ --format text | xml ]
```

### Description

Lists the contents of the token cache. The token cache is used by the [authentication token login authority](#).

Option	Description
<code>--creationtime</code>	Lists the time each token in the cache was created.
<code>--format text   xml</code>	Specifies the output format (default: text).

### Examples

```
tarantella tokencache list --creationtime
```

Lists all entries in the token cache and the time the tokens were created.

#### Related topics

- [The tarantella tokencache command](#)
- [The authentication token login authority](#)
- [Using the authentication token login authority for automatic logins](#)

## The tarantella tscal command

### Syntax

```
tarantella tscal free | list | return
```

### Description

Use the `tarantella tscal` command to manage Microsoft Windows Terminal Services Client Access Licenses (CALs) for non-Windows clients.

Subcommand	Description
<code>free</code>	Frees a Terminal Services CAL for use by another non-Windows client.
<code>list</code>	Lists the Terminal Services CALs currently reserved for non-Windows clients.
<code>return</code>	Returns Terminal Services CALs to the Windows license server.

**Note** All commands allow the `--help` option: you can use `tarantella tscal subcommand --help` to get help on a specific command.

### Examples

```
tarantella tscal list
```

Lists the Terminal Services CALs currently reserved for non-Windows clients.

#### Related topics

- [Do I need to license Windows Terminal Services?](#)

## The tarantella tscal free command

### Syntax

```
tarantella tscal free [ --inuseby user | --calid id ]
```

### Description

Use the `tarantella tscal free` command to free a Microsoft Windows Terminal Services Client Access License (CAL) so that it may be used by another non-Windows client.

You can only free a CAL if the user has no emulator sessions which use Windows Terminal Services.

**Note** Freed CALs are not returned to the Windows license server.

You should not need to run this command as Secure Global Desktop automatically frees a CAL as soon as a user exits their last Windows application. However, if a Secure Global Desktop server is removed from an array or it loses contact with the array, it may still be listed as using CALs. In this situation, you can run this command to free a CAL.

If you do not use any arguments, the command frees all CALs that have no emulator sessions which use Windows Terminal Services.

If you run this command on a secondary server in a Secure Global Desktop array and the primary server is unavailable, the CAL information may not be completely accurate. This is because the primary server is responsible for updating all array members with changes to CAL information. The command warns you if the primary is unavailable.

Argument	Description
----------	-------------

<code>--inuseby user</code>	<p>Free only the CALs for a particular user where <i>user</i> is either:</p> <ul style="list-style-type: none"><li>• the <a href="#">TFN</a> name of a user or</li><li>• a wild card filter.</li></ul> <p>The <code>*</code> character is the only character you can use in a wild card filter. It represents a string of any length containing any characters. So an <code>--inuseby "*"green*"</code> argument frees only the unused CALs for users whose TFN name contains the string 'green'.</p>
<code>--calid id</code>	<p>The ID of the CAL you want to free. Use the <code>tarantella tscal list</code> command to obtain the ID of the CAL you wish to free.</p>

## Examples

```
tarantella tscal free --inuseby ".../_ens/o=Indigo Insurance/ou=Sales/cn=Elizabeth Blue"
```

Frees the CALs for Elizabeth Blue.

### Related topics

- [The tarantella tscal command](#)
- [Do I need to license Windows Terminal Services?](#)



## The tarantella tscal list command

### Syntax

```
tarantella tscal list [ --inuseby user | --inuse | --free ]
                    [ --type name ]
                    [ --format text|xml ]
```

### Description

Use the `tarantella tscal list` command to list the Microsoft Windows Terminal Services Client Access Licenses (CALs) currently reserved for use by non-Windows clients.

If you do not use any arguments, the command lists all CALs and shows whether or not they are in use.

If you run this command on a secondary server in a Secure Global Desktop array and the primary server is unavailable, the list may not be completely accurate. This is because the primary server is responsible for updating all array members with changes to CAL information. The command warns you if the primary is unavailable.

Argument	Description
<code>--inuseby <i>user</i></code>	<p>List only the CALs being used by a particular user where <i>user</i> is either:</p> <ul style="list-style-type: none"><li>• the <a href="#">TFN</a> name of a user or</li><li>• a wild card filter.</li></ul> <p>You can use the <code>tarantella emulatorsession list</code> command to determine the TFN name of a user.</p> <p>The <code>*</code> character is the only character you can use in a wild card filter. It represents a string of any length containing any characters. So an <code>--inuseby "*green*"</code> argument lists only the CALs for users whose TFN name contains the string 'green'.</p>
<code>--inuse</code>	List only the CALs that are currently in use.

<code>--free</code>	List only the CALs that are currently not in use.
<code>--type name</code>	List only the CALs that can connect to a particular type of Terminal Services server. This is either <code>WinNT4-TS-CAL</code> or <code>Win200x-TS-CAL</code> .  <b>Note</b> The name is not case sensitive.
<code>--format text   xml</code>	Specifies the output format (default: text).

## Examples

```
tarantella tscal list --free
```

Lists the CALs for non-Windows clients that are currently not in use.

### Related topics

- [The tarantella tscal command](#)
- [Do I need to license Windows Terminal Services?](#)

## The tarantella tscal return command

### Syntax

```
tarantella tscal return --free
```

### Description

Use the `tarantella tscal return` command return all free Microsoft Windows Terminal Services Client Access Licenses (CALs) to the Windows license server.

**Note** The Windows license server may not re-issue the returned CALs until approximately 90 days have elapsed since they were last in use.

Use the `tarantella tscal free` command to free a CAL so that it can be returned.

You should not need to run this command as Secure Global Desktop automatically returns a CAL if it has not been used for 90 days. However, if a Secure Global Desktop server is removed from an array, you can use this command to manually return the CALs.

Argument	Description
<code>--free</code>	Returns all free CALs to the Windows license server.

### Examples

```
tarantella tscal return --free
```

Returns all free CALs to the Windows license server.

#### Related topics

- [The tarantella tscal command](#)
- [Do I need to license Windows Terminal Services?](#)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## The tarantella uninstall command

### Syntax

```
tarantella uninstall { [ package... ] [ --purge ] | --list }
```

### Description

Removes Secure Global Desktop or parts of it from your system, or lists the installed Secure Global Desktop packages.

Option	Description
<i>package...</i>	Names individual packages to uninstall. For example, you can use this option to remove just the Secure Global Desktop X font packages or a Connectivity Pack. If <i>package</i> is omitted, the command uninstalls all Secure Global Desktop packages.
--purge	If all Secure Global Desktop packages are being removed, also removes all configuration information related to your organization. If --purge is omitted, configuration information is left intact.
--list	Lists all Secure Global Desktop packages currently installed.

### Examples

```
tarantella uninstall --purge
```

Completely uninstalls Secure Global Desktop, removing all configuration information.

```
tarantella uninstall tta3270
```

Removes the Sun Secure Global Desktop Mainframe Connectivity Pack. Configuration information is left intact.

### Related topics

- The tarantella setup command
- The tarantella version command

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## The tarantella version command

### Syntax

```
tarantella version
```

### Description

Displays the version numbers of Secure Global Desktop components installed on the host, together with information about the host.

Information about installed Secure Global Desktop components is also available on the webtop: click the ? button, in the lower-left corner of the sco/tta/standard [webtop theme](#).

### Examples

```
tarantella version
```

Displays the version numbers of installed Secure Global Desktop components.

#### Related topics

- [The tarantella uninstall command](#)

## The tarantella webserver command

### Syntax

```
tarantella webserver start | stop | restart | add_trusted_user |  
delete_trusted_user | list_trusted_users
```

### Description

Use the `tarantella webserver` command to control the Secure Global Desktop Web Server.

This command has no effect on the Secure Global Desktop server.

Subcommand	Description
<code>start</code>	Starts the Secure Global Desktop Web Server.
<code>stop</code>	Stops the Secure Global Desktop Web Server.
<code>restart</code>	Restarts the Secure Global Desktop Web Server.
<code>add_trusted_user</code>	Adds the username and password of a user that is to be trusted by the third party login authority.
<code>delete_trusted_user</code>	Deletes the username and password of a user that is to be trusted by the third party login authority.
<code>list_trusted_users</code>	Lists the usernames of the users that are to be trusted by the third party login authority.

**Note** All commands allow the `--help` option: you can use `tarantella webserver subcommand --help` to get help on a specific command.

### Examples

```
tarantella webserver start
```

Starts the Secure Global Desktop Web Server.



## Related topics

- [Introducing the Secure Global Desktop Web Server](#)

## The tarantella webserver add trusted user command

### Syntax

```
tarantella webserver add_trusted_user username
```

### Description

Adds the username and password of a user that is to be trusted for [third party authentication](#).

After you enter the *username*, Secure Global Desktop prompts you to enter the password. The password must be at least six characters long.

You must restart the Secure Global Desktop Web Server (`tarantella webserver restart`) to activate the new user.

You can't use this command to change the password of a trusted user. You must delete the trusted user first (`tarantella webserver delete_trusted_user`).

This command adds the username to the "database" of Tomcat users in `/opt/tarantella/webserver/tomcatversion/conf/tomcat-users.xml` and creates an SHA digest of the password. The user is also assigned the "SGDEExternalAuth" role, which is required to access the Secure Global Desktop external authentication web service.

### Examples

```
tarantella webserver add_trusted_user L3nNy_G0db3r
```

Adds L3nNy\_G0db3r as a trusted user.

#### Related topics

- The tarantella webserver command
- Web server/third party authentication
- Introducing web server authentication
- Trusted users and third party authentication

## The tarantella webserver delete trusted user command

### Syntax

```
tarantella webserver delete_trusted_user username
```

### Description

Deletes the username and password of a user that is to be trusted for [third party authentication](#).

You must restart the Secure Global Desktop Web Server (`tarantella webserver restart`) to deactivate the user.

This command removes the username from the "database" of Tomcat users in `/opt/tarantella/webserver/tomcatversion/conf/tomcat-users.xml`.

### Examples

```
tarantella webserver delete_trusted_user L3nNy_G0db3r
```

Deletes L3nNy\_G0db3r as a trusted user.

#### Related topics

- [The tarantella webserver command](#)
- [Web server/third party authentication](#)
- [Introducing web server authentication](#)
- [Trusted users and third party authentication](#)

## The tarantella webserver list trusted users command

### Syntax

```
tarantella webserver list_trusted_users
```

### Description

Lists the usernames of the users that are to be trusted for [third party authentication](#).

Each username is separated by a comma. The command also shows whether or not the third party authentication is currently enabled.

This command lists the usernames in the "database" of Tomcat users in `/opt/tarantella/webserver/tomcatversion/conf/tomcat-users.xml`.

### Examples

```
tarantella webserver list_trusted_users
```

Lists trusted users.

#### Related topics

- [The tarantella webserver command](#)
- [Web server/third party authentication](#)
- [Introducing web server authentication](#)
- [Trusted users and third party authentication](#)

## The tarantella webserver restart command

### Syntax

```
tarantella webserver restart [ --http ] [ --ssl ] [ --servlet ]
```

### Description

Use the `tarantella webserver restart` command to restart the Secure Global Desktop Web Server.

If you do not use any arguments, the command restarts both the Secure Global Desktop Web Server and Java™ Servlet/JavaServer Pages services.

**Note** If you restart both the Secure Global Desktop Web Server and Java Servlet/JavaServer Pages services using separate subsequent commands, you must restart the Java Servlet/JavaServer Pages services first.

Argument	Description
<code>--http</code>	Restarts the Secure Global Desktop Web Server without restarting Java Servlet/JavaServer Pages services.
<code>--servlet</code>	Restarts Java Servlet/JavaServer Pages services without restarting the Secure Global Desktop Web Server.
<code>--ssl</code>	Restarts the Secure Global Desktop Web Server with SSL enabled.

### Examples

```
tarantella webserver restart
```

Restarts the Secure Global Desktop Web Server and Java Servlet/JavaServer Pages services.

### Related topics

- Introducing the Secure Global Desktop Web Server
- The tarantella webservice command

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## The tarantella webserver start command

### Syntax

```
tarantella webserver start [ --http ] [ --ssl ] [ --servlet ]
```

### Description

Use the `tarantella webserver start` command to start the Secure Global Desktop Web Server and Java™ Servlet/JavaServer Pages services on the host.

If you do not use any arguments, the command starts both the Secure Global Desktop Web Server and Java Servlet/JavaServer Pages services.

**Note** If you start both the Secure Global Desktop Web Server and Java Servlet/JavaServer Pages services using separate subsequent commands, you must start the Java Servlet/JavaServer Pages services first.

Argument	Description
<code>--http</code>	Starts the Secure Global Desktop Web Server without starting Java Servlet/JavaServer Pages services.
<code>--servlet</code>	Starts Java Servlet/JavaServer Pages services without starting the Secure Global Desktop Web Server.
<code>--ssl</code>	Starts the Secure Global Desktop Web Server with SSL enabled.

### Examples

```
tarantella webserver start
```

Starts the Secure Global Desktop Web Server and Secure Global Desktop web services.

### Related topics



- Introducing the Secure Global Desktop Web Server
- The tarantella webservice command

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## The tarantella webserver stop command

### Syntax

```
tarantella webserver stop [ --http ] [ --servlet ]
```

### Description

Use the `tarantella webserver stop` command to stop the Secure Global Desktop Web Server and Java™ Servlet/JavaServer Pages services on the host.

If you do not use any arguments, the command stops both the Secure Global Desktop Web Server and Java Servlet/JavaServer Pages services.

Argument	Description
<code>--http</code>	Stops the Secure Global Desktop Web Server without stopping Java Servlet/JavaServer Pages services.
<code>--servlet</code>	Stops Java Servlet/JavaServer Pages services without stopping the Secure Global Desktop Web Server.

### Examples

```
tarantella webserver stop
```

Stops the Secure Global Desktop Web Server and Secure Global Desktop web services.

#### Related topics

- [Introducing the Secure Global Desktop Web Server](#)
- [The tarantella webserver command](#)



## The tarantella webtopsession command

### Syntax

```
tarantella webtopsession list | logout
```

### Description

This command allows Secure Global Desktop Administrators to list and end webtop sessions.

Subcommand	Description
list	Lists webtop sessions matching the person or server specified.
logout	Logs users out of their webtop.

**Note** All commands allow the `--help` option: you can use `tarantella webtopsession subcommand --help` to get help on a specific command.

### Examples

```
tarantella webtopsession list \  
  --server ".../_ens/o=Indigo Insurance/cn=detroit"
```

Displays details of all webtop sessions maintained by the Secure Global Desktop server detroit.

```
tarantella webtopsession logout \  
  --person ".../_ens/o=Indigo Insurance/ou=Marketing/cn=Emma Rald"
```

Logs out Emma Rald from her webtop.

### Related topics

- Understanding webtop and emulator sessions
- The tarantella status command
- The tarantella emulatorsession command

## The tarantella webtopsession list command

### Syntax

```
tarantella webtopsession list [ --person pobj | --server serv ]  
                             [ --format text|count|xml ]
```

### Description

Lists webtop sessions matching the person or server specified.

For each session, the following details display:

- Print state - shows whether the user has paused printing or not.
- Client - the IP address of the client.
- Logged in at - the timestamp when the user logged in.
- User - the [TFN name](#) of the user.
- Logged in to - the Secure Global Desktop server hosting the webtop session.
- Connection type - whether the connection is a standard or a secure connection.

**Note** The Sessions tab in [Object Manager](#) also lists the webtop sessions related to person objects, [profile objects](#) and host objects.

Option	Description
<code>--person <i>pobj</i></code>	Displays details of webtop sessions matching the person specified. Use a <a href="#">TFN name</a> for <i>pobj</i> .
<code>--server <i>serv</i></code>	Displays details of webtop sessions matching the server specified. Use a <a href="#">TFN name</a> or a peer DNS name for <i>serv</i> .
<code>--format <i>text   count   xml</i></code>	Specifies the output format (default: <code>text</code> ). Use <code>count</code> to display only the number of matching sessions.

If neither *pobj* nor *serv* is specified, the command lists all webtop sessions across the array.

[Guest users](#) and [anonymous users](#) have unique TFN names, even though they may share the same

[login profile](#). To name a guest or anonymous user, use the unique name and not the name of the profile object. For example, `.../_dns/newyork.indigo-insurance.com/_anon/1`.

**Note** Make sure you quote any object names containing spaces, for example `".../_ens/o=Indigo Insurance"`.

## Examples

```
tarantella webtopsession list \  
--server ".../_ens/o=Indigo Insurance/cn=detroit"
```

Displays details of all webtop sessions maintained by the Secure Global Desktop server detroit.

```
tarantella webtopsession list
```

Displays all webtop sessions across the array.

### Related topics

- [The tarantella webtopsession logout command](#)
- [Understanding webtop and emulator sessions](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## The tarantella webtopsession logout command

### Syntax

```
tarantella webtopsession logout --person pobj...
                                [--format text|quiet]
```

### Description

Ends the webtop session for each person specified. This has the effect of logging them out of their webtop.

**Note** The Sessions tab in [Object Manager](#) lists the webtop sessions related to person objects, [profile objects](#) and host objects and allows you to log users out of Secure Global Desktop.

Option	Description
<code>--person <i>pobj...</i></code>	Ends the webtop session of the specified person. Use a <a href="#">TFN</a> name for <i>pobj</i> .
<code>--format text   quiet</code>	Specifies the output format (default: text). With <code>--format quiet</code> , no messages are displayed and the exit code indicates the number of sessions logged out.

[Guest users](#) and [anonymous users](#) have unique TFN names, even though they may share the same [login profile](#). To name a guest or anonymous user, use the unique name and not the name of the profile object. For example, `.../_dns/newyork.indigo-insurance.com/_anon/1`.

**Note** Make sure you quote any object names containing spaces, for example `".../_ens/o=Indigo Insurance"`.

### Examples

```
tarantella webtopsession logout \  
  --person ".../_ens/o=Indigo Insurance/ou=Marketing/cn=Emma Rald"
```

Logs out Emma Rald from her webtop.



```
tarantella webtopsession logout \  
--person ../_dns/newyork.indigo-insurance.com/_anon/1
```

Ends an anonymous user's webtop session.

### Related topics

- [The tarantella webtopsession list command](#)
- [Understanding webtop and emulator sessions](#)
- [The Secure Global Desktop datastore and Tarantella Federated Naming](#)

## How does Secure Global Desktop use applets?

### If you are using the browser-based webtop

If you are using the browser-based webtop, the Sun Secure Global Desktop Client Helper is available as an applet. The applet is responsible for:

- downloading and installing the Sun Secure Global Desktop Client
- starting the Sun Secure Global Desktop Client
- managing the display engine for applications that display on the webtop or in a new browser window (in-place applications) and
- responding to instructions received from the Sun Secure Global Desktop Client, for example prompting the web browser to re-draw the screen.

The browser-based webtop also uses the [terminal emulator](#) and [X emulator](#) applets to display applications on the webtop or in a new browser window. However, these applets must not be customized or scripted. If you do want to customize or script them, you must use the *classic* webtop.

Use of these applets is optional. If you do not use them, applications can't be displayed on the webtop or in a new browser window and users have to manually refresh their webtop display.

### If you are using the classic webtop

If you are using the classic webtop, applets are used to authenticate users, render webtops, and to display applications.

The following applets are supplied:

- [Client drive mapping \(CDM\)](#)
- [Framework](#)
- [Login](#)
- [Print](#)
- [Terminal emulator](#)
- [Webtop script](#)
- [Webtop tray](#)
- [X emulator](#)

These applets are used in HTML pages, which together with graphics files make up Secure Global Desktop themes. For example, the X emulator applet `XDE.class` is used in the HTML page `xde.html` that forms part of the `sco/tta/standard` webtop theme.

You can use JavaScript to manipulate applets. This enables you to create your own custom webtops or dispense with the webtop altogether. [Launching applications from JavaScript](#) describes how users can bypass the Webtop mechanism and launch applications when they point their web browser at a particular web page.

The emulator applets let you use applet parameters to override application object attributes, if you want to. However, you can only use this method to configure X and character applications -- you can't use applet parameters to change the way a Windows application behaves.

**Note** If you create your own themes, you **must** use the `TTAAPPLET` element when you include one of the Secure Global Desktop applets.

#### Related topics

- [The TTAAPPLET tag](#)
- [Login applet](#)
- [Framework applet](#)
- [Webtop tray applet](#)
- [Webtop script applet](#)
- [Print applet](#)
- [Terminal emulator applet](#)
- [X emulator applet](#)

## The ttawebtop.cgi CGI program

**Note** The ttawebtop.cgi program can only be used to access the *classic* functionality of Secure Global Desktop.

When you click on a link for an application, Secure Global Desktop constructs a special URL containing information necessary to display and resume the application. The information is specified in a query string that is passed to the Secure Global Desktop CGI program `ttawebtop.cgi`. Secure Global Desktop uses `ttawebtop.cgi` to substitute placeholders in the HTML file containing the emulator applet with values from the query string. For example, `ttawebtop.cgi` replaces `%%OBJECTNAME%%` in `xde.html`, by obtaining the object's **TFN name** from the URL.

If you don't use the webtop to run applications, for example you use an HTML form, you need to build the URL yourself.

Use this URL syntax:

```
http://server/tarantella/cgi-bin/ttawebtop.cgi/document?  
ob=objname&aw=width&ah=height&ti=title
```

where:

- *server* is the DNS name of the Secure Global Desktop host.
- *document* is the URL of the HTML file containing the emulator applet. If you use the default HTML file and the `sco/tta/standard` webtop theme: `tarantella/resources/webtops/sco/tta/standard/locale=en-us/xde.html` (or `tde.html` for a terminal emulator).

The following information must be supplied in the query string, if not specified with applet parameter values.

Argument	Description
<code>ob=objname</code>	The object representing the application you want to run. Use a <b>TFN name</b> for <i>objname</i> .  You must URL-encode <i>objname</i> , see below for more details.

<code>aw=width</code>	The width (in pixels) of the emulator applet.
<code>ah=height</code>	The height (in pixels) of the emulator applet.
<code>ti=title</code>	The title text for the HTML page in which the emulator displays. Defaults to either "X Emulator" or "Terminal Emulator" if this argument is omitted.

## URL encoding

The URL of the HTML file containing the emulator applet must be encoded using the valid characters and format specified in [RFC1738](#). This means characters such as `<`, `>`, `"` and `/` are not allowed in the search (query string) section of the URL except in their encoded version. For example:

use ...	instead of ...
<code>%20</code>	space
<code>%22</code>	"
<code>%2f</code>	/
<code>%3c</code>	<
<code>%3e</code>	>

Some other characters, for example `&` and `=` have special meaning in the search section of a URL and, if you do not want them to be interpreted in that way, you must encode them (for example `&` becomes `%26` and `=` becomes `%3d`).

For additional security, for example to prevent cross-site scripting attacks, `ttawebtop.cgi` also substitutes the following encoded characters with their HTML character entities:

this ...	becomes ...
<code>%22</code>	<code>&amp;quot;</code> ;
<code>%26</code>	<code>&amp;amp;</code> ;
<code>%3c</code>	<code>&amp;lt;</code> ;
<code>%3e</code>	<code>&amp;gt;</code> ;

This prevents scripts encoded `%3cSCRIPT%3esome_script_code%3c%2fSCRIPT%3e` from being

returned and executed in the html passed back to the client.

## Example

```
http://newyork.indigo-insurance.com/tarantella/cgi-bin/ttawebtop.cgi/  
tarantella/  
resources/webtops/sco/tta/standard/locale=en-us/xde.html?  
ob=...%2f_ens%2fo%3dorg%2fcn%3dxterm&aw=640&ah=480&ti=xterm
```

Displays the application represented by the object `.../_ens/o=org/cn=xterm` in the `sco/tta/standard` webtop theme's `xde.html` file. The size is 640x480, and the title is "xterm".

### Related topics

- [Webtop script applet parameters](#)
- [Webtop tray applet parameters](#)

## The TTAAPPLET tag

In HTML, you use the `APPLET` tag to include applets in HTML pages. However, in Secure Global Desktop themes, a special tag called `TTAAPPLET` is used instead.

When a page containing the `TTAAPPLET` tag is requested, the `ttawebtop.cgi` cgi-bin program replaces the `TTAAPPLET` with an `APPLET` tag. This automatically generated `APPLET` tag contains all the essential information needed to display the application. This information includes:

- The Java™ archive type for the user's web browser.
- The size of applet required to display the application.
- The TCP port used to communicate with the Secure Global Desktop server.

**Note** The Secure Global Desktop applets are only used with the *classic* webtop.

## Attributes

Any attributes you specify for the `TTAAPPLET` tag appear for the automatically generated `APPLET` tag.

Also, the `archive` attribute lets you specify a [Java archive](#). Usually you should use the value `asad` here.

You can include a terminal emulator applet in an HTML page in the following way (note that you must supply other [terminal emulator applet parameters](#) such as the name of the application and the ASAD port number):

```
<ttaapplet
  code="com/tarantella/tta/client/applets/TDE.class"
  name="Tarantella Terminal Emulator">
```

`ttawebtop.cgi` replaces the `TTAAPPLET` tag with an `APPLET` tag with the name `Tarantella Terminal Emulator`, using the code found in `/opt/tarantella/var/docroot/java/com/tarantella/tta/client/applets/TDE.class`.

## CALCWIDTH and CALCHEIGHT

You can use the placeholders `%%CALCWIDTH%%` and `%%CALCHEIGHT%%` to let Secure Global Desktop

decide the correct size for the [webtop tray applet](#).

You can use these placeholders in a `TTAAPPLET` element like this:

```
<ttaapplet code="SmartIconHost"  
           width="%%CALCWIDTH%%"  
           height="%%CALCHEIGHT%%">
```

Secure Global Desktop replaces `%%CALCWIDTH%%` and `%%CALCHEIGHT%%` with the optimum width and height for the webtop tray applet, taking into account that applet's settings for the width and height of links, margins and link layout.

**Note** To allow Secure Global Desktop to calculate `%%CALCWIDTH%%` and `%%CALCHEIGHT%%` correctly, you must use a special format to specify values for certain applet parameters. If you need to use a special format for a particular applet parameter, its [parameter description](#) will tell you so.

#### Related topics

- [Login applet](#)
- [Framework applet](#)
- [Webtop tray applet](#)
- [Webtop script applet](#)
- [Print applet](#)
- [Terminal emulator applet](#)
- [X emulator applet](#)



## Launching applications from JavaScript

### Problem

You have an application that you want to publish on your internal web site. You want to bypass the Webtop mechanism and launch the application when a user points their web browser at that page.

### Solution

You can customize the way your applications are displayed by modifying whichever emulator applet page your application uses. You can use JavaScript to manipulate these applets. This allows you to create custom webtops or dispense with the webtop altogether and launch applications directly.

**Note** The Secure Global Desktop applets are only used with the *classic* webtop.

### Alternatives

- You can create a new webtop theme that automatically launches your application when a user logs in to Secure Global Desktop. Although this new theme does not bypass the Webtop, it can be configured to look and behave as if the application were being launched directly.

### Case study

Indigo Insurance wants to use JavaScript to bypass the Webtop mechanism and launch a Microsoft PowerPoint presentation when a user points their web browser at that page. The standard X emulator page, `xde.html`, should display the application.

### Solution

1. On the same web server that provides access to Secure Global Desktop, in a directory that users can access from a web browser, create a new file called `launch_my_app.html` with the following content:

```
<HTML>
<HEAD>
<TITLE>Indigo Insurance PowerPoint presentation</TITLE>

<SCRIPT LANGUAGE="JavaScript">
```

```

// Launch an application object. Arguments:
// - object's TFN name in datastore.
// - applet width in pixels.
// - applet height in pixels.
// - emulator applet page (usually xde.html or tde.html).
//
// Emulator applet pages assumed to be in
// $TTADIR/resources/webtops/

function launch(object, width, height, applet_page)
{
    // This is the page's URL.
    this_url="%%CGIPASSTHRU%%";

    // Check that it has been run through ttawebtop.cgi
    if (this_url.indexOf("ttawebtop.cgi") == -1)
    {
        document.write("Error - Must run through ttawebtop.cgi!");
        return;
    }

    // Get the Tarantella parts from the URL.
    a = this_url.split("/");
    loc = "";
    i = 3;

    while (a[i] != "cgi-bin")
    {
        loc += a[i]+"/";
        i++;
    }
    tta_url = a[0] + "://" + a[2] + "/" + loc + "cgi-bin/ttawebtop.cgi/"
+
        loc + "resources/webtops/" + applet_page;

    // Generate a timestamp based on the number of milliseconds since
    // 1/1 1970 00:00:00.
    var date = new Date();
    var timestamp = Date.parse(date);

    // Build the final URL.
    url = tta_url + "?ob=" + object

```

```

        + "&aw=" + width
        + "&ah=" + height
        + "&ts=" + timestamp;

    // Launch the application. Replace the current page.
    location.href = url;

}

</SCRIPT>

</HEAD>

<BODY>
<p>Click the button to launch the PowerPoint presentation:</p>

<FORM>
<INPUT TYPE=button VALUE="Please click"
onclick='launch("...%2F_ens%2Fo%3DIndigo Insurance%2Fcn%3Dppt_pres",
640, 480, "sco/tta/standard/locale=en-us/tde.html")'>
</FORM>

</BODY>
</HTML>

```

This example web page invites the user to press a button. When they do, they are prompted for their Secure Global Desktop username and password (and their username and password for the application server, unless Secure Global Desktop has cached this information). They will then see the presentation.

2. If you have enabled Secure Global Desktop security services, you will need to change the value of `AsadPort` in `xde.html` from 3144 to 5307. You need to do this whether your users get standard or SSL connections.
3. To launch the application, `launch_my_app.html` must be passed through the Secure Global Desktop CGI program `ttawebtop.cgi` manually, by using a URL of the form:

```

http://server.indigo-insurance.com/tarantella/cgi-bin/ttawebtop.cgi/
dest_dir/launch_my_app.html

```

where `dest_dir` is the path to the web page on the web server. If the web page's URL was `http://server.indigo-insurance.com/docs/launch_my_app.html` for example, `dest_dir` would be `docs`.

Launching the application object involves constructing the URL that Secure Global Desktop would use to launch the application from the webtop. In this example, `launch_my_app.html` employs JavaScript to parse the details of the `ppt_pres` Windows Application object and construct the URL. This process bypasses the Webtop mechanism and launches the application directly.

## Next steps

- Login themes, webtop themes and icon themes together define the look-and-feel of Secure Global Desktop. We recommend customizing your themes to completely change how your users interact with Secure Global Desktop and your applications. JavaScript constitutes just a small part of what can be accomplished using themes.

### Related topics

- [The ttawebtop.cgi CGI program](#)

## Logging in with the Secure Global Desktop applets

The following Secure Global Desktop applets have the ability to log a user in to Secure Global Desktop:

- [Client drive mapping \(CDM\) applet](#)
- [Print applet](#)
- [Terminal emulator applet](#)
- [Webtop script applet](#)
- [Webtop tray applet](#)
- [X emulator applet](#)

**Note** Although the browser-based webtop makes use of the terminal emulator and X emulator applets, the above applets can only be used to log users in to the *classic* webtop.

The login functionality depends on the presence (or absence) of the `TarantellaUsername`, `TarantellaPassword` and `LoginGUIMask` parameters for these applets. The functionality works on a "if needed" basis, that is the user is only logged in or prompted to log in, if they are not already logged in. For example, if you have several applets on the same page, only the first applet to initialize and detect that the user is not logged in will prompt for a username and password. Applets that initialize subsequently would not prompt for this information.

### When to use the parameters

If you use the standard Secure Global Desktop classic webtop, you do not need to use these parameters.

If you use a page or frameset which contain several applets that load at the same time or you define an entry point to Secure Global Desktop which does not log the user in, you must add the parameters to **every** applet on the page/frameset. You have to do this because you cannot be certain which applet will initialize first.

### How the login works

If an applet detects that the user is not logged in, it attempts to log the user in using the value of the `TarantellaUsername` parameter as the username and the value of the `TarantellaPassword` parameter as the password. If the value of the `TarantellaUsername` parameter is an empty string (""), the applet tries to log the user in **anonymously** (without a password).

If the login attempt is unsuccessful or the `TarantellaUsername` parameter is missing and bit 1 of the `LoginGUIMask` parameter is set, the user will be prompted to log in.

### Related topics

- [Framework applet](#)

## Applet parameter data types

Data type	Definition
Alignment indicator	Valid values are <code>left</code> , for left-alignment, <code>center</code> for centered and <code>right</code> for right-alignment.
Boolean	Valid values are <code>true</code> , <code>yes</code> , <code>no</code> and <code>false</code> .  The values <code>true</code> and <code>yes</code> are equivalent, as are the values <code>false</code> and <code>no</code> .
Boolean with automatic	Valid values are <code>On</code> , <code>Off</code> , and <code>Automatic</code> .
Border type	Valid values are <code>Normal</code> , <code>Indented</code> , and <code>Raised</code> .
Color definition	A decimal or hexadecimal RGB value. Hexadecimal RGB values may be specified with or without a <code>#</code> character. For example, <code>660099</code> and <code>#660099</code> both specify the color purple. Decimal RGB values must be comma-separated, for example <code>102,0,153</code> .
Color name	A color name, such as <code>red</code> , <code>white</code> or <code>PapayaWhip</code> .  Color names are resolved to RGB values by the file specified as the <code>RGB Database</code> in the <a href="#">X Protocol Engine properties</a> . By default, this file is <code>/opt/tarantella/etc/data/rgb.txt</code> .  If you supply an invalid name, Secure Global Desktop uses the color <code>black</code> .
Connection method	The mechanism used to access a server. Valid values are <code>telnet</code> , <code>rexec</code> and <code>ssh</code> .
Control code	Valid values are <code>7-bit</code> and <code>8-bit</code> .
Cursor type	Valid values are <code>Off</code> , <code>Block</code> , and <code>Underline</code> .

Font family name	<p>A font name.</p> <p>Helvetica, TimesRoman and Courier are the available font names.</p> <p><b>Note</b> Some browsers running on particular client devices may not provide all these fonts. Be aware that these font names only specify the font you would like the browser to use -- they don't guarantee the browser will use that font.</p>
Graphic filename	<p>A path to a GIF or JPEG graphics file. Specify paths relative to the login theme directory (for example, <code>/opt/tarantella/var/docroot/resources/login/sco/tta/standard/locale=en-us</code>).</p>
Host	<p>Identifies a host. You specify a host using the <b>ENS</b> name of a <b>host</b> object, a DNS name or an IP address. If you specify a DNS name or an IP address, there <b>must</b> be a corresponding host object in ENS with that DNS name or IP address as the value of its <b>Address</b> attribute.</p>
Integer	<p>A single, positive whole number.</p> <p>When used to specify widths or heights, all sizes are in pixels.</p>
Keypad mode	<p>Valid values are <code>Numeric</code> and <code>Application</code>.</p>
Layout indicator	<p>Valid values are <code>vertical</code>, to display links in a vertical column, and <code>horizontal</code>, to display links in a horizontal row.</p>
Order indicator	<p>Valid values are <code>organization</code> (same as Secure Global Desktop version 1.x), <code>alphabetical (ignores case)</code>, <code>type</code> (alphabetically by type and alphabetically within type) and <code>any</code> (unpredictable).</p>
Resumability type	<p>A resumability model. Valid values are <code>never</code>, <code>session</code> and <code>forever</code>.</p>
Root type	<p>Valid values are <code>default</code> and <code>color</code>.</p>
Scroll style	<p>Valid values are <code>Normal</code>, <code>Jump</code>, and <code>Scroll</code>.</p>
Session end type	<p>Valid values are <code>LastClient</code>, <code>WindowManager</code>, <code>WindowManagerAlone</code>, <code>LoginScript</code> and <code>NoWindows</code>.</p>



Side indicator	Valid values are <code>iconleft</code> to attach text to the left side of an icon, <code>iconright</code> to attach text to the right side of an icon, <code>icontop</code> to attach text to the top of an icon and <code>iconbottom</code> to attach text to the bottom of an icon.
Status line	Valid values are <code>None</code> , <code>Indicator</code> , <code>HostWritable</code> , <code>Standard</code> and <code>Extended</code> .
String	A sequence of alphanumeric characters.
Style indicator	Valid values are <code>plain</code> , <code>bold</code> , <code>italic</code> and <code>bold-italic</code> .
Terminal type	A type of terminal. Valid values are <code>ansi</code> , <code>vt420</code> and <code>wyse60</code> .

### Related topics

- [Login applet](#)
- [Framework applet](#)
- [Webtop tray applet](#)
- [Webtop script applet](#)
- [Print applet](#)
- [Terminal emulator applet](#)
- [X emulator applet](#)

## Client drive mapping (CDM) applet

The client drive mapping (CDM) applet allows users to access drives on their Microsoft Windows client device from applications running through Secure Global Desktop.

**Note** The CDM applet can only be used with the *classic* webtop.

- Value to use for the `TTAAPPLET` code attribute:  
`com/tarantella/tta/client/applets/CDMChannel.class`
- Used by all webtop themes supplied with Secure Global Desktop.
- [Applet parameters](#)
- Public methods:
  - [login](#)
  - [logout](#)
  - [scriptStart](#)

### Related topics

- [Login applet](#)
- [Framework applet](#)
- [Webtop tray applet](#)
- [Webtop script applet](#)
- [Print applet](#)
- [X emulator applet](#)
- [The TTAAPPLET tag](#)
- [Terminal emulator applet](#)

## Client drive mapping (CDM) applet parameters

The CDM applet has the following parameters:

Parameter	Type	Default	Description
AsadPort	Integer	No default	<p>The TCP port the CDM applet uses to communicate with the Secure Global Desktop server.</p> <p>Use the placeholder <code>%%ASADPORT%%</code> to let Secure Global Desktop supply the correct value for this parameter. You should only enter a particular value for this parameter (rather than the placeholder) if you're sure you know what you're doing.</p> <p>This parameter has no default value. Communication with the Secure Global Desktop server is only possible if you supply a valid TCP port number (or use <code>%%ASADPORT%%</code>).</p>
DebugMask	Integer	0	<p>Forces the CDM applet to log verbose debug output to the Java™ Console.</p> <p>Only use this parameter if fewer client drives than expected display and this is not due to the settings in Object Manager. The debug output shows why drives have not been found and stored in the webtop session object.</p> <p><b>Note</b> You must also enable the Java Console in the web browser to see the output.</p>

Download	String	No default	<p>Controls whether the <code>TTAWinCDM.exe</code> file is downloaded to the client or not. This parameter is only used for Netscape Browsers.</p> <p>The value of this parameter is either <code>On</code> or <code>Off</code>.</p> <p>The parameter must be <code>On</code> to give Netscape users access to full CDM functionality.</p>
HostBackgroundColor	Color definition	FFFFFF (White)	The background color.
LoginGUIMask	Integer	"2"	<p>A bitmask in the range 0 to 15 which controls the appearance of the Secure Global Desktop log in dialog.</p> <p>The bits are as follows:</p> <ul style="list-style-type: none"> <li>● Bit 1 - controls whether or not the log in dialog box displays. This is where the user enters their username and password.</li> <li>● Bit 2 - controls whether or not the ambiguous/aged password dialog box displays.</li> <li>● Bit 3 - controls whether or not the error dialog box displays.</li> <li>● Bit 4 - controls whether or not the log in dialog displays before credentials are submitted. This forces the user to click OK to log in. The values for the username and password are taken from the <code>TarantellaUsername</code> and <code>TarantellaPassword</code> parameters.</li> </ul> <p>If the value of this parameter is:</p>

			<ul style="list-style-type: none"> <li>• 0 - no dialog boxes display.</li> <li>• 15 - all dialog boxes display.</li> </ul> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>
ProxyFrame	String	"_self"	<p>The frame which the applet using this parameter runs in.</p> <p>This parameter is used by the applet that determines the proxy configuration and should not be changed unless you know what you are doing.</p>
ProxyServer	String	"DIRECT"	<p>This parameter is used to determine which proxy server, if any, should be used. If this parameter is omitted, Secure Global Desktop will ignore any proxy server configuration and attempt to connect directly to the Secure Global Desktop server.</p> <p>Use the placeholder <code>%%PROXY%%</code> to let Secure Global Desktop supply the correct value for this parameter.</p>
Scripting	Boolean	"false"	<p>This parameter is used with the <a href="#">scriptStart</a> method to release/wake-up the applet.</p> <p>If the parameter is missing or incorrect, the default of <code>false</code> is used.</p>

TarantellaPassword	String	""	<p>The password the applet uses to log in to a Secure Global Desktop server.</p> <p>If the value of the <code>TarantellaUsername</code> parameter is an empty string (""), the applet tries to log the user in <b>anonymously</b> (without a password).</p> <p>If you are concerned about security, you may not want to use this parameter. Users can see the password you supply (by viewing the page source) and they may be authenticated to Secure Global Desktop as a different user.</p> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>
TarantellaUsername	String	No default	<p>The username the applet uses to log in to a Secure Global Desktop server.</p> <p>If this parameter is used, the applet tries to log the user in to Secure Global Desktop using the values for the <code>TarantellaUsername</code> and <code>TarantellaPassword</code> parameters. If the value of this parameter is an empty string (""), the applet tries to log the user in <b>anonymously</b> (without a password).</p> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>

## Related topics

- [Client drive mapping \(CDM\) applet](#)
- [Applet parameter data types](#)

## login method

### Syntax

```
int login(String user, String password)
```

### Description

The `login` method allows users to log in to Secure Global Desktop without having to use the login applet. It can be used with the following Secure Global Desktop applets:

- [Client drive mapping \(CDM\)](#)
- [Framework](#)
- [Print](#)
- [Terminal emulator](#)
- [Webtop script](#)
- [Webtop tray](#)
- [X emulator](#)

This method requires the username and password of the user to log in.

The `login` method returns 0 if the user is successfully logged in otherwise it returns the relevant error code.

**Note** For all applets, except the Framework applet, we recommend that you only use this method if you have exhausted all other means for logging a user in and that you also use the [scriptStart](#) method.

### Examples

```
<SCRIPT Language="JavaScript">
function login(username, password)
{
    status = document.applets[0].login(username, password);

    if (status != 0)
        alert ( "Failed to log in: error " + status );
}

```



```
</SCRIPT>
```

Defines a function that logs a user in, or displays a dialog containing the error code.

Note that the applet must be present in the same web page as the `login` method.

### Related topics

- [How does Secure Global Desktop use applets?](#)

## logout method

### Syntax

```
int logout()
```

### Description

The `logout` method allows users to log out of Secure Global Desktop. It can be used with the following Secure Global Desktop applets:

- Client drive mapping (CDM)
- Framework
- Print
- Terminal emulator
- Webtop script
- Webtop tray
- X emulator

The `logout` method returns 0 if the user is successfully logged out otherwise it returns the relevant error code.

### Examples

```
<SCRIPT Language="JavaScript">
function logout()
{
    status = document.applets[0].logout();

    if (status != 0)
        alert ( "Failed to log out: error " + status );
}
</SCRIPT>
```

Defines a function that logs a user out, or displays a dialog containing the error code.

Note that the applet must be present in the same web page as the `logout` method.

## Related topics

- [How does Secure Global Desktop use applets?](#)

## scriptStart method

### Syntax

```
void scriptStart()
```

### Description

The `scriptStart` method when used with the Scripting parameter allows you to use JavaScript to release/wake-up the applet.

It can be used with the following Secure Global Desktop applets:

- [Client drive mapping \(CDM\)](#)
- [Framework](#)
- [Print](#)
- [Terminal emulator](#)
- [Webtop script](#)
- [Webtop tray](#)
- [X emulator](#)

### Examples

```
<SCRIPT Language="JavaScript">
function login()
{
    user=document.FrmLogin.FldUsername.value;
    pass=document.FrmLogin.FldPassword.value;
    app=document.applets["TTAScript"]
    if(app.login(user,pass) == 0)
    {
        app.scriptStart()
        document.applets["TTAPrint"].scriptStart()
    }
}
</SCRIPT>
```

Defines a function that loads the Print applet only when the user has logged in using JavaScript. It assumes the webtop script applet (TTAScript) and the Print applet (TTAPrint) have been embedded on a page and that both applets have the Scripting parameter set to true. The page also contains an HTML form for collecting the username and password.

### Related topics

- [How does Secure Global Desktop use applets?](#)

## Framework applet

The framework applet controls users' Secure Global Desktop sessions. For instance, if a user hasn't logged into Secure Global Desktop, it is the framework applet that detects this and displays the [login applet](#).

**Note** The framework applet can only be used with the *classic* webtop.

- Value to use for the `TTAAPPLET` `code` attribute:  
`com/tarantella/tta/client/applets/BootStrapShell.class`
- [Applet parameters](#)
- Public methods:
  - `addValue`
  - `getUserName`
  - `getValue`
  - `getWebtopFramesetURL`
  - `getWebtopURL`
  - `isLoggedIn`
  - `login`
  - `logout`
  - `removeValue`
  - `scriptStart`

### Related topics

- [Login applet](#)
- [Webtop tray applet](#)
- [Webtop script applet](#)
- [Print applet](#)
- [Terminal emulator applet](#)
- [X emulator applet](#)
- [The TTAAPPLET tag](#)



## Framework applet parameters

The [framework applet](#) has the following parameters:

Parameter	Type	Default	Description
AnonLogin	Boolean	false	<p>This parameter is used to control whether users see the standard Secure Global Desktop login page or the kiosk-style login page. Whether anonymous users can log or not is controlled by the <a href="#">Anonymous user login authority</a> setting in Array Manager.</p> <p>Use the placeholder <code>%%ANONLOGIN%%</code> to let Secure Global Desktop supply the correct value for this parameter. You should only enter a particular value for this parameter (rather than the placeholder) if you're sure you know what you're doing.</p>
AsadKeepAlive	Integer	100	<p>The interval in seconds at which "keep alive" packets are sent from the client to the server.</p>
AsadPort	Integer	No default	<p>The TCP port the framework applet uses to communicate with the Secure Global Desktop server.</p> <p>Use the placeholder <code>%%ASADPORT%%</code> to let Secure Global Desktop supply the correct value for this parameter. You should only enter a particular value for this parameter (rather than the placeholder) if you're sure you know what you're doing.</p> <p>This parameter has no default value. Communication with the Secure Global</p>



			<p>Desktop server is only possible if you supply a valid TCP port number (or use <code>%%ASADPORT%%</code>).</p>
<code>DoLogin</code>	<b>Boolean</b>	<code>true</code>	<p>This parameter is used to determine whether the applet should start the login process.</p>
<code>DoLogout</code>	<b>Boolean</b>	<code>false</code>	<p>This parameter is used to determine whether the applet should start the logout process.</p> <p>This parameter takes precedence over <code>DoLogin</code> if both parameters are simultaneously set to <code>true</code>.</p>
<code>LoginGUIMask</code>	<b>Integer</b>	<code>"2"</code>	<p>A bitmask in the range 0 to 15 which controls the appearance of the Secure Global Desktop log in dialog.</p> <p>The bits are as follows:</p> <ul style="list-style-type: none"> <li>• Bit 1 - controls whether or not the log in dialog box displays. This is where the user enters their username and password.</li> <li>• Bit 2 - controls whether or not the ambiguous/aged password dialog box displays.</li> <li>• Bit 3 - controls whether or not the error dialog box displays.</li> <li>• Bit 4 - controls whether or not the log in dialog displays before credentials are submitted. This forces the user to click OK to log in. The values for the username and password are taken from the <code>TarantellaUsername</code> and <code>TarantellaPassword</code> parameters.</li> </ul> <p>If the value of this parameter is:</p>

			<ul style="list-style-type: none"> <li>• 0 - no dialog boxes display.</li> <li>• 15 - all dialog boxes display.</li> </ul> <p><b>Note</b> This parameter is only active in <a href="#">scripting mode</a>.</p>
ProxyFrame	String	"_self"	<p>The frame which the applet using this parameter runs in.</p> <p>This parameter is used by the applet that determines the proxy configuration and should not be changed unless you know what you are doing.</p>
ProxyServer	String	"DIRECT"	<p>This parameter is used to determine which proxy server, if any, should be used. If this parameter is omitted, Secure Global Desktop will ignore any proxy server configuration and attempt to connect directly to the Secure Global Desktop server.</p> <p>Use the placeholder <code>%%PROXY%%</code> to let Secure Global Desktop supply the correct value for this parameter.</p>
Scripting	Boolean	"false"	<p>This parameter is used with the <a href="#">scriptStart</a> method to release/wake-up the applet.</p> <p>If the parameter is missing or incorrect, the default of <code>false</code> is used.</p>

TarantellaPassword	String	""	<p>The password the applet uses to log in to a Secure Global Desktop server.</p> <p>If the value of the <code>TarantellaUsername</code> parameter is an empty string (""), the applet tries to log the user in anonymously (without a password).</p> <p>If you are concerned about security, you may not want to use this parameter. Users can see the password you supply (by viewing the page source) and they may be authenticated to Secure Global Desktop as a different user.</p> <p><b>Note</b> This parameter is only active in <a href="#">scripting mode</a>.</p>
TarantellaUsername	String	No default	<p>The username the applet uses to log in to a Secure Global Desktop server.</p> <p>If this parameter is used, the applet tries to log the user in to Secure Global Desktop using the values for the <code>TarantellaUsername</code> and <code>TarantellaPassword</code> parameters. If the value of this parameter is an empty string (""), the applet tries to log the user in anonymously (without a password).</p> <p><b>Note</b> This parameter is only active in <a href="#">scripting mode</a>.</p>
TargetFrame	String	"WebtopFrame"	<p>The name of the frame into which the framework applet loads other components, such as the <a href="#">login applet</a>.</p>

URLLoginFailure	String	""	<p>The URL of the page that is to be loaded into the <code>TargetFrame</code> if the login fails.</p> <p>If this parameter is missing, the standard Secure Global Desktop login page is loaded into the <code>TargetFrame</code>. This loads the Secure Global Desktop Login applet.</p> <p>If the value of this parameter is "", no page is loaded.</p> <p><b>Note</b> This parameter is only active in <a href="#">scripting mode</a>.</p>
URLLoginSuccess	String	""	<p>The URL of the page that is to be loaded into the <code>TargetFrame</code> if the login succeeds.</p> <p>If this parameter is missing, the standard Secure Global Desktop webtop is loaded into the <code>TargetFrame</code>.</p> <p>If the value of this parameter is "", no page is loaded.</p> <p><b>Note</b> This parameter is only active in <a href="#">scripting mode</a>.</p>

## Using scripting mode to log a user in

When **both** the `DoLogin` and `DoLogout` parameters are missing or set to `false`, the framework applet is in "scripting mode". This means you can use the `TarantellaUsername`, `TarantellaPassword`, `LoginGUIMask`, `URLLoginSuccess` and `URLLoginFailure` parameters to log a user in to Secure Global Desktop.

If the `TarantellaUsername` parameter is missing and bit 1 of the `LoginGUIMask` parameter is set, the user will be prompted to log in. If the `LoginGUIMask` parameter is missing or bit 1 is not set, you can only log a user in using the `login` method.

If the `TarantellaUsername` parameter contains a username (any text), the applet tries to log the user in as that username and it uses the value of the `TarantellaPassword` parameter as the password. If the value of the `TarantellaUsername` parameter is an empty string (""), the applet tries to log the user in anonymously.

If the login succeeds and the `URLLoginSuccess` parameter is:

- a valid URL - it loads the URL into the frame specified by the `TargetFrame` parameter.
- an empty string ("") - nothing further happens.
- missing - the standard webtop is loaded into the frame specified by the `TargetFrame` parameter.

If the login fails and the `URLLoginFailure` parameter is:

- a valid URL - it loads the URL into the frame specified by the `TargetFrame` parameter.
- an empty string ("") - depending on the setting for the `LoginGUIMask` parameter, the log in dialog displays.
- missing - the standard Secure Global Desktop login page is loaded into the frame specified by the `TargetFrame` parameter.

#### Related topics

- [Framework applet](#)
- [Applet parameter data types](#)

## addValue (framework applet)

### Syntax

```
void addValue(String key, String value)
```

### Description

The `addValue` method is used to store general information. *value* is the information to store *key* is its name.

### Examples

```
<SCRIPT Language="JavaScript">
function addvalue(key, value)
{
    document.applets[0].addValue(key, value);
}
</SCRIPT>
```

Defines a function that allows you to store arbitrary information within the framework applet.

Note that the framework applet must be present in the same web page as the `addvalue` method.

#### Related topics

- [Framework applet](#)
- [removeValue \(framework applet\)](#)
- [getValue \(framework applet\)](#)

## `getUserName` (framework applet)

### Syntax

```
String getUserName()
```

### Description

The `getUserName` method returns the user's **TFN name** in the Secure Global Desktop datastore. This can be useful if you want to use JavaScript to control a user's Secure Global Desktop session.

By default, the framework applet, `BootStrapShell` resides in a frame called `StateFrame`, and has the name `Tarantella Framework`. From a document in the same browser window as the framework applet, you can call the `getUserName` method with the following JavaScript code:

```
top.StateFrame.document.applets["Tarantella Framework"].getUserName()
```

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

function whoAmI() {
    alert("You are " + top.StateFrame.document.applets["Tarantella
Framework"].getUserName());
}

</SCRIPT>

<FORM>
    <INPUT TYPE=button VALUE="Who am I?" onclick="whoAmI()">
</FORM>
```

This example adds a button beneath the links on users' webtops. When a user clicks this button, Secure Global Desktop displays a short message indicating the current user's TFN name.

Add the code to the HTML document containing the webtop tray applet (`left.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you are using the `sco/tta/standard` webtop theme. If you're using another theme, with different frame names and layouts, or different applet names, you'll need to modify the lines that invoke the `getUserName` method to access the login applet used by your new theme.

### Related topics

- [Framework applet](#)



## `getValue` (framework applet)

### Syntax

```
String getValue(String key)
```

### Description

The `getValue` method returns general information matching the *key* string.

### Examples

```
<SCRIPT Language="JavaScript">
function getvalue(key)
{
    value = document.applets[0].getValue(key);
    alert("The value is: " + value);
}
</SCRIPT>
```

Defines a function that displays a dialog showing the value of an arbitrary key stored with the framework applet.

Note that the framework applet must be present in the same web page as the `getvalue` method.

#### Related topics

- [Framework applet](#)
- [addValue \(framework applet\)](#)
- [removeValue \(framework applet\)](#)

## getWebtopFramesetURL (framework applet)

### Syntax

```
string getWebtopFramesetURL()
```

### Description

The `getWebtopFramesetURL` method is used to get the URL for the webtop frameset. To select the correct theme and locale, call this method after the user has logged in.

If this method is:

- successful, it returns the URL of the webtop frameset.
- unsuccessful, it returns an empty string ("").

### Examples

```
<SCRIPT Language="JavaScript">
function Wait()
{
    setTimeout("DoLogin()", 4000);
}
function DoLogin()
{
    var applet = top.StateFrame.document.applets["Tarantella Framework"];
    status = applet.login("", "");
    if (status == 0)
    {
        frameset = applet.getWebtopFramesetURL();
        applet.showDocument(frameset, "MainFrame");
    }
}
</SCRIPT>
```

Defines a function that returns the URL of the webtop frameset. It assumes that the Framework applet is in a frame called "StateFrame" (this is its normal location).

## Related topics

- [Framework applet](#)

## getWebtopURL (framework applet)

### Syntax

```
string getWebtopURL()
```

### Description

The `getWebtopURL` method is used to get the URL for the webtop frame. To select the correct theme and locale, call this method after the user has logged in. This method only applies to the `left.html` page.

If this method is:

- successful, it returns the URL of the webtop frame.
- unsuccessful, it returns an empty string ("").

### Examples

```
<SCRIPT Language="JavaScript">
function Wait()
{
    setTimeout("DoLogin()", 4000);
}
function DoLogin()
{
    var applet = top.StateFrame.document.applets["Tarantella Framework"];
    status = applet.login("", "");
    if (status == 0)
    {
        frameset = applet.getWebtopURL();
        applet.showDocument(frameset, "MainFrame");
    }
}
</SCRIPT>
```

Defines a function that returns the URL of the webtop frame. It assumes that the Framework applet is in a frame called "StateFrame" (this is its normal location).

## Related topics

- [Framework applet](#)

## isLoggedIn (framework applet)

### Syntax

```
int isLoggedIn()
```

### Description

Use the `isLoggedIn` method to test whether a user is logged in.

This return value...	Indicates...
0	The user is logged in.
>0	The user is not logged in.

### Examples

```
<SCRIPT Language="JavaScript">
function Wait()
{
    setTimeout("DoLogin()", 4000);
}
function DoLogin()
{
    var applet = top.StateFrame.document.applets["Tarantella Framework"];
    status = 0;
    if (!applet.isLoggedIn())
        status=applet.login("", "");
    if (status == 0)
    {
        frameset = applet.getWebtopURL();
        applet.showDocument(frameset, "MainFrame");
    }
}
</SCRIPT>
```

Defines a function that tests whether a user is logged in before returning the URL of the webtop frame. It assumes that the Framework applet is in a frame called "StateFrame" (this is its normal location).

### Related topics

- [Framework applet](#)

## removeValue (framework applet)

### Syntax

```
string removeValue(String key)
```

### Description

The `removeValue` method removes general information matching the `key` string. `removeValue` returns the value specified by `key`.

### Examples

```
<SCRIPT Language="JavaScript">
function removevalue(key)
{
    value = document.applets[0].removeValue(key);
    alert("Key " + key + " has been removed.");
}
</SCRIPT>
```

Defines a function that removes a key and value stored with the framework applet.

Note that the framework applet must be present in the same web page as the `removevalue` method.

#### Related topics

- [Framework applet](#)
- [addValue \(framework applet\)](#)
- [getValue \(framework applet\)](#)



## Login applet

The login applet controls the appearance of the screen users see when they log in to Secure Global Desktop.

The login applet is used by login themes to obtain users' usernames and passwords. This information is passed to a Secure Global Desktop server for verification to let users access Secure Global Desktop.

**Note** The login applet can only be used with the *classic* webtop.

- Value to use for the `TTAAPPLET` `code` attribute:  
`com/tarantella/tta/client/applets/LoginApp.class`
- Used by all login themes supplied with Secure Global Desktop.
- [Applet parameters](#)
- Public methods:
  - `resetNamePassword`

### Related topics

- [Framework applet](#)
- [Webtop tray applet](#)
- [Webtop script applet](#)
- [Print applet](#)
- [Terminal emulator applet](#)
- [X emulator applet](#)
- [The TTAAPPLET tag](#)

## Login applet parameters

**Note** The diagrams of the login applet's parameters may help you to understand the parameters described in this topic.

The login applet has the following parameters:

Parameter	Type	Default	Description
AsadPort	Integer	No default	<p>The TCP port the login applet uses to communicate with the Secure Global Desktop server.</p> <p>Use the placeholder <code>%%ASADPORT%%</code> to let Secure Global Desktop supply the correct value for this parameter. You should only enter a particular value for this parameter (rather than the placeholder) if you're sure you know what you're doing.</p> <p>This parameter has no default value. Communication with the Secure Global Desktop server is only possible if you supply a valid TCP port number (or use <code>%%ASADPORT%%</code>).</p>
HintsBackgroundColor	Color definition	192, 192, 192 (Grey)	The background color of the hints area.
HintsFontFamily	Font family	Browser dependent	The font used to display hints.
HintsFontSize	Integer	Browser dependent	The point size of the font used to display hints.
HintsFontStyle	Style indicator	plain	The style of font used to display hints.
HintsForegroundColor	Color definition	0, 0, 0 (Black)	The color hints appear in.

HintsHeight	Integer	0	<p>The height of the hints area.</p> <p>The hints area is used by Secure Global Desktop to display messages about the login process for the user.</p> <p>The hints area is bottom-aligned within the applet area.</p> <p>The setting 0 means Secure Global Desktop doesn't display hints to the user.</p>
LoginButtonDownImage	Graphic filename	No graphic	<p>A graphics file to represent the button when it is clicked.</p>
LoginButtonUpImage	Graphic filename	No graphic	<p>A graphics file to represent the button in its unclicked (default) state.</p> <p>If you don't specify this image, the login applet doesn't provide a login button.</p> <p>If the login button overlaps <code>MainImage</code> or <code>TitleImage</code>, <code>LoginButtonUpImage</code> obscures these images.</p>
LoginButtonX	Integer	0	<p>The gap between the login button's left edge and the title area's left side. The value 0 (the default) means the login button's left edge is aligned with the title area's left side.</p>
LoginButtonY	Integer	0	<p>The gap between the top edge of the applet area and the top of the login button. The value 0 (the default) means the top of the login button is aligned with the title area's top edge.</p>
MainImage	Graphic filename	No graphic	<p>The background image that the login applet displays.</p> <p>The login applet displays this image horizontally centered and top-aligned within the applet area. If you specify <code>MainImageY</code>, <code>MainImage</code> appears offset from the top of the applet area by this amount.</p> <p>All other elements (captions and text boxes, for example) are displayed in front of <code>MainImage</code>, except for <code>TitleImage</code>.</p>

<code>MainImageY</code>	Integer	0	The gap between the background image <code>MainImage</code> and the top of the applet area.
<code>NameCaptionCenterY</code>	Integer	0	The gap between the top edge of the applet area and the center of the username caption area. The value 0 (the default) means the center of the username caption area is aligned with the applet area's top edge.  The username caption area displays the text specified by <code>NameCaptionText</code> .
<code>NameCaptionFontFamily</code>	Font family	Browser dependent	The font used to display <code>NameCaptionText</code> .
<code>NameCaptionFontSize</code>	Integer	Browser dependent	The point size of the font used to display <code>NameCaptionText</code> .
<code>NameCaptionFontStyle</code>	Style indicator	<code>plain</code>	The style of font used to display <code>NameCaptionText</code> . <code>&lt;td&gt;</code>
<code>NameCaptionForegroundColor</code>	Color definition	<code>0,0,0 (Black)</code>	The color of <code>NameCaptionText</code> .
<code>NameCaptionHorizontalAlignment</code>	Alignment indicator	<code>left</code>	How <code>NameCaptionText</code> is aligned within the username caption area.
<code>NameCaptionText</code>	String	<code>" "</code>	The text displayed in the username caption area, for example, <code>"Username"</code> .
<code>NameCaptionWidth</code>	Integer	0	The width of the username caption area.  The username caption area doesn't clip <code>NameCaptionText</code> -- text is allowed to extend beyond the width of the username caption area. This setting is used to calculate the position of text when used with <code>NameCaptionHorizontalAlignment</code> values of <code>center</code> and <code>right</code> .  A value of 0 means the applet won't display <code>NameCaptionText</code> .

NameCaptionX	Integer	0	<p>The gap between the username caption area's left edge and the applet area's left side. The value 0 (the default) means the username caption area's left edge is aligned with the applet area's left side.</p> <p>The username caption area displays the text specified by <code>NameCaptionText</code>.</p>
NameEditBackgroundColor	Color definition	255, 255, 255 (White)	The color of the username text box's background.
NameEditCenterY	Integer	0	The gap between the top edge of the applet area and the center of the username text box. The value 0 (the default) means the center of the username text box is aligned with the applet area's top edge.
NameEditFontFamily	Font family	Browser dependent	The font used to display text in the username text box.
NameEditFontSize	Integer	Browser dependent	The point size of the font used to display text in the username text box.
NameEditFontStyle	Style indicator	plain	The style of font used to display text in the username text box.
NameEditForegroundColor	Color definition	0, 0, 0 (Black)	The color of text displayed in the username text box.
NameEditText	String	""	Any default text to appear in the username text box. By default, the username text box is empty.
NameEditWidth	Integer	0	The width of the username text box.
NameEditX	Integer	0	The gap between the username text box's left edge and the applet area's left side. The value 0 (the default) means the username text box's left edge is aligned with the applet area's left side.

<code>PasswordCaptionCenterY</code>	Integer	0	<p>The gap between the top edge of the applet area and the center of the password caption area. The value 0 (the default) means the center of the password caption area is aligned with the applet area's top edge.</p> <p>The password caption area displays the text specified by <code>PasswordCaptionText</code>.</p>
<code>PasswordCaptionFontFamily</code>	Font family	Browser dependent	The font used to display <code>PasswordCaptionText</code> .
<code>PasswordCaptionFontSize</code>	Integer	Browser dependent	The point size of the font used to display <code>PasswordCaptionText</code> .
<code>PasswordCaptionFontStyle</code>	Style indicator	plain	The style of font used to display <code>PasswordCaptionText</code> .
<code>PasswordCaptionForegroundColor</code>	Color definition	0, 0, 0 (Black)	The color of <code>PasswordCaptionText</code> .
<code>PasswordCaptionHorizontalAlignment</code>	Alignment indicator	left	How <code>PasswordCaptionText</code> is aligned within the title area.
<code>PasswordCaptionText</code>	String	""	The text displayed in the password caption area, for example, "Password".
<code>PasswordCaptionWidth</code>	Integer	0	<p>The width of the password caption area.</p> <p>The password caption area doesn't clip <code>PasswordCaptionText</code> -- text is allowed to extend beyond the width of the password caption area. This setting is used to calculate the position of text when used with <code>PasswordCaptionHorizontalAlignment</code> values of <code>center</code> and <code>right</code>.</p>

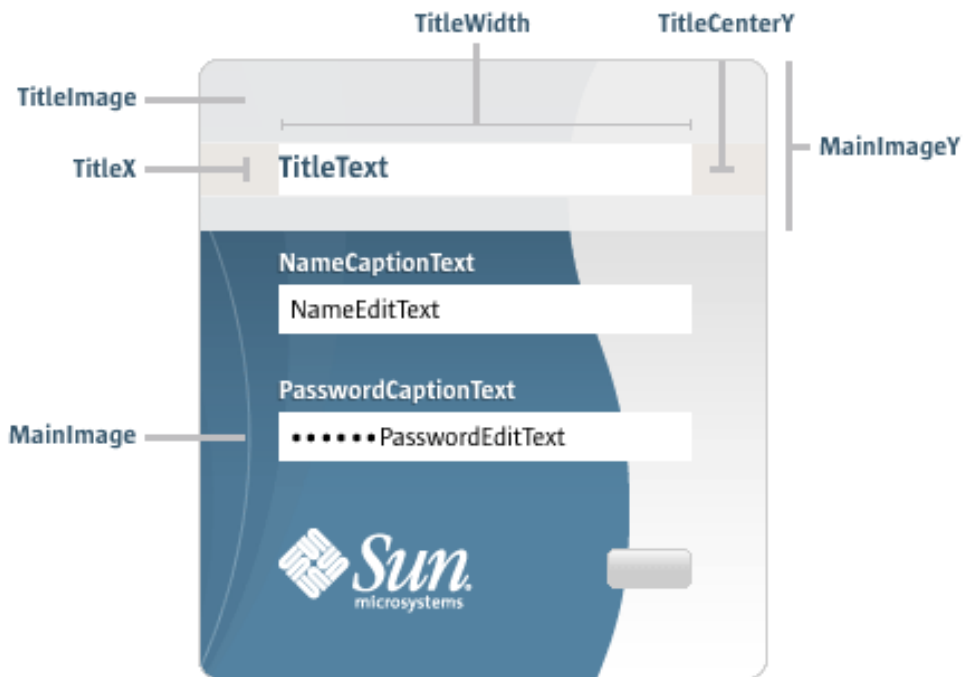
PasswordCaptionX	Integer	0	<p>The gap between the password caption area's left edge and the applet area's left side. The value 0 (the default) means the password caption area's left edge is aligned with the applet area's left side.</p> <p>The password caption area displays the text specified by <code>PasswordCaptionText</code>.</p>
PasswordEditBackgroundColor	Color definition	255, 255, 255 (White)	The color of the password text box's background.
PasswordEditCenterY	Integer	0	The gap between the top edge of the applet area and the center of the password text box. The value 0 (the default) means the center of the password text box is aligned with the applet area's top edge.
PasswordEditFontFamily	Font family	Browser dependent	The font used to display text in the password text box.
PasswordEditFontSize	Integer	Browser dependent	The point size of the font used to display text in the password text box.
PasswordEditFontStyle	Style indicator	plain	The style of font used to display text in the password text box.
PasswordEditForegroundColor	Color definition	0, 0, 0 (Black)	The color of any text displayed in the password text box.
PasswordEditText	String	""	Any default password text to appear in the password text box. The actual text will be hidden by asterisks. By default, the password text box is empty.
PasswordEditWidth	Integer	0	The width of the password text box.
PasswordEditX	Integer	0	The gap between the password text box's left edge and the applet area's left side. The value 0 (the default) means the password text box's left edge is aligned with the applet area's left side.

TargetFrame	String	"_self"	<p>The name of the frame used to display the webtop tray applet.</p> <p>Use the placeholder <code>%%TARGETFRAME%%</code> to let Secure Global Desktop supply the correct value for this parameter.</p>
TitleCenterY	Integer	0	<p>The gap between the top edge of the applet area and the center of the title area. The value 0 (the default) means the center of the title area is aligned with the applet area's top edge.</p> <p>Note that the title area only displays the text specified by <code>TitleText</code>. This setting doesn't affect how the applet displays <code>TitleImage</code>.</p>
TitleFontFamily	Font family	Browser dependent	The font used to display <code>TitleText</code> .
TitleFontSize	Integer	Browser dependent	The point size of the font used to display <code>TitleText</code> .
TitleFontStyle	Style indicator	plain	The style of font used to display <code>TitleText</code> .
TitleForegroundColor	Color definition	0,0,0 (Black)	The color of <code>TitleText</code> .
TitleHorizontalAlignment	Alignment indicator	left	How <code>TitleText</code> is aligned within the title area.
TitleImage	Graphic filename	No graphic	<p>A graphic file to be used either as a title or the background to <code>TitleText</code>.</p> <p>The login applet displays this image horizontally centered and top-aligned within the applet area.</p> <p>If you specify <code>MainImage</code>, use <code>MainImageY</code> to offset <code>MainImage</code>. If you don't, <code>MainImage</code> will obscure <code>TitleImage</code>.</p>

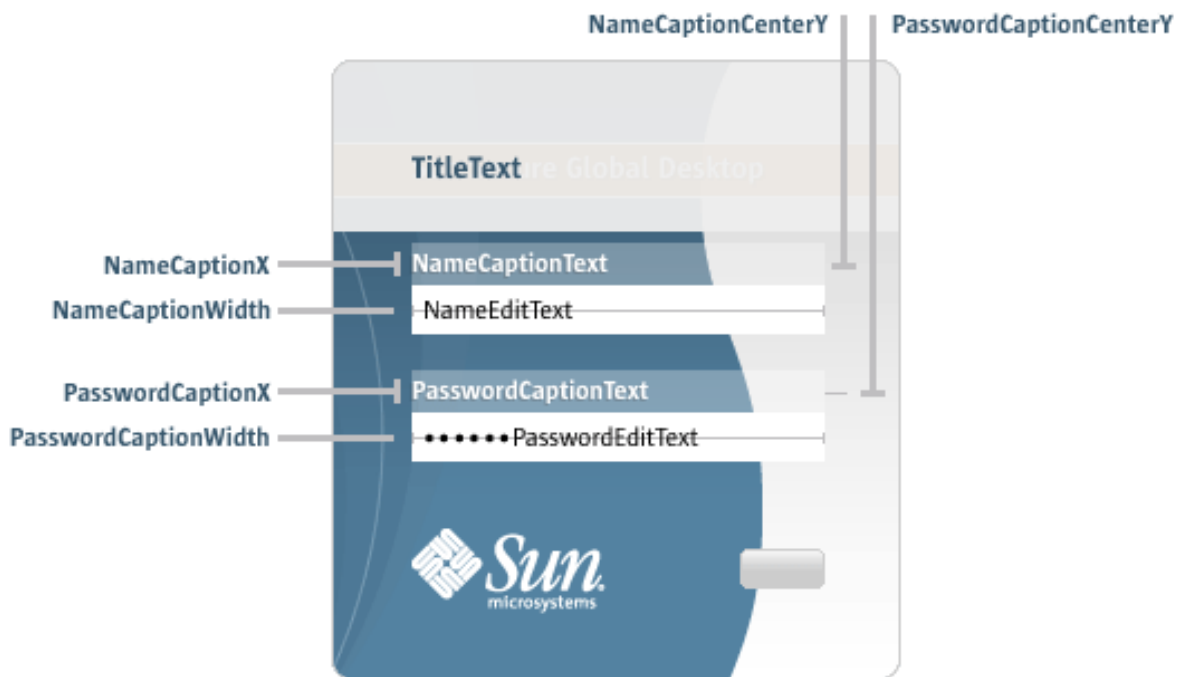


TitleText	String	""	The text displayed in the title area, for example, "Welcome to Secure Global Desktop".
TitleWidth	Integer	0	<p>The width of the title area.</p> <p>The title area doesn't clip <code>TitleText</code> -- text is allowed to extend beyond the width of the title area. This setting is used to calculate the position of text when used with <code>TitleHorizontalAlignment</code> values of <code>center</code> and <code>right</code>.</p> <p>A value of 0 means the applet won't display <code>TitleText</code>.</p> <p>Note that the title area only displays the text specified by <code>TitleText</code>. This setting doesn't affect how the applet displays <code>TitleImage</code>.</p>
TitleX	Integer	0	<p>The gap between the title area's left edge and the applet area's left side. The value 0 (the default) means the title area's left edge is aligned with the applet area's left side.</p> <p>Note that the title area only displays the text specified by <code>TitleText</code>. This setting doesn't affect how the applet displays <code>TitleImage</code>.</p>

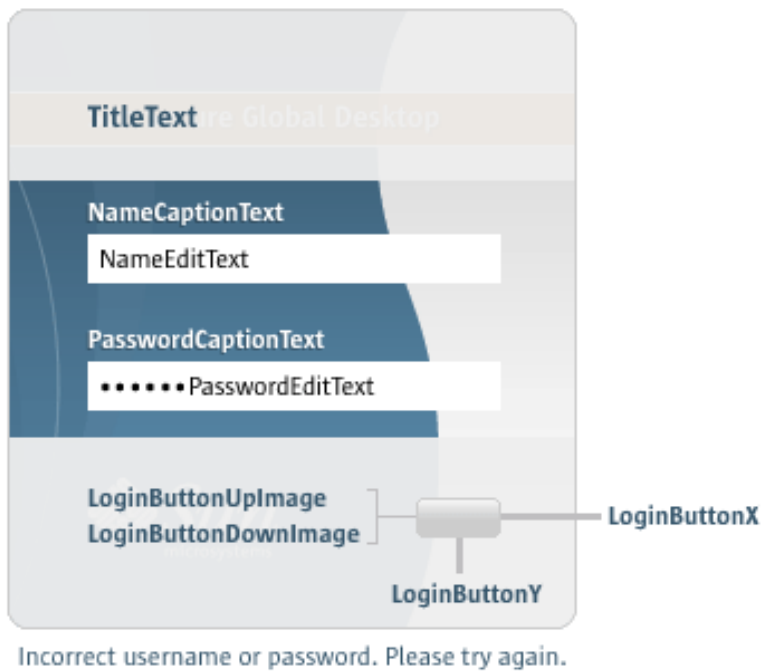
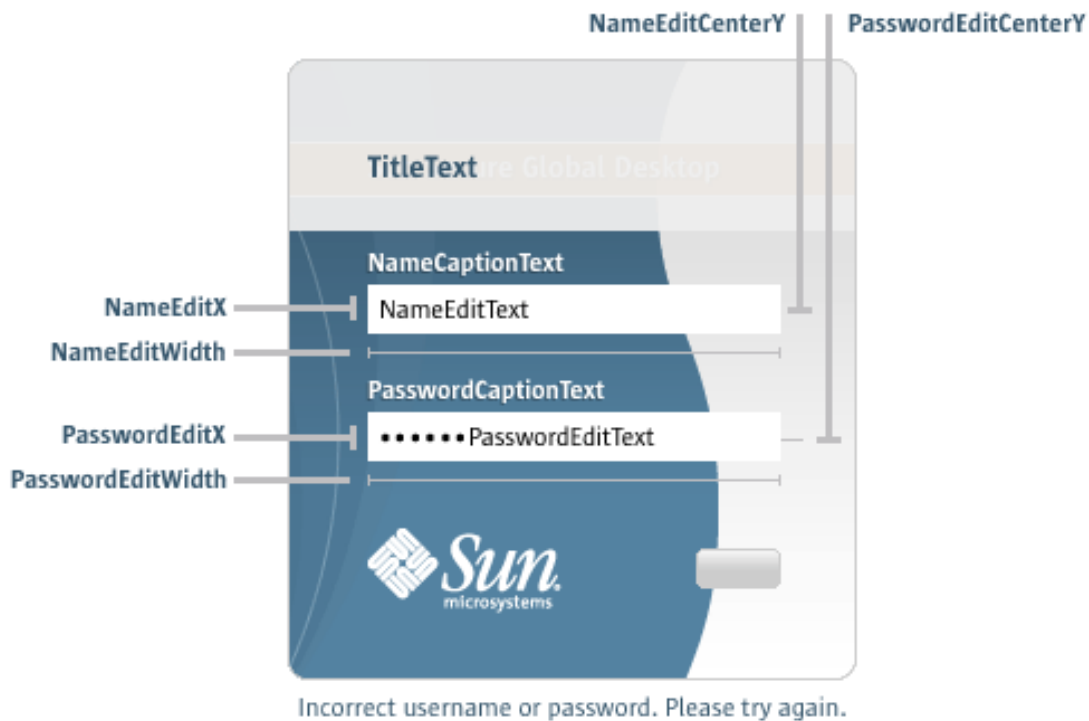
## Diagrams of the login applet's parameters



Incorrect username or password. Please try again. **HintsHeight**



Incorrect username or password. Please try again.



### Related topics

- [Login applet](#)
- [Applet parameter data types](#)

## resetNamePassword (login applet)

### Syntax

```
void resetNamePassword()
```

### Description

The `resetNamePassword` method clears any text in the login applet's Username and Password edit boxes.

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

function emptyBoxes() {
    document.applets["Tarantella Login"].resetNamePassword();
}

</SCRIPT>

<FORM>
    <INPUT TYPE=button VALUE="Clear" onclick="emptyBoxes()">
</FORM>
```

This example adds a button beneath the login applet which clears the Username and Password.

Add the code to the HTML document containing the login applet (`index.html`, in the `sco/tta/standard` login theme for example), after the `TTAAPPLET` declaration.

#### Related topics

- [Login applet](#)



## Print applet

The print applet provides status information about the Secure Global Desktop printing system and allows print jobs to be controlled.

**Note** The print applet can only be used with the *classic* webtop.

- Value to use for the `TTAAPPLET` code attribute:  
`com/tarantella/tta/client/applets/Print.class`
- Used by all webtop themes supplied with Secure Global Desktop.
- [Applet parameters](#)
- Public methods:
  - [cancelCurrentJob](#)
  - [countJobs](#)
  - [getActive](#)
  - [getEnabled](#)
  - [getPrinterName](#)
  - [getPrinterPort](#)
  - [getPrinterType](#)
  - [getPrintState](#)
  - [getUnixTempdir](#)
  - [getWindowsTempdir](#)
  - [login](#)
  - [logout](#)
  - [scriptStart](#)
  - [setActive](#)
  - [setEnabled](#)
  - [setPausedState](#)
  - [setPrinterName](#)
  - [setPrinterPort](#)
  - [setPrinterType](#)
  - [setUnixTempdir](#)
  - [setWindowsTempdir](#)

## Related topics

- [Login applet](#)
- [Framework applet](#)
- [Webtop tray applet](#)
- [Webtop script applet](#)
- [Terminal emulator applet](#)
- [X emulator applet](#)
- [The TTAAPPLET tag](#)

## Print applet parameters

The [print applet](#) has the following parameters:

Parameter	Type	Default	Description
<code>Active</code>	Boolean	<code>false</code>	Specifies whether the print applet attempts to make itself the working applet. Set this to <code>true</code> to give one print applet the priority over another. For example, if two or more print applets are <a href="#">enabled</a> in the same Secure Global Desktop session. Note that setting this value to <code>true</code> for more than one applet running simultaneously is not recommended.
<code>Enabled</code>	Boolean	<code>true</code>	Specifies whether a print applet can be the working applet. Only the working applet can be used to control and receive information about your print jobs. Use this parameter when two or more print applets are running simultaneously in the same Secure Global Desktop session. To give one print applet the priority over others when determining the working applet, set the <a href="#">Active</a> parameter to <code>true</code> . Note that if only one print applet is running it will be the working applet even if <code>Enabled</code> is set to <code>false</code> .
<code>HostBackgroundColor</code>	Color definition	<code>FFFFFF</code> (White)	The background color.



ImageGap	Integer	1	The size (in pixels) of the gap between the printing icons.
ImageSize	Integer	32	<p>The size (in pixels) of the printing icons.</p> <p>By default, Secure Global Desktop has 19 x 19 icons available.</p> <p>Note that if you're using icons larger than the default you may need to <a href="#">increase the size of the print applet</a>.</p>
LayoutStyle	Layout indicator	horizontal	How print icons appear on the webtop, either horizontally (in a row) or vertically (in a column). The order in which icons appear is always: print status, pause/restart printing, cancel printing.
LoginGUIMask	Integer	"2"	<p>A bitmask in the range 0 to 15 which controls the appearance of the Secure Global Desktop log in dialog.</p> <p>The bits are as follows:</p> <ul style="list-style-type: none"> <li>• Bit 1 - controls whether or not the log in dialog box displays. This is where the user enters their username and password.</li> <li>• Bit 2 - controls whether or not the ambiguous/aged password dialog box displays.</li> <li>• Bit 3 - controls whether or not the error dialog box displays.</li> <li>• Bit 4 - controls whether or not the log in dialog displays before credentials are submitted. This forces the user to click OK to log in. The values for the</li> </ul>

			<p>username and password are taken from the <code>TarantellaUsername</code> and <code>TarantellaPassword</code> parameters.</p> <p>If the value of this parameter is:</p> <ul style="list-style-type: none"> <li>• 0 - no dialog boxes display.</li> <li>• 15 - all dialog boxes display.</li> </ul> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>
<code>PrinterType</code>	<b>String</b>	<i>default printer type</i>	<p>The client device's default printer type. Valid values are: <code>PostScript</code>, <code>PCL</code>, <code>Text</code>. This list can be extended. The <a href="#">tta_print_converter script</a> contains more information on how to do this.</p> <p>If no value is specified, the print applet cooperates with the <code>ttaprinter.cgi</code> CGI program to determine the default printer type (the default behavior).</p>
<code>PrintImageDir</code>	<b>String</b>	<i>Java archive</i>	<p>The URL of the print applet icons.</p> <p>The URL may be absolute or relative to the HTML page containing the print applet.</p> <p>If any of icon files are missing or no URL is specified, Secure Global Desktop looks first in the <a href="#">signed Java™ archive</a> containing the print applet and then in <code>images</code> (relative to the <a href="#">print applet's codebase</a>).</p>

Scripting	Boolean	"false"	<p>This parameter is used with the <a href="#">scriptStart</a> method to release/wake-up the applet.</p> <p>If the parameter is missing or incorrect, the default of <code>false</code> is used.</p>
TarantellaPassword	String	" "	<p>The password the applet uses to log in to a Secure Global Desktop server.</p> <p>If the value of the <code>TarantellaUsername</code> parameter is an empty string (" "), the applet tries to log the user in <a href="#">anonymously</a> (without a password).</p> <p>If you are concerned about security, you may not want to use this parameter. Users can see the password you supply (by viewing the page source) and they may be authenticated to Secure Global Desktop as a different user.</p> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>

TarantellaUsername	String	No default	<p>The username the applet uses to log in to a Secure Global Desktop server.</p> <p>If this parameter is used, the applet tries to log the user in to Secure Global Desktop using the values for the <code>TarantellaUsername</code> and <code>TarantellaPassword</code> parameters. If the value of this parameter is an empty string (""), the applet tries to log the user in <b>anonymously</b> (without a password).</p> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>
UseNative	String	Default	<p>Specifies whether to use native methods for printer discovery and printing on Windows systems. Valid values are: <code>Always</code> and <code>Never</code>. If other values are specified, the applet works in its default manner, attempting to print normally (using Java technology methods), but trying native methods if that fails.</p>

### Related topics

- [Print applet](#)
- [Applet parameter data types](#)

## `cancelCurrentJob` (print applet)

### Syntax

```
boolean cancelCurrentJob()
```

### Description

The `cancelCurrentJob` method cancels the most recent print job in the Secure Global Desktop print queue. `cancelCurrentJob` reports success or failure by returning `true` or `false`.

### Examples

```
result = cancelCurrentJob();
```

Sets result to true or false depending on whether the job was successfully canceled.

#### Related topics

- [Print applet](#)

## countJobs (print applet)

### Syntax

```
int countJobs()
```

### Description

The `countJobs` method returns how many print jobs the user has available. This includes both print jobs currently printing and those in the print queue.

### Examples

```
jobs = countJobs();  
alert("Number of jobs: " + jobs);
```

Displays a dialog showing the number of jobs in the print queue for the user.

#### Related topics

- [Print applet](#)

## getActive (print applet)

### Syntax

```
boolean getActive()
```

### Description

The `getActive` method lets you determine whether the print applet attempts to make itself the **working applet** by returning `true` or `false`.

`true` means the print applet will **actively** attempt to make itself the working applet. `false` means the print applet won't make any special effort to do this (the default behavior).

### Examples

```
amIActive = getActive();
```

Determines whether the print applet attempts to make itself the working applet.

#### Related topics

- [Print applet](#)
- [setActive \(print applet\)](#)
- [setEnabled \(print applet\)](#)
- [getEnabled \(print applet\)](#)

## `getEnabled` (print applet)

### Syntax

```
boolean getEnabled()
```

### Description

The `getEnabled` method lets you check whether a print applet can be the [working applet](#).

`getEnabled` returns `true` if a print applet can be the working applet and `false` if it can't.

### Examples

```
amIEnabled = getEnabled();
```

Determines whether the print applet can be the working applet.

#### Related topics

- [Print applet](#)
- [setActive \(print applet\)](#)
- [getActive \(print applet\)](#)
- [setEnabled \(print applet\)](#)



## getPrinterName (print applet)

### Syntax

```
String getPrinterName()
```

### Description

The `getPrinterName` method lets you determine the client device's printer name. `getPrinterName` returns the string used to specify the printer name.

### Examples

```
printer = getPrinterName();  
alert("Printer is " + printer);
```

Displays a dialog showing the name of the client device's default printer.

#### Related topics

- [Print applet](#)
- [setPrinterName \(print applet\)](#)

## getPrinterPort (print applet)

### Syntax

```
String getPrinterPort()
```

### Description

The `getPrinterPort` method lets you determine the client device's printer port. `getPrinterPort` returns the string used to specify the printer port.

### Examples

```
myPort = getPrinterPort();
```

Determines the client device's printer prt.

#### Related topics

- [Print applet](#)
- [setPrinterPort \(print applet\)](#)

## getPrinterType (print applet)

### Syntax

```
String getPrinterType()
```

### Description

The `getPrinterType` method lets you determine the type of the client device's default printer. `getPrinterType` returns one of the following printer types:

- PCL
- PostScript
- Text
- Unknown

Unknown means the printer type is unavailable.

**Note** This list can be extended by modifying the file `printertypes.txt`. For more information, see [The tta\\_print\\_converter script](#).

### Examples

```
myType = getPrinterType();
```

Determines the type of the client device's default printer.

#### Related topics

- [Print applet](#)
- [Configuring Secure Global Desktop print job conversion](#)
- [setPrinterType \(print applet\)](#)



## getPrintState (print applet)

### Syntax

```
int getPrintState()
```

### Description

The `getPrintState` method returns status information about the print applet and the Secure Global Desktop printing system.

This return value...	Indicates...
0	The print applet is in the process of starting.
1	The print applet is able to print no print jobs are queued.
2	The print applet is currently printing.
3	The print applet is paused.
4	The client's default printer is offline the print applet is paused.
5	The Secure Global Desktop printing system is paused.
6	The Secure Global Desktop printing system is disabled.
7	An error has occurred. The print applet is unable to print.
8	An error has occurred in an array of Secure Global Desktop servers. The print applet is unable to print.

### Examples

```
currentState = getPrintState();  
alert("Printing state: " + currentState);
```

Displays a dialog showing the current printing state.

## Related topics

- [Print applet](#)
- [setPausedState \(print applet\)](#)

## getUnixTempDir (print applet)

### Syntax

```
String getUnixTempDir()
```

### Description

The `getUnixTempDir` method lets you determine the temporary download location for print jobs on the UNIX client device. `getUnixTempDir` returns the string used to specify the download location for print jobs.

### Examples

```
UnixTmp = getUnixTempDir();  
alert("Downloading jobs to " + UnixTmp);
```

Displays a dialog indicating where jobs are downloaded to temporarily before printing on the UNIX client device.

#### Related topics

- [Print applet](#)
- [setUnixTempDir \(print applet\)](#)
- [getWindowsTempDir \(print applet\)](#)

## getWindowsTempDir (print applet)

### Syntax

```
String getWindowsTempDir()
```

### Description

The `getWindowsTempDir` method lets you determine the temporary download location for print jobs on the Windows client device. `getWindowsTempDir` returns the string used to specify the download location for print jobs.

### Examples

```
WinTmp = getWindowsTempDir();  
alert("Downloading jobs to " + WindowsTmp);
```

Displays a dialog indicating where jobs are downloaded to temporarily before printing on the Windows client device.

#### Related topics

- [Print applet](#)
- [setWindowsTempDir \(print applet\)](#)
- [getUnixTempDir \(print applet\)](#)



## setActive (print applet)

### Syntax

```
void setActive( boolean active )
```

### Description

The `setActive` method lets you specify whether the print applet attempts to make itself the working applet.

Set `active` to `true` to give one print applet priority over another. For example, if two print applets are [enabled](#) in the same Secure Global Desktop session. Note that setting `active` to `true` for more than one applet running simultaneously is not recommended.

If `active` is set to `false`, the print applet doesn't actively attempt to make itself the working applet (the default behavior).

### Examples

```
setActive(1);
```

The print applet tries to make itself the working applet.

#### Related topics

- [Print applet](#)
- [getActive \(print applet\)](#)
- [setEnabled \(print applet\)](#)
- [getEnabled \(print applet\)](#)

## setEnabled (print applet)

### Syntax

```
void setEnabled(boolean enabled)
```

### Description

The `setEnabled` method lets you specify whether a print applet can be the working applet. Only the working applet can be used to control and receive information about your print jobs.

To allow a print applet to be the working applet, set *enabled* to `true`. Use this method when two or more print applets are running simultaneously in the same Secure Global Desktop session. To give one print applet the priority over others when determining the working applet, use the `setActive` method.

Note that if only one print applet is running it will be the working applet even if *enabled* is set to `false`.

### Examples

```
setEnabled(1);
```

The print applet can be the working applet.

#### Related topics

- [Print applet](#)
- [setActive \(print applet\)](#)
- [getActive \(print applet\)](#)
- [setEnabled \(print applet\)](#)

## setPausedState (print applet)

### Syntax

```
boolean setPausedState(boolean state)
```

### Description

The `setPausedState` method lets you pause and restart printing. Set *state* to `true` to pause and `false` to restart.

`setPausedState` reports success or failure by returning `true` or `false`.

### Examples

```
setPausedState(0);
```

Restarts printing on the client device.

#### Related topics

- [Print applet](#)
- [getPrintState \(print applet\)](#)

## setPrinterName (print applet)

### Syntax

```
boolean setPrinterName(string name)
```

### Description

The `setPrinterName` method lets you set the client device's printer name.

`setPrinterName` reports success or failure by returning `true` or `false`.

### Examples

```
setPrinterName("public_printer");
```

Sets the client device's printer name.

#### Related topics

- [Print applet](#)
- [getPrinterName \(print applet\)](#)

## setPrinterPort (print applet)

### Syntax

```
boolean setPrinterPort(String port)
```

### Description

The `setPrinterPort` method lets you set the client device's printer port. `setPrinterPort` reports success or failure by returning `true` or `false`.

**Note** This method has no effect on UNIX systems.

### Examples

```
setPrinterPort ("\\brussels\tta");
```

Sets the printer port to the Windows printer `brussels tta` (this applies only to client devices running Microsoft Windows).

#### Related topics

- [Print applet](#)
- [getPrinterPort \(print applet\)](#)

## `setPrinterType` (print applet)

### Syntax

```
boolean setPrinterType(String type)
```

### Description

The `setPrinterType` method lets you set the type of the client device's default printer. Acceptable printer *types* are:

- PCL
- PostScript
- Text

**Note** This list can be extended by modifying the file `printertypes.txt`. For more information, see [The `tta\_print\_converter` script](#).

`setPrinterType` reports success or failure by returning `true` or `false`.

If you don't use `setPrinterType`, the print applet attempts to discover the printer type itself.

### Examples

```
setPrinterType("PostScript");
```

Sets the printer type to PostScript.

#### Related topics

- [Print applet](#)
- [Configuring Secure Global Desktop print job conversion](#)
- [setPrinterType \(print applet\)](#)



## setUnixTempDir (print applet)

### Syntax

```
boolean setUnixTempDir(String dir)
```

### Description

The `setUnixTempDir` method lets you specify the download location for print jobs on the UNIX client device.

`setUnixTempDir` reports success or failure by returning `true` or `false`.

### Examples

```
setUnixTempDir( "/home/tta/tmp" );
```

Downloads print jobs to `/home/tta/tmp` before printing.

#### Related topics

- [Print applet](#)
- [getUnixTempDir \(print applet\)](#)
- [setWindowsTempDir \(print applet\)](#)



## setWindowsTempDir (print applet)

### Syntax

```
boolean setWindowsTempDir(String dir)
```

### Description

The `setWindowsTempDir` method lets you specify the download location for print jobs on the Windows client device.

`setWindowsTempDir` reports success or failure by returning `true` or `false`.

### Examples

```
setWindowsTempDir("c:\windows\temp");
```

Downloads print jobs to `c:\windows\temp` before printing.

#### Related topics

- [Print applet](#)
- [getWindowsTempDir \(print applet\)](#)
- [setUnixTempDir \(print applet\)](#)

## Terminal emulator applet

The terminal emulator applet emulates SCO Console, VT420, and Wyse 60 terminals.

**Note** Although the terminal emulator applet is used by the browser-based webtop to display applications on the webtop or in a new browser window, it must not be customized or scripted. If you want to customize or script this applet you must use the *classic* webtop.

- Value to use for the `TTAAPPLET` `code` attribute:  
`com/tarantella/tta/client/applets/TDE.class`
- Used by all webtop themes supplied with Secure Global Desktop.
- [Applet parameters](#)
- Public methods:
  - [getEmulatorState](#)
  - [getText](#)
  - [login](#)
  - [logout](#)
  - [scriptStart](#)
  - [sendKeys](#)
  - [setText](#)
  - [suspendApplication](#)

### Related topics

- [Login applet](#)
- [Framework applet](#)
- [Webtop tray applet](#)
- [Webtop script applet](#)
- [Print applet](#)
- [X emulator applet](#)
- [The TTAAPPLET tag](#)



## Terminal emulator applet parameters

The parameters in this topic may be used with the [terminal emulator applet](#).

Applet parameters take precedence over object attributes. For example, if you have an application object with its [Font Family](#) attribute set to `Courier`, but display it in an HTML page containing the terminal emulator applet with its `FontFamily` parameter set to `Helvetica`, the application will be displayed in a Helvetica font. Applet parameters that override object attributes in this way are listed in the table below with a default of "Object attribute value".

Parameter	Type	Default	Description
<code>AnswerBackMessage</code>	<a href="#">String</a>	Object attribute value	<p>A message. When an inquiry is sent from the application server to the emulator, the emulator transmits back an answerback message. The answerback message is sent automatically whenever a connection is opened.</p> <p>This parameter is only available to terminal emulators of <code>TerminalType vt420</code> and <code>wyse60</code>.</p>
<code>Appearance</code>	<a href="#">Border type</a>	Object attribute value	The appearance of the display frame's border, normal (flat), raised or indented.
<code>Application</code>	<a href="#">String</a>	Object attribute value	<p>The full pathname of the application on the application server, for instance, <code>/home/bin/scripts/shell</code>.</p> <p>To enter command line arguments, use the <code>Arguments</code> parameter.</p>
<code>ApplicationKeyMode</code>	<a href="#">Boolean</a>	Object attribute value	<p>Whether you want the application to change the codes generated by keypad keys. Otherwise, the keypad generates numbers.</p> <p>This parameter is only available to terminal emulators of <code>TerminalType wyse60</code>.</p>
<code>ApplicationServer</code>	<a href="#">Host</a>	Object attribute value	The application server you want to run the application on.
<code>Arguments</code>	<a href="#">String</a>	Object attribute value	Any command line arguments to the application.

AsadPort	Integer	No default	<p>The TCP port the terminal emulator applet uses to communicate with the Secure Global Desktop server.</p> <p>Use the placeholder <code>%%ASADPORT%%</code> to let Secure Global Desktop supply the correct value for this parameter. You should only enter a particular value for this parameter (rather than the placeholder) if you're sure you know what you're doing.</p> <p>This parameter has no default value. Communication with the Secure Global Desktop server is only possible if you supply a valid TCP port number (or use <code>%%ASADPORT%%</code>).</p>
AutoWrap	Boolean	Object attribute value	<p>Whether characters you type beyond the right-hand edge of the emulator window will appear on the following line. If not, any characters you type after you reach the right-hand edge of the emulator window will not be visible, although they will still be placed in the keyboard input buffer.</p>
BackgroundColor	Color definition	000000 (black)	<p>The background color.</p>
CodePage	String	Object attribute value	<p>The character set you want the terminal emulator to use. You can set this to 437 (International), 850 (Multilingual), 860 (Portuguese), 863 (Canadian-French), or 865 (Danish-Norwegian).</p> <p>This parameter is only available to terminal emulators of <code>TerminalType ansi</code>.</p>
Color <i>n</i>	Color definition	Object attribute value	<p>An entry in the <a href="#">color map</a>, where <i>n</i> is the number of the entry in the range 0 to 15. Use this to override entries in the color map specified in an object's <a href="#">Color Map</a> attribute.</p>
Columns	Integer	Object attribute value	<p>The number of columns in the emulator window Secure Global Desktop displays.</p> <p>Scroll bars appear if the number of lines you specify results in an emulator window larger than the terminal emulator applet.</p>
ConnectionMethod	Connection method	Object attribute value	<p>The mechanism for accessing the application server.</p> <p>The settings <code>telnet</code> and <code>rexec</code> let you use the corresponding standard UNIX communication tools.</p> <p>The setting <code>ssh</code> lets Secure Global Desktop servers communicate securely with application servers. This option is only available if you've already obtained and installed <a href="#">SSH</a>.</p>

ControlCode	Control code	Object attribute value	<p>Whether escape sequences are sent to the application server as 7-bit or 8-bit control codes.</p> <p>This parameter is only available to terminal emulators of <code>TerminalType vt420</code>.</p>
Cursor	Cursor type	Object attribute value	<p>The cursor style used in the terminal emulator.</p> <ul style="list-style-type: none"> <li>• <code>Off</code> means no cursor is shown.</li> <li>• <code>Block</code> means the cursor is a single, filled character square.</li> <li>• <code>Underline</code> means the cursor is a single underscore character.</li> </ul>
CursorKeyMode	Boolean	Object attribute value	<p>Whether you want the cursor keys to always generate cursor movement codes. Otherwise, the application can change the codes generated by the cursor keys.</p> <p>This parameter is only available to terminal emulators of <code>TerminalType vt420</code>.</p>
Environment	String	Object attribute value	<p>Any environment variable settings required by the application on the application server. Enter these in the form <code>VARIABLE=Setting</code>. To set more than one variable, use the parameter names <code>Environment1</code>, <code>Environment2</code> and so on. For example, to set three environment variables, specify them as follows:</p> <pre>&lt;PARAM NAME="Environment" VALUE="Variable=Setting"&gt; &lt;PARAM NAME="Environment1" VALUE="Variable=Setting"&gt; &lt;PARAM NAME="Environment2" VALUE="Variable=Setting"&gt;</pre>
FixedFontSize	Boolean	Object attribute value	<p>Whether Secure Global Desktop can choose the best font size to use for the given size of the terminal emulator applet.</p> <p>The value <code>true</code> indicates that Secure Global Desktop is allowed to choose the best font size. <code>false</code> indicates that Secure Global Desktop must use the font size specified by <code>FontSize</code>.</p>
FontFamily	Font name	Browser dependent	The font to use in the application.
FontSize	Integer	Browser dependent	The font's point size.
ForegroundColor	Color definition	FFFFFF (white)	The foreground color.

KeyboardMap	String	Object attribute value	The keyboard map used by the application. Secure Global Desktop provides default text-format keyboard maps. See <a href="#">Terminal Emulator Keyboard Maps</a> for more information.
KeypadMode	Keypad mode	Object attribute value	<p>The behavior of the keypad.</p> <ul style="list-style-type: none"> <li>• <code>Numeric</code> means the keypad generates numbers.</li> <li>• <code>Application</code> means the application can change the codes generated by the keypad keys.</li> </ul> <p>This parameter is only available to terminal emulators of <code>TerminalType vt420</code>.</p>
Lines	Integer	Object attribute value	<p>The number of lines in the emulator window Secure Global Desktop displays.</p> <p>Scroll bars appear if the number of lines you specify results in an emulator window larger than the terminal emulator applet.</p>
LoginGUIMask	Integer	"2"	<p>A bitmask in the range 0 to 15 which controls the appearance of the Secure Global Desktop log in dialog.</p> <p>The bits are as follows:</p> <ul style="list-style-type: none"> <li>• Bit 1 - controls whether or not the log in dialog box displays. This is where the user enters their username and password.</li> <li>• Bit 2 - controls whether or not the ambiguous/aged password dialog box displays.</li> <li>• Bit 3 - controls whether or not the error dialog box displays.</li> <li>• Bit 4 - controls whether or not the log in dialog displays before credentials are submitted. This forces the user to click OK to log in. The values for the username and password are taken from the <code>TarantellaUsername</code> and <code>TarantellaPassword</code> parameters.</li> </ul> <p>If the value of this parameter is:</p> <ul style="list-style-type: none"> <li>• 0 - no dialog boxes display.</li> <li>• 15 - all dialog boxes display.</li> </ul> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>
LoginScript	String	Object attribute value	The <a href="#">login script</a> used to log in to the application server, for example <code>unix.exp</code> .

ObjectXFN	String	""	<p>The application object's <a href="#">TFN name</a>.</p> <p>Use the placeholder <code>%%OBJECTNAME%%</code> to let Secure Global Desktop supply the correct value for this parameter. You should only enter a particular value for this parameter (rather than the placeholder) if you're sure you know what you're doing.</p>
Password	String	Password cache or prompt	<p>A password to authenticate users on an application server.</p> <p>If a valid password is specified, together with a valid username in the <code>Username</code> parameter, this username and password is used instead of any previously cached password for the authentication server.</p> <p>If you don't specify values for <b>both</b> the <code>Username</code> <b>and</b> <code>Password</code> parameters, Secure Global Desktop uses a cached username and password, if available.</p> <p>In all other circumstances (specifying a valid <code>Password</code> but not specifying a value for <code>Username</code>, for example), Secure Global Desktop prompt users for a valid username and password.</p> <p>Users can still press the Shift key when they click a link to force Secure Global Desktop to prompt for this information.</p> <p><b>Note</b> You may not want to use this parameter if you are concerned about security. Users will be able to see the password you supply here using their web browsers, and may be authenticated to the application server as another user.</p>
PromptforAuth	Boolean	false	Whether to display a dialog box that prompts the user for application server authentication.
Resumable	Resumability type	Object attribute value	<p>The <a href="#">resumability model</a> for the application.</p> <ul style="list-style-type: none"> <li>• Use <code>never</code> to specify that users can't resume the application.</li> <li>• Use <code>session</code> to specify that users can only resume the application until they log out of Secure Global Desktop.</li> <li>• Use <code>forever</code> to specify that users can always resume the application.</li> </ul>
Scottaappletheight	Integer	Object attribute value	The height of the application in pixels.
Scottaappletwidth	Integer	Object attribute value	The width of the application in pixels.



<code>Scottaattributemap</code>	String	Object attribute value	The full pathname of the <a href="#">attribute map</a> to use.
<code>Scottacolormap</code>	String	Object attribute value	Specifies the color map to use for the application. A color map maps logical colors, <code>Color_1</code> , <code>Color_2</code> and so on, to displayed colors.
<code>Scottaemulator</code>	String	No default	The type of emulation required for the application: SCO Console, VT420 or Wyse 60.  Note that not all character application attributes apply to all emulation types.
<code>Scottafullscreen</code>	Boolean	Object attribute value	Whether the application starts at the <a href="#">maximum size</a> (true) or sized according to the <a href="#">Width</a> and <a href="#">Height</a> attributes (false).
<code>Scripting</code>	Boolean	"false"	This parameter is used with the <a href="#">scriptStart</a> method to release/wake-up the applet.  If the parameter is missing or incorrect, the default of <code>false</code> is used.
<code>ScrollStyle</code>	Scroll style	Object attribute value	The scrolling speed of output sent to the terminal emulator.  <ul style="list-style-type: none"> <li>• <code>Normal</code> specifies that data appears a single line at a time.</li> <li>• <code>Jump</code> specifies that data appears several lines at a time. This is the fastest style of scrolling.</li> <li>• <code>Smooth</code> specifies that data appears one pixel at a time. This is the slowest style of scrolling.</li> </ul>
<code>StatusLine</code>	String	Object attribute value	The information displayed in the status line.  For VT420 emulators:  <ul style="list-style-type: none"> <li>• <code>None</code> specifies that no status line appears.</li> <li>• <code>Indicator</code> displays the position of the cursor and the print mode.</li> <li>• <code>HostWritable</code> displays messages from the host.</li> </ul> For Wyse 60 emulators:  <ul style="list-style-type: none"> <li>• <code>None</code> specifies that no status line appears.</li> <li>• <code>Standard</code> displays the time according to the terminal's clock, and cursor, line and column indicators.</li> <li>• <code>Extended</code> displays the Protection, Write Protect, Insert and Lock flags.</li> </ul> This parameter is only available to terminal emulators of <code>TerminalType vt420</code> and <code>wyse60</code> .

TarantellaPassword	String	""	<p>The password the applet uses to log in to a Secure Global Desktop server.</p> <p>If the value of the <code>TarantellaUsername</code> parameter is an empty string (""), the applet tries to log the user in <a href="#">anonymously</a> (without a password).</p> <p>If you are concerned about security, you may not want to use this parameter. Users can see the password you supply (by viewing the page source) and they may be authenticated to Secure Global Desktop as a different user.</p> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>
TarantellaUsername	String	No default	<p>The username the applet uses to log in to a Secure Global Desktop server.</p> <p>If this parameter is used, the applet tries to log the user in to Secure Global Desktop using the values for the <code>TarantellaUsername</code> and <code>TarantellaPassword</code> parameters. If the value of this parameter is an empty string (""), the applet tries to log the user in <a href="#">anonymously</a> (without a password).</p> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>
TerminalType	Terminal type	Object attribute value	<p>The type of terminal being emulated: <code>ansi</code>, <code>vt420</code>, or <code>wyse60</code>.</p>
TerminationFrame	String	Current frame	<p>The frame in which Secure Global Desktop displays the URL specified by <code>TerminationURL</code>.</p> <p>If no value is specified for <code>TerminationURL</code>, this parameter has no effect.</p>
TerminationURL	String	""	<p>The URL to display when the emulator session terminates. The URL is displayed in the current frame, or in the frame specified in the <code>TerminationFrame</code> parameter.</p> <p>By default, no URL is displayed when the emulator session terminates: Secure Global Desktop continues to display the HTML page containing the terminal emulator applet.</p> <p>If you're using the <code>sco/tta/standard</code> webtop theme, you could set this to <code>display.html</code> to display the "Your Webtop" page when the emulator session ends.</p>

Username	String	Password cache or prompt	<p>A username to authenticate users with on the application server. This username is used to authenticate all users who run the application.</p> <p>If a valid username is specified, together with a valid password in the <code>Password</code> parameter, this username and password is used instead of any previously cached password for the authentication server.</p> <p>If you don't specify values for <b>both the</b> <code>Username</code> <b>and</b> <code>Password</code> parameters, Secure Global Desktop uses a cached username and password, if available.</p> <p>In all other circumstances (specifying a valid <code>Username</code> but not specifying a value for <code>Password</code>, for example), Secure Global Desktop prompts users for a valid username and password.</p> <p>Users can still press the Shift key when they click a link to force Secure Global Desktop to prompt for this information.</p>
----------	--------	--------------------------	---

#### Related topics

- [Terminal emulator applet](#)
- [Applet parameter data types](#)

## getEmulatorState (terminal emulator applet)

### Syntax

```
int getEmulatorState()
```

### Description

The `getEmulatorState` method returns the status code associated with the emulator session's display engine. This allows you to determine if an emulator session is starting, running or stopped.

This return value...	Indicates...
0	The terminal emulator session is starting, but hasn't yet connected to the application server.
1	The terminal emulator session is running.
2	The terminal emulator session has disconnected from the application server.
3	An error has occurred, and the terminal emulator session has been terminated.
4	The terminal emulator session has been suspended.
5	The terminal emulator session has finished.

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

window.onerror = trapError

function trapError(message, url, line) {
    alert("There's no terminal emulator session running");
    return true
}

function getState() {
    state = top.WebtopFrame.DisplayFrame.document.applets["Tarantella
```

```

Terminal Emulator"].getEmulatorState();

switch (state) {
    case 0 :
        output = "The terminal emulator session is starting.";
        break;
    case 1 :
        output = "The terminal emulator session is running.";
        break;
    case 2 :
        output = "The terminal emulator session has disconnected.";
        break;
    case 3 :
        output = "An error has occurred.";
        break;
    case 4 :
        output = "The terminal emulator session has been suspended.";
        break;
    case 5 :
        output = "The terminal emulator session has finished.";
        break;
}

alert(output);
}

</SCRIPT>

<FORM>
    <INPUT TYPE=button VALUE="Get state" onclick="getState()">
</FORM>

```

This example adds a button beneath the links on users' webtops. When a user clicks this button, Secure Global Desktop displays a short message indicating the current state of the terminal emulator applet.

Add the code to the HTML document containing the webtop tray applet (`left.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you're using the `sco/tta/standard` webtop theme. If you're using another theme, with different frame names and layouts, or different applet names, you'll need to modify the lines that invoke the `getEmulatorState` method to access the terminal emulator applet used by your new theme.

## Related topics

- [Terminal emulator applet](#)

## getText (terminal emulator applet)

### Syntax

```
string getText( [ strLine, strCol, ] strLength)
```

### Description

This function retrieves text from the terminal emulator screen.

If you specify a position to retrieve text from (using the optional *strLine* and *strCol* parameters), this method returns *strLength* characters of text from the specified position.

If you don't specify a position in this way, this method returns *strLength* characters of text from the current cursor position.

The screen coordinates *strLine* and *strCol* coordinates are calculated from the top left corner of the emulator screen and begin at line 0, column 0.

If the position and number of characters you specify mean the method attempts to retrieve text from beyond the end of a line, this method returns an empty string. For example, in an 80 column screen, invoking the method with `getText(0,70,10)` will return the last 10 characters of the first line. However, invoking the method with `getText(0,70,11)` returns an empty string (since the method tries to retrieve the 81st column in the 80 column display).

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

function fiveByTen() {
    output = ""

    for (var line = 0 ; line < 5 ; line++) {
        current_text = document.applets["Tarantella Terminal Emulator"].
getText(line, "0", "10");
        output = output + current_text + "\n";
    }
}
```

```
    alert(output);
}

</SCRIPT>

<FORM>
  <INPUT TYPE=button VALUE="Display Text" onclick="fiveByTen()">
</FORM>
```

This example adds a button beneath the terminal emulator applet. When a user clicks the button, Secure Global Desktop displays the first 10 characters of the first 5 lines of the terminal emulator screen.

Add the code to the HTML document containing the terminal emulator applet (`tde.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you are using the `sco/tta/standard` webtop theme. If you're using another theme, with different frame names and layouts, or different applet names, you'll need to modify the line that invokes the `getText` method to access the terminal emulator applet used by your new theme.

## Related topics

- [Terminal emulator applet](#)



## `sendKey` (terminal emulator applet)

### Syntax

```
void sendKey(strKey, strModifier)
```

### Description

The `sendKey` method sends the specified action key (*strKey*) to the application being displayed by the terminal emulator applet. Action keys are keys that you can't send to applications using the `setText` method (`Return` or `Delete`, for example).

You can also specify one or more modifier keys to use (`Shift` or `Ctrl`, for example).

The action keys (*strKey*) you can send are:

- `CapsLock`
- `Delete`
- `Down`
- `End`
- `Enter`
- `Escape`
- `F1` to `F12`
- `Home`
- `Insert`
- `Left`
- `NumLock`
- `PageDown`
- `PageUp`
- `Pause`
- `PrintScreen`
- `Return`
- `Right`
- `ScrollLock`
- `Tab`

- Up

The modifier keys (*strModifier*) you can send are:

To send this modifier key...	Use this value...
No modifier key	0
Shift	1
Ctrl	2
Alt	4

To specify more than one modifier key, add values together. For example, use 5 to specify `Shift+Alt` or 7 to specify `Shift+Ctrl+Alt`.

## Examples

```
<SCRIPT LANGUAGE="JavaScript">

function pageUp() {
    document.applets["Tarantella Terminal Emulator"].sendKeys("PageUp", 0);
}

function pageDown() {
    document.applets["Tarantella Terminal Emulator"].sendKeys("PageDown", 0);
}

</SCRIPT>

<FORM>
  <INPUT TYPE=button VALUE="Scroll Page Up" onclick="pageUp()">
  <INPUT TYPE=button VALUE="Scroll Page Down" onclick="pageDown()">
</FORM>
```

This example adds two buttons beneath the terminal emulator applet. When a user clicks one of the buttons, Secure Global Desktop sends `PageUp` or `PageDown`, as appropriate.

Add the code to the HTML document containing the terminal emulator applet (`tde.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you are using the `sco/tta/standard` webtop theme. If you're using another

theme, with different frame names and layouts, or different applet names, you'll need to modify the lines that invoke the `sendKeys` method to access the terminal emulator applet used by your new theme.

### Related topics

- [Terminal emulator applet](#)

## setText (terminal emulator applet)

### Syntax

```
void setText(strString)
```

### Description

The `setText` method sends the specified text (*strString*) to the application being displayed by the terminal emulator applet.

**Note** The `sendKey` method is also available, which lets you send special action keys to applications.

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

function showDir() {
    document.applets["Tarantella Terminal Emulator"].setText("ls");
    document.applets["Tarantella Terminal Emulator"].sendKey("Return",0);
}

</SCRIPT>

<FORM>
  <INPUT TYPE=button VALUE="Directory listing" onclick="showDir()">
</FORM>
```

This example adds a button beneath the terminal emulator applet. When a user clicks the button, Secure Global Desktop sends the characters `l` and `s` followed by a carriage return to the application. If this application is a UNIX shell, these characters are interpreted as an instruction to run the `ls` UNIX command. This command lists the contents of the current directory.

This example also uses the terminal emulator applet's `sendKey` method to send the carriage return keystroke needed to run the command.

Add the code to the HTML document containing the terminal emulator applet (`tde.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you are using the `sco/tta/standard` webtop theme. If you're using another theme, with different frame names and layouts, or different applet names, you'll need to modify the lines that invoke the `setText` and `sendKey` methods to access the terminal emulator applet used by your new theme.

### Related topics

- [Terminal emulator applet](#)

## suspendApplication (terminal emulator applet)

### Syntax

```
void suspendApplication()
```

### Description

The `suspendApplication` method suspends or ends the current emulator session:

- If the application is resumable, the session is suspended.
- If the application isn't resumable, the session ends and the application exits.

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

window.onerror = trapError

function trapError(message, url, line) {
    alert("There's no terminal emulator session to stop");
    return true
}

function stopEmulator() {
    top.WebtopFrame.DisplayFrame.document.applets["Tarantella Terminal
Emulator"].suspendApplication();
    alert("Terminal emulator session stopped");
}

</SCRIPT>

<FORM>
    <INPUT TYPE=button VALUE="Stop" onclick="stopEmulator()">
</FORM>
```

This example adds a button beneath the links on users' webtops. When a user clicks this button, Secure Global Desktop stops the current terminal emulator session, if one is running.

Add the code to the HTML document containing the webtop tray applet (`left.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you are using the `sco/tta/standard` webtop theme. If you're using another theme, with different frame names and layouts, or different applet names, you'll need to modify the lines that invoke the `suspendApplication` method to access the terminal emulator applet used by your new theme.

### Related topics

- [Terminal emulator applet](#)

## Webtop script applet

The webtop script applet provides a way for you to customize the appearance of the links on a user's webtop without rendering them.

**Note** The webtop script applet can only be used with the *classic* webtop.

- Value to use for the `TTAAPPLET` code attribute:  
`com/tarantella/tta/client/applets/WebtopScriptEngine.class`
- Not used by default.
- Applet parameters
- Public methods:
  - `areObjectsInitialized`
  - `closeHierarchyLevel`
  - `getApplicationType`
  - `getCurrentIteratorElement`
  - `getIteratorForAllOpenHierarchyLevels`
  - `getIteratorForHierarchyLevel`
  - `getIteratorHasMoreElements`
  - `getLaunchWaitTimeOut`
  - `getNextIteratorElement`
  - `getNumberOfObjects`
  - `getNumberOfObjectsInGroup`
  - `getObjectClass`
  - `getObjectDisplayName`
  - `getObjectDisplayNameByName`
  - `getObjectFullName`
  - `getObjectImageName`
  - `getObjectImageNameByName`
  - `getObjectPlacement`
  - `getParentGroupName`
  - `getTotalNumberOfObjects`
  - `isApplication`
  - `isDocument`



- `isGroup`
- `isHierarchyEnabled`
- `isOpenGroup`
- `isRunning`
- `killIterator`
- `launchByObjectName`
- `launchByObjectNumber`
- `login`
- `logout`
- `openHierarchyLevel`
- `receivedEvent`
- `scriptStart`
- `setLaunchWaitTimeOut`

#### **Related topics**

- [Webtop tray applet](#)
- [Login applet](#)
- [Framework applet](#)
- [Print applet](#)
- [Terminal emulator applet](#)
- [X emulator applet](#)
- [The TTAAPPLET tag](#)

## Webtop script applet parameters

The [webtop script applet](#) has the following parameters.

Parameter	Type	Default	Description
AsadPort	Integer	No default	<p>The TCP port the webtop tray or webtop script applet uses to communicate with the Secure Global Desktop server.</p> <p>Use the placeholder <code>%%ASADPORT%%</code> to let Secure Global Desktop supply the correct value for this parameter. You should only enter a particular value for this parameter (rather than the placeholder) if you're sure you know what you're doing.</p> <p>This parameter has no default value. Communication with the Secure Global Desktop server is only possible if you supply a valid TCP port number (or use <code>%%ASADPORT%%</code>).</p>
LoginGUIMask	Integer	"2"	<p>A bitmask in the range 0 to 15 which controls the appearance of the Secure Global Desktop log in dialog.</p> <p>The bits are as follows:</p> <ul style="list-style-type: none"> <li>• Bit 1 - controls whether or not the log in dialog box displays. This is where the user enters their username and password.</li> <li>• Bit 2 - controls whether or not the ambiguous/aged password dialog box displays.</li> <li>• Bit 3 - controls whether or not the</li> </ul>

			<p>error dialog box displays.</p> <ul style="list-style-type: none"> <li>• Bit 4 - controls whether or not the log in dialog displays before credentials are submitted. This forces the user to click OK to log in. The values for the username and password are taken from the TarantellaUsername and TarantellaPassword parameters.</li> </ul> <p>If the value of this parameter is:</p> <ul style="list-style-type: none"> <li>• 0 - no dialog boxes display.</li> <li>• 15 - all dialog boxes display.</li> </ul> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>
LogoutAfter	Integer	0	<p>The number of minutes of the timeout period. If a webtop is idle for this period of time, the user is automatically logged out.</p> <p>A value of 0 means do <b>not</b> automatically log out. If the value is missing or not an integer, the value defaults to 0.</p> <p>This parameter is only available to web browsers with Java™ technology enabled. It is not available to the Sun Secure Global Desktop Native Client.</p> <p>Suspended applications are counted as running and so prevent automatic logout.</p> <p>The applet checks for running sessions every 1/20th of the timeout period and so could miss short bursts of activity and wrongly log a user out.</p> <p>The applet does not take into account</p>

			print or client drive mapping activity and so, for example, a user could be printing when they are logged out.
ObjectCount	Integer	0	<p>The number of links on the webtop.</p> <p>Use the placeholder <code>%%OBJECTCOUNT%%</code> to let Secure Global Desktop calculate the correct value for this parameter. You should only supply a particular value for this parameter (rather than the placeholder) if you're sure you know what you're doing.</p>
ObjectNumber	Integer	0	The number from which links are numbered.
Scripting	Boolean	"false"	<p>This parameter is used with the <a href="#">scriptStart</a> method to release/wake-up the applet.</p> <p>If the parameter is missing or incorrect, the default of <code>false</code> is used.</p>
TarantellaPassword	String	""	<p>The password the applet uses to log in to a Secure Global Desktop server.</p> <p>If the value of the <code>TarantellaUsername</code> parameter is an empty string (""), the applet tries to log the user in <a href="#">anonymously</a> (without a password).</p> <p>If you are concerned about security, you may not want to use this parameter. Users can see the password you supply (by viewing the page source) and they may be authenticated to Secure Global Desktop as a different user.</p> <p>See <a href="#">Logging in with the Secure Global</a></p>

			<p><a href="#">Desktop applets</a> for details of when and how you use this parameter.</p>
TarantellaUsername	String	No default	<p>The username the applet uses to log in to a Secure Global Desktop server.</p> <p>If this parameter is used, the applet tries to log the user in to Secure Global Desktop using the values for the <code>TarantellaUsername</code> and <code>TarantellaPassword</code> parameters. If the value of this parameter is an empty string (""), the applet tries to log the user in <a href="#">anonymously</a> (without a password).</p> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>
TargetFrame	String	"DisplayFrame"	<p>The name of the frame used to display document objects that don't have the <a href="#">Open In New Browser Window</a> attribute set, and for application objects that have their <a href="#">Display Using</a> attribute set to Webtop.</p> <p><code>DisplayFrame</code> (the default) is the frame used by the <code>sco/tta/standard</code> webtop theme.</p>
UseHierarchy	Boolean	false	<p>If set to true, enables webtop hierarchy mode and the scripting interface for manipulating the visible hierarchy.</p>

## Related topics

- Webtop script applet
- Webtop tray applet
- Applet parameter data types

## areObjectsInitialized (webtop script and webtop tray applets)

### Syntax

```
bool areObjectsInitialized()
```

### Description

Returns `true` when the webtop script or webtop tray applet is fully loaded. If not fully loaded, it returns `false`. You can use this to ensure that you only call the webtop applet's methods once the applet is loaded. If you call an applet's methods before it is loaded, you get JavaScript errors.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
var value = null;
var loop = 0;
var webtopApplet = top.WebtopFrame.HiddenFrame.WebtopTray.document.applets
["Tarantella Webtop"];

while (value == null) {
    value = webtopApplet.areObjectsInitialized();
    loop++;
    if ( loop > 10000 ) break;
}

if ( value == false) {
    alert("An error occurred. The webtop tray applet isn't available");
}
```

The code waits until the webtop applet is available, displaying an error message if it isn't available within a reasonable time.

You could use code similar to this to replace the webtop with a new mechanism of your own.

**Note** The code doesn't form a complete example. You'll need to add your own code and adapt it to

produce a working example.

### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)



## closeHierarchyLevel (webtop script and webtop tray applets)

### Syntax

```
String closeHierarchyLevel(String location)
```

### Description

For hierarchical webtops, closes a level of the hierarchy, freeing up the resources associated with that level.

For *location*, use the full [TFN name](#) of the group to close.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
applet.closeHierarchyLevel("../_ens/o=Indigo Insurance/cn=Applications");
```

Closes the Application group, freeing up resources.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)
- [openHierarchyLevel \(webtop script and webtop tray applets\)](#)

## `getApplicationType` (webtop script and webtop tray applets)

### Syntax

```
String getApplicationType(String objectName)
```

### Description

Returns the object type of *objectName*. This can be "DOCUMENTTYPE", "GROUPTYPE", or "APPLICATIONTYPE".

For *objectName*, use the full [TFN name](#) of an object on the user's webtop.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
objType = applet.getApplicationType("../_ens/o=Indigo Insurance/ou=Finance/  
ou=Administration/cn=Phone List");  
alert("The object type is: " + objType);
```

Obtains and displays the type of the Phone List object.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)

## `getCurrentIteratorElement` (webtop script and webtop tray applets)

### Syntax

```
String getCurrentIteratorElement(String iteratorHandle)
```

### Description

Returns the name of the current object found in the iterator identified by the iterator handle.

*iteratorHandle* is the handle to an iterator previously created with one of the `getIterator` methods.

Repeated calls to `getCurrentIteratorElement` will always return the same object name.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
current = applet.getCurrentIteratorElement(iterator);
```

Returns the current object for the iterator handle named.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)
- [openHierarchyLevel](#) (webtop script and webtop tray applets)
- [getNextIteratorElement](#) (webtop script and webtop tray applets)
- [getIteratorHasMoreElements](#) (webtop script and webtop tray applets)
- [getIteratorForHierarchyLevel](#) (webtop script and webtop tray applets)

- `getIteratorForAllOpenHierarchyLevels`  
(webtop script and webtop tray applets)
- `killIterator` (webtop script and webtop tray applets)

[Secure Global Desktop Administration Guide](#) > [Applets](#) > `getIteratorForAllOpenHierarchyLevels` (webtop script and webtop tray applets)

## `getIteratorForAllOpenHierarchyLevels` (webtop script and webtop tray applets)

### Syntax

```
String getIteratorForAllOpenHierarchyLevels(String iteratorContentType)
```

### Description

Returns a handle to an iterator that can parse all the objects the webtop script applet currently knows about. This is useful if you want to manipulate multiple webtop objects.

*iteratorContentType* is the type of object to be parsed using the iterator, and may be "GROUPTYPE", "ALLTYPE", "APPLICATIONTYPE", or "DOCUMENTTYPE".

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
iterator = applet.getIteratorForAllOpenHierarchyLevels("ALLTYPE");  
  
while (applet.getIteratorHasMoreElements(iterator) == "TRUE") {  
    current = applet.getNextIteratorElement(iterator);  
}
```

Shows how you can iterate through all objects on all open levels in sequential order.

**Note** The code doesn't form a complete example. You'll need to add your own code and adapt it to produce a working example.

### Related topics

- Webtop script applet
- Webtop tray applet
- openHierarchyLevel (webtop script and webtop tray applets)
- getCurrentIteratorElement (webtop script and webtop tray applets)
- getNextIteratorElement (webtop script and webtop tray applets)
- getIteratorHasMoreElements (webtop script and webtop tray applets)
- getIteratorForHierarchyLevel (webtop script and webtop tray applets)
- killIterator (webtop script and webtop tray applets)

## `getIteratorForHierarchyLevel` (webtop script and webtop tray applets)

### Syntax

```
String getIteratorForHierarchyLevel(String levelName,  
                                   String iteratorContentType)
```

### Description

Returns a handle to an iterator that allows objects on a particular application level to be parsed in sequential order. This is useful if you want to manipulate multiple webtop objects in sequential order.

*levelName* is the full [TFN name](#) name of the application level for which an iterator is required.

*iteratorContentType* is the type of object to be parsed using the iterator, and may be "GROUPTYPE", "ALLTYPE", "APPLICATIONTYPE", or "DOCUMENTTYPE".

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
iterator = applet.getIteratorForHierarchyLevel("../_ens/o=Indigo Insurance/  
cn=Applications", "ALLTYPE");  
  
while (applet.getIteratorHasMoreElements(iterator) == "TRUE"){  
    current = applet.getNextIteratorElement(iterator);  
}
```

Iterates through all objects in the Applications group, previously opened with [openHierarchyLevel](#).

**Note** The code doesn't form a complete example. You'll need to add your own code and adapt it to produce a working example.

### Related topics

- Webtop script applet
- Webtop tray applet
- openHierarchyLevel (webtop script and webtop tray applets)
- getCurrentIteratorElement (webtop script and webtop tray applets)
- getNextIteratorElement (webtop script and webtop tray applets)
- getIteratorHasMoreElements (webtop script and webtop tray applets)
- getIteratorForAllOpenHierarchyLevels (webtop script and webtop tray applets)
- killIterator (webtop script and webtop tray applets)



## `getIteratorHasMoreElements` (webtop script and webtop tray applets)

### Syntax

```
String getIteratorHasMoreElements(String iteratorHandle)
```

### Description

Returns "TRUE" if the iterator identified by the iterator handle contains more object names otherwise, it returns "FALSE".

*iteratorHandle* is the handle to an iterator previously created with one of the `getIterator` methods.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
while (applet.getIteratorHasMoreElements(iterator) == "TRUE") {  
    current = applet.getNextIteratorElement(iterator);  
}
```

Iterates through all elements, checking each time if any more elements remain.

### Related topics

- Webtop script applet
- Webtop tray applet
- openHierarchyLevel (webtop script and webtop tray applets)
- getCurrentIteratorElement (webtop script and webtop tray applets)
- getNextIteratorElement (webtop script and webtop tray applets)
- getIteratorForHierarchyLevel (webtop script and webtop tray applets)
- getIteratorForAllOpenHierarchyLevels (webtop script and webtop tray applets)
- killIterator (webtop script and webtop tray applets)

## `getLaunchWaitTimeOut` (webtop script and webtop script applets)

### Syntax

```
void getLaunchWaitTimeOut(int newTimeOut)
```

### Description

Returns the maximum length of time in seconds to wait before attempting a new launch, which may have been previously set with `setLaunchWaitTimeOut`.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
timeout = applet.getLaunchWaitTimeOut();
```

Sets the variable `timeout` to the current maximum launch timeout.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)
- [setLaunchWaitTimeOut](#) (webtop script and webtop tray applets)

## getNextIteratorElement (webtop script and webtop tray applets)

### Syntax

```
String getNextIteratorElement(String iteratorHandle)
```

### Description

Returns the name of the next object found in the iterator identified by *iteratorHandle*.

*iteratorHandle* is the handle to an iterator previously created with one of the `getIterator` methods.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
while (applet.getIteratorHasMoreElements(iterator) == "TRUE"){  
    current = applet.getNextIteratorElement(iterator);  
}
```

Iterates through all elements in sequential order.

**Note** The code doesn't form a complete example. You'll need to add your own code and adapt it to produce a working example.

### Related topics

- Webtop script applet
- Webtop tray applet
- openHierarchyLevel (webtop script and webtop tray applets)
- getCurrentIteratorElement (webtop script and webtop tray applets)
- getIteratorHasMoreElements (webtop script and webtop tray applets)
- getIteratorForHierarchyLevel (webtop script and webtop tray applets)
- getIteratorForAllOpenHierarchyLevels (webtop script and webtop tray applets)
- killIterator (webtop script and webtop tray applets)

## `getNumberOfObjects` (webtop script and webtop tray applets)

### Syntax

```
int getNumberOfObjects()
```

### Description

Returns the number of links on the webtop.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

function showLinkCount() {
    alert("There are " + document.applets["Tarantella Webtop"].
getNumberOfObjects()
        + " links on the webtop");
}

</SCRIPT>

<FORM>
    <INPUT TYPE=button VALUE="How many links?" onclick="showLinkCount()">
</FORM>
```

This example adds a button beneath the links on users' webtops. When a user clicks this button, Secure Global Desktop displays a message containing the number of links on the webtop.

Add the code to the HTML document containing the webtop tray applet (`left.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you are using the `sco/tta/standard` webtop theme. If you're using another theme, with different frame names and layouts, or different applet names, you'll need to modify the line that invokes the `getNumberOfObjects` method to access the webtop tray applet used by your new

theme.

### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)

## `getNumberOfObjectsInGroup` (webtop script and webtop tray applets)

### Syntax

```
int getNumberOfObjectsInGroup (String groupName,  
                               String objectType)
```

### Description

Returns a count of objects from an open application group.

*groupName* is the full [TFN name](#) of the application group from which to obtain the count.

*objectType* defines which objects are included in the count, and may be "GROUPTYPE", "ALLTYPE", "APPLICATIONTYPE" or "DOCUMENTTYPE".

**Note** To use this method, the `UseHierarchy` parameter must be set to `true`.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
obNumber = applet.getNumberOfObjectsInGroup("../_ens/o=Indigo Insurance/  
cn=Applications", "DOCUMENTTYPE");  
alert("The number of documents in the Applications group is: " + obNumber);
```

Displays the number of documents in the Applications group.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)





## getObjectClass (webtop script and webtop tray applets)

### Syntax

```
String getObjectClass(String objectName)
```

### Description

Returns a string representing the application type. This string can be "scottahtmldocument", "scottacharacterapplication", "scottaxapplication", "scottawindowsapplication", "scottawebapplication", or "scottaGroupOfNames".

*objectName* is the full [TFN name](#) of an object on the user's webtop.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
objType = applet.getObjectClass("../_ens/o=Indigo Insurance/ou=Finance/  
ou=Administration/cn=Phone List");  
alert("The application type is: " + objType);
```

Displays a dialog indicating the type of the Phone List object.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)

## getObjectDisplayName (webtop script and webtop tray applets)

### Syntax

```
String getObjectDisplayName(int objectNumber)
```

### Description

Returns the name Secure Global Desktop displays as part of the link if the webtop tray applet's `ShowIcon` parameter has the value `true`.

*objectNumber* specifies a link on the webtop. The value `0` specifies the first link on the webtop, `1` the second and so on. The method returns an error if *objectNumber* is greater than the number of links on the webtop.

**Note** You can use the applet's `ObjectNumber` parameter to change the number from which links are numbered (default is zero).

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

function showLinkLabels() {
    output = "The webtop tray contains these links:\n";
    count_links = document.applets["Tarantella Webtop"].getNumberOfObjects();

    for (var link = 0 ; link < count_links ; link++) {
        obj_name = document.applets["Tarantella Webtop"].getObjectDisplayName
(link);
        output = output + "\t" + obj_name + "\n";
    }

    alert(output);
}
```

```
</SCRIPT>

<FORM>
  <INPUT TYPE=button VALUE="Which links?" onclick="showLinkLabels()">
</FORM>
```

This example adds a button beneath the links on users' webtops. When a user clicks this button, Secure Global Desktop displays the names of all objects which have a link on the webtop.

Add the code to the HTML document containing the webtop tray applet (`left.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you are using the `sco/tta/standard` webtop theme. If you're using another theme, with different frame names and layouts, or different applet names, you'll need to modify the lines that invoke the `getObjectDisplayName` and `getNumberOfObjects` methods to access the webtop tray applet used by your new theme.

### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)
- [getObjectDisplayNameByName \(webtop script and webtop tray applets\)](#)

## getObjectDisplayNameByName (webtop script and webtop tray applets)

### Syntax

```
String getObjectDisplayNameByName(String objectName)
```

### Description

Returns the name Secure Global Desktop displays as part of the link if the webtop tray applet's `ShowIcon` parameter has the value `true`.

*objectName* is the full [TFN name](#) name of an application on the user's webtop.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
disName = applet.getObjectDisplayNameByName("../_ens/o=Indigo Insurance/  
ou=Finance/ou=Administration/cn=Phone List");  
alert("The application display name is: " + disName);
```

Displays a dialog containing the display name of the Phone List object.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)
- [getObjectDisplayName \(webtop script and webtop tray applets\)](#)

## getObjectFullName (webtop script and webtop tray applets)

### Syntax

```
String getObjectFullName(int objectNumber)
```

### Description

Returns the [TFN name](#) of the object represented by the specified link.

*objectNumber* specifies a link on the webtop. The value 0 specifies the first link on the webtop, 1 the second and so on. The method returns an error if *objectNumber* is greater than the number of links on the webtop.

**Note** You can use the applet's `ObjectNumber` parameter to change the number from which links are numbered (default is zero).

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

function showLinkTFN() {
    output = "The webtop tray contains links to these objects:\n";
    count_links = document.applets["Tarantella Webtop"].getNumberOfObjects();

    for (var link = 0 ; link < count_links ; link++) {
        tfn_name = document.applets["Tarantella Webtop"].getObjectFullName
(link);
        output = output + "\t" + tfn_name + "\n";
    }

    alert(output);
}

</SCRIPT>
```

```
<FORM>
  <INPUT TYPE=button VALUE="TFN Names?" onclick="showLinkTFN(">
</FORM>
```

This example adds a button beneath the links on users' webtops. When a user clicks this button, Secure Global Desktop displays the TFN names of all objects which have a link on the webtop.

Add the code to the HTML document containing the webtop tray applet (`left.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you are using the `sco/tta/standard` webtop theme. If you're using another theme, with different frame names and layouts, or different applet names, you'll need to modify the lines that invoke the `getNumberOfObjects` and `getObjectFullName` methods to access the webtop tray applet used by your new theme.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)

## getObjectImageName (webtop script and webtop tray applets)

### Syntax

```
String getObjectImageName(int objectNumber)
```

### Description

Returns the name of the image associated with the specified link. This is the icon Secure Global Desktop displays as part of the link if the webtop tray applet's `ShowIcon` parameter has the value `true`.

This image is specified by the associated object's [Webtop Icon](#) attribute. The information returned depends on the attribute's value:

- If the attribute specifies a filename, this method returns the image's basename, with no suffix.
- If the attribute specifies a URL, this method returns the full URL used to obtain the image.

*objectNumber* specifies a link on the webtop. The value `0` specifies the first link on the webtop, `1` the second and so on. The method returns an error if *intObjectNumber* is greater than the number of links on the webtop.

**Note** You can use the applet's `ObjectNumber` parameter to change the number from which links are numbered (default is zero).

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

function showLinkIcons() {
    output = "The webtop tray contains links which use these images:\n";
    count_links = document.applets["Tarantella Webtop"].getNumberOfObjects();

    for (var link = 0 ; link < count_links ; link++) {
        img_name = document.applets["Tarantella Webtop"].getObjectImageName
```



```
(link);
    output = output + "\t" + img_name + "\n";
}

alert(output);
}

</SCRIPT>

<FORM>
  <INPUT TYPE=button VALUE="Images?" onclick="showLinkIcons()" >
</FORM>
```

This example adds a button beneath the links on users' webtops. When a user clicks this button, Secure Global Desktop displays the image names associated with each link on the webtop.

Add the code to the HTML document containing the webtop tray applet (`left.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you are using the `sco/tta/standard` webtop theme. If you're using another theme, with different frame names and layouts, or different applet names, you'll need to modify the lines that invoke the `getNumberOfObjects` and `getObjectImageName` methods to access the webtop tray applet used by your new theme.

## Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)
- [getObjectImageNameByName \(webtop script and webtop tray applets\)](#)

## `getObjectImageNameByName` (webtop script and webtop tray applets)

### Syntax

```
String getObjectImageNameByName(String objectName)
```

### Description

Returns the name of the image associated with the specified link. This is the icon Secure Global Desktop displays as part of the link if the webtop tray applet's `ShowIcon` parameter has the value `true`.

This image is specified by the associated object's [Webtop Icon](#) attribute. The information returned depends on the attribute's value:

- If the attribute specifies a filename, this method returns the image's basename, with no suffix.
- If the attribute specifies a URL, this method returns the full URL used to obtain the image.

*objectName* is the full [TFN name](#) of an application on the user's webtop.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
imageName = applet.getObjectImageNameByName("../_ens/o=Indigo Insurance/  
ou=Finance/ou=Administration/cn=Phone List");  
alert("The image name is: " + imageName);
```

Displays the image name associated with the Phone List application.

#### Related topics

- Webtop script applet
- Webtop tray applet
- getObjectImageName (webtop script and webtop tray applets)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## `getObjectPlacement` (webtop script and webtop tray applets)

### Syntax

```
String getObjectPlacement(String objectName)
```

### Description

Returns a string representing where the application will be launched. This string can be "mainbrowser", "multiplewindows", "newbrowser", "awtwindow", "localx" or "kiosk".

*objectName* is the full [TFN name](#) of an application on the user's webtop.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
launchLoc = applet.getObjectPlacement("../_ens/o=Indigo Insurance/  
ou=Finance/ou=Administration/cn=Phone List");  
alert("The application launch location is: " + launchLoc);
```

Displays a dialog indicating where the application will be launched.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)

## `getParentGroupName` (webtop script and webtop tray applets)

### Syntax

```
String getParentGroupName(String objectName)
```

### Description

Returns the full [TFN name](#) of *objectName*'s parent. If the parent is the top level of the hierarchy and the webtop is in hierarchy mode, "TopLevel" is returned. If the webtop is not in hierarchy mode, "FlatWebtop" is returned.

*objectName* is the full TFN name of an application on the user's webtop.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
parName = applet.getParentGroupName("../_ens/o=Indigo Insurance/ou=Finance/  
ou=Administration/cn=Phone List");  
alert("Application parent name is: " + parName);
```

Displays the name of the parent of the Phone List object in the webtop hierarchy.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)

## getTotalNumberOfObjects (webtop script and webtop tray applets)

### Syntax

```
int getTotalNumberOfObjects (String objectType)
```

### Description

Returns the number of objects of type *objectType* found on the user's webtop. If the webtop is in hierarchy mode, returns the number of objects found on all open levels of the hierarchy.

*objectType* may be "GROUPTYPE" "ALLTYPE" "APPLICATIONTYPE" or "DOCUMENTTYPE".

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
docObjects = applet.getTotalNumberOfObjects("DOCUMENTTYPE");  
alert("The number of document objects on the webtop is: " + docObjects);
```

Displays the number of document objects on the user's webtop.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)

## `isApplication` (webtop script and webtop tray applets)

### Syntax

```
String isApplication(String objectName)
```

### Description

Returns "TRUE" if the object is an application otherwise, it returns "FALSE".

*objectName* is the full [TFN name](#) of an object on the user's webtop.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
verdict = applet.isApplication("../_ens/o=Indigo Insurance/ou=Finance/  
ou=Administration/cn=Phone List");  
if (verdict == "TRUE")  
    alert("The object is an application!");  
else  
    alert("The object is NOT an application!");
```

Displays a dialog indicating whether the Phone List object is an application or not.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)

## `isDocument` (webtop script and webtop tray applets)

### Syntax

```
String isDocument(String objectName)
```

### Description

Returns "TRUE" if the object is a document otherwise, it returns "FALSE".

*objectName* is the full [TFN name](#) of an object on the user's webtop.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
verdict = applet.isDocument("../_ens/o=Indigo Insurance/ou=Finance/  
ou=Administration/cn=Phone List");  
if (verdict == "TRUE")  
    alert("The object is a document!");  
else  
    alert("The object is NOT a document!");
```

Displays a dialog indicating whether the Phone List object is a document or not.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)



## isGroup (webtop script and webtop tray applets)

### Syntax

```
String isGroup(String objectName)
```

### Description

Returns "TRUE" if the object is a group otherwise, it returns "FALSE".

*objectName* is the full [TFN name](#) of an object on the user's webtop.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
verdict = applet.isGroup("../_ens/o=Indigo Insurance/ou=Finance/  
ou=Administration/cn=Phone List");  
if (verdict == "TRUE")  
    alert("The object is a group!");  
else  
    alert("The object is NOT a group!");
```

Displays a dialog indicating whether the Phone List object is a group or not.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)

## isHierarchyEnabled (webtop script and webtop tray applets)

### Syntax

```
String isHierarchyEnabled()
```

### Description

Returns "TRUE" if the webtop is in hierarchy mode, otherwise it returns "FALSE".

You can enable hierarchy mode by setting the `UseHierarchy` parameter to `true`.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
verdict = applet.isHierarchyEnabled();
if (verdict == "TRUE")
    alert("The webtop is in hierarchy mode!");
else
    alert("The webtop is not in hierarchy mode!");
```

Displays a dialog indicating whether the webtop is in hierarchy mode or not.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)

## isOpenGroup (webtop script and webtop tray applets)

### Syntax

```
String isOpenGroup(String location)
```

### Description

Returns "TRUE" if the client has downloaded the contents of the application group from the server, and returns "FALSE" if the group's contents have not been downloaded.

*location* is the full [TFN name](#) of a group object.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
verdict = applet.isOpenGroup("../_ens/o=Indigo Insurance/cn=Applications");  
if (verdict == "TRUE")  
    alert("Contents of "Applications" downloaded!");  
else  
    alert("Contents of "Applications" NOT downloaded!");
```

Displays a dialog indicating whether the contents of the Applications group has been downloaded.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)

## isRunning (webtop script and webtop tray applets)

### Syntax

```
String isRunning(String objectName)
```

### Description

Returns "TRUE" if the object is a running application otherwise, it returns "FALSE".

*objectName* is the full [TFN name](#) of an object on the user's webtop.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
verdict = applet.isRunning("../_ens/o=Indigo Insurance/ou=Finance/  
ou=Administration/cn=Phone List");  
if (verdict == "TRUE")  
    alert("The object is a running application!");  
else  
    alert("The object is NOT a running application!");
```

Displays a dialog indicating whether the Phone List object is a running application or not.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)

## killIterator (webtop script and webtop tray applets)

### Syntax

```
void killIterator(String iteratorHandle)
```

### Description

Frees any resources associated with the iterator identified by the iterator handle. `killIterator` should be called when the iterator is no longer needed.

`iteratorHandle` is the handle to an iterator previously created with one of the `getIterator` methods.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
applet.killIterator(iterator)
```

Frees resources associated with the iterator handle.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)
- [openHierarchyLevel \(webtop script and webtop tray applets\)](#)
- [getCurrentIteratorElement \(webtop script and webtop tray applets\)](#)
- [getNextIteratorElement \(webtop script and webtop tray applets\)](#)
- [getIteratorHasMoreElements \(webtop script and webtop tray applets\)](#)
- [getIteratorForHierarchyLevel \(webtop script and webtop tray applets\)](#)

- `getIteratorForAllOpenHierarchyLevels`  
(webtop script and webtop tray applets)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## launchByObjectName (webtop script and webtop tray applets)

### Syntax

```
String launchByObjectName(String ObjectTFNName)
```

### Description

Activates the specified object, just as if a user had clicked its link on their webtop.

*ObjectTFNName* specifies the [TFN name](#) of the object to activate.

**Note** You can only use this method to activate the objects that appear on a user's webtop -- the links that the webtop tray applet is currently displaying.

This method returns `OK` if Secure Global Desktop successfully launches the application (or displays the document) represented by the link, and `Error` otherwise.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

function startApplication() {
    app_tfn_name = ".../_ens/o=Indigo Insurance/ou=Finance/cn=XClaim";
    document.applets["Tarantella Webtop"].launchByObjectName(app_tfn_name);
}

</SCRIPT>

<FORM>
    <INPUT TYPE=button VALUE="Start XClaim" onclick="startApplication()">
</FORM>
```

This example adds a button beneath the links on users' webtops. When a user clicks this button, Secure Global Desktop activates the XClaim object on their webtop.

Add the code to the HTML document containing the webtop tray applet (`left.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you are using the `sco/tta/standard` webtop theme. If you're using another theme, with different frame names and layouts, or different applet names, you'll need to modify the line that invokes the `launchByObjectName` method to access the webtop tray applet used by your new theme. You'll also need to modify it to launch a valid object name.

### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)
- [launchByObjectNumber \(webtop script and webtop tray applets\)](#)



## launchByObjectNumber (webtop script and webtop tray applets)

### Syntax

```
string launchByObjectNumber(int objectNumber)
```

### Description

Activates the specified link, just as if a user had clicked it on their webtop.

*objectNumber* specifies a link on the webtop. The value 0 specifies the first link on the webtop, 1 the second and so on.

**Note** You can use the applet's `ObjectNumber` parameter to change the number from which links are numbered (default is zero).

This method returns `OK` if Secure Global Desktop successfully launches the application (or displays the document) represented by the link, and `Error` otherwise.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

function launchFirstLink() {
    document.applets["Tarantella Webtop"].launchByObjectNumber(0);
}

</SCRIPT>

<FORM>
    <INPUT TYPE=button VALUE="Activate First Link" onclick="launchFirstLink
    ()">
</FORM>
```

This example adds a button beneath the links on users' webtops. When a user clicks this button, Secure

Global Desktop activates the first link on their webtop.

Add the code to the HTML document containing the webtop tray applet (`left.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you are using the `sco/tta/standard` webtop theme. If you're using another theme, with different frame names and layouts, or different applet names, you'll need to modify the line that invokes the `launchByObjectNumber` method to access the webtop tray applet used by your new theme.

### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)
- [launchByObjectName \(webtop script and webtop tray applets\)](#)

## `openHierarchyLevel` (webtop script and webtop tray applets)

### Syntax

```
String openHierarchyLevel(String location)
```

### Description

Obtains the members of a group object and makes the contents available for scripting.

For *location*, use the full [TFN name](#) of the group to open.

Returns "OK" if the operation succeeds, or "Error" if it fails.

The parent of the group must be open for any group to open correctly.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
verdict = applet.openHierarchyLevel("../_ens/o=Indigo Insurance/  
cn=Applications");  
if (verdict == "OK")  
    alert("Contents of application group downloaded!");  
else  
    alert("Error!");
```

Obtains the members of the Applications group, and displays a dialog reporting success or failure.

### Related topics

- Webtop script applet
- Webtop tray applet
- closeHierarchyLevel (webtop script and webtop tray applets)
- getCurrentIteratorElement (webtop script and webtop tray applets)
- getNextIteratorElement (webtop script and webtop tray applets)
- getIteratorHasMoreElements (webtop script and webtop tray applets)
- getIteratorForHierarchyLevel (webtop script and webtop tray applets)
- getIteratorForAllOpenHierarchyLevels (webtop script and webtop tray applets)
- killIterator (webtop script and webtop tray applets)

## `receivedEvent` (webtop script and webtop tray applets)

### Syntax

```
String receivedEvent()
```

### Description

Returns "TRUE" if the run state of an application on the webtop has changed since the last call to `receivedEvent()`. Otherwise it returns "FALSE".

### Examples

```
verdict = applet.receivedEvent();
if (verdict == "TRUE")
    alert("The run state of an application on the webtop has changed!");
else
    alert("No changes this time!");
```

Displays a dialog indicating whether the run state of an application has changed.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)

## setLaunchWaitTimeOut (webtop script and webtop tray applets)

### Syntax

```
void setLaunchWaitTimeOut(int newTimeOut)
```

### Description

Specifies the maximum length of time in seconds to wait before attempting a new launch.

Under normal circumstances, Secure Global Desktop does not allow an application launch to start until the previous application launch has been completed. `setLaunchWaitTimeOut` allows the webtop to be told the maximum length of time to wait before attempting the next launch.

This method can be used with either the [webtop script applet](#) or the [webtop tray applet](#).

### Examples

```
applet.setLaunchWaitTimeOut(10)
```

Waits a maximum of 10 seconds before attempting a new launch.

#### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)
- [getLaunchWaitTimeOut \(webtop script and webtop script applets\)](#)

## Webtop tray applet

The webtop tray applet displays the links on a user's webtop and renders them, typically using an icon and a text label.

**Note** The webtop tray applet can only be used with the *classic* webtop.

- Value to use for the `TTAAPPLET` code attribute:  
`com/tarantella/tta/client/applets/SmartIconHost.class`
- Used by all webtop themes supplied with Secure Global Desktop.
- [Applet parameters](#)
- Public methods:
  - `areObjectsInitialized`
  - `closeHierarchyLevel`
  - `getApplicationType`
  - `getCurrentIteratorElement`
  - `getIteratorForAllOpenHierarchyLevels`
  - `getIteratorForHierarchyLevel`
  - `getIteratorHasMoreElements`
  - `getLaunchWaitTimeOut`
  - `getNextIteratorElement`
  - `getNumberOfObjects`
  - `getNumberOfObjectsInGroup`
  - `getObjectClass`
  - `getObjectDisplayName`
  - `getObjectDisplayNameByName`
  - `getObjectFullName`
  - `getObjectImageName`
  - `getObjectImageNameByName`
  - `getObjectPlacement`
  - `getParentGroupName`
  - `getTotalNumberOfObjects`
  - `isApplication`
  - `isDocument`

- [isGroup](#)
- [isHierarchyEnabled](#)
- [isOpenGroup](#)
- [isRunning](#)
- [killIterator](#)
- [launchByObjectName](#)
- [launchByObjectNumber](#)
- [login](#)
- [logout](#)
- [openGroup](#)
- [openHierarchyLevel](#)
- [openParentGroup](#)
- [receivedEvent](#)
- [scriptStart](#)
- [setLaunchWaitTimeOut](#)

#### Related topics

- [Webtop script applet](#)
- [Login applet](#)
- [Framework applet](#)
- [Print applet](#)
- [Terminal emulator applet](#)
- [X emulator applet](#)
- [The TTAAPPLET tag](#)



## Webtop tray applet parameters

The [webtop tray applet](#) has the following parameters.

Parameter	Type	Default	Description
<code>AsadPort</code>	Integer	No default	<p>The TCP port the webtop tray or webtop script applet uses to communicate with the Secure Global Desktop server.</p> <p>Use the placeholder <code>%%ASADPORT%%</code> to let Secure Global Desktop supply the correct value for this parameter. You should only enter a particular value for this parameter (rather than the placeholder) if you're sure you know what you're doing.</p> <p>This parameter has no default value. Communication with the Secure Global Desktop server is only possible if you supply a valid TCP port number (or use <code>%%ASADPORT%%</code>).</p>
<code>AttachLabelTo</code>	Side indicator	<code>iconright</code>	The side of the icon where labels appear.

BorderWidth	Integer	1	The width of the border that the webtop tray applet draws around highlighted links. Typically, you'll use values in the range 0 to 10. Use the value 0 to specify that highlighted links don't have a border.
BottomMargin	Integer	0	<p>The gap between the webtop tray's bottom edge and the bottom of the last link. (If <code>LayoutStyle</code> is <code>horizontal</code>, this is the gap between the webtop tray's bottom edge and the bottom of <i>all</i> links.)</p> <p>If you're using the <code>%%</code> <code>CALCWIDTH%%</code> and <code>%%</code> <code>CALCHEIGHT%%</code> placeholders, specify this parameter's value in the form <code>%%BOTTOMMARGIN value%%</code>. For example, to use a value of 10: <code>&lt;param name="BottomMargin" value="%%BOTTOMMARGIN 10%%"&gt;</code>.</p>
DisplayOrder	order	organization	The order in which to display links.
HostBackgroundColor	Color definition	255, 255, 255 (White)	The background color of the webtop tray applet.

IconSize	Integer	32	<p>The size of any icons used to display links.</p> <p>You can set this to 16 (16 x 16 pixels), 24, 32 or 48.</p> <p>If you specify a size for which no corresponding images exist, Secure Global Desktop doesn't display icons as part of links (just as if you had specified <code>ShowIcon</code> to be <code>false</code>).</p>
IconTheme	String	sco/tta/standard	<p>The icon theme of any icons used to display links.</p> <p>If you specify a theme that doesn't exist, Secure Global Desktop doesn't display icons as part of links (just as if you had specified <code>ShowIcon</code> to be <code>false</code>).</p>
IconToLabelGap	Integer	8	<p>The gap between icons and their labels.</p> <p>If <code>ShowLabel</code> or <code>ShowIcon</code> are set to <code>false</code>, this setting is ignored.</p>
LabelColor	Color definition	0, 0, 0 (Black)	The color of links' labels.
LabelFontFamily	Font family	Browser dependent	The font used to display links' labels.

LabelFontSize	Integer	Browser-dependent	The point size of the font used to display links' labels
LabelFontStyle	Style indicator	plain	The style of font used to display links' labels.
LaunchWaitTimeOut	integer	0	How long (in seconds) an application launch is assumed to take if the server doesn't notify the client that a launch has succeeded or failed. The webtop tray applet uses this parameter to reset a link to its default state (no highlighting).
LayoutStyle	Layout indicator	vertical	<p>How links appear on the webtop, either vertically (in a column) or horizontally (in a row).</p> <p>If you're using the %% CALCWIDTH%% and %% CALCHEIGHT%% placeholders, specify this parameter's value in the form %%LAYOUTSTYLE value%%. For example, to use a value of vertical: &lt;param name="LayoutStyle" value="%%LAYOUTSTYLE vertical%%"&gt;.</p>

LeftMargin	Integer	0	<p>The gap between the webtop tray's left edge and the links' left edges. (If <code>LayoutStyle</code> is <code>horizontal</code>, this is the gap between the webtop tray's left edge and the first link's left edge.)</p> <p>If you're using the <code>%%CALCWIDTH%%</code> and <code>%%CALCHEIGHT%%</code> placeholders, specify this parameter's value in the form <code>%%LEFTMARGIN value%%</code>. For example, to use a value of 10: <code>&lt;param name="LeftMargin" value="%%LEFTMARGIN 10%%"&gt;</code>.</p>
LoggedInAsFormat	string	""	<p>The form of message displayed in the status bar when users move the cursor over the webtop tray applet's background.</p> <p>The placeholder <code>%%PERSONLABEL%%</code> is replaced with the current user's name and connection type. For example, with the value <code>"You are %%PERSONLABEL%%"</code>, users see a message like <code>"You are Mulan Rouge (standard connection)"</code>.</p>

LoginGUIMask

Integer

"2"

A bitmask in the range 0 to 15 which controls the appearance of the Secure Global Desktop log in dialog.

The bits are as follows:

- Bit 1 - controls whether or not the log in dialog box displays. This is where the user enters their username and password.
- Bit 2 - controls whether or not the ambiguous/aged password dialog box displays.
- Bit 3 - controls whether or not the error dialog box displays.
- Bit 4 - controls whether or not the log in dialog displays before credentials are submitted. This forces the user to click OK to log in. The values for the username and password are taken from the TarantellaUsername and TarantellaPassword parameters.

If the value of this parameter is:

- 0 - no dialog boxes display.
- 15 - all dialog boxes display.

See [Logging in with the Secure Global Desktop applets](#) for details of when and how you use this parameter.

LogoutAfter	Integer	0	<p>The number of minutes of the timeout period. If a webtop is idle for this period of time, the user is automatically logged out.</p> <p>A value of 0 means do <b>not</b> automatically log out. If the value is missing or not an integer, the value defaults to 0.</p> <p>This parameter is only available to web browsers with Java™ technology enabled. It is not available to the Sun Secure Global Desktop Native Client.</p> <p>Suspended applications are counted as running and so prevent automatic logout.</p> <p>The applet checks for running sessions every 1/20th of the timeout period and so could miss short bursts of activity and wrongly log a user out.</p> <p>The applet does not take into account print or client drive mapping activity and so, for example, a user could be printing when they are logged out.</p>
ObjectBackgroundColor	Color definition	255, 255, 255 (White)	The background color of all links.

ObjectBottomShadow	Color definition	0, 0, 0 (Black)	<p>The color of the bottom border that the webtop tray applet displays around highlighted links.</p> <p>The top border color is used for the bottom and right borders of unclicked (default) links, and the top and left borders of clicked links.</p>
ObjectCount	Integer	0	<p>The number of links on the webtop.</p> <p>Use the placeholder <code>%%OBJCOUNT%%</code> to let Secure Global Desktop calculate the correct value for this parameter. You should only supply a particular value for this parameter (rather than the placeholder) if you're sure you know what you're doing.</p>
ObjectGap	Integer	10	<p>The gap between links. If <code>LayoutStyle</code> is <code>vertical</code>, this is the gap between the bottom of one link and the top of the next. If <code>LayoutStyle</code> is <code>horizontal</code>, this is the gap between the right side of one link and the left of the next.</p> <p>If you're using the <code>%%CALCWIDTH%%</code> and <code>%%CALCHEIGHT%%</code> placeholders, specify this parameter's value in the form <code>%%OBJGAP value%%</code>. For example, to use a value of 10: <code>&lt;param name="ObjectGap"</code></p>



			value="%%OBJGAP 10%%">.
ObjectHeight	Integer	34	<p>The height of each link.</p> <p>If you're using the %% CALCWIDTH%% and %% CALCHEIGHT%% placeholders, specify this parameter's value in the form %%OBJHEIGHT <i>value</i> %%. For example, to use a value of 40: &lt;param name="ObjectHeight" value="%%OBJHEIGHT 40% %%"&gt;.</p>
ObjectNumber	Integer	0	The number from which links are numbered.
ObjectTopShadow	Color definition	255, 255, 255 (White)	<p>The color of the top border that the webtop tray applet displays around highlighted links.</p> <p>The top border color is used for the top and left borders of unclicked (default) links, and the bottom and right borders of clicked links.</p>
ObjectWidth	Integer	100	<p>The width of each link.</p> <p>If you're using the %% CALCWIDTH%% and %% CALCHEIGHT%% placeholders, specify this parameter's value in the form %%OBJWIDTH <i>value</i> %. For example, to use a value of 130: &lt;param name="ObjectWidth" value="%%OBJWIDTH 130%</p>

			<code>%"&gt;</code> .
PageName	string	No default	<p>The name of the page/file hosting the applet.</p> <p>This parameter is required if you are using Internet Explorer 6.0 with Sun Java™ Plug-in.</p> <p>This parameter is harmless if it is used in a web client that doesn't need it.</p>
RightMargin	Integer	0	<p>The gap between the webtop tray's right edge and the links' right edges. (If <code>LayoutStyle</code> is <code>horizontal</code>, this is the gap between the webtop tray's right edge and the first link's right edge.)</p> <p>If you're using the <code>%%</code> <code>CALCWIDTH%%</code> and <code>%%</code> <code>CALCHEIGHT%%</code> placeholders, specify this parameter's value in the form <code>%%RIGHTMARGIN value%%</code>. For example, to use a value of 10: <code>&lt;param name="RightMargin" value="%%RIGHTMARGIN 10% %"&gt;</code>.</p>

Scripting	Boolean	"false"	<p>This parameter is used with the <a href="#">scriptStart</a> method to release/ wake-up the applet.</p> <p>If the parameter is missing or incorrect, the default of <code>false</code> is used.</p>
ShowIcon	Boolean	true	<p>Specifies whether the webtop tray applet displays icons as part of the links it shows.</p>
ShowLabel	Boolean	true	<p>Specifies whether the webtop tray applet displays labels as part of the links it shows.</p>
TarantellaPassword	String	""	<p>The password the applet uses to log in to a Secure Global Desktop server.</p> <p>If the value of the <code>TarantellaUsername</code> parameter is an empty string (""), the applet tries to log the user in <a href="#">anonymously</a> (without a password).</p> <p>If you are concerned about security, you may not want to use this parameter. Users can see the password you supply (by viewing the page source) and they may be authenticated to Secure Global Desktop as a different user.</p> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>

TarantellaUsername	String	No default	<p>The username the applet uses to log in to a Secure Global Desktop server.</p> <p>If this parameter is used, the applet tries to log the user in to Secure Global Desktop using the values for the <code>TarantellaUsername</code> and <code>TarantellaPassword</code> parameters. If the value of this parameter is an empty string (<code>""</code>), the applet tries to log the user in <a href="#">anonymously</a> (without a password).</p> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>
TargetFrame	String	<code>"DisplayFrame"</code>	<p>The name of the frame used to display document objects that don't have the <a href="#">Open In New Browser Window</a> attribute set, and for application objects that have their <a href="#">Display Using</a> attribute set to Webtop.</p> <p><code>DisplayFrame</code> (the default) is the frame used by the <code>sco/</code> <code>tta/standard</code> webtop theme.</p>

TopMargin	Integer	0	<p>The gap between the webtop tray's top edge and the top of the first link. (If <code>LayoutStyle</code> is <code>horizontal</code>, this is the gap between the webtop tray's top edge and the top of <i>all</i> links.)</p> <p>If you're using the <code>%%CALCWIDTH%%</code> and <code>%%CALCHEIGHT%%</code> placeholders, specify this parameter's value in the form <code>%%TOPMARGIN value %%</code>. For example, to use a value of 10: <code>&lt;param name="TopMargin" value="%%TOPMARGIN 10%%"&gt;</code>.</p>
UseHierarchy	Boolean	false	<p>If set to true, enables webtop hierarchy mode and the scripting interface for manipulating the visible hierarchy.</p>

### Related topics

- [Webtop script applet](#)
- [Webtop tray applet](#)
- [Applet parameter data types](#)

## openGroup (webtop tray applet)

### Syntax

```
void openGroup(String groupName)
```

### Description

Takes the name of a group object found on the user's webtop and displays its contents in the webtop tray.

Use a full [TFN name](#) for *groupName*.

### Examples

```
applet.OpenGroup("../_ens/o=Indigo Insurance/cn=Applications")
```

Shows the members of the Applications group in the webtop tray.

#### Related topics

- [Webtop tray applet](#)
- [Webtop script applet](#)

## `openParentGroup` (webtop tray applet)

### Syntax

```
void openParentGroup()
```

### Description

Displays the previously viewed group. `openParentGroup` can be called multiple times. If the currently displayed application group is the top level of the hierarchy, calls to this method will be ignored.

### Examples

```
applet.openParentGroup()
```

Shows the parent group in the webtop tray.

#### Related topics

- [Webtop tray applet](#)
- [Webtop script applet](#)

## X emulator applet

The X emulator applet displays X and Windows applications on the client device.

**Note** Although the X emulator applet is used by the browser-based webtop to display applications on the webtop or in a new browser window, it must not be customized or scripted. If you want to customize or script this applet you must use the *classic* webtop.

- Value to use for the `TTAAPPLET` `code` attribute:  
`com/tarantella/tta/client/applets/XDE.class`
- Used by all webtop themes supplied with Secure Global Desktop.
- [Applet parameters](#)
- Public methods:
  - `getProperty`
  - `getEmulatorState`
  - `login`
  - `logout`
  - `registerProperty`
  - `scriptStart`
  - `setProperty`
  - `suspendApplication`
  - `unregisterProperty`

### Related topics

- [Login applet](#)
- [Framework applet](#)
- [Webtop script applet](#)
- [Webtop tray applet](#)
- [Print applet](#)
- [Terminal emulator applet](#)
- [The TTAAPPLET tag](#)





## X emulator applet parameters

The parameters in this topic may be used with the [X emulator applet](#).

Applet parameters take precedence over object attributes. For example, if you have an application object with its [Middle Mouse Timeout](#) attribute set to 50, but display it in an HTML page containing the X emulator applet with its `MiddleMouseTimeout` parameter set to 100, the timeout will be 100 milliseconds. Applet parameters that override object attributes in this way are listed in the table below with a default of "Object attribute value".

Parameter	Type	Default	Description
<code>Application</code>	String	Object attribute value	<p>The full pathname of the application on the application server, for instance, <code>/usr/local/bin/xclaim</code>.</p> <p>To enter command line arguments (such as <code>-geometry</code>), use the <code>Arguments</code> parameter.</p> <p>To launch a complete Windows session, use <code>-</code> (a single hyphen).</p>
<code>ApplicationServer</code>	Host	Object attribute value	The application server you want to run the application on.
<code>Arguments</code>	String	Object attribute value	Any command line arguments to the application, for instance, <code>-geometry</code> . Note that as the X Protocol Engine runs on the Secure Global Desktop server, you must not set the <code>-display</code> argument.
<code>AsadPort</code>	Integer	No default	<p>The TCP port the emulator applet uses to communicate with the Secure Global Desktop server.</p> <p>Use the placeholder <code>%%ASADPORT%%</code> to let Secure Global Desktop supply the correct value for this parameter. You should only enter a particular value for this parameter (rather than the placeholder) if you're sure you know what you're doing.</p> <p>This parameter has no default value. Communication with the Secure Global Desktop server is only possible if you supply a valid TCP port number (or use <code>%%ASADPORT%%</code>).</p>
<code>BackgroundColor</code>	Color definition	000000 (black)	The background color.

Compression	Boolean with automatic	Object attribute value	<p>Whether X protocol requests are compressed for transmission. Compressing requests can increase the performance of many applications. For some applications, however, compressing requests can decrease performance.</p> <ul style="list-style-type: none"> <li>• <code>On</code> specifies that X protocol requests are compressed for transmission.</li> <li>• <code>Off</code> specifies that X protocol requests aren't compressed for transmission.</li> <li>• <code>Automatic</code> specifies that Secure Global Desktop compresses X protocol requests only when it would increase the performance of the application.</li> </ul>
ConnectionMethod	Connection method	Object attribute value	<p>The mechanism for accessing the application server.</p> <p>The settings <code>telnet</code> and <code>rexec</code> let you use the corresponding standard UNIX communication tools.</p> <p>The setting <code>ssh</code> lets Secure Global Desktop servers communicate securely with application servers. This option is only available if you've already obtained and installed <a href="#">SSH</a>.</p>
Continuous	Boolean with automatic	Object attribute value	<p>Whether X protocol requests are executed in order, or optimized for best performance.</p> <ul style="list-style-type: none"> <li>• <code>On</code> specifies that X protocol requests are optimized (may be executed out of order).</li> <li>• <code>Off</code> specifies that X protocol requests aren't optimized (are always executed in order). Use this mode for applications where the order in which requests are executed is critical (applications that use animation, for example).</li> <li>• <code>Automatic</code> specifies that Secure Global Desktop optimizes X protocol requests only when it would increase the performance of the application.</li> </ul>
DelayedUpdate	Boolean	Object attribute value	<p>Whether delayed updates of the display are allowed.</p> <p>If you allow delayed update, Secure Global Desktop accumulates changes before updating the display. This can improve the performance of your application.</p> <p>If your application's display must always be exact, use the value <code>false</code>.</p>
Environment	String	Object attribute value	<p>Any environment variable settings required by the application on the application server. Enter these in the form <code>VARIABLE=Setting</code>. To set more than one variable, use the parameter names <code>Environment1</code>, <code>Environment2</code> and so on. For example, to set three environment variables, specify them as follows:</p> <pre>&lt;PARAM NAME="Environment" VALUE="Variable=Setting"&gt; &lt;PARAM NAME="Environment1" VALUE="Variable=Setting"&gt; &lt;PARAM NAME="Environment2" VALUE="Variable=Setting"&gt;</pre>
ForegroundColor	Color definition	FFFFFF (white)	The foreground color.

GraphicsAcceleration	Boolean	Object attribute value	<p>Whether acceleration is allowed.</p> <p>Acceleration optimizes how graphics are rendered and improves performance at the expense of smoothness and accuracy. For instance, colors may not always be accurate.</p> <p>If your application's display must always be accurate, use the value <code>false</code>.</p>
KeymapLocked	Boolean	Object attribute value	<p>Whether the keyboard mappings are fixed. The value <code>false</code> means an X client can change the default keyboard mappings.</p>
LoginGUIMask	Integer	"2"	<p>A bitmask in the range 0 to 15 which controls the appearance of the Secure Global Desktop log in dialog.</p> <p>The bits are as follows:</p> <ul style="list-style-type: none"> <li>• Bit 1 - controls whether or not the log in dialog box displays. This is where the user enters their username and password.</li> <li>• Bit 2 - controls whether or not the ambiguous/aged password dialog box displays.</li> <li>• Bit 3 - controls whether or not the error dialog box displays.</li> <li>• Bit 4 - controls whether or not the log in dialog displays before credentials are submitted. This forces the user to click OK to log in. The values for the username and password are taken from the <code>TarantellaUsername</code> and <code>TarantellaPassword</code> parameters.</li> </ul> <p>If the value of this parameter is:</p> <ul style="list-style-type: none"> <li>• 0 - no dialog boxes display.</li> <li>• 15 - all dialog boxes display.</li> </ul> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>
LoginScript	String	Object attribute value	<p>The <a href="#">login script</a> used to log in to the application server, for example <code>unix.exp</code>.</p>
MiddleMouseTimeout	Integer	Object attribute value	<p>The maximum time (in milliseconds) which may elapse between pressing the left and right mouse buttons.</p> <p>This setting enables you to emulate the middle mouse button on a two-button mouse by pressing the left and the right mouse buttons in quick succession.</p>
ObjectXFN	String	""	<p>The application object's <a href="#">TFN name</a>.</p> <p>Use the placeholder <code>%%OBJECTNAME%%</code> to let Secure Global Desktop supply the correct value for this parameter. You should only enter a particular value for this parameter (rather than the placeholder) if you're sure you know what you're doing.</p>

Password	String	Password cache or prompt	<p>A password to authenticate users on an application server.</p> <p>If a valid password is specified, together with a valid username in the <code>Username</code> parameter, this username and password is used instead of any previously cached password for the authentication server.</p> <p>If you don't specify values for <b>both</b> the <code>Username</code> <b>and</b> <code>Password</code> parameters, Secure Global Desktop uses a cached username and password, if available.</p> <p>In all other circumstances (specifying a valid <code>Password</code> but not specifying a value for <code>Username</code>, for example), Secure Global Desktop prompts users for a valid username and password.</p> <p>Users can still press the Shift key when they click a link to force Secure Global Desktop to prompt for this information.</p>
PromptforAuth	Boolean	false	Whether to display a dialog box which prompts the user for third tier authentication.
Resumable	String	Object attribute value	<p>The resumability model for the application. You can set this to <code>never</code>, <code>session</code>, or <code>forever</code>. <code>Never</code> means that the application can never be resumed and clicking the link always starts a new application instance. <code>Session</code> means that the application keeps running and is resumable until the user logs out of Secure Global Desktop. <code>Forever</code> means that the application keeps running after the user logs out of Secure Global Desktop, and can be resumed when they next log in. See the <a href="#">Resumability</a> attribute.</p>
RootColor	Color name	Object attribute value	<p>The X emulator's background color.</p> <p>This parameter only has an effect if you specify a <code>RootType</code> value of <code>color</code>.</p>
RootType	Root type	Object attribute value	<p>The appearance of the X emulator's background.</p> <ul style="list-style-type: none"> <li><code>default</code> means the X emulator's background uses the X windows default background pattern and color.</li> <li><code>color</code> means the X emulator's background is the color specified by <code>RootColor</code>.</li> </ul>
Scottaappleheight	Integer	Object attribute value	The height of the application in pixels.
Scottaappletwidth	Integer	Object attribute value	The width of the application in pixels.
Scottaeurokeymapping	String	Object attribute value	The keycode mapping required by the application to support the euro character. The options are <code>unicode</code> and <code>iso8859-15</code> .

Scottfullscreen	Boolean	Object attribute value	Whether the application starts at the <a href="#">maximum size</a> (true) or sized according to the <a href="#">Width</a> and <a href="#">Height</a> attributes (false).
Scottinterlacedimages	String	Object attribute value	How images are transmitted and displayed. The options are <code>automatic</code> , <code>on</code> and <code>off</code> . See <a href="#">Interlaced Images</a> for details.
Scottmonitorresolution	Integer	Object attribute value	The <a href="#">monitor resolution</a> (in dots per inch) which Secure Global Desktop reports to X applications asking for this information.
Scottantdomain	String	No default	The Windows domain to use for the application server authentication process.
Scottprotocolarguments	String	No default	The command-line arguments to use with the <a href="#">Windows Protocol</a> .  Valid settings depend on the Windows Protocol.
Scottshareresources	Boolean	Object attribute value	Whether emulator sessions for applications configured to <a href="#">Display Using</a> client window management try to share resources.
Scotttrylocalwindowsapplication	Boolean	false	Whether to try starting the Windows application from the user's client device.
Scottawincursor	Boolean	false	Causes WinCenter to display the appropriate cursor from the Windows application in addition to the cursor from the client device.  This attribute applies to the WinCenter <a href="#">Windows Protocol</a> only.  Although the WinCenter protocol is no longer supported, legacy windows application objects can continue to use it.
Scottwindowcloseaction	String	Object attribute value	What happens if the user closes the main application window using the Window Manager decoration. See <a href="#">Window Close Action</a> for details.
Scottwindowsapplicationserver	String	No default	The full <a href="#">TFN name</a> of application servers that can run the Windows application. For example, <code>.../_ens/o=Indigo Insurance/ou=IT/cn=london</code> .  If you don't specify an application server, the application may run on any Secure Global Desktop server in the array that supports that type of application.
Scripting	Boolean	"false"	This parameter is used with the <a href="#">scriptStart</a> method to release/wake-up the applet.  If the parameter is missing or incorrect, the default of <code>false</code> is used.

SessionEndsWhen	Session end type	Object attribute value	<p>What causes the X emulator session to terminate.</p> <ul style="list-style-type: none"> <li>• <code>LastClient</code> specifies that Secure Global Desktop maintains a count of the number of X clients running on a particular session. When this count reaches zero, the session terminates.</li> <li>• <code>WindowManager</code> specifies that Secure Global Desktop terminates the session when the window manager exits. This is irrespective of the number of X clients running in the window manager.</li> <li>• <code>WindowManagerAlone</code> terminates the session when the last remaining client is the window manager.</li> <li>• <code>LoginScript</code> terminates the session when the login script completes.</li> <li>• <code>NoWindows</code> terminates the session when no windows are visible. This is useful for window managers (such as OpenLook) that run X clients in the background.</li> <li>• <code>LoginScriptNoWindows</code> terminates the session when either the login script completes or no windows are visible. Use this for applications that are always resumable and that use X clients as this forces a session to close if an application server is re-booted or disconnected from the network.</li> </ul>
TarantellaPassword	String	""	<p>The password the applet uses to log in to a Secure Global Desktop server.</p> <p>If the value of the <code>TarantellaUsername</code> parameter is an empty string (""), the applet tries to log the user in <a href="#">anonymously</a> (without a password).</p> <p>If you are concerned about security, you may not want to use this parameter. Users can see the password you supply (by viewing the page source) and they may be authenticated to Secure Global Desktop as a different user.</p> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>
TarantellaUsername	String	No default	<p>The username the applet uses to log in to a Secure Global Desktop server.</p> <p>If this parameter is used, the applet tries to log the user in to Secure Global Desktop using the values for the <code>TarantellaUsername</code> and <code>TarantellaPassword</code> parameters. If the value of this parameter is an empty string (""), the applet tries to log the user in <a href="#">anonymously</a> (without a password).</p> <p>See <a href="#">Logging in with the Secure Global Desktop applets</a> for details of when and how you use this parameter.</p>
TerminationFrame	String	Current frame	<p>The frame in which Secure Global Desktop displays the URL specified by <code>TerminationURL</code>.</p> <p>If no value is specified for <code>TerminationURL</code>, this parameter has no effect.</p>

TerminationURL	String	""	<p>The URL to display when the emulator session terminates. It is displayed in the current frame, or in the frame specified in the TerminationFrame parameter.</p> <p>By default, no URL is displayed when the emulator session terminates: Secure Global Desktop continues to display the HTML page containing the terminal emulator applet.</p> <p>If you're using the <code>sco/tta/standard</code> webtop theme, you could set this to <code>display.html</code> to display the "Your Webtop" message when the emulator session ends.</p>
Username	String	Password cache or prompt	<p>A username to authenticate users with on the application server. This username is used to authenticate all users who run the application.</p> <p>If a valid username is specified, together with a valid password in the Password parameter, this username and password is used instead of any previously cached password for the authentication server.</p> <p>If you don't specify values for <b>both</b> the Username <b>and</b> Password parameters, Secure Global Desktop uses a cached username and password, if available.</p> <p>In all other circumstances (specifying a valid Username but not specifying a value for Password, for example), Secure Global Desktop prompts users for a valid username and password.</p> <p>Users can still press the Shift key when they click a link to force Secure Global Desktop to prompt for this information.</p> <p><b>Note</b> You may not want to use this parameter if you are concerned about security. Users will be able to see the password you supply here using their web browsers, and may be authenticated to the application server as another user.</p>
ViewHostReply	Boolean	Object attribute value	Whether messages from the application server are also logged on the Secure Global Desktop server.
WindowManager	String	Object attribute value	<p>Any command lines to execute additional applications on the application server. You can use this to run a window manager required by the main application. To set more than one, use the parameter names <code>WindowManager1</code>, <code>WindowManager2</code> and so on. For example, to set three applications, specify them as follows:</p> <pre>&lt;PARAM NAME="WindowManager" VALUE="application"&gt; &lt;PARAM NAME="WindowManager1" VALUE="application"&gt; &lt;PARAM NAME="WindowManager2" VALUE="application"&gt;</pre>

#### Related topics

- X emulator applet
- Applet parameter data types





## getEmulatorState (X emulator applet)

### Syntax

```
int getEmulatorState()
```

### Description

The `getEmulatorState` method returns the status code associated with the emulator session's display engine. This allows you to determine if an emulator session is starting, running or stopped.

This return value...	Indicates...
0	The X emulator session is starting, but hasn't yet connected to the application server.
1	The X emulator session is running.
2	The X emulator session has disconnected from the application server.
3	An error has occurred, and the X emulator session has been terminated.
4	The X emulator session has been suspended.
5	The X emulator session has finished.

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

window.onerror = trapError

function trapError(message, url, line) {
    alert("There's no X emulator session currently running");
    return true
}

function getState() {
    state = top.WebtopFrame.DisplayFrame.document.applets["Tarantella X
```

```

Emulator"].getEmulatorState();

switch (state) {
    case 0 :
        output = "The X emulator session is starting.";
        break;
    case 1 :
        output = "The X emulator session is running.";
        break;
    case 2 :
        output = "The X emulator session has disconnected.";
        break;
    case 3 :
        output = "An error has occurred.";
        break;
    case 4 :
        output = "The X emulator session has been suspended.";
        break;
    case 5 :
        output = "The X emulator session has finished.";
        break;
}

alert(output);
}

</SCRIPT>

<FORM>
    <INPUT TYPE=button VALUE="Get state" onclick="getState()">
</FORM>

```

This example adds a button beneath the links on users' webtops. When a user clicks this button, Secure Global Desktop displays a short message indicating the current state of the X emulator applet.

Add the code to the HTML document containing the webtop tray applet (`left.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you are using the `sco/tta/standard` webtop theme. If you're using another theme, with different frame names and layouts, or different applet names, you'll need to modify the lines that invoke the `getEmulatorState` method to access the X emulator applet used by your new theme.

## Related topics

- [X emulator applet](#)

## getProperty (X emulator applet)

### Syntax

```
string getProperty(window, property)
```

### Description

The `getProperty` method returns the value of a particular X property associated with an X window on the application server.

*window* is the name of the X window whose properties you're interested in. (This name is contained in the X window's `WM_NAME` X property.) Use an empty string ("") to specify the root window.

*property* is the name of the X property whose value this method returns. For example, the `WM_COMMAND` X property contains the command used to start the application that the X window is displaying.

**Note** You can only use this method to get the values of X properties you have previously registered an interest in (using the `registerProperty` method). If you try to retrieve a property's value without first registering it, `getProperty` returns `null`.

This method can only retrieve the values of X properties of type `STRING`. If you use the method to retrieve a value for an X property of another type, the method returns `null`.

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

function showProperty() {
    var XEmulatorApplet = document.applets["Tarantella X Emulator"];
    var value = null;

    // Register an interest in the property WM_COMMAND

    XEmulatorApplet.registerProperty("xterm", "WM_COMMAND");

    // Keep trying to retrieve the X property value.
    // It takes a finite amount of time to register the property. Until
```

```

// the property is registered, getProperty() returns NULL.

var loop=0;

while (value == null) {
    value = XEmulatorApplet.getProperty("xterm", "WM_COMMAND");
    loop++;
    if ( loop > 10000 ) break;
}

// Output either the value of the property, or an error message

if (value != null) {
    alert("The X property WM_COMMAND has the value " + value);
} else {
    alert("Couldn't access the X property WM_COMMAND");
}

// Unregister the X property

XEmulatorApplet.unregisterProperty("xterm", "WM_COMMAND");
}

</SCRIPT>

<FORM>
<INPUT TYPE=button VALUE="Get Property Value" onclick="showProperty()">
</FORM>

```

This example adds a button beneath the X emulator applet. When a user clicks the button, Secure Global Desktop displays the value of the X property `WM_COMMAND` associated with the X window whose name is `xterm`.

**Note** This example assumes the window name is `xterm`. You will need to change the code if you're using a different window name. This example also uses the X emulator applet's `registerProperty` and `unregisterProperty` methods to retrieve the property value.

Add the code to the HTML document containing the X emulator applet (`xde.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

## Related topics

- X emulator applet
- setProperty (X emulator applet)
- registerProperty (X emulator applet)
- unregisterProperty (X emulator applet)

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## registerProperty (X emulator applet)

### Syntax

```
void registerProperty(window, property)
```

### Description

The `registerProperty` method registers an interest a particular X property. You'll need to use this method if you want to use `getProperty` to retrieve a property's value.

*window* is the name of the X window whose properties you're interested in. (This name is contained in the X window's `WM_NAME` X property.) Use an empty string ("") to specify the root window.

*property* is the name of the X property you want to register. For example, the `WM_COMMAND` X property contains the command used to start the application that the X window is displaying.

If you're using X properties to communicate between an application and the client device, you'll probably need to write code to run on the client which "polls" a particular X property periodically. In this case, your code will call the `getProperty` method frequently. Thus, it's important that the `getProperty` method should not be a slow operation.

Registering properties lets Secure Global Desktop cache these properties' value on the client device. These cached values are updated whenever the corresponding X properties change. The `getProperty` method can now use the cached value rather than querying the application itself -- a much faster operation.

**Note** If you use the `getProperty` method to retrieve a property's value without first registering it, `getProperty` returns `null`. You don't need to register an X property in order to change its value with the `setProperty` method.

Once you've finished with a particular X property, you can use the `unregisterProperty` to tell Secure Global Desktop to stop checking for changes in that particular property. This helps keep performance overheads to a minimum.

### Examples



```
<SCRIPT LANGUAGE="JavaScript">

function register() {

    // Register an interest in the X property WM_COMMAND

    var XEmulatorApplet = document.applets["Tarantella X Emulator"];
    XEmulatorApplet.registerProperty("xterm", "WM_COMMAND");
}

function unregister() {

    // Unregister the X property WM_COMMAND

    var XEmulatorApplet = document.applets["Tarantella X Emulator"];
    XEmulatorApplet.unregisterProperty("xterm", "WM_COMMAND");
}

function showProperty() {
    var XEmulatorApplet = document.applets["Tarantella X Emulator"];
    var value = null;

    // Retrieve the value of the X property WM_COMMAND

    value = XEmulatorApplet.getProperty("xterm", "WM_COMMAND");

    // If WM_COMMAND is set, display it value. Otherwise, display an
    // error message.

    if (value != null) {
        alert("The X property WM_COMMAND has the value " + value);
    } else {
        alert("Couldn't access the X property WM_COMMAND");
    }
}

</SCRIPT>

<FORM>
  <INPUT TYPE=button VALUE="Register" onclick="register()">
  <INPUT TYPE=button VALUE="Get Property Value" onclick="showProperty()">
  <INPUT TYPE=button VALUE="Unregister" onclick="unregister()">
</FORM>
```

This example adds three buttons beneath the X emulator applet:

- The Register button registers the X property `WM_COMMAND` for the window `xterm` when a user clicks it.
- The Get Property Value button displays the value of the X property `WM_COMMAND` when a user clicks it, if the property is currently registered. Otherwise, it displays an error message.
- The Unregister button unregisters the X property when a user clicks it.

**Note** This example assumes the window name is `xterm`. You will need to change the code if you're using a different window name.

Add the code to the HTML document containing the X emulator applet (`xde.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

### Related topics

- [X emulator applet](#)
- [getProperty \(X emulator applet\)](#)
- [setProperty \(X emulator applet\)](#)
- [unregisterProperty \(X emulator applet\)](#)

## setProperty (X emulator applet)

### Syntax

```
void setProperty(window, property, value)
```

### Description

The `setProperty` method sets the value of a particular X property associated with an X window on the application server. If the X property doesn't already exist, this method creates it.

*window* is the name of the X window whose properties you're interested in. (This name is contained in the X window's `WM_NAME` X property.) Use an empty string ("") to specify the root window.

*property* is the name of the X property whose value this method sets.

*value* is the value you want to give to the specified X property.

This method can only set the values of X properties of type `STRING`. If you use the method to specify a value for an X property of another type, its type is changed to `STRING`.

**Note** Unlike the `getProperty` method, you don't need to [register](#) a property in order to change its value with `setProperty`.

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

function setProperty() {
    var XEmulatorApplet = document.applets["Tarantella X Emulator"];

    // Get the value of the X Property text box

    XPropertyName = document.userInput.xproperty.value;

    // Get the value of the Value text box

    XPropertyValue = document.userInput.val.value;
```

```

// Set the specified X property to the specified value

XEmulatorApplet.setProperty("xterm", XPropertyName, XPropertyValue);
}

function getProperty() {
    var XEmulatorApplet = document.applets["Tarantella X Emulator"];
    var value = null;

    // Get the value of the X Property text box

    XPropertyName = document.userInput.xproperty.value;

    // Register an interest in the specified X property

    XEmulatorApplet.registerProperty("xterm", XPropertyName);

    // Keep trying to retrieve the X property value.
    // It takes a finite amount of time to register the property. Until
    // the property is registered, getProperty() returns NULL.

    var loop=0;

    while (value == null) {
        value = XEmulatorApplet.getProperty("xterm", XPropertyName);
        loop++;
        if ( loop > 10000 ) break;
    }

    // Display the X property's value in the Value text box

    document.userInput.val.value = value;
}

</SCRIPT>

<FORM name="userInput">
    <p>X Property:
    <INPUT TYPE=text name=xproperty value=WM_COMMAND>

    <p>Value:
    <INPUT TYPE=text name=val value=null>

```

```
<p><INPUT TYPE=button VALUE="Set X Property" onclick="setProperty()">
<INPUT TYPE=button VALUE="Get X Property" onclick="getProperty()">
</FORM>
```

This example adds two text boxes and two buttons beneath the X emulator applet:

- When a user clicks the Set Property button, the specified X property is set to the specified value.
- When a user clicks the Get Property button, the specified X property's value is displayed.

**Note** This example assumes the window name is `xterm`. You will need to change the code if you're using a different window name.

Add the code to the HTML document containing the X emulator applet (`xde.html`, in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

### Related topics

- [X emulator applet](#)
- [getProperty \(X emulator applet\)](#)
- [unregisterProperty \(X emulator applet\)](#)
- [registerProperty \(X emulator applet\)](#)

## suspendApplication (X emulator applet)

### Syntax

```
void suspendApplication()
```

### Description

The `suspendApplication` method suspends or ends the current emulator session:

- If the application is resumable, the session is suspended.
- If the application isn't resumable, the session ends and the application exits.

### Examples

```
<SCRIPT LANGUAGE="JavaScript">

window.onerror = trapError

function trapError(message, url, line) {
    alert("There's no X emulator session to stop");
    return true
}

function stopEmulator() {
    top.WebtopFrame.DisplayFrame.document.applets["Tarantella X Emulator"].
suspendApplication();
    alert("X emulator session stopped");
}

</SCRIPT>

<FORM>
    <INPUT TYPE=button VALUE="Stop" onclick="stopEmulator()">
</FORM>
```

This example adds a button beneath the links on users' webtops. When a user clicks this button, Secure Global Desktop stops the current X emulator session, if one is running.

Add the code to the HTML document containing the webtop tray applet (`left.html` in the `sco/tta/standard` webtop theme), after the `TTAAPPLET` declaration.

**Note** This example assumes you are using the `sco/tta/standard` webtop theme. If you're using another theme, with different frame names and layouts, or different applet names, you'll need to modify the lines that invoke the `suspendApplication` method to access the X emulator applet used by your new theme.

#### Related topics

- [X emulator applet](#)

## unregisterProperty (X emulator applet)

### Syntax

```
void unregisterProperty(window, property)
```

### Description

The `unregisterProperty` method tells Secure Global Desktop to stop checking for changes in a previously registered X property.

*window* is the name of the X window whose property you want to unregister. (This name is contained in the X window's `WM_NAME` X property.) Use an empty string ("") to specify the root window.

*property* is the name of the X property you want to unregister. For example, the `WM_COMMAND` X property contains the command used to start the application that the X window is displaying.

Unregistering X properties when you're finished with them helps keep performance overheads to a minimum.

**Note** Once you've unregistered an X property in this way, you won't be able to use the `getProperty` method to retrieve its value.

### Examples

See the example for the `registerProperty` method to see how `unregisterProperty` is used.

#### Related topics

- [X emulator applet](#)
- [getProperty \(X emulator applet\)](#)
- [setProperty \(X emulator applet\)](#)
- [registerProperty \(X emulator applet\)](#)





# Sun Secure Global Desktop Software Administration Guide

## Getting started [Next section](#)

- Tutorials
  - [Introducing Sun Secure Global Desktop Software](#)
  - [Understanding webtop and emulator sessions](#)
  - [Integrating Secure Global Desktop with the desktop Start Menu](#)
  - [Introducing Array Manager](#)
  - [Introducing Object Manager](#)
  - [Securing client connections with Secure Global Desktop security services](#)
  - [Introducing the three-tier architecture](#)
  - [Objects and the organizational hierarchy](#)
  - [Users and trusted Secure Global Desktop servers](#)
- Case studies
  - [Creating and configuring a person object](#)
  - [Creating and publishing an application object to users](#)
  - [Using shadowing to troubleshoot a user's problem](#)
- Reference
  - [The tarantella command](#)
  - [Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop](#)
  - [Licensing and Sun Secure Global Desktop Software](#)
  - [Setting up and dismantling a Secure Global Desktop array](#)
  - [Sun Secure Global Desktop Software legal and copyright information](#)
- Frequently asked questions
  - [How do I add new Secure Global Desktop Administrators?](#)
  - [What do I need to tell my users?](#)
  - [Do I need to license Windows Terminal Services?](#)

## Clients and webtops [Next section](#)

- Tutorials
  - [Introducing Sun Secure Global Desktop Software](#)

- Integrating Secure Global Desktop with the desktop Start Menu
- Securing client connections with Secure Global Desktop security services
- **Reference**
  - Working with the Sun Secure Global Desktop Client
  - Configuring the Sun Secure Global Desktop Client for desktop Start Menu integration
  - Profiles and the Sun Secure Global Desktop Client
  - Native Client preferences files on UNIX, Linux and Mac OS X client devices
  - Relocating the browser-based webtop to your own JSP container
  - Running the Native Client from the command line
  - Profile Editing (--editprofile)
  - Secure Global Desktop and Java archives
- **Frequently asked questions**
  - Can users access Secure Global Desktop without Java technology?
  - Does the browser-based webtop use themes?
  - How can I make additional Native Clients available?

## **Arrays, servers and load balancing** Next section

- **Tutorials**
  - Introducing Array Manager
  - Introducing the Secure Global Desktop Web Server
  - Introducing webtop and emulator session load balancing
  - Introducing application server load balancing
  - The Secure Global Desktop datastore and Tarantella Federated Naming
- **Reference**
  - Backing up and restoring a Secure Global Desktop installation
  - Application Launch properties (array-wide)
  - Array properties (array-wide)
  - Channel Protocol Engine properties (server-specific)
  - Character Protocol Engine properties (server-specific)
  - Emulator Sessions properties (array-wide)
  - Execution Protocol Engine properties (server-specific)
  - General properties (server-specific)
  - Licenses properties (array-wide)
  - Load Balancing properties (array-wide)
  - Print Protocol Engine properties (server-specific)
  - Printing properties (array-wide)

- Secure Global Desktop Login properties (array-wide)
- Security properties (array-wide)
- Security properties (server-specific)
- Setting up and dismantling a Secure Global Desktop array
- Smart Card Protocol Engine properties
- Tuning properties (server-specific)
- X Protocol Engine properties (server-specific)
- Audio Protocol Engine properties (server-specific)
- Configuring application server load balancing
- Editing application server load balancing properties
- Tuning application server load balancing
- Using log filters for auditing
- Using log filters to troubleshoot problems with the Secure Global Desktop server
- Configuring your own web server for use with Secure Global Desktop
- Hosts tab (--appserv)
- Location (--location)
- The tarantella archive command
- The tarantella array command
- The tarantella arraymanager command
- The tarantella config command
- The tarantella query command
- The tarantella restart command
- The tarantella start command
- The tarantella status command
- The tarantella stop command
- Managing unauthenticated connections to Secure Global Desktop
- Troubleshooting
  - Troubleshooting CPU/memory-based application server load balancing
  - All login authorities are disabled and no-one can access Secure Global Desktop
  - Every server in the array has been disabled and no-one can access Secure Global Desktop
  - Users are unable to relocate their webtop sessions
- Frequently asked questions
  - What is an array?
  - What's in the Secure Global Desktop installation directory?
  - Where is Secure Global Desktop installed?

- **Tutorials**
  - Secure Global Desktop and user authentication
  - Understanding webtop and emulator sessions
  - Introducing web server authentication
  - Login authorities
- **Case studies**
  - Creating and configuring a person object
  - Populating the Secure Global Desktop organizational hierarchy using a batch script
- **Reference**
  - Person object
  - Execution Protocol Engine properties (server-specific)
  - Roles in Secure Global Desktop
  - Secure Global Desktop Login properties (array-wide)
  - The Active Directory login authority
  - The Anonymous user login authority
  - The ENS login authority
  - The LDAP login authority
  - The NT login authority
  - The SecurID login authority
  - The UNIX group login authority
  - The UNIX user login authority
  - The authentication token login authority
  - Using shared accounts for "guest" users
  - Web server/third party authentication
  - Working with users in different locales
  - Denying users access to Secure Global Desktop after failed login attempts
  - Enabling the Active Directory login authority
  - Enabling the LDAP login authority
  - Enabling the NT login authority
  - Enabling the SecurID login authority
  - Enabling web server authentication for the browser-based webtop
  - Enabling web server authentication for the classic webtop
  - Mirroring your LDAP organization in ENS
  - Security considerations of using web server authentication
  - Using Directory Services Integration
  - Using the authentication token login authority for automatic logins

- Bandwidth Limit (--bandwidth)
- Client Drive Mapping (--cdm)
- Connections (--conntype)
- Description (--description)
- Email Address (--email)
- Increasing launch timeouts
- Inherit parent's webtop content (--inherit)
- Keyboard Map (--keymap)
- Links tab (--links)
- Login Script (--login)
- Login script Tcl commands
- Login script variables
- Login scripts supplied with Secure Global Desktop
- May log in to Secure Global Desktop (--enabled)
- Name (--name) objects with "common name"
- Preferred Locale (--preflocale)
- Shared between users (guest) (--shared)
- Surname (--surname)
- The tarantella Tcl command
- The tarantella cache command
- The tarantella emulatorsession command
- The tarantella object command
- The tarantella passcache command
- The tarantella role command
- The tarantella tokencache command
- The tarantella webtopsession command
- Username (--user)
- Using SecurID for application server authentication
- Webtop Theme (--webtop)
- Windows NT Domain (--ntdomain)
- Client printers (--mapprinters)
- Driver name (--pdfdriver)
- Let users print to a PDF local file (--pdfviewerenabled)
- Let users print to a PDF printer (--pdfenabled)
- Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
- Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
- The tarantella tokencache delete command

- The tarantella tokencache list command
- Trusted users and third party authentication
- User-specific printing configuration (--userprintingconfig)
- Troubleshooting
  - A session doesn't end when the user exits the application
  - Users are unable to copy and paste text or graphics
  - Users experience problems with web server authentication
  - Using Windows Terminal Services, users are prompted for usernames and passwords too often
  - An "Ambiguous username" dialog is displayed when a user tries to log in
  - LDAP users can't log in to Secure Global Desktop
  - Users see font problems
  - A login script returns an error
  - All login authorities are disabled and no-one can access Secure Global Desktop
  - Secure Global Desktop uses too much of my network's bandwidth
- Frequently asked questions
  - What do I need to tell my users?
  - How do I tell what connection type a user gets?
  - What happens when a user's password expires?
  - What is a role object?
  - Can I deny an LDAP user access to Secure Global Desktop?
  - Can I use PKI client certificates with web server authentication?
  - Can I use SafeWord PremierAccess with web server authentication?
  - Can I use other web authentication schemes with Secure Global Desktop web server authentication?
  - What are login scripts?

## **Applications, documents and hosts** Next section

- Tutorials
  - Understanding webtop and emulator sessions
  - Using copy and paste with Secure Global Desktop
  - Using shadowing in the classroom
- Case studies
  - Creating and publishing an application object to users
  - Populating the Secure Global Desktop organizational hierarchy using a batch script
  - Remapping or hiding Windows 2000/2003 application server drives

- Launching applications from JavaScript
- Using shadowing to troubleshoot a user's problem
- Reference
  - 3270 application object
  - 5250 application object
  - Character application object
  - Document object
  - Host object
  - Windows application object
  - X application object
  - Application Launch properties (array-wide)
  - Character Protocol Engine properties (server-specific)
  - Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop
  - Configuring client drive mapping
  - Emulator Sessions properties (array-wide)
  - Load Balancing properties (array-wide)
  - X Protocol Engine properties (server-specific)
  - Available to run applications (--available)
  - Configuring access to serial ports
  - Load Balancing Algorithm (--loadbal)
  - Mirroring your LDAP organization in ENS
  - Using Directory Services Integration
  - Using seamless windows for Windows applications
  - Using smart cards with Windows applications
  - 3270 Host (--hostname)
  - AS/400 Host (--hostname)
  - Address (--address)
  - Allow delayed updates (--delayed)
  - Answerback Message (--answermsg)
  - Application Command (--app)
  - Application key mode (--appkeymode)
  - Application supports 3-button mouse only (--force3button)
  - Arguments For Command (--args)
  - Attribute Map (--attributemap)
  - Authentication (--auth)
  - Background Color (--3270bg) 3270
  - Background Color (--bg) 5250



- Border Style (--border)
- Client's maximum size (--maximize)
- Clipboard Access (--clipboard)
- Clipboard Security Level (--clipboardlevel)
- Close Telnet Action (--3270tnclose) 3270
- Close Telnet Action (--tnclose) 5250
- Code Page (--codepage)
- Color (--rootcolor)
- Color Map (--colormap)
- Color depth (--depth)
- Color quality (--quality)
- Columns (--cols)
- Command Compression (--compression)
- Command Execution (--execution)
- Connection Method (--method)
- Cursor (--cursor)
- Cursor Keys (--cursorkeys)
- Description (--description)
- Display Using (--displayusing)
- Emulation Type (--emulator)
- Emulator Applet Page (--empage)
- Enable File and Settings menus (--3270si) 3270
- Enable File and Settings menus (--si) 5250
- Enable X Security Extension (--securityextension)
- Enable menu bar (--3270mb) 3270
- Enable menu bar (--mb) 5250
- Environment Variables (--env)
- Escape Sequences (--escape)
- Euro Character (--euro)
- Fixed font size (--fixedfont)
- Font Family (--font)
- Font Size (--fontsize)
- Foreground Color (--3270fg) 3270
- Foreground Color (--fg) 5250
- Height (--height)
- Host Locale (--hostlocale)

- Hosts tab (--appserv)
- Interlaced Images (--interlaced)
- Keep launch connection open (--keepopen)
- Keyboard Map (--keymap)
- Keyboard Type (--3270kt) 3270
- Keyboard Type (--kt) 5250
- Keypad (--keypad)
- LDAP Groups (--ldapgroups)
- LDAP Search (--ldapsearch)
- LDAP Users (--ldapusers)
- Launching a single application without displaying a webtop
- Lines (--lines)
- Location (--location)
- Lock keymap (--lockkeymap)
- Login Script (--login)
- Max Instances (--maxinstances)
- Maximize the emulator window (--3270ma) 3270
- Maximize the emulator window (--ma) 5250
- Middle Mouse Timeout (--middlemouse)
- Monitor Resolution (--dpi)
- Name (--name) objects with "common name"
- Open in new browser window (--newbrowser)
- Port Number (--portnumber) 3270
- Port Number (--portnumber) 5250
- Protocol Arguments (--protoargs)
- Resumable (--resumable)
- Resumable For (--resumetimeout)
- Root Window (--roottype)
- Scale to fit window (--scalable)
- Scroll Style (--scrollstyle)
- Serial Port Mapping (--serialport)
- Session Ends When (--endswhen)
- Share resources between similar sessions (--share)
- Soft Button Levels (--3270bl) 3270
- Soft Button Levels (--bl) 5250
- Status Line (--statusline)
- Terminal Type (--termttype)

- Terminal emulator attribute maps
- Terminal emulator color maps
- Terminal emulator keyboard maps
- The tarantella emulatorsession command
- The tarantella object command
- Try running from client first (--trylocal)
- URL (--url)
- Use Windows cursor (--wincursor)
- Use graphics acceleration (--accel)
- Using Remote Desktop on Microsoft Windows XP Professional
- Webtop Hints (--hints)
- Webtop Icon (--icon)
- Width (--width)
- Window Close Action (--windowclose)
- Window Manager (--winmgr)
- Windows NT Domain (--ntdomain)
- Windows Protocol (--winproto)
- Wrap long lines (--autowrap)
- Customizing the Native Client for UNIX
- **Troubleshooting**
  - A session doesn't end when the user exits the application
  - An application exits immediately after starting
  - An application won't start
  - An application's animation appears "jumpy"
  - Applications disappear after about two minutes
  - Users are having problems accessing client drives
  - Users complain of poor performance with the Windows desktop
  - When X authorization is enabled, applications fail to start
  - A Kiosk application isn't appearing full-screen
  - An application requires a richer set of cursors
  - In some X applications, the ALT and ALT GR keys do not work
  - Troubleshooting sound in Windows applications
  - Users are unable to use smart cards with Windows applications
  - Users have problems displaying high color X applications
  - Running Windows applications on client devices
  - Secure Global Desktop uses too much of my network's bandwidth

- Users see window clipping with Client Window Management applications
- Frequently asked questions
  - Can I run another SMB service with client drive mapping?
  - Do I need to license Windows Terminal Services?
  - How do I enable sound in Windows applications?
  - Can I prevent users from launching applications with a different username and password?
  - Can I use Secure Global Desktop to access VMS applications?
  - How do I run a Common Desktop Environment (CDE) session?
  - How do I use my own X fonts?
  - What X fonts are installed?
  - Can I access a web application through Secure Global Desktop?
  - Can I use multiple monitors with Secure Global Desktop?

## Organizing your resources Next section

- Tutorials
  - Introducing Object Manager
  - Objects and the organizational hierarchy
- Case studies
  - Populating the Secure Global Desktop organizational hierarchy using a batch script
- Reference
  - Active Directory container object
  - Domain component object
  - Group object
  - Organization object
  - Organizational unit object
  - Client Drive Mapping (--cdm)
  - Connections (--conntype)
  - Description (--description)
  - Inherit parent's webtop content (--inherit)
  - Links tab (--links)
  - Members tab (--member)
  - Name (--name) domain component object
  - Name (--name) organization object
  - Name (--name) organizational unit object
  - Naming objects in the organizational hierarchy
  - The tarantella object command

- Webtop Theme (--webtop)
- Client printers (--mapprinters)
- Driver name (--pdfdriver)
- Let users print to a PDF local file (--pdfviewerenabled)
- Let users print to a PDF printer (--pdfenabled)
- Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
- Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
- User-specific printing configuration (--userprintingconfig)
- Troubleshooting
  - All Administrators have been removed and no-one can use the administration tools
- Frequently asked questions
  - What is ENS?
  - What is the Tarantella System Objects organization?

## Security [Next section](#)

- Tutorials
  - Securing client connections with Secure Global Desktop security services
  - Security and Secure Global Desktop
  - Improving security between Secure Global Desktop servers and application servers
  - Improving security between client devices and Secure Global Desktop servers
  - Users and trusted Secure Global Desktop servers
  - Sharing web server and Secure Global Desktop server certificates
- Case studies
  - Obtaining and installing an X.509 certificate
  - Giving secure connections across the Internet
  - Giving secure connections to a Secure Global Desktop server
  - Giving secure connections to all users in a department
  - Using Secure Global Desktop with the HTTPS port through a firewall
  - Using Secure Global Desktop with firewalls
- Reference
  - Securing connections between Secure Global Desktop servers
  - Securing connections to Active Directory and LDAP directory servers
  - Securing the SOAP connections to a Secure Global Desktop server
  - Security properties (array-wide)
  - Security properties (server-specific)
  - User prompts and X.509 certificates

- Using Secure Global Desktop with proxy servers
- Connections (--conntype)
- Installing and using SSH with Secure Global Desktop
- Selecting a cipher suite for secure connections
- The tarantella security command
- Tuning the SSL Daemon process
- **Troubleshooting**
  - Solaris OS users are unable to log in when Secure Global Desktop security services are running
  - Users are unable to connect to Secure Global Desktop when it is in firewall forwarding mode
- **Frequently asked questions**
  - What are X.509 certificates and why do I need one?
  - What certificates does Secure Global Desktop support?
  - How can I support users with a client-side firewall that only allows connections on the HTTPS port?
  - How do I tell what connection type a user gets?
  - What are peer DNS names and external DNS names?
  - Can I use an X.509 certificate for another product with Secure Global Desktop?
  - How do I support additional Certificate Authorities?
  - What are Secure Global Desktop security services?
  - Can I use PKI client certificates with web server authentication?
  - Can I use SafeWord PremierAccess with web server authentication?
  - Can I use other web authentication schemes with Secure Global Desktop web server authentication?
  - What ports does Secure Global Desktop use?
  - Can I chain Certificate Authority certificates?

## **Printing** Next section

- **Tutorials**
  - Introducing Secure Global Desktop printing
- **Reference**
  - Print Protocol Engine properties (server-specific)
  - Printing properties (array-wide)
  - Configuring printing for UNIX, Linux and Mac OS X clients
  - Configuring printing if you use the Common UNIX Printing System (CUPS)
  - Configuring the Secure Global Desktop server to accept remote print requests
  - Printing from a Microsoft Windows 2000/2003 application server

- Printing from a Microsoft Windows NT 3.51 application server
- Printing from a Microsoft Windows NT 4 application server
- Printing from a UNIX or Linux application server
- The prtinstall.en.sh script
- Configuring Secure Global Desktop PDF printing
- The tarantella print command
- Client printers (--mapprinters)
- Configuring Secure Global Desktop print job conversion
- Driver name (--pdfdriver)
- Let users print to a PDF local file (--pdfviewerenabled)
- Let users print to a PDF printer (--pdfenabled)
- Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
- Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
- User-specific printing configuration (--userprintingconfig)
- Troubleshooting
  - Users cannot print from applications displayed through Secure Global Desktop
  - Troubleshooting printer preferences and settings
  - When Secure Global Desktop printing has been disabled, print jobs can still be queued
  - Windows 2000 users are unable to print a file from a mapped network drive
  - With Secure Global Desktop PDF printing, fonts don't print as expected
- Frequently asked questions
  - If the array changes, do I have to re-configure printing?
  - Why do users see a printer called \_Default in their Windows application?
  - Can I force users to print only to their default client printer?
  - Can I set a time limit for print jobs?
  - Do I have to use distributed printing?
  - Can I change the name of the printer in the Windows 2000/2003 application session?

## Commands Next section

- Reference
  - The tarantella command
  - The tarantella Tcl command
  - The tarantella archive command
  - The tarantella array command
  - The tarantella arraymanager command
  - The tarantella cache command

- The tarantella config command
- The tarantella emulatorsession command
- The tarantella help command
- The tarantella license command
- The tarantella object command
- The tarantella objectmanager command
- The tarantella passcache command
- The tarantella print command
- The tarantella query command
- The tarantella restart command
- The tarantella role command
- The tarantella security command
- The tarantella setup command
- The tarantella start cdm command
- The tarantella start command
- The tarantella status command
- The tarantella stop cdm command
- The tarantella stop command
- The tarantella tokencache command
- The tarantella uninstall command
- The tarantella version command
- The tarantella webserver command
- The tarantella webtopsession command
- The tarantella array detach command
- The tarantella array join command
- The tarantella array list command
- The tarantella array make\_primary command
- The tarantella config edit command
- The tarantella config list command
- The tarantella emulatorsession end command
- The tarantella emulatorsession info command
- The tarantella emulatorsession list command
- The tarantella emulatorsession shadow command
- The tarantella emulatorsession suspend command
- The tarantella license add command
- The tarantella license info command
- The tarantella license list command



- The tarantella license query command
- The tarantella license remove command
- The tarantella license status command
- The tarantella object add\_host command
- The tarantella object add\_link command
- The tarantella object add\_member command
- The tarantella object delete command
- The tarantella object edit command
- The tarantella object list\_attributes command
- The tarantella object list\_contents command
- The tarantella object new\_3270app command
- The tarantella object new\_5250app command
- The tarantella object new\_charapp command
- The tarantella object new\_container command
- The tarantella object new\_dc command
- The tarantella object new\_doc command
- The tarantella object new\_group command
- The tarantella object new\_host command
- The tarantella object new\_org command
- The tarantella object new\_orgunit command
- The tarantella object new\_person command
- The tarantella object new\_windowsapp command
- The tarantella object new\_xapp command
- The tarantella object remove\_host command
- The tarantella object remove\_link command
- The tarantella object remove\_member command
- The tarantella object rename command
- The tarantella object script command
- The tarantella passcache delete command
- The tarantella passcache edit command
- The tarantella passcache list command
- The tarantella passcache new command
- The tarantella print cancel command
- The tarantella print list command
- The tarantella print move command
- The tarantella print pause command

- The tarantella print resume command
- The tarantella print start command
- The tarantella print status command
- The tarantella print stop command
- The tarantella query audit command
- The tarantella query billing command
- The tarantella query errlog command
- The tarantella query uptime command
- The tarantella role add\_link command
- The tarantella role add\_member command
- The tarantella role list command
- The tarantella role list\_links command
- The tarantella role list\_members command
- The tarantella role remove\_link command
- The tarantella role remove\_member command
- The tarantella security certinfo command
- The tarantella security certrequest command
- The tarantella security certuse command
- The tarantella security customca command
- The tarantella security decryptkey command
- The tarantella security fingerprint command
- The tarantella security peerca command
- The tarantella security start command
- The tarantella security stop command
- The tarantella tokencache delete command
- The tarantella tokencache list command
- The tarantella tscal command
- The tarantella tscal free command
- The tarantella tscal list command
- The tarantella tscal return command
- The tarantella webserver add\_trusted\_user command
- The tarantella webserver delete\_trusted\_user command
- The tarantella webserver list\_trusted\_users command
- The tarantella webserver restart command
- The tarantella webserver start command
- The tarantella webserver stop command
- The tarantella webtopsession list command

- The tarantella webtopsession logout command

## Applets [Back to top](#)

- Case studies
  - Launching applications from JavaScript
- Reference
  - The ttawebtop.cgi CGI program
  - Client drive mapping (CDM) applet
  - Client drive mapping (CDM) applet parameters
  - Framework applet
  - Framework applet parameters
  - Login applet
  - Login applet parameters
  - Print applet
  - Print applet parameters
  - Terminal emulator applet
  - Terminal emulator applet parameters
  - The TTAAPPLET tag
  - Webtop script applet
  - Webtop script applet parameters
  - Webtop tray applet
  - Webtop tray applet parameters
  - X emulator applet
  - X emulator applet parameters
  - Applet parameter data types
  - Logging in with the Secure Global Desktop applets
  - addValue (framework applet)
  - areObjectsInitialized (webtop script and webtop tray applets)
  - cancelCurrentJob (print applet)
  - closeHierarchyLevel (webtop script and webtop tray applets)
  - countJobs (print applet)
  - getActive (print applet)
  - getApplicationType (webtop script and webtop tray applets)
  - getCurrentIteratorElement (webtop script and webtop tray applets)
  - getEmulatorState (X emulator applet)
  - getEmulatorState (terminal emulator applet)

- `getEnabled` (print applet)
- `getIteratorForAllOpenHierarchyLevels` (webtop script and webtop tray applets)
- `getIteratorForHierarchyLevel` (webtop script and webtop tray applets)
- `getIteratorHasMoreElements` (webtop script and webtop tray applets)
- `getLaunchWaitTimeOut` (webtop script and webtop script applets)
- `getNextIteratorElement` (webtop script and webtop tray applets)
- `getNumberOfObjects` (webtop script and webtop tray applets)
- `getNumberOfObjectsInGroup` (webtop script and webtop tray applets)
- `getObjectClass` (webtop script and webtop tray applets)
- `getObjectDisplayName` (webtop script and webtop tray applets)
- `getObjectDisplayNameByName` (webtop script and webtop tray applets)
- `getObjectFullName` (webtop script and webtop tray applets)
- `getObjectImageName` (webtop script and webtop tray applets)
- `getObjectImageNameByName` (webtop script and webtop tray applets)
- `getObjectPlacement` (webtop script and webtop tray applets)
- `getParentGroupName` (webtop script and webtop tray applets)
- `getPrintState` (print applet)
- `getPrinterName` (print applet)
- `getPrinterPort` (print applet)
- `getPrinterType` (print applet)
- `getProperty` (X emulator applet)
- `getText` (terminal emulator applet)
- `getTotalNumberOfObjects` (webtop script and webtop tray applets)
- `getUnixTempDir` (print applet)
- `getUserName` (framework applet)
- `getValue` (framework applet)
- `getWebtopFramesetURL` (framework applet)
- `getWebtopURL` (framework applet)
- `getWindowsTempDir` (print applet)
- `isApplication` (webtop script and webtop tray applets)
- `isDocument` (webtop script and webtop tray applets)
- `isGroup` (webtop script and webtop tray applets)
- `isHierarchyEnabled` (webtop script and webtop tray applets)
- `isLoggedIn` (framework applet)
- `isOpenGroup` (webtop script and webtop tray applets)
- `isRunning` (webtop script and webtop tray applets)
- `killIterator` (webtop script and webtop tray applets)

- launchByObjectName (webtop script and webtop tray applets)
- launchByObjectNumber (webtop script and webtop tray applets)
- login method
- logout method
- openGroup (webtop tray applet)
- openHierarchyLevel (webtop script and webtop tray applets)
- openParentGroup (webtop tray applet)
- receivedEvent (webtop script and webtop tray applets)
- registerProperty (X emulator applet)
- removeValue (framework applet)
- resetNamePassword (login applet)
- scriptStart method
- sendKey (terminal emulator applet)
- setActive (print applet)
- setEnabled (print applet)
- setLaunchWaitTimeOut (webtop script and webtop tray applets)
- setPausedState (print applet)
- setPrinterName (print applet)
- setPrinterPort (print applet)
- setPrinterType (print applet)
- setProperty (X emulator applet)
- setText (terminal emulator applet)
- setUnixTempDir (print applet)
- setWindowsTempDir (print applet)
- suspendApplication (X emulator applet)
- suspendApplication (terminal emulator applet)
- unregisterProperty (X emulator applet)
- Frequently asked questions
  - How does Secure Global Desktop use applets?

# Sun Secure Global Desktop Software Administration Guide

## Getting started [Next section](#)

- For new Secure Global Desktop Administrators
  - [How do I add new Secure Global Desktop Administrators?](#)
  - [Introducing Sun Secure Global Desktop Software](#)
  - [The tarantella command](#)
  - [Understanding webtop and emulator sessions](#)
  - [What do I need to tell my users?](#)
  - [Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop](#)
  - [Do I need to license Windows Terminal Services?](#)
  - [Integrating Secure Global Desktop with the desktop Start Menu](#)
  - [Introducing Array Manager](#)
  - [Introducing Object Manager](#)
  - [Securing client connections with Secure Global Desktop security services](#)
  - [Creating and configuring a person object](#)
  - [Creating and publishing an application object to users](#)
  - [Introducing the three-tier architecture](#)
  - [Objects and the organizational hierarchy](#)
  - [Users and trusted Secure Global Desktop servers](#)
  - [Sun Secure Global Desktop Software legal and copyright information](#)
- For day-to-day Secure Global Desktop administration
  - [Licensing and Sun Secure Global Desktop Software](#)
  - [Setting up and dismantling a Secure Global Desktop array](#)
  - [Using shadowing to troubleshoot a user's problem](#)

## Clients and webtops [Next section](#)

- For new Secure Global Desktop Administrators
  - [Introducing Sun Secure Global Desktop Software](#)
  - [Working with the Sun Secure Global Desktop Client](#)
  - [Configuring the Sun Secure Global Desktop Client for desktop Start Menu integration](#)

- Integrating Secure Global Desktop with the desktop Start Menu
- Profiles and the Sun Secure Global Desktop Client
- Securing client connections with Secure Global Desktop security services
- For day-to-day Secure Global Desktop administration
  - Can users access Secure Global Desktop without Java technology?
  - Does the browser-based webtop use themes?
  - Profile Editing (--editprofile)
- For in-depth Secure Global Desktop administration
  - Native Client preferences files on UNIX, Linux and Mac OS X client devices
  - Running the Native Client from the command line
  - How can I make additional Native Clients available?
  - Secure Global Desktop and Java archives
- For Secure Global Desktop customizers
  - Relocating the browser-based webtop to your own JSP container

## **Arrays, servers and load balancing** Next section

- For new Secure Global Desktop Administrators
  - Introducing Array Manager
  - Introducing the Secure Global Desktop Web Server
  - Introducing webtop and emulator session load balancing
  - Introducing application server load balancing
  - The Secure Global Desktop datastore and Tarantella Federated Naming
  - Troubleshooting CPU/memory-based application server load balancing
  - What is an array?
  - Configuring your own web server for use with Secure Global Desktop
  - The tarantella restart command
  - The tarantella start command
  - The tarantella status command
  - The tarantella stop command
  - What's in the Secure Global Desktop installation directory?
  - Where is Secure Global Desktop installed?
- For day-to-day Secure Global Desktop administration
  - Application Launch properties (array-wide)
  - Array properties (array-wide)
  - Channel Protocol Engine properties (server-specific)
  - Character Protocol Engine properties (server-specific)

- Emulator Sessions properties (array-wide)
- Execution Protocol Engine properties (server-specific)
- General properties (server-specific)
- Licenses properties (array-wide)
- Load Balancing properties (array-wide)
- Print Protocol Engine properties (server-specific)
- Printing properties (array-wide)
- Secure Global Desktop Login properties (array-wide)
- Security properties (array-wide)
- Security properties (server-specific)
- Setting up and dismantling a Secure Global Desktop array
- Smart Card Protocol Engine properties
- Tuning properties (server-specific)
- X Protocol Engine properties (server-specific)
- Audio Protocol Engine properties (server-specific)
- Configuring application server load balancing
- Using log filters for auditing
- Using log filters to troubleshoot problems with the Secure Global Desktop server
- Hosts tab (--appserv)
- Location (--location)
- The tarantella array command
- The tarantella query command
- Users are unable to relocate their webtop sessions
- For in-depth Secure Global Desktop administration
  - Backing up and restoring a Secure Global Desktop installation
  - Editing application server load balancing properties
  - Tuning application server load balancing
  - All login authorities are disabled and no-one can access Secure Global Desktop
  - Every server in the array has been disabled and no-one can access Secure Global Desktop
  - The tarantella archive command
  - The tarantella arraymanager command
  - The tarantella config command
  - Managing unauthenticated connections to Secure Global Desktop

## **Users and authentication** Next section

- For new Secure Global Desktop Administrators



- A session doesn't end when the user exits the application
- Secure Global Desktop and user authentication
- Understanding webtop and emulator sessions
- What do I need to tell my users?
- Working with users in different locales
- Creating and configuring a person object
- For day-to-day Secure Global Desktop administration
  - Person object
  - Execution Protocol Engine properties (server-specific)
  - Login authorities
  - Roles in Secure Global Desktop
  - Secure Global Desktop Login properties (array-wide)
  - The Active Directory login authority
  - The Anonymous user login authority
  - The ENS login authority
  - The LDAP login authority
  - The NT login authority
  - The SecurID login authority
  - The UNIX group login authority
  - The UNIX user login authority
  - The authentication token login authority
  - Users are unable to copy and paste text or graphics
  - Using Windows Terminal Services, users are prompted for usernames and passwords too often
  - Using shared accounts for "guest" users
  - Web server/third party authentication
  - An "Ambiguous username" dialog is displayed when a user tries to log in
  - Enabling the Active Directory login authority
  - Enabling the LDAP login authority
  - Enabling the NT login authority
  - Enabling the SecurID login authority
  - LDAP users can't log in to Secure Global Desktop
  - Mirroring your LDAP organization in ENS
  - Using Directory Services Integration
  - Using the authentication token login authority for automatic logins
  - What is a role object?
  - Bandwidth Limit (--bandwidth)

- Client Drive Mapping (--cdm)
- Connections (--conntype)
- Description (--description)
- Email Address (--email)
- Inherit parent's webtop content (--inherit)
- Keyboard Map (--keymap)
- Links tab (--links)
- Login Script (--login)
- May log in to Secure Global Desktop (--enabled)
- Name (--name) objects with "common name"
- Preferred Locale (--preflocale)
- Shared between users (guest) (--shared)
- Surname (--surname)
- The tarantella emulatorsession command
- The tarantella object command
- The tarantella role command
- The tarantella webtopsession command
- Username (--user)
- Using SecurID for application server authentication
- Webtop Theme (--webtop)
- Windows NT Domain (--ntdomain)
- Client printers (--mapprinters)
- Driver name (--pdfdriver)
- Let users print to a PDF local file (--pdfviewerenabled)
- Let users print to a PDF printer (--pdfenabled)
- Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
- Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
- User-specific printing configuration (--userprintingconfig)
- For in-depth Secure Global Desktop administration
  - How do I tell what connection type a user gets?
  - Introducing web server authentication
  - Users experience problems with web server authentication
  - Denying users access to Secure Global Desktop after failed login attempts
  - Enabling web server authentication for the browser-based webtop
  - Enabling web server authentication for the classic webtop
  - Populating the Secure Global Desktop organizational hierarchy using a batch script
  - Security considerations of using web server authentication

- Users see font problems
- What happens when a user's password expires?
- All login authorities are disabled and no-one can access Secure Global Desktop
- Can I deny an LDAP user access to Secure Global Desktop?
- Can I use PKI client certificates with web server authentication?
- Can I use SafeWord PremierAccess with web server authentication?
- Can I use other web authentication schemes with Secure Global Desktop web server authentication?
- The tarantella cache command
- The tarantella passcache command
- The tarantella tokencache command
- Secure Global Desktop uses too much of my network's bandwidth
- The tarantella tokencache delete command
- The tarantella tokencache list command
- Trusted users and third party authentication
- For Secure Global Desktop customizers
  - A login script returns an error
  - Increasing launch timeouts
  - Login script Tcl commands
  - Login script variables
  - Login scripts supplied with Secure Global Desktop
  - The tarantella Tcl command
  - What are login scripts?

## **Applications, documents and hosts** Next section

- For new Secure Global Desktop Administrators
  - A session doesn't end when the user exits the application
  - An application exits immediately after starting
  - An application won't start
  - Understanding webtop and emulator sessions
  - Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop
  - Configuring client drive mapping
  - Do I need to license Windows Terminal Services?
  - Creating and publishing an application object to users
  - Using copy and paste with Secure Global Desktop
- For day-to-day Secure Global Desktop administration

- 3270 application object
- 5250 application object
- Character application object
- Document object
- Host object
- Windows application object
- X application object
- An application's animation appears "jumpy"
- Application Launch properties (array-wide)
- Applications disappear after about two minutes
- Character Protocol Engine properties (server-specific)
- Emulator Sessions properties (array-wide)
- Load Balancing properties (array-wide)
- X Protocol Engine properties (server-specific)
- Available to run applications (--available)
- Configuring access to serial ports
- How do I enable sound in Windows applications?
- Load Balancing Algorithm (--loadbal)
- Mirroring your LDAP organization in ENS
- Users are having problems accessing client drives
- Users complain of poor performance with the Windows desktop
- Using Directory Services Integration
- Using seamless windows for Windows applications
- Using smart cards with Windows applications
- 3270 Host (--hostname)
- A Kiosk application isn't appearing full-screen
- AS/400 Host (--hostname)
- Address (--address)
- Allow delayed updates (--delayed)
- An application requires a richer set of cursors
- Answerback Message (--answermsg)
- Application Command (--app)
- Application key mode (--appkeymode)
- Application supports 3-button mouse only (--force3button)
- Arguments For Command (--args)
- Attribute Map (--attributemap)
- Authentication (--auth)

- Background Color (--3270bg) 3270
- Background Color (--bg) 5250
- Border Style (--border)
- Can I use Secure Global Desktop to access VMS applications?
- Client's maximum size (--maximize)
- Clipboard Access (--clipboard)
- Clipboard Security Level (--clipboardlevel)
- Close Telnet Action (--3270tnclose) 3270
- Close Telnet Action (--tnclose) 5250
- Code Page (--codepage)
- Color (--rootcolor)
- Color Map (--colormap)
- Color depth (--depth)
- Color quality (--quality)
- Columns (--cols)
- Command Compression (--compression)
- Command Execution (--execution)
- Connection Method (--method)
- Cursor (--cursor)
- Cursor Keys (--cursorkeys)
- Description (--description)
- Display Using (--displayusing)
- Emulation Type (--emulator)
- Emulator Applet Page (--empage)
- Enable File and Settings menus (--3270si) 3270
- Enable File and Settings menus (--si) 5250
- Enable X Security Extension (--securityextension)
- Enable menu bar (--3270mb) 3270
- Enable menu bar (--mb) 5250
- Environment Variables (--env)
- Escape Sequences (--escape)
- Euro Character (--euro)
- Fixed font size (--fixedfont)
- Font Family (--font)
- Font Size (--fontsize)
- Foreground Color (--3270fg) 3270

- Foreground Color (--fg) 5250
- Height (--height)
- Host Locale (--hostlocale)
- Hosts tab (--appserv)
- How do I run a Common Desktop Environment (CDE) session?
- In some X applications, the ALT and ALT GR keys do not work
- Interlaced Images (--interlaced)
- Keep launch connection open (--keepopen)
- Keyboard Map (--keymap)
- Keyboard Type (--3270kt) 3270
- Keyboard Type (--kt) 5250
- Keypad (--keypad)
- LDAP Groups (--ldapgroups)
- LDAP Search (--ldapsearch)
- LDAP Users (--ldapusers)
- Lines (--lines)
- Location (--location)
- Lock keymap (--lockkeymap)
- Login Script (--login)
- Max Instances (--maxinstances)
- Maximize the emulator window (--3270ma) 3270
- Maximize the emulator window (--ma) 5250
- Middle Mouse Timeout (--middlemouse)
- Monitor Resolution (--dpi)
- Name (--name) objects with "common name"
- Open in new browser window (--newbrowser)
- Port Number (--portnumber) 3270
- Port Number (--portnumber) 5250
- Protocol Arguments (--protoargs)
- Resumable (--resumable)
- Resumable For (--resumetimeout)
- Root Window (--roottype)
- Scale to fit window (--scalable)
- Scroll Style (--scrollstyle)
- Serial Port Mapping (--serialport)
- Session Ends When (--endswhen)
- Share resources between similar sessions (--share)

- Soft Button Levels (--3270bl) 3270
- Soft Button Levels (--bl) 5250
- Status Line (--statusline)
- Terminal Type (--termtype)
- The tarantella emulatorsession command
- The tarantella object command
- Troubleshooting sound in Windows applications
- Try running from client first (--trylocal)
- URL (--url)
- Use Windows cursor (--wincursor)
- Use graphics acceleration (--accel)
- Users are unable to use smart cards with Windows applications
- Users have problems displaying high color X applications
- Using Remote Desktop on Microsoft Windows XP Professional
- Using shadowing to troubleshoot a user's problem
- Webtop Hints (--hints)
- Webtop Icon (--icon)
- Width (--width)
- Window Close Action (--windowclose)
- Window Manager (--winmgr)
- Windows NT Domain (--ntdomain)
- Windows Protocol (--winproto)
- Wrap long lines (--autowrap)
- Can I access a web application through Secure Global Desktop?
- Customizing the Native Client for UNIX
- Running Windows applications on client devices
- Users see window clipping with Client Window Management applications
- For in-depth Secure Global Desktop administration
  - Can I run another SMB service with client drive mapping?
  - Populating the Secure Global Desktop organizational hierarchy using a batch script
  - Remapping or hiding Windows 2000/2003 application server drives
  - When X authorization is enabled, applications fail to start
  - Can I prevent users from launching applications with a different username and password?
  - How do I use my own X fonts?
  - Using shadowing in the classroom
  - What X fonts are installed?

- Can I use multiple monitors with Secure Global Desktop?
- Secure Global Desktop uses too much of my network's bandwidth
- For Secure Global Desktop customizers
  - Launching a single application without displaying a webtop
  - Launching applications from JavaScript
  - Terminal emulator attribute maps
  - Terminal emulator color maps
  - Terminal emulator keyboard maps

## Organizing your resources Next section

- For new Secure Global Desktop Administrators
  - Introducing Object Manager
  - Objects and the organizational hierarchy
  - What is ENS?
  - What is the Tarantella System Objects organization?
- For day-to-day Secure Global Desktop administration
  - Active Directory container object
  - Domain component object
  - Group object
  - Organization object
  - Organizational unit object
  - Client Drive Mapping (--cdm)
  - Connections (--conntype)
  - Description (--description)
  - Inherit parent's webtop content (--inherit)
  - Links tab (--links)
  - Members tab (--member)
  - Name (--name) domain component object
  - Name (--name) organization object
  - Name (--name) organizational unit object
  - Naming objects in the organizational hierarchy
  - The tarantella object command
  - Webtop Theme (--webtop)
  - Client printers (--mapprinters)
  - Driver name (--pdfdriver)
  - Let users print to a PDF local file (--pdfviewerenabled)



- Let users print to a PDF printer (--pdfenabled)
- Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
- Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
- User-specific printing configuration (--userprintingconfig)
- For in-depth Secure Global Desktop administration
  - Populating the Secure Global Desktop organizational hierarchy using a batch script
  - All Administrators have been removed and no-one can use the administration tools

## Security [Next section](#)

- For new Secure Global Desktop Administrators
  - Obtaining and installing an X.509 certificate
  - What are X.509 certificates and why do I need one?
  - Giving secure connections across the Internet
  - Giving secure connections to a Secure Global Desktop server
  - Giving secure connections to all users in a department
  - Securing client connections with Secure Global Desktop security services
  - Securing connections to Active Directory and LDAP directory servers
  - Securing the SOAP connections to a Secure Global Desktop server
  - Security and Secure Global Desktop
  - What are peer DNS names and external DNS names?
  - Improving security between Secure Global Desktop servers and application servers
  - Improving security between client devices and Secure Global Desktop servers
  - Users and trusted Secure Global Desktop servers
  - Sharing web server and Secure Global Desktop server certificates
- For day-to-day Secure Global Desktop administration
  - Securing connections between Secure Global Desktop servers
  - Security properties (array-wide)
  - Security properties (server-specific)
  - Solaris OS users are unable to log in when Secure Global Desktop security services are running
  - What are Secure Global Desktop security services?
  - Connections (--conntype)
  - Selecting a cipher suite for secure connections
  - The tarantella security command
  - Tuning the SSL Daemon process
- For in-depth Secure Global Desktop administration

- What certificates does Secure Global Desktop support?
- How can I support users with a client-side firewall that only allows connections on the HTTPS port?
- How do I tell what connection type a user gets?
- User prompts and X.509 certificates
- Using Secure Global Desktop with proxy servers
- Using Secure Global Desktop with the HTTPS port through a firewall
- Can I use an X.509 certificate for another product with Secure Global Desktop?
- How do I support additional Certificate Authorities?
- Users are unable to connect to Secure Global Desktop when it is in firewall forwarding mode
- Can I use PKI client certificates with web server authentication?
- Can I use SafeWord PremierAccess with web server authentication?
- Can I use other web authentication schemes with Secure Global Desktop web server authentication?
- Installing and using SSH with Secure Global Desktop
- Using Secure Global Desktop with firewalls
- What ports does Secure Global Desktop use?
- Can I chain Certificate Authority certificates?

## **Printing** Next section

- For new Secure Global Desktop Administrators
  - Introducing Secure Global Desktop printing
  - Configuring printing for UNIX, Linux and Mac OS X clients
  - Configuring printing if you use the Common UNIX Printing System (CUPS)
  - Configuring the Secure Global Desktop server to accept remote print requests
  - Printing from a Microsoft Windows 2000/2003 application server
  - Printing from a Microsoft Windows NT 3.51 application server
  - Printing from a Microsoft Windows NT 4 application server
  - Printing from a UNIX or Linux application server
  - Configuring Secure Global Desktop PDF printing
- For day-to-day Secure Global Desktop administration
  - Print Protocol Engine properties (server-specific)
  - Printing properties (array-wide)
  - Users cannot print from applications displayed through Secure Global Desktop
  - The prtinstall.en.sh script
  - Why do users see a printer called \_Default in their Windows application?

- The tarantella print command
- Troubleshooting printer preferences and settings
- When Secure Global Desktop printing has been disabled, print jobs can still be queued
- Windows 2000 users are unable to print a file from a mapped network drive
- Can I change the name of the printer in the Windows 2000/2003 application session?
- Client printers (--mapprinters)
- Driver name (--pdfdriver)
- Let users print to a PDF local file (--pdfviewerenabled)
- Let users print to a PDF printer (--pdfenabled)
- Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
- Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
- User-specific printing configuration (--userprintingconfig)
- With Secure Global Desktop PDF printing, fonts don't print as expected
- For in-depth Secure Global Desktop administration
  - If the array changes, do I have to re-configure printing?
  - Can I force users to print only to their default client printer?
  - Can I set a time limit for print jobs?
  - Do I have to use distributed printing?
- For Secure Global Desktop customizers
  - Configuring Secure Global Desktop print job conversion

## Commands Next section

- For new Secure Global Desktop Administrators
  - The tarantella command
  - The tarantella help command
  - The tarantella objectmanager command
  - The tarantella restart command
  - The tarantella start command
  - The tarantella status command
  - The tarantella stop command
  - The tarantella uninstall command
- For day-to-day Secure Global Desktop administration
  - The tarantella array command
  - The tarantella emulatorsession command
  - The tarantella license command
  - The tarantella object command

- The tarantella print command
- The tarantella query command
- The tarantella role command
- The tarantella security command
- The tarantella start cdm command
- The tarantella stop cdm command
- The tarantella version command
- The tarantella webserver command
- The tarantella webtopsession command
- The tarantella array detach command
- The tarantella array join command
- The tarantella array list command
- The tarantella array make\_primary command
- The tarantella emulatorsession end command
- The tarantella emulatorsession info command
- The tarantella emulatorsession list command
- The tarantella emulatorsession shadow command
- The tarantella emulatorsession suspend command
- The tarantella license add command
- The tarantella license info command
- The tarantella license list command
- The tarantella license query command
- The tarantella license remove command
- The tarantella license status command
- The tarantella object add\_host command
- The tarantella object add\_link command
- The tarantella object add\_member command
- The tarantella object delete command
- The tarantella object edit command
- The tarantella object list\_attributes command
- The tarantella object list\_contents command
- The tarantella object new\_3270app command
- The tarantella object new\_5250app command
- The tarantella object new\_charapp command
- The tarantella object new\_container command
- The tarantella object new\_dc command
- The tarantella object new\_doc command

- The tarantella object new\_group command
- The tarantella object new\_host command
- The tarantella object new\_org command
- The tarantella object new\_orgunit command
- The tarantella object new\_person command
- The tarantella object new\_windowsapp command
- The tarantella object new\_xapp command
- The tarantella object remove\_host command
- The tarantella object remove\_link command
- The tarantella object remove\_member command
- The tarantella object rename command
- The tarantella object script command
- The tarantella print cancel command
- The tarantella print list command
- The tarantella print move command
- The tarantella print pause command
- The tarantella print resume command
- The tarantella print start command
- The tarantella print status command
- The tarantella print stop command
- The tarantella query audit command
- The tarantella query billing command
- The tarantella query errlog command
- The tarantella query uptime command
- The tarantella role add\_link command
- The tarantella role add\_member command
- The tarantella role list command
- The tarantella role list\_links command
- The tarantella role list\_members command
- The tarantella role remove\_link command
- The tarantella role remove\_member command
- The tarantella security certinfo command
- The tarantella security certrequest command
- The tarantella security certuse command
- The tarantella security customca command
- The tarantella security decryptkey command

- The tarantella security fingerprint command
- The tarantella security peerca command
- The tarantella security start command
- The tarantella security stop command
- The tarantella tscal command
- The tarantella tscal free command
- The tarantella tscal list command
- The tarantella tscal return command
- The tarantella webserver add\_trusted\_user command
- The tarantella webserver delete\_trusted\_user command
- The tarantella webserver list\_trusted\_users command
- The tarantella webserver restart command
- The tarantella webserver start command
- The tarantella webserver stop command
- The tarantella webtopsession list command
- The tarantella webtopsession logout command
- For in-depth Secure Global Desktop administration
  - The tarantella archive command
  - The tarantella arraymanager command
  - The tarantella cache command
  - The tarantella config command
  - The tarantella passcache command
  - The tarantella setup command
  - The tarantella tokencache command
  - The tarantella config edit command
  - The tarantella config list command
  - The tarantella passcache delete command
  - The tarantella passcache edit command
  - The tarantella passcache list command
  - The tarantella passcache new command
  - The tarantella tokencache delete command
  - The tarantella tokencache list command
- For Secure Global Desktop customizers
  - The tarantella Tcl command

- For new Secure Global Desktop Administrators
  - How does Secure Global Desktop use applets?
- For Secure Global Desktop customizers
  - The ttawebtop.cgi CGI program
  - Client drive mapping (CDM) applet
  - Client drive mapping (CDM) applet parameters
  - Framework applet
  - Framework applet parameters
  - Launching applications from JavaScript
  - Login applet
  - Login applet parameters
  - Print applet
  - Print applet parameters
  - Terminal emulator applet
  - Terminal emulator applet parameters
  - The TTAAPPLET tag
  - Webtop script applet
  - Webtop script applet parameters
  - Webtop tray applet
  - Webtop tray applet parameters
  - X emulator applet
  - X emulator applet parameters
  - Applet parameter data types
  - Logging in with the Secure Global Desktop applets
  - addValue (framework applet)
  - areObjectsInitialized (webtop script and webtop tray applets)
  - cancelCurrentJob (print applet)
  - closeHierarchyLevel (webtop script and webtop tray applets)
  - countJobs (print applet)
  - getActive (print applet)
  - getApplicationType (webtop script and webtop tray applets)
  - getCurrentIteratorElement (webtop script and webtop tray applets)
  - getEmulatorState (X emulator applet)
  - getEmulatorState (terminal emulator applet)
  - getEnabled (print applet)
  - getIteratorForAllOpenHierarchyLevels (webtop script and webtop tray applets)
  - getIteratorForHierarchyLevel (webtop script and webtop tray applets)

- `getIteratorHasMoreElements` (webtop script and webtop tray applets)
- `getLaunchWaitTimeOut` (webtop script and webtop script applets)
- `getNextIteratorElement` (webtop script and webtop tray applets)
- `getNumberOfObjects` (webtop script and webtop tray applets)
- `getNumberOfObjectsInGroup` (webtop script and webtop tray applets)
- `getObjectClass` (webtop script and webtop tray applets)
- `getObjectDisplayName` (webtop script and webtop tray applets)
- `getObjectDisplayNameByName` (webtop script and webtop tray applets)
- `getObjectFullName` (webtop script and webtop tray applets)
- `getObjectImageName` (webtop script and webtop tray applets)
- `getObjectImageNameByName` (webtop script and webtop tray applets)
- `getObjectPlacement` (webtop script and webtop tray applets)
- `getParentGroupName` (webtop script and webtop tray applets)
- `getPrintState` (print applet)
- `getPrinterName` (print applet)
- `getPrinterPort` (print applet)
- `getPrinterType` (print applet)
- `getProperty` (X emulator applet)
- `getText` (terminal emulator applet)
- `getTotalNumberOfObjects` (webtop script and webtop tray applets)
- `getUnixTempDir` (print applet)
- `getUserName` (framework applet)
- `getValue` (framework applet)
- `getWebtopFramesetURL` (framework applet)
- `getWebtopURL` (framework applet)
- `getWindowsTempDir` (print applet)
- `isApplication` (webtop script and webtop tray applets)
- `isDocument` (webtop script and webtop tray applets)
- `isGroup` (webtop script and webtop tray applets)
- `isHierarchyEnabled` (webtop script and webtop tray applets)
- `isLoggedIn` (framework applet)
- `isOpenGroup` (webtop script and webtop tray applets)
- `isRunning` (webtop script and webtop tray applets)
- `killIterator` (webtop script and webtop tray applets)
- `launchByObjectName` (webtop script and webtop tray applets)
- `launchByObjectNumber` (webtop script and webtop tray applets)



- login method
- logout method
- openGroup (webtop tray applet)
- openHierarchyLevel (webtop script and webtop tray applets)
- openParentGroup (webtop tray applet)
- receivedEvent (webtop script and webtop tray applets)
- registerProperty (X emulator applet)
- removeValue (framework applet)
- resetNamePassword (login applet)
- scriptStart method
- sendKey (terminal emulator applet)
- setActive (print applet)
- setEnabled (print applet)
- setLaunchWaitTimeOut (webtop script and webtop tray applets)
- setPausedState (print applet)
- setPrinterName (print applet)
- setPrinterPort (print applet)
- setPrinterType (print applet)
- setProperty (X emulator applet)
- setText (terminal emulator applet)
- setUnixTempDir (print applet)
- setWindowsTempDir (print applet)
- suspendApplication (X emulator applet)
- suspendApplication (terminal emulator applet)
- unregisterProperty (X emulator applet)

# Sun Secure Global Desktop Software Administration Guide

## For new Secure Global Desktop Administrators [Next section](#)

- Getting started
  - [How do I add new Secure Global Desktop Administrators?](#)
  - [Introducing Sun Secure Global Desktop Software](#)
  - [The tarantella command](#)
  - [Understanding webtop and emulator sessions](#)
  - [What do I need to tell my users?](#)
  - [Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop](#)
  - [Do I need to license Windows Terminal Services?](#)
  - [Integrating Secure Global Desktop with the desktop Start Menu](#)
  - [Introducing Array Manager](#)
  - [Introducing Object Manager](#)
  - [Securing client connections with Secure Global Desktop security services](#)
  - [Creating and configuring a person object](#)
  - [Creating and publishing an application object to users](#)
  - [Introducing the three-tier architecture](#)
  - [Objects and the organizational hierarchy](#)
  - [Users and trusted Secure Global Desktop servers](#)
  - [Sun Secure Global Desktop Software legal and copyright information](#)
- Clients and webtops
  - [Introducing Sun Secure Global Desktop Software](#)
  - [Working with the Sun Secure Global Desktop Client](#)
  - [Configuring the Sun Secure Global Desktop Client for desktop Start Menu integration](#)
  - [Integrating Secure Global Desktop with the desktop Start Menu](#)
  - [Profiles and the Sun Secure Global Desktop Client](#)
  - [Securing client connections with Secure Global Desktop security services](#)
- Arrays, servers and load balancing
  - [Introducing Array Manager](#)
  - [Introducing the Secure Global Desktop Web Server](#)
  - [Introducing webtop and emulator session load balancing](#)

- Introducing application server load balancing
- The Secure Global Desktop datastore and Tarantella Federated Naming
- Troubleshooting CPU/memory-based application server load balancing
- What is an array?
- Configuring your own web server for use with Secure Global Desktop
- The tarantella restart command
- The tarantella start command
- The tarantella status command
- The tarantella stop command
- What's in the Secure Global Desktop installation directory?
- Where is Secure Global Desktop installed?
- **Users and authentication**
  - A session doesn't end when the user exits the application
  - Secure Global Desktop and user authentication
  - Understanding webtop and emulator sessions
  - What do I need to tell my users?
  - Working with users in different locales
  - Creating and configuring a person object
- **Applications, documents and hosts**
  - A session doesn't end when the user exits the application
  - An application exits immediately after starting
  - An application won't start
  - Understanding webtop and emulator sessions
  - Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop
  - Configuring client drive mapping
  - Do I need to license Windows Terminal Services?
  - Creating and publishing an application object to users
  - Using copy and paste with Secure Global Desktop
- **Organizing your resources**
  - Introducing Object Manager
  - Objects and the organizational hierarchy
  - What is ENS?
  - What is the Tarantella System Objects organization?
- **Security**
  - Obtaining and installing an X.509 certificate
  - What are X.509 certificates and why do I need one?
  - Giving secure connections across the Internet

- Giving secure connections to a Secure Global Desktop server
- Giving secure connections to all users in a department
- Securing client connections with Secure Global Desktop security services
- Securing connections to Active Directory and LDAP directory servers
- Securing the SOAP connections to a Secure Global Desktop server
- Security and Secure Global Desktop
- What are peer DNS names and external DNS names?
- Improving security between Secure Global Desktop servers and application servers
- Improving security between client devices and Secure Global Desktop servers
- Users and trusted Secure Global Desktop servers
- Sharing web server and Secure Global Desktop server certificates
- **Printing**
  - Introducing Secure Global Desktop printing
  - Configuring printing for UNIX, Linux and Mac OS X clients
  - Configuring printing if you use the Common UNIX Printing System (CUPS)
  - Configuring the Secure Global Desktop server to accept remote print requests
  - Printing from a Microsoft Windows 2000/2003 application server
  - Printing from a Microsoft Windows NT 3.51 application server
  - Printing from a Microsoft Windows NT 4 application server
  - Printing from a UNIX or Linux application server
  - Configuring Secure Global Desktop PDF printing
- **Commands**
  - The tarantella command
  - The tarantella help command
  - The tarantella objectmanager command
  - The tarantella restart command
  - The tarantella start command
  - The tarantella status command
  - The tarantella stop command
  - The tarantella uninstall command
- **Applets**
  - How does Secure Global Desktop use applets?

## **For day-to-day Secure Global Desktop administration** [Next section](#)

- **Getting started**
  - Licensing and Sun Secure Global Desktop Software

- Setting up and dismantling a Secure Global Desktop array
- Using shadowing to troubleshoot a user's problem
- **Clients and webtops**
  - Can users access Secure Global Desktop without Java technology?
  - Does the browser-based webtop use themes?
  - Profile Editing (--editprofile)
- **Arrays, servers and load balancing**
  - Application Launch properties (array-wide)
  - Array properties (array-wide)
  - Channel Protocol Engine properties (server-specific)
  - Character Protocol Engine properties (server-specific)
  - Emulator Sessions properties (array-wide)
  - Execution Protocol Engine properties (server-specific)
  - General properties (server-specific)
  - Licenses properties (array-wide)
  - Load Balancing properties (array-wide)
  - Print Protocol Engine properties (server-specific)
  - Printing properties (array-wide)
  - Secure Global Desktop Login properties (array-wide)
  - Security properties (array-wide)
  - Security properties (server-specific)
  - Setting up and dismantling a Secure Global Desktop array
  - Smart Card Protocol Engine properties
  - Tuning properties (server-specific)
  - X Protocol Engine properties (server-specific)
  - Audio Protocol Engine properties (server-specific)
  - Configuring application server load balancing
  - Using log filters for auditing
  - Using log filters to troubleshoot problems with the Secure Global Desktop server
  - Hosts tab (--appserv)
  - Location (--location)
  - The tarantella array command
  - The tarantella query command
  - Users are unable to relocate their webtop sessions
- **Users and authentication**
  - Person object
  - Execution Protocol Engine properties (server-specific)

- Login authorities
- Roles in Secure Global Desktop
- Secure Global Desktop Login properties (array-wide)
- The Active Directory login authority
- The Anonymous user login authority
- The ENS login authority
- The LDAP login authority
- The NT login authority
- The SecurID login authority
- The UNIX group login authority
- The UNIX user login authority
- The authentication token login authority
- Users are unable to copy and paste text or graphics
- Using Windows Terminal Services, users are prompted for usernames and passwords too often
- Using shared accounts for "guest" users
- Web server/third party authentication
- An "Ambiguous username" dialog is displayed when a user tries to log in
- Enabling the Active Directory login authority
- Enabling the LDAP login authority
- Enabling the NT login authority
- Enabling the SecurID login authority
- LDAP users can't log in to Secure Global Desktop
- Mirroring your LDAP organization in ENS
- Using Directory Services Integration
- Using the authentication token login authority for automatic logins
- What is a role object?
- Bandwidth Limit (--bandwidth)
- Client Drive Mapping (--cdm)
- Connections (--conntype)
- Description (--description)
- Email Address (--email)
- Inherit parent's webtop content (--inherit)
- Keyboard Map (--keymap)
- Links tab (--links)
- Login Script (--login)
- May log in to Secure Global Desktop (--enabled)

- Name (--name) objects with "common name"
- Preferred Locale (--preflocale)
- Shared between users (guest) (--shared)
- Surname (--surname)
- The tarantella emulatorsession command
- The tarantella object command
- The tarantella role command
- The tarantella webtopsession command
- Username (--user)
- Using SecurID for application server authentication
- Webtop Theme (--webtop)
- Windows NT Domain (--ntdomain)
- Client printers (--mapprinters)
- Driver name (--pdfdriver)
- Let users print to a PDF local file (--pdfviewerenabled)
- Let users print to a PDF printer (--pdfenabled)
- Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
- Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
- User-specific printing configuration (--userprintingconfig)
- Applications, documents and hosts
  - 3270 application object
  - 5250 application object
  - Character application object
  - Document object
  - Host object
  - Windows application object
  - X application object
  - An application's animation appears "jumpy"
  - Application Launch properties (array-wide)
  - Applications disappear after about two minutes
  - Character Protocol Engine properties (server-specific)
  - Emulator Sessions properties (array-wide)
  - Load Balancing properties (array-wide)
  - X Protocol Engine properties (server-specific)
  - Available to run applications (--available)
  - Configuring access to serial ports

- How do I enable sound in Windows applications?
- Load Balancing Algorithm (--loadbal)
- Mirroring your LDAP organization in ENS
- Users are having problems accessing client drives
- Users complain of poor performance with the Windows desktop
- Using Directory Services Integration
- Using seamless windows for Windows applications
- Using smart cards with Windows applications
- 3270 Host (--hostname)
- A Kiosk application isn't appearing full-screen
- AS/400 Host (--hostname)
- Address (--address)
- Allow delayed updates (--delayed)
- An application requires a richer set of cursors
- Answerback Message (--answermsg)
- Application Command (--app)
- Application key mode (--appkeymode)
- Application supports 3-button mouse only (--force3button)
- Arguments For Command (--args)
- Attribute Map (--attributemap)
- Authentication (--auth)
- Background Color (--3270bg) 3270
- Background Color (--bg) 5250
- Border Style (--border)
- Can I use Secure Global Desktop to access VMS applications?
- Client's maximum size (--maximize)
- Clipboard Access (--clipboard)
- Clipboard Security Level (--clipboardlevel)
- Close Telnet Action (--3270tnclose) 3270
- Close Telnet Action (--tnclose) 5250
- Code Page (--codepage)
- Color (--rootcolor)
- Color Map (--colormap)
- Color depth (--depth)
- Color quality (--quality)
- Columns (--cols)
- Command Compression (--compression)



- Command Execution (--execution)
- Connection Method (--method)
- Cursor (--cursor)
- Cursor Keys (--cursorkeys)
- Description (--description)
- Display Using (--displayusing)
- Emulation Type (--emulator)
- Emulator Applet Page (--empage)
- Enable File and Settings menus (--3270si) 3270
- Enable File and Settings menus (--si) 5250
- Enable X Security Extension (--securityextension)
- Enable menu bar (--3270mb) 3270
- Enable menu bar (--mb) 5250
- Environment Variables (--env)
- Escape Sequences (--escape)
- Euro Character (--euro)
- Fixed font size (--fixedfont)
- Font Family (--font)
- Font Size (--fontsize)
- Foreground Color (--3270fg) 3270
- Foreground Color (--fg) 5250
- Height (--height)
- Host Locale (--hostlocale)
- Hosts tab (--appserv)
- How do I run a Common Desktop Environment (CDE) session?
- In some X applications, the ALT and ALT GR keys do not work
- Interlaced Images (--interlaced)
- Keep launch connection open (--keepopen)
- Keyboard Map (--keymap)
- Keyboard Type (--3270kt) 3270
- Keyboard Type (--kt) 5250
- Keypad (--keypad)
- LDAP Groups (--ldapgroups)
- LDAP Search (--ldapsearch)
- LDAP Users (--ldapusers)
- Lines (--lines)

- Location (--location)
- Lock keymap (--lockkeymap)
- Login Script (--login)
- Max Instances (--maxinstances)
- Maximize the emulator window (--3270ma) 3270
- Maximize the emulator window (--ma) 5250
- Middle Mouse Timeout (--middlemouse)
- Monitor Resolution (--dpi)
- Name (--name) objects with "common name"
- Open in new browser window (--newbrowser)
- Port Number (--portnumber) 3270
- Port Number (--portnumber) 5250
- Protocol Arguments (--protoargs)
- Resumable (--resumable)
- Resumable For (--resumetimeout)
- Root Window (--roottype)
- Scale to fit window (--scalable)
- Scroll Style (--scrollstyle)
- Serial Port Mapping (--serialport)
- Session Ends When (--endswhen)
- Share resources between similar sessions (--share)
- Soft Button Levels (--3270bl) 3270
- Soft Button Levels (--bl) 5250
- Status Line (--statusline)
- Terminal Type (--termttype)
- The tarantella emulatorsession command
- The tarantella object command
- Troubleshooting sound in Windows applications
- Try running from client first (--trylocal)
- URL (--url)
- Use Windows cursor (--wincursor)
- Use graphics acceleration (--accel)
- Users are unable to use smart cards with Windows applications
- Users have problems displaying high color X applications
- Using Remote Desktop on Microsoft Windows XP Professional
- Using shadowing to troubleshoot a user's problem
- Webtop Hints (--hints)

- Webtop Icon (--icon)
- Width (--width)
- Window Close Action (--windowclose)
- Window Manager (--winmgr)
- Windows NT Domain (--ntdomain)
- Windows Protocol (--winproto)
- Wrap long lines (--autowrap)
- Can I access a web application through Secure Global Desktop?
- Customizing the Native Client for UNIX
- Running Windows applications on client devices
- Users see window clipping with Client Window Management applications
- **Organizing your resources**
  - Active Directory container object
  - Domain component object
  - Group object
  - Organization object
  - Organizational unit object
  - Client Drive Mapping (--cdm)
  - Connections (--conntype)
  - Description (--description)
  - Inherit parent's webtop content (--inherit)
  - Links tab (--links)
  - Members tab (--member)
  - Name (--name) domain component object
  - Name (--name) organization object
  - Name (--name) organizational unit object
  - Naming objects in the organizational hierarchy
  - The tarantella object command
  - Webtop Theme (--webtop)
  - Client printers (--mapprinters)
  - Driver name (--pdfdriver)
  - Let users print to a PDF local file (--pdfviewerenabled)
  - Let users print to a PDF printer (--pdfenabled)
  - Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
  - Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
  - User-specific printing configuration (--userprintingconfig)
- **Security**

- Securing connections between Secure Global Desktop servers
- Security properties (array-wide)
- Security properties (server-specific)
- Solaris OS users are unable to log in when Secure Global Desktop security services are running
- What are Secure Global Desktop security services?
- Connections (--conntype)
- Selecting a cipher suite for secure connections
- The tarantella security command
- Tuning the SSL Daemon process
- **Printing**
  - Print Protocol Engine properties (server-specific)
  - Printing properties (array-wide)
  - Users cannot print from applications displayed through Secure Global Desktop
  - The prtinstall.en.sh script
  - Why do users see a printer called \_Default in their Windows application?
  - The tarantella print command
  - Troubleshooting printer preferences and settings
  - When Secure Global Desktop printing has been disabled, print jobs can still be queued
  - Windows 2000 users are unable to print a file from a mapped network drive
  - Can I change the name of the printer in the Windows 2000/2003 application session?
  - Client printers (--mapprinters)
  - Driver name (--pdfdriver)
  - Let users print to a PDF local file (--pdfviewerenabled)
  - Let users print to a PDF printer (--pdfenabled)
  - Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
  - Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
  - User-specific printing configuration (--userprintingconfig)
  - With Secure Global Desktop PDF printing, fonts don't print as expected
- **Commands**
  - The tarantella array command
  - The tarantella emulatorsession command
  - The tarantella license command
  - The tarantella object command
  - The tarantella print command
  - The tarantella query command

- The tarantella role command
- The tarantella security command
- The tarantella start cdm command
- The tarantella stop cdm command
- The tarantella version command
- The tarantella webserver command
- The tarantella webtopsession command
- The tarantella array detach command
- The tarantella array join command
- The tarantella array list command
- The tarantella array make\_primary command
- The tarantella emulatorsession end command
- The tarantella emulatorsession info command
- The tarantella emulatorsession list command
- The tarantella emulatorsession shadow command
- The tarantella emulatorsession suspend command
- The tarantella license add command
- The tarantella license info command
- The tarantella license list command
- The tarantella license query command
- The tarantella license remove command
- The tarantella license status command
- The tarantella object add\_host command
- The tarantella object add\_link command
- The tarantella object add\_member command
- The tarantella object delete command
- The tarantella object edit command
- The tarantella object list\_attributes command
- The tarantella object list\_contents command
- The tarantella object new\_3270app command
- The tarantella object new\_5250app command
- The tarantella object new\_charapp command
- The tarantella object new\_container command
- The tarantella object new\_dc command
- The tarantella object new\_doc command
- The tarantella object new\_group command
- The tarantella object new\_host command

- The tarantella object new\_org command
- The tarantella object new\_orgunit command
- The tarantella object new\_person command
- The tarantella object new\_windowsapp command
- The tarantella object new\_xapp command
- The tarantella object remove\_host command
- The tarantella object remove\_link command
- The tarantella object remove\_member command
- The tarantella object rename command
- The tarantella object script command
- The tarantella print cancel command
- The tarantella print list command
- The tarantella print move command
- The tarantella print pause command
- The tarantella print resume command
- The tarantella print start command
- The tarantella print status command
- The tarantella print stop command
- The tarantella query audit command
- The tarantella query billing command
- The tarantella query errlog command
- The tarantella query uptime command
- The tarantella role add\_link command
- The tarantella role add\_member command
- The tarantella role list command
- The tarantella role list\_links command
- The tarantella role list\_members command
- The tarantella role remove\_link command
- The tarantella role remove\_member command
- The tarantella security certinfo command
- The tarantella security certrequest command
- The tarantella security certuse command
- The tarantella security customca command
- The tarantella security decryptkey command
- The tarantella security fingerprint command
- The tarantella security peerca command

- The tarantella security start command
- The tarantella security stop command
- The tarantella tscal command
- The tarantella tscal free command
- The tarantella tscal list command
- The tarantella tscal return command
- The tarantella webserver add\_trusted\_user command
- The tarantella webserver delete\_trusted\_user command
- The tarantella webserver list\_trusted\_users command
- The tarantella webserver restart command
- The tarantella webserver start command
- The tarantella webserver stop command
- The tarantella webtopsession list command
- The tarantella webtopsession logout command

## **For in-depth Secure Global Desktop administration** [Next section](#)

- Clients and webtops
  - Native Client preferences files on UNIX, Linux and Mac OS X client devices
  - Running the Native Client from the command line
  - How can I make additional Native Clients available?
  - Secure Global Desktop and Java archives
- Arrays, servers and load balancing
  - Backing up and restoring a Secure Global Desktop installation
  - Editing application server load balancing properties
  - Tuning application server load balancing
  - All login authorities are disabled and no-one can access Secure Global Desktop
  - Every server in the array has been disabled and no-one can access Secure Global Desktop
  - The tarantella archive command
  - The tarantella arraymanager command
  - The tarantella config command
  - Managing unauthenticated connections to Secure Global Desktop
- Users and authentication
  - How do I tell what connection type a user gets?
  - Introducing web server authentication
  - Users experience problems with web server authentication
  - Denying users access to Secure Global Desktop after failed login attempts

- Enabling web server authentication for the browser-based webtop
- Enabling web server authentication for the classic webtop
- Populating the Secure Global Desktop organizational hierarchy using a batch script
- Security considerations of using web server authentication
- Users see font problems
- What happens when a user's password expires?
- All login authorities are disabled and no-one can access Secure Global Desktop
- Can I deny an LDAP user access to Secure Global Desktop?
- Can I use PKI client certificates with web server authentication?
- Can I use SafeWord PremierAccess with web server authentication?
- Can I use other web authentication schemes with Secure Global Desktop web server authentication?
- The tarantella cache command
- The tarantella passcache command
- The tarantella tokencache command
- Secure Global Desktop uses too much of my network's bandwidth
- The tarantella tokencache delete command
- The tarantella tokencache list command
- Trusted users and third party authentication
- **Applications, documents and hosts**
  - Can I run another SMB service with client drive mapping?
  - Populating the Secure Global Desktop organizational hierarchy using a batch script
  - Remapping or hiding Windows 2000/2003 application server drives
  - When X authorization is enabled, applications fail to start
  - Can I prevent users from launching applications with a different username and password?
  - How do I use my own X fonts?
  - Using shadowing in the classroom
  - What X fonts are installed?
  - Can I use multiple monitors with Secure Global Desktop?
  - Secure Global Desktop uses too much of my network's bandwidth
- **Organizing your resources**
  - Populating the Secure Global Desktop organizational hierarchy using a batch script
  - All Administrators have been removed and no-one can use the administration tools
- **Security**
  - What certificates does Secure Global Desktop support?
  - How can I support users with a client-side firewall that only allows connections on the HTTPS port?



- How do I tell what connection type a user gets?
- User prompts and X.509 certificates
- Using Secure Global Desktop with proxy servers
- Using Secure Global Desktop with the HTTPS port through a firewall
- Can I use an X.509 certificate for another product with Secure Global Desktop?
- How do I support additional Certificate Authorities?
- Users are unable to connect to Secure Global Desktop when it is in firewall forwarding mode
- Can I use PKI client certificates with web server authentication?
- Can I use SafeWord PremierAccess with web server authentication?
- Can I use other web authentication schemes with Secure Global Desktop web server authentication?
- Installing and using SSH with Secure Global Desktop
- Using Secure Global Desktop with firewalls
- What ports does Secure Global Desktop use?
- Can I chain Certificate Authority certificates?
- **Printing**
  - If the array changes, do I have to re-configure printing?
  - Can I force users to print only to their default client printer?
  - Can I set a time limit for print jobs?
  - Do I have to use distributed printing?
- **Commands**
  - The tarantella archive command
  - The tarantella arraymanager command
  - The tarantella cache command
  - The tarantella config command
  - The tarantella passcache command
  - The tarantella setup command
  - The tarantella tokencache command
  - The tarantella config edit command
  - The tarantella config list command
  - The tarantella passcache delete command
  - The tarantella passcache edit command
  - The tarantella passcache list command
  - The tarantella passcache new command
  - The tarantella tokencache delete command
  - The tarantella tokencache list command

## For Secure Global Desktop customizers [Back to top](#)

- Clients and webtops
  - [Relocating the browser-based webtop to your own JSP container](#)
- Users and authentication
  - [A login script returns an error](#)
  - [Increasing launch timeouts](#)
  - [Login script Tcl commands](#)
  - [Login script variables](#)
  - [Login scripts supplied with Secure Global Desktop](#)
  - [The tarantella Tcl command](#)
  - [What are login scripts?](#)
- Applications, documents and hosts
  - [Launching a single application without displaying a webtop](#)
  - [Launching applications from JavaScript](#)
  - [Terminal emulator attribute maps](#)
  - [Terminal emulator color maps](#)
  - [Terminal emulator keyboard maps](#)
- Printing
  - [Configuring Secure Global Desktop print job conversion](#)
- Commands
  - [The tarantella Tcl command](#)
- Applets
  - [The ttawebtop.cgi CGI program](#)
  - [Client drive mapping \(CDM\) applet](#)
  - [Client drive mapping \(CDM\) applet parameters](#)
  - [Framework applet](#)
  - [Framework applet parameters](#)
  - [Launching applications from JavaScript](#)
  - [Login applet](#)
  - [Login applet parameters](#)
  - [Print applet](#)
  - [Print applet parameters](#)
  - [Terminal emulator applet](#)
  - [Terminal emulator applet parameters](#)
  - [The TTAAPPLET tag](#)
  - [Webtop script applet](#)

- Webtop script applet parameters
- Webtop tray applet
- Webtop tray applet parameters
- X emulator applet
- X emulator applet parameters
- Applet parameter data types
- Logging in with the Secure Global Desktop applets
- addValue (framework applet)
- areObjectsInitialized (webtop script and webtop tray applets)
- cancelCurrentJob (print applet)
- closeHierarchyLevel (webtop script and webtop tray applets)
- countJobs (print applet)
- getActive (print applet)
- getApplicationType (webtop script and webtop tray applets)
- getCurrentIteratorElement (webtop script and webtop tray applets)
- getEmulatorState (X emulator applet)
- getEmulatorState (terminal emulator applet)
- getEnabled (print applet)
- getIteratorForAllOpenHierarchyLevels (webtop script and webtop tray applets)
- getIteratorForHierarchyLevel (webtop script and webtop tray applets)
- getIteratorHasMoreElements (webtop script and webtop tray applets)
- getLaunchWaitTimeOut (webtop script and webtop script applets)
- getNextIteratorElement (webtop script and webtop tray applets)
- getNumberOfObjects (webtop script and webtop tray applets)
- getNumberOfObjectsInGroup (webtop script and webtop tray applets)
- getObjectClass (webtop script and webtop tray applets)
- getObjectDisplayName (webtop script and webtop tray applets)
- getObjectDisplayNameByName (webtop script and webtop tray applets)
- getObjectFullName (webtop script and webtop tray applets)
- getObjectImageName (webtop script and webtop tray applets)
- getObjectImageNameByName (webtop script and webtop tray applets)
- getObjectPlacement (webtop script and webtop tray applets)
- getParentGroupName (webtop script and webtop tray applets)
- getPrintState (print applet)
- getPrinterName (print applet)
- getPrinterPort (print applet)
- getPrinterType (print applet)

- getProperty (X emulator applet)
- getText (terminal emulator applet)
- getTotalNumberOfObjects (webtop script and webtop tray applets)
- getUnixTempDir (print applet)
- getUsername (framework applet)
- getValue (framework applet)
- getWebtopFramesetURL (framework applet)
- getWebtopURL (framework applet)
- getWindowsTempDir (print applet)
- isApplication (webtop script and webtop tray applets)
- isDocument (webtop script and webtop tray applets)
- isGroup (webtop script and webtop tray applets)
- isHierarchyEnabled (webtop script and webtop tray applets)
- isLoggedIn (framework applet)
- isOpenGroup (webtop script and webtop tray applets)
- isRunning (webtop script and webtop tray applets)
- killIterator (webtop script and webtop tray applets)
- launchByObjectName (webtop script and webtop tray applets)
- launchByObjectNumber (webtop script and webtop tray applets)
- login method
- logout method
- openGroup (webtop tray applet)
- openHierarchyLevel (webtop script and webtop tray applets)
- openParentGroup (webtop tray applet)
- receivedEvent (webtop script and webtop tray applets)
- registerProperty (X emulator applet)
- removeValue (framework applet)
- resetNamePassword (login applet)
- scriptStart method
- sendKey (terminal emulator applet)
- setActive (print applet)
- setEnabled (print applet)
- setLaunchWaitTimeOut (webtop script and webtop tray applets)
- setPausedState (print applet)
- setPrinterName (print applet)
- setPrinterPort (print applet)

- `setPrinterType` (print applet)
- `setProperty` (X emulator applet)
- `setText` (terminal emulator applet)
- `setUnixTempDir` (print applet)
- `setWindowsTempDir` (print applet)
- `suspendApplication` (X emulator applet)
- `suspendApplication` (terminal emulator applet)
- `unregisterProperty` (X emulator applet)

# Sun Secure Global Desktop Software Administration Guide

## For new Secure Global Desktop Administrators [Next section](#)

- Tutorials
  - [Introducing Sun Secure Global Desktop Software](#)
  - [Secure Global Desktop and user authentication](#)
  - [Understanding webtop and emulator sessions](#)
  - [Integrating Secure Global Desktop with the desktop Start Menu](#)
  - [Introducing Array Manager](#)
  - [Introducing Object Manager](#)
  - [Introducing Secure Global Desktop printing](#)
  - [Introducing the Secure Global Desktop Web Server](#)
  - [Introducing webtop and emulator session load balancing](#)
  - [Securing client connections with Secure Global Desktop security services](#)
  - [Security and Secure Global Desktop](#)
  - [Improving security between Secure Global Desktop servers and application servers](#)
  - [Improving security between client devices and Secure Global Desktop servers](#)
  - [Introducing application server load balancing](#)
  - [Introducing the three-tier architecture](#)
  - [Objects and the organizational hierarchy](#)
  - [The Secure Global Desktop datastore and Tarantella Federated Naming](#)
  - [Users and trusted Secure Global Desktop servers](#)
  - [Using copy and paste with Secure Global Desktop](#)
  - [Sharing web server and Secure Global Desktop server certificates](#)
- Case studies
  - [Obtaining and installing an X.509 certificate](#)
  - [Giving secure connections across the Internet](#)
  - [Giving secure connections to a Secure Global Desktop server](#)
  - [Giving secure connections to all users in a department](#)
  - [Creating and configuring a person object](#)
  - [Creating and publishing an application object to users](#)
- Reference

- The tarantella command
- Working with the Sun Secure Global Desktop Client
- Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop
- Configuring client drive mapping
- Configuring the Sun Secure Global Desktop Client for desktop Start Menu integration
- Profiles and the Sun Secure Global Desktop Client
- Securing connections to Active Directory and LDAP directory servers
- Securing the SOAP connections to a Secure Global Desktop server
- Working with users in different locales
- Configuring printing for UNIX, Linux and Mac OS X clients
- Configuring printing if you use the Common UNIX Printing System (CUPS)
- Configuring the Secure Global Desktop server to accept remote print requests
- Printing from a Microsoft Windows 2000/2003 application server
- Printing from a Microsoft Windows NT 3.51 application server
- Printing from a Microsoft Windows NT 4 application server
- Printing from a UNIX or Linux application server
- Configuring Secure Global Desktop PDF printing
- Configuring your own web server for use with Secure Global Desktop
- The tarantella help command
- The tarantella objectmanager command
- The tarantella restart command
- The tarantella start command
- The tarantella status command
- The tarantella stop command
- The tarantella uninstall command
- Sun Secure Global Desktop Software legal and copyright information
- **Troubleshooting**
  - A session doesn't end when the user exits the application
  - An application exits immediately after starting
  - An application won't start
  - Troubleshooting CPU/memory-based application server load balancing
- **Frequently asked questions**
  - How do I add new Secure Global Desktop Administrators?
  - How does Secure Global Desktop use applets?
  - What are X.509 certificates and why do I need one?
  - What do I need to tell my users?
  - Do I need to license Windows Terminal Services?

- What are peer DNS names and external DNS names?
- What is ENS?
- What is an array?
- What is the Tarantella System Objects organization?
- What's in the Secure Global Desktop installation directory?
- Where is Secure Global Desktop installed?

## **For day-to-day Secure Global Desktop administration** [Next section](#)

- Tutorials
  - Login authorities
- Case studies
  - Using shadowing to troubleshoot a user's problem
- Reference
  - 3270 application object
  - 5250 application object
  - Active Directory container object
  - Character application object
  - Document object
  - Domain component object
  - Group object
  - Host object
  - Organization object
  - Organizational unit object
  - Person object
  - Windows application object
  - X application object
  - Application Launch properties (array-wide)
  - Array properties (array-wide)
  - Channel Protocol Engine properties (server-specific)
  - Character Protocol Engine properties (server-specific)
  - Emulator Sessions properties (array-wide)
  - Execution Protocol Engine properties (server-specific)
  - General properties (server-specific)
  - Licenses properties (array-wide)
  - Licensing and Sun Secure Global Desktop Software
  - Load Balancing properties (array-wide)



- Print Protocol Engine properties (server-specific)
- Printing properties (array-wide)
- Roles in Secure Global Desktop
- Secure Global Desktop Login properties (array-wide)
- Securing connections between Secure Global Desktop servers
- Security properties (array-wide)
- Security properties (server-specific)
- Setting up and dismantling a Secure Global Desktop array
- Smart Card Protocol Engine properties
- The Active Directory login authority
- The Anonymous user login authority
- The ENS login authority
- The LDAP login authority
- The NT login authority
- The SecurID login authority
- The UNIX group login authority
- The UNIX user login authority
- The authentication token login authority
- Tuning properties (server-specific)
- Using shared accounts for "guest" users
- Web server/third party authentication
- X Protocol Engine properties (server-specific)
- Audio Protocol Engine properties (server-specific)
- Available to run applications (--available)
- Configuring access to serial ports
- Configuring application server load balancing
- Enabling the Active Directory login authority
- Enabling the LDAP login authority
- Enabling the NT login authority
- Enabling the SecurID login authority
- Load Balancing Algorithm (--loadbal)
- Mirroring your LDAP organization in ENS
- The prtinstall.en.sh script
- Using Directory Services Integration
- Using log filters for auditing
- Using log filters to troubleshoot problems with the Secure Global Desktop server
- Using seamless windows for Windows applications

- Using smart cards with Windows applications
- Using the authentication token login authority for automatic logins
- 3270 Host (--hostname)
- AS/400 Host (--hostname)
- Address (--address)
- Allow delayed updates (--delayed)
- Answerback Message (--answermsg)
- Application Command (--app)
- Application key mode (--appkeymode)
- Application supports 3-button mouse only (--force3button)
- Arguments For Command (--args)
- Attribute Map (--attributemap)
- Authentication (--auth)
- Background Color (--3270bg) 3270
- Background Color (--bg) 5250
- Bandwidth Limit (--bandwidth)
- Border Style (--border)
- Client Drive Mapping (--cdm)
- Client's maximum size (--maximize)
- Clipboard Access (--clipboard)
- Clipboard Security Level (--clipboardlevel)
- Close Telnet Action (--3270tnclose) 3270
- Close Telnet Action (--tnclose) 5250
- Code Page (--codepage)
- Color (--rootcolor)
- Color Map (--colormap)
- Color depth (--depth)
- Color quality (--quality)
- Columns (--cols)
- Command Compression (--compression)
- Command Execution (--execution)
- Connection Method (--method)
- Connections (--conntype)
- Cursor (--cursor)
- Cursor Keys (--cursorkeys)
- Description (--description)

- Display Using (--displayusing)
- Email Address (--email)
- Emulation Type (--emulator)
- Emulator Applet Page (--empage)
- Enable File and Settings menus (--3270si) 3270
- Enable File and Settings menus (--si) 5250
- Enable X Security Extension (--securityextension)
- Enable menu bar (--3270mb) 3270
- Enable menu bar (--mb) 5250
- Environment Variables (--env)
- Escape Sequences (--escape)
- Euro Character (--euro)
- Fixed font size (--fixedfont)
- Font Family (--font)
- Font Size (--fontsize)
- Foreground Color (--3270fg) 3270
- Foreground Color (--fg) 5250
- Height (--height)
- Host Locale (--hostlocale)
- Hosts tab (--appserv)
- Inherit parent's webtop content (--inherit)
- Interlaced Images (--interlaced)
- Keep launch connection open (--keepopen)
- Keyboard Map (--keymap)
- Keyboard Type (--3270kt) 3270
- Keyboard Type (--kt) 5250
- Keypad (--keypad)
- LDAP Groups (--ldapgroups)
- LDAP Search (--ldapsearch)
- LDAP Users (--ldapusers)
- Lines (--lines)
- Links tab (--links)
- Location (--location)
- Lock keymap (--lockkeymap)
- Login Script (--login)
- Max Instances (--maxinstances)
- Maximize the emulator window (--3270ma) 3270

- Maximize the emulator window (--ma) 5250
- May log in to Secure Global Desktop (--enabled)
- Members tab (--member)
- Middle Mouse Timeout (--middlemouse)
- Monitor Resolution (--dpi)
- Name (--name) domain component object
- Name (--name) objects with "common name"
- Name (--name) organization object
- Name (--name) organizational unit object
- Naming objects in the organizational hierarchy
- Open in new browser window (--newbrowser)
- Port Number (--portnumber) 3270
- Port Number (--portnumber) 5250
- Preferred Locale (--preflocale)
- Profile Editing (--editprofile)
- Protocol Arguments (--protoargs)
- Resumable (--resumable)
- Resumable For (--resumetimeout)
- Root Window (--roottype)
- Scale to fit window (--scalable)
- Scroll Style (--scrollstyle)
- Selecting a cipher suite for secure connections
- Serial Port Mapping (--serialport)
- Session Ends When (--endswhen)
- Share resources between similar sessions (--share)
- Shared between users (guest) (--shared)
- Soft Button Levels (--3270bl) 3270
- Soft Button Levels (--bl) 5250
- Status Line (--statusline)
- Surname (--surname)
- Terminal Type (--termtype)
- The tarantella array command
- The tarantella emulatorsession command
- The tarantella license command
- The tarantella object command
- The tarantella print command

- The tarantella query command
- The tarantella role command
- The tarantella security command
- The tarantella start cdm command
- The tarantella stop cdm command
- The tarantella version command
- The tarantella webserver command
- The tarantella webtopsession command
- Try running from client first (--trylocal)
- Tuning the SSL Daemon process
- URL (--url)
- Use Windows cursor (--wincursor)
- Use graphics acceleration (--accel)
- Username (--user)
- Using Remote Desktop on Microsoft Windows XP Professional
- Using SecurID for application server authentication
- Webtop Hints (--hints)
- Webtop Icon (--icon)
- Webtop Theme (--webtop)
- Width (--width)
- Window Close Action (--windowclose)
- Window Manager (--winmgr)
- Windows NT Domain (--ntdomain)
- Windows Protocol (--winproto)
- Wrap long lines (--autowrap)
- Client printers (--mapprinters)
- Customizing the Native Client for UNIX
- Driver name (--pdfdriver)
- Let users print to a PDF local file (--pdfviewerenabled)
- Let users print to a PDF printer (--pdfenabled)
- Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
- Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
- The tarantella array detach command
- The tarantella array join command
- The tarantella array list command
- The tarantella array make\_primary command
- The tarantella emulatorsession end command

- The tarantella emulatorsession info command
- The tarantella emulatorsession list command
- The tarantella emulatorsession shadow command
- The tarantella emulatorsession suspend command
- The tarantella license add command
- The tarantella license info command
- The tarantella license list command
- The tarantella license query command
- The tarantella license remove command
- The tarantella license status command
- The tarantella object add\_host command
- The tarantella object add\_link command
- The tarantella object add\_member command
- The tarantella object delete command
- The tarantella object edit command
- The tarantella object list\_attributes command
- The tarantella object list\_contents command
- The tarantella object new\_3270app command
- The tarantella object new\_5250app command
- The tarantella object new\_charapp command
- The tarantella object new\_container command
- The tarantella object new\_dc command
- The tarantella object new\_doc command
- The tarantella object new\_group command
- The tarantella object new\_host command
- The tarantella object new\_org command
- The tarantella object new\_orgunit command
- The tarantella object new\_person command
- The tarantella object new\_windowsapp command
- The tarantella object new\_xapp command
- The tarantella object remove\_host command
- The tarantella object remove\_link command
- The tarantella object remove\_member command
- The tarantella object rename command
- The tarantella object script command
- The tarantella print cancel command

- The tarantella print list command
- The tarantella print move command
- The tarantella print pause command
- The tarantella print resume command
- The tarantella print start command
- The tarantella print status command
- The tarantella print stop command
- The tarantella query audit command
- The tarantella query billing command
- The tarantella query errlog command
- The tarantella query uptime command
- The tarantella role add\_link command
- The tarantella role add\_member command
- The tarantella role list command
- The tarantella role list\_links command
- The tarantella role list\_members command
- The tarantella role remove\_link command
- The tarantella role remove\_member command
- The tarantella security certinfo command
- The tarantella security certrequest command
- The tarantella security certuse command
- The tarantella security customca command
- The tarantella security decryptkey command
- The tarantella security fingerprint command
- The tarantella security peerca command
- The tarantella security start command
- The tarantella security stop command
- The tarantella tscal command
- The tarantella tscal free command
- The tarantella tscal list command
- The tarantella tscal return command
- The tarantella webserver add\_trusted\_user command
- The tarantella webserver delete\_trusted\_user command
- The tarantella webserver list\_trusted\_users command
- The tarantella webserver restart command
- The tarantella webserver start command
- The tarantella webserver stop command

- The tarantella webtopsession list command
- The tarantella webtopsession logout command
- User-specific printing configuration (--userprintingconfig)
- **Troubleshooting**
  - An application's animation appears "jumpy"
  - Applications disappear after about two minutes
  - Users are unable to copy and paste text or graphics
  - Users cannot print from applications displayed through Secure Global Desktop
  - Using Windows Terminal Services, users are prompted for usernames and passwords too often
  - An "Ambiguous username" dialog is displayed when a user tries to log in
  - LDAP users can't log in to Secure Global Desktop
  - Solaris OS users are unable to log in when Secure Global Desktop security services are running
  - Users are having problems accessing client drives
  - Users complain of poor performance with the Windows desktop
  - A Kiosk application isn't appearing full-screen
  - An application requires a richer set of cursors
  - In some X applications, the ALT and ALT GR keys do not work
  - Troubleshooting printer preferences and settings
  - Troubleshooting sound in Windows applications
  - Users are unable to use smart cards with Windows applications
  - Users have problems displaying high color X applications
  - When Secure Global Desktop printing has been disabled, print jobs can still be queued
  - Windows 2000 users are unable to print a file from a mapped network drive
  - Running Windows applications on client devices
  - Users are unable to relocate their webtop sessions
  - Users see window clipping with Client Window Management applications
  - With Secure Global Desktop PDF printing, fonts don't print as expected
- **Frequently asked questions**
  - Can users access Secure Global Desktop without Java technology?
  - Does the browser-based webtop use themes?
  - How do I enable sound in Windows applications?
  - What are Secure Global Desktop security services?
  - What is a role object?
  - Why do users see a printer called \_Default in their Windows application?
  - Can I use Secure Global Desktop to access VMS applications?



- How do I run a Common Desktop Environment (CDE) session?
- Can I access a web application through Secure Global Desktop?
- Can I change the name of the printer in the Windows 2000/2003 application session?

## **For in-depth Secure Global Desktop administration** [Next section](#)

- **Tutorials**
  - Introducing web server authentication
  - Using shadowing in the classroom
- **Case studies**
  - Using Secure Global Desktop with the HTTPS port through a firewall
  - Populating the Secure Global Desktop organizational hierarchy using a batch script
  - Remapping or hiding Windows 2000/2003 application server drives
  - Using Secure Global Desktop with firewalls
- **Reference**
  - Backing up and restoring a Secure Global Desktop installation
  - User prompts and X.509 certificates
  - Using Secure Global Desktop with proxy servers
  - Denying users access to Secure Global Desktop after failed login attempts
  - Editing application server load balancing properties
  - Enabling web server authentication for the browser-based webtop
  - Enabling web server authentication for the classic webtop
  - Native Client preferences files on UNIX, Linux and Mac OS X client devices
  - Running the Native Client from the command line
  - Security considerations of using web server authentication
  - Tuning application server load balancing
  - Installing and using SSH with Secure Global Desktop
  - Secure Global Desktop and Java archives
  - The tarantella archive command
  - The tarantella arraymanager command
  - The tarantella cache command
  - The tarantella config command
  - The tarantella passcache command
  - The tarantella setup command
  - The tarantella tokencache command
  - Managing unauthenticated connections to Secure Global Desktop
  - The tarantella config edit command

- The tarantella config list command
- The tarantella passcache delete command
- The tarantella passcache edit command
- The tarantella passcache list command
- The tarantella passcache new command
- The tarantella tokencache delete command
- The tarantella tokencache list command
- Trusted users and third party authentication
- **Troubleshooting**
  - Users experience problems with web server authentication
  - Users are unable to connect to Secure Global Desktop when it is in firewall forwarding mode
  - Users see font problems
  - When X authorization is enabled, applications fail to start
  - All Administrators have been removed and no-one can use the administration tools
  - All login authorities are disabled and no-one can access Secure Global Desktop
  - Every server in the array has been disabled and no-one can access Secure Global Desktop
  - Secure Global Desktop uses too much of my network's bandwidth
- **Frequently asked questions**
  - What certificates does Secure Global Desktop support?
  - Can I run another SMB service with client drive mapping?
  - How can I support users with a client-side firewall that only allows connections on the HTTPS port?
  - How do I tell what connection type a user gets?
  - Can I use an X.509 certificate for another product with Secure Global Desktop?
  - How do I support additional Certificate Authorities?
  - If the array changes, do I have to re-configure printing?
  - What happens when a user's password expires?
  - Can I deny an LDAP user access to Secure Global Desktop?
  - Can I force users to print only to their default client printer?
  - Can I prevent users from launching applications with a different username and password?
  - Can I set a time limit for print jobs?
  - Can I use PKI client certificates with web server authentication?
  - Can I use SafeWord PremierAccess with web server authentication?
  - Can I use other web authentication schemes with Secure Global Desktop web server authentication?
  - Do I have to use distributed printing?
  - How can I make additional Native Clients available?

- How do I use my own X fonts?
- What X fonts are installed?
- What ports does Secure Global Desktop use?
- Can I chain Certificate Authority certificates?
- Can I use multiple monitors with Secure Global Desktop?

## **For Secure Global Desktop customizers** [Back to top](#)

- Case studies
  - Launching applications from JavaScript
- Reference
  - Relocating the browser-based webtop to your own JSP container
  - The ttawebtop.cgi CGI program
  - Client drive mapping (CDM) applet
  - Client drive mapping (CDM) applet parameters
  - Framework applet
  - Framework applet parameters
  - Increasing launch timeouts
  - Launching a single application without displaying a webtop
  - Login applet
  - Login applet parameters
  - Login script Tcl commands
  - Login script variables
  - Login scripts supplied with Secure Global Desktop
  - Print applet
  - Print applet parameters
  - Terminal emulator applet
  - Terminal emulator applet parameters
  - Terminal emulator attribute maps
  - Terminal emulator color maps
  - Terminal emulator keyboard maps
  - The TTAAPPLET tag
  - The tarantella Tcl command
  - Webtop script applet
  - Webtop script applet parameters
  - Webtop tray applet
  - Webtop tray applet parameters

- X emulator applet
- X emulator applet parameters
- Applet parameter data types
- Configuring Secure Global Desktop print job conversion
- Logging in with the Secure Global Desktop applets
- addValue (framework applet)
- areObjectsInitialized (webtop script and webtop tray applets)
- cancelCurrentJob (print applet)
- closeHierarchyLevel (webtop script and webtop tray applets)
- countJobs (print applet)
- getActive (print applet)
- getApplicationType (webtop script and webtop tray applets)
- getCurrentIteratorElement (webtop script and webtop tray applets)
- getEmulatorState (X emulator applet)
- getEmulatorState (terminal emulator applet)
- getEnabled (print applet)
- getIteratorForAllOpenHierarchyLevels (webtop script and webtop tray applets)
- getIteratorForHierarchyLevel (webtop script and webtop tray applets)
- getIteratorHasMoreElements (webtop script and webtop tray applets)
- getLaunchWaitTimeOut (webtop script and webtop script applets)
- getNextIteratorElement (webtop script and webtop tray applets)
- getNumberOfObjects (webtop script and webtop tray applets)
- getNumberOfObjectsInGroup (webtop script and webtop tray applets)
- getObjectClass (webtop script and webtop tray applets)
- getObjectDisplayName (webtop script and webtop tray applets)
- getObjectDisplayNameByName (webtop script and webtop tray applets)
- getObjectFullName (webtop script and webtop tray applets)
- getObjectImageName (webtop script and webtop tray applets)
- getObjectImageNameByName (webtop script and webtop tray applets)
- getObjectPlacement (webtop script and webtop tray applets)
- getParentGroupName (webtop script and webtop tray applets)
- getPrintState (print applet)
- getPrinterName (print applet)
- getPrinterPort (print applet)
- getPrinterType (print applet)
- getProperty (X emulator applet)
- getText (terminal emulator applet)

- getTotalNumberOfObjects (webtop script and webtop tray applets)
- getUnixTempDir (print applet)
- getUsername (framework applet)
- getValue (framework applet)
- getWebtopFramesetURL (framework applet)
- getWebtopURL (framework applet)
- getWindowsTempDir (print applet)
- isApplication (webtop script and webtop tray applets)
- isDocument (webtop script and webtop tray applets)
- isGroup (webtop script and webtop tray applets)
- isHierarchyEnabled (webtop script and webtop tray applets)
- isLoggedIn (framework applet)
- isOpenGroup (webtop script and webtop tray applets)
- isRunning (webtop script and webtop tray applets)
- killIterator (webtop script and webtop tray applets)
- launchByObjectName (webtop script and webtop tray applets)
- launchByObjectNumber (webtop script and webtop tray applets)
- login method
- logout method
- openGroup (webtop tray applet)
- openHierarchyLevel (webtop script and webtop tray applets)
- openParentGroup (webtop tray applet)
- receivedEvent (webtop script and webtop tray applets)
- registerProperty (X emulator applet)
- removeValue (framework applet)
- resetNamePassword (login applet)
- scriptStart method
- sendKey (terminal emulator applet)
- setActive (print applet)
- setEnabled (print applet)
- setLaunchWaitTimeOut (webtop script and webtop tray applets)
- setPausedState (print applet)
- setPrinterName (print applet)
- setPrinterPort (print applet)
- setPrinterType (print applet)
- setProperty (X emulator applet)

- setText (terminal emulator applet)
- setUnixTempDir (print applet)
- setWindowsTempDir (print applet)
- suspendApplication (X emulator applet)
- suspendApplication (terminal emulator applet)
- unregisterProperty (X emulator applet)
- Troubleshooting
  - A login script returns an error
- Frequently asked questions
  - What are login scripts?

# Sun Secure Global Desktop Software Administration Guide

## Tutorials [Next section](#)

- Getting started
  - [Introducing Sun Secure Global Desktop Software](#)
  - [Understanding webtop and emulator sessions](#)
  - [Integrating Secure Global Desktop with the desktop Start Menu](#)
  - [Introducing Array Manager](#)
  - [Introducing Object Manager](#)
  - [Securing client connections with Secure Global Desktop security services](#)
  - [Introducing the three-tier architecture](#)
  - [Objects and the organizational hierarchy](#)
  - [Users and trusted Secure Global Desktop servers](#)
- Clients and webtops
  - [Introducing Sun Secure Global Desktop Software](#)
  - [Integrating Secure Global Desktop with the desktop Start Menu](#)
  - [Securing client connections with Secure Global Desktop security services](#)
- Arrays, servers and load balancing
  - [Introducing Array Manager](#)
  - [Introducing the Secure Global Desktop Web Server](#)
  - [Introducing webtop and emulator session load balancing](#)
  - [Introducing application server load balancing](#)
  - [The Secure Global Desktop datastore and Tarantella Federated Naming](#)
- Users and authentication
  - [Secure Global Desktop and user authentication](#)
  - [Understanding webtop and emulator sessions](#)
  - [Introducing web server authentication](#)
  - [Login authorities](#)
- Applications, documents and hosts
  - [Understanding webtop and emulator sessions](#)
  - [Using copy and paste with Secure Global Desktop](#)
  - [Using shadowing in the classroom](#)

- Organizing your resources
  - Introducing Object Manager
  - Objects and the organizational hierarchy
- Security
  - Securing client connections with Secure Global Desktop security services
  - Security and Secure Global Desktop
  - Improving security between Secure Global Desktop servers and application servers
  - Improving security between client devices and Secure Global Desktop servers
  - Users and trusted Secure Global Desktop servers
  - Sharing web server and Secure Global Desktop server certificates
- Printing
  - Introducing Secure Global Desktop printing

## Case studies Next section

- Getting started
  - Creating and configuring a person object
  - Creating and publishing an application object to users
  - Using shadowing to troubleshoot a user's problem
- Users and authentication
  - Creating and configuring a person object
  - Populating the Secure Global Desktop organizational hierarchy using a batch script
- Applications, documents and hosts
  - Creating and publishing an application object to users
  - Populating the Secure Global Desktop organizational hierarchy using a batch script
  - Remapping or hiding Windows 2000/2003 application server drives
  - Launching applications from JavaScript
  - Using shadowing to troubleshoot a user's problem
- Organizing your resources
  - Populating the Secure Global Desktop organizational hierarchy using a batch script
- Security
  - Obtaining and installing an X.509 certificate
  - Giving secure connections across the Internet
  - Giving secure connections to a Secure Global Desktop server
  - Giving secure connections to all users in a department
  - Using Secure Global Desktop with the HTTPS port through a firewall
  - Using Secure Global Desktop with firewalls



- Applets
  - Launching applications from JavaScript

## Reference [Next section](#)

- Getting started
  - The tarantella command
  - Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop
  - Licensing and Sun Secure Global Desktop Software
  - Setting up and dismantling a Secure Global Desktop array
  - Sun Secure Global Desktop Software legal and copyright information
- Clients and webtops
  - Working with the Sun Secure Global Desktop Client
  - Configuring the Sun Secure Global Desktop Client for desktop Start Menu integration
  - Profiles and the Sun Secure Global Desktop Client
  - Native Client preferences files on UNIX, Linux and Mac OS X client devices
  - Relocating the browser-based webtop to your own JSP container
  - Running the Native Client from the command line
  - Profile Editing (--editprofile)
  - Secure Global Desktop and Java archives
- Arrays, servers and load balancing
  - Backing up and restoring a Secure Global Desktop installation
  - Application Launch properties (array-wide)
  - Array properties (array-wide)
  - Channel Protocol Engine properties (server-specific)
  - Character Protocol Engine properties (server-specific)
  - Emulator Sessions properties (array-wide)
  - Execution Protocol Engine properties (server-specific)
  - General properties (server-specific)
  - Licenses properties (array-wide)
  - Load Balancing properties (array-wide)
  - Print Protocol Engine properties (server-specific)
  - Printing properties (array-wide)
  - Secure Global Desktop Login properties (array-wide)
  - Security properties (array-wide)
  - Security properties (server-specific)
  - Setting up and dismantling a Secure Global Desktop array

- Smart Card Protocol Engine properties
- Tuning properties (server-specific)
- X Protocol Engine properties (server-specific)
- Audio Protocol Engine properties (server-specific)
- Configuring application server load balancing
- Editing application server load balancing properties
- Tuning application server load balancing
- Using log filters for auditing
- Using log filters to troubleshoot problems with the Secure Global Desktop server
- Configuring your own web server for use with Secure Global Desktop
- Hosts tab (--appserv)
- Location (--location)
- The tarantella archive command
- The tarantella array command
- The tarantella arraymanager command
- The tarantella config command
- The tarantella query command
- The tarantella restart command
- The tarantella start command
- The tarantella status command
- The tarantella stop command
- Managing unauthenticated connections to Secure Global Desktop
- **Users and authentication**
  - Person object
  - Execution Protocol Engine properties (server-specific)
  - Roles in Secure Global Desktop
  - Secure Global Desktop Login properties (array-wide)
  - The Active Directory login authority
  - The Anonymous user login authority
  - The ENS login authority
  - The LDAP login authority
  - The NT login authority
  - The SecurID login authority
  - The UNIX group login authority
  - The UNIX user login authority
  - The authentication token login authority
  - Using shared accounts for "guest" users

- Web server/third party authentication
- Working with users in different locales
- Denying users access to Secure Global Desktop after failed login attempts
- Enabling the Active Directory login authority
- Enabling the LDAP login authority
- Enabling the NT login authority
- Enabling the SecurID login authority
- Enabling web server authentication for the browser-based webtop
- Enabling web server authentication for the classic webtop
- Mirroring your LDAP organization in ENS
- Security considerations of using web server authentication
- Using Directory Services Integration
- Using the authentication token login authority for automatic logins
- Bandwidth Limit (--bandwidth)
- Client Drive Mapping (--cdm)
- Connections (--conntype)
- Description (--description)
- Email Address (--email)
- Increasing launch timeouts
- Inherit parent's webtop content (--inherit)
- Keyboard Map (--keymap)
- Links tab (--links)
- Login Script (--login)
- Login script Tcl commands
- Login script variables
- Login scripts supplied with Secure Global Desktop
- May log in to Secure Global Desktop (--enabled)
- Name (--name) objects with "common name"
- Preferred Locale (--preflocale)
- Shared between users (guest) (--shared)
- Surname (--surname)
- The tarantella Tcl command
- The tarantella cache command
- The tarantella emulatorsession command
- The tarantella object command
- The tarantella passcache command

- The tarantella role command
- The tarantella tokencache command
- The tarantella webtopsession command
- Username (--user)
- Using SecurID for application server authentication
- Webtop Theme (--webtop)
- Windows NT Domain (--ntdomain)
- Client printers (--mapprinters)
- Driver name (--pdfdriver)
- Let users print to a PDF local file (--pdfviewerenabled)
- Let users print to a PDF printer (--pdfenabled)
- Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
- Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
- The tarantella tokencache delete command
- The tarantella tokencache list command
- Trusted users and third party authentication
- User-specific printing configuration (--userprintingconfig)
- Applications, documents and hosts
  - 3270 application object
  - 5250 application object
  - Character application object
  - Document object
  - Host object
  - Windows application object
  - X application object
  - Application Launch properties (array-wide)
  - Character Protocol Engine properties (server-specific)
  - Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop
  - Configuring client drive mapping
  - Emulator Sessions properties (array-wide)
  - Load Balancing properties (array-wide)
  - X Protocol Engine properties (server-specific)
  - Available to run applications (--available)
  - Configuring access to serial ports
  - Load Balancing Algorithm (--loadbal)
  - Mirroring your LDAP organization in ENS
  - Using Directory Services Integration

- Using seamless windows for Windows applications
- Using smart cards with Windows applications
- 3270 Host (--hostname)
- AS/400 Host (--hostname)
- Address (--address)
- Allow delayed updates (--delayed)
- Answerback Message (--answermsg)
- Application Command (--app)
- Application key mode (--appkeymode)
- Application supports 3-button mouse only (--force3button)
- Arguments For Command (--args)
- Attribute Map (--attributemap)
- Authentication (--auth)
- Background Color (--3270bg) 3270
- Background Color (--bg) 5250
- Border Style (--border)
- Client's maximum size (--maximize)
- Clipboard Access (--clipboard)
- Clipboard Security Level (--clipboardlevel)
- Close Telnet Action (--3270tnclose) 3270
- Close Telnet Action (--tnclose) 5250
- Code Page (--codepage)
- Color (--rootcolor)
- Color Map (--colormap)
- Color depth (--depth)
- Color quality (--quality)
- Columns (--cols)
- Command Compression (--compression)
- Command Execution (--execution)
- Connection Method (--method)
- Cursor (--cursor)
- Cursor Keys (--cursorkeys)
- Description (--description)
- Display Using (--displayusing)
- Emulation Type (--emulator)
- Emulator Applet Page (--empage)

- Enable File and Settings menus (--3270si) 3270
- Enable File and Settings menus (--si) 5250
- Enable X Security Extension (--securityextension)
- Enable menu bar (--3270mb) 3270
- Enable menu bar (--mb) 5250
- Environment Variables (--env)
- Escape Sequences (--escape)
- Euro Character (--euro)
- Fixed font size (--fixedfont)
- Font Family (--font)
- Font Size (--fontsize)
- Foreground Color (--3270fg) 3270
- Foreground Color (--fg) 5250
- Height (--height)
- Host Locale (--hostlocale)
- Hosts tab (--appserv)
- Interlaced Images (--interlaced)
- Keep launch connection open (--keepopen)
- Keyboard Map (--keymap)
- Keyboard Type (--3270kt) 3270
- Keyboard Type (--kt) 5250
- Keypad (--keypad)
- LDAP Groups (--ldapgroups)
- LDAP Search (--ldapsearch)
- LDAP Users (--ldapusers)
- Launching a single application without displaying a webtop
- Lines (--lines)
- Location (--location)
- Lock keymap (--lockkeymap)
- Login Script (--login)
- Max Instances (--maxinstances)
- Maximize the emulator window (--3270ma) 3270
- Maximize the emulator window (--ma) 5250
- Middle Mouse Timeout (--middlemouse)
- Monitor Resolution (--dpi)
- Name (--name) objects with "common name"
- Open in new browser window (--newbrowser)

- Port Number (--portnumber) 3270
- Port Number (--portnumber) 5250
- Protocol Arguments (--protoargs)
- Resumable (--resumable)
- Resumable For (--resumetimeout)
- Root Window (--roottype)
- Scale to fit window (--scalable)
- Scroll Style (--scrollstyle)
- Serial Port Mapping (--serialport)
- Session Ends When (--endswhen)
- Share resources between similar sessions (--share)
- Soft Button Levels (--3270bl) 3270
- Soft Button Levels (--bl) 5250
- Status Line (--statusline)
- Terminal Type (--termttype)
- Terminal emulator attribute maps
- Terminal emulator color maps
- Terminal emulator keyboard maps
- The tarantella emulatorsession command
- The tarantella object command
- Try running from client first (--trylocal)
- URL (--url)
- Use Windows cursor (--wincursor)
- Use graphics acceleration (--accel)
- Using Remote Desktop on Microsoft Windows XP Professional
- Webtop Hints (--hints)
- Webtop Icon (--icon)
- Width (--width)
- Window Close Action (--windowclose)
- Window Manager (--winmgr)
- Windows NT Domain (--ntdomain)
- Windows Protocol (--winproto)
- Wrap long lines (--autowrap)
- Customizing the Native Client for UNIX
- Organizing your resources
  - Active Directory container object

- Domain component object
- Group object
- Organization object
- Organizational unit object
- Client Drive Mapping (--cdm)
- Connections (--conntype)
- Description (--description)
- Inherit parent's webtop content (--inherit)
- Links tab (--links)
- Members tab (--member)
- Name (--name) domain component object
- Name (--name) organization object
- Name (--name) organizational unit object
- Naming objects in the organizational hierarchy
- The tarantella object command
- Webtop Theme (--webtop)
- Client printers (--mapprinters)
- Driver name (--pdfdriver)
- Let users print to a PDF local file (--pdfviewerenabled)
- Let users print to a PDF printer (--pdfenabled)
- Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
- Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
- User-specific printing configuration (--userprintingconfig)
- **Security**
  - Securing connections between Secure Global Desktop servers
  - Securing connections to Active Directory and LDAP directory servers
  - Securing the SOAP connections to a Secure Global Desktop server
  - Security properties (array-wide)
  - Security properties (server-specific)
  - User prompts and X.509 certificates
  - Using Secure Global Desktop with proxy servers
  - Connections (--conntype)
  - Installing and using SSH with Secure Global Desktop
  - Selecting a cipher suite for secure connections
  - The tarantella security command
  - Tuning the SSL Daemon process
- **Printing**



- Print Protocol Engine properties (server-specific)
- Printing properties (array-wide)
- Configuring printing for UNIX, Linux and Mac OS X clients
- Configuring printing if you use the Common UNIX Printing System (CUPS)
- Configuring the Secure Global Desktop server to accept remote print requests
- Printing from a Microsoft Windows 2000/2003 application server
- Printing from a Microsoft Windows NT 3.51 application server
- Printing from a Microsoft Windows NT 4 application server
- Printing from a UNIX or Linux application server
- The prtinstall.en.sh script
- Configuring Secure Global Desktop PDF printing
- The tarantella print command
- Client printers (--mapprinters)
- Configuring Secure Global Desktop print job conversion
- Driver name (--pdfdriver)
- Let users print to a PDF local file (--pdfviewerenabled)
- Let users print to a PDF printer (--pdfenabled)
- Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
- Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
- User-specific printing configuration (--userprintingconfig)
- **Commands**
  - The tarantella command
  - The tarantella Tcl command
  - The tarantella archive command
  - The tarantella array command
  - The tarantella arraymanager command
  - The tarantella cache command
  - The tarantella config command
  - The tarantella emulatorsession command
  - The tarantella help command
  - The tarantella license command
  - The tarantella object command
  - The tarantella objectmanager command
  - The tarantella passcache command
  - The tarantella print command
  - The tarantella query command

- The tarantella restart command
- The tarantella role command
- The tarantella security command
- The tarantella setup command
- The tarantella start cdm command
- The tarantella start command
- The tarantella status command
- The tarantella stop cdm command
- The tarantella stop command
- The tarantella tokencache command
- The tarantella uninstall command
- The tarantella version command
- The tarantella webserver command
- The tarantella webtopsession command
- The tarantella array detach command
- The tarantella array join command
- The tarantella array list command
- The tarantella array make\_primary command
- The tarantella config edit command
- The tarantella config list command
- The tarantella emulatorsession end command
- The tarantella emulatorsession info command
- The tarantella emulatorsession list command
- The tarantella emulatorsession shadow command
- The tarantella emulatorsession suspend command
- The tarantella license add command
- The tarantella license info command
- The tarantella license list command
- The tarantella license query command
- The tarantella license remove command
- The tarantella license status command
- The tarantella object add\_host command
- The tarantella object add\_link command
- The tarantella object add\_member command
- The tarantella object delete command
- The tarantella object edit command
- The tarantella object list\_attributes command

- The tarantella object list\_contents command
- The tarantella object new\_3270app command
- The tarantella object new\_5250app command
- The tarantella object new\_charapp command
- The tarantella object new\_container command
- The tarantella object new\_dc command
- The tarantella object new\_doc command
- The tarantella object new\_group command
- The tarantella object new\_host command
- The tarantella object new\_org command
- The tarantella object new\_orgunit command
- The tarantella object new\_person command
- The tarantella object new\_windowsapp command
- The tarantella object new\_xapp command
- The tarantella object remove\_host command
- The tarantella object remove\_link command
- The tarantella object remove\_member command
- The tarantella object rename command
- The tarantella object script command
- The tarantella passcache delete command
- The tarantella passcache edit command
- The tarantella passcache list command
- The tarantella passcache new command
- The tarantella print cancel command
- The tarantella print list command
- The tarantella print move command
- The tarantella print pause command
- The tarantella print resume command
- The tarantella print start command
- The tarantella print status command
- The tarantella print stop command
- The tarantella query audit command
- The tarantella query billing command
- The tarantella query errlog command
- The tarantella query uptime command
- The tarantella role add\_link command

- The tarantella role add\_member command
- The tarantella role list command
- The tarantella role list\_links command
- The tarantella role list\_members command
- The tarantella role remove\_link command
- The tarantella role remove\_member command
- The tarantella security certinfo command
- The tarantella security certrequest command
- The tarantella security certuse command
- The tarantella security customca command
- The tarantella security decryptkey command
- The tarantella security fingerprint command
- The tarantella security peerca command
- The tarantella security start command
- The tarantella security stop command
- The tarantella tokencache delete command
- The tarantella tokencache list command
- The tarantella tscal command
- The tarantella tscal free command
- The tarantella tscal list command
- The tarantella tscal return command
- The tarantella webserver add\_trusted\_user command
- The tarantella webserver delete\_trusted\_user command
- The tarantella webserver list\_trusted\_users command
- The tarantella webserver restart command
- The tarantella webserver start command
- The tarantella webserver stop command
- The tarantella webtopsession list command
- The tarantella webtopsession logout command
- Applets
  - The ttawebtop.cgi CGI program
  - Client drive mapping (CDM) applet
  - Client drive mapping (CDM) applet parameters
  - Framework applet
  - Framework applet parameters
  - Login applet
  - Login applet parameters

- Print applet
- Print applet parameters
- Terminal emulator applet
- Terminal emulator applet parameters
- The TTAAPPLET tag
- Webtop script applet
- Webtop script applet parameters
- Webtop tray applet
- Webtop tray applet parameters
- X emulator applet
- X emulator applet parameters
- Applet parameter data types
- Logging in with the Secure Global Desktop applets
- addValue (framework applet)
- areObjectsInitialized (webtop script and webtop tray applets)
- cancelCurrentJob (print applet)
- closeHierarchyLevel (webtop script and webtop tray applets)
- countJobs (print applet)
- getActive (print applet)
- getApplicationType (webtop script and webtop tray applets)
- getCurrentIteratorElement (webtop script and webtop tray applets)
- getEmulatorState (X emulator applet)
- getEmulatorState (terminal emulator applet)
- getEnabled (print applet)
- getIteratorForAllOpenHierarchyLevels (webtop script and webtop tray applets)
- getIteratorForHierarchyLevel (webtop script and webtop tray applets)
- getIteratorHasMoreElements (webtop script and webtop tray applets)
- getLaunchWaitTimeOut (webtop script and webtop script applets)
- getNextIteratorElement (webtop script and webtop tray applets)
- getNumberOfObjects (webtop script and webtop tray applets)
- getNumberOfObjectsInGroup (webtop script and webtop tray applets)
- getObjectClass (webtop script and webtop tray applets)
- getObjectDisplayName (webtop script and webtop tray applets)
- getObjectDisplayNameByName (webtop script and webtop tray applets)
- getObjectFullName (webtop script and webtop tray applets)
- getObjectImageName (webtop script and webtop tray applets)

- getObjectImageNameByName (webtop script and webtop tray applets)
- getObjectPlacement (webtop script and webtop tray applets)
- getParentGroupName (webtop script and webtop tray applets)
- getPrintState (print applet)
- getPrinterName (print applet)
- getPrinterPort (print applet)
- getPrinterType (print applet)
- getProperty (X emulator applet)
- getText (terminal emulator applet)
- getTotalNumberOfObjects (webtop script and webtop tray applets)
- getUnixTempDir (print applet)
- getUsername (framework applet)
- getValue (framework applet)
- getWebtopFramesetURL (framework applet)
- getWebtopURL (framework applet)
- getWindowsTempDir (print applet)
- isApplication (webtop script and webtop tray applets)
- isDocument (webtop script and webtop tray applets)
- isGroup (webtop script and webtop tray applets)
- isHierarchyEnabled (webtop script and webtop tray applets)
- isLoggedIn (framework applet)
- isOpenGroup (webtop script and webtop tray applets)
- isRunning (webtop script and webtop tray applets)
- killIterator (webtop script and webtop tray applets)
- launchByObjectName (webtop script and webtop tray applets)
- launchByObjectNumber (webtop script and webtop tray applets)
- login method
- logout method
- openGroup (webtop tray applet)
- openHierarchyLevel (webtop script and webtop tray applets)
- openParentGroup (webtop tray applet)
- receivedEvent (webtop script and webtop tray applets)
- registerProperty (X emulator applet)
- removeValue (framework applet)
- resetNamePassword (login applet)
- scriptStart method
- sendKey (terminal emulator applet)

- setActive (print applet)
- setEnabled (print applet)
- setLaunchWaitTimeOut (webtop script and webtop tray applets)
- setPausedState (print applet)
- setPrinterName (print applet)
- setPrinterPort (print applet)
- setPrinterType (print applet)
- setProperty (X emulator applet)
- setText (terminal emulator applet)
- setUnixTempDir (print applet)
- setWindowsTempDir (print applet)
- suspendApplication (X emulator applet)
- suspendApplication (terminal emulator applet)
- unregisterProperty (X emulator applet)

## Troubleshooting Next section

- Arrays, servers and load balancing
  - Troubleshooting CPU/memory-based application server load balancing
  - All login authorities are disabled and no-one can access Secure Global Desktop
  - Every server in the array has been disabled and no-one can access Secure Global Desktop
  - Users are unable to relocate their webtop sessions
- Users and authentication
  - A session doesn't end when the user exits the application
  - Users are unable to copy and paste text or graphics
  - Users experience problems with web server authentication
  - Using Windows Terminal Services, users are prompted for usernames and passwords too often
  - An "Ambiguous username" dialog is displayed when a user tries to log in
  - LDAP users can't log in to Secure Global Desktop
  - Users see font problems
  - A login script returns an error
  - All login authorities are disabled and no-one can access Secure Global Desktop
  - Secure Global Desktop uses too much of my network's bandwidth
- Applications, documents and hosts
  - A session doesn't end when the user exits the application
  - An application exits immediately after starting

- An application won't start
- An application's animation appears "jumpy"
- Applications disappear after about two minutes
- Users are having problems accessing client drives
- Users complain of poor performance with the Windows desktop
- When X authorization is enabled, applications fail to start
- A Kiosk application isn't appearing full-screen
- An application requires a richer set of cursors
- In some X applications, the ALT and ALT GR keys do not work
- Troubleshooting sound in Windows applications
- Users are unable to use smart cards with Windows applications
- Users have problems displaying high color X applications
- Running Windows applications on client devices
- Secure Global Desktop uses too much of my network's bandwidth
- Users see window clipping with Client Window Management applications
- Organizing your resources
  - All Administrators have been removed and no-one can use the administration tools
- Security
  - Solaris OS users are unable to log in when Secure Global Desktop security services are running
  - Users are unable to connect to Secure Global Desktop when it is in firewall forwarding mode
- Printing
  - Users cannot print from applications displayed through Secure Global Desktop
  - Troubleshooting printer preferences and settings
  - When Secure Global Desktop printing has been disabled, print jobs can still be queued
  - Windows 2000 users are unable to print a file from a mapped network drive
  - With Secure Global Desktop PDF printing, fonts don't print as expected

## Frequently asked questions [Back to top](#)

- Getting started
  - How do I add new Secure Global Desktop Administrators?
  - What do I need to tell my users?
  - Do I need to license Windows Terminal Services?
- Clients and webtops
  - Can users access Secure Global Desktop without Java technology?
  - Does the browser-based webtop use themes?



- How can I make additional Native Clients available?
- **Arrays, servers and load balancing**
  - What is an array?
  - What's in the Secure Global Desktop installation directory?
  - Where is Secure Global Desktop installed?
- **Users and authentication**
  - What do I need to tell my users?
  - How do I tell what connection type a user gets?
  - What happens when a user's password expires?
  - What is a role object?
  - Can I deny an LDAP user access to Secure Global Desktop?
  - Can I use PKI client certificates with web server authentication?
  - Can I use SafeWord PremierAccess with web server authentication?
  - Can I use other web authentication schemes with Secure Global Desktop web server authentication?
  - What are login scripts?
- **Applications, documents and hosts**
  - Can I run another SMB service with client drive mapping?
  - Do I need to license Windows Terminal Services?
  - How do I enable sound in Windows applications?
  - Can I prevent users from launching applications with a different username and password?
  - Can I use Secure Global Desktop to access VMS applications?
  - How do I run a Common Desktop Environment (CDE) session?
  - How do I use my own X fonts?
  - What X fonts are installed?
  - Can I access a web application through Secure Global Desktop?
  - Can I use multiple monitors with Secure Global Desktop?
- **Organizing your resources**
  - What is ENS?
  - What is the Tarantella System Objects organization?
- **Security**
  - What are X.509 certificates and why do I need one?
  - What certificates does Secure Global Desktop support?
  - How can I support users with a client-side firewall that only allows connections on the HTTPS port?
  - How do I tell what connection type a user gets?
  - What are peer DNS names and external DNS names?

- Can I use an X.509 certificate for another product with Secure Global Desktop?
- How do I support additional Certificate Authorities?
- What are Secure Global Desktop security services?
- Can I use PKI client certificates with web server authentication?
- Can I use SafeWord PremierAccess with web server authentication?
- Can I use other web authentication schemes with Secure Global Desktop web server authentication?
- What ports does Secure Global Desktop use?
- Can I chain Certificate Authority certificates?
- **Printing**
  - If the array changes, do I have to re-configure printing?
  - Why do users see a printer called \_Default in their Windows application?
  - Can I force users to print only to their default client printer?
  - Can I set a time limit for print jobs?
  - Do I have to use distributed printing?
  - Can I change the name of the printer in the Windows 2000/2003 application session?
- **Applets**
  - How does Secure Global Desktop use applets?

# Sun Secure Global Desktop Software Administration Guide

## Tutorials [Next section](#)

- For new Secure Global Desktop Administrators
  - [Introducing Sun Secure Global Desktop Software](#)
  - [Secure Global Desktop and user authentication](#)
  - [Understanding webtop and emulator sessions](#)
  - [Integrating Secure Global Desktop with the desktop Start Menu](#)
  - [Introducing Array Manager](#)
  - [Introducing Object Manager](#)
  - [Introducing Secure Global Desktop printing](#)
  - [Introducing the Secure Global Desktop Web Server](#)
  - [Introducing webtop and emulator session load balancing](#)
  - [Securing client connections with Secure Global Desktop security services](#)
  - [Security and Secure Global Desktop](#)
  - [Improving security between Secure Global Desktop servers and application servers](#)
  - [Improving security between client devices and Secure Global Desktop servers](#)
  - [Introducing application server load balancing](#)
  - [Introducing the three-tier architecture](#)
  - [Objects and the organizational hierarchy](#)
  - [The Secure Global Desktop datastore and Tarantella Federated Naming](#)
  - [Users and trusted Secure Global Desktop servers](#)
  - [Using copy and paste with Secure Global Desktop](#)
  - [Sharing web server and Secure Global Desktop server certificates](#)
- For day-to-day Secure Global Desktop administration
  - [Login authorities](#)
- For in-depth Secure Global Desktop administration
  - [Introducing web server authentication](#)
  - [Using shadowing in the classroom](#)

## Case studies [Next section](#)

- For new Secure Global Desktop Administrators

- Obtaining and installing an X.509 certificate
- Giving secure connections across the Internet
- Giving secure connections to a Secure Global Desktop server
- Giving secure connections to all users in a department
- Creating and configuring a person object
- Creating and publishing an application object to users
- For day-to-day Secure Global Desktop administration
  - Using shadowing to troubleshoot a user's problem
- For in-depth Secure Global Desktop administration
  - Using Secure Global Desktop with the HTTPS port through a firewall
  - Populating the Secure Global Desktop organizational hierarchy using a batch script
  - Remapping or hiding Windows 2000/2003 application server drives
  - Using Secure Global Desktop with firewalls
- For Secure Global Desktop customizers
  - Launching applications from JavaScript

## Reference [Next section](#)

- For new Secure Global Desktop Administrators
  - The tarantella command
  - Working with the Sun Secure Global Desktop Client
  - Configuring Microsoft Windows Terminal Services for use with Secure Global Desktop
  - Configuring client drive mapping
  - Configuring the Sun Secure Global Desktop Client for desktop Start Menu integration
  - Profiles and the Sun Secure Global Desktop Client
  - Securing connections to Active Directory and LDAP directory servers
  - Securing the SOAP connections to a Secure Global Desktop server
  - Working with users in different locales
  - Configuring printing for UNIX, Linux and Mac OS X clients
  - Configuring printing if you use the Common UNIX Printing System (CUPS)
  - Configuring the Secure Global Desktop server to accept remote print requests
  - Printing from a Microsoft Windows 2000/2003 application server
  - Printing from a Microsoft Windows NT 3.51 application server
  - Printing from a Microsoft Windows NT 4 application server
  - Printing from a UNIX or Linux application server
  - Configuring Secure Global Desktop PDF printing
  - Configuring your own web server for use with Secure Global Desktop

- The tarantella help command
- The tarantella objectmanager command
- The tarantella restart command
- The tarantella start command
- The tarantella status command
- The tarantella stop command
- The tarantella uninstall command
- Sun Secure Global Desktop Software legal and copyright information
- For day-to-day Secure Global Desktop administration
  - 3270 application object
  - 5250 application object
  - Active Directory container object
  - Character application object
  - Document object
  - Domain component object
  - Group object
  - Host object
  - Organization object
  - Organizational unit object
  - Person object
  - Windows application object
  - X application object
  - Application Launch properties (array-wide)
  - Array properties (array-wide)
  - Channel Protocol Engine properties (server-specific)
  - Character Protocol Engine properties (server-specific)
  - Emulator Sessions properties (array-wide)
  - Execution Protocol Engine properties (server-specific)
  - General properties (server-specific)
  - Licenses properties (array-wide)
  - Licensing and Sun Secure Global Desktop Software
  - Load Balancing properties (array-wide)
  - Print Protocol Engine properties (server-specific)
  - Printing properties (array-wide)
  - Roles in Secure Global Desktop
  - Secure Global Desktop Login properties (array-wide)
  - Securing connections between Secure Global Desktop servers

- Security properties (array-wide)
- Security properties (server-specific)
- Setting up and dismantling a Secure Global Desktop array
- Smart Card Protocol Engine properties
- The Active Directory login authority
- The Anonymous user login authority
- The ENS login authority
- The LDAP login authority
- The NT login authority
- The SecurID login authority
- The UNIX group login authority
- The UNIX user login authority
- The authentication token login authority
- Tuning properties (server-specific)
- Using shared accounts for "guest" users
- Web server/third party authentication
- X Protocol Engine properties (server-specific)
- Audio Protocol Engine properties (server-specific)
- Available to run applications (--available)
- Configuring access to serial ports
- Configuring application server load balancing
- Enabling the Active Directory login authority
- Enabling the LDAP login authority
- Enabling the NT login authority
- Enabling the SecurID login authority
- Load Balancing Algorithm (--loadbal)
- Mirroring your LDAP organization in ENS
- The prtinstall.en.sh script
- Using Directory Services Integration
- Using log filters for auditing
- Using log filters to troubleshoot problems with the Secure Global Desktop server
- Using seamless windows for Windows applications
- Using smart cards with Windows applications
- Using the authentication token login authority for automatic logins
- 3270 Host (--hostname)
- AS/400 Host (--hostname)

- Address (--address)
- Allow delayed updates (--delayed)
- Answerback Message (--answermsg)
- Application Command (--app)
- Application key mode (--appkeymode)
- Application supports 3-button mouse only (--force3button)
- Arguments For Command (--args)
- Attribute Map (--attributemap)
- Authentication (--auth)
- Background Color (--3270bg) 3270
- Background Color (--bg) 5250
- Bandwidth Limit (--bandwidth)
- Border Style (--border)
- Client Drive Mapping (--cdm)
- Client's maximum size (--maximize)
- Clipboard Access (--clipboard)
- Clipboard Security Level (--clipboardlevel)
- Close Telnet Action (--3270tnclose) 3270
- Close Telnet Action (--tnclose) 5250
- Code Page (--codepage)
- Color (--rootcolor)
- Color Map (--colormap)
- Color depth (--depth)
- Color quality (--quality)
- Columns (--cols)
- Command Compression (--compression)
- Command Execution (--execution)
- Connection Method (--method)
- Connections (--conntype)
- Cursor (--cursor)
- Cursor Keys (--cursorkeys)
- Description (--description)
- Display Using (--displayusing)
- Email Address (--email)
- Emulation Type (--emulator)
- Emulator Applet Page (--empage)
- Enable File and Settings menus (--3270si) 3270

- Enable File and Settings menus (--si) 5250
- Enable X Security Extension (--securityextension)
- Enable menu bar (--3270mb) 3270
- Enable menu bar (--mb) 5250
- Environment Variables (--env)
- Escape Sequences (--escape)
- Euro Character (--euro)
- Fixed font size (--fixedfont)
- Font Family (--font)
- Font Size (--fontsize)
- Foreground Color (--3270fg) 3270
- Foreground Color (--fg) 5250
- Height (--height)
- Host Locale (--hostlocale)
- Hosts tab (--appserv)
- Inherit parent's webtop content (--inherit)
- Interlaced Images (--interlaced)
- Keep launch connection open (--keepopen)
- Keyboard Map (--keymap)
- Keyboard Type (--3270kt) 3270
- Keyboard Type (--kt) 5250
- Keypad (--keypad)
- LDAP Groups (--ldapgroups)
- LDAP Search (--ldapsearch)
- LDAP Users (--ldapusers)
- Lines (--lines)
- Links tab (--links)
- Location (--location)
- Lock keymap (--lockkeymap)
- Login Script (--login)
- Max Instances (--maxinstances)
- Maximize the emulator window (--3270ma) 3270
- Maximize the emulator window (--ma) 5250
- May log in to Secure Global Desktop (--enabled)
- Members tab (--member)
- Middle Mouse Timeout (--middlemouse)



- Monitor Resolution (--dpi)
- Name (--name) domain component object
- Name (--name) objects with "common name"
- Name (--name) organization object
- Name (--name) organizational unit object
- Naming objects in the organizational hierarchy
- Open in new browser window (--newbrowser)
- Port Number (--portnumber) 3270
- Port Number (--portnumber) 5250
- Preferred Locale (--preflocale)
- Profile Editing (--editprofile)
- Protocol Arguments (--protoargs)
- Resumable (--resumable)
- Resumable For (--resumetimeout)
- Root Window (--roottype)
- Scale to fit window (--scalable)
- Scroll Style (--scrollstyle)
- Selecting a cipher suite for secure connections
- Serial Port Mapping (--serialport)
- Session Ends When (--endswhen)
- Share resources between similar sessions (--share)
- Shared between users (guest) (--shared)
- Soft Button Levels (--3270bl) 3270
- Soft Button Levels (--bl) 5250
- Status Line (--statusline)
- Surname (--surname)
- Terminal Type (--termttype)
- The tarantella array command
- The tarantella emulatorsession command
- The tarantella license command
- The tarantella object command
- The tarantella print command
- The tarantella query command
- The tarantella role command
- The tarantella security command
- The tarantella start cdm command
- The tarantella stop cdm command

- The tarantella version command
- The tarantella webserver command
- The tarantella webtopsession command
- Try running from client first (--trylocal)
- Tuning the SSL Daemon process
- URL (--url)
- Use Windows cursor (--wincursor)
- Use graphics acceleration (--accel)
- Username (--user)
- Using Remote Desktop on Microsoft Windows XP Professional
- Using SecurID for application server authentication
- Webtop Hints (--hints)
- Webtop Icon (--icon)
- Webtop Theme (--webtop)
- Width (--width)
- Window Close Action (--windowclose)
- Window Manager (--winmgr)
- Windows NT Domain (--ntdomain)
- Windows Protocol (--winproto)
- Wrap long lines (--autowrap)
- Client printers (--mapprinters)
- Customizing the Native Client for UNIX
- Driver name (--pdfdriver)
- Let users print to a PDF local file (--pdfviewerenabled)
- Let users print to a PDF printer (--pdfenabled)
- Make PDF file printer the default for Windows 2000/3 (--pdfviewerisdefault)
- Make PDF printer the default for Windows 2000/3 (--pdfisdefault)
- The tarantella array detach command
- The tarantella array join command
- The tarantella array list command
- The tarantella array make\_primary command
- The tarantella emulatorsession end command
- The tarantella emulatorsession info command
- The tarantella emulatorsession list command
- The tarantella emulatorsession shadow command
- The tarantella emulatorsession suspend command

- The tarantella license add command
- The tarantella license info command
- The tarantella license list command
- The tarantella license query command
- The tarantella license remove command
- The tarantella license status command
- The tarantella object add\_host command
- The tarantella object add\_link command
- The tarantella object add\_member command
- The tarantella object delete command
- The tarantella object edit command
- The tarantella object list\_attributes command
- The tarantella object list\_contents command
- The tarantella object new\_3270app command
- The tarantella object new\_5250app command
- The tarantella object new\_charapp command
- The tarantella object new\_container command
- The tarantella object new\_dc command
- The tarantella object new\_doc command
- The tarantella object new\_group command
- The tarantella object new\_host command
- The tarantella object new\_org command
- The tarantella object new\_orgunit command
- The tarantella object new\_person command
- The tarantella object new\_windowsapp command
- The tarantella object new\_xapp command
- The tarantella object remove\_host command
- The tarantella object remove\_link command
- The tarantella object remove\_member command
- The tarantella object rename command
- The tarantella object script command
- The tarantella print cancel command
- The tarantella print list command
- The tarantella print move command
- The tarantella print pause command
- The tarantella print resume command
- The tarantella print start command

- The tarantella print status command
  - The tarantella print stop command
  - The tarantella query audit command
  - The tarantella query billing command
  - The tarantella query errlog command
  - The tarantella query uptime command
  - The tarantella role add\_link command
  - The tarantella role add\_member command
  - The tarantella role list command
  - The tarantella role list\_links command
  - The tarantella role list\_members command
  - The tarantella role remove\_link command
  - The tarantella role remove\_member command
  - The tarantella security certinfo command
  - The tarantella security certrequest command
  - The tarantella security certuse command
  - The tarantella security customca command
  - The tarantella security decryptkey command
  - The tarantella security fingerprint command
  - The tarantella security peerca command
  - The tarantella security start command
  - The tarantella security stop command
  - The tarantella tscal command
  - The tarantella tscal free command
  - The tarantella tscal list command
  - The tarantella tscal return command
  - The tarantella webserver add\_trusted\_user command
  - The tarantella webserver delete\_trusted\_user command
  - The tarantella webserver list\_trusted\_users command
  - The tarantella webserver restart command
  - The tarantella webserver start command
  - The tarantella webserver stop command
  - The tarantella webtopsession list command
  - The tarantella webtopsession logout command
  - User-specific printing configuration (--userprintingconfig)
- For in-depth Secure Global Desktop administration

- Backing up and restoring a Secure Global Desktop installation
- User prompts and X.509 certificates
- Using Secure Global Desktop with proxy servers
- Denying users access to Secure Global Desktop after failed login attempts
- Editing application server load balancing properties
- Enabling web server authentication for the browser-based webtop
- Enabling web server authentication for the classic webtop
- Native Client preferences files on UNIX, Linux and Mac OS X client devices
- Running the Native Client from the command line
- Security considerations of using web server authentication
- Tuning application server load balancing
- Installing and using SSH with Secure Global Desktop
- Secure Global Desktop and Java archives
- The tarantella archive command
- The tarantella arraymanager command
- The tarantella cache command
- The tarantella config command
- The tarantella passcache command
- The tarantella setup command
- The tarantella tokencache command
- Managing unauthenticated connections to Secure Global Desktop
- The tarantella config edit command
- The tarantella config list command
- The tarantella passcache delete command
- The tarantella passcache edit command
- The tarantella passcache list command
- The tarantella passcache new command
- The tarantella tokencache delete command
- The tarantella tokencache list command
- Trusted users and third party authentication
- For Secure Global Desktop customizers
  - Relocating the browser-based webtop to your own JSP container
  - The ttawebtop.cgi CGI program
  - Client drive mapping (CDM) applet
  - Client drive mapping (CDM) applet parameters
  - Framework applet
  - Framework applet parameters

- Increasing launch timeouts
- Launching a single application without displaying a webtop
- Login applet
- Login applet parameters
- Login script Tcl commands
- Login script variables
- Login scripts supplied with Secure Global Desktop
- Print applet
- Print applet parameters
- Terminal emulator applet
- Terminal emulator applet parameters
- Terminal emulator attribute maps
- Terminal emulator color maps
- Terminal emulator keyboard maps
- The TTAAPPLET tag
- The tarantella Tcl command
- Webtop script applet
- Webtop script applet parameters
- Webtop tray applet
- Webtop tray applet parameters
- X emulator applet
- X emulator applet parameters
- Applet parameter data types
- Configuring Secure Global Desktop print job conversion
- Logging in with the Secure Global Desktop applets
- addValue (framework applet)
- areObjectsInitialized (webtop script and webtop tray applets)
- cancelCurrentJob (print applet)
- closeHierarchyLevel (webtop script and webtop tray applets)
- countJobs (print applet)
- getActive (print applet)
- getApplicationType (webtop script and webtop tray applets)
- getCurrentIteratorElement (webtop script and webtop tray applets)
- getEmulatorState (X emulator applet)
- getEmulatorState (terminal emulator applet)
- getEnabled (print applet)

- `getIteratorForAllOpenHierarchyLevels` (webtop script and webtop tray applets)
- `getIteratorForHierarchyLevel` (webtop script and webtop tray applets)
- `getIteratorHasMoreElements` (webtop script and webtop tray applets)
- `getLaunchWaitTimeOut` (webtop script and webtop script applets)
- `getNextIteratorElement` (webtop script and webtop tray applets)
- `getNumberOfObjects` (webtop script and webtop tray applets)
- `getNumberOfObjectsInGroup` (webtop script and webtop tray applets)
- `getObjectClass` (webtop script and webtop tray applets)
- `getObjectDisplayName` (webtop script and webtop tray applets)
- `getObjectDisplayNameByName` (webtop script and webtop tray applets)
- `getObjectFullName` (webtop script and webtop tray applets)
- `getObjectImageName` (webtop script and webtop tray applets)
- `getObjectImageNameByName` (webtop script and webtop tray applets)
- `getObjectPlacement` (webtop script and webtop tray applets)
- `getParentGroupName` (webtop script and webtop tray applets)
- `getPrintState` (print applet)
- `getPrinterName` (print applet)
- `getPrinterPort` (print applet)
- `getPrinterType` (print applet)
- `getProperty` (X emulator applet)
- `getText` (terminal emulator applet)
- `getTotalNumberOfObjects` (webtop script and webtop tray applets)
- `getUnixTempDir` (print applet)
- `getUserName` (framework applet)
- `getValue` (framework applet)
- `getWebtopFramesetURL` (framework applet)
- `getWebtopURL` (framework applet)
- `getWindowsTempDir` (print applet)
- `isApplication` (webtop script and webtop tray applets)
- `isDocument` (webtop script and webtop tray applets)
- `isGroup` (webtop script and webtop tray applets)
- `isHierarchyEnabled` (webtop script and webtop tray applets)
- `isLoggedInIn` (framework applet)
- `isOpenGroup` (webtop script and webtop tray applets)
- `isRunning` (webtop script and webtop tray applets)
- `killIterator` (webtop script and webtop tray applets)
- `launchByObjectName` (webtop script and webtop tray applets)

- launchByObjectNumber (webtop script and webtop tray applets)
- login method
- logout method
- openGroup (webtop tray applet)
- openHierarchyLevel (webtop script and webtop tray applets)
- openParentGroup (webtop tray applet)
- receivedEvent (webtop script and webtop tray applets)
- registerProperty (X emulator applet)
- removeValue (framework applet)
- resetNamePassword (login applet)
- scriptStart method
- sendKey (terminal emulator applet)
- setActive (print applet)
- setEnabled (print applet)
- setLaunchWaitTimeOut (webtop script and webtop tray applets)
- setPausedState (print applet)
- setPrinterName (print applet)
- setPrinterPort (print applet)
- setPrinterType (print applet)
- setProperty (X emulator applet)
- setText (terminal emulator applet)
- setUnixTempDir (print applet)
- setWindowsTempDir (print applet)
- suspendApplication (X emulator applet)
- suspendApplication (terminal emulator applet)
- unregisterProperty (X emulator applet)

## Troubleshooting Next section

- For new Secure Global Desktop Administrators
  - A session doesn't end when the user exits the application
  - An application exits immediately after starting
  - An application won't start
  - Troubleshooting CPU/memory-based application server load balancing
- For day-to-day Secure Global Desktop administration
  - An application's animation appears "jumpy"
  - Applications disappear after about two minutes



- Users are unable to copy and paste text or graphics
- Users cannot print from applications displayed through Secure Global Desktop
- Using Windows Terminal Services, users are prompted for usernames and passwords too often
- An "Ambiguous username" dialog is displayed when a user tries to log in
- LDAP users can't log in to Secure Global Desktop
- Solaris OS users are unable to log in when Secure Global Desktop security services are running
- Users are having problems accessing client drives
- Users complain of poor performance with the Windows desktop
- A Kiosk application isn't appearing full-screen
- An application requires a richer set of cursors
- In some X applications, the ALT and ALT GR keys do not work
- Troubleshooting printer preferences and settings
- Troubleshooting sound in Windows applications
- Users are unable to use smart cards with Windows applications
- Users have problems displaying high color X applications
- When Secure Global Desktop printing has been disabled, print jobs can still be queued
- Windows 2000 users are unable to print a file from a mapped network drive
- Running Windows applications on client devices
- Users are unable to relocate their webtop sessions
- Users see window clipping with Client Window Management applications
- With Secure Global Desktop PDF printing, fonts don't print as expected
- For in-depth Secure Global Desktop administration
  - Users experience problems with web server authentication
  - Users are unable to connect to Secure Global Desktop when it is in firewall forwarding mode
  - Users see font problems
  - When X authorization is enabled, applications fail to start
  - All Administrators have been removed and no-one can use the administration tools
  - All login authorities are disabled and no-one can access Secure Global Desktop
  - Every server in the array has been disabled and no-one can access Secure Global Desktop
  - Secure Global Desktop uses too much of my network's bandwidth
- For Secure Global Desktop customizers
  - A login script returns an error

## Frequently asked questions [Back to top](#)

- For new Secure Global Desktop Administrators

- How do I add new Secure Global Desktop Administrators?
- How does Secure Global Desktop use applets?
- What are X.509 certificates and why do I need one?
- What do I need to tell my users?
- Do I need to license Windows Terminal Services?
- What are peer DNS names and external DNS names?
- What is ENS?
- What is an array?
- What is the Tarantella System Objects organization?
- What's in the Secure Global Desktop installation directory?
- Where is Secure Global Desktop installed?
- For day-to-day Secure Global Desktop administration
  - Can users access Secure Global Desktop without Java technology?
  - Does the browser-based webtop use themes?
  - How do I enable sound in Windows applications?
  - What are Secure Global Desktop security services?
  - What is a role object?
  - Why do users see a printer called \_Default in their Windows application?
  - Can I use Secure Global Desktop to access VMS applications?
  - How do I run a Common Desktop Environment (CDE) session?
  - Can I access a web application through Secure Global Desktop?
  - Can I change the name of the printer in the Windows 2000/2003 application session?
- For in-depth Secure Global Desktop administration
  - What certificates does Secure Global Desktop support?
  - Can I run another SMB service with client drive mapping?
  - How can I support users with a client-side firewall that only allows connections on the HTTPS port?
  - How do I tell what connection type a user gets?
  - Can I use an X.509 certificate for another product with Secure Global Desktop?
  - How do I support additional Certificate Authorities?
  - If the array changes, do I have to re-configure printing?
  - What happens when a user's password expires?
  - Can I deny an LDAP user access to Secure Global Desktop?
  - Can I force users to print only to their default client printer?
  - Can I prevent users from launching applications with a different username and password?
  - Can I set a time limit for print jobs?

- Can I use PKI client certificates with web server authentication?
- Can I use SafeWord PremierAccess with web server authentication?
- Can I use other web authentication schemes with Secure Global Desktop web server authentication?
- Do I have to use distributed printing?
- How can I make additional Native Clients available?
- How do I use my own X fonts?
- What X fonts are installed?
- What ports does Secure Global Desktop use?
- Can I chain Certificate Authority certificates?
- Can I use multiple monitors with Secure Global Desktop?
- For Secure Global Desktop customizers
  - What are login scripts?

## Sun Secure Global Desktop Software Administration Guide

- ["Always use smart card" box initial setting attribute \(--launch-alwayssmartcard-initial\)](#)
- ["Always use smart card" box state setting attribute \(--launch--alwayssmartcard-state\)](#)
- ["common name" objects, names](#)
- ["Print to Local PDF File" printer](#)
  - [enable for array](#)
  - [enable for user](#)
- ["Save password" box initial setting attribute \(--launch-savepassword-initial\)](#)
- ["Save password" box state setting attribute \(--launch-savepassword-state\)](#)
- ["Universal PDF" printer](#)
  - [enable for array](#)
  - [enable for user](#)
- [--file option](#)
- [3270 application objects](#)
  - [creating from the command line](#)
  - [overview](#)
- [3270 hosts](#)
- [3270.exp login script](#)
- [5250 application objects](#)
  - [creating from the command line](#)
  - [overview](#)
- [5250.exp login script](#)
- [accounts, guest](#)
- [Active Directory container objects](#)
  - [creating from the command line](#)
  - [overview](#)
- [Active Directory login attribute \(--login-ad\)](#)
- [Active Directory login authority](#)
  - [about](#)
  - [enabling](#)
- [Active Directory users](#)
  - [about](#)

- authenticating
- Directory Services Integration
- **Active Directory**
  - Base Domain attribute (--login-ad-base-domain)
  - Default Domain attribute (--login-ad-default-domain)
  - Directory Services Integration
  - LDAP Server URL attribute (--login-ldap-url)
  - Use Certificates attribute (--login-ldap-pki-enabled)
- **addresses**
  - Address attribute (--address)
  - email
  - network
- **addValue public method (framework applet)**
- **Administrators**
  - adding Secure Global Desktop Administrators
  - Global Administrators role
  - removing all
- **algorithm, emulator session load balancing**
- **Allow delayed updates attribute (--delayed)**
- **Allow smart card authentication attribute (--launch-allowsmartcard)**
- **Always use smart card box, configuring**
- **ambiguous usernames, problems on login**
- **animation problems**
- **anonymous user login authority**
- **anonymous users**
  - about
  - Anonymous user login attribute (--login-anon)
- **ansikey.txt (SCO Console emulator keyboard map)**
- **Answerback Message attribute (--answermsg)**
- **Apache web servers**
  - configuring for Secure Global Desktop
- **applet parameters**
  - client drive mapping (CDM) applet
  - data types
  - framework applet
  - login applet
  - print applet

- terminal emulator applet
- webtop script applet
- webtop tray applet
- X emulator applet
- **applets**
  - about
  - client drive mapping (CDM) applet
  - framework applet
  - including in Secure Global Desktop themes
  - login applet
  - login parameters
  - print applet
  - terminal emulator applet
  - using Java™ archives
  - webtop script applet
  - webtop tray applet
  - X emulator applet
- **application launch**
  - Application Launch Properties panel, Array Manager
  - configuring launch dialog
  - resetting passwords
- **application objects**
  - creating
  - overview
  - publishing to users
- **application problems**
  - animation appears jumpy
  - application doesn't start
  - application exits immediately
- **application servers**
  - authenticating, Windows domain
  - load balancing
  - load balancing, algorithm
  - load balancing, configuration
  - load balancing, default algorithm
  - load balancing, properties
  - load balancing, troubleshooting

- load balancing, tuning
- locations
- network addresses
- remapping/hiding drives
- secure communication with Secure Global Desktop
- server affinity
- UNIX/Linux, printing from
- Windows 2000/2003, printing from
- Windows NT 3.51, printing from
- Windows NT 4, printing from
- Application supports 3-button mouse only attribute (--force3button)
- applications
  - Application Command attribute (--app)
  - Application Key Mode attribute (--appkeymode)
  - color depth
  - color maps
  - color quality
  - display modes
  - enabling sound
  - height
  - key mode
  - launching single
  - launching using JavaScript
  - minutes resumable for
  - resumability settings
  - running locally, problems
  - starting from local devices
  - troubleshooting sound
  - ttawebtop CGI program
  - VMS applications
  - width
- archives.txt (Java™ archives configuration file)
- archiving Secure Global Desktop server log files
- areObjectsInitialized public method (webtop script and webtop tray applets)
- arguments, command-line
- Array Manager
  - about

- Application Launch Properties panel
- Array Properties panel
- Audio Protocol Engine Properties panel
- Channel Protocol Engine Properties panel
- Character Protocol Engine Properties panel
- Emulator Sessions Properties panel
- Execution Protocol Engine Properties panel
- General Properties panel
- Licenses Properties panel
- Load Balancing Properties panel
- Print Protocol Engine Properties panel
- Printing Properties panel
- Secure Global Desktop Login Properties panel
- Security Properties (array-wide) panel
- Security Properties (server-specific) panel
- Smart Card Protocol Engine Properties panel
- starting
- Tuning Properties panel
- X Protocol Engine Properties panel
- Array Properties panel, Array Manager
- arrays
  - about
  - array-wide properties
  - backing-up
  - creating
  - deny Secure Global Desktop login
  - dismantling
  - members, tuning application launch
  - restoring
  - status of sessions
  - tarantella array command
  - tarantella array detach command
  - tarantella array join command
  - tarantella array list command
  - tarantella array make\_primary command
- AS/400 hosts



- attribute maps
  - Attribute Map attribute (--attributemap)
  - terminal emulator
- attributes, object
  - "common name" object
  - 3270 host
  - 3270 port number
  - 5250 port number
  - address
  - answerback message
  - application
  - application key mode
  - application supports 3-button mouse only
  - arguments for command
  - AS/400 host
  - attribute map
  - authentication
  - available to run applications
  - bandwidth limit
  - border style
  - client drive mapping
  - client printers
  - client's maximum size
  - clipboard access
  - clipboard security level
  - code page
  - color
  - color depth
  - color map
  - color quality
  - columns
  - command compression
  - command execution
  - connection method
  - connections
  - cursor
  - cursor keys

- o delayed updates
- o description
- o display using
- o driver name
- o email address
- o emulation type
- o emulator applet page
- o environment variables
- o escape sequences
- o euro character
- o fixed font size
- o font family
- o font size
- o guest accounts
- o height
- o host locale
- o Hosts tab
- o inherit parent's webtop content
- o interlaced images
- o keep launch connection open
- o keyboard map
- o keyboard type (3270)
- o keyboard type (5250)
- o keypad
- o let users print to a PDF local file
- o let users print to a PDF printer
- o lines
- o Links tab
- o load balancing algorithm
- o location
- o locking keymaps
- o login script
- o make PDF file printer the default for Windows 2000/3
- o make PDF printer the default for Windows 2000/3
- o Max Instances
- o maximize emulator window (3270)

- maximize emulator window (5250)
- may log in to Secure Global Desktop
- Members tab
- menu bar enabled/disabled (3270)
- menu bar enabled/disabled (5250)
- menus enabled or disabled (3270)
- menus enabled or disabled (5250)
- middle mouse timeout
- monitor resolution
- name of domain component object
- name of organization object
- name of organizational unit object
- open in new browser window
- preferred locales
- profile editing
- protocol arguments
- resumable
- resumable for
- root window
- scale to fit window
- scroll style
- serial port mapping
- session ends when
- share resources between similar sessions
- shared between users
- soft button levels displayed (3270)
- soft button levels displayed (5250)
- status line
- surname
- telnet close option (3270)
- telnet close option (5250)
- terminal type
- text window background color (3270)
- text window background color (5250)
- text window foreground color (3270)
- text window foreground color (5250)
- try running from client first

- URL
- use graphics acceleration
- use Windows cursor
- user-specific printing configuration
- username
- Webtop Hints
- webtop icon
- webtop theme
- width
- window close action
- Window Manager
- Windows domain
- Windows protocol
- wrap long lines
- Audio Protocol Engine Properties panel, Array Manager
- audio
  - Compression attribute (--audiope-compression)
  - Enable audio service attribute (--array-audio)
  - enabling
  - Sound quality attribute (--array-audio-quality)
  - troubleshooting
- audit
  - using log filters
- Authentication token login attribute (--login-atla)
- authentication token login authority
  - about
- Authentication token login authority
  - enabling
- authentication token users
  - about
- authentication
  - authenticating users on application servers
  - Authentication attribute (--auth)
  - user
  - web server
- authrequest Tcl command, login scripts
- Automatic login

- Available to run applications attribute (--available)
- back-up
  - array
- background color, text window (3270)
- background color, text window (5250)
- bandwidth
  - Bandwidth Limit attribute (--bandwidth)
  - network, problems with
- batch scripts, populating organizational hierarchies using
- billing, enabling
- BootStrapShell applet
- border styles
  - Border Style attribute (--border)
  - terminal window
- browsers
  - opening objects in new windows
- button levels (3270)
- button levels (5250)
- CAB libraries
- caching Java™ archives
- cancelCurrentJob public method (print applet)
- canceltimer Tcl command, login scripts
- CDE application, running
- CDE session, running
- Certificate Authorities
  - chaining certificates
  - installing CA certificates
  - installing root certificates
  - supported
- certificates
  - Certificate Authorities certificates
  - chaining
  - from other products
  - installing
  - obtaining
  - overview
  - PKI client certificates

- root certificates
- sharing Secure Global Desktop server
- tarantella security certinfo command
- tarantella security certrequest command
- tarantella security certuse command
- tarantella security customca command
- tarantella security decryptkey command
- tarantella security peerca command
- user prompts
- X.509
- CGI programs
  - emulator applet parameters
  - ttawebtop
- chaining Certificate Authority certificates
- Channel Protocol Engine Properties panel, Array Manager
- character application objects
  - creating from the command line
  - overview
- Character Protocol Engine
  - Array Manager Properties panel
  - Command-line Arguments attribute (--cpe-args)
- cipher suites
- classroom shadowing
- client devices
  - PKI client certificates
  - secure communication with Secure Global Desktop
- client drive mapping (CDM) applet public methods
  - login
  - logout
  - scriptStart
- client drive mapping (CDM) applet
  - overview
  - parameters
- Client Drive Mapping attribute (--cdm)
- client drive mapping
  - applet

- configuring
- enabling and disabling
- fallback drive
- limitations
- other SMB services
- problems
- remapping/hiding application server drives
- Samba
- setting up
- tarantella start cdm command
- tarantella stop cdm command
- WINS and
- Client printers (--printing-mapprinters)
- Client printers attribute (--mapprinters)
- Client Window Management
  - display mode
  - maximum display height attribute (--xpe-cwm-maxheight)
  - maximum display width attribute (--xpe-cwm-maxwidth)
  - maximum size
- Client's maximum size attribute (--maximize)
- clienttimer Tcl command, login scripts
- clipboard
  - Client security level attribute (--clipboard-clientlevel)
  - Clipboard Access attribute (--clipboard)
  - Clipboard Security Level attribute (--clipboardlevel)
  - Enable copy and paste attribute (--clipboard-enabled)
  - introduction
  - troubleshooting
- close action, window
- closeHierarchyLevel public method (webtop script and webtop tray applets)
- code pages
  - Code Page attribute (--codepage)
  - emulator
- Color depth attribute (--depth)
- color maps
  - application
  - Color Map attribute (--colormap)

- terminal emulator
- Color quality attribute (--quality)
- colors
  - Color attribute (--rootcolor)
  - mapping character attributes to
  - problems displaying
  - root window
  - Text window background color (--3270bg) 3270
  - Text window background color (--bg) 5250
  - text window foreground color (3270)
  - text window foreground color (5250)
- columns
  - Columns attribute (--cols)
  - terminal window
- COM port
  - configuring access to
  - Enable serial port mapping attribute (--array-serialport)
  - Serial Port Mapping attribute (--serialport)
- commands
  - Arguments For Command attribute (--args)
  - Command Compression attribute (--compression)
  - Command Execution attribute (--execution)
  - compressing
  - optimizing
- Common Desktop Environment application, running
- Common Desktop Environment session, running
- Common UNIX Printing System (CUPS)
- connection types
  - Connection Types attribute (--security-connectiontypes)
  - Connection Types: Apply when users log in attribute (--security-applyconnections)
  - discovering for users
- connections
  - applying on log in
  - configuring
  - Connection Method attribute (--method)
  - Connections attribute (--conntype)
  - methods



- secure (departmental users)
- secure (Internet)
- secure (Secure Global Desktop servers)
- types available
- unauthenticated
- container objects
  - creating from the command line
  - overview
- copy and paste
  - Client security level attribute (--clipboard-clientlevel)
  - Clipboard Access attribute (--clipboard)
  - Clipboard Security Level attribute (--clipboardlevel)
  - Enable copy and paste attribute (--clipboard-enabled)
  - introduction
  - troubleshooting
- copyright information
- countJobs public method (print applet)
- CUPS
- cursors
  - Cursor attribute (--cursor)
  - Cursor Keys attribute (--cursorkeys)
  - richer set required
  - styles
- datastore, Secure Global Desktop
- decommissioning Secure Global Desktop servers
- default.printerinfo.txt file
  - \_Default printer
  - UNIX client configuration
  - Windows 2000/2003 printer drivers
- departmental users
- depth, color
- descriptions
  - Description attribute (--description)
  - object
- desktop Start Menu integration
  - introduction
- directory servers

- configuring
- Directory Services Integration
- LDAP Server URL attribute (--login-ldap-url)
- secure (SSL) connections
- Directory Services Integration
  - LDAP groups
  - LDAP search
  - LDAP users
  - using
- displaying applications
  - allowing delayed display updates
  - display modes
  - Display Using attribute (--displayusing)
- distribution units
- DNS names
  - DNS Name attribute (--server-dns-external)
  - peer and external
- document objects
  - creating from the command line
  - overview
- domain component objects
  - creating from the command line
  - names
  - overview
- drive letters, unexpected/missing
- Driver name attribute (--pdfdriver)
- Driver name attribute (--printing-pdfdriver)
- drives, remapping/hiding on application servers
- Email Address attribute (--email)
- Emulation Type attribute (--emulator)
- emulator sessions
  - classroom shadowing
  - controlling
  - displaying information about
  - Emulator Sessions Properties panel, Array Manager
  - ending (command-line)
  - ending (object configuration)

- introduction
- listing
- load balancing
- load balancing algorithm
- Load Balancing Properties panel, Array Manager
- properties, Array Manager
- shadowing
- shadowing example
- sharing resources between
- suspending
- tarantella emulatorsession command
- tarantella emulatorsession end command
- tarantella emulatorsession info command
- tarantella emulatorsession list command
- tarantella emulatorsession shadow command
- tarantella emulatorsession suspend command
- emulator windows
  - maximizing (3270)
  - maximizing (5250)
- emulators
  - code pages
  - emulation types
  - Emulator Applet Page attribute (--empage)
- Enable billing services attribute (--array-billingservices)
- Enable resource synchronization attribute (--array-resourcesync)
- Enable X Security Extension (--securityextension)
- Encryption key, password cache
- ENS (Enterprise Naming System)
  - about
  - ENS login attribute (--login-ens)
- ENS login authority
- ENS users
- Environment Variables attribute (--env)
- error messages returned by login scripts
- Escape Sequences attribute (--escape)
- essential information for users
- euro character

- Euro Character attribute (--euro)
- using with 3270 character applications
- using with character applications
- using with SCO Console applications
- Execution Protocol Engine
  - Command-line Arguments attribute (--execpe-args)
  - Properties panel, Array Manager
- external authentication
  - classic web server authentication
  - third party authentication
- external DNS names
  - about
  - configuring
- Fallback Drive attribute (--array-cdm-fallbackdrive)
- File Descriptors attribute (--tuning-maxfiledescriptors)
- Firewall Forwarding URL attribute ( --security-firewallurl)
- firewalls
  - configuring
  - connection problems with firewall forwarding
  - DNS names
  - forwarding URL
  - traversing, client
  - using the HTTPS port for Secure Global Desktop connections
- Fixed font size attribute (--fixedfont)
- font paths
  - adding fonts
  - Font Path attribute (--xpe-fontpath)
- fonts
  - adding, X
  - fixed font size
  - Font Family attribute (--font)
  - font servers
  - Font Size attribute (--fontsize)
  - fonts.alias file
  - fonts.dir file
  - installed, X

- problems
- foreground color, text window (3270)
- foreground color, text window (5250)
- framework applet public methods
  - addValue
  - getUsername
  - getValue
  - getWebtopFramesetURL
  - getWebtopURL
  - isLoggedIn
  - login
  - logout
  - removeValue
  - scriptStart
- framework applet
  - about
  - parameters
- full-screen display mode
- General Properties panel, Array Manager
- Generate authentication tokens attribute (--login-autotoken)
- getActive public method (print applet)
- getApplicationType public method (webtop script and webtop tray applets)
- getCurrentIteratorElement public method (webtop script and webtop tray applets)
- getEmulatorState public method (terminal emulator applet)
- getEmulatorState public method (X emulator applet)
- getEnabled public method (print applet)
- getIteratorForAllOpenHierarchyLevels public method (webtop script and webtop tray applets)
- getIteratorForHierarchyLevel public method (webtop script and webtop tray applets)
- getIteratorHasMoreElements public method (webtop script and webtop tray applets)
- getLaunchWaitTimeOut public method (webtop script and webtop tray applets)
- getNextIteratorElement public method (webtop script and webtop tray applets)
- getNumberOfObjects public method (webtop script and webtop tray applets)
- getNumberOfObjectsInGroup public method (webtop script and webtop tray applets)
- getObjectClass public method (webtop script and webtop tray applets)
- getObjectDisplayName public method (webtop script and webtop tray applets)
- getObjectDisplayNameByName public method (webtop script and webtop tray applets)
- getObjectFullName public method (webtop script and webtop tray applets)

- getObjectImageNameByName public method (webtop script and webtop tray applets)
- getName public method (webtop script and webtop tray applets)
- getObjectPlacement public method (webtop script and webtop tray applets)
- getParentGroupName public method (webtop script and webtop tray applets)
- getPrinterName public method (print applet)
- getPrinterPort public method (print applet)
- getPrinterType public method (print applet)
- getPrintState public method (print applet)
- getProperty public method (X emulator applet)
- getText public method (terminal emulator applet)
- getTotalNumberOfObjects public method (webtop script and webtop tray applets)
- getUnixTempDir public method (print applet)
- getUsername public method (framework applet)
- getValue public method (framework applet)
- getWebtopFramesetURL public method (framework applet)
- getWebtopURL public method (framework applet)
- getWindowsTempDir public method (print applet)
- Ghostscript
- Global Administrators role object
- graphics acceleration, using
- group objects
  - creating from the command line
  - members
  - overview
- guest accounts
- guest users
- Height attribute (--height)
- height, application
- hierarchies
  - populating organizational
- host objects
  - creating from the command line
  - overview
- hosts
  - 3270 Host attribute (--hostname)
  - AS/400 Host attribute (--hostname)
  - available for application launch

- Hosts tab attribute (--appserv)
- HTTP proxy servers
  - client configuration
  - supported
  - using with Secure Global Desktop
- If Launch Fails attribute (--launch-details-showonerror)
- If Password Has Expired attribute (--launch-expiredpassword)
- If SSL Daemon Doesn't Start attribute (--security-ssldaemon-failmode)
- Independent Window display mode
- Inherit parent's webtop content attribute (--inherit)
- install.cgi
- installation directory
  - backing up
  - contents
  - location
  - restoring
- intelligent array routing
  - application server
  - Secure Global Desktop server
- Interlaced Images attribute (--interlaced)
- Internet connections
- IP filtering
- isApplication public method (webtop script and webtop tray applets)
- isDocument public method (webtop script and webtop tray applets)
- isGroup public method (webtop script and webtop tray applets)
- isHierarchyEnabled public method (webtop script and webtop tray applets)
- isLoggedIn public method (framework applet)
- isOpenGroup public method (webtop script and webtop tray applets)
- isRunning public method (webtop script and webtop tray applets)
- JavaScript, launching applications using
- Java™ archives
  - about
  - CAB libraries
  - caching
  - configuration file (archives.txt)
  - removing

- signed
  - zips
- Java™ Virtual Machine
  - settings
- Keep launch connection open attribute (--keepopen)
- keepalives, changing
- Kerberos authentication
  - configuring
- key files
  - decrypting for use with certificates
  - tarantella security decryptkey command
- Keyboard Map attribute (--keymap)
- Keyboard Map attribute (--xpe-keymap)
- keyboard mapping
  - locking keymaps
  - map files, application-specific
  - map files, default
  - terminal emulator
- keyboard types (3270)
- keyboard types (5250)
- Keypad attribute (--keypad)
- killIterator public method (webtop script and webtop tray applets)
- Kiosk
  - application not appearing full screen
  - display mode
- Launch Details initial setting attribute (--launch-details-initial)
- Launch Details state setting attribute (--launch-details-state)
- Launch Dialog attribute (--launch-showdialogafter)
- launchByObjectName public method (webtop script and webtop tray applets)
- launchByObjectNumber public method (webtop script and webtop tray applets)
- launching applications
  - increasing launch timeouts
  - keeping connections open
  - Launch Details attribute authentication dialog setting (--launch-details-display)
  - Launch Details attribute initial setting (--launch-details-initial)
  - Launch Details attribute state setting (--launch-details-state)
  - Launch Dialog attribute (--launch-showdialogafter)



- launching single
  - using JavaScript
- LDAP login attribute (--login-ldap)
- LDAP login authority
  - about
  - enabling
- LDAP servers
  - configuring
  - Directory Services Integration
  - LDAP Server URL attribute (--login-ldap-url)
  - secure (SSL) connections
- LDAP users
  - authenticating
  - denying login
  - Directory Services Integration
  - login problems
  - webtops
- Idaps transport
- legal information
- Let users access client drives attribute (--array-cdm)
- Let users print to a PDF local file attribute (--pdfviewerenabled)
- Let users print to a PDF local file attribute (--printing-pdfviewerenabled)
- Let users print to a PDF printer attribute (--pdfenabled)
- Let users print to a PDF printer attribute (--printing-pdfenabled)
- licensing
  - about
  - commands for Windows Terminal Services CALs
  - free Windows Terminal Services CALs
  - Licenses Properties panel, Array Manager
  - list Windows Terminal Services CALs
  - return Windows Terminal Services CALs
  - tarantella license add command
  - tarantella license command
  - tarantella license info command
  - tarantella license list command
  - tarantella license query command
  - tarantella license remove command

- tarantella license status command
  - Windows Terminal Services
- limitations, client drive mapping
- limiting bandwidth
- Lines (--lines) attribute
- links, webtop
  - Links tab attribute (--links)
  - tarantella role add\_link command
  - tarantella role list\_links command
  - tarantella role remove\_link command
- Load Balancing Algorithm attribute (--loadbal)
- load balancing
  - application server, algorithm
  - application server, configuration
  - application server, default algorithm
  - application server, properties
  - application server, troubleshooting
  - application server, tuning
  - application servers
  - emulator sessions
  - emulator sessions algorithm
  - server affinity
  - webtop sessions
- local devices, starting applications from
- locales, preferred
- locallaunch Tcl command, login scripts
- location
  - application server
  - Location attribute (--location)
  - Location attribute (--server-location)
  - Secure Global Desktop server
- Lock keymap attribute (--lockkeymap)
- log files
  - archiving
  - configuring
  - displaying billing information
  - displaying component error logs

- displaying filtered log entries
- displaying uptime for array members
- examining
- for auditing
- Log Directory attribute (--server-logdir)
- Log Filter attribute (--array-logfilter)
- using syslog
- log filters
  - configuring
  - for auditing
- logging in using person objects
- login applet
  - overview
  - parameters
  - public method (resetNamePassword)
- login authorities
  - about
  - Active Directory login authority
  - all disabled
  - anonymous user login authority
  - authentication token login authority
  - configuring
  - ENS login authority
  - LDAP login authority
  - NT login authority
  - SecurID login authority
  - UNIX group login authority
  - UNIX user login authority
- login denied
  - after failed login attempts
- login problems, ambiguous usernames
- login profiles
- login public method
- login scripts
  - error messages
  - Login Script attribute (--login)

- Login Script Directory attribute (--execpe-scriptdir)
- overview
- script variables
- supplied with Secure Global Desktop
- tarantella Tcl command
- Tcl commands
- Login Theme attribute (--login-theme)
- login
  - denying LDAP users
- LoginApp applet
- logout public method
- long lines, wrapping
- Make PDF file printer the default for Windows 2000/3 attribute (--pdfviewerisdefault)
- Make PDF file printer the default for Windows 2000/3 attribute (--printing-pdfviewerisdefault)
- Make PDF printer the default for Windows 2000/3 attribute (--pdfisdefault)
- Make PDF printer the default for Windows 2000/3 attribute (--printing-pdfisdefault)
- Max Instances (--maxinstances)
- maximize emulator window attribute (3270)
- maximize emulator window attribute (5250)
- maximum size of client
- May log in to Secure Global Desktop attribute (--enabled)
- Members tab attribute (--member)
- menu bar enabled/disabled (3270)
- menu bar enabled/disabled (5250)
- menus enabled/disabled (3270)
- menus enabled/disabled (5250)
- messages, answerback
- Middle Mouse Timeout attribute (--middlemouse)
- monitor resolution
  - application-specific
  - default
  - Monitor Resolution attribute (--dpi)
  - Monitor Resolution attribute (--xpe-monitorresolution)
- monitor
  - using multiple
- Name attribute
  - "common name" objects

- domain component objects
- organization objects
- organizational unit objects
- **names**
  - "common name" objects
  - 3270 hosts
  - AS/400 hosts
  - domain component objects
  - expiring name mappings
  - external DNS
  - listing name mappings
  - organization objects
  - organizational unit objects
  - peer DNS
- **Native Client**
  - command-line options
  - customizing appearance, UNIX
  - making available for download
  - proxy server support
  - user preferences file
  - where to download
- **Netscape web servers**
  - configuring for Secure Global Desktop
- **network addresses for application servers, specifying**
- **network bandwidth, problems with**
- **no files shown, client drive mapping**
- **NT login attribute (--login-nt)**
- **NT login authority**
  - about
  - enabling
- **NT users**
- **numeric keypads**
- **object attributes**
  - "common name" object
  - 3270 host
  - 3270 port number
  - 5250 port number

- address
- answerback message
- application
- application key mode
- application supports 3-button mouse only
- arguments for command
- AS/400 host
- attribute map
- authentication
- available to run applications
- bandwidth limit
- border style
- client drive mapping
- client printers
- client's maximum size
- clipboard access
- clipboard security level
- code page
- color
- color depth
- color map
- color quality
- columns
- command compression
- command execution
- connection method
- connections
- cursor
- cursor keys
- delayed updates
- description
- display using
- driver name
- email address
- emulation type
- emulator applet page

- environment variables
- escape sequences
- euro character
- fixed font size
- font family
- font size
- guest accounts
- height
- host locale
- Hosts tab
- inherit parent's webtop content
- interlaced images
- keep launch connection open
- keyboard map
- keypad
- let users print to a PDF local file
- let users print to a PDF printer
- lines
- Links tab
- load balancing algorithm
- location
- locking keymaps
- login script
- make PDF file printer the default for Windows 2000/3
- make PDF printer the default for Windows 2000/3
- Max Instances (--maxinstances)
- may log in to Secure Global Desktop
- Members tab
- middle mouse timeout
- monitor resolution
- name of domain component object
- name of organization object
- name of organizational unit object
- open in new browser window
- preferred locales
- profile editing
- protocol arguments

- resumable
- resumable for
- root window
- scale to fit window
- scroll style
- serial port mapping
- session ends when
- share resources between similar sessions
- shared between users
- status line
- surname
- terminal type
- try running from client first
- URL
- use graphics acceleration
- use Windows cursor
- user-specific printing configuration
- username
- Webtop Hints (--hints)
- webtop icon
- webtop theme
- width
- window close action
- Window Manager
- Windows NT domain
- Windows protocol
- wrap long lines
- object command, tarantella
- Object Manager
  - about
  - starting from the command line
- objects
  - 3270 application
  - 5250 character application
  - Active Directory container
  - advice on naming



- character application
- descriptions
- document
- domain component
- group, overview
- host
- organization
- organizational unit
- overview
- person
- TFN names
- Windows application
- X application
- Open in new browser window attribute (--newbrowser)
- openGroup public method (webtop tray applet)
- openHierarchyLevel public method (webtop script and webtop tray applets)
- openParentGroup public method (webtop tray applet)
- organization objects
  - creating from the command line
  - names
  - overview
- organizational hierarchies
  - overview
  - populating
- organizational unit objects
  - creating from the command line
  - overview
- pages, emulator applet
- panels, Array Manager
  - Application Launch Properties (array)
  - Array Properties (array-wide)
  - Audio Protocol Engine Properties
  - Channel Protocol Engine Properties
  - Character Protocol Engine Properties (server)
  - Emulator Sessions Properties (array)
  - Execution Protocol Engine Properties (server)
  - General Properties (server)

- Licenses Properties (array)
- Load Balancing Properties (array)
- Print Protocol Engine Properties
- Printing Properties (array-wide)
- Secure Global Desktop Login Properties (array)
- Security Properties (array-wide)
- Security Properties (server-specific)
- Smart Card Protocol Engine Properties
- Tuning Properties (server)
- X Protocol Engine Properties (server)
- password problems, users prompted too often
- passwords
  - caching Secure Global Desktop passwords
  - handling password expiry
  - Password Cache: Generate new encryption key on restart attribute (--security-newkeyonrestart)
  - resetting on application launch
  - trying Secure Global Desktop passwords
- PDF printing
  - array properties
  - configuring
  - troubleshooting font problems
- peer DNS names
- person objects
  - creating and configuring
  - creating from the command line
  - logging in using
  - overview
  - sharing between users
  - surnames
- populating organizational hierarchies
- port numbers
  - 3270 Port Number attribute (--portnumber)
  - 5250 Port Number attribute (--portnumber)
  - Port Numbers (connections between array members) attribute (--array-port-peer)
  - Port Numbers (encrypted connections) attribute (--array-port-encrypted)
  - Port Numbers (unencrypted connections) attribute (--array-port-unencrypted)

- ports
  - 3270 TCP number
  - 5250 TCP number
  - client firewalls
  - connections between Secure Global Desktop servers
  - encrypted connections
  - unencrypted connections
  - used by Secure Global Desktop
  - using the HTTPS port for Secure Global Desktop connections
- Preferred Locale attribute (--preflocale)
- primary servers
- print applet public methods
  - cancelCurrentJob
  - countJobs
  - getActive
  - getEnabled
  - getPrinterName
  - getPrinterPort
  - getPrinterType
  - getPrintState
  - getUnixTempDir
  - getWindowsTempDir
  - login
  - logout
  - scriptStart
  - setActive
  - setEnabled
  - setPausedState
  - setPrinterName
  - setPrinterPort
  - setPrinterType
  - setUnixTempDir
  - setWindowsTempDir
- print applet
  - overview
  - parameters
- Print Name Mappings: Expire after attribute (--security-printmappings-timeout)

- Print Protocol Engine Properties panel, Array Manager
- print queue
  - disabling
- print status information, displaying
- Print to Local PDF File printer
  - configuring
- printer types, default
- printer
  - `_Default printer`
  - configuration on UNIX/Linux application servers
  - configuration on Windows 2000/2003 application servers
  - configuration on Windows NT 3.51 application servers
  - configuration on Windows NT 4 application servers
  - drivers for Windows 2000/2003
  - preferences for Windows 2000/2003
  - preferences, troubleshooting
  - printer name in Windows 2000/2003 session
  - settings, troubleshooting
  - UNIX clients, drivers for Windows 2000/2003
  - UNIX configuration script
- `printernamemap.txt` file
- `printertypes.txt` file
- Printing Properties panel, Array Manager
- printing
  - `_Default printer`
  - administering services across arrays
  - array change, configuration
  - array-wide PDF printing properties
  - Common UNIX Printing System (CUPS)
  - configuration summary
  - disabling print queue
  - distributed printing
  - drivers, for UNIX client devices
  - introduction
  - mapped network drive problems
  - multiple printer support
  - name mappings, expiring

- name mappings, listing
- print applet
- print job conversion
- print job formats
- print job lifetime
- remote print request
- Secure Global Desktop PDF printing
- tarantella print command
- to client default printer only
- troubleshooting
- UNIX client configuration
- UNIX/Linux application servers
- using only primary server
- Windows 2000/2003 application servers
- Windows 2000/2003 printer drivers
- Windows NT 3.51 application servers
- Windows NT 4 application servers
- **problems**
  - ambiguous usernames on login
  - animation appears jumpy
  - application doesn't start
  - application exits immediately
  - application requires richer set of cursors
  - client drive mapping
  - Kiosk application not appearing full screen
  - running applications locally
  - Secure Global Desktop uses too much network bandwidth
  - session doesn't end when user exits
  - window clipping
- **Process Tuning (Channel Protocol Engine)**
  - Exit after attribute (--cdmpe-exitafter)
- **Process Tuning (Character Protocol Engine)**
  - Exit after attribute (--cpe-exitafter)
  - Maximum sessions per engine attribute (--cpe-maxsessions)
  - Maximum users per engine attribute (--cpe-maxusers)
- **Process Tuning (Execution Protocol Engine)**

- Exit after attribute (--execpe-exitafter)
- Maximum sessions per engine attribute (--execpe-maxsessions)
- Maximum users per engine attribute (--execpe-maxusers)
- Process Tuning (Print Protocol Engine)
  - Exit after attribute (--ppe-exitafter)
- Process Tuning (X Protocol Engine)
  - Exit after attribute (--xpe-exitafter)
  - Maximum sessions per engine attribute (--xpe-maxsessions)
  - Maximum users per engine attribute (--xpe-maxusers)
- Processing Limits: Maximum simultaneous connections attribute (--tuning-maxconnections)
- Processing Limits: Maximum simultaneous requests attribute (--tuning-maxrequests)
- procs.exp login script
- profile
  - Enable user profile editing attribute (--array-editprofile)
  - Profile Editing attribute (--editprofile)
  - Sun Secure Global Desktop Client configuration settings
- progress Tcl command, login scripts
- Proprietary Rights Notice
- Protocol Arguments attribute (--protoargs)
- proxy servers
  - classic webtop configuration check
  - exception lists
  - Native Client settings
  - supported
  - timeouts
  - using with Secure Global Desktop
  - web client settings
- public methods
  - addValue (framework applet)
  - areObjectsInitialized (webtop script and webtop tray applets)
  - cancelCurrentJob (print applet)
  - closeHierarchyLevel (webtop script and webtop tray applets)
  - countJobs (print applet)
  - getActive (print applet)
  - getApplicationType (webtop script and webtop tray applets)
  - getCurrentIteratorElement (webtop script and webtop tray applets)
  - getEmulatorState (terminal emulator applet)

- getEmulatorState (X emulator applet)
- getEnabled (print applet)
- getIteratorForAllOpenHierarchyLevels (webtop script and webtop tray applets)
- getIteratorForHierarchyLevel (webtop script and webtop tray applets)
- getIteratorHasMoreElements (webtop script and webtop tray applets)
- getLaunchWaitTimeOut (webtop script and webtop tray applets)
- getNextIteratorElement (webtop script and webtop tray applets)
- getNumberOfObjects (webtop script and webtop tray applets)
- getNumberOfObjectsInGroup (webtop script and webtop tray applets)
- getObjectClass (webtop script and webtop tray applets)
- getObjectDisplayName (webtop script and webtop tray applets)
- getObjectDisplayNameByName (webtop script and webtop tray applets)
- getObjectFullName (webtop script and webtop tray applets)
- getObjectImageNameByName (webtop script and webtop tray applets)
- getObjectImageName (webtop script and webtop tray applets)
- getObjectPlacement (webtop script and webtop tray applets)
- getParentGroupName (webtop script and webtop tray applets)
- getPrinterName (print applet)
- getPrinterPort (print applet)
- getPrinterType (print applet)
- getPrintState (print applet)
- getProperty (X emulator applet)
- getText (terminal emulator applet)
- getTotalNumberOfObjects (webtop script and webtop tray applets)
- getUnixTempDir (print applet)
- getUsername (framework applet)
- getValue (framework applet)
- getWebtopFramesetURL (framework applet)
- getWebtopURL (framework applet)
- getWindowsTempDir (print applet)
- isApplication (webtop script and webtop tray applets)
- isDocument (webtop script and webtop tray applets)
- isGroup (webtop script and webtop tray applets)
- isHierarchyEnabled (webtop script and webtop tray applets)
- isLoggedIn (framework applet)
- isOpenGroup (webtop script and webtop tray applets)
- isRunning (webtop script and webtop tray applets)

- killIterator (webtop script and webtop tray applets)
- launchByObjectName (webtop script and webtop tray applets)
- launchByObjectNumber (webtop script and webtop tray applets)
- login method
- logout method
- openGroup (webtop tray applet)
- openHierarchyLevel (webtop script and webtop tray applets)
- openParentGroup (webtop tray applet)
- receivedEvent (webtop script and webtop tray applets)
- registerProperty (X emulator applet)
- removeValue (framework applet)
- resetNamePassword (login applet)
- scriptStart
- sendKey (terminal emulator applet)
- setActive (print applet)
- setEnabled (print applet)
- setLaunchWaitTimeOut (webtop script and webtop tray applets)
- setPausedState (print applet)
- setPrinterName (print applet)
- setPrinterPort (print applet)
- setPrinterType (print applet)
- setProperty (X emulator applet)
- setText (terminal emulator applet)
- setUnixTempDir (print applet)
- setWindowsTempDir (print applet)
- suspendApplication (terminal emulator applet)
- suspendApplication (X emulator applet)
- unregisterProperty (X emulator applet)
- publishing application objects to users
- quality, color
- query string arguments, ttawebtop CGI program
- receivedEvent public method (webtop script and webtop tray applets)
- Recycle Bin problems, client drive mapping
- Redirection URL attribute (--server-redirecturl)
- registerProperty public method (X emulator applet)
- removeValue public method (framework applet)



- `resetNamePassword` public method (login applet)
- resource synchronization
  - enabling
  - Resource Synchronization attribute (`--tuning-resourcesync-time`)
  - scheduling
- resources, sharing between emulator sessions
- restarting Secure Global Desktop
- restore
  - array
- Resumable For attribute (`--resumetimeout`)
- resuming applications
  - application settings
  - configuring timeouts
  - emulator sessions
  - Resumability Timeout: Always attribute (`--sessions-timeout-always`)
  - Resumability Timeout: webtop session attribute (`--sessions-timeout-session`)
  - Resumable attribute (`--resumable`)
- RGB Database attribute (`--xpe-rgbdatabase`)
- role objects
  - about
  - Global Administrator
  - `tarantella role add_link` command
  - `tarantella role add_member` command
  - `tarantella role` command
  - `tarantella role list` command
  - `tarantella role list_links` command
  - `tarantella role list_members` command
  - `tarantella role remove_link` command
  - `tarantella role remove_member` command
- roles, about
- root certificates
  - chaining
  - installing
  - supported
  - user prompts
- root windows
  - appearance

- color
  - Root Window attribute (--roottype)
- SafeWord® PremierAccess™
- Save password box, configuring
- Save Secure Global Desktop login details in cache attribute (--launch-savettapassword)
- Scale to fit window attribute (--scalable)
- SCO Console emulator keyboard map
- **scripts**
  - login scripts supplied with Secure Global Desktop
  - populating organizational hierarchies using
  - prtinstall.en.sh
  - tta\_print\_converter
- scriptStart public method
- Scroll Style attribute (--scrollstyle)
- seamless window mode
- **seamless windows**
  - Gnome 2.0.0 Desktop problem
  - using
- secondary servers
- **Secure (SSL) proxy servers**
  - client configuration
  - supported
  - using with Secure Global Desktop
- **secure connections**
  - availability
  - between Secure Global Desktop servers
  - cipher suites
  - configuring
  - departmental users
  - Internet
  - LDAP directory servers
  - Secure Global Desktop servers
  - tuning
- **Secure Global Desktop Administrators**
  - adding
  - fallback
  - Global Administrators role

- removing all
- Secure Global Desktop applets, about
- Secure Global Desktop datastore
- Secure Global Desktop Login attribute (--server-login)
- Secure Global Desktop Login Properties panel, Array Manager
- Secure Global Desktop organizational hierarchies, populating
- Secure Global Desktop security services
  - about
  - certificate prompts
  - sharing web server and Secure Global Desktop server certificates
  - supported certificates
  - X.509 certificates
- Secure Global Desktop servers
  - archiving log files
  - improving security between client devices and Secure Global Desktop servers
  - improving security between Secure Global Desktop servers and application servers
  - secure connections to
  - sharing web server and Secure Global Desktop server certificates
- Secure Global Desktop themes, including applets in
- Secure Global Desktop Web Server
  - about
  - sharing Secure Global Desktop server certificates
- Secure Global Desktop
  - introduction
- secure intra-array communication
- SecurID login attribute (--login-securid)
- SecurID login authority
  - about
  - enabling
- SecurID users
- SecurID
  - application server authentication
  - Secure Global Desktop authentication
- Security Properties (array-wide) panel, Array Manager
- Security Properties (server-specific) panel, Array Manager
- security
  - about security

- array-wide properties
- getting started
- improving security between client devices and Secure Global Desktop servers
- improving security between Secure Global Desktop servers and application servers
- login problem on Solaris OS
- server-specific properties
- tarantella security certinfo command
- tarantella security certrequest command
- tarantella security certuse command
- tarantella security command
- tarantella security customca command
- tarantella security decryptkey command
- tarantella security fingerprint command
- tarantella security peerca command
- tarantella security start command
- tarantella security stop command
- web services
- sendKey public method (terminal emulator applet)
- **serial port**
  - configuring access to
  - Enable serial port mapping attribute (--array-serialport)
  - Serial Port Mapping attribute (--serialport)
- server affinity
- Server JVM Size initial amount attribute (--tuning-jvm-initial)
- Server JVM Size maximum amount (--tuning-jvm-max attribute)
- Server JVM Size scaling factor attribute (--tuning-jvm-scale)
- server security
- **servers**
  - application launch
  - general settings
  - security settings
  - sharing Secure Global Desktop server certificates
  - tuning graphical emulator processes
  - tuning printing processes
  - tuning Secure Global Desktop channel processes
  - tuning terminal emulator processes
  - tuning the Secure Global Desktop server

- Session Ends When attribute (--endswhen)
- session IDs
  - emulator sessions
- Session Start Timeout attribute (--xpe-sessionstarttimeout)
- sessions
  - classroom shadowing
  - ending (command-line)
  - ending (object configuration)
  - problems with
  - shadowing
  - shadowing example
- setActive public method (print applet)
- setbuffer Tcl command, login scripts
- setEnabled public method (print applet)
- setLaunchWaitTimeOut public method (webtop script and webtop tray applets)
- setPausedState public method (print applet)
- setPrinterName public method (print applet)
- setPrinterPort public method (print applet)
- setPrinterType public method (print applet)
- setProperty public method (X emulator applet)
- setText public method (terminal emulator applet)
- setUnixTempDir public method (print applet)
- setWindowsTempDir public method (print applet)
- shadowing emulator sessions
- Share resources between similar sessions attribute (--share)
- shared accounts
- Shared between users (guest) attribute (--shared)
- sharing person objects between users
- Show Authentication Dialog attribute (--launch-showauthdialog)
- Show Launch Details box, configuring
- signed Java™ archives
- Smart Card Protocol Engine Properties panel, Array Manager
- smart card
  - application server authentication dialog settings
  - Compression attribute (--scardpe-compression)
  - Enable smart card service attribute (--array-scard)

- enabling
  - troubleshooting
- SmartIconHost applet
- SOCKS proxy servers
  - client configuration
  - supported
  - using with Secure Global Desktop
- soft button levels displayed (3270)
- soft button levels displayed (5250)
- sound
  - enabling
  - troubleshooting
- SSH (Secure SHell)
  - enabling
  - installing
  - using with Secure Global Desktop
  - X Security Extension
- SSL accelerators
- SSL connections
  - availability
  - between Secure Global Desktop servers
  - cipher suites
  - configuring
  - LDAP directory servers
  - tuning
- SSL Daemon
- standalone servers
- starting applications from local devices
- starting Secure Global Desktop
- Status Line attribute (--statusline)
- status line styles
- status of array sessions
- stopping Secure Global Desktop
- Sun Secure Global Desktop Client
- Sun Secure Global Desktop Client
  - about
  - command line for

- configuring Integrated mode
- desktop Start Menu integration
- Enable user profile editing attribute (--array-editprofile)
- Profile Editing attribute (--editprofile)
- profile settings
- proxy server support
- Sun Secure Global Desktop Native Client
  - command-line options
  - customizing appearance, UNIX
  - making available for download
  - proxy server support
  - user preferences file
  - where to download
- Surname attribute (--surname)
- surnames, person objects
- suspendApplication public method (terminal emulator applet)
- suspendApplication public method (X emulator applet)
- suspending emulator sessions
- syslog
  - logging to
- System Objects organization, about
- tarantella array command
  - detach
  - join
  - list
  - make\_primary
  - overview
- tarantella cache command
- tarantella command
  - archive
  - arraymanager
  - help
  - objectmanager
  - overview
  - restart
  - setup
  - start

- status
- uninstall
- version
- tarantella config command
  - edit
  - list
  - overview
- tarantella emulatorsession command
  - end
  - info
  - list
  - overview
  - shadow
  - suspend
- Tarantella Federated Naming (TFN), introduction
- tarantella license command
  - add
  - info
  - list
  - overview
  - query
  - remove
  - status
- tarantella object command
  - add\_host
  - add\_link
  - add\_member
  - delete
  - edit
  - list\_attributes
  - list\_contents
  - new\_3270app
  - new\_5250charapp
  - new\_charapp
  - new\_container
  - new\_dc
  - new\_doc



- new\_group
- new\_host
- new\_org
- new\_orgunit
- new\_person
- new\_windowsapp
- new\_xapp
- overview
- remove\_host
- remove\_link
- remove\_member
- rename
- script
- tarantella passcache command
  - delete
  - edit
  - list
  - new
  - overview
- tarantella print command
  - cancel
  - list
  - move
  - overview
  - pause
  - resume
  - start
  - status
  - stop
- tarantella query command
  - audit
  - billing
  - errlog
  - overview
  - uptime
- tarantella role command

- add\_link
- add\_member
- list
- list\_links
- list\_members
- overview
- remove\_link
- remove\_member
- tarantella security command
  - certinfo
  - certrequest
  - certuse
  - customca
  - decryptkey
  - fingerprint
  - overview
  - peerca
  - start
  - stop
- tarantella start cdm command
- Tarantella System Objects organization, about
- tarantella tokencache command
  - delete
  - list
  - overview
- tarantella tscal command
  - free
  - list
  - overview
  - return
- tarantella webserver command
  - add\_trusted\_user
  - delete\_trusted\_user
  - list\_trusted\_users
  - overview
  - restart
  - start

- stop
- tarantella webtopsession command
  - list
  - logout
  - overview
- tarantellastop cdm command
- Tcl commands
- TCP ports
  - 3270 port number
  - 5250 port number
  - used by Secure Global Desktop
- TDE applet
- Telnet close option (--3270tnclose) 3270
- Telnet close option (--tnclose) 5250
- terminal emulator applet public methods
  - getEmulatorState
  - getText
  - login
  - logout
  - scriptStart
  - sendKey
  - setText
  - suspendApplication
- terminal emulator applet
  - overview
  - parameters
- terminal emulator
  - attribute maps
  - color maps
  - keyboard maps
- Terminal Type attribute (--termtype)
- terminal windows
  - border styles
  - columns
  - lines
  - scale to fit window
  - scrolling style

- text window
  - background color (3270)
  - background color (5250)
  - foreground color (3270)
  - foreground color (5250)
- TFN (Tarantella Federated Naming), introduction
- themes
  - browser-based webtop
  - login
  - webtop
- third party authentication
- third party authentication
  - trusted users
- third party users
  - about
  - Directory Services Integration
  - webtops
- three-tier architecture, about
- timeouts
  - launch, increasing
  - resumability
  - session start
- TLS connections
  - between Secure Global Desktop servers
  - cipher suites
  - tuning
- trademark information
- trusted users
- Try running from client first attribute (--trylocal)
- Try Secure Global Desktop password if cached attribute (--launch-trycachedpassword)
- TTAAPPLET tag
- ttawebtop CGI program
  - query string arguments
  - running applications
- Tuning Properties panel, Array Manager
- tuning
  - application launch, array members

- graphical emulator processes, array members
- printing processes, array members
- Secure Global Desktop channel processes
- Secure Global Desktop servers
- terminal emulator processes, array members
- **UDP ports**
  - used by Secure Global Desktop
- **UIDs (usernames)**
- **uninstalling Secure Global Desktop**
- **Universal PDF printer**
  - configuring
- **UNIX group login attribute (--login-unix-group)**
- **UNIX group login authority**
- **UNIX groups**
- **UNIX user login attribute (--login-unix-user)**
- **UNIX user login authority**
- **UNIX users**
- **unix.exp login script**
- **unixwin.exp login script**
- **unregisterProperty public method (X emulator applet)**
- **URL (--url) attribute**
- **URLs, object**
- **Use graphics acceleration attribute (--accel)**
- **Use Windows cursor attribute (--wincursor)**
- **Use WINS for better performance attribute (--array-cdm-wins)**
- **user authentication**
- **user identity mapping**
- **user types**
  - Active Directory users
  - anonymous users
  - authentication token users
  - ENS users
  - guest users
  - LDAP users
  - NT users
  - SecurID users
  - shared users

- UNIX groups
- UNIX users
- web users
- User-specific printing configuration attribute (--userprintingconfig)
- Username attribute (--user)
- usernames, login problems
- users
  - authenticating
  - authenticating on application servers
  - connection types
  - essential information
  - secure connections
  - TFN names
- variables
  - environment
  - login script
- version numbers, displaying
- VMS applications
- vt420key.txt (VT420 emulator keyboard map)
- w60key.txt (Wyse 60 emulator keyboard map)
- wcpwts.exp login script
- web applications
- web browsers
  - Java™ archives
- web server authentication
  - about
  - configuring for browser-based webtop
  - configuring for classic webtop
  - Directory Services Integration
  - introducing
  - PKI client certificates
  - SafeWord® PremierAccess™
  - security considerations
  - troubleshooting
  - using variables other than remote\_user
  - using with other authentication schemes
- web servers

- configuring for Secure Global Desktop
- sharing Secure Global Desktop server certificates
- tarantella webserver command
- the Secure Global Desktop Web Server
- **web services**
  - https connections
- **web users**
- **web users**
  - Directory Services Integration
  - webtops
- **Webtop Hints (--hints)**
- **Webtop Icon attribute (--icon)**
- **webtop script applet public methods**
  - areObjectsInitialized
  - closeHierarchyLevel
  - getApplicationType
  - getCurrentIteratorElement
  - getIteratorForAllOpenHierarchyLevels
  - getIteratorForHierarchyLevel
  - getIteratorHasMoreElements
  - getLaunchWaitTimeOut
  - getNextIteratorElement
  - getNumberOfObjects
  - getNumberOfObjectsInGroup
  - getObjectClass
  - getObjectDisplayName
  - getObjectDisplayNameByName
  - getObjectFullName
  - getObjectImageNameByName
  - getObjectImageName
  - getObjectPlacement
  - getParentGroupName
  - getTotalNumberOfObjects
  - isApplication
  - isDocument
  - isGroup

- isHierarchyEnabled
- isOpenGroup
- isRunning
- killIterator
- launchByObjectName
- launchByObjectNumber
- login
- logout
- openHierarchyLevel
- receivedEvent
- scriptStart
- setLaunchWaitTimeOut
- webtop script applet
  - about
  - parameters
- webtop sessions
  - introduction
  - load balancing
  - Object Manager list
  - problem relocating
  - tarantella webtopsession list command
  - tarantella webtopsession logout command
  - tarantella webtopsession overview command
- Webtop Theme attribute (--webtop)
- webtop tray applet public methods
  - areObjectsInitialized
  - closeHierarchyLevel
  - getApplicationType
  - getCurrentIteratorElement
  - getIteratorForAllOpenHierarchyLevels
  - getIteratorForHierarchyLevel
  - getIteratorHasMoreElements
  - getLaunchWaitTimeOut
  - getNextIteratorElement
  - getNumberOfObjects
  - getNumberOfObjectsInGroup
  - getObjectClass



- getObjectDisplayName
- getObjectDisplayNameByName
- getObjectFullName
- getObjectImageNameByName
- getObjectName
- getObjectPlacement
- getParentGroupName
- getTotalNumberOfObjects
- isApplication
- isDocument
- isGroup
- isHierarchyEnabled
- isOpenGroup
- isRunning
- killIterator
- launchByObjectName
- launchByObjectNumber
- login
- logout
- openGroup
- openHierarchyLevel
- openParentGroup
- receivedEvent
- scriptStart
- setLaunchWaitTimeOut
- **webtop tray applet**
  - about
  - parameters
- **webtops**
  - browser-based and themes
  - Directory Services Integration
  - framework applet
  - icons
  - inheriting content
  - LDAP Groups (--ldapgroups)
  - LDAP Search (--ldapsearch)
  - LDAP users

- LDAP Users (--ldapusers)
- login applet
- print applet
- relocating to another host
- terminal emulator applet
- themes
- webtop script applet
- webtop tray applet
- without Java™ technology
- X emulator applet
- WebtopScriptEngine applet
- Width attribute (--width)
- width, application
- wincenter.exp login script
- Window Close Action attribute (--windowclose)
- Window Manager attribute (--winmgr)
- Windows application objects
  - creating from the command line
  - overview
- Windows application server authentication domain
- Windows cursors
- Windows NT Domain attribute (--ntdomain)
- Windows Protocol attribute (--winproto)
- Windows Terminal Services
  - commands for managing CALs
  - configuring for use with Secure Global Desktop
  - free CALs
  - licensing
  - list CALs
  - passwords and usernames
  - return CALs
  - setting working directory
  - Windows desktop performance
- Windows XP Remote Desktop
- windows, emulator
  - maximizing (3270)

- maximizing (5250)
- windows.exp login script
- windows
  - opening objects in new browser
  - problems with clipping
- WINS, and client drive mapping
- working directories, setting (Windows Terminal Services)
- Wrap long lines attribute (--autowrap)
- Wyse 60 emulator keyboard map
- X application objects
  - ALT and ALT GR key problems
  - creating from the command line
  - overview
- X authorization (xauth)
  - enabling
  - troubleshooting
- X emulator applet public methods
  - getEmulatorState
  - getProperty
  - login
  - logout
  - registerProperty
  - scriptStart
  - setProperty
  - suspendApplication
  - unregisterProperty
- X emulator applet
  - overview
  - parameters
- X extensions
  - supported
  - X Security Extension
- X font paths
  - adding fonts
  - attribute
- X fonts
  - adding

- installed
- X Protocol Engine Properties panel, Array Manager
- X Protocol Engine, Command-line Arguments attribute (--xpe-args)
- X.509 certificates
  - chaining
  - from other products
  - installing
  - installing Certificate Authority certificates
  - installing root certificates
  - obtaining
  - overview
  - sharing Secure Global Desktop server
  - supported
  - tarantella security certinfo command
  - tarantella security certrequest command
  - tarantella security certuse command
  - tarantella security customca command
  - tarantella security decryptkey command
  - tarantella security peerca command
  - user prompts
- XDE applet
- zip archives

## Introducing Sun Secure Global Desktop Software

### Read this topic to...

- Understand what Secure Global Desktop is.

Secure Global Desktop provides you with secure, remote access to desktop applications running on application servers.

You could be writing a report on a computer in the office, administering UNIX servers on your PC at home, or checking stock databases with a laptop on the train, Secure Global Desktop lets you do all this.

Secure Global Desktop also lets you run applications over a [secure network connection](#) to safeguard corporate and private data.

With Secure Global Desktop, you access all the applications that you can run from a single place, the [webtop](#).

To access a webtop, all you need is either a web browser with Java™ technology enabled or the Sun Secure Global Desktop Native Client (your Secure Global Desktop Administrator will tell you which to use) and something to run it on.

### Related topics

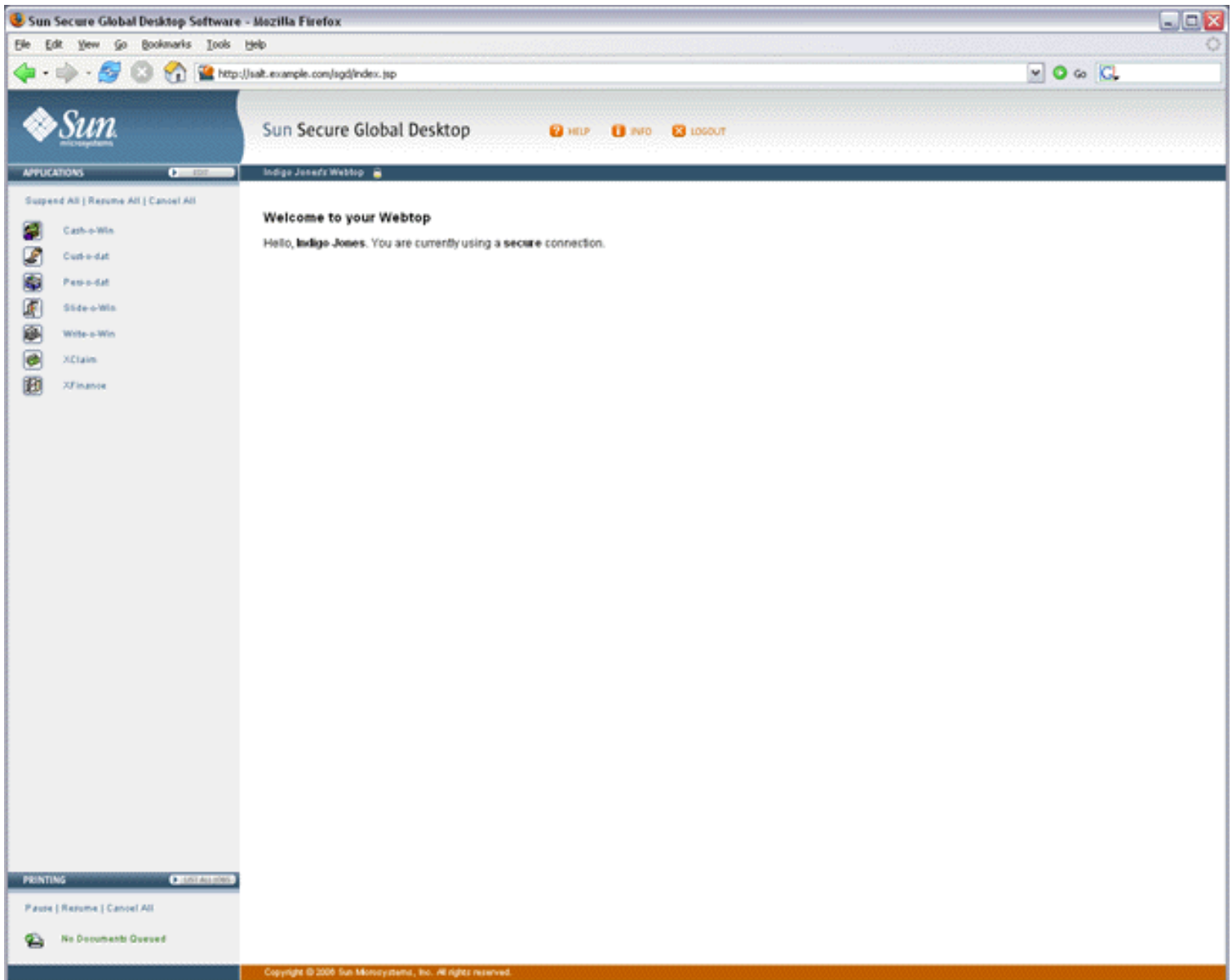
- [Using your webtop](#)

## Using your webtop

### Read this topic to...

- Understand how to use your webtop.

Your webtop is a special web page that lists the applications that you can run and lets you run them:



## Running applications

You use the Applications area of the webtop to manage the applications you can use:

To start an application, you click its link on your webtop. In a few moments the application appears, ready for you to use.



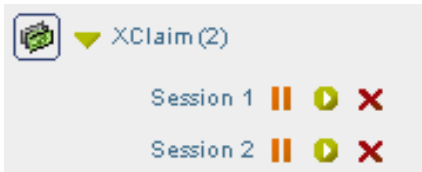
When you start an application, you may be asked for a username and password. This is your username and password for the application server that will run the application.

You don't have to exit an application before starting another. Just click another link.

Secure Global Desktop Administrators configure how the applications appear. Some may appear on the webtop and others in a separate window.

If you have difficulties, contact your Secure Global Desktop Administrator.

When an application is running, a triangle appears in front of the application's name on the webtop and a number appears in brackets after it. The session toolbar also appears below the application name.



The number in brackets is the number of separate instances of the application that you have started. Secure Global Desktop Administrators configure how many instances of an application you can start. To find out how many instances of an application you are allowed, point to its link on the webtop. The popup that displays states the number of sessions allowed.

There is a separate session toolbar for each running instance of the application:

- Click **||** to suspend an application.
- Click **▶** to resume an application.
- Click **✖** to end an application.

**Note** Suspending and resuming applications is explained below.

Click the triangle to hide and show the session toolbars for the application sessions.



You can manage all your application sessions at once:

[Suspend All](#) | [Resume All](#) | [Cancel All](#)

- Click **Suspend All** to suspend all running applications.
- Click **Resume All** to resume all suspended applications.
- Click **Cancel All** to end all running or suspended applications.

## Suspending and resuming applications

Some applications can be configured to keep running even when they're not displayed. These are "resumable" applications.

To see if an application is resumable or not, point to its link on your webtop and look at the popup window that displays.

If the popup window says...	This means...
Not resumable	<p>This application will exit when you log out of Secure Global Desktop. You can't suspend or resume, non-resumable applications.</p> <p><b>Note</b> Non-resumable applications only have a cancel button <b>X</b> in the session toolbar.</p>
Resumable until log out	<p>This application continues running until you log out of Secure Global Desktop. While you are logged in, you can suspend and resume these applications.</p>
Always resumable	<p>This application continues running even after you have logged out of Secure Global Desktop. When you log in again, click the resume button <b>▶</b> to display the running application again.</p>

To close an application's window without ending the application, you *suspend* the application. To display the window again and start using the application, you *resume* the application.

As an application is still running even though it's not displayed, you could start writing an urgent report in the office and then log out of Secure Global Desktop at the end of the day (the application is suspended). When you get home, you could log in to Secure Global Desktop again, resume the application and carry on writing the report.

**Note** If you logged in to Secure Global Desktop without typing a username and password, resumable applications are only resumable until you log out.

## Editing your settings

You can edit some settings that control how you use Secure Global Desktop. To do this, you click the Edit button in the Applications area of the webtop.

- Use the Client Settings tab to edit your profiles, see [Working with profiles](#) for more details.
- Use the Edit Groups tab to edit how applications display on your webtop.

## Groups

Only a Secure Global Desktop Administrator can add an application to, or remove an application from, the list of applications that you can run. However, you can choose how and when those applications display on your webtop. You do this by creating groups.

Groups are useful for grouping similar applications together or for hiding applications you do not use very often. How you use groups is up to you.



To create a group:

1. On the webtop, click Edit.
2. Click the Edit Groups tab.
3. Click Add New Group.
4. Type a name for the group.
5. In Choose your content, check the boxes for the applications and documents you want to include in the group.
6. Set the display options for the group.
  - o To hide the applications **and** the group so that they do not display on your webtop, uncheck the box next to I want to see this group on my webtop when I log in.
  - o To hide the contents of the group so that only the group name displays when you first log in, uncheck the box next to I want to see the contents of this group when I log in.

**Name**

Enter name:

**Choose your content**

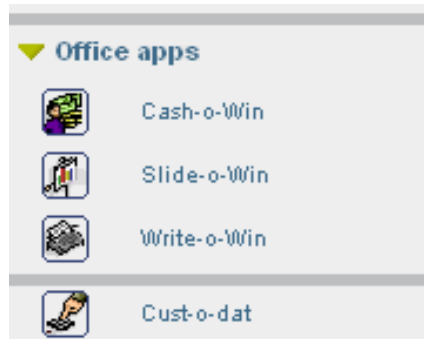
Cash-o-Win  Cust-o-dat  Pers-o-dat  
 Slide-o-Win  Write-o-Win  XClaim  
 XFinance

**Set your display options**

I want to see this group on my webtop when I log in  
 I want to see the contents of this group when I log in

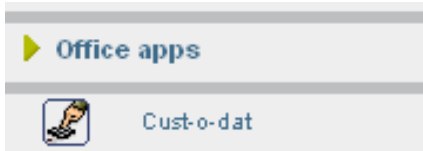
7. Click Save Group.
8. Click Update.

The names of the webtop groups you create display on the webtop.



A separator line also displays to show you which applications are in the group.

Click the triangle to hide and show the applications in the group.



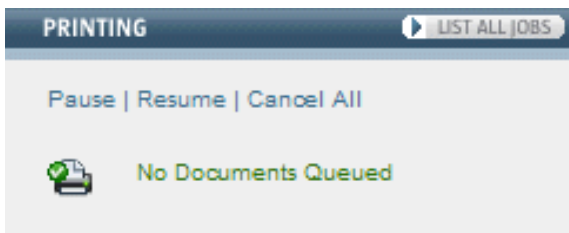
You can add as many groups as you like. You can change or delete a group whenever you like. After making a change you must click Update.

## Printing

Secure Global Desktop lets you print from your applications to your client device's printer.

If you are printing from an application running on a Windows 2000/2003 or a UNIX application server, you can choose which printer you print to. For all other types of application server, you can only print to your default printer.

You use the Printing area of the webtop to manage your print jobs:



When documents are printing, the webtop tells you how many print jobs are in the queue.



Click Pause to temporarily stop printing. The printer icon changes to show you when printing is paused.



If you pause printing, any print jobs that are pending are held in a queue until you either cancel them or resume printing.

Click Resume to start printing again after you have paused it.

Click Cancel All to delete all your print jobs.

To manage print jobs individually, click List all jobs. The webtop displays a list of all the print jobs in the queue, along with information about the job, for example the number of copies and the printer that will be used. If you have paused printing, click  to print just that one print job. To cancel a print job, click .

## Logging out

You should always log out of Secure Global Desktop before closing your web browser.

To log out of Secure Global Desktop, click the Logout button on your webtop and click OK when prompted for confirmation.



## Related topics

- [Introducing Sun Secure Global Desktop Software](#)
- [What usernames and passwords do I use for Secure Global Desktop?](#)
- [Using the classic webtop](#)

## Using Secure Global Desktop from your desktop Start Menu

### Read this topic to...

- Understand how to use Secure Global Desktop from your desktop Start Menu
- Understand the differences between using Secure Global Desktop from a webtop and from the Start Menu
- Learn how to add Secure Global Desktop to your Start Menu

You can use Secure Global Desktop from your desktop Start Menu. When you use Secure Global Desktop in this way, the links for starting applications display in your desktop Start Menu instead of [on your webtop](#). This means you can run applications through Secure Global Desktop in the same way as applications installed on your client device.

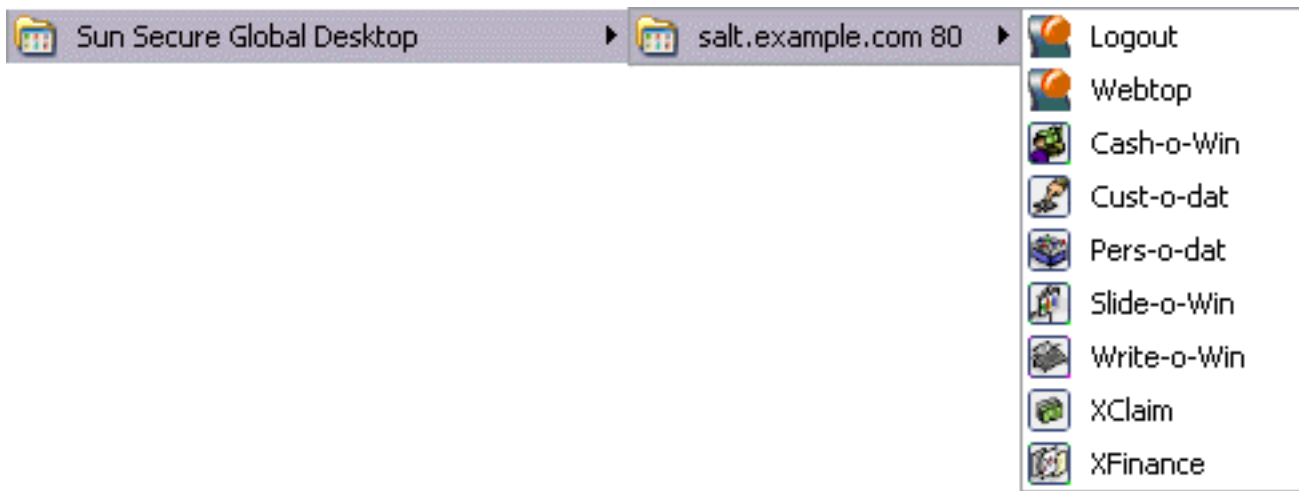
### Working with the Start Menu

You log in to Secure Global Desktop by clicking the Login link on your desktop Start Menu.



**Note** If you log in to more than one Secure Global Desktop server, there is a Login link for each server in the Start Menu. You can only be logged in to a single Secure Global Desktop server at any one time. Once you have logged in, the login links for other Secure Global Desktop servers are removed from the Start Menu.

Once you have logged in to Secure Global Desktop, the Start Menu is updated with the links for the applications you can run through Secure Global Desktop.



To start an application, you click its link on the Start Menu. To start another instance of the application, you click the link again.

Unlike the webtop, you cannot suspend and resume individual applications. Instead, when you log out of Secure Global Desktop, your running applications are either suspended or ended (depending on how they have been configured). When you log in again, any suspended applications you have are resumed automatically.

You cannot manage individual print jobs from the Start Menu and so print jobs go straight to the selected printer.

If you need to display a webtop, for example to be able to edit your profile, resume a suspended application or manage printing, you click the Webtop link on the Start Menu. The webtop displays in your default web browser.

If you have arranged any of your webtop content to [display in groups](#), those groups are also used in the Start Menu. If the group is configured to hide webtop content, the content does not display in the Start Menu.

To log out of Secure Global Desktop, you click the Logout link on the Start Menu.

## Adding Secure Global Desktop to your desktop Start Menu

To add Secure Global Desktop to your desktop Start Menu, you usually have to perform an initial login to display a webtop, and then [edit your profile](#), as follows:

1. Start a web browser and go the `http://server.example.com/sgd` URL.
2. Log in and display a webtop.
3. Edit your profile.
  - Click the Edit button in the Applications area of the webtop and then click the Client Settings

tab.

- Check the Add applications to Start Menu box.
- To log in automatically, check the Automatic Client Login box.
- To start the Secure Global Desktop Client when you log in to your desktop, check the Connect on System Login box.
- Configure the proxy server settings.
- Click Save.

**Note** Your Secure Global Desktop Administrator can tell you whether you can use automatic logins and what proxy server settings to use.

4. Log out of Secure Global Desktop.
5. Log in to Secure Global Desktop **using the Login link** on your desktop Start Menu.

**Note** To use Secure Global Desktop from the Start Menu, you always log in using the Start Menu. If you start a web browser and log in, your applications will not display in the Start Menu.

After the initial login, and depending on your profile, you may not need to use a web browser to access Secure Global Desktop.

#### Related topics

- [Using your webtop](#)

## Working with profiles

Every time you log in to Secure Global Desktop, the Sun Secure Global Desktop Client program runs on your client device. Each time the Secure Global Desktop Client starts it uses a profile. A profile is a group of configuration settings that control the Secure Global Desktop Client. The settings in a profile define:

- How the Secure Global Desktop Client connects to a Secure Global Desktop server, for example the URL to connect to and the proxy server to use.
- The operating mode of the Secure Global Desktop Client, for example whether to display a webtop (Webtop mode) or whether the list of applications that you can run displays in the desktop Start Menu (Integrated mode).
- How the Secure Global Desktop Client behaves, for example, if it loses a connection to a Secure Global Desktop server.

**Note** The Secure Global Desktop Client and profiles are not used with the [classic webtop](#).

You have one profile (one group of settings) for each Secure Global Desktop server you connect to.

## Editing profiles

You can only edit profiles if your Secure Global Desktop Administrator has configured Secure Global Desktop to let you do this.

You can only edit profiles from a webtop. On your webtop, click the Edit button in the Applications area of the webtop and then click the Client Settings tab.

You can only edit your own profiles and you can only edit the profile for the Secure Global Desktop server you are currently connected to.

When you first edit a profile, the settings are the settings your Administrator has configured for you.

To restore a profile to the system default settings, click the Reset button.

**Note** You must log out of Secure Global Desktop and log in again for changes to your profile to take effect.

## Profile settings

The following table lists the settings available in a profile with a description of what they do.

If you are unsure about a setting, ask your Secure Global Desktop Administrator for help.

Setting	Description
Login URL	<ul style="list-style-type: none"><li>• The Secure Global Desktop URL to use for the profile, usually <code>http://server.example.com/sgd</code>.</li><li>• In Webtop mode, the URL is loaded automatically in your default web browser so that you can log in and access your webtop.</li><li>• In Integrated mode, the URL is only loaded in the your default web browser if you need to log in to Secure Global Desktop, or if the Secure Global Desktop Client needs to obtain proxy server settings.</li><li>• The default Login URL is <code>http://server.example.com:80/sgd/index.jsp</code>.</li></ul>
Connect on System Login	<ul style="list-style-type: none"><li>• If enabled, the Secure Global Desktop Client is started automatically with this profile whenever you log in to your client device.</li><li>• If enabled, the Secure Global Desktop Client creates an application shortcut or symbolic link for itself in the startup folder for your desktop system.</li><li>• This is disabled by default.</li></ul>
Automatic Client Login	<ul style="list-style-type: none"><li>• If enabled, as soon as the Secure Global Desktop Client starts, it will attempt to log you in automatically to Secure Global Desktop. Your Administrator can tell you whether automatic logins are being used.</li><li>• Only enable this option if the Add applications to Start Menu is enabled.</li><li>• This is disabled by default.</li></ul>



Add applications to Start Menu	<ul style="list-style-type: none"><li>• Controls how you use Secure Global Desktop.</li><li>• If enabled, the applications you can run display in the desktop Start Menu on the client device (Integrated mode).</li><li>• If disabled, the applications you can run display on a webtop in a web browser (Webtop mode).</li><li>• With Integrated mode, you cannot suspend and resume individual applications or pause and resume individual print jobs.</li><li>• This is disabled by default.</li></ul>
Alternative PDF viewer	<ul style="list-style-type: none"><li>• The application command for an alternative PDF viewer to use with PDF printing.</li><li>• If the application is not on your <code>PATH</code>, type the full path to the application.</li><li>• This setting only applies to UNIX, Linux and Mac OS X client devices.</li></ul>
Logging	<ul style="list-style-type: none"><li>• Controls the amount of information that is output to the Secure Global Desktop Client log file.</li><li>• The output is logged to a text file in the same directory as the Secure Global Desktop Client.</li><li>• The default is Errors only.</li></ul>
Preferred Language	<ul style="list-style-type: none"><li>• The default language to use when the Secure Global Desktop Client is started from the command line, for example when the Secure Global Desktop Client is in Integrated mode.</li><li>• The language selected is used for messages displayed by the Secure Global Desktop Client, the login dialog, and the webtop.</li><li>• The default is en.</li></ul>
Check for Local X Server	<ul style="list-style-type: none"><li>• If enabled, the Secure Global Desktop Client checks whether there is an X server running on the client device.</li><li>• Enabling this option can improve performance when launching X applications that are configured to display using an X server on the client device.</li><li>• This setting only applies to Windows client devices.</li><li>• This is disabled by default.</li></ul>

Proxy settings	<ul style="list-style-type: none"><li>● Settings that control how the Secure Global Desktop Client determines what proxy servers to use.</li><li>● Use default web browser settings means use the proxy server settings configured in your default web browser.</li><li>● Manual proxy settings allows you to define the proxy server settings in the profile. You can specify either an HTTP or a SOCKS proxy server or both.</li><li>● In Integrated mode, if the proxy settings are determined from a web browser, the Secure Global Desktop Client has to start your web browser at least once in order to detect what the proxy settings are.</li><li>● If the proxy settings are determined from a web browser, the settings are stored and used the next time the Secure Global Desktop Client starts.</li><li>● If Establish proxy settings on session start is enabled, every time the Secure Global Desktop Client starts, the default web browser is started so that the proxy settings can be determined. The stored proxy settings are not used.</li><li>● The default is: Use default web browser settings. Establish proxy settings on session start is disabled.</li></ul>
Connection Failure	<ul style="list-style-type: none"><li>● Settings that control what the Secure Global Desktop Client does if the connection to a Secure Global Desktop server is lost, whether to always reconnect, to never reconnect or to ask you what to do.</li><li>● If the Secure Global Desktop Client reconnects, these settings control how many attempts are made to reconnect and the time in seconds between each attempt.</li><li>● If the Secure Global Desktop Client is unable to reconnect, the webtop session ends and any running applications are ended or suspended, depending on how they have been configured for you.</li><li>● The default settings are: Always attempt to reconnect, Number of attempts: 6, and Interval: 10.</li></ul>

## Related topics

- [Introducing Sun Secure Global Desktop Software](#)

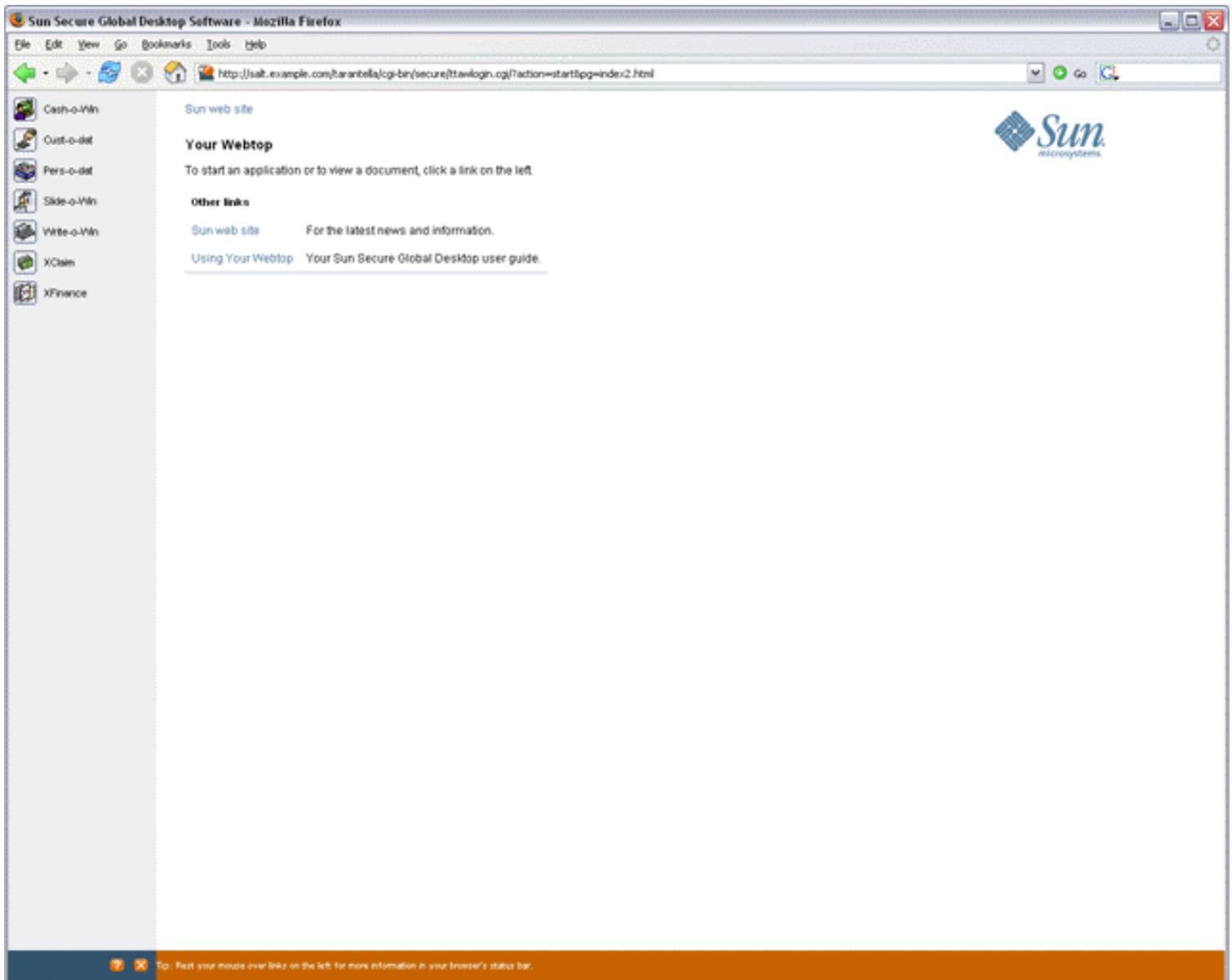


## Using the classic webtop

### Read this topic to...

- Understand how to use the classic webtop.

If you use a web browser to access the classic webtop, the webtop is a special web page.

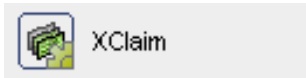


To access an application, just click its link on your webtop.



In a few moments the application appears, ready for you to use. When you start an application, you may need to supply a password for the application server that will run it. If you have difficulties, contact your Secure Global Desktop Administrator. Secure Global Desktop Administrators configure how the applications appear. Some may appear on your webtop, and others may use their own windows.

A cog appears on the application's icon on your webtop to show that the application is running.



You do not have to exit an application to start another. Just click another link.

## Resumable applications

Some applications may be configured to keep running even when they are not displayed: these are "resumable" applications. If the icon for an application includes a cog, you can resume it. Just click the link to display the application again, exactly as you left it.

As the application is still running even though it is not displayed, you could start a lengthy calculation and let it complete while you travel. At your destination, you could display the application again to see the results.

To see if an application is resumable or not, point to its link on your webtop, and look for a message in the status bar at the bottom of the window.

If the message includes...	This means...
Not resumable	This application will exit when you follow another link on your webtop. The next time you click the link, a new instance of this application starts.
Resumable until log out	This application continues running when you follow other links on your webtop. The next time you click the link, the running application is displayed. This application continues running until you log out of Secure Global Desktop. When you log in to Secure Global Desktop again and click the application's link, a new instance of this application starts.
Always resumable	This application continues running when you follow other links on your webtop and when you log out of Secure Global Desktop. When you log in to Secure Global Desktop again and click the application's link, the running application is displayed.

**Note** If you logged in to Secure Global Desktop without typing a username and password, resumable applications are only resumable until you log out.

## Printing

Secure Global Desktop lets you print from your applications to your client device's printer.

If you are printing from an application running on a Windows 2000/2003 or a UNIX application server, you can choose which printer you print to. For all other types of application server, you can only print to your default printer.

If you are using a web browser, point to the printer icon on your webtop and a message appears in the status bar at the bottom of the window to say which is your current default printer.

The webtop lets you:

- See when documents are printing. Status bar information shows you when print jobs are spooling to your client device's printer.
- Pause your print jobs. The number of print jobs you have waiting in the queue is shown on the status bar.
- Cancel your print jobs.

If you are using a web browser for Secure Global Desktop:

- To pause your current print job and any new ones, click the Pause button. Click the Pause button again to restart.



- To cancel your current print job, click the Cancel button.



If you are using the Sun Secure Global Desktop Native Client, use the Print menu to pause and restart printing, and to cancel print jobs.

If you have paused printing, any print jobs that are pending are held in a queue until you either cancel them or resume printing. You may see a warning message if you log in and you have print jobs paused in the queue. The message reminds you about the print jobs and allows you to start printing them.

## Logging out

You should always log out of Secure Global Desktop before exiting your web browser or the Sun Secure Global Desktop Native Client.

If you are using a web browser for Secure Global Desktop, click the Log Out icon on your webtop, and click OK when prompted for confirmation.



To log out of Secure Global Desktop from the Sun Secure Global Desktop Native Client, click Log Out on the Webtop menu, and click OK when prompted for confirmation.

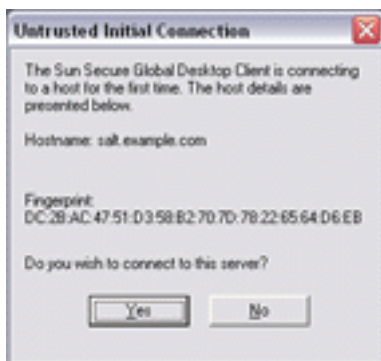
### Related topics

- [Where can I find the Native Client?](#)
- [What usernames and passwords do I use for Secure Global Desktop?](#)



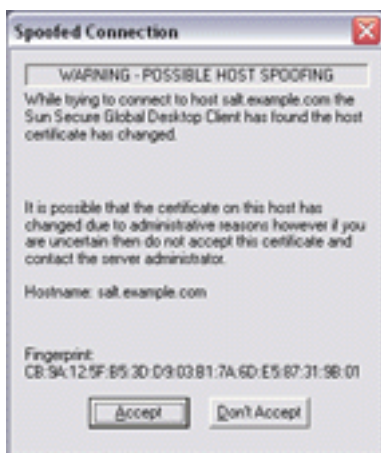
## Why do I see an Untrusted Initial Connection message?

The first time you connect to a Secure Global Desktop server, you see an Untrusted Initial Connection message. This is a security message to help you be sure that the server you are connecting to can be trusted.



The message displays a hostname and a fingerprint. You should check these details with the information provided by your Secure Global Desktop Administrator **before** clicking Yes.

Once you have clicked Yes, you will not see the message again unless there is a problem. If there is a problem, a Spoofed Connection message displays.



If you see a Spoofed Connection message, make a note of the details displayed and Click No. Contact your Administrator.

### Related topics



- Using your webtop

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## Do I lose my work if I accidentally close my web browser?

Usually, you won't lose any work if you accidentally close your web browser (without logging out) or if your web browser crashes. However, this depends how the Secure Global Desktop Administrator configured the applications you use in Secure Global Desktop, and how you logged in to Secure Global Desktop.

### Application configuration

If an application is configured to be "Not Resumable", then it exits when you log out of Secure Global Desktop or if your browser or client device crashes. Typically applications are configured to be Not Resumable if they're used only for short periods at a time, and not for business-critical functions.

Applications configured to be "Always Resumable", or "Resumable Until Log Out", continue to run if you close your web browser. Simply restart, log in to Secure Global Desktop again and resume the applications that are still running.

To see if an application is resumable or not, point to its link on your webtop and look at the popup window that displays (or look in the status bar at the bottom of the window).

### Who you're logged in as

If you logged in to Secure Global Desktop anonymously (you didn't supply a username and password) or you're using a shared webtop (where more than one person logs in using the same username and password), then your applications exit if your browser or client device crashes.

**Why?** In both cases, Secure Global Desktop can't tell when you log in to Secure Global Desktop again that you're the same user as before, because you're not using a unique username and password.

#### Related topics

- [Using your webtop](#)

## When I click a link to start an application, an error message appears

Try the following:

- Make sure you supplied the correct username and password for the application server. If Secure Global Desktop doesn't prompt you for this information, try [Shift-clicking the link](#) to force the prompt to appear.
- Log out of Secure Global Desktop and exit your web browser (or the Sun Secure Global Desktop Native Client), then restart it and log in to Secure Global Desktop again. Click the application's link.
- Use Secure Global Desktop from a different client device.
- Contact a Secure Global Desktop Administrator, supplying all the information shown in the error message.

### Related topics

- [Using your webtop](#)

## When I print from an application, the output doesn't appear

### Have you paused printing?

Make sure that your webtop indicates that printing is not paused.



**Note** If you are using the [classic webtop](#), check that the Pause button has not been pressed. If you are using the Sun Secure Global Desktop Native Client, check the status bar.

### Is your printer set up correctly?

Make sure your printer is set up correctly, for example, by printing a web page to the printer from a web browser.

### Have you printed to the right printer?

If you are printing from a Windows 2000/2003 or UNIX application server, you can choose which printer you print to. If you do not select a printer, you will print to your default printer.

For all other application servers, you always print to your default printer.

To see which printer is your default printer, point to the printer icon on your webtop and a popup displays the name of your default printer.

**Note** If you are using the [classic webtop](#) the name of the default printer displays in the status bar when you point to the printer icon on your webtop.

If you want to change your default printer, you must log out of Secure Global Desktop, change the default printer, then log in to Secure Global Desktop again.

### Is the message "No Client Printer Available" displayed?

Make sure that your webtop does not display a "No Client Printer Available" message and the printer icon contains a red X.



This means that Secure Global Desktop doesn't support printing for your client device or for your printer.

**Note** If you are using the [classic webtop](#), the webtop displays a "Can't Print" message and the printer icon contains a red X.

Your Secure Global Desktop Administrator may be able to help enable printing.

## Next steps

Please contact a Secure Global Desktop Administrator.

### Related topics

- [Using your webtop](#)

## I have another problem

Try the following:

- Exit your web browser or Native Client, then restart it and log in to Secure Global Desktop again.
- Restart your client device.
- Try using Secure Global Desktop from a different client device.
- Ask a Secure Global Desktop Administrator for help.

If you're using a web browser to log in to Secure Global Desktop, you can display a page containing information useful for Support:

Click the Info button on your webtop and then click the "Detailed diagnostics" link at the bottom of the page.



For the [classic webtop](#), click the About button on your webtop and then click the "Detailed information useful to help diagnose problems" link at the bottom of the page.



### Related topics

- [Using your webtop](#)

## What usernames and passwords do I use for Secure Global Desktop?

When you use Sun Secure Global Desktop Software, you are using at least two, and maybe more, computers:

- Your client device.
- The Secure Global Desktop server.
- Application servers, which run your applications.

Correspondingly, to use Secure Global Desktop you need to know the following usernames and passwords.

Username and password	Description
Client device	When you first start your client device, you may need to supply a password (for example, a Windows password). This password is nothing to do with Secure Global Desktop.
Secure Global Desktop server	When you log in to Secure Global Desktop, you need to type a username and password so that the Secure Global Desktop server knows who you are and can display your webtop. You won't need to type this password again until the next time you log in to Secure Global Desktop.  You may also be able to log in to Secure Global Desktop anonymously, that is, without typing a username and password.
Application servers	When you start an application, you may need to supply a password for the application server that runs it. The Secure Global Desktop server can remember these passwords, so you don't need to type them every time: use the Save This Password option, if available, when you type your username and password.  If you want to use a different username and password to run an application, you can <a href="#">force Secure Global Desktop to prompt you</a> .

## Related topics

- [Using your webtop](#)
- [How do I force Secure Global Desktop to prompt me for a username and password?](#)
- [Who am I logged in to Secure Global Desktop as?](#)
- [I have another problem](#)



## Where can I find the Native Client?

To install the Sun Secure Global Desktop Native Client, download and run the Setup program from:

`http://server.example.com`


where *server.example.com* is the name of a Secure Global Desktop server.

**Note** The Native Client can only be used to access the *classic* webtop.

### Related topics

- [Using your webtop](#)

## How can I tell whether my connection to Secure Global Desktop is secure?

If you have a secure connection, the locked padlock symbol  displays below the webtop menu bar. When you first log in, the page that displays on the webtop also tells you whether you have a secure or a standard connection.

Secure connections to Secure Global Desktop are available only if a Secure Global Desktop Administrator has enabled them.

You may not automatically receive a secure connection, or you may only get a secure connection under certain circumstances. Contact your Secure Global Desktop Administrator if you don't get a secure connection when you need one.

### If you're using the classic webtop

If you're using the [classic webtop](#), point to an area **between the links** on your webtop. If you have a secure connection, the status bar shows a message of the form:

"Secure Global Desktop user: *username* (SSL connection)" .

#### Related topics

- [Using your webtop](#)

## How do I change the way an application is displayed?

A Secure Global Desktop Administrator defines how an application is normally displayed. But if you press Control when you click an application's link on a webtop, it may display differently.

For applications normally displayed...	Use Control-click to display them...
On your Webtop	In an independent window
In a new browser window	On your Webtop
In an independent window	On your Webtop
Using an X server on your client device	On your Webtop

**Note** Pressing control has no effect if you are clicking an application's link [on the desktop Start Menu](#).

For applications that display full-screen or in a seamless window or applications that integrate with your local window manager, pressing Control has no effect.

If an Administrator has defined an application to display in a seamless window, you can switch the application between a seamless and an independent window by pressing the SCROLL LOCK key.

### Fitting an application to the size of the window

A graphical application that displays in an independent window may be scaled to fit the size of the window in which it displays. If you re-size the window, Secure Global Desktop rescales the application to fit the new window size without displaying any scroll bars.

You switch the application between being scaled and not being scaled by pressing the SCROLL LOCK key.

To see if an application displays in a scalable window, point to its link on your webtop and look at the popup that displays (or look in the status bar at the bottom of the window).

### Related topics

- Using your webtop

Copyright © 1997-2006 Sun Microsystems, Inc. All rights reserved.

## How do I copy information between applications?

For **Windows and X applications**, use the normal method for the application you are copying from, and then the usual method for the application you are pasting to. You may not be allowed to copy and paste information from particular applications. This is configured by your Secure Global Desktop Administrator. If you are not allowed to copy and paste between an application, you will paste the following message instead of the information you copied:

```
Sun Secure Global Desktop Software: Copied data not available to this application
```

For **character applications**, click with the right mouse button, and then click Copy or Paste as appropriate. To select a column of text, hold down the Shift key while selecting the text.

You can copy information between different types of application, for example from an xterm running on an application server to a text editor running on your client device.

You can only copy and paste **graphics** to or from Microsoft Windows 2000/2003 applications. If you are using the *classic webtop*, you can only do this if you're using the Native Client for Microsoft Windows.

### Related topics

- [Using your webtop](#)

## Who am I logged in to Secure Global Desktop as?

Who you're logged in to Sun Secure Global Desktop Software as displays on the webtop toolbar (next to the padlock symbol).

If the toolbar says you're logged in as "Guest user" then you're either logged in anonymously (you didn't type a username and password) or you're using a webtop that's shared with other users.

These details also display on the webtop when you first log in.

### If you're using the classic webtop

If you're using the [classic webtop](#), point to an area **between the links** on your webtop. The status bar shows a message of the form:

"Secure Global Desktop user: *username (connection type)*",

where *username* is who you're logged in as and *connection type* is "SSL connection" if you have a secure connection and "standard connection" otherwise.

If the username is of the form ".../\_dns/server/\_anon/number", then you're either logged in anonymously or you're using a shared webtop.

#### Related topics

- [Using your webtop](#)
- [What usernames and passwords do I use for Secure Global Desktop?](#)
- [How do I force Secure Global Desktop to prompt me for a username and password?](#)

## Can I add applications or documents to my Webtop?

No. Only a Secure Global Desktop Administrator can add an application to, or remove an application from, the list of applications that you can run. If you want more applications, contact an Administrator.

However, you can choose how and when your applications display on your webtop. You do this by creating [webtop groups](#).

**Note** You can't do this on the [classic webtop](#).

### Related topics

- [Using your webtop](#)

## How do I force Secure Global Desktop to prompt me for a username and password?

Hold down the Shift key when you click an application's link.

Forcing Sun Secure Global Desktop Software to prompt you for a username and password means Secure Global Desktop won't use any username and password that has already been saved for the application server. This is useful if you want to run an application as another user.

If the Save This Password box is checked, the new username and password are saved in the password cache, replacing any previously saved username and password for you on this application server. This username and password is used for any other applications you run on this application server.

If you're logged in to Secure Global Desktop anonymously, or as a shared user, holding down the Shift key has no effect.

### Related topics

- [Using your webtop](#)
- [When I click a link to start an application, an error message appears](#)
- [Who am I logged in to Secure Global Desktop as?](#)



[Using Your Webtop](#) > How do I start a Windows application using a different Windows domain?

## How do I start a Windows application using a different Windows domain?

You can't do this yourself. Ask a Secure Global Desktop Administrator to do this for you.

### Related topics

- [Using your webtop](#)

## What happens if my password for a server changes or expires?

If your password has changed, Sun Secure Global Desktop Software detects that your old password is no longer valid, and prompts you.

If your password has expired, you may be given the opportunity to set a new password. If not, please contact a Secure Global Desktop Administrator.

### Related topics

- [Using your webtop](#)

## How do I use a single-button Apple Macintosh mouse with applications?

Many Microsoft Windows and X applications make use of a middle mouse button or a right mouse button. To use these applications from an Apple Macintosh mouse with one button, you click the button while holding down a key on the keyboard.

- To simulate a **middle** mouse button click, press **Alt** while clicking the mouse button.
- To simulate a **right** mouse button click, press **Command** while clicking the mouse button.

### Related topics

- [Using your webtop](#)

## Glossary of terms used with Secure Global Desktop

Term	Definition
Application	A program running on a server. Secure Global Desktop lets you access your applications using a web browser (or the Sun Secure Global Desktop Native Client) on any client device.
Client device	The hardware you run your web browser or Sun Secure Global Desktop Native Client on when you use Secure Global Desktop. For example, a PC or a Network Computer.
Link	Provides access to documents and applications on your webtop. Usually an icon with a label.
Password	A secret set of characters that, together with your username, proves your identity to a server. You may have different passwords (and usernames) on different servers.
Profile	A group of configuration settings that control the Secure Global Desktop Client.
Server	A computer, or software, that provides services to client devices. The Secure Global Desktop server lets you see your webtop. Other servers may run applications which are displayed on your webtop.
Secure Global Desktop Administrators	The people who can configure Secure Global Desktop, put links on user's webtops and set up applications.
Sun Secure Global Desktop Native Client	Software you run on your client device to access Secure Global Desktop if you can't run a web browser with Java technology enabled.
Secure Global Desktop server	The Secure Global Desktop software you log in to using your web browser (or the Sun Secure Global Desktop Native Client) to see your webtop.

Username	The unique name by which servers identify you. You may have different usernames on different servers.
Web browser with Java™ technology enabled	Software you run on your client device to access Secure Global Desktop. For example, Microsoft Internet Explorer.
Webtop	The special web page you see when you log in to Secure Global Desktop, providing access to applications.

### Related topics

- [Using your webtop](#)

## Sun Secure Global Desktop Software legal information

Copyright © 1997-2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights - Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo, Java, Solaris and SPARC are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon architecture developed by Sun Microsystems, Inc.

UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Adobe is a registered trademark of Adobe Systems, Incorporated.

Products covered by and information contained in this service manual are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY

INVALID.

Copyright © 1997-2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuels relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains listés à l'adresse <http://www.sun.com/patents> et un ou les brevets supplémentaires ou les applications de brevet en attente aux Etats - Unis et dans les autres pays.

Cette distribution peut comprendre des composants développés par des tierces parties.

Sun, Sun Microsystems, le logo Sun, Java, Solaris et SPARC sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Adobe est une marque enregistrée de Adobe Systems, Incorporated.

Les produits qui font l'objet de ce manuel d'entretien et les informations qu'il contient sont régis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes biologiques et chimiques ou du nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

## Related topics

- [Using your webtop](#)



## Using Your Webtop

### Tutorials

- [Introducing Sun Secure Global Desktop Software](#)
- [Using your webtop](#)
- [Using Secure Global Desktop from your desktop Start Menu](#)
- [Using the classic webtop](#)

### Reference

- [Working with profiles](#)
- [Glossary of terms used with Secure Global Desktop](#)
- [Sun Secure Global Desktop Software legal information](#)

### Troubleshooting

- [Do I lose my work if I accidentally close my web browser?](#)
- [When I click a link to start an application, an error message appears](#)
- [When I print from an application, the output doesn't appear](#)
- [I have another problem](#)

### Frequently asked questions

- [What usernames and passwords do I use for Secure Global Desktop?](#)
- [How can I tell whether my connection to Secure Global Desktop is secure?](#)
- [How do I change the way an application is displayed?](#)
- [How do I copy information between applications?](#)
- [Who am I logged in to Secure Global Desktop as?](#)
- [Why do I see an Untrusted Initial Connection message?](#)
- [Can I add applications or documents to my Webtop?](#)
- [How do I force Secure Global Desktop to prompt me for a username and password?](#)
- [How do I start a Windows application using a different Windows domain?](#)
- [What happens if my password for a server changes or expires?](#)
- [How do I use a single-button Apple Macintosh mouse with applications?](#)

- [Where can I find the Native Client?](#)

Copyright © 1997-2006 Sun Microsystems, Inc. All Rights Reserved.

## Using Your Webtop

- anonymous users
  - closing browser
  - Webtop username
- applications
  - adding/removing from your Webtop
  - changing how displayed
  - error message when starting
- authentication
  - application server
  - needed for Secure Global Desktop
- browsers, closing
- changing your Webtop
- Control key
- copy and paste
- crashes, losing work
- desktop Start Menu
  - using
- documents, adding/removing from your Webtop
- error messages, starting an application
- legal information
- losing work, crashes
- Macintosh, mouse buttons
- mouse buttons, Macintosh
- Native Client, installing
- other problems
- passwords
  - changed
  - expired
  - needed for Secure Global Desktop
- printing, problems
- problems, other
- profile

- Sun Secure Global Desktop Client configuration settings
- prompts, forcing, username and password
- Proprietary Rights Notice
- secure connections
- shared accounts
  - closing browser
  - Webtop username
- Shift key
- spoofed connection message
- SSL connections
- standard connections
- Sun Secure Global Desktop Client
  - profile settings
- Sun Secure Global Desktop Native Client, installing
- Sun Secure Global Desktop Software
  - glossary of terms
  - introduction
- untrusted initial connection message
- user, Secure Global Desktop
- usernames, needed for Secure Global Desktop
- Webtop usernames
- Webtops
  - changing
- webtops
  - classic webtop
  - introduction
- Windows applications, NT domains
- Windows domains, changing