Sun Secure Global Desktop 4.31 Release Notes

Sun Microsystems, Inc.
www.sun.com

Part No. 820-1086
May 2007, Revision 01

Please
Recycle

Contents

Preface ix

1. System Requirements and Support 1

Hardware Requirements 1

Operating System Requirements 2

Operating System Modifications 3

Fedora Core 6 3

5250 and 3270 Applications 3

SUSE Linux Enterprise Server 9 With Service Pack 2 3

SUSE Linux Enterprise Server 10 3

Solaris 8, 9 and 10 OS 3

Solaris 8 OS `/dev/random` Pseudo Device 4

Web Server Requirements 4

Network Requirements 4

Browser-Based Webtop Requirements 5

Classic Webtop Requirements 7

Limitation of the Classic Clients 9

SGD Enhancement Module Requirements 9

Supported Application Types 10

Supported Protocols 10

Security Support 11

Proxy Server Support 13

Supported Authentication Methods 13

SecurID Authentication 13

Supported LDAP Directory Servers 14

Printing Support 14

Smart Card Support 15

2. New Features and Changes 17

New Features in Version 4.31 17

Audio Support in X Applications 17

Support for the Remote Desktop on Microsoft Windows Vista 18

SSH Client Settings 18

New Features in Version 4.30 19

Integration with the Desktop Start Menu 19

Single Sign-On 20

Managing Client Configuration With Profiles 20

Mobile Proxy Server Configuration 21

Enhanced Command Line for the SGD Client 22

Manually Installable SGD Client 22

New X Server 22

New Enable X Security Extension Attribute 23

PDF Printing for UNIX Platform, Linux, and Mac OS X Clients 24

Client Drive Mapping for UNIX Platform and Linux Applications 24

Support for Serial Ports in Windows Applications 25

Support for the Remote Desktop on Microsoft Windows XP Professional 26

Support for Connections to the Console Session With Windows Server 2003 Terminal Services 26

Initial Connection Security 26

Protecting Clients Against Unauthorized Servers 27

Controlled Copy And Paste 27

Support for SecurID for Application Server Authentication 28

Localized User Interface 28

Translated Documentation 29

Language Support in Expect Scripts 29

Changes in Version 4.31 29

SecurID Authentication on Solaris x86 Platforms 30

Support for Multiple SGD Servers in Integrated Mode 30

Array Routes 30

SGD Start-up Scripts 30

Untrusted Initial Connection Message 31

Windows Key Disabled 31

Changes in Version 4.30 31

Single Installable Package 31

SSL Daemon Always Running 31

User Preferences File on UNIX Platform, Linux, and Mac OS X Client Devices 32

Window Close Action (`--windowclose`) Attribute 32

Support for PAM for UNIX Platform User Authentication 32

PDF Printing 33

Client Certificates for Active Directory Login Authority 33

SGD Certificate Store 33

Licensing 33

Application Connection Methods 34

Simultaneous Webtop Connections Attribute 34

Mainframe (3270) Applications 34

3. Support Statements, Known Issues, and Bug Fixes 35

End-Of-Support Statements 35

Retirement of the Classic Clients 36

Known Bugs and Issues 36

602423 - Return Key and Keypad Enter Key Issues 36

6375418 - Non-ASCII Characters in Input Method Windows 37

6443840 - Automatic Proxy Server Configuration Scripts Fail 39

6448990 - Backslash and Yen Keys Problems 39

6456278 - Integrated Mode Does Not Work for the Root User 40

6458111 - Gnome Main Menu Crashes Using Integrated Mode 40

6540417 - Printer Preferences Are Not Stored 41

6544844 - Printing Fails if SELinux is Enforcing 41

6544890 - Enhancement Module Start-up Script Error 41

6461864 and 6476661 - Automatic Login and Integrated Mode Fails With the Gnome Desktop 42

6468716 - Keyboard Does Not Work in Gnome Sessions 42

6470197 - Compiling SGD Web Server Modules Fails 43

6476194 - No KDE Desktop Menu Item for the SGD Client 43

6477187 - Client Drive Mapping Fails Without the Client for Microsoft Networks 44

6480880 - SGD Client Fails With Relocated Webtops 44

6481148 - Localized Text Not Used During Installation 45

6481312 - Upgrading Resets the Available Connection Types 45

6482912 - SGD Client Not Installed Automatically 45

6486551 - Unavailable Application Server Not Detected 46

6528952 - SGD Audio Driver Not Installed on Upgrade 46

Sun Type 7 Japanese Keyboard Issues 46

Start Menu Items Not Sorted Alphabetically 47

No Start Menu Entries on Sun Java Desktop Systems 47

Bug Fixes in Version 4.31 48

Bug Fixes in Version 4.30 49
Administration Tools 49
Application Launch 50
Clients and Webtop 51
Emulation 51
Installation and Upgrade 52
Internationalization and Localization 53
Other 53
Printing 54
Security 55
Server 55
User Authentication 56
Web Services 56

Preface

The *Sun Secure Global Desktop 4.31 Release Notes* provide information about the system requirements and support, and the new features and changes, for this version of Sun Secure Global Desktop Software. This document is written for system administrators.

Using System Commands

This document might not contain information on basic UNIX® system commands and procedures such as shutting down the system, booting the system, and configuring devices. Refer to your system documentation for this information. This document does, however, contain information about specific Secure Global Desktop commands.

Shell Prompts

Shell	Prompt
C shell	*machine-name*%
C shell superuser	*machine-name*#
Bourne shell and Korn shell	$
Bourne shell and Korn shell superuser	#

Typographic Conventions

Typeface*	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your .login file. Use ls -a to list all files. % You have mail.
AaBbCc123	What you type, when contrasted with on-screen computer output	% **su** Password:
AaBbCc123	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the *User's Guide*. These are called *class* options. To delete a file, type **rm** *filename*.

* **The settings on your browser might differ from these settings.**

Related Documentation

The documents listed as online are available at `http://www.sun.com/documentation`.

Application	Title	Part Number	Format	Location
Installation	*Sun Secure Global Desktop 4.31 Installation Guide*	820-1087-10	HTML PDF	Online Software CD and online
Administration	*Sun Secure Global Desktop 4.31 Administration Guide*	801-1088-10	HTML	Online

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Sun at `docfeedback@sun.com`.

Please include document title and part number (*Sun Secure Global Desktop 4.31 Release Notes*, part number 820-1086) in the subject line of your email message.

CHAPTER 1

System Requirements and Support

This chapter contains the system requirements for installing and using Sun Secure Global Desktop Software (SGD) version 4.31.

Topics in this chapter include the following:

- "Hardware Requirements" on page 1
- "Operating System Requirements" on page 2
- "Web Server Requirements" on page 4
- "Network Requirements" on page 4
- "Browser-Based Webtop Requirements" on page 5
- "Classic Webtop Requirements" on page 7
- "SGD Enhancement Module Requirements" on page 9
- "Supported Application Types" on page 10
- "Supported Protocols" on page 10
- "Security Support" on page 11
- "Proxy Server Support" on page 13
- "Supported Authentication Methods" on page 13
- "Printing Support" on page 14
- "Smart Card Support" on page 15

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 (`http://www.sun.com/secure/contact/`).

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

- What is needed to install and run SGD
- What is needed for each user that logs in to SGD on the host and runs applications

The following are the requirements for installing and running SGD:

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

This is *in addition to* what is required for the operating system itself and assumes the server is used only for SGD.

The following are the requirements to support users who log in to SGD and run applications:

- Minimum 20 megabytes for each user.
- On SPARC® technology platforms (SPARC platforms), 15 megahertz for each user.
- On x86 platforms, 20 megahertz for each user.

Caution – The actual CPU and memory requirements can vary significantly depending on the applications used.

Operating System Requirements

The following table describes the supported installation platforms for SGD.

Operating System	Supported Versions
Solaris OS on SPARC platforms	8, 9, 10
Solaris OS on x86 platforms	10
Red Hat Enterprise Linux (Intel x86 32-bit)	4, 5
Fedora Linux (Intel x86 32-bit)	Core 6
SUSE Linux Enterprise Server (Intel x86 32-bit)	9, 10

Operating System Modifications

You might have to make some operating system modifications. Without these modifications, SGD might not install properly or operate correctly.

Fedora Core 6

SGD fails to 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.

5250 and 3270 Applications

The `libXm.so.3` library is required to support 5250 and 3270 applications. This library is available in the OpenMotif 2.2 package.

SUSE Linux Enterprise Server 9 With Service Pack 2

SGD fails to 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. Obtain and install version 2 of the library before installing SGD.

SUSE Linux Enterprise Server 10

SGD fails to 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. Obtain and install the required version of these libraries before installing SGD.

Solaris 8, 9 and 10 OS

You must install at least the End User Solaris OS distribution to get the libraries required by SGD. If you do not, SGD does not install.

SGD fails to install if the `/usr/lib/libsendfile.so` library is not available on the host. This library might be included with the Core Solaris Libraries (`SUNWcsl`) package, or you might have to apply patch number 111297 to obtain it.

Solaris 8 OS `/dev/random` Pseudo Device

Users might not be able log in to SGD on Solaris 8 OS platforms if the host does not have the `/dev/random` pseudo device. You might have to install patch number 112438 to obtain this device.

Web Server Requirements

A web server is an essential part of a working SGD installation. When you install SGD, you install the SGD Web Server. The SGD Web Server is an Apache web server that is pre-configured for use with SGD. The SGD Web Server consists of the following components listed in the following table.

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

You can use your own web server with SGD. How you do this is described in the *Sun Secure Global Desktop Software 4.31 Administration Guide*.

Network Requirements

You must configure your network for use with SGD. The following are the main requirements:

- 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 SGD on the following TCP ports:

- **80** - For HTTP connections between client devices and the SGD Web Server. The port number might vary depending on the port selected on installation.
- **443** - For HTTPS connections between client devices and the SGD web server.
- **3144** - For standard (unencrypted) connections between client devices and SGD.
- **5307** - For secure (SSL-based) connections between client devices and SGD.

Note – The initial connection between a client device and SGD is *always* secure. After the user logs in to SGD, the connection is downgraded to a standard connection. When you first install SGD, TCP ports 3144 and 5307 must be open for connections to SGD. You can configure SGD to use always use secure connections.

- To run applications, SGD must be able to make TCP/IP connections to application servers. The types of applications determine which TCP ports must be open, for example:
  - **22** - For X and character applications using SSH
  - **23** - For Windows, X and character applications using Telnet
  - **3389** - For Windows applications using Windows Terminal Services
  - **6010 and above** - For X applications

The *Sun Secure Global Desktop Software 4.31 Administration Guide* has detailed information about all the ports used by SGD and how to use SGD with firewalls.

Browser-Based Webtop Requirements

To use the browser-based webtop at `http://server.example.com/sgd`, you need the SGD Client and a supported web browser.

The SGD Client can operate in two modes:

- **Webtop mode** - The SGD Client uses a special web page, called a webtop, to display the controls for a user's interaction with SGD. This is the default mode.
- **Integrated mode** - the SGD Client displays the controls for SGD in the user's desktop Start menu. Depending on other configuration factors, a web browser might 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 SGD Client is operating in integrated mode.

Supported Client Platform	Supported Web Browsers	Integrated Mode Support
Microsoft Windows Vista	Internet Explorer 7.0+ Mozilla 1.5+ Mozilla Firefox 2.0+	Microsoft Windows Start Menu
Microsoft Windows XP Professional	Internet Explorer 6.0+, 7.0+ Mozilla 1.5+ Mozilla Firefox 2.0+	Microsoft Windows Start Menu
Microsoft Windows 2000 Professional	Internet Explorer 6.0+, 7.0+ Mozilla 1.5+ Mozilla Firefox 2.0+	Microsoft Windows Start Menu
Solaris 8+ OS on SPARC platforms	Mozilla 1.5+ Mozilla Firefox 2.0+	Sun Java Desktop System Start Menu
Solaris 10 OS on x86 platforms	Mozilla 1.5+ Mozilla Firefox 2.0+	Sun Java Desktop System Start Menu
Mac OS X 10.4+	Safari 2.0+ Mozilla Firefox 2.0+	Not supported
Fedora Linux (Intel x86 32-bit) Core 6	Mozilla 1.5+ Mozilla Firefox 2.0+	Gnome or KDE Start Menu
Red Hat Desktop version 4	Mozilla 1.5+ Mozilla Firefox 2.0+	Gnome or KDE Start Menu
SUSE Linux Enterprise Desktop 10	Mozilla 1.5+ Mozilla Firefox 2.0+	Gnome or KDE Start Menu
Ubuntu 6.10	Mozilla 1.5+ Mozilla Firefox 2.0+	Gnome Start Menu

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

Web browsers must have the JavaScript™ programming language enabled.

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

- Downloading and installing the SGD Client automatically
- Displaying an application in a web browser window
- Determining proxy server settings from the user's default web browser.

If Java technology is not available, the SGD Client can be downloaded and installed manually.

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

- Sun Java Plug-in tool version 1.6.0
- Sun Java Plug-in tool version 1.5.0

Note – Sun Java Plug-in tool version 1.6.0 is the *only* supported plug-in for Microsoft Windows Vista platforms.

When users start more than one webtop session using the same client device and web browser, the webtop sessions join rather than the new session ending the existing session. For webtop sessions to join in this way, the web browser must be configured to allow permanent cookies. If permanent cookies are not allowed, webtop sessions always end and this might cause application windows to disappear.

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

Serial port mapping is only supported on UNIX, Linux, and Microsoft Windows platforms.

Classic Webtop Requirements

To use the classic webtop at `http://server.example.com/tarantella`, you need either the SGD Native Client or the Java technology client running in a web browser.

The SGD Native Clients and Java technology clients are no longer being actively developed, but they are still supported. These clients will not be available in *the next release* of SGD.

The following table lists the supported client platforms, the supported web browsers, and the supported SGD Native Clients.

Supported Client Platform	Supported Web Browsers	Supported Native Client
Microsoft Windows Vista	Internet Explorer 7.0+ Mozilla 1.5+ Mozilla Firefox 2.0+	Native Client for Microsoft Windows
Microsoft Windows XP Professional	Internet Explorer 6.0+, 7.0+ Mozilla 1.5+ Mozilla Firefox 2.0+	Native Client for Microsoft Windows
Microsoft Windows 2000 Professional	Internet Explorer 6.0+, 7.0+ Mozilla 1.5+ Mozilla Firefox 2.0+	Native Client for Microsoft Windows
Solaris 8+ OS on SPARC platforms	Mozilla 1.5+ Mozilla Firefox 2.0+	Native Client for UNIX systems
Solaris 10 OS on x86 platforms	Mozilla 1.5+ Mozilla Firefox 2.0+	Native Client for UNIX systems
Mac OS X 10.4+	Safari 2.0+ Mozilla Firefox 2.0+	Native Client for Mac OS X
Fedora Linux (Intel x86 32-bit) Core 6	Mozilla 1.5+ Mozilla Firefox 2.0+	Native Client for Linux
Red Hat Desktop version 4	Mozilla 1.5+ Mozilla Firefox 2.0+	Native Client for Linux
SUSE Linux Enterprise Desktop 10	Mozilla 1.5+ Mozilla Firefox 2.0+	Native Client for Linux
Ubuntu 6.10	Mozilla 1.5+ Mozilla Firefox 2.0+	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 tool version 1.6.0
- Sun Java Plug-in tool version 1.5.0

Because of changes to security in SGD version 4.0, you cannot use the version 4.x SGD Native Clients or Java technology clients to connect to a version 3.x SGD server. You must use a version 3.x client instead.

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

Limitation of the Classic Clients

The following are the limitations of the classic clients:

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

SGD Enhancement Module Requirements

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

- Advanced load balancing
- Client drive mapping
- Seamless windows (Windows platforms only)
- Audio (UNIX or Linux platforms only)

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

Operating System	Supported Versions
Microsoft Windows	Windows Server 2003 Windows 2000 Server Microsoft Windows XP Professional* Microsoft Windows Vista Ultimate* Microsoft Windows Vista Business*
Solaris OS on SPARC platforms	8, 9, 10
Solaris OS on x86 platforms	10
Red Hat Enterprise Linux (Intel x86 32-bit)	4, 5
Fedora Linux (Intel x86 32-bit)	Core 6
SUSE Linux Enterprise Server (Intel x86 32-bit)	9, 10

* On Microsoft Windows XP Professional and Microsoft Windows Vista platforms, only the client drive mapping component of the Enhancement Module is supported. Seamless windows and advanced load balancing are not supported

Application Servers that are not supported platforms for the SGD Enhancement Module can used with SGD to access a supported application type using any of the supported protocols.

Supported Application Types

You can use SGD 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)

Supported Protocols

SGD supports the following protocols:

- Microsoft Remote Desktop Protocol (RDP) version 5.2
- X11
- 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

SGD 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.

SGD supports Base 64-encoded PEM-format X.509 certificates that are 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 SGD 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 SGD Native Clients, you can only use HTTP and SOCKS v5 proxy servers.

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

Supported Authentication Methods

The following mechanisms are the supported mechanisms for authenticating users to SGD:

- 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

SGD works with versions 4, 5, and 6 of the RSA Authentication Manager (formerly known as RSA ACE/Server).

Supported LDAP Directory Servers

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

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

Other directory servers might 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 the following directory servers:

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

Other directory servers might work, but are not supported.

Printing Support

SGD supports printing to PostScript, PCL, and text-only printers attached to the user's client device.

The SGD `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 SGD host.

To support SGD PDF printing, Ghostscript version 6.52 or later must installed on the SGD host. The Ghostscript distribution must include the `ps2pdf` program. Microsoft Windows clients devices must have Adobe Reader version 4.0 or later.

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

When printing from a windows application that uses the Microsoft RDP protocol, SGD supports the printers supported by the Microsoft Windows application server.

Smart Card Support

SGD 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 do the following:

- 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.

SGD works with any Personal Computer Smart Card (PCSC)-compliant smart card and reader.

Logging on to a Windows Server 2003 application server using a smart card has been tested successfully with smart cards listed in the following table.

Client Operating System and Libraries	Smart Card
Microsoft Windows XP Vista	ActivCard 64K CryptoFlex 32K GemPlus GPK16000
Microsoft Windows XP Professional	ActivCard 64K CryptoFlex 32K GemPlus GPK16000
Microsoft Windows 2000 Professional	ActivCard 64K CryptoFlex 32K GemPlus GPK16000
Solaris OS with Sun Ray™ thin client PCSC Bypass package (`SUNWsrcbp`)	ActivCard 64K CryptoFlex 32K
Fedora Linux with `pcsc-lite 1.2.0`	ActivCard 64K CryptoFlex 32K GemPlus GPK16000

CHAPTER 2

New Features and Changes

This chapter describes the new features and changes in versions 4.30 and 4.31 of SGD.

Topics in this chapter include the following:

- "New Features in Version 4.31" on page 17
- "New Features in Version 4.30" on page 19
- "Changes in Version 4.31" on page 29
- "Changes in Version 4.30" on page 31

New Features in Version 4.31

This section describes the features that are new in the Sun Secure Global Desktop Software 4.31 release.

Audio Support in X Applications

SGD Administrators can now enable sound in X applications accessed using SGD.

To hear sound in X applications, the following conditions must be met:

- The client device must be capable of playing sound.
- The SGD Client or SGD Native Client must be used to connect to SGD.
- The UNIX audio module of the SGD Enhancement Module must be installed and running on the application server.

- The X application must output sound using the Open Sound System (OSS). If your system uses the Advanced Linux Sound Architecture (ALSA), you might have to enable the ALSA OSS emulation modules in the kernel.
- The SGD UNIX audio service must be enabled in Array Manager. The service is disabled by default.

The UNIX audio module contains an OSS audio driver emulator. The audio driver emulator is installed in the kernel when you install UNIX audio module of the SGD Enhancement Module.

Note – As the UNIX audio module includes an audio driver emulator, the application server itself does not actually need to have a sound card.

Some X applications are hard-coded to use the `/dev/audio` or `/dev/dsp` devices for audio output. A new attribute for X application objects, UNIX Audio - enable LD_PRELOAD (`--unixaudiopreload`), enables an SGD audio redirection library to force the X application to use the SGD audio device.

Support for the Remote Desktop on Microsoft Windows Vista

Microsoft Windows Vista includes the Remote Desktop feature that enables you to access a computer using the Remote Desktop Protocol. You can now use SGD 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 SGD Enhancement Module on Microsoft Windows Vista client devices to provide support for client drive mapping. Advanced load balancing and seamless windows are not supported.

SSH Client Settings

A new SSH Arguments (`--ssharguments`) attribute is available for the following object types:

- X application
- Character application
- 3270 application
- 5250 application

With this attribute, you can specify the command-line arguments for the SSH client when the connection method for an application is SSH.

New Features in Version 4.30

This section describes the features that are new in the Sun Secure Global Desktop Software 4.30 release.

Integration with the Desktop Start Menu

The SGD Client can now operate in either of the following modes:

- **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) displays 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, you might not need to use a web browser.

Note – Use Integrated 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, you must log in to SGD using the Login link on the 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, it has no controls for suspending and resuming applications. Instead, when you log out, the Client automatically suspends or ends all running emulator sessions. When you log in again, the Client automatically resumes all suspended sessions.

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

If you need to display a webtop, for example to 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 configure the 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 SGD, you click the Logout link on the Start menu.

For details of which desktop systems can be used with Integrated mode, see "Browser-Based Webtop Requirements" on page 5.

Single Sign-On

You can now configure the SGD Client to start 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 authenticated automatically to SGD. To obtain an authentication token, users must perform an initial log in using a web browser and then manually generate the authentication token by editing their client profile. A separate token is needed for each SGD server the user connects to.

Managing Client Configuration With Profiles

The desktop Start menu and single sign-on features mean that the SGD Client requires some configuration to connect to SGD. Not only that, different configurations might 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, version 4.3 introduces client profiles as the method for storing a group of SGD Client settings. Each client profile allows you to configure the following:

- The URL to connect to SGD
- The operating mode of the SGD Client, whether Webtop mode or Integrated mode
- Whether automatic logins are enabled
- Whether the SGD Client starts automatically when the user logs in to their client device
- Proxy server configuration, whether the settings are configured manually in the profile or determined automatically from the web browser
- Reconnection settings for controlling what happens when the SGD Client loses its connection to SGD
- Logging settings for controlling what information is written to the SGD Client log file

- The path to the PDF viewer used for PDF printing on Solaris OS, Linux, and Mac OS X clients

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

Administrators can control whether users can create and edit their own client profiles. User profile editing can be enabled globally, 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.

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

When the SGD Client connects to SGD, the profile configured for the user is copied from SGD to the client device. If a user edits their profile, the changes are stored *only* on the client device.

Mobile Proxy Server Configuration

When connecting to SGD from different locations, the SGD Client often needs different client proxy server settings. Ensuring that users have the correct proxy settings can also be difficult to administer. Version 4.3 introduces mobile proxy server configuration. With mobile proxy server configuration, the SGD Client uses the settings in the client profile to determine the proxy server settings. The proxy server settings can be specified as follows:

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

If the SGD Client is running in Integrated mode and configured to use the web browser settings, the SGD Client obtains the proxy settings by loading the URL specified in the profile in the user's default web browser. As the SGD Client caches the settings it obtains, the SGD 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 determine the proxy settings from a web browser, the web browser must have Java technology enabled.

Enhanced Command Line for the SGD Client

The command line for the SGD Client on all platforms has been enhanced to support client profiles. You can use arguments to specify the following:

- The profile to use.
- The URL to connect to SGD. This overrides the URL in the profile.
- The preferred language to use.
- The application to start. This is for launching single applications.

With the enhancements to the command line, you can create your own scripts for starting the SGD Client and for running single applications.

Manually Installable SGD Client

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

New X Server

This release includes a new X server, based on X11R6.8.2. The new X server delivers significant speed and bandwidth improvements 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`) that enables 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 Platform, Linux, and Mac OS X Clients

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

Client Platform	Default PDF Viewer
Solaris OS on SPARC technology 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 client profile used by the SGD Client.

Note – When selecting a PDF printer on UNIX platform, 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 Platform and Linux Applications

Client drive mapping is now available for UNIX platform and Linux applications. This applies to the SGD 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 platform, 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 platform, or Linux applications.

The drives that are mapped for UNIX platform, 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 platform and Linux applications, the following conditions must be met:

- The SGD Enhancement Module must be installed and running on the UNIX platform 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 SGD client drive mapping service must be started in the array using the `tarantella start cdm` command.
- The access rights to client drives must be configured in Object Manager (for Windows clients) and in the user's configuration file (UNIX platform, 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, the following conditions must be met:

- 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 enabled for either an organization, an organizational unit or a person object. Access permissions can be inherited.
- SGD clients must be able to enumerate the serial ports on client devices. The *Sun 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 SGD Client and the Native Client running on Windows, Solaris platform, and Linux client devices.

Support for the Remote Desktop on Microsoft Windows XP Professional

Microsoft Windows XP Professional includes the Remote Desktop feature that enables you to access a computer using the Remote Desktop Protocol. You can now use SGD 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 SGD Enhancement Module on Microsoft Windows XP Professional client devices 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 SGD Terminal Services Client (`ttatsc`) now supports an additional `-console` option that enables 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 Security

The initial connection between an SGD Client and an SGD server is now secured with SSL. However, after the user logs in, the connection is downgraded to a standard connection. To be able to use SSL permanently for connections to SGD, you must enable SGD security services.

TCP Port 5307 is used for SSL-based connections between SGD Clients and SGD. You might have to open this port in your firewall to allow SGD Clients to connect.

SGD has an array routes feature that allows you to configure server-side SOCKS proxy servers. You configure array routes with the following command:

```
tarantella config edit \
--tarantella-config-array-netservice-proxy-routes route ...
```

If a route includes the `:ssl` option, you must configure the SGD SSL Daemon to accept unencrypted connections using the Accept plaintext on secure port attribute on the server-specific Security Properties panel in Array Manager or with the following command:

```
tarantella config edit --security-acceptplaintext 1
```

Protecting Clients Against Unauthorized Servers

As the SGD 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 SGD.

When a user connects to a SGD 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 host name and fingerprint of the security certificate for the server they are connecting to. Users should check these details *before* clicking Yes. Once a user agrees to the connection, they are not prompted again unless there is a problem.

To ensure that users only connect to SGD servers that are trusted, SGD Administrators should do the following:

- Provide users with a list of host names 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 SGD host has its own self-signed security certificate. Administrators should obtain and install a valid X.509 certificate for each SGD host.

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

Controlled Copy And Paste

SGD 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 SGD 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 enables Administrators to secure the data available through particular applications.
- The SGD Client can be assigned a Clipboard Security Level. Data can only be copied to applications running on the client device if the SGD Client has the same Clipboard Security Level or higher as the source application. This enables Administrators to secure the flow of data outside of SGD.

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 SGD 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 SGD, 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 SGD. When you are ready to use SecurID authentication, configure the application to use the `securid/unix.exp` Login script.

Localized User Interface

Version 4.3 contains localized user interfaces for the following languages:

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

By visiting a different URL or selecting a language on the SGD Web Server home page (`http://server.example.com`), users can run a webtop in their preferred language. The SGD 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 SGD Native Client and Java technology client

Translated Documentation

The following table lists the translations of SGD Documentation that 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 are translated into Japanese.

Language Support in Expect Scripts

The Expect scripts used to start applications on application servers are enhanced to support system prompts in different languages. By default, the languages supported by SGD are supported.

To enable the Expect scripts to work with system prompts in different languages, a new Host Locale (`--hostlocale`) attribute on host objects enables you to specify the locale of the host.

Changes in Version 4.31

This section describes the changes since the Sun Secure Global Desktop Software 4.30 release.

SecurID Authentication on Solaris x86 Platforms

In version 4.31, you can use the SecurID login authority when SGD is installed on Solaris x86 platforms.

Support for Multiple SGD Servers in Integrated Mode

In version 4.30, it is possible to connect only to one SGD server when the SGD Client is in Integrated mode. In version 4.31, Integrated mode can be used with multiple SGD servers. In the desktop Start menu, a login link is available for each SGD server.

Array Routes

SGD has an array routes feature that enables you to configure server-side SOCKS proxy servers. You configure array routes with the following command:

```
tarantella config edit \
--tarantella-config-array-netservice-proxy-routes route ...
```

Array routes are enhanced so that you can now configure a direct connection type. Use `CTDIRECT` as the connection type to specify the clients that can connect without using a proxy server.

The following is an example array route:

```
"192.168.5.*:CTDIRECT:"
"192.168.10.*.*:CTSOCKS:taurus.indigo-insurance.com:8080"
```

With this configuration, clients with IP addresses beginning `192.168.5` have a direct connection. Clients with IP addresses beginning `192.168.10` connect using the SOCKS proxy server `taurus.indigo-insurance.com` on TCP port 8080.

SGD Start-up Scripts

In version 4.31, the start-up scripts that ensure SGD services stop and start when a host is rebooted are renamed and restructured. The `*Tarantella` and `*TarantellaWebserver` scripts are replaced by a single script named `*sun.com-sgd-base`. The `*tem` script for the SGD Enhancement Module is now named `*sun.com-sgd-em`.

Untrusted Initial Connection Message

The Untrusted Initial Connection warning message that displays when users first connect to an SGD server is enhanced. Users can now view the server's security certificate from this message.

Windows Key Disabled

By default, the Windows key is now disabled in SGD Windows Terminal Services sessions. The Windows key is honored in local Windows sessions only. To display the Windows Start menu in an SGD Terminal Services Session, press Alt+Home.

The SGD Terminal Services Client (`ttatsc`) now supports an additional `-windowskey on|off` option that enables you to enable support for the Windows key. You can specify this option with the Protocol Arguments (`--protoargs`) attribute on the Windows application object.

Changes in Version 4.30

This section describes the changes since the Sun Secure Global Desktop Software 4.20 release.

Single Installable Package

Version 4.3 introduces a single package for installing SGD. When you install SGD, you install all the packages that previously had to be installed separately, including the font packages. The license keys installed in the array control the SGD components that can be used.

SSL Daemon Always Running

As the initial connection to SGD is now always secure, this means that the SGD SSL Daemon is always running even if SGD security services are not enabled.

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

In previous releases, a user preferences file was used to configure the SGD Client on UNIX platform, 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.

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 is 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 might end or suspend the emulator session. The default is to end the session.

Support for PAM for UNIX Platform User Authentication

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

- ENS
- UNIX User
- UNIX Group

SGD uses PAM for user authentication, account operations and password operations.

When you install SGD on Linux platforms, Setup automatically creates PAM configuration entries for SGD 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 SGD (`tarantella`) in the `/etc/pam.conf` file if required.

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

PDF Printing

As a result of the changes introduced in this release to support PDF printing on UNIX platform, Linux, and Mac OS X client devices, the Display Adobe Reader Print dialog (`--pdfprompt`) attribute is 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 the client printer to which a print job is sent, 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, a new Use Certificates checkbox is available on the SGD Login properties panel in Array Manager. If Active Directory is configured to require client certificate and you created and installed a client certificate for SGD, then you no longer need to configure the username and password of a privileged user.

SGD Certificate Store

The password used for the SGD 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 the `keytool` application.

Licensing

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 are automatically converted and your existing Maintenance and Right to Upgrade license keys are deleted.

Application Connection Methods

From version 4.1, SGD 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.

Simultaneous Webtop Connections Attribute

From version 4.1, SGD 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 is applied.

Mainframe (3270) Applications

From version 4.0, SGD uses a different emulator for mainframe (3270) applications. 3270 character and 3270 X application objects are no longer available and are 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 are deleted when you upgrade. You must re-configure these applications.

CHAPTER 3

Support Statements, Known Issues, and Bug Fixes

This chapter contains support information for SGD.

Topics in this chapter include the following:

- "End-Of-Support Statements" on page 35
- "Retirement of the Classic Clients" on page 36
- "Known Bugs and Issues" on page 36
- "Bug Fixes in Version 4.31" on page 48
- "Bug Fixes in Version 4.30" on page 49

End-Of-Support Statements

The following table lists the end-of-support dates for SGD products.

Software and Version	End of Full Support	End of Limited Support	End of Service Life
Sun Secure Global Desktop Software 4.2	November 8, 2008	November 8, 2012	November 8, 2012
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 3.44*			December 31, 2007
Secure Global Desktop Enterprise Edition 3.42			March 31, 2007
Tarantella Enterprise 3 (including TASP)			March 31, 2007

* Japanese only

For details of the Sun End of Service Life (EOSL) Policy, see `http://www.sun.com/service/eosl/`.

Customers with a valid support agreement can upgrade to the latest version of SGD free of charge.

Retirement of the Classic Clients

SGD version 4.31 is the last release to contain the Java technology clients, the SGD Native Clients and the classic webtop. The next release will not contain these clients.

As a result of this change, from the next release of SGD, you cannot configure applications to display in a web browser window. The webtop and new browser options for the Display Using attribute (`--displayusing`) will be removed.

Known Bugs and Issues

This section lists the known bugs and issues with SGD version 4.31.

602423 - Return Key and Keypad Enter Key Issues

Problem: SGD 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 SGD 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.

Note – The Java technology clients are unable to distinguish between Return and the keypad Enter key.

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* or *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
```

Caution – The X keymap is a global user resource, so all applications for that user might be affected by this change. If any of these applications do not handle `KP_Enter`, then you might need to consult your X or Windows application vendor for assistance.

6375418 - Non-ASCII Characters in Input Method Windows

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.

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

The *Sun Secure Global Desktop Software Administration Guide* has more detailed information on using your own X fonts.

▼ How to Add Font Path Configuration

The following instructions assume that the SGD server is installed on a Solaris 10 OS platform and that 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 SGD host.**

```
svcadm restart xfs
```

3. **Configure SGD with the location of the font server.**

   a. **In Array Manager, select X Protocol Engine properties.**

   b. **In the Font Path box, type the details of the font server.**

      For example, `tcp/boston:7100`

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

6443840 - Automatic Proxy Server Configuration Scripts Fail

Problem: Proxy server automatic configuration scripts can specify a list of proxy servers to try. If the first proxy server in the list is unavailable, the browser tries the other proxy servers in turn until it finds one that is available.

If you are using Microsoft Internet Explorer with Sun Java Plug-in tool version 1.5.0, only the first proxy server in the list is used. If that proxy server is not available, the connection fails.

Cause: A known issue.

Solution: Use Sun Java Plug-in tool version 1.6.0.

6448990 - Backslash and Yen Keys Problems

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

Cause: A known 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

Problem: On Solaris 10 x86 platforms, enabling Integrated mode when you are logged in as the `root` user does not add applications to the desktop Start menu. You might 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: No solution is currently available.

6458111 - Gnome Main Menu Crashes Using Integrated Mode

Problem: On client devices running SUSE Linux Enterprise Server 10, the Gnome Main Menu crashes when using the SGD Client in Integrated mode. 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
```

6540417 - Printer Preferences Are Not Stored

Problem: When a user changes their printer preferences in a Windows application that is configured to use the RDP protocol, the changes are not stored. When they use the application again, the original printer preferences are set.

Cause: A known issue.

Solution: The workaround is to set the color depth of the application object to match the number of colors supported by the Microsoft Windows application server. By default, SGD Windows applications use 16-bit color. Microsoft Windows 2000 application servers only support 8-bit color.

6544844 - Printing Fails if SELinux is Enforcing

Problem: When SGD is installed on Red Hat Enterprise Linux 5 platforms, printing fails if the SELinux Setting is set to enforcing.

Cause: A known issue.

Solution: The workaround is to change the SELinux Setting to permissive or disabled.

6544890 - Enhancement Module Start-up Script Error

Problem: On Solaris OS platforms, if you run the system start-up script for the SGD Enhancement Module (`/etc/init.d/sun.com-sgd-em`) manually to start or restart the Enhancement Module, the following error displays:

```
Starting Sun Secure Global Desktop Enhancement Module       failed
```

Cause: A missing lock file directory.

Solution: The error can be ignored safely. The SGD Enhancement Module is started.

6461864 and 6476661 - Automatic Login and Integrated Mode Fails With the Gnome Desktop

Problem: After enabling Automatic Client Login or Integrated mode, the SGD Client does not start automatically when you log in to the Gnome Desktop and the Start menu is not updated with webtop content when you log in to SGD. This problem affects SUSE Linux Enterprise Server 9 and Red Hat Enterprise Linux 4.

Cause: 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 `pkill gnome-panel` command to restart the gnome-panel and pick up new menu information.

Note – You must run the `pkill gnome-panel` command to update the menu *each time* the menu changes.

6468716 - Keyboard Does Not Work in Gnome Sessions

Problem: After starting a Gnome session on Solaris 10 OS on Sparc platforms, users are unable to input anything with the keyboard. The mouse, however, does work.

Cause: A known bug with remote Gnome sessions. The Sun Microsystems bug reference is 6239595.

Solution: This problem was fixed in patch number 119542. This patch was also included in a cumulative patch ID 122212 for the Gnome Desktop.

The workaround is to create a Gnome configuration file `/etc/gconf/gconf.xml.defaults/apps/gnome_settings_daemon/keybindings/%gconf.xml` with the following content:

```
<?xml version="1.0"?>
<gconf>
<entry name="volume_up" mtime="1110896708" type="string">
<stringvalue></stringvalue>
</entry>
<entry name="volume_mute" mtime="1110896705" type="string">
<stringvalue></stringvalue>
</entry>
<entry name="volume_down" mtime="1110896702" type="string">
<stringvalue></stringvalue>
</entry>
```

```
<entry name="help" mtime="1110896698" type="string">
<stringvalue></stringvalue>
</entry>
</gconf>
```

6470197 - Compiling SGD Web Server Modules Fails

Problem: When you compile your own Apache modules for use with the SGD 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 SGD 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 - No KDE Desktop Menu Item for the SGD Client

Problem: Shortcuts for the SGD 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 Login menu for the SGD Client in Integrated mode not to display.

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

```
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 automatically use this setting.

6477187 - Client Drive Mapping Fails Without the Client for Microsoft Networks

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.

▼ How to Enable the Client for Microsoft Networks

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

6480880 - SGD Client Fails With Relocated Webtops

Problem: If you relocate the browser-based webtop to your own JavaServer Pages™ (JSP™) software container, the Client refuses to connect to SGD when it is Integrated mode.

Cause: The SGD Client requires some files from the Axis web application.

Solution: Copy the Axis web application to the remote host. Copy everything in the `/opt/tarantella/webserver/tomcat/`*version*`/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 Not Used During Installation

Problem: When you install SGD 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 SGD.

6481312 - Upgrading Resets the Available Connection Types

Problem: After upgrading to version 4.3, a server that was configured to accept only secure connections now accepts standard and secure connections.

Cause: A known issue.

Solution: Re-configure the server to accept only secure connections. In Array Manager, on the Security Properties panel for the server, uncheck the box next to Standard connections. Alternatively run the following command:

```
tarantella config edit --security-connectiontypes ssl
```

6482912 - SGD Client Not Installed Automatically

Problem: Using Internet Explorer 7 on Microsoft Windows Vista platforms, the SGD Client cannot be downloaded and installed automatically. 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 SGD Client from downloading and installing automatically.

Solution: Add the SGD server to the list of Trusted Sites in Internet Explorer's Security Settings.

6486551 - Unavailable Application Server Not Detected

Problem: The Fewest Application Sessions method of load balancing applications does not detect when an application server is unavailable to launch applications. The result is that SGD tries to launch an application on a server that is not available and it does not fail over to the next available host.

Cause: A known issue.

Solution: This problem will be fixed in a future release of SGD.

The workaround is to edit the host object in Object Manager and uncheck the box for the Available to launch applications attribute (`--available false`). This removes the host from the list of servers that can run applications.

6528952 - SGD Audio Driver Not Installed on Upgrade

Problem: The SGD Enhancement Module version 4.31 has a UNIX audio module that includes a kernel audio driver. If you upgrade a version 4.31 SGD Enhancement Module, a "Driver (sgdadem) not installed" message displays.

Cause: Kernel modules cannot be removed if they are in use.

Solution: The message can be ignored. The SGD audio driver has never changed.

Sun Type 7 Japanese Keyboard Issues

Problem: Users with Sun Type 7 Japanese keyboards cannot input characters correctly using SGD.

Cause: Missing Solaris OS keytable on the client device.

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

Platform	Patch
Solaris 10 OS on SPARC platforms	121868
Solaris 9 OS on SPARC platforms	113764
Solaris 8 OS on SPARC platforms	111075

Platform	Patch
Solaris 10 OS on x86 platforms	121869
Solaris 9 OS on x86 platforms	113765
Solaris 8 OS on x86 platforms	114539

Start Menu Items Not Sorted Alphabetically

Problem: When using the SGD Client in Integrated mode on Microsoft Windows client devices, users might 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.

No Start Menu Entries on Sun Java Desktop Systems

Problem: On Sun Java Desktop Systems, users may find that Start menu entries are not created for SGD 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 for Solaris OS on SPARC technology platforms
- 119907 for Solaris OS on x86 platforms

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

Bug Fixes in Version 4.31

The following table lists the significant bugs that are fixed in the 4.31 release.

Reference	Description
2140625	Time zone redirection is fixed for clients on UNIX platforms.
2145026	Licensing information is not copied to all the secondaries until after a restart.
2145602	X application launch is slow or times out. Possible error in the Input Method handling in the `procs.exp` script.
2145932	Windows key functionality is being held when returning to SGD session.
2146043	Using client drive mapping, you cannot overwrite a larger file.
2146285	Tomcat fails and icons do not appear on the webtop.
6440254	The proxy server authentication dialog does not display realm information.
6443192	Upgrading using the `pkgadd` command on Solaris OS reports hundreds of file conflicts.
6443840	The SGD Client does not understand proxy failover from proxy server configuration (PAC) files
6474180	The `HARD_SERVER_LIMIT` of the SGD Web Server isincreased to 1024.
6480225	In Integrated mode, applications fail to resume on UNIX client platforms.
6494450	Client drive mapping cannot handle files larger than 2 gigabytes.
6499639	A recursive directory request causes a segmentation fault when using client drive mapping on UNIX and Linux platforms.
6503627	The `xfrbelgian.txt` keyboard map file contains a mistake.
6518152	Start menu is not updated on a using Integrated mode on Microsoft Windows Vista client devices.
6518638	The `tarantella print cancel` command deletes all print jobs instead of just the selected job.
6525384	XRDP does not work with SGD.
6528037	Page Not Found displays on the webtop when a group containing hosts is deployed by mistake to a webtop.
6506222	A user's `.Xdefaults` file is not used when launching an application.

Bug Fixes in Version 4.30

This section lists the significant bugs that are fixed in the 4.30 release. The bug fixes are divided into the following areas:

- "Administration Tools" on page 49
- "Application Launch" on page 50
- "Clients and Webtop" on page 50
- "Emulation" on page 51
- "Installation and Upgrade" on page 52
- "Internationalization and Localization" on page 52
- "Other" on page 53
- "Printing" on page 54
- "Security" on page 54
- "Server" on page 55
- "User Authentication" on page 55
- "Web Services" on page 56

Administration Tools

The following bugs with the SGD administration tools are fixed.

Reference	Description
6433525	`/usr/bin` owner is changed to ttasys on startup.
6436735	The `tarantella object new_xapp` command does not accept the `--accel` 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 must not be passed using environment.
6450323	Attributes cannot be specified in object creation but can be set in object edit.
6451537	`tarantella license` commands and Array Manager display obsolete software components.

Application Launch

The following bugs with launching applications are fixed.

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 `optimizelaunch` enabled in the `unix.exp` login script, the expired password handler does not work.
6405808	The filtering script (`runsubscript.exp`) 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 occurs when the host is not known to SSH.
6434660	Password expiry handling on application launch is broken.
6447551	There should only be one ttacpe process created for each webtop session.
6455378	Launch failure when SSH used over `su` for an application running on the SGD 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 are not recognized and cause a prompt when launching in-place applications.
6476180	Root window stays around when logging out of a kiosk Gnome session.

Clients and Webtop

The following bugs with the SGD clients and webtop are fixed.

Reference	Description
6408157	Local X server application does not launch from the JSP software 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.

Reference	Description
6417631	UNIX Native Client: redraw problems with kiosk applications.
6424776	SGD Client produces errors and exits when logging out of the webtop.
6432133	The SGD Native Client causes a segmentation fault if you close the connection progress window.
6465959	When SGD restarts, the SGD Client spins and sends out hundreds of network packets.
6468173	On Sun Ray thin clients, the wait cursor is no longer set permanently.

Emulation

The following emulation bugs are fixed.

Reference	Description
6381531	Edited `colormap.txt` intermittently ignored when security is enabled.
6386091	SGD Native Client for Windows 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` exits with a segmentation fault.
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	Performance improvements for Windows applications.
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 saving time. Time always out by one hour.
6472959	ESC-NumLock does not work as expected from Solaris OS client and Sun Ray thin clients.

Installation and Upgrade

The following installation and upgrade bugs are fixed.

Reference	Description
6355269	The default configuration for a Java Desktop System 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 and server does not start.
6407985	SGD incorrectly handles large amount of free disk space at install.
6430913	Web server configuration file (`httpd.conf`) is not upgraded correctly.
6446020	Unable to uninstall SGD if the external DNS name is incorrect.
6453638	Cannot log in to a SGD server after an upgrade.
6462429	SGD is uninstalled even though user selects No.

Internationalization and Localization

The following internationalization and localization bugs are fixed.

Reference	Description
6354105	In Configuration Wizard, the application list shows corrupt strings with multi-byte characters.
6355226	The Connection Progress dialog cannot display multi-byte 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 `native-cdm-config` file.
6419511	Windows applications should have Unicode as the Euro symbol default.

Reference	Description
6419523	Server LANG environment overrides client locale setting.
6447594	Client window mode should be accessed with an IP address instead of UNIX platform socket.
6450008	Cannot generate an apostrophe with a Swedish keyboard.

Other

The following miscellaneous bugs are fixed.

Reference	Description
6375600	Authentication fails with ActivCard - Cyberflex 64k Smart Card (also bug ref 607218).
6384746	Able to read Common Gateway Interface Files (`.cgi`) files using a web browser.
6390126	A large number of users logging in in quick succession hangs the SGD server.
6393623	New browser window gets launched when new browser windows applications are launched with the CTRL key pressed.
6407855	SGD 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	SGD Enhancement Module for Solaris OS x86 platforms appears to fail.
6409765	Error copying large files from client to server over a slow network in RDP sessions.
6410161	Using telnet to connect to localhost port 1023 causes the Protocol Engine Manager to use 100% CPU.
6416384	RDP-based audio output stops playing when using a Sun Ray thin client.
6418965	Client window manager applications display Minimize and Maximize buttons that are not present in original application.
6430243	SGD 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 the keepalive to 0 causes keepalives to be sent continuously.
6442142	Quitting Gnome session causes ttaxpe to use 100% CPU.
6446271	SGD Web Server starts but remains attached to the console.
6466415	Secure LDAP does not work without security licenses installed.

Printing

The following printing bugs are fixed.

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 no printer is configured on the client device.
6427852	Login delay induced by inaccessible network printer attached to client device.

Security

The following security bugs are fixed.

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 expires.
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	SSL daemon core dumps due to `sigsegv`, signal 11.
6469123	OpenSSL security patch secadv_20060905.txt needs to applied.
6476728	OpenSSL security patch secadv_20060928.txt needs to be applied.
6478735	Fixed a vulnerability with the SGD Cascading Stylesheets.

Server

The following bugs with SGD servers and arrays are fixed.

Reference	Description
6379743	`tarantella status` 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

The following bugs with user authentication are fixed.

Reference	Description
6383417	If the `krb5.conf` file has errors, user login hangs and the server continuously writes exceptions to `jserver.log`.
6400123	Ambiguous login is not allowed if invalid credentials are provided the first time.
6415709	Active Directory authentication fails silently if one tree of a forest is not configured in the `krb5.conf` file.
6439688	SGD Native Client for Windows 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 is not recognized when using SGD (fixed for Windows Clients only).
6465569	Active Directory PKI infrastructure does not failover to the next global catalog server.
6471877	SecurID login authority does not work correctly.

Web Services

The following bugs with SGD web services are fixed.

Reference	Description
6391262	Anonymous users can create and edit webtop groups. This information is stored on disk and not cleaned up.
6427185	SGD Web Server exposes too much information.