

Sun™ Ray™ Enterprise Server Software 1.1 Administrator's Guide



THE NETWORK IS THE COMPUTER™

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900 USA
650 960-1300 Fax 650 969-9131

Part No. 805-7915-11
April 2000, Revision A

Send comments about this document to: docfeedback@sun.com

Copyright 2000 Sun Microsystems, Inc., 901 San Antonio Road • Palo Alto, CA 94303-4900 USA. All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Portions of this product may be derived from the UNIX® system, licensed from Novell, Inc., and from the Berkeley 4.3 BSD system, licensed from the University of California. UNIX is a registered trademark in the United States and in other countries and is exclusively licensed by X/Open Company Ltd. Third-party software, including font technology in this product, is protected by copyright and licensed from Sun's suppliers. RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a).

Sun, Sun Microsystems, the Sun logo, Sun Ray, Sun WebServer, ShowMe TV, SunCamera, Java, JDK, docs.sun.com, and Solaris are trademarks, registered trademarks, or service marks 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 an architecture developed by Sun Microsystems, Inc.

Netscape and Netscape Navigator are trademarks or registered trademarks of Netscape Communications Corporation in the United States and other countries.

Adobe® is a registered trademark of Adobe Systems, Incorporated.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

This product uses CryptoLib 1.2. The authors of CryptoLib are Jack Lacy, Don Mitchell, and Matt Blaze. Copyright (c) 1991, 1992, 1993, 1994, 1995 by AT&T. Permission to use, copy, and modify this software without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software. NOTE: Some of the algorithms in cryptolib may be covered by patents. It is the responsibility of the user to ensure that any required licenses are obtained. SOME PARTS OF CRYPTOLIB MAY BE RESTRICTED UNDER UNITED STATES EXPORT REGULATIONS. THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHORS NOR AT&T MAKE ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE. U.S. Government approval required when exporting the product.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a).

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 2000 Sun Microsystems, Inc., 901 San Antonio Road • Palo Alto, CA 94303-4900 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système UNIX® licencié par Novell, Inc. et du système Berkeley 4.3 BSD licencié par l'Université de Californie. UNIX est une marque enregistrée aux Etats-Unis et dans d'autres pays, et licenciée exclusivement par X/Open Company Ltd. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Sun, Sun Microsystems, the Sun logo, Sun Ray, Sun WebServer, ShowMe TV, SunCamera, Java, JDK, docs.sun.com, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, 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.



Netscape et Netscape Navigator est une marque de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays.

Adobe est une marque enregistree de Adobe Systems, Incorporated.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

Ce produit utilise CryptoLib 1.2. Les auteurs de CryptoLib sont Jack Lacy, Don Mitchell et Matt Blaze. Copyright (c) 1991, 1992, 1993, 1994, 1995 AT&T. Le présent avis autorise l'utilisation, la copie et la modification de ce logiciel sans redevance aucune, à condition que ce même avis figure dans son intégralité sur toutes les copies de tout logiciel qui soit ou inclue une copie ou une modification de ce logiciel ainsi que sur toutes les copies de la documentation d'accompagnement de ce logiciel. REMARQUE : Il est possible que certains algorithmes de Cryptolib soient protégés par des brevets. Il incombe à l'utilisateur de s'assurer qu'il dispose des éventuelles licences nécessaires. L'EXPORTATION DE CERTAINES PARTIES DE CE PRODUIT EST LIMITEE PAR LA REGLEMENTATION DES ETATS-UNIS EN MATIERE D'EXPORTATION. CE LOGICIEL EST FOURNI "EN L'ETAT", SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE. EN PARTICULIER, PAS PLUS LES AUTEURS QU'AT&T N'OFFRENT DE GARANTIE COMMERCIALISATION OU L'ADEQUATION A UN USAGE PARTICULIER.

CETTE PUBLICATION EST FOURNIE "EN L'ETAT" ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDEE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A REpondre A UNE UTILISATION PARTICULIERE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT NUL ET NON AVENU.



Please
Recycle



Adobe PostScript

Contents

Preface xvii

1. Sun Ray System Overview 1

Accessing the Latest Sun Ray Information 1

What's New in Version 1.1 1

Improvements Over Previous Release 2

Patches Included in Release 2

Installation and Upgrade Script 3

New Administration Application 3

New Features in this Release 3

Failover Capability 3

Additional Smart Card Support 3

Sun Enterprise 10000 Server Support Provided 4

Sun Ray System 5

Sun Ray Hardware 6

Sun Ray Server 6

Sun Ray 1 Enterprise Appliance 6

Firmware Module 7

Front Panel Features 7

Back Panel Features 8

Video Capabilities	10
Audio Capabilities	10
Power Cycling Requirements	14
Sun Ray Interconnect Fabric	14
Workgroup Scenario	14
Department Scenario	16
Connecting Sun Ray Enterprise Appliances with Other Devices	17
Sun Ray Server Software	17
Authentication Manager	19
Mobility—Hot Desking	21
Session Manager	22
Sessions and Services	23
Changes in a Session	23
Session Manager Port	24
Administering Sun Ray Server Ports	24
Virtual Device Drivers	24
Determining 8-Bit Status	25
OpenGL Considerations	25
2. Sun Ray Software and Hardware Requirements	27
Software Requirements	27
Solaris Operating Environment	27
Other Software	28
Web Server Conditions	28
Web Browser Conditions	28
LDAP Server Conditions	28
Patch Requirements	29
Hardware Requirements	29

Minimal Hardware Requirements	29
Sizing Hardware Requirements	30
Requirements for Servers	30
Hardware Systems	30
Disk Space	31
Memory	32
Ethernet Card	33
Requirements for the Interconnect Fabric Components	34
Network Considerations	34
Specifications for Switches	34
Specifications for Hubs	35
Specifications For Cable	35
Specifications for the Sun Ray 1 Enterprise Appliance Components	36
Specifications for Monitors	36
Specifications for Keyboards and Mice	37
Specifications for Smart Cards	37
Specifications for Other Devices	37
3. Configuring the Software	39
LDAP Datastore Entry Limitations	39
LDAP Entry Formula	40
Collecting Key Configuration Parameters	40
Configuration Worksheet	40
Using the Configuration Script	43
▼ To Run the Configuration Script	43
Testing the Installation and Configuration	47
▼ To Test the Command-Line Interface of the Administration Application	47
▼ To Test the Web-Based Interface of the Administration Application	47

- 4. SSL Certificate Configuration 49**
 - Secure Socket Layer Certificate 49
 - Local Root Certificate Authority 50
 - Distinguished Name 50
 - Required Information 51
 - Configuring SSL 51
 - ▼ To Configure SSL on the Primary Sun Ray Server 52
 - ▼ To Configure Certificates on Failover Servers 54
 - Troubleshooting SSL Configuration 55
 - ▼ To Remove All SSL Information 55

- 5. Initial Setup 57**
 - Using the Default System Configuration 57
 - Configuring the Sun Ray Interconnect Fabric 58
 - A Note to Sun Enterprise 10000 Administrators 59
 - ▼ To Configure the Interconnect 59
 - Setting System Parameters 62
 - ▼ To Set System Parameters 62

- 6. Administering the Sun Ray System 65**
 - Interfaces on the Sun Ray Interconnect Fabric 65
 - ▼ To Add an Interface 66
 - ▼ To Delete an Interface 66
 - ▼ To Remove All Interfaces 67
 - ▼ To Print the Sun Ray Interconnect Configuration 67
 - PROM Version Management 67
 - Examples 68
 - ▼ To Disable the `utload` Command 69
 - ▼ To Enable the `utload` Command 69

Choosing an Authentication Policy	70
Enabling an Authentication Policy	71
▼ To Enable an Authentication Policy	71
▼ To Configure a Token Reader	73
utpolicy Considerations	73
Changing Policies and the utpolicy Command	73
Removing Old Policies	75
User Management	76
Printer Administration	76
Defining Desktop Properties	76
Using Sun Ray 1 Settings	77
Configuring Sun Ray 1 Settings	79
▼ To Change the Hot Key Setting (Non-Sun Keyboards) Sitewide	80
▼ To Change the Hot Key Setting (Non-Sun Keyboards) for a User	81
Session Manager	81
▼ To Restart the Session Manager	82
System Monitoring	82
▼ To List All X Servers Running	82
▼ To Search for Runaway Processes	82
▼ To Start the OpenWindows™ Performance Meter for Server Statistics	84
▼ To Check Network Packets	84
▼ To Check Network Status	84
▼ To Access DHCP Information	85
7. Administration Application	87
Administration Application Overview	87
Sun Ray 1 Appliances	87
Sun Ray Users	88

Administration Data	89
Token Readers	89
Using the Administration Application	91
Web-Based Interface (Logging In)	91
▼ To Log Into the Web-Based Interface	91
Command-Line Interface	95
▼ To Use the Command-Line Interface	95
8. Managing Sun Ray 1 Appliances	97
Main Administration Page	98
Changing the Administrator's Password	99
▼ To Change the Administrator's Password	99
Viewing System Status	100
▼ To View System Status	100
Listing All Desktops	103
▼ To List All Desktops From the Web-Based Interface	103
▼ To List All Desktops From the Command-Line Interface	104
Searching for Desktops	105
▼ To Search for Desktops From the Web-Based Interface	105
▼ To Search for Desktops From the Command-Line Interface	106
Listing Currently Connected Desktops	107
▼ To List Currently Connected Desktops From the Web-Based Interface	107
▼ To List Currently Connected Desktops From the Command-Line Interface	108
Listing Desktops in Dump Format	108
▼ To Output the Desktop List in Dump Format From the Command-Line Interface	109
Displaying a Desktop's Current Properties	109

- ▼ To Display a Desktop's Current Properties From the Web-Based Interface 109
- ▼ To Display a Desktop's Current Properties From the Command-Line Interface 111
- Editing Single Desktop's Properties 112
 - ▼ To Edit Single Desktop's Properties From the Web-Based Interface 112
 - ▼ To Edit Single Desktop's Properties From the Command-Line Interface 113
- Editing the Properties of Multiple Desktops 113
 - ▼ To Edit the Properties of Multiple Desktops From the Command-Line Interface 114
- Viewing Failover Group Status 115
 - ▼ To View Failover Group Status 116
 - Interpreting Failover Group Status Information 117
 - Example Configurations 118
- Examining Log Files 121
 - Viewing Message Logs 122
 - ▼ To View Messages Logs 122
 - Viewing Authentication Logs 123
 - ▼ To View Authentication Logs 123
 - Viewing Administration Logs 123
 - ▼ To View Administration Logs 124
 - Viewing Archived Logs 125
 - ▼ To View Archived Logs 125
- Reset/Restart Sun Ray Services 126
 - ▼ To Reset Sun Ray Services 126
 - ▼ To Restart Sun Ray Services 126
- Locating Token Readers 127
 - ▼ To Locate Token Readers 127
- Restarting Sun Directory Services 128

▼	To Restart Sun Directory Services	128
	Changing Policies	129
	Solaris Authentication Considerations	129
	Changing the Local/Group Policy	129
▼	To Change the Local/Group Policy	129
	Accessing Online Documentation	131
▼	To Access Online Documentation	131
	Smart Card Usage and Solaris Lock Screen	132
	End Users Using CDE	132
	End Users Using OpenWindows	132
	System Wide Default	133
	Ordering Sun Ray 1 Smart Cards	133
9.	Managing Sun Ray Users	135
	User Fields	136
	Adding and Deleting Users	136
	Adding a Single User	136
▼	To Add a Single User From the Web-Based Interface	136
▼	To Add a Single User From the Command-Line Interface	138
	Adding Multiple Users	139
▼	To Add Multiple Users From the Command-Line Interface	139
	Deleting a Single User	141
▼	To Delete a Single User From the Web-Based Interface	141
▼	To Delete a Single User From the Command-Line Interface	142
	Deleting Multiple Users	142
▼	To Delete Multiple Users From the Command-Line Interface	142
	Finding Users	144
	Listing All Users by ID	144

- ▼ To List All Users by ID From the Web-Based Interface 144
- ▼ To List All Users by ID From the Command-Line Interface 145

Viewing All Users by Name 146

- ▼ To View All Users by Name From the Web-Based Interface 146

Searching for Desktops (Users) 147

- ▼ To Find a Desktop (User) From the Web-Based Interface 147
- ▼ To Search for Users from the Command-line Interface 148

Listing Current Users 149

- ▼ To List Currently Logged In Users From the Web-Based Interface 149
- ▼ To List Currently Logged In Users From the Command-Line Interface 150

Listing Users in Dump Format 151

- ▼ To Output the User List in Dump Format From the Command-Line Interface 151

User Properties 152

Displaying Properties 152

- ▼ To Display a User's Current Properties From the Web-Based Interface 152
- ▼ To Display a User's Current Properties From the Command-Line Interface 155

Editing a Single User's Properties 155

- ▼ To Edit a Single User's Properties From the Web-Based Interface 155
- ▼ To Edit a Single User's Properties From the Command-Line Interface 157

Editing Multiple Users' Properties 157

- ▼ To Edit Multiple Users' Properties From the Command-Line Interface 157

Administering Tokens 159

Adding a Token to a Single User 159

- ▼ To Add a Token to a User From the Web-Based Interface 159

- ▼ To Add a Token to a User From the Command-Line Interface 159
- Deleting a Token From a Single User 161
- ▼ To Delete a Token From a User from the Web-Based Interface 161
- ▼ To Delete a Token From a User From the Command-Line Interface 161
- Enabling or Disabling a User's Token 162
- ▼ To Enable or Disable a User's Token From the Web-Based Interface 162
- ▼ To Enable or Disable a User's Token From the Command-Line Interface 162
- Getting a Token ID From a Token Reader 163
- ▼ To Get a Token ID from a Token Reader From the Web-Based Interface 163
- ▼ To Get a Token ID From a Token Reader From the Command-Line Interface 164
- Managing Smart Cards From Different Vendors 165
- ▼ To View/List The Configured Smart Cards 165
 - ▼ To View/List The Configured Smart Cards From the Command-Line Interface 167
- ▼ To View the Properties for a Particular Smart Card 168
 - ▼ To View The Properties of Smart Cards From the Command-Line Interface 168
- Smart Cards Probe Order 169
- ▼ To View The Smart Card Probe Order 169
 - Changing the Smart Card Probe Order 169
- ▼ To Change the Smart Card Probe Order 169
 - ▼ To Change The Smart Card Probe Order From the Command-Line Interface 170
- Adding Smart Cards 171
- ▼ To Add a Smart Card 171
- ▼ To Add a Smart Card From the Command-Line Interface 173

	Deleting Smart Cards	173
▼	To Delete a Smart Card	173
▼	To Delete a Smart Card From the Command-Line Interface	174
	Smart Card Vendor Configuration Files	175
▼	To Load A Configuration File Into the Directory	175
▼	To Load/Add A Configuration File Into the Database	175
▼	To Verify the Configuration File Addition	176
	OpenWindows Considerations	178
▼	To Alter OpenWindows Properties	178
10.	Removing the Sun Ray Software	179
	Using Scripts to Uninstall the Software	179
▼	To Unconfigure the Sun Ray Server Software	180
▼	To Uninstall the Sun Ray Software	183
	Manually Uninstalling the Software	186
▼	To Remove the Sun Ray Server Software	186
	SunDS 3.1 and Sun WebServer 2.1	187
A.	Troubleshooting	189
	Appliance Questions	189
▼	To Power Cycle a Sun Ray 1 Appliance	196
	User Questions	196
▼	To Modify the Time-Out Value	200
	Server Questions	201
B.	The Green Newt Cursor	205
	Is There Really a Problem?	205
	Is the Problem Caused by Hardware?	206
	Is the <code>dtlogin</code> Daemon Up-to-Date?	206

Is the <code>dtlogin</code> Session Hung?	207
▼ To Identify and Unconfigure the <code>dtlogin</code> Session	208
Are the Configuration Files Corrupt?	209
▼ To Determine the Integrity of the Configuration Files	210
▼ To Replace the <code>Xservers</code> and <code>Xconfig</code> Files	211
C. Security	213
Physical Access	214
Superuser Access	214
Sun Ray User	214
Non-Sun Ray Clients on the Interconnect	215
Switches	215
D. Tips for Using Non-Sun Web Servers	217
E. Tips for Language Selection	219
Language Selection for System Administrators	219
Sun Ray Web-based Interface of the Administration Application	219
Self-Registration GUI	220
Input to the Self-Registration GUI	220
Language Selection for Users	221
Using Solaris <code>admintool(1m)</code> in non-English locales	221
Henkan Key or Hangul Key	222
F. Errors From the Authentication Manager	223
Message Format	223
Error Messages	225
Glossary	235
Index	241

Preface

The *Sun Ray Enterprise Server Software 1.1 Administrator's Guide* provides instructions for setting up, administering, and monitoring a system of Sun Ray™ 1 enterprise appliances. These instructions are designed for an experienced system administrator with networking knowledge.

Before You Read This Book

Read the *Sun Ray Enterprise Server Software 1.1 Product Notes* and the *Sun Ray Enterprise Server Software 1.1 Installation Guide*.

This guide assumes that you have installed the Sun Ray server software on your server from the Sun Ray enterprise server software 1.1 CD and that you have added the required patches.

How This Book Is Organized

Chapter 1 describes the Sun Ray 1 hardware and how the Sun Ray software works.

Chapter 2 describes the hardware and software requirements for a Sun Ray system. It also gives the specifications for hardware that is compatible with the Sun Ray 1 hardware.

Chapter 3 describes how to configure the Sun Ray server software and the supporting software.

Chapter 4 describes how to configure a secured socket layer (SSL) for increased security.

Chapter 5 describes how to configure a default Sun Ray system.

Chapter 6 details how to modify the Sun Ray system from the available options.

Chapter 7 introduces the Sun Ray administration application, which is used to manage Sun Ray users and Sun Ray 1 enterprise appliances.

Chapter 8 describes how to use the Sun Ray administration application to manage Sun Ray 1 enterprise appliances.

Chapter 9 describes how to use the Sun Ray administration application to manage Sun Ray users.

Chapter 10 describes how to remove the Sun Ray server software from the server.

Appendix A provides troubleshooting information.

Appendix B provides information on the green newt cursor.

Appendix C provides security information.

Appendix D provides tips for using non-Sun™ web servers.

Appendix E describes the different components in the Sun Ray server software where a language selection can be made.

Appendix F lists error messages from the Authentication Manager and their meanings.

Using UNIX Commands

This document does not contain information on basic UNIX® commands and procedures such as shutting down the system, booting the system, or configuring devices. For this information, see the AnswerBook2™ online documentation for the Solaris™ 2.6 or 7 software environment.

This document does contain information about unique Sun Ray system commands.

Typographic Conventions

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; on-screen computer output.	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. % You have mail.
AaBbCc123	What you type, when contrasted with on-screen computer output.	% su Password:
<i>AaBbCc123</i>	Book titles, new words or terms, words to be emphasized. Command-line variable; replace with a real name or value.	Read Chapter 6 in the <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be <code>root</code> to do this. To delete a file, type <code>rm filename</code> .

Shell Prompts

TABLE P-2 Shell Prompts

Shell	Prompt
C shell	<i>machine_name</i> %
C shell superuser	<i>machine_name</i> #
Bourne shell and Korn shell	\$
Bourne shell and Korn shell superuser	#

Documentation Set

The Sun Ray enterprise server software includes documentation available as

hardcopy or online.

TABLE P-3 Sun Ray Enterprise Server 1.1 Documentation Set

Title	Part Number	Location
<i>Sun Ray Enterprise Server Software 1.1 Product Notes</i>	805-7918-11	Hardcopy, in box
<i>Sun Ray Enterprise Server Software 1.1 Installation Guide</i>	805-7916-11	Hardcopy, in box
<i>Sun Ray Enterprise Server Software 1.1 Administrator's Guide</i>	805-7915-11	On CD, in /cdrom/cdrom0/docs/C directory (this document)
<i>Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide</i>	806-4181-10	On CD, in /cdrom/cdrom0/docs/C directory

Related Documentation

TABLE P-4 Related Documentation

Title	Part Number	Location
<i>Sun Ray 1 Troubleshooting Guide</i>	805-7871-11	Hardcopy, in Sun Ray 1 appliance box
<i>Sun Ray 1 Safety and Compliance Guide</i>	805-7870-10	Hardcopy, in Sun Ray 1 appliance box
<i>Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide</i>	806-4181-10	On CD, in /cdrom/cdrom0/docs/C directory

Accessing Sun Documentation Online

The docs.sun.comSM web site enables you to access SunTM technical documentation on the Web. You can browse the docs.sun.com archive or search for a specific book title or subject at:

<http://docs.sun.com>

Sun Welcomes Your Comments

We are interested in improving our documentation and welcome your comments and suggestions. You can email your comments to us at:

`docfeedback@sun.com`

Please include the part number of your document in the subject line of your email.

Sun Ray System Overview

This chapter describes the following components and how they work:

- “Accessing the Latest Sun Ray Information” on page 1
- “What’s New in Version 1.1” on page 1
- “Sun Ray System” on page 5
- “Sun Ray Hardware” on page 6
- “Sun Ray Server Software” on page 17

Accessing the Latest Sun Ray Information

The Sun Ray website address has changed. The new address is shown below. All the characters should be entered in lower case:

`http://www.sun.com/sunray1`

What’s New in Version 1.1

The Sun Ray enterprise server software 1.1 includes several improvements and new features.

Improvements Over Previous Release

Through continuous testing and customer feedback, bugs discovered in the previous release software have been corrected, the installation and upgrade script (utinstall) was refined, and the Administration application has been extended.

Patches Included in Release

The 1.1 version of the Sun Ray server software integrates the following patches:

TABLE 1-1 Patches Included With the Sun Ray Enterprise Server Software 1.1

Software	Patches and Location			
Solaris 2.6 operating environment	105181-17	105210-25	105284-31	105390-02
	105490-07	105568-14	105633-30	105669-09
	105703-18	106040-13	106123-04	106409-01
	107272-02	107381-01	108396-01	
	/cdrom/cdrom0/Patches/Solaris_2.6			
Solaris 7 operating environment	106980-07	107078-18	107081-10	107180-12
	107248-02	107250-02	107636-03	108374-01
	/cdrom/cdrom0/Patches/Solaris_7			
LDAP client	106497-01			
	/cdrom/cdrom0/LDAP_client/Solaris_2.6/Patches			
SunDS 3.1	106621-05			
	/cdrom/cdrom0/Sun_Directory_Services_3.1/Solaris_2.6+/Patches			
Sun WebServer™ 2.1	107609-03			
	/cdrom/cdrom0/Sun_WebServer_2.1/Solaris_2.6+/Patches			

This list is not complete and newer or additional patches may be available on the CD-ROM. Refer to the *Sun Ray Enterprise Server Software 1.1 Product Notes* for more current patch information. Additionally, patch information is available at this URL:

<http://www.sun.com/products/sunray1/patches.html>

Installation and Upgrade Script

The `utinstall` script has been refined to ease the process of installing or upgrading to the Sun Ray Enterprise Server Software 1.1. Bugs have been fixed, the script status is more informative, and the script reports any discrepancies and informs the system administrator if a particular action needs to be taken.

New Administration Application

Release 1.0 of the Sun Ray server software provided a basic graphical user interface. In this release, an improved, user-friendly, and feature-rich GUI is provided as the default means of administering the Sun Ray server. Command-line interaction with the Sun Ray server is also possible. Refer to “Administration Application Overview” on page 87.

New Features in this Release

New features have been added to the Sun Ray server software so that power users can customize their servers with special abilities. More information about these features and installing them is in the *Sun Ray Enterprise Server Software 1.1 Advanced Administrator’s Guide*.

Failover Capability

New in this release is the Failover option. Two or more Sun Ray servers may “back-up” each other so that in the event of a Sun Ray server failure, a reserve Sun Ray server is available. For additional information regarding the failover feature (including architectural and configuration recommendations), refer to the *Sun Ray Enterprise Server 1.1 Advanced Administrator’s Guide*.

Additional Smart Card Support

In release 1.1 of the Sun Ray enterprise server software, the Sun Ray server can be configured to recognize additional standard smart card formats. This enables diverse card security protocols from different smart card vendors. Refer to “Managing Smart Cards From Different Vendors” on page 165.

Sun Enterprise 10000 Server Support Provided

The Sun Ray server software now supports the Sun Enterprise™ 10000 server. For additional information see “Sun Enterprise 10000 Server Support Provided” on page 4.

Sun Ray System

The Sun Ray system consists of a Sun™ server with the Solaris operating environment running the Sun Ray enterprise server software, Sun Ray 1 enterprise appliances, and an *interconnect fabric* (network) that ties the server and the appliances together (FIGURE 1-1). The software is installed on a server running the Solaris 2.6 or Solaris 7 operating environment.

With the Sun Ray server software, an end user has access to all Solaris applications and a variety of X Windows and legacy (mainframe) applications (currently third-party emulations). With the installation of third-party applications such as MetaFrame™ from Citrix, an end user can access Microsoft Windows NT applications.

Note – Because the Sun Ray server software is server-based technology, the ratio of appliances to servers depends on the type of applications and their access patterns.

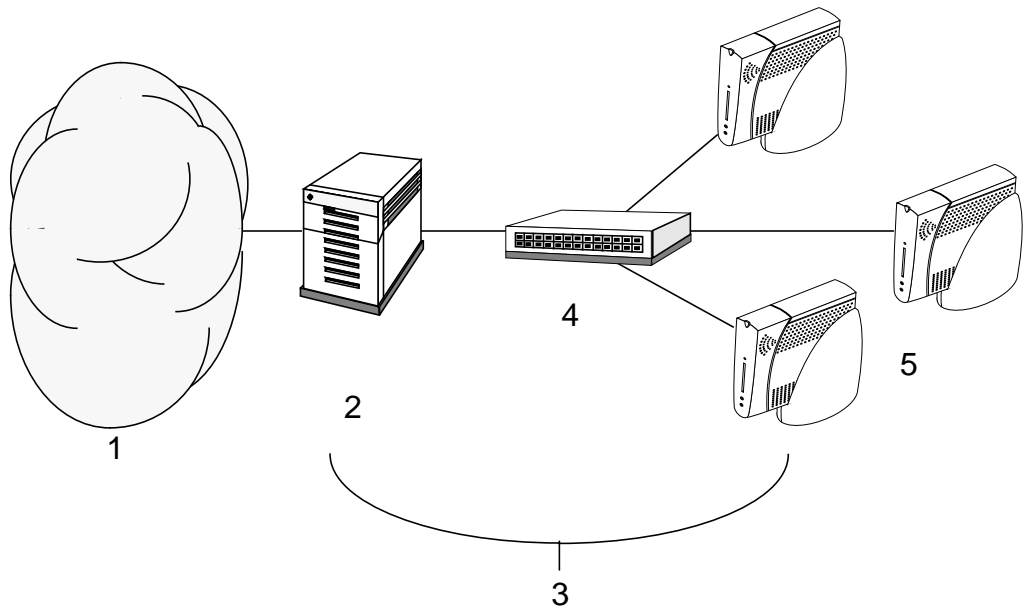


FIGURE 1-1 An Example Sun Ray System

Legend:

1. Local area network (LAN)—existing connection to intranet or internet

2. Sun Ray server—executes applications
3. Interconnect fabric—private network dedicated to Sun Ray 1 appliances (not part of the LAN)
4. Ethernet switch
5. Sun Ray 1 appliances

The Sun Ray system administrator's responsibilities are to set up, modify, and administer the Sun Ray server software and the interconnect fabric (Sun Ray network) as shown in FIGURE 1-1.

Peripheral devices such as keyboards and mice that are added to the appliances via USB are automatically recognized when attached (*hot-pluggable*). The Sun Ray server administers these peripherals.

Sun Ray Hardware

This section describes the various hardware components specific to the Sun Ray system:

- Server
- Appliance
- Interconnect fabric

This section does not discuss the Sun Ray network configuration.

Sun Ray Server

The Sun Ray server software is designed to operate on a server running the Solaris 2.6 or Solaris 7 operating environment and is used to support the appliances. See “Sun Ray Server Software” on page 17 for more information.

Sun Ray 1 Enterprise Appliance

The Sun Ray 1 appliance is the ultimate thin client. It delivers the full functionality of a workstation or a multimedia PC. The key features of the units include:

- 24-bit, 2D accelerated graphics at up to 1280x1024 resolution at 85 Hz (640 x 480 at 60 Hz is its lowest resolution)

- Multichannel audio input and output capabilities
- Composite video input
- Smart card reader
- USB ports that support hot-pluggable peripherals

Each appliance requires a monitor, keyboard, and mouse.

Essentially, the appliance acts as a frame buffer on the client-side of the Sun Ray network. Applications are run on the server and render their output to a *virtual frame buffer*. The Sun Ray server software formats and sends the rendered output to the appropriate appliance, where it is interpreted and displayed.

Sun Ray 1 appliances are identical, with the exception of the Ethernet MAC address. If an appliance fails, you can just replace it with another appliance. Sun Ray 1 appliance IP addresses are leased. IP address leasing is managed by the Dynamic Host Configuration Protocol (DHCP).

Firmware Module

The Sun Ray 1 appliance has a small firmware module that can be updated from the server. This module checks the hardware with a power-on self test (POST) and boots the unit. The Sun Ray 1 appliance also contacts the server to authenticate the end user, and handles low-level input (such as keyboard, mouse, and display information) and output. If there is a problem with the appliance, the module displays an on-screen display (OSD) icon on the screen. Refer *Appendix A, Troubleshooting* for additional information.

Front Panel Features

The two most visible connectors (FIGURE 1-2) are the headphone output and the microphone input below the smart card reader slot. The headphone connector is designed to work with low impedance stereo headphones. The end user can adjust the headphone and speaker volume using a Sun keyboard or using the Settings screen. The microphone input supports non-powered and self-powered microphones. The end user can adjust the volume level and microphone input from the Settings screen.

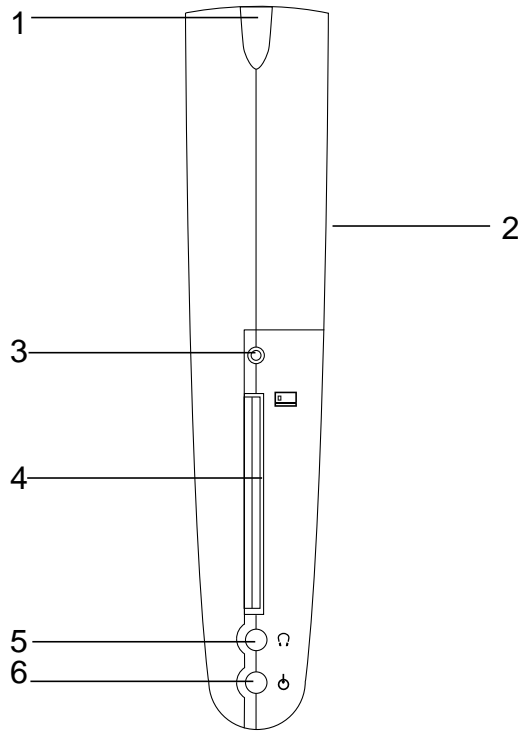


FIGURE 1-2 Front Features of the Sun Ray 1 Enterprise Appliance

Legend:

1. Power—LED illuminates when the appliance is powered on
2. Speaker—Plays back a stereo audio signal mixed into a monaural signal
3. Smart card reader LED—Illuminates when a smart card is inserted
4. Smart card reader—Accepts a valid smart card
5. Headphone output—Designed to work with low impedance stereo headphones
6. Microphone input—Microphone volume is adjustable through software

Back Panel Features

In addition to the speaker near the front of the appliance you can also attach speakers to the line-out connection on the rear of the appliance (FIGURE 1-3).

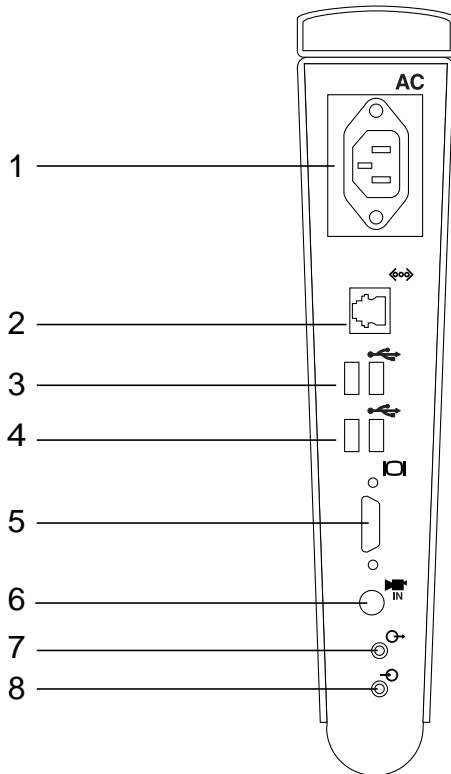


FIGURE 1-3 Rear Features of the Sun Ray 1 Enterprise Appliance

Legend:

1. Power—The power cord connects to this receptable
2. Network Connector—100BASE-T Ethernet cable receptacle (RJ-45)
3. USB port 1 and 2—Standard USB port for peripherals
4. USB port 3 and 4—Standard USB port for peripherals
5. Video—Output for a standard (15-pin VGA) monitor
6. Video in—Input for a device that provides a composite video signal
7. Stereo audio signal line-out 1/8 inch (3.5mm) stereo mini-plug—Output to an audio device
8. Stereo audio signal line-in 1/8 inch (3.5mm) stereo mini-plug—Input from an audio device

Note – USB keyboards and mice can be attached to any available USB port on a Sun Ray 1 appliance.

Video Capabilities

The video in (*composite*) connector accepts video signals supplied by standard VCRs, camcorders, video disc players, or video cameras. Stereo audio can be supplied through the line-in port. The following television video standards are compatible with the Sun Ray 1 appliance:

- NTSC M
- PAL B/G/I

Connecting Devices

The Sun Ray 1 appliance can use the SunCamera™ II video camera via the composite video input connector (FIGURE 1-3). You can also attach standard VCRs or camcorders using the composite video connector. The Sun Ray 1 appliance does not manipulate or edit the incoming composite video stream. Refer to your application (for example, video conferencing or video editing) documentation for details on how to bring the data into an application.

Always refer to the product manual for complete instructions about the device you want to attach.

Audio Capabilities

The Sun Ray 1 appliance can connect with other audio equipment to record and play back sound. The volume can be adjusted via the keyboard or through the window manager or through the Settings screen. Refer to “Using Sun Ray 1 Settings” on page 77.

The Sun Ray 1 appliance senses the presence of headphone, microphone, and line-in and reflects their presence in the Settings screen. The Sun Ray server software also plays/records at 48 khz and provides all common sample rates conversions from 8 kHz to 48 kHz.

Adjusting Volume

The end user can use the Sun keyboard's audio keys (FIGURE 1-4) to increase or decrease the volume from the speaker or headphone. Changes can also be made and are reflected on the Settings screen. For example, pressing the Audio Volume Up key (item 3 in FIGURE 1-4) to increase the volume is also reflected via the slider on the Settings screen.

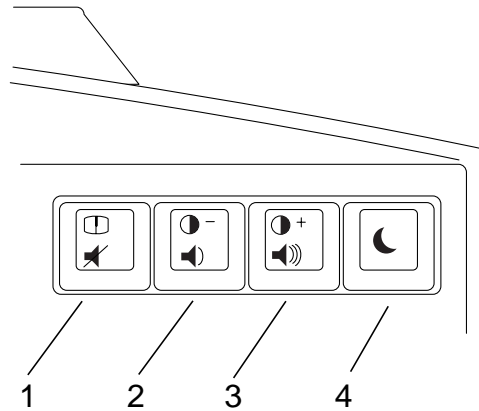


FIGURE 1-4 Audio Key Icons

Legend:

1. Mute Audio key
2. Audio Volume Down key
3. Audio Volume Up key
4. Power Control key

Audio Muting

Instant muting of audio is available either from the keyboard or the Settings screen. Pressing the Mute Audio key on an appliance's keyboard is also reflected on the Settings screen (the mute OSD is momentarily flashed on the screen as well).

Audio Playback

The Sun Ray server software mixes with other protocol-based sources, such as media players and the X11 bell, at the desktop during playback. The application playback volume does not affect the desktop volume control. The Sun Ray server software uses a master volume controller (FIGURE 1-5) that allows several feeds (for example, from applications).

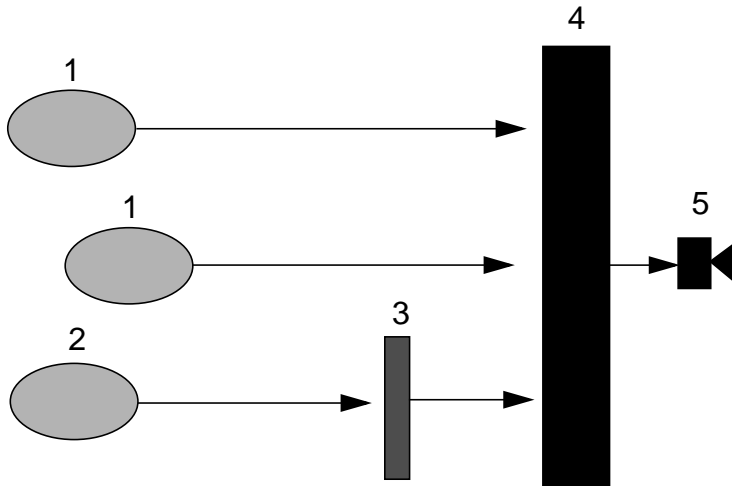


FIGURE 1-5 Sun Ray Server Software Master Volume Strategy

Legend:

1. Direct application(s) volume levels (for example, X11 bell)
2. Solaris `/dev/audio` application
3. Solaris audio device emulator volume control
4. Sun Ray master volume controller
5. Audio output

The Sun Ray 1 appliance uses an internal speaker, located on the right-hand side of the casing, to playback a stereo audio signal mixed into a monaural signal.

Audio playback via headphones is also available (FIGURE 1-2). Adjust the headphone volume using the Settings screen or the Sun keyboard. Keyboard beeps can be controlled through the Common Desktop Environment (CDE). Refer to the `xset` man page for additional information.

Audio Recording

Refer to your recording application's documentation for specific information on recording sound.

Connecting Devices

Audio line-in and line-out are located on the rear of the appliance. Use these connections for recording standard audio output similar to VCRs, tape decks, and for external powered speakers and power amps.

Note – The audio line-out is at a fixed level and is not adjustable. Audio line input level can be adjusted through the Settings screen.

You can use a variety of external audio devices with a Sun Ray 1 appliance. Always refer to the product manual for complete instructions about the device the end user wants to attach.

Device Emulation Capabilities

Each time an end user logs into a Sun Ray 1 appliance, a script automatically assigns the `$AUDIODEV` environment variable to that session. One `utaudio(1)` real-time process is assigned to each session. Refer to the `audio(7i)` man page for more information.

Note – If a program is “hardwired” to use `/dev/audio`, there is a dynamic library supplied (directed to by the `LD_PRELOAD` environment variable in each session), which redirects requests to the Sun Ray 1 appliance audio device emulator. For more information about the library, see “Troubleshooting” on page 189.

The emulated audio device follows the end user session during hot desking. The device name appears in the `$AUDIODEV_environment` variable but is transparently interpreted by audio programs for Sun systems. Device nodes currently appear in the `/tmp/SUNWut/dev/utaudio` directory.

Caution – Do not remove the `/tmp/SUNWut/dev/utaudio` directory. Deleting this directory prevents existing end users (with `utaudio` sessions) from using their audio pseudo device nodes. This directory tree is completely recreated at boot time.

If your application uses `/dev/audio`, the Sun Ray server software reroutes the audio signal appropriately.

Power Cycling Requirements

If you or an end user must power cycle an appliance using the power cord (not the keyboard sequence Control + Power), you or the end user should disconnect the power cord, wait 15 seconds, and reconnect the power cord.

Sun Ray Interconnect Fabric

The Sun Ray interconnect fabric is a dedicated and private network. The Sun Ray 1 appliances are connected to the server over this network using an application-specific protocol. This network is based on 10/100BASE-T Ethernet technology, using unmanaged (*level-2*) switches or hubs and *category 5* wiring.

Note – Category 3 wiring using 10BASE-T equipment can be used, but with reduced performance.

Each Sun Ray 1 appliance is attached to the interconnect fabric via its built-in 10/100BASE-T interface.

The scenarios described in the following paragraphs are intended to be conservative methods of providing good desktop performance to Sun Ray users at a low cost. Many other network scenarios are possible.

Caution – To avoid performance degradation, do not connect Sun Ray 1 appliances to networks with other devices.

Currently, 100BASE-T and gigabit Ethernet provide the lowest cost and most simple operation.

Workgroup Scenario

For small workgroups with between five and 50 Sun Ray 1 appliances, the Sun Ray server uses either single 100BASE-T cards or a quad 100Base-T card to connect to small (eight to 12 port), shared 100BASE-T hubs. These hubs, in turn connect to the Sun Ray 1 appliances.

For example (FIGURE 1-6), a Sun Enterprise™ 2 (or a similar model) server with a Sun quad FastEthernet™ card and four inexpensive 100BASE-T hubs can easily support 24 users. Each link from the Sun Enterprise 2 transmits the traffic for six Sun Ray 1 appliances. This example represents a 6 to 1 multiplexing ratio.

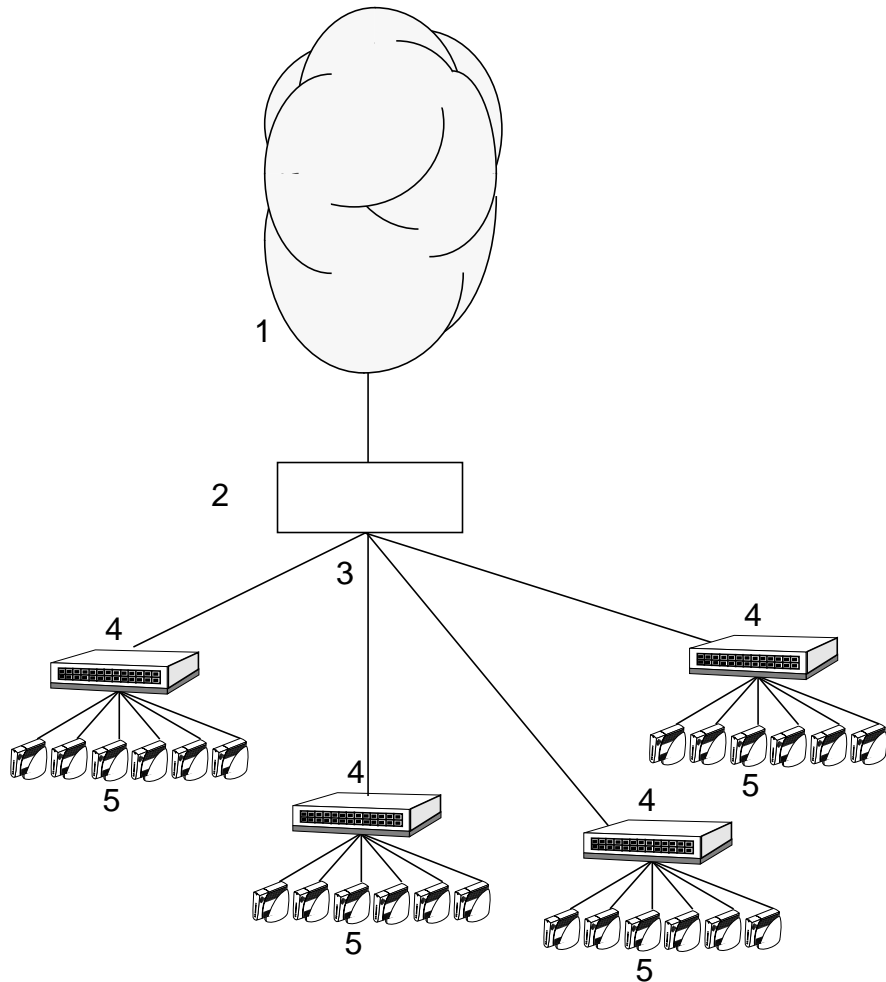


FIGURE 1-6 Workgroup Scenario

Legend:

1. Local area network (LAN)—existing connection to intranet/internet
2. Sun Enterprise Ultra10 server (or higher)
3. Quad network interface card (NIC)
4. 100BASE-T hub (eight to 12 ports)
5. Sun Ray 1 appliances

Department Scenario

For departments with groups consisting of 100 or more Sun Ray 1 appliances, the Sun Ray server software uses multiple gigabit Ethernet cards to connect to large 100BASE-T switches. For example, a 100 user departmental system consisting of an Sun Enterprise 450 server, two gigabit Ethernet cards, and two large (72-port) switches deliver services to the 100 Sun Ray 1 appliances (FIGURE 1-7). In this example, the gigabit links are transmitting the traffic for up to 72 Sun Ray 1 appliances. This example represents a 8 to 1 ratio over the end 100BASE-T link speed.

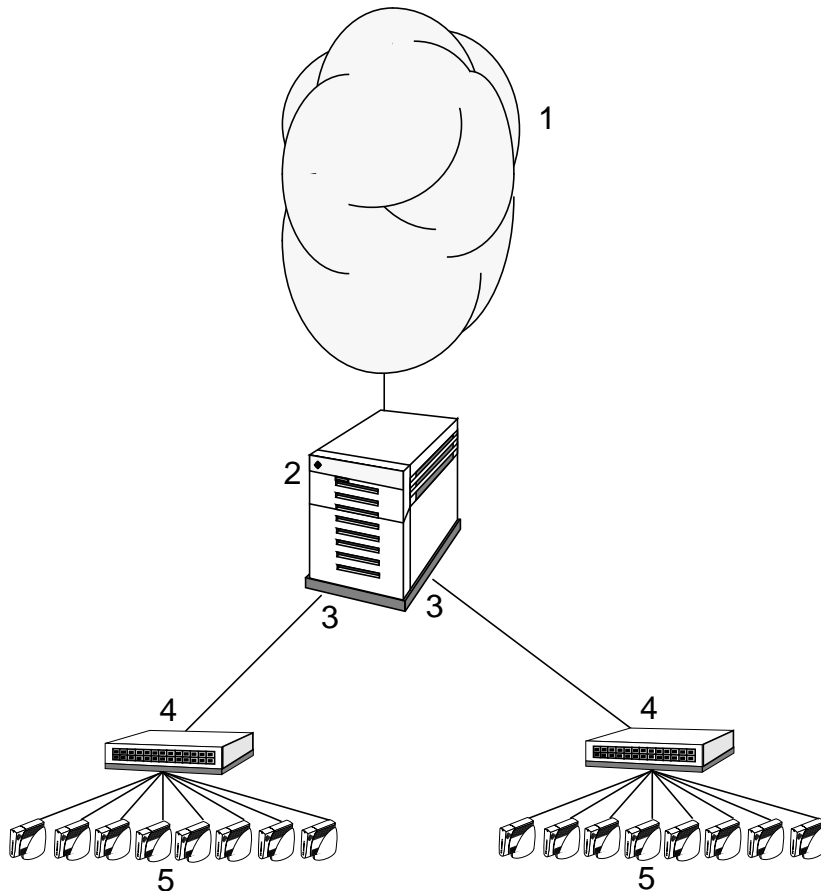


FIGURE 1-7 Department Scenario

Legend:

1. Local area network (LAN)—Existing connection to intranet/internet

2. Sun Enterprise 450 server (or higher)
3. Gigabit Ethernet card (gem0 and gem1) or equivalent
4. 72-port, 100BASE-T switch with gigabit uplink
5. Sun Ray 1 appliances

Connecting Sun Ray Enterprise Appliances with Other Devices

The Sun Ray interconnect fabric is a *dedicated* and *private* network. Each Sun Ray 1 enterprise appliance must be connected to the interconnect fabric via its built-in network interface. This means that the Sun Ray 1 appliances are attached to a dedicated switch.

Note – The Sun Ray interconnect fabric is not a corporate LAN. It is not to be shared with the corporate LAN or to be used in place of a corporate LAN. Do not connect Sun Ray 1 enterprise appliances to networks with other devices.

Sun Ray Server Software

Using the Sun Ray server software, you configure the network connections, select an authentication protocol, administer users, define desktop properties, and monitor the system. The Sun Ray server software includes:

- User authentication and access control
- Session management
- Device management
- System administration tools
- Virtual device drivers for all supported/optimized rendering APIs

The Sun Ray server software process consists of several stages:

1. The Sun Ray server software formats and sends the rendered output to the appropriate appliance over the Sun Ray network.
2. Each communication from the server is validated before it is interpreted.

3. Next, the information is displayed on the appliance's monitor. All input (for example, keystrokes and mouse clicks) is transmitted back to the appropriate application. FIGURE 1-8 illustrates the components and the distribution of the Sun Ray server software.
4. An end user, using the Settings screen, has control over the mouse, monitor resolution, audio, and video on the appliance.

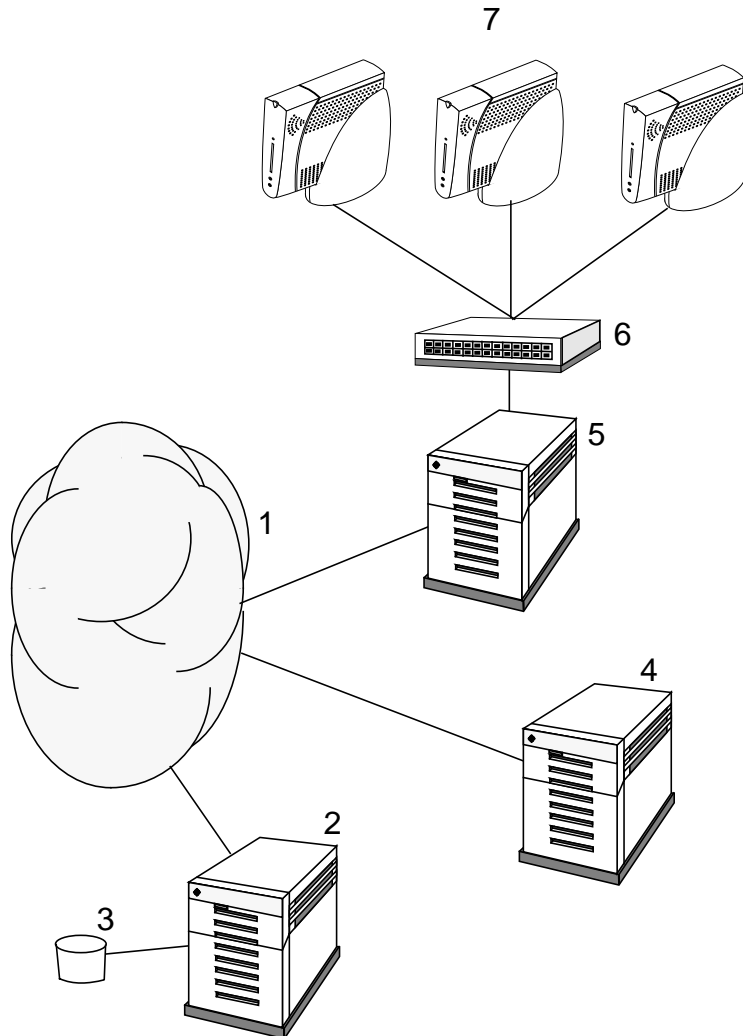


FIGURE 1-8 Distribution of Software in the Sun Ray System

Legend:

1. LAN
2. Backend server
3. Database
4. Solaris server
5. Sun Ray server
 - a. Solaris operating environment
 - b. Sun Ray Enterprise Server Software
 - c. Windowing system
 - d. Applications
6. Switch
7. Sun Ray 1 appliances

Authentication Manager

There are two unique system functions that are crucial to the proper and continued operation of the Sun Ray system. The first of these is the Authentication Manager. The second function is the Session Manager (For more information see “Session Manager” on page 22). For information on administering ports see “Administering Sun Ray Server Ports” on page 24.

The Authentication Manager’s main task is to implement the chosen policies for identifying and authenticating end users at Sun Ray 1 enterprise appliances. The Authentication Manager is also responsible for verifying user identities and for implementing site access policies. It must be available any time an end user attempts to access the system using a Sun Ray 1 enterprise appliance. The Authentication Manager is not visible to the end user.

When an end user first accesses the system, the enterprise appliance takes a *token* and uses it to present credentials to the Authentication Manager to request access. If the user inserts a smart card, the smart card’s type and ID are used as the token. If the user is not using a smart card, the enterprise appliance’s built-in type and ID (the unit’s Ethernet address) are supplied as the token. Every token contains a type and ID that uniquely identifies the token to the Sun Ray system. For smart cards, the type is often derived from the card manufacturer. For enterprise appliances, the type is *pseudo*.

The Authentication Manager uses pluggable components called *modules* to implement various site-selectable authentication *policies*. The site administrator can construct a combination of the different modules and their options to implement a policy tailored to the site's needs. The modules are:

- ZeroAdmin — Any type of token is accepted. Users are automatically passed through to the `dtlogin` screen. This module is designed primarily for workstation-replacement implementations.
- Registered — The token is only accepted *if* the token has been registered in the Sun Ray administration database *and* the token is enabled. If the token does not meet these conditions, it is rejected. If accepted, the user is passed through to the `dtlogin` screen. This module is designed for sites that want to restrict access to only certain users or enterprise appliances.

Once the user is presented with the `dtlogin` screen, the Authentication Manager has successfully completed its tasks.

Users can be registered in two ways:

- Central Registration—One or more site administrators are responsible for assigning smart cards and/or enterprise appliances to authorized users and registering users' tokens in the Sun Ray administration database.
- Self-Registration—Users are allowed to register themselves in the Sun Ray administration database. If this mode is enabled and the Authentication Manager is presented with a token that is not registered, the user is prompted with a registration screen that is similar to the information a site administrator would request.

Note – If self-registration is enabled, users still can be centrally registered as well.

Note – If a token has already been registered, but has been disabled, the user will *not* have an opportunity to re-register the token; the user must contact the site administrator to re-enable the token.

The interaction between the Authentication Manager and the enterprise appliance works as follows:

1. An end user accesses an enterprise appliance.
2. The enterprise appliance (item 2 in FIGURE 1-9) sends the user's token information to the Authentication Manager (item 3) and requests access. If a smart card is presented to the appliance, the smart card's type and ID are the token. If not, the appliance's built-in type (`pseudo`) and ID (the unit's Ethernet address) are sent.

3. The Authentication Manager passes the request to the first of the authentication modules (item 4) in the list that makes up the current policy. Each module can either accept responsibility or decline (which passes the request to the next module in the list). If a module accepts responsibility, it decides whether to allow or deny the user; no other modules will be consulted.
4. If the Authentication Manager runs through the entire list of modules and no module takes responsibility for the request, the user is denied.
5. If the user is accepted, the Authentication Manager starts an X Windows session (item 5) for the user, which takes the user to the dtlogin screen (item 6).

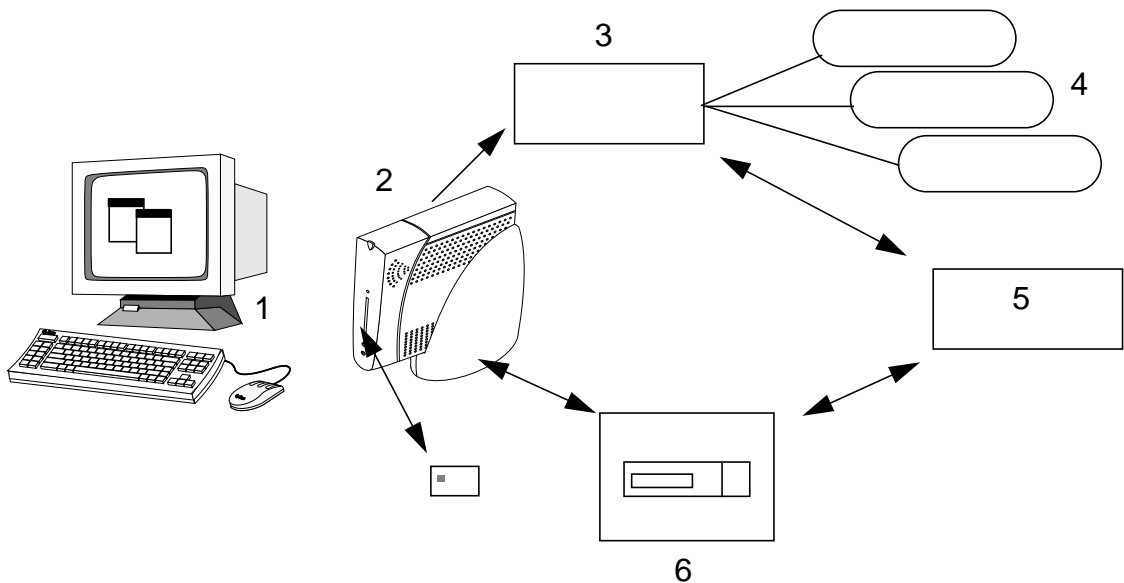


FIGURE 1-9 Authentication and Session Manager Interaction

Mobility—Hot Desking

Depending on the authentication policy selected, users can be *mobile* within the workgroup. This means that if an end user starts a session on one appliance and moves to another, the session follows the end user to the new appliance. For more information on sessions, see “Session Manager” on page 22.

Session Manager

This section describes how the Session Manager interacts with the Authentication Manager and directs services to the end user. The Session Manager is used at start up, for services, for managing screen real estate, and as a rendezvous point for the Authentication Manager. The steps below describe how the process starts and ends:

1. After a user's token is authenticated, the Authentication Manager determines if a session exists for the token. If it does not, the Authentication Manager asks the Session Manager to create a session and then starts the appropriate service(s) for the session according to its policy. This usually involves starting an X server for the session.
2. When services are started, they explicitly join the session by contacting the Session Manager.
3. The Authentication Manager informs the Session Manager that the session associated with the token is to be connected to a specific Sun Ray 1 appliance. The Session Manager then informs each service in the session that it should connect directly to the appliance.
4. When the Authentication Manager determines that the session associated with a token should be disconnected from an appliance, it notifies the Session Manager which, in turn, notifies all the services in the session to disconnect.
5. The Session Manager mediates control of the screen real-estate between competing services in a session and notifies them of clip region changes.

Note – It is important to keep the session ID private. If the end user's session ID is revealed, unauthorized applications can connect directly to the appliance. The `xprop(1)` command can reveal an end user's secret session ID. Also, careless use of the `xhost(1)` command (for example, typing `xhost +`) can allow someone to use `xprop` to capture an end user's session ID. This action can expose the end user's screen images and keyboard input to anyone interested. Use `xhost username@system` to enable only those trusted by the system administrator to access the display and the end user's appliance.

For information on administering ports see “Administering Sun Ray Server Ports” on page 24.

Sessions and Services

A *session* consists of a group of services controlled by the Session Manager. The session is associated with an end user via an authentication token. A *service* is any application that can directly connect to the Sun Ray 1 appliance. This can include audio, video, X servers, and device control of the appliance. For example, `dtmail` is not a service because it is accessed through an X server.

The Session Manager keeps track of sessions and services by mapping services to sessions, and binding and unbinding related services to or from a specific appliance.

The Session Manager only takes authentication from authorized Authentication Managers listed in the `/etc/opt/SUNWut/auth.permit` file.

Changes in a Session

The Session Manager is consulted only if the state of the session changes, or if other services are added. When an end user's token is no longer mapped to an appliance (for example, when a card is removed), the Session Manager disconnects the services from the appliance, but the services remain active on the server. For example, programs attached to the X server continue to run, although their output is not visible.



Caution – The Session Manager daemon must be running all the time. You can verify it is running by using the `ps` command and looking for `utsessiond`.

If the Authentication Manager quits, the Session Manager disconnects all the sessions authorized by it and tells all the sessions that they will have to be re-authenticated. The services are disconnected, but still active.

If the Session Manager is disrupted, it automatically restarts. Each service contacts the Session Manager and requests being added back to a particular session. If you need to stop and restart both the Authentication Manager and Session Manager, type:

```
# /etc/init.d/utsvc stop
```

This command restarts both managers:

```
# /etc/init.d/utsvc start
```

Session Manager Port

The Session Manager is configured to accept connections on a specific TCP port (the default is 7007). The Authentication Manager contacts the Session Manager to create and control the attachment and detachment of sessions to appliances by way of a callback mechanism. If the callback address matches what is in the Session Manager file (the list of permitted addresses), then the Session Manager replies to the call and the two managers can converse.

Administering Sun Ray Server Ports

It is imperative that you do not assign other services to use the Sun Ray enterprise server ports. The following list details the port usage in the `/etc/inet/services` file.

- `sunraySessionMgr 7007/tcp`
- `sunrayAuthService 7009/tcp`
- `sunrayAuthCallback 7010/tcp`

Virtual Device Drivers

All display rendering (for example, fonts, blending, overlays, compositing) is executed on the Sun Ray server software. Pixels are sent to the Sun Ray 1 appliance in an application-specific format. The Sun Ray server software does not modify or change any APIs. The Sun Ray 1 appliance uses a virtual device driver for each available rendering API (for example, the X11 interface). All rendering from Java™ is done from the X server (from UNIX® servers), or the Win32 interface (from Microsoft Windows NT servers). Rendering output from the Win32 interface is translated to the native Sun Ray protocol through the use of Citrix clients running on Solaris servers.

Since the Sun Ray 1 appliance uses 24-bit graphics, an internal translation program translates legacy programs that require 8-bit indexed color into the 24-bit format acceptable for use by the Sun Ray 1 appliances. The default visual type is 24 *bpp* (bits per pixel) with 8-bit displays disabled).

The Sun Ray appliance attempts to determine the monitor's screen resolution using DDC 2B (display Data Channel). When successful, the Sun Ray appliance uses the best resolution possible for a given session. For example, if a session is at the default resolution 1280x1024, the Sun Ray appliance uses the highest refresh rate closest to 1280x1024 (that the monitor claims to support). If the user were configured (using `utxconfig`) for 1024x768, the Sun Ray appliance would attempt to use the highest refresh rate as close to 1024x768 as possible.

Note – If a monitor is not capable of DDC, the firmware selects the best resolution and refresh rate for the session (based on the server settings). Refer to the `utconfig(1m)` man page for additional information.

When there is no DDC response from the monitor, the Sun Ray appliance uses the value that is built into the firmware as the display resolution. The Sun Ray appliance can be loaded with two different choices of firmware. The first Sun Ray appliance model shipped with the sun default screen size of 1152x900 at 66 Hz (for use with older Sun monitors). The second Sun Ray appliance model uses the industry standard default screen size of 640x480 at 60 Hz. The installation program can choose which default should be in effect by selecting the correct firmware version.

Determining 8-Bit Status

The Sun Ray 1 appliance uses 24-bit graphics. If an application uses only 8-bit visual types an error message is displayed stating that 24-bit graphics is required. For more information regarding those error messages, refer to “Troubleshooting” on page 189.

OpenGL Considerations

Currently, only OpenGL[®] 1.2 is compatible with the Sun Ray 1 enterprise appliance. In addition, using OpenGL applications with the 8-bit default visual may inadvertently cause a user’s X server to crash.

Note – It is recommended that you use 24-bit visual to run OpenGL. When using the 8-bit visual, the display could become corrupted or the X server could crash. On the 64-bit kernel with 8-bit emulation, even `ogl_install_check` does not display properly. Currently there is no patch available for OpenGL 1.1.2.

You can download the latest OpenGL packages from the following web sites:

<http://www.sun.com/solaris/opengl>

and

<http://www.opengl.org>

Sun Ray Software and Hardware Requirements

This chapter describes the specifications for servers, monitors, switches, mice, keyboards, and smart cards that are compatible with the Sun Ray interfaces. It gives guidelines for server sizing for various applications and lists the minimum sizes for the directories that are to hold the Sun Ray server software.

This chapter covers these topics:

- “Software Requirements” on page 27
 - “Hardware Requirements” on page 29
-

Software Requirements

- The Sun Ray server software is designed to run with the server edition of the Solaris 2.6 or Solaris 7 operating environment.
- The Sun Ray server software must be installed on the server with the appropriate patches. See the *Sun Ray Enterprise Server Software 1.1 Installation Guide* for details.

Solaris Operating Environment

The Sun Ray server must be preconfigured with a “full cluster” install of the server version 2.6 or 7 of the Solaris operating environment. You can check the version by typing the following command as a user of the Sun Ray server:

```
% uname -r
```

A response of 5.6 means Solaris 2.6 software, a response of 5.7 means Solaris 7 software. If the server has a lower version, contact your Sun Microsystems representative to purchase a newer version of the Solaris software. Alternatively, you can go to this URL:

<http://www.sun.com/software/solaris/how-to-buy.html>

Other Software

Web Server Conditions

The Sun Ray server software includes, requires, and installs the Sun WebServer™ 2.1 web server software. If you already have a different web server configured on the Sun Ray server, it can coexist with the Sun WebServer, however it *must* not be using port 1660. Port 1660 is reserved by the Sun WebServer for the Sun Ray Administration application.

Web Browser Conditions

To view the Sun Ray administration GUI, you must have a web browser installed on the system which shall access the Administration application. For best results, use Netscape Communicator™ 4.5.1 or a later version. The Netscape Communicator web browser is available at this URL:

<http://www.netscape.com/download>

Note – The Sun Ray Administration application does not support the HotJava™ Browser nor the StarOffice™ web browser. Java 1.1.x is supported. Java 1.2 is not supported.

LDAP Server Conditions

The Sun Ray server software includes, requires, and installs the SunDS lightweight directory access protocol (LDAP) server. If you already have a different LDAP server configured on the Sun Ray server, it can coexist with SunDS, however it must not be using port 389. Port 389 is reserved for use by the SunDS LDAP server. If this situation is not feasible, refer to “Changing the LDAP Server Port” in the *Sun Ray Enterprise Server 1.1 Installation Guide*.

Patch Requirements

For the Sun Ray software to function properly, certain patches are necessary. Most of these patches are automatically installed by the `utinstall` script. However, if the `utinstall` script encounters a newer version of a patch than what the `utinstall` script was going to install, the script does not replace this patch. This way, only the latest versions of patches are installed.

Hardware Requirements

The Sun Ray system requires:

- A Sun server based on the UltraSPARC™ processor (Ultra 10 or higher)
- At least one dedicated Ethernet interface installed on the Sun Ray server in addition to any used for a LAN
- Interconnect fabric of cables, switches, and hubs
- A monitor, keyboard, and mouse for each Sun Ray 1 enterprise appliance to be installed
- Smart cards (optional)

Minimal Hardware Requirements

The following table lists minimal requirements for a Sun Ray server:

TABLE 2-1 Minimum Sun Ray Server Requirements

Aspect	Minimal Requirement	Comment
CPU	UltraSPARC™ 300 MHz	More/faster processors are needed as appliances increase and application complexity increases.
Memory	256 Mbytes	More memory is needed as appliances increase and as applications demand.
Hard Drive	1 Gbyte of free space	More space is needed as users increase. This value does not include swap space.

Sizing Hardware Requirements

The following table provides quick, generic sizing requirements. The values computed do not guarantee satisfactory performance for your Sun Ray server installation.

TABLE 2-2 Sizing Hardware Requirements

Aspect	Equation	Comment
CPU	$((\# \text{ of appliances} \times \% \text{ activity} \times 5\%) + (10\% \text{ for OS})) \times 300 \text{ MHz}$ Example with 40 appliances at 50% activity: $((40 \times 50\% \times 5\%) + (10\%)) \times 300 = 330 \text{ MHz}$	Round up to nearest CPU speed configurable or multiple CPUs*.
Memory	$(\# \text{ of appliances} \times \% \text{ activity} \times 40 \text{ Mbyte}) + 64 \text{ Mbyte for OS}$ Example with 40 appliances at 50% activity: $(40 \times 50\% \times 40) + 64 = 864 \text{ Mbyte}$	Round up to nearest Mbyte configurable.
Hard Drive Swap Space	$(\# \text{ of appliances} \times 50 \text{ Mbyte}) - \text{memory} + 500 \text{ Mbyte (tmp)}$ Example with 40 appliances: $(40 \times 50) - 864 + 500 = 1636 \text{ Mbyte}$	Round up to nearest Mbyte configurable.

* If more than one CPU is used, hard drive swap space must be evenly divided to one spindle per each CPU.

For more thorough information regarding proper provisioning of a Sun Ray server, refer to this URL:

<http://www.sun.com/products/sunray1>

Your Sun Microsystems sales representative can also be of assistance.

Requirements for Servers

This section describes the hardware requirements for the Sun Ray server.

- “Hardware Systems” on page 30
- “Disk Space” on page 31
- “Memory” on page 32
- “Ethernet Card” on page 33

Hardware Systems

The Sun Ray server runs on UltraSPARC servers supported by the Solaris 2.6 or Solaris 7 operating environment. Possible Sun Ray servers (4u platform) include:

- Sun Enterprise Ultra™ 10S
- Enterprise 250/450

- Enterprise 3500/4500

Disk Space

Note – When configuring the server, suggested server configuration includes about 50-100 MB of swap space per session. Refer to the *Sun Ray Enterprise Server Software 1.1 Installation Guide* for additional disk space related information.

The standard installation of the Sun Ray server software requires at least 10 MB of disk space. The following table lists the disk space requirements for specific directories.

TABLE 2-3 Sun Ray Server Software Disk Space Requirements

Product	Default Installation Path	Requirements
Sun Ray core software	/	1MB
	/opt	8MB
	/var	1MB + log files
LDAP client libraries	/usr	350K
Sun Directory Services 3.1	/opt/SUNWconn The default location for the directory database is /var.	<ul style="list-style-type: none"> • 25 MB disk space in /opt • 2.0MB in /var • 0.4MB in /etc You must allow enough disk space for the database. 1,000 entries require roughly 1.5MB of disk space, 64MB of RAM, and 128MB of swap.
Sun WebServer 2.1	/usr	<ul style="list-style-type: none"> • Software—9.5MB and 2MB disk space for documents and log files. • Memory—64MB minimum, 96MB is recommended. • Requires JDK™ 1.1.6 or compatible version.
JDK 1.1.6	/usr	31.5MB

Memory

The level of performance of a Sun Ray 1 appliance is a function of the server's resources, the number of active sessions, and the specific applications being run by the active sessions.

TABLE 2-4 Suggested System Configurations

System	Processor(s)	Memory	Number of Sessions
Enterprise 450	Four 300 MHz UltraSPARCs	2-4 GB	20-30/CPU
Enterprise 4500	Eight 336 MHz UltraSPARCs	4-8 GB	30-45/CPU

Note – The suggested server configuration includes at least two processors, about 25 active sessions per CPU, 20-40 MB RAM or more for each active session (simultaneous use), and about 50-100 MB of swap space per session.

From initial testing, 25-40 MB or more per session handles Netscape™ Communicator, Adobe® Photoshop and FrameMaker, and personal information management (PIM, for example, email, calendar, and text editing) applications. Response time becomes noticeable to users when more than 25 active users on one CPU are running a highly interactive application. For medium interactive applications like PIM, up to 50 active users can be satisfied with the response time.

Our tests show that for all applications 80% of the interconnect fabric traffic was less than 10 Mbps and the average traffic was approximately 1 Mbps per user.

Ethernet Card

A dedicated Ethernet card must be installed in the Sun Ray server for the Sun Ray interconnect fabric. The following table lists the compatible Ethernet cards for use with the Sun Ray server's interconnect fabric.

TABLE 2-5 Ethernet Interfaces

Interface	Example Device Name	Speed (Mb/s)	Comments
Gigabit Ethernet	gem0	1000	This high-speed interface is the ideal server to ethernet switch solution.
SunFastEthernet™	hme2	100	
Lance Ethernet	le1	10	Traditional 10 Mbps Ethernet is too slow for many Sun Ray services. Use at least 100BASE-T interfaces.
QEC/MACE Ethernet	qe0	10	
Quad FastEthernet	qfe0, qfe1, qfe2, qfe3	100	Four individual Ethernet interfaces on one card. Ensure that the SUNWqfed package is installed on the system if you are using this card. The SUNWqfed package was not part of the original Solaris 2.6 release. There has been at least one patch released for the SUNWqfed package since its initial release.

Refer to the following web site for information regarding the latest driver patches and updates:

<http://access1.sun.com>

Note – 10BASE-T has limited bandwidth, so rendering video and complicated web pages can overtax it. The Sun Ray interconnect fabric is intended to be run on category 5 wire, but will run on category 3 wire and 10BASE-T.

Note – The internal hme0 interface can be used if the server LAN connection is not Ethernet (for example, modem or ATM), thus reusing the hardware.

Requirements for the Interconnect Fabric Components

The Sun Ray interconnect fabric is composed of all of the components (cables, switches, and hubs) that connect the Sun Ray server to the appliances.

This environment must be composed of hardware components that provide maximum bandwidth (under a variety of situations), minimize latency, and prevent high levels of congestion from occurring between the Sun Ray 1 appliance and the Sun Ray server.

This section describes the following requirements for the interconnect fabric:

- “Network Considerations” on page 34
- “Specifications for Switches” on page 34
- “Specifications for Hubs” on page 35

Note – Information regarding configuring the Interconnect Fabric for use in a failover environment (for example, failover properties and restrictions) can be found in the *Sun Ray Enterprise Server Software 1.1 Advanced Administrator’s Guide*.

Network Considerations

Follow these guidelines when constructing a new Sun Ray network or modifying your existing configuration:

- Do not use a public or company network to connect Sun Ray 1 appliances to the Sun Ray server.
- Do not configure the Sun Ray server as a router.
- Always assume that moderate amounts of statistical traffic multiplexing exists (10:1 is a very safe and conservative ratio; for example, 100 appliances can be connected via one gigabit link).
- Use simple and inexpensive network equipment that does not require extensive network management features.
- Use full-duplex networks whenever possible.

Specifications for Switches

An *Ethernet switch* connects computing nodes on a local area network. Refer to the following web site for information regarding compatible switches for use in your *Sun Ray* interconnect fabric:

<http://www.sun.com/sunray1>

When selecting switches, consider the following factors:

- All ports must autonegotiate well
- Seek out switches with the following characteristics:
 - Full-duplex
 - Non-blocking
 - Full bisectional bandwidth
 - Large amounts of buffering
- Avoid switches with the following characteristics:
 - Non-negotiating
 - Strict cut-through
 - Unbuffered
 - Half-duplex

Tip – You can extend the distance between your server and switch by using fiber optic cabling.

For additional information on switches refer to the *Sun Ray Enterprise Server Software 1.1 Advanced Administrative Guide*.

Specifications for Hubs

When selecting hubs, consider the following factors:

- Do not use hubs if you do not have to. Switches are the economically preferred choice.
- Hubs are half-duplex; switches are full duplex.
- Use hubs only to get *fan out* (between switches and appliances).
- Do not skimp on bandwidth at the switch when using hubs (do all sharing at hubs; make switches full bandwidth).
- Do not use hubs with more than 12 ports.

You can use hubs for installations with fewer than 30 appliances.

Specifications For Cable

Cable selection and routing is also important.

- Use only category 5 or faster Ethernet cabling.
- Cable multiple switches in a daisy-chain rather than a cascade.

Specifications for the Sun Ray 1 Enterprise Appliance Components

This section describes specifications for Sun Ray 1 appliance components.

- “Specifications for Monitors” on page 36
- “Specifications for Keyboards and Mice” on page 37
- “Specifications for Smart Cards” on page 37
- “Specifications for Other Devices” on page 37

Note – For a current list of tested and verified components see:
<http://www.sun.com/nc/sunray1>.

Specifications for Monitors

Sun Ray 1 appliances work with multisync VGA monitors that adhere to this specification.

TABLE 2-6 Monitor Requirements

Property	Value
Video data polarity	Positive going illuminates pixels. Negative going darkens pixels.
Video level (red, green, blue)	0.755 Volts peak
Black level	0.055 Volts peak
Blanking level	0.00 Volts peak
Sync type	Composite or separate horizontal and vertical, DDC definable by monitor
Sync level	TTL
Sync polarity	Positive or negative, DDC definable
Termination	75 Ohms (video and sync)
Horizontal frequency range	43 kHz - 92 kHz, non-interlaced
Vertical frequency range	60Hz - 85Hz, non-interlaced
Protocols	VESA's DDC2B, EDID V1.0

The typical display rates are 1152x900 at 66Hz, 1152x900 at 76Hz, and 1280x1024 at 76Hz.

Note – To make use of the *DDC* data, the monitor must be connected to the appliance and powered on before the appliance is powered on. If no *DDC* data is available from the monitor, 1152x900 at 66Hz is the default resolution set by the appliance.

Video Input Devices

TABLE 2-7 Specifications for Composite Video Devices

Property	Value
Supported standards	NTSC M, PAL B/G/I
Video level	1.0 Volt peak
Video polarity	Positive
Sync polarity	Negative
Termination	75 Ohms

Specifications for Keyboards and Mice

The Sun Ray 1 appliance is designed to work with the Sun Type 6 USB keyboard and the Sun USB Mouse. Some non-Sun USB keyboards and mice will work with the Sun Ray 1 appliance.

Specifications for Smart Cards

See the following URL for a list of valid smart cards:

<http://www.sun.com/sunray1>

Specifications for Other Devices

Sun Microphone™ II works with Sun Ray 1 appliances; SunCamera II works with Sun Ray 1 appliances. The current release of the software does not include support for video input; it is planned for a later release.

Configuring the Software

This chapter describes how to run the configuration script or use the detailed instructions to configure SunDS 3.1, Sun WebServer 2.1, and the Sun Ray server software.

Note – If you do not configure SunDS and the Sun Ray server software, the Sun Ray administration application and other Sun Ray services will not work. The web-based interface of the Sun Ray administration application additionally requires a configured web server.

This chapter is organized as follows:

- “LDAP Datastore Entry Limitations” on page 39
- “Collecting Key Configuration Parameters” on page 40
- “Configuration Worksheet” on page 40
- “Using the Configuration Script” on page 43
- “Testing the Installation and Configuration” on page 47

LDAP Datastore Entry Limitations

A 10,000 entry limit exists with the SunDS 3.1 datastore license shipped with the Sun Ray server. If a very large number of registered users or desktops is anticipated, the system administrator should use the formula shown below to determine whether an unlimited SunDS license should be purchased and installed.

Note – If more than 10,000 licenses are required, information on purchasing an unlimited SunDS license can be provided by your Sun Sales representative.

LDAP Entry Formula

For Sun Ray server 1.1 release datastore, apply the following:

$$11 + (\text{desktops} * 2) + (\text{users} * 3) + (\text{smart cards}) < 10000$$

For example:

3000 users, 490 desktops, and 8 types of smart card, translates into:

$$11 + (490 * 2) + (3000 * 3) + (8) = 9999$$

Note – The above information represents one maximum configuration that could be used *without* purchasing an unlimited license.

Collecting Key Configuration Parameters

Before configuring the Sun Ray server software and supporting software, you need to choose some important parameters to use throughout the configuration. If you use the automated configuration script, you are asked for these values and they are substituted in the appropriate places. If you choose to do the configuration by hand, you are instructed where to place the substitutions as you work on the files.

Please read the worksheet below; fill it out with your choices and keep it on hand as you use the automated configuration script or perform the manual configuration steps.

Many of these parameters are related to the operation of the SunDS LDAP server that stores administration data for the Sun Ray server. It is strongly recommended that you use the suggested default values (where given) unless you are experienced with LDAP data design and administration.

Configuration Worksheet

Fill out this worksheet before proceeding to either the configuration script or manual configuration steps.

Note – Many of the variables associated with the Sun Ray product have a prefix of ‘ut’.

@(HOSTNAME)

- Name: Hostname
- Description: Hostname of the Sun Ray server.
- Note: If you use the automated configuration script, this parameter is filled in for you.
- Example: sunray1

My value: _____

@(ROOTENTRY)

- Name: UT root entry
- Description: This entry is created to serve as the top-level Sun Ray entry in the LDAP data hierarchy. All Sun Ray administration data is located beneath this entry. Since the Sun Ray administration data is kept in its own data store, this is also the root entry for the data store.
- Note: This value must be of the object class type “organization.” Unless you have an existing LDAP hierarchy and are experienced with LDAP data design and administration, use the default value.
- Default value: o=utdata
- Example: o=utdata

My value: _____

Note – If the server is intended to be part of a failover group, then the value entered for *@(ROOTENTRY)* must be the same as used for all other servers in the group.

@(ROOTNAME)

- Name: UT root name
- Description: The portion of the *@(ROOTENTRY)* variable defined above that is after the equals sign (=). If you use the automated configuration script, this parameter is filled in for you.
- Default value: utdata
- Example: utdata

My value: _____

Note – In a failover configuration, the value entered for *@(ROOTNAME)* while running `utconfig`, must be the same as used for all other servers (secondary servers) in the group.

@(UTPASSWD)

- Name: UT administration password
- Description: Password for an entry that is created within the Sun Ray LDAP data hierarchy that LDAP client-server connections use for authentication. With this password, clients such as the Sun Ray command-line and web-based administration application can access and change Sun Ray administration data. Without this password, clients can access, but can not change the Sun Ray administration data. This is the same password that you use when you enter the web-based administration application (the UT administrator's name is "admin").

My value: _____

Note – If the server is intended to be part of a failover group, then the value entered for *@(UTPASSWD)* must be the same as used for all other servers in the group.

@(WEBSERVER_NAME)

- Name: UT administration web server instance name
- Description: This is the name of the Sun WebServer instance that is created to display the web-based administration application. The Sun WebServer supports multiple instances: each can display a different site or serve a different purpose.
- Default value: `utadmin`

My value: _____

@(WEBSERVER_PORT)

- Name: UT administration web sever port number
- Description: The web server that displays the web-based administration application runs on this port. For example, if you select port 1660, the URL you enter into your browser to use the administration application is `http://localhost:1660`.
- Note: Public web servers generally use port 80 or port 8080, so avoid using either of these or anything similar for the administration server.
- Default value: `1660`

My value: _____

@(CGI_USER)

- Name: CGI username
- Description: Unique UNIX username that the web-based administration application will be run as. The configuration script and instructions below prompt you to create this user, if it does not already exist.
- Note: For security reasons, this should not be the standard `root` or `nobody` UNIX user. This should be an isolated user account that is not used by an existing user. If you already have such a user for administering web servers, you can use it here.
- Default value: `www`

My value: _____

Using the Configuration Script

The configuration script configures all of the supporting software products. Use this script unless you are an experienced system administrator and need to customize the configuration.

▼ To Run the Configuration Script

1. As superuser, type:

```
# cd /opt/SUNWut/sbin
# ./utconfig
```

Note – Fill out the configuration worksheet before continuing.

2. Answer the continuation prompt: Continue ([y]/n)?

Type **y**.

The configuration script prompts you for values (default values in brackets). For example:

```
Using hostname: sunray1
Enter UT root entry [o=utdata]:
Using UT root name: utdata (derived from UT root entry)
Enter UT admin password: <value>
Re-enter UT admin password: <value>
Enter SunDS 'rootdn' [cn=admin,o=utdata]:
```

3. Answer the prompt to use Remote Access.

If you answer **n**, the script will skip to Step 5.

If you answer **y**, the `utconfig` script asks if you want enable secure socket layer (SSL). SSL makes remote access of the Administration application more secure.

4. Answer the prompt for Secure Socket Layer (SSL).

If you answer **n**, the script will skip to Step 5.

Note – If you choose to use Remote Access with the Administration application, and choose *not* to enable SSL, you create a security risk.

If you answer **y**, you will need to configure an SSL certificate.

Note – The SSL certificate *must* be configured before any remote access can be performed. You should configure the SSL certificate after finishing this chapter. Chapter 4 provides instructions how to configure a basic SSL certificate.

5. Answer the prompt for Sun WebServer.

Type **n** if you do not want to configure the Sun WebServer.

Type **y** if you want to configure the Sun WebServer. The configuration script prompts you for values (default values in brackets). For example:

```
Enter UT admin web server instance name [utadmin]:
Enter UT admin web server port number [1660]:
Enter CGI username [www]:
```

The values you have entered are shown. For example:

```
About to configure the following software products:

Sun Directory Services 3.1
  Hostname: sunray1
  UT root entry: o=utdata
  UT root name: utdata
  UT utdata admin password: (not shown)
  SunDS 'rootdn': cn=admin,o=utdata

Sun Web Server 2.1
  UT admin web server instance name: utadmin
  UT admin web server port number: 1660
  CGI username: www

Sun Ray enterprise server 1.1
```

6. Answer the continuation prompt.

```
# Continue ([y]/n)? y
```

Once you confirm, the script begins configuring the products and outputs to the screen the various operations it performs.

7. Answer the prompt for groupSignature.

If you are in a group environment then the `groupSignature` must be the same for all group members. A group of 1 is valid. This prevents unintended results when additional browsers are brought online.

8. After the script has completed, check in `/var/tmp/utconfig.xxx.log` to see if there were any errors. (`xxx` is the process id of the script).

9. Once completed successfully, see “Testing the Installation and Configuration” on page 47.

Testing the Installation and Configuration

To test your installation and configuration, try running the administration application using both the command-line and web-based interfaces.

▼ To Test the Command-Line Interface of the Administration Application

1. Log into the Sun Ray server.
2. Run the following command:

```
% /opt/SUNWut/sbin/utuser -l
```

If the command shows a list of users, or shows 0 users, the software is installed correctly. If the command responds with any errors, a configuration error has occurred and should be corrected. Usually, you can find informative messages detailing the problem in the `/var/adm/messages` file.

3. Once completed successfully, see “Initial Setup” on page 57.

▼ To Test the Web-Based Interface of the Administration Application

1. Log into the Sun Ray server.

Note – If you have configured for SSL then you must install the appropriate certificates for your system and access the URL `http://<hostname>:1660`.

2. Start up a web browser and access the URL `http://localhost:1660`. You should see the web-based administration application’s login page.

If you specified a different port number when you configured the web server, use it here.

If you get a message that says you do not have permission to access a document, the web server is indicating that you tried to connect from a remote machine. Make sure that:

- You are running a browser on the Sun Ray server or one of its appliances
- The browser is *not* using a different machine as an HTTP Proxy Server to proxy the connection to the web server.

Note – If you are trying to connect from a remote server and you enabled SSL in the `utconfig` script, you must first configure an SSL certificate. Chapter 4 provides instructions for configuring an SSL certificate.

3. Enter the administrator username (`admin`) and Sun Ray password (this is the `UTPASSWD` from the worksheet) and click on Log In.

4. Click on the Users link.

5. Click on the List All Users (by ID) link.

If you get a result page or "No Users Found" message, the software is installed correctly. If the command responds with any errors, a configuration error has occurred and should be corrected. Usually, you can find informative messages detailing the problem in the `/var/adm/messages` file.

6. Once completed successfully, see "Initial Setup" on page 57.

SSL Certificate Configuration

This chapter describes a basic procedure to configure a secure socket layer (SSL) certificate for the Sun Ray web server. By configuring the SSL certificate, access to the Administration application from a remote client can be made more secure.

Complete information about setting up and administering SSL certificates is available in Chapter 3 of the *Sun WebServer 2.1 Installation Guide*. This guide is provided on the Sun Ray enterprise server software 1.1 CD-ROM as the `/cdrom/cdrom0/Sun_WebServer_2.1/Solaris_2.6+/Docs/SWS_Installation.ps` file.

Topics in this chapter include:

- “Secure Socket Layer Certificate” on page 49
- “Required Information” on page 51
- “Configuring SSL” on page 51
- “Troubleshooting SSL Configuration” on page 55

After successfully configuring the SSL certificate, continue on to Chapter 5.

Secure Socket Layer Certificate

For the Sun WebServer to use secure socket layer (SSL) encryption, it must have public and private keys, and a PKCS#7 certificate to present to clients. The certificate contains information including the web server’s identity and public key, and the issuer’s identity and digital signature. The SSL library uses the Federated Naming Service (FNS) to store this information. Certificates are typically signed by third-party certificate authorities (CA), such as VeriSign.

Local Root Certificate Authority

A certificate authority (CA) creates and maintains credentials for a web server. For the Sun Ray web server, the root certificate authority (RootCA) creates and maintains the credentials locally. The RootCA user creates credentials for itself, and then uses these credentials to create key packages and sign certificates for any additional web servers. The RootCA user is any user name other than root.

Distinguished Name

A distinguished name (DN) is a globally unique identifier for each user or host that is issued key packages and certificates. The DN is also used in the key package and certificate. The DN is composed of attributes delimited by commas, ordered from most to least significant.

The DN and its attributes are provided by the user in this form:

cn=commonname , ou=organizationunit , o=organization , l=locality , st=state , c=country

Attributes may contain text, numbers, and spaces. The following table explains these attributes in detail:

TABLE 4-1 Distinguished Name Attributes

Attribute	Example	Comment
<i>cn=commonname</i>	<i>cn=sunray.eng.fun.com</i>	The common name must be unique, such as a host name. In this example, a fully-qualified domain name is preferred.
<i>ou=organizationunit</i>	<i>ou=engineering</i>	In a hierarchy, the group in which the common name belongs.
<i>o=organization</i>	<i>o=funmicrosystems</i>	The greater group of all organization units, such as a company.
<i>l=locality</i>	<i>l=laffland</i>	The location of the organization, such as a city or district.
<i>st=state</i>	<i>st=bliss</i>	The state or province where the locality is found. <i>Must</i> be fully spelled out, no abbreviations.
<i>c=country</i>	<i>c=we</i>	The country in which the state or province exists. May be a two-letter abbreviation.

This is an example of a complete DN:

cn=sunray.eng.fun.com , ou=engineering , o=funmicrosystems , l=laffland , st=bliss , c=we

Required Information

Before you configure the Sun WebServer for SSL, you will need the following information:

TABLE 4-2 Required Information

Information	example	Comment
RootCA user	<i>rcauser</i>	Existing user, or new one.
RootCA directory	<i>/var/certs</i>	
RootCA Distinguished Name	<i>cn=rcauser, o=fun, c=we</i>	Simplified for table.
RootCA password	<i>rcapass</i>	Requested when the RootCA is used to sign credentials.
Sun Ray server root password	<i>rootpass</i>	Root password of Sun Ray server.
Web server domain name	<i>eng.fun.com</i>	
*Web server IP address	<i>192.144.31.118</i>	
*Web server Distinguished Name	<i>ou=eng, o=fun, l=laffland, st=bliss, c=we</i>	Every attribute except the common name. Simplified for table.
*Web server certificate directory	<i>/var/certs/192.144.31.118</i>	Directory is the IP address of the web server.
*Web server certificate password	<i>webpass</i>	Requested when configuring the web server's credentials.

* Additional values must be provided for each failover Sun Ray server.

Configuring SSL

Note – The following procedures use the example values listed in TABLE 4-1 and TABLE 4-2. These values are for example only. You must provide real values to properly configure SSL

▼ To Configure SSL on the Primary Sun Ray Server

1. Log in or use the `rlogin` command to become superuser on the Sun Ray server.
2. Verify the `skiserv` and `cryptorand` processes are running. If not, restart them using the following commands:

```
# /etc/init.d/cryptorand stop
# /etc/init.d/skiserv stop
# /etc/init.d/cryptorand start
# /etc/init.d/skiserv start
```

3. Create the local RootCA user:

```
# useradd -c "Root CA user" -m -k /etc/skel -d /var/certs rcauser
# passwd rcauser
New password: rcapass
Re-enter new passwd: rcapass
# chmod 700 /var/certs
# chown rcauser /var/certs
```

4. Become the RootCA user and run the `crca` script to create the RootCA credentials:

```
# su rcauser
$ /usr/bin/crca
```

- a. The `crca` script asks for the following:

- RootCA distinguished name (cn=*rcauser*,o=*fun*,st=*bliss*,c=*we*)
- RootCA directory (*/var/certs*)
- RootCA password (*rcapass*)
- RootCA password again

- b. The `crca` script asks to store the credentials in the name server, type *y* (yes).

- c. Type the root password for the Sun Ray server:

```
Password: rootpass
```

5. Create the web server certificate directory and set permissions and ownership:

```
$ mkdir /var/certs/192.144.31.118
$ chmod 700 /var/certs/192.144.31.118
$ chown rcauser /var/certs/192.144.31.118
```

6. Run the `sslgenrcd` script to generate the web server certificate:

```
$ /usr/http/bin/sslgenrcd -r rcauser -d /var/certs/192.144.31.118 -i 192.144.31.118
```

a. When asked to enter the host name of the `httpd` server, press the Return key.

b. The `sslgenrcd` script asks for the following:

- Web server domain name (*eng.fun.com*)
- Web server DN without common name (*ou=eng,o=fun,l=laffland,st=bliss,c=we*)
- Web server certificate password (*webpass*)
- Web server certificate password again

c. The `sslgenrcd` script asks for the RootCA password:

```
skilogin: Enter your own key package password: rcpass
```

7. Install the web server certificate as superuser:

```
$ exit
# /usr/http/bin/sslstore -i 192.144.31.118 -p /var/certs/192.144.31.118 0
```

a. The `sslstore` script asks for the web server certificate password:

```
/usr/bin/skilogin; Enter host key package password: webpass
```

8. Configure the web server to use SSL

Note – This step is automatically performed by the `utconfig` script when the user is asked whether to enable SSL.

a. Open the `/etc/http/utadmin.httpd.conf` file in a text editor.

b. Find the text `ssl_enable "no"` and change it to `ssl_enable "yes"`.

c. Save the file.

9. Start or restart the web server to use SSL:

```
# /usr/bin/htserver start
```

```
# /usr/bin/htserver restart
```

▼ To Configure Certificates on Failover Servers

Note – The Sun Ray server software *must* be installed on the failover server before performing this procedure.

1. Log in or use the `rlogin` command to become the RootCA user of the RootCA Sun Ray server.
2. Create a second web server certificate directory for the failover server. For example:

```
$ mkdir /var/certs/192.144.31.119  
$ chmod 700 /var/certs/192.144.31.119  
$ chown rcauser /var/certs/192.144.31.119
```

3. Perform Step 6 and its sub-steps in the previous procedure using values for the failover server, then return here.
4. Copy the `/var/certs/192.144.31.119` directory and its contents to the failover server.
5. Log in or use the `rlogin` command to become the superuser of the failover Sun Ray server.
6. Perform Step 7 through Step 9 as described in the previous procedure using values for the failover server, then return here.
7. When the failover server is operating satisfactorily, remove the `/var/certs/192.144.31.119` directory from the failover server.

Troubleshooting SSL Configuration

The SSL configuration must be without error. Any problem that occurs because of an SSL configuration is best corrected by reconfiguring SSL altogether, as this is the fastest, most sure way to correct the problem. Before reconfiguring SSL, you must completely remove any configuration information.

▼ To Remove All SSL Information

Note – The following procedure will remove all SSL information, including RootCA information.

1. Log in or use the `rlogin` command to become superuser on the Sun Ray server.

2. Stop the `skiserv` server:

```
# /etc/init.d/skiserv stop
```

3. Remove the Federated Naming Service directory:

```
# /usr/bin/rm -rf /var/fn
```

4. Start the `skiserv` server:

```
# /etc/init.d/skiserv start
```

5. Reconfigure SSL according to the procedure “To Configure SSL on the Primary Sun Ray Server” on page 52.

Initial Setup

This chapter describes the initial setup of the Sun Ray system:

- “Using the Default System Configuration” on page 57
- “Configuring the Sun Ray Interconnect Fabric” on page 58
- “Setting System Parameters” on page 62

Note – To view any of the specific commands for Sun Ray system, type:

```
% man -a -M /opt/SUNWut/man command
```

or type:

```
% setenv MANPATH=/opt/SUNWut/man
```

followed by

```
% man command
```

Using the Default System Configuration

After installing the Sun Ray server software on your server, you need to configure the Sun Ray interconnect fabric for the network interface card you have installed (see “Configuring the Sun Ray Interconnect Fabric” on page 58). The default sets up 225 possible appliance connections per interface. The actual sessions are not created until appliances are connected into the Sun Ray interconnect fabric, so choosing the default does not use up space or degrade performance.

At the factory, a version of the firmware is loaded into the Sun Ray 1 enterprise appliances. When an appliance is connected, the firmware in the appliance is automatically changed to the version of the firmware on the server if the versions are different. To ensure that all the units have the same firmware, you can run the `utfwadm` command (see “PROM Version Management” on page 67).

The Sun Ray 1 appliances are smart card ready. The default authorization protocol presents every user with a Solaris `dtlogin` screen and uses the regular Solaris login of `userid` and password. The default protocol accepts any valid smart card and creates a session for the user. The smart card user is also prompted with a Solaris `dtlogin` screen.

To add users to the Solaris system, use regular Solaris methods.

The default key sequence for the Settings screen display is `Shift+Props` on the Sun keyboard. See “Defining Desktop Properties” on page 76, for instructions on how to change the default key sequence.

Configuring the Sun Ray Interconnect Fabric

Run the `utadm` command to configure the network interface card (NIC), the DHCP service for the interconnect fabric, and the Sun Ray log management function. The default DHCP setup configures each interface for 225 hosts and uses private network addresses for the Sun Ray interconnect fabric. When you configure the interconnect fabric, the version of the firmware on the appliances is automatically changed to version of the firmware on the server if the versions are different.

Note – The Sun Ray server software works with other products that use DHCP.

Note – If you have just installed the Ethernet controller, remember to boot the server with the `-r` flag so that the system looks for the new interface and creates the appropriate device files.

Note – For information on configuring interfaces, IP addresses, and DHCP data for the failover feature, refer to the *Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide*. If the IP addresses and DHCP configuration data are not set up properly at the time the interfaces are configured, the failover feature will not work properly.

A Note to Sun Enterprise 10000 Administrators

If you are using Alternate Pathing (AP) netgroup on an Enterprise 10000, your interface name must be the same as your AP metanetwork name. For additional information refer to *Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide* or a Sun support representative.

▼ To Configure the Interconnect

For information on Failover feature configuration, see the *Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide*.

1. Type:

```
# /opt/SUNWut/sbin/utadm -a interface_name {-a interface_name}...
```

Some interface names are hme[0-9], qfe[0-9], or gem[0-9].

For example:

```
# /opt/SUNWut/sbin/utadm -a gem0
```

A dialog similar to the following is initiated; respond **y** if the default values are acceptable.

```
Configuring the Sun Ray Interconnect Fabric

### Configuring /etc/nsswitch.conf
### Disabling Routing
### configuring gem0 interface at subnet 128
  Selected values for interface "gem0"
    host address:      192.168.128.1
    net mask:         255.255.255.0
    net address:      192.168.128.0
    host name:        sunray-128
    net name:         SunRay-128
    first unit address: 192.168.128.3
    last unit address: 192.168.128.254
    firmware server:  192.168.128.1
  Accept as is? ([Y]/N): y
### successfully setup "/etc/hostname.gem0" file
### successfully setup "/etc/inet/hosts" file
### successfully setup "/etc/netmasks" file
### successfully setup "/etc/inet/networks" file
### finished install of "gem0" interface
### Building network tables - this will take a few minutes
### Configuring DHCP Service for Sun Ray
```

If the default values are unacceptable, respond **n** and enter new values. A dialog similar to the following will be displayed. In the dialog below, the network is changed from 192.168.128 to 192.168.129 and configured for maximum of 14

sessions.

```
Configuring the Sun Ray Interconnect Fabric

### configuring /etc/nsswitch.conf
### Disabling Routing
### configuring gem0 interface at subnet 128
  Selected values for interface "gem0"
    host address:      192.168.128.1
    net mask:         255.255.255.0
    net address:      192.168.128.0
    host name:       sunray1-128
    net name:        SunRay-128
    first unit address: 192.168.128.3
    last unit address: 192.168.128.254
    firmware server:  192.168.128.1
Accept as is? ([Y]/N): n
new host address: [192.168.128.1] 192.168.129.1
new netmask: [255.255.255.0]
new first Sun Ray address: [192.168.129.3]
new last Sun Ray address: [192.168.129.254] 192.168.129.16
  Selected values for interface "gem0"
    host address:      192.168.129.1
    net mask:         255.255.255.0
    net address:      192.168.129.0
    host name:       sunray1-129
    net name:        SunRay-129
    first unit address: 192.168.129.3
    last unit address: 192.168.129.16
    firmware server:  192.168.129.1
Accept as is? ([Y]/N): y
### successfully setup "/etc/hostname.gem0" file
hostname "sunray1-129" appears in "/etc/inet/hosts" file with
another IP
address, fix?([Y]/N): y
### successfully setup "/etc/inet/hosts" file
### successfully setup "/etc/netmasks" file
### successfully setup "/etc/inet/networks" file
### finished install of "gem0" interface
### Building network tables - this will take a few minutes
### Configuring DHCP Service for Sun Ray
```

The remaining output should be similar (but may vary slightly) to the following:

```
### Configuring DHCP Service for Sun Ray

### stopped DHCP daemon
### started DHCP daemon
### Configuring firmware version for Sun Ray
    All the units served by "sunray1" on the 192.168.128.0
    network interface, running firmware other than version
    "1.1_8,REV=1999.01.12.20.15" will be upgraded at their next power-on.

### Configuring Sun Ray Logging Functions
syslog service starting.
```

2. Reboot the server and power cycle the appliances.

Note – You can type `utadm -p` to list the current interface configuration.

Setting System Parameters

Because there are many sessions on one server, the maximum number of processes per user (`maxuprc`) and number of terminals (`pt_cnt`) need to be increased from the default Solaris levels. Set the `pt_cnt` value to the maximum number of users multiplied by the average number of terminal windows per user (for example, software developers use 8-10 terminal windows). When you run the `utadm` command to configure the interconnect fabric, a message tells you to increase these numbers if they are low.

▼ To Set System Parameters

1. In `/etc/system`, as `root`, use a text editor to set these parameters. For example:

```
set maxuprc=50
set pt_cnt=999
```

2. Reboot the system.

Your Sun Ray system is ready to use. If you want to use any authentication policy other than the default, see “Choosing an Authentication Policy” on page 70. See “Adding and Deleting Users” on page 136 to add users in a way that conforms with the policy you have chosen.

Administering the Sun Ray System

This chapter provides the following information on configuration options:

- “Interfaces on the Sun Ray Interconnect Fabric” on page 65
- “PROM Version Management” on page 67
- “Choosing an Authentication Policy” on page 70
- “User Management” on page 76
- “Printer Administration” on page 76
- “Defining Desktop Properties” on page 76
- “Session Manager” on page 81
- “System Monitoring” on page 82

Note – For more information on any specific commands for the Sun Ray system, see the corresponding man page. Sun Ray man pages are located in the `/opt/SUNWut/man` directory.

Interfaces on the Sun Ray Interconnect Fabric

Use the `utadm` command to manage the Sun Ray interconnect fabric. With it you can add, delete, remove, or list interfaces.

Note – You must have superuser privileges to run `utadm`.

Note – For information on configuring interfaces, IP addresses, and DHCP data for the failover feature, refer to the *Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide*. If the IP addresses and DHCP configuration data are not set up properly at the time the interfaces are configured, the failover feature will not work properly.

▼ To Add an Interface

- **Type:**

```
# /opt/SUNWut/sbin/utadm -a interface_name {-a interface_name} ...
```

This command configures the network interface *interface_name* as a Sun Ray interconnect. You can specify a subnet address or use the default address, which is selected from reserved private subnet numbers between 192.168.128.0 and 192.168.254.0. After an interconnect is selected, appropriate entries are made in the *hosts*, *networks*, and *netmasks* files. (These files are created if they don't exist.) The network interface is activated.

You can use any valid Solaris network interface. For example, *hme[0-9]*, *qfe[0-9]*.

Note – For information on Failover feature configuration, see the *Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide*.

▼ To Delete an Interface

- **Type:**

```
# /opt/SUNWut/sbin/utadm -d interface_name {-d interface_name} ...
```

This command deletes the entries that were made in the *hosts*, *networks*, and *netmasks* files, and deactivates the interface as a Sun Ray interconnect.

▼ To Remove All Interfaces

- Type:

```
# /opt/SUNWut/sbin/utadm -r
```

This command removes all of the entries and all of the structure relating to all of the Sun Ray interfaces. Use the `utadm -r` command to prepare for removal of the Sun Ray software.

▼ To Print the Sun Ray Interconnect Configuration

- Type:

```
# /opt/SUNWut/sbin/utadm -p
```

For each interface, this command displays the hostname, network, netmask, and number of IP addresses assigned to Sun Ray units by DHCP.

PROM Version Management

This section lists the options for managing the firmware on the PROM in the Sun Ray 1 enterprise appliance. Use the `utfwadm` command primarily to keep the firmware version on the server and appliances in sync. Use the command to do the following:

- Setting and unsetting the DHCP version variable
- Upgrading selected appliances or all appliances
- Upgrading selected subnets or all subnets

Note – If you have defined the DHCP version variable, when a new appliance is plugged in and the versions of the firmware on the server and on the appliance are not the same, the appliance’s firmware is changed to the version on the server.

You must have superuser privileges to run `utfwadm`. Use this command to select which appliances will be upgraded. You can make the selection appliance by appliance or by subnet.

TABLE 6-1 Options of the `utfwadm` Command

Option	Description
-A	Adds appliances to the list of appliances to be upgraded and also sets the appropriate DHCP version variable.
-D	Removes the specified appliances from the list of appliances to be upgraded. It unsets the appropriate DHCP version variable. However, the appliances are still upgraded.
-a	Designates all the appliances.
-e with a full Ethernet address (MAC address)	Gives a specific appliance with its Ethernet address. The address entered is read as hex.
-n <i>interface_name</i>	Specifies what subnet the appliances are on. For more than one interface, use a series of -n <i>interface_name</i> entries. For all interfaces, use -n <i>all</i> .
-f with a path	Specifies the path to where the upgrade files are located. If -f is not used, the upgrade is taken from the default firmware files, which are located in: <code>/opt/SUNWut/lib/firmware</code>

Note – See the `utfwadm(1m)` man page for more details.

Examples

- To update all of the appliances on the `hme1` interface, type;

```
# /opt/SUNWut/sbin/utfwadm -A -a -n hme1
```

Note – Reboot the server. You must power cycle the Sun Ray 1 appliances to force a firmware upgrade.

- To update an appliance with Ethernet (MAC) address 08:00:20:4c:12:1f, type:

```
# utfwadm -A -e 0800204c121f -n hme1
```

- To upgrade appliances with addresses of 08:00:20:4c:12:1c, 08:00:20:4c:12:1d, and 08:00:20:4c:12:1e, type:

```
# utfwadm -A -e 0800204c121c -n hme1
# utfwadm -A -e 0800204c121d -n hme1
# utfwadm -A -e 0800204c121e -n hme1
```

▼ To Disable the utload Command

If you want to force all users to stay on the same firmware version, set the *allowFWload* value to false. This renders the *utload* command inactive and prevents a user from downloading firmware to an appliance.

1. **Open the** `/etc/opt/SUNWut/auth.props` **file with a text editor.**
2. **Locate the Allow Firmload Download section (near the end of the file listing) and uncomment the entry and set the value to false.**

```
allowFWLoad = false
```

▼ To Enable the utload Command

The default is true. However, if you need to enable the download, follow this procedure.

1. **Open the** `/etc/opt/SUNWut/auth.props` **file with a text editor.**
2. **Locate the Allow Firmload Download section (near the end of the file listing), and uncomment the entry and set the value to true.**

```
allowFWLoad = true
```

Choosing an Authentication Policy

When choosing an authentication policy (for an overview see “Authentication Manager” on page 19), there are several questions you need to answer with respect to smart card (*card*) users and non-smart card (*pseudo*) users. Answer the questions by checking the appropriate boxes (multiple boxes can be checked for each question).

TABLE 6-2 Authentication Policy Questions

Question	Smart Card Users (<i>card</i>)	Non-Smart Card Users (<i>pseudo</i>)
1. What types of users <i>must</i> be registered? (Users that are not registered are rejected by the Authentication Manager.)	<input type="checkbox"/>	<input type="checkbox"/>
2. Of those users chosen in question 1, which types are allowed to self-register? (Any user can still be centrally registered, regardless of your choice here.)	<input type="checkbox"/>	<input type="checkbox"/>
3. Of those users <i>not</i> chosen in question 1, which types (if any) are allowed to fall through to the ZeroAdmin module (that grants access to all users)?	<input type="checkbox"/>	<input type="checkbox"/>

The following table describes some sample authentication policies and shows how you would answer the above questions to specify them. The answers (one of these: none, card, pseudo, or both) to these questions directly correlate to options you give to the Authentication Manager configuration command described in the next section.

TABLE 6-3 Sample Authentication Policies

Sample Authentication Policy	Question 1 (-r option)	Question 2 (-s option)	Question 3 (-z option)
1. Allow all kinds of users to use the system without registering. This is the default policy for the Sun Ray system.	none	none	both
2. Only allow registered smart cards that have been created by a site administrator. Self-registration is not enabled and users must insert a smart card to use an appliance.	card	none	none
3. Ignore all smart cards but allow non-card users. The appliances behave like traditional workstations.	none	none	pseudo
4. All smart cards must be registered but non-card users can still use appliances. Card users can self-register.	card	card	pseudo
5. All smart card and non-card users must be registered, but only card users are allowed to self-register.	both	card	none

Enabling an Authentication Policy

The `utpolicy` command allows you to specify the authentication policy for your Sun Ray server. The arguments you provide to this command are very similar to the questions you answered in TABLE 6-2. It takes your input and forms the necessary combinations of authentication modules to implement the desired policy.

▼ To Enable an Authentication Policy

1. Answer the questions in TABLE 6-2 and keep the answers handy for Step 2.

2. Type the following command:

```
# /opt/SUNWut/sbin/utpolicy -a -r <Answer To Question 1> -s <Answer To Question 2> -z  
<Answer To Question 3>
```

Where the values for each answer can be `card`, `pseudo`, or `both`. If you answered “none” for a specific question, you should omit that argument (including the flag) on the command line.

Note – If you are using self-registration and do not want to require the user to enter a Solaris user name and password for validation, add the `-p` flag to the `utpolicy` command line. The `-p` flag can be typed anywhere in the command line.



Caution – Using the `-p` flag allows anyone with an unregistered smart card (if `-r card` or `-r both` is specified) or unregistered appliance (if `-r pseudo` or `-r both` is specified) to register.

Note – Example policy 2, 4 and 5 should be entered with the token reader configuration information to assist with the central registration of users (see “To Configure a Token Reader” on page 73).

The table below shows the command line you would type for each of the five examples given in TABLE 6-3:

TABLE 6-4 Commands Used to Set Sample Authentication Policies

Example #	Command to Type
1	# utpolicy -a -z both
2	# utpolicy -a -r card
3	# utpolicy -a -z pseudo
4	# utpolicy -a -r card -s card -z pseudo
5	# utpolicy -a -r both -s card

3. Reboot your Sun Ray server.

Note – The Authentication Manager will not start using the new policy until the service is restarted. If you want to clear out any existing session(s) before instituting a new policy without booting, refer to TABLE 6-5.

▼ To Configure a Token Reader

This command specifies an appliance for registering smart cards.

- **Select a policy and add** `-t clear -t add:nnnnnnnnnnnn` **to the command. For example, type:**

```
# /opt/SUNWut/sbin/utpolicy -a -r card -z pseudo -t clear -t add:nnnnnnnnnnnn
```

Where `nnnnnnnnnnnn` is the full Ethernet address (for example, `0800204c121c`) of the appliance you want to use as a smart card reader. At this writing, the Ethernet address must be lower case.

utpolicy Considerations

This sections describes changes to the `utpolicy` command options and how policies can be managed. For additional information on policy changes, see “Removing Old Policies” on page 75.

Changing Policies and the utpolicy Command

The `utpolicy` command now prints one of the two following messages (FIGURE 6-1 and FIGURE 6-2) after a policy change is applied:

Note – If you add a token reader, you may need to power cycle or reset the appliance being used exclusively as a token reader.

```
THE MOST RECENT POLICY CHANGE WAS SIGNIFICANT.
```

```
(If you cannot afford to terminate existing sessions, then you can
restart the authentication manager without clearing existing
sessions. Note that some sessions that were granted access under
the old policy may persist. Use the following command to restart
the authentication manager without clearing existing sessions:
"/opt/SUNWut/sbin/utpolicy -i soft")
```

```
The authentication manager must be restarted for changes to take
effect. Note that all existing sessions will be terminated. Please
run the following command:
```

```
/opt/SUNWut/sbin/utpolicy -i clear
```

FIGURE 6-1 utpolicy Policy Change Message (1 of 2)

Another possible message, notifying you that the Authentication Manager should be restarted, might also be displayed (FIGURE 6-2):

```
The authentication manager must be restarted for changes to take
effect. If a significant policy change has been made then the
following command should be run, note that all existing sessions
will be terminated:
```

```
/opt/SUNWut/sbin/utpolicy -i clear
```

```
If a minor policy change was made, such as adding a dedicated card
reader terminal, then it is not necessary to terminate existing
sessions and the following command is preferred:
```

```
/opt/SUNWut/sbin/utpolicy -i soft
```

FIGURE 6-2 utpolicy Policy Change Message (2 of 2)

Removing Old Policies

Use the `utpolicy -i clear` command instead of rebooting the server. Refer to the additional `utpolicy` command information described in TABLE 6-5 for additional information.

TABLE 6-5 `utpolicy` (clear and soft) Commands

Command/Option	Result
<code>/opt/SUNWut/sbin/utpolicy -i clear</code>	Use this option if a significant policy change has been made. All existing sessions will be terminated.
<code>/opt/SUNWut/sbin/utpolicy -i soft</code>	Use this option if a minor policy change was made, such as adding a dedicated token reader (smart card reader terminal). With such minor changes, it is not necessary to terminate existing sessions.

User Management

Currently all users are seen as regular Solaris users. Refer to your Solaris documentation for more information on managing Solaris users. For details on managing Sun Ray users, see “Managing Sun Ray Users” on page 135.

Printer Administration

When you add a printer for use by the Sun Ray 1 appliances, you add it as a regular network or local (server) printer (use Solaris Admintool). You do not add it to the Sun Ray interconnect fabric. Printers attached directly to Sun Ray 1 appliances are not supported in this release.

Defining Desktop Properties

This section describes how to use and configure the Sun Ray 1 Settings GUI (graphic user interface), which is used to change settings on a Sun Ray 1 enterprise appliance.

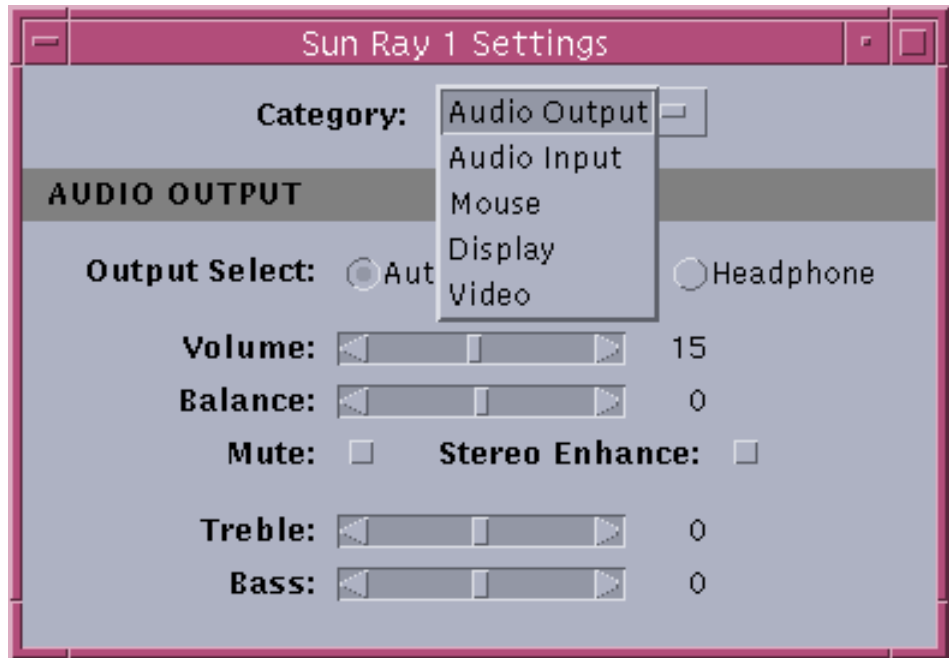


FIGURE 6-3 Settings Screen

Using Sun Ray 1 Settings

Sun Ray 1 Settings is an interactive GUI that allows the user to view and change the settings for the Sun Ray 1 enterprise appliance the user is currently logged into. It can be launched in one of two ways:

- By default, the Sun Ray server starts an instance for each session when the user logs in via `dtlogin`. The Sun Ray 1 Settings Screen (GUI) will remain hidden until the user presses the hot key (by default Shift+Props). Pressing the hot key again will cause it to close.
- Alternatively, the user can launch another instance by typing the following command:

```
% /opt/SUNWut/bin/utsettings
```

In either case, the Sun Ray 1 Settings GUI contacts the Session Manager to determine which enterprise appliance is currently being used and connects to that unit to get the current values. The GUI also keeps open a connection to the Session Manager so the Session Manager can notify the GUI if the user moves to another appliance (by removing the user's smart card and inserting it into another enterprise appliance).

If the user moves to another enterprise appliance, Sun Ray 1 Settings will "follow" the user by connecting to the new appliance and retrieving the new appliance's current settings. Although the application follows the user from appliance to appliance, the settings remain with the appliance. For example, if the user uses Sun Ray 1 Settings to set the volume on appliance #1 to 28, then moves to appliance #2, Sun Ray 1 Settings updates itself to display appliance #2's current volume. If the user returns to appliance #1 and no one else has changed its settings, Sun Ray 1 Settings again displays a volume of 28.

Once the Settings GUI is launched, the user can use the Category pulldown to see groups of Audio Output, Audio Input, Mouse, Display, and Video settings. To change a setting, the user simply moves or changes the appropriate slider, checkbox or pulldown and the appliance is updated immediately. The only exception is the "Resolution/Refresh Rate" setting, which prompts the user with confirmation dialogs before and after the change is made on the appliance.

The Sun Ray 1 Settings GUI supports the following command-line option:

TABLE 6-6 Command-Line Options

Option	Description
-H	Starts the Settings screen in <i>hot key</i> mode. In this mode, the Settings screen is hidden and waits for the hot key to be pressed before being displayed. Press the hot key again to close the Settings screen. The hot key can be user-defined or site-defined, but defaults to Shift+Props (hold the Shift key down and then press the Props key). The Settings screen follows the user to other appliances while in this mode. For more information defining the hot key, see "Configuring Sun Ray 1 Settings" on page 79.

Note – Only one instance of Sun Ray 1 settings can be running in hot key mode per session.

Configuring Sun Ray 1 Settings

Sun Ray 1 Settings allows for the configuration of the hot key that users press to display and hide the Sun Ray 1 Settings GUI. This customization can be done on three levels:

- As a site-wide default setting
- As a user default setting
- As a site-wide mandatory setting

To support these levels of customization, the Sun Ray 1 Settings GUI looks for the following Java properties files at start-up time in the following order:

- `/etc/opt/SUNWut/utsettings_defaults.properties` (sitewide defaults)—This file is read in first and contains helpful default properties. Any properties specified here override any defaults built into the application itself.
- `/home/anyuser/.utsettings.properties` (user defaults)—This file is read second and contains the user's preferred values for the properties. Properties specified here override any application or sitewide defaults.
- `/etc/opt/SUNWut/utsettings_mandatory.properties` (sitewide mandatory defaults) — This file is read in last and contains sitewide mandatory settings that cannot be overridden by the user. Any properties specified here override any application, sitewide or user defaults.

Example uses:

- If a site has purchased PC-style keyboards that do not contain the Sun Props key, the site can use the sitewide defaults file to specify a function key instead. Users can still specify their preferences (via the user defaults file), if so desired.
- If a site has a mandatory policy for all appliances to use a standard hot key (perhaps for ease of training and support), the site could use the sitewide mandatory defaults file to specify this standard key. In this case, users would not be allowed to specify their own preferences.

The format of the hot key entry in these properties files is:

```
utsettings.hotkey=value
```

where *value* is a valid X keysym name preceded by one or more of the supported modifiers (Ctrl, Shift, Alt, Meta), in any order. Example values are shown in the following table.

TABLE 6-7 Example Hot Key Values

Example Value	Notes
Shift SunProps	This is the application default.
F3	
Shift F4	
Ctrl Shift Alt F5	

▼ To Change the Hot Key Setting (Non-Sun Keyboards) Sitewide

1. **As root, open the** `/etc/opt/SUNWut/utsettings_defaults.properties` **file in a text editor.**

Note – If you want to make the change mandatory, change the value in the `/etc/opt/SUNWut/utsettings_mandatory.properties` file.

2. **Locate the original hot key entry and place a # in front of that statement.**

The # effectively comments out the first hot key property.

```
# utsettings.hotkey=Shift SunProps
```

3. **Type in the new hot key property after the first statement. For example,**

```
utsettings.hotkey=Shift F8
```

4. **Save the** `utsettings_defaults.properties` **file.**

The new hot key takes effect when the next user logs in. The next user to log in uses the new hot key to display the Sun Ray 1 Settings screen. Users that were logged in prior to changing the hot key use the old value.

▼ To Change the Hot Key Setting (Non-Sun Keyboards) for a User

1. In the user's home directory (`/home/username`), ask the user to type:

```
% touch .utsettings.properties
```

This creates the `.utsettings.properties` file.

2. Ask the user to edit the `.utsettings.properties` file. Add a line to the file with the value the user wants for the hot key. For example:

```
utsettings.hotkey=Shift F8
```

3. Ask the user save the `.utsettings.properties` file.
4. Ask the user log out and log back in to have the new hot key take effect.

Session Manager

The Session Manager is a Sun Ray enterprise server software daemon. It interacts with the Authentication Managers and services. If you are using the default Sun Ray system, you do not need to change any of the Session Manager's default settings. However, if you need to you can a unique Sun Ray command, `utsessiond`, to:

- Restart the Session Manager daemon
- Set the Session Manager's host name
- Set the Session Manager's listen port
- Specify allowed Authentication Managers

Note – You must be superuser to use this command.

▼ To Restart the Session Manager

- If the Session Manager exits and does not automatically restart, type:

```
# /etc/init.d/utsvc stop stops all daemons  
# /etc/init.d/utsvc start starts all daemons
```

System Monitoring

For the default Sun Ray system, an appliance is mapped to a session and each smart card is mapped to a session. There is a one-to-one correspondence between session numbers and X server numbers.

▼ To List All X Servers Running

- Make your terminal window wider, then type:

```
% ps -ef | grep Xsun
```

Note – If root's Xsun process (usually process ID 1) dies and leaves other child Xsun processes as orphans, new end users will receive a green newt cursor on their screen.

▼ To Search for Runaway Processes

Runaway processes may use a large percentage of `cpu` or `vsz`, or have an application or X server which uses more than 100 Mbytes.

● Use the `ps` command to search for runaway processes: Type:

```
% ps -o rss -o vsz -o pcpu -o args -e -o user
or
% ps -o rss,vsz,pcpu,args,user -e
```

For easier reading, you can save this process information to a file and sort it.

TABLE 6-8 Some Options for the `ps` Command

Option/Specification	Description
<code>-o</code>	Formats the output of this command.
<code>-e</code>	Lists every process now running.
<code>rss</code>	Gives the resident set size of the process in kilobytes.
<code>vsz</code>	Gives the total size in kilobytes for the process in virtual memory.
<code>pcpu</code>	Gives the percentage of CPU time used by the process compared to the amount of CPU time available.
<code>args</code>	Lists the complete command used to start a process.
<code>user</code>	Lists the user that started the process by userid.

The following log files track certain events:

- `/var/opt/SUNWut/log/messages`—Events from the appliances and Authentication Manager
- `/var/adm/message`—Normal system messages and events from the Session Manager

Note – DHCP parameters control the level of logging for the Sun Ray 1 appliances.

A cleanup program automatically removes unused and disconnected sessions after 15 minutes.

Other useful monitoring tools include:

- Performance meter—Displays the system performance
- `snoop` command—Analyzes network data at the packet level
- `netstat` command—Provides network statistics
- `dhtadm` command—Configures DHCP information
- Solaris Resource Manager (SRM)—Allocates and controls major system resources

▼ To Start the OpenWindows™ Performance Meter for Server Statistics

- Type:

```
% /usr/openwin/bin/perfmeter -a -d
```

▼ To Check Network Packets

1. To run the `snoop` command for network packet (DHCP) information (output to file `/tmp/trace.snoop` the activity of Sun Ray 1 appliance `08:00:20:af:24:1c`), as superuser type:

```
# snoop -o /tmp/trace.snoop 08:00:20:af:24:1c
```

2. To run the `snoop` command for the specified network, type:

```
# snoop -d hme1
```

▼ To Check Network Status

1. To run the `netstat` command for network status:

```
% netstat -i
```

This command lists loopback, internet/intranet and Sun Ray network status and level of traffic.

2. Run the `netstat` command to list which ports are active and what is listening (for example, Session Manager on 7007, and authentication on 7009 and 7010), timeout, and restart, type:

```
% netstat -n
```

▼ To Access DHCP Information

- **Run the `dhtadm` command:**

```
# dhtadm -P
```

This command displays the DHCP table, including IP addresses.

Administration Application

This chapter introduces Sun Ray administration concepts and describes how to get started with the Sun Ray administration application.

This chapter provides the following information for the Administration application:

- “Administration Application Overview” on page 87
 - “Token Readers” on page 89
 - “Using the Administration Application” on page 91
-

Administration Application Overview

The Sun Ray system uses UNIX concepts wherever possible and only adds functionality specific to the Sun Ray server software where needed. The Sun Ray administration application can be used to administer Sun Ray users and Sun Ray 1 enterprise appliances (desktops). Below is a brief overview of the two concepts and how they differ from traditional UNIX concepts.

Sun Ray 1 Appliances

Although Sun Ray 1 enterprise appliances have much of the same functionality as a traditional workstation, they are subtly different. Unlike traditional workstations, Sun Ray 1 appliances are not named; they are uniquely identified by their built-in Ethernet address. The appliances do not run the Solaris operating environment, but instead run a very small microkernel in firmware that allows them to connect to a Solaris server.

As each appliance's state changes, it notifies the Sun Ray administration framework, which updates the appliance's entry in the administration database. Using the administration application, administrators can list appliances, check each appliance's current properties, and assign related information to each appliance (for example, unit location and department).

For more details on managing Sun Ray appliances, see "Managing Sun Ray 1 Appliances" on page 97.

Sun Ray Users

The concept of a Sun Ray user is a level above the traditional UNIX user concept. The Sun Ray user is identified by a token (usually a smart card, but it can also be an appliance's built-in ID), which gives the user access to an XWindows session. This session begins with a standard `dtlogin` screen that requires the user to log in with a UNIX username and password before being presented with the user's normal desktop windowing environment. (Note that there is no formal connection between a Sun Ray user and a standard UNIX user account; a Sun Ray user can log in as any UNIX account that the user has a password for).

However, if the user starts a Sun Ray session with a smart card, the user can remove the smart card, insert it in any other enterprise appliance connected to the same Sun Ray server, and the user's session "follows" the user, thus allowing the user to have instantaneous access to the user's windowing environment and current applications from multiple appliances.

The amount of Sun Ray user administration functionality that is available depends on the current authentication policy. The default policy allows *all* cards and *all* appliances access without any registration, so the administration database is not consulted or updated with regard to users. Smart card users can still take their sessions from appliance to appliance, but the cards are not named or tracked.

If an authentication policy involving registered users or appliances is enabled, the Sun Ray administration database is consulted before allowing a specific user or appliance access to a session (depending on the policy). Sun Ray users can be created, modified, and deleted centrally by an administrator using the Sun Ray administration application. Sun Ray users can also be created by the users themselves if the current authentication policy has enabled self-registration. Tokens can be added to a user (for example, if a user's card has been left at home and the user needs access to the current session) and removed from a user (for example, if a user's card has been lost or damaged). Tokens can also be enabled or disabled as needed. User statistics, including lists of users, current logins, and individual user properties are also available.

For more details on the Authentication Manager and choosing an appropriate authentication policy, see "Choosing an Authentication Policy" on page 70.

For more details on managing Sun Ray users, see “Managing Sun Ray Users” on page 135.

Administration Data

Sun Ray administration data comes from two sources: an LDAP data store that keeps persistent administration data, and the Authentication Manager, which is queried as needed for dynamic data. Sun Ray administration data is kept in its own LDAP data store that grants read access to all LDAP clients, but only allows changes by LDAP clients that connect as the privileged UT Admin user. As with any other LDAP data, Sun Ray administration data is accessible via standard LDAP interfaces and applications. However, this data should not be modified by any applications other than the standard ones provided with the Sun Ray server software or else the Sun Ray system may not operate properly.

Token Readers

If you enable an authentication policy with registered users, you need to identify smart card IDs. Some manufacturers print the smart card ID on the card itself, but many do not. Since all of the administrative functions refer to this token ID, the Sun Ray server software provides a way to designate one or more specific enterprise appliances as dedicated token readers. These dedicated appliances can be used by site administrators to administer Sun Ray users.

The most common scenario is that of a site administrator, whose hardware configuration is shown in the figure below.

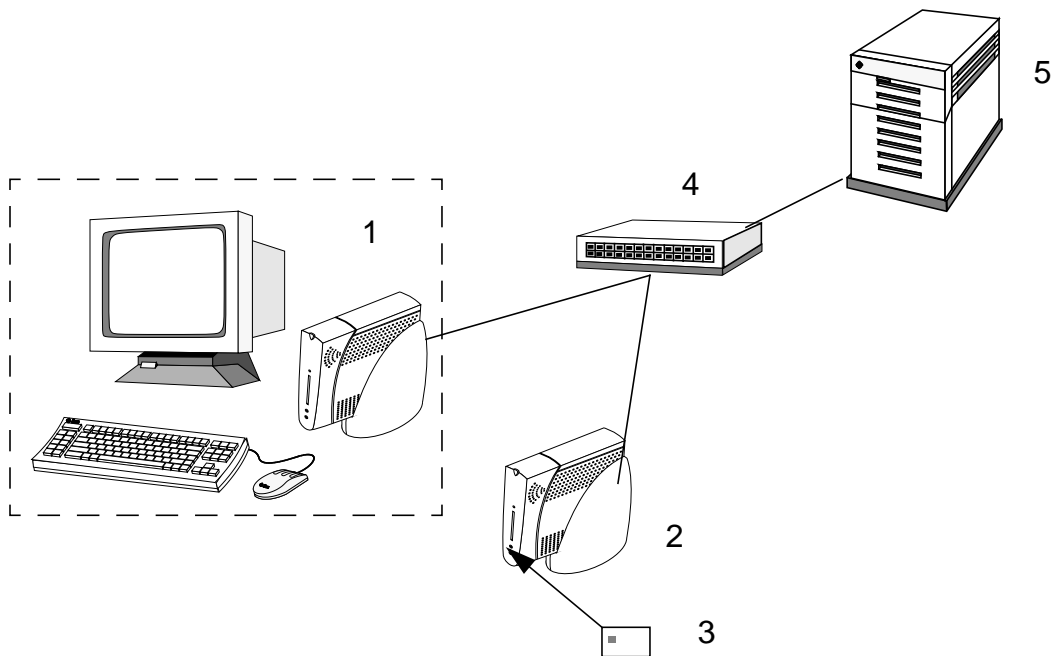


FIGURE 7-1 Using a Token Reader to Register Smart Cards

Legend:

1. Personal enterprise appliance
2. Token reader appliance
3. Smart card
4. Switch
5. Server

The site administrator still uses a personal enterprise appliance in a normal fashion, but connects an additional appliance(s) to the same server as a token reader(s). Note that the Token Reader will not be used for normal Sun Ray services, so it does not need a keyboard, mouse, or monitor connected to it. For information on locating Token Readers, refer to “Locating Token Readers” on page 127.

Once the Sun Ray server software has been configured so that this extra appliance(s) is designated as a token reader(s), the site administrator can tell the administration applications to read a smart card’s ID instead of typing it in.

To Configure a token reader, read “Choosing an Authentication Policy” on page 70, then follow the procedure, “To Configure a Token Reader” on page 73.

Using the Administration Application

The Sun Ray server software provides two ways to use the administration application, a web-based graphical interface and a command-line interface.

Web-Based Interface (Logging In)

If you chose to install and configure the supporting software required to run the web-based interface of the administration application, you can administer your Sun Ray users and appliances from a web browser.

Note – The HotJava™ Browser is not supported. Both the Netscape 4.05 Communicator (or higher) and Internet Explorer 4.0 (or higher) are recommended.

▼ To Log Into the Web-Based Interface

1. **Log into your Sun Ray server’s console or any enterprise appliance attached to it and start up your normal windowing environment.**
2. **Start your preferred browser, such as Netscape™ Communicator.**
3. **Type the following URL in the browser’s location field:**

`http://<hostname>:1660`

Note – If you chose a different port when you configured the Sun Ray supporting software, substitute it for the “1660” in the URL above.

A login screen similar to the following one appears:



FIGURE 7-2 Login Frame

If you get a message denying access, make sure that:

- You are running a browser on the Sun Ray server or one of its appliances.
 - The browser is *not* using a different machine as an HTTP proxy server to proxy the connection to the web server.
4. Enter the administrator username `admin` and the UT administration password you specified when you configured the Sun Ray server software.
 5. If a different locale is desired, select one from the Language pulldown list.

Note – Ensure that correct X server fonts (associated with a chosen locale) are loaded and the correct locale is set, before changing the language. It is also recommended that you do not override the browser fonts. Use default fonts as specified in the HTML standard.

6. Click the Log In button.

The Sun Ray Main Administration page displays and your administration login session begins. Once the administrator logs into the system, the login link changes to *logout* to reflect the administrator's status.

Click on the Refresh button to refresh the data displayed on the Main Administration page. For information on the information displayed on the Systems Status frame, refer to TABLE 8-2.



FIGURE 7-3 Main (Initial) Administration Page

Administration login sessions are limited to 30 minutes for security reasons. Once 30 minutes of inactivity occurs, you are asked to log in again. You can log out at any time by clicking on the Logout link on the navigation frame.

7. Select a category to examine.

- Admin—Provides links to password, policy, and reset services and to token reader information. See “Managing Sun Ray 1 Appliances” on page 97 for further instructions on using the web-based interface.

- Desktops—Provides links for view all, view current, and find desktop information. See “Managing Sun Ray 1 Appliances” on page 97.
- Failover—Provides a link to the failover status frame information. See “Viewing Failover Group Status” on page 115. For additional information on configuring the failover feature, refer to the *Sun Ray Enterprise Server Software 1.1 Advanced Administrator’s Guide*.
- Log Files—Provides links to view the contents of the message log, authentication log, administration log, as well as archived logs. Refer to “Examining Log Files” on page 121 for additional information.
- Smart Cards—Provides links for configuring, probe order, and adding and deleting smart cards. Refer to “Managing Smart Cards From Different Vendors” on page 165 for additional information.
- Status—Provides a link to the summary status frame. “Viewing System Status” on page 100.
- Users—Provides a link to perform user-centric tasks (view by ID, add user, etc.). Refer to *Chapter 8* for more detailed information.
- Online Documents—Provides a link to locale-specific online documentation. Refer to “Accessing Online Documentation” on page 131
- Logout—Allows the system administrator to logout of a session.

Command-Line Interface

The command-line interface of the administration application is offered through two programs, `utuser` (for managing users) and `utdesktop` (for managing desktops). These programs are both installed in `/opt/SUNWut/sbin`, which you can add to your path if you expect to use them frequently.

The command-line programs offer more functionality than their web-based equivalents and add batch operations for performing management operations on multiple users or appliances with a single command.

▼ To Use the Command-Line Interface

1. **Log in to the Sun Ray server.**
2. **Become superuser.**

Note – The command-line programs can be run as superuser or as a normal non-privileged user. However, superuser root is required for any operations that change or delete any administration data. Other operations (for example, listing users) can be run by normal users.

3. Run the appropriate `utdesktop` or `utuser` command.

Please see “Managing Sun Ray 1 Appliances” on page 97 and “Managing Sun Ray Users” on page 135 for further instructions on using the command-line interface.

Managing Sun Ray 1 Appliances

This chapter describes how to use the Sun Ray web-based and command-line administration application to manage your Sun Ray 1 enterprise appliances. The following procedures for managing appliances (desktops) are covered:

- “Main Administration Page” on page 98
- “Changing the Administrator’s Password” on page 99
- “Viewing System Status” on page 100
- “Listing All Desktops” on page 103
- “Searching for Desktops” on page 105
- “Listing Currently Connected Desktops” on page 107
- “Listing Desktops in Dump Format” on page 108
- “Displaying a Desktop’s Current Properties” on page 109
- “Editing Single Desktop’s Properties” on page 112
- “Editing the Properties of Multiple Desktops” on page 113
- “Viewing Failover Group Status” on page 115
- “Examining Log Files” on page 121
- “Reset/Restart Sun Ray Services” on page 126
- “Smart Card Usage and Solaris Lock Screen” on page 132
- “Ordering Sun Ray 1 Smart Cards” on page 133

See “Administration Application” on page 87, for background about Sun Ray 1 appliances and the administration application.

For the web-based interface, this chapter assumes you have already launched your browser, and logged in to the web-based application. All of the functionality detailed in this chapter can be reached from the Main (initial) Administration page, as shown in FIGURE 8-1.

For the command-line interface, this chapter assumes you are logged into the Sun Ray server as superuser, have /opt/SUNWut/sbin in your path, and are at a shell prompt.

Main Administration Page

The Main Administration page is initial page displayed once a system administrator successfully logs into the server.

Sun Ray 1 Administration

Summary status for server netraj118

SunRay Policy

Current SunRay Policy: policy

DeskTop Summary Status

Units Connected:	3
Units Disconnected:	0
Token card readers:	1

User Summary Status

Users in database:	0
Users logged in:	3
Users logged out:	-3
Inactive sessions:	0
Enabled cards:	0
Disabled cards:	0
Users logged in with cards:	3
Users logged in without cards:	0

System Information

Description	kbytes	Used	Available
Root File System	120455	33785	89670
Swap Space	1856232	1112	1855120

Refresh

FIGURE 8-1 Main Administration Page

For additional information on the Summary Status data “Viewing System Status” on page 100.

Changing the Administrator's Password

▼ To Change the Administrator's Password

The password allows an administrator to use the Administration application to access and change Sun Ray administration data. Without a password, administrator's can access, but can not change the Sun Ray administration data.

1. **From the Main Administration menu, click on Admin►Password.**

A frame similar to the following display.

Change Admin Password

Current password:

New password:

Reenter new password:

FIGURE 8-2 Changing Administrator's Password Frame

2. **Enter current password.**
3. **Enter a new password.**
4. **Re-enter the new password.**
Click Reset Fields if to clear the fields and start again.

Note – Refer to the `passwd` man page for information on proper syntax for passwords.

5. Press the Change button.

The new password takes affect and the LDAP data hierarchy is updated.

TABLE 8-1 Change Admin Password Properties Descriptions

Option	Description
Current Password	Field for the current password
New Password	Field for the new password
Reenter New Password	Field for the new password to be entered a second time.

Viewing System Status

▼ To View System Status

- 1. From the Main Administration menu, click on Status►Summary Status.**

A frame similar to the following displays.

Summary status for server nimbus

SunRay Policy			
Current SunRay Policy:		policy	
DeskTop Summary Status			
Units Connected:		0	
Units Disconnected:		0	
Token card readers:		0	
User Summary Status			
Users in database:		2	
Users logged in:		0	
Users logged out:		2	
Enabled cards:		2	
Disabled cards:		0	
Users logged in with cards:		0	
Users logged in without cards:		0	
System Information			
Description	kbytes	Used	Available
Root File System	2548941	704282	1844659
Swap Space	2083800	24	2083776

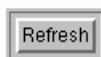


FIGURE 8-3 System Status Frame

Clicking on the Refresh button displays the most current system statistics.

TABLE 8-2 System Status Frame Field Descriptions

Options	Description
Sun Ray Policy	
Current Sun Ray Policy	Current policy name is displayed here.
DeskTop Summary Status	
Units attached	Total number of Sun Ray 1 appliances attached to the interconnect fabric.

TABLE 8-2 System Status Frame Field Descriptions

Options	Description
Units logged in	Total number of Sun Ray 1 appliances logged into of the Sun Ray server.
Units logged out	Total number of Sun Ray 1 appliances logged off of the.Sun Ray server.
Token card readers	Total number of Sun Ray 1 appliances designated as token card readers attached to the interconnect fabric.
User Summary Status	
Users in database	Total number of users in the LDAP database.
Users logged in	Total number of users logged in to the system.
Users logged out	Total number of users who have logged off in a specified time frame.
Inactive sessions	Total number of inactive sessions.
Enabled cards	Total number of enabled smart cards.
Disabled cards	Total number of disable smart cards.
Users logged in with cards	Total number of users logged in with smart cards.
Users logged in without cards	Total number of users logged in not using smart cards.
System Information	
Root File System	Total, used and available disk space available for the Sun Ray server.
Swap Space	Total, used and available swap space available for the Sun Ray server.
Memory	Total, used and available memory available for the Sun Ray server.

Listing All Desktops

▼ To List All Desktops From the Web-Based Interface

1. From the Main Administration menu, click on Desktops>View All.

A table similar to the following displays in the body frame, with the complete list of desktops in the administration database. If more than one page of information is displayed, use the Previous (previous page of data), Next (next page of data) or Home (returns to first page) links to navigate.

View All Desktops

Desktop ID	Location	Other Info
080020b56513		
080020b5653c		
080020b60d30		

Home Previous Next

FIGURE 8-4 List All Desktops Frame

2. Use the navigation buttons at the bottom of the page to view additional pages of results of more than 20 desktops.

The buttons allow you to view the next 20 desktops, previous 20 desktops, or to go back to the first page of 20 desktops. Refer to TABLE 8-3 for additional information.

TABLE 8-3 View All Desktop Properties Fields

Option	Description
Desktop ID	This is the desktop's unique ID (the appliance's Ethernet address).
Location	An optional field that administrators can fill out to identify the appliance's location.
Other Info	An optional field that administrators can fill out to display any additional information associated with the appliance.

▼ To List All Desktops From the Command-Line Interface

- **Type the following command:**

```
# utdesktop -l
```

This command displays the complete list of desktops in the administration database. For example:

```
# utdesktop -l

Desktop ID      Location                Other Info
-----
08002086e18f   SFO12-2103             Token Reader
080020a85112   SFO12-210              John Smith's office
080020a8512c   SFO12-2105             John Smith's office

3 desktops total.
```

Searching for Desktops

▼ To Search for Desktops From the Web-Based Interface

1. Click **Desktops**►**Find desktop**.

The Find Desktop frame appears.

Find Desktop

- Search for All Desktops that Contain:

Desktop ID: and

Location: and

Other Info:

2. From the Find Desktop page, fill out the Desktop ID, Location, and Other Info fields with the values you want to search on.

3. Press the Search button.

A results page similar to the following is shown, displaying all matches in the administration database. If more than one search value is entered, the search performs a logical AND. Only those results that match all the specified values are returned.

Find Desktop

Desktop ID	Location	Other Info
080020b56513		

Home Previous Next

FIGURE 8-5 Search Results Frame

4. Use the navigation buttons at the bottom of the page to view additional pages of results of more than 20 desktops.

▼ To Search for Desktops From the Command-Line Interface

- Type the following command:

```
# utdesktop -li <substring>
```

Where *<substring>* is the full or partial Desktop ID you want to search for. This command displays the list of appliances in the administration database whose Token IDs match this substring. For example:

```
# utdesktop -li a851

Desktop ID      Location      Other Info
-----
080020a85112   SFO12-2103
080020a8512c   SFO12-2105   John Smith's office

2 desktops total.
```

Listing Currently Connected Desktops

▼ To List Currently Connected Desktops From the Web-Based Interface

Note – The Authentication Manager must be operating to perform these procedures.

1. Starting at the Main Administration page, click **Desktops**►**View current**.

A frame similar to the following displays, listing only the desktops that are currently connected to this Sun Ray server and communicating with the Authentication Manager or any other Sun Ray server in the same failover group as this Sun Ray server.

View Current Desktops

Desktop ID	Location	Other Info	Current User
080020b56513			pseudo.080020b56513
080020b5653c			mondex.9998008800007658
080020b60d30			pseudo.080020b60d30

[Home](#) [Previous](#) [Next](#)

FIGURE 8-6 List of Current Desktops Frame

2. Use the navigation buttons at the bottom of the page to view additional pages of results of more than 20 desktops.

The buttons allow you to view the next 20 desktops, previous 20 desktops, or to go back to the first page of 20 desktops.

▼ To List Currently Connected Desktops From the Command-Line Interface

1. Type the following command:

```
# utdesktop -lc
```

The command lists only the desktops that are currently connected to this Sun Ray server and communicating with the Authentication Manager or any other Sun Ray server in the same failover group as this server. For example:

```
# utdesktop -lc

Desktop ID   Location                Current User
-----
080020a85112 SFO12-2103             MicroPayflex.00004f9665000100 (John Parker)
080020a8512c SFO12-2105

2 desktops currently connected.
```

2. Type the following command to get a longer listing:

```
# utdesktop -Lc
```

The longer listing displays the same information as the normal listing, but adds the *Other Info* column.

3. Or you can view currently connected desktops and the servers they are connected to by typing the following command:

```
# utdesktop -G
```

Listing Desktops in Dump Format

There is no web-based interface for this procedure.

▼ To Output the Desktop List in Dump Format From the Command-Line Interface

- Type the following command:

```
# utdesktop -o
```

The command outputs the full list of desktops from the administration database in comma-delimited format. For example:

```
# utdesktop -o
08002086e18f,SFO12-2103,Token Reader
080020a85112,SFO12-2103,
080020a8512c,SFO12-2105,John Smith's office
```

The format of each line is:

```
<Desktop ID>,<Location>,<Other Info>
```

This output can be saved to a file and used later to perform a batch edit operation. For example, use this command when moving or upgrading a Sun Ray enterprise server.

Displaying a Desktop's Current Properties

▼ To Display a Desktop's Current Properties From the Web-Based Interface

1. Starting at the **Desktops** page, perform a list or search operation (see FIGURE 8-4, FIGURE 8-5, or FIGURE 8-6).
2. Click on the **Desktop ID** hyperlink for the desktop of interest.

A frame similar to the following displays:

Desktops

Current Properties:

Desktop ID: 080020b56513
Model: CoronaP1
Firmware erikse200001121516,Boot:1.3;
Revision: 1999.05.18-15:14:06-PDT
Location:
Other Info:

Token Reader: No
Current Status: Up
Last Status Update at: Tue 18 Jan 2000 12:36:17 PM PST
First Connection: Tue 18 Jan 2000 12:36:17 PM PST
Current User: [pseudo_080020b56513](#)

Edit Properties

FIGURE 8-7 Desktop Properties Frame

The page shows information about the appliance (desktop) as obtained from the administration database and Authentication Manager. The following fields are displayed:

TABLE 8-4 Desktop Properties Fields

Option	Description
Desktop ID	The desktop's unique ID (the appliance's Ethernet address).
Model	The desktop model.
Firmware Revision	The version of the firmware currently loaded in the desktop.
Location	An optional field that administrators can fill out to identify the appliance's location.
Other Info	An optional field that administrators can fill out to display any additional information associated with the appliance.

TABLE 8-4 Desktop Properties Fields (*Continued*)

Option	Description
Token Reader	Specifies whether the appliance is set up as a token reader.
Current Status	The current state of the appliance: up or down.
Last Status Update at	The date and time that the Current Status field was last updated.
First Connection	The date and time the appliance was first recognized by the Sun Ray server.
Current User	The Token ID of the current smart card user. If the user is registered, the user's name is displayed as well.

▼ To Display a Desktop's Current Properties From the Command-Line Interface

- Type the following command:

```
# utdesktop -p <Desktop ID>
```

Where *<Desktop ID>* is the ID you want to get properties for. The command displays all information about the specified desktop, as obtained from the administration database and Authentication Manager. For example:

```
# utdesktop -p 080020a85112

Current Properties:
Desktop ID           = 080020a85112
Model                = CoronaP1
Firmware Revision    = 1.0,REV=1999.04.22.19.24
Location             = SFO12-2103
Other Info           =

Current Status       = Up
Last Status Update at = 04/29/1999 16:06:38
First Connection     = 04/29/1999 15:40:04
Current User         = MicroPayflex.00004f9665000100 (John Parker)
```

See TABLE 8-4 for descriptions of the fields displayed.

Editing Single Desktop's Properties

▼ To Edit Single Desktop's Properties From the Web-Based Interface

1. Starting at the Desktop Properties frame for the desktop you want to edit, click the **Edit Properties** button.

A frame similar to the following displays.

Edit Desktop Properties

To edit this desktop's properties, change any of the editable fields below and press **Save Changes**.

Desktop ID: 080020b56513

Model: CoronaP1

Firmware: erikse200001121516,Boot:1.3;

Revision: 1999.05.18-15:14:06-PDT

Location:

Other Info:

Token Reader: Yes No

Current Status: Up

Last Status Update at: Tue 18 Jan 2000 12:36:17 PM PST

First Connection: Tue 18 Jan 2000 12:36:17 PM PST

Current User: [pseudo_080020b56513](#)

FIGURE 8-8 Edit Desktop Properties Frame

2. Change any of the editable fields. When finished, click the Save Changes button. The changes are saved to the administration database.

▼ To Edit Single Desktop's Properties From the Command-Line Interface

- Type the following command:

```
# utdesktop -e "<Desktop ID>, <Location>, <Other Info>"
```

Where *<Location>* and *<Other Info>* can be left empty if you want to clear the respective field. The command updates the desktop's information in the administration database. For example:

```
# utdesktop -e "080020a85112,SFO12-2103,John's Office"
1 Desktop Modified
```

To specify one of the optional fields, enter no text between the commas. The following example clears the Location field:

```
# utdesktop -e "080020a85112,,John's Office,"
1 Desktop Modified.
```

Tip – Use the output of the `utdesktop -o` command as input to this command (line by line). Remember to put quotes around the data.

Editing the Properties of Multiple Desktops

There is no web-based interface for this procedure.

▼ To Edit the Properties of Multiple Desktops From the Command-Line Interface

1. Prepare a file with the desktop information. Each desktop should be on a separate line. For example:

```
<Desktop ID>, <Location>, <Other Info>
```

Note – You can use the output of `utdesktop -o` to create this file.

2. Type the following command:

```
# utdesktop -ef <filename>
```

where *<filename>* is the desktops file you created in Step 1. For each line in the specified file, the command checks to see if any modifications have been made, and when found, saves them to the administration database,

For example:

```
# utdesktop -o > desktops
# cat desktops
08002086e18f,SF012-2103,Token Reader
080020a85112,SF012-2103,
080020a8512c,SF012-2105,John Smith's office
# vi desktops
# cat desktops
08002086e18f,SF012-2103,Token Reader
080020a85112,SF012-2103,Desktop 1
080020a8512c,SF012-2105,Desktop 2
# utdesktop -ef desktops
No modifications necessary for 08002086e18f.
Modified 080020a85112
Modified 080020a8512c

2 desktops modified
1 desktop did not require changes
```

Viewing Failover Group Status

The Failover Group Status frame (FIGURE 8-9) describes the health and current state of multiple Sun Ray servers within your failover group. It also describes the health of any Sun Ray servers that have responded to a Sun Ray broadcast.






- The Failover Group Status frame provides information on group membership and network connectivity.
- Sun Ray servers are constantly gathering information from other Sun Ray servers including their interface configuration and reachability.
- Failover Group Status only displays public networks and Sun Ray interconnect fabrics.

For example, in FIGURE 8-9, the second column (from the left) is public network (denoted by the 192.144.167.0 IP address). The third and fourth columns display information on two Sun Ray interconnect fabrics.

Note – The Sun Ray server broadcasts do not traverse over routers or non-Sun Ray servers.

For more information on Failover Groups refer to the *Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide*. TABLE 8-5 describes the Failover Group status icons.

TABLE 8-5 Sun Ray Failover (F/O) Group Status Icons

Icons	Name/Description
	Sun Ray fabric: A Sun Ray interconnect fabric is established and functioning properly.
	Sun Ray fabric - Unreachable: A Sun Ray interconnect fabric is not established. This network is unreachable from the server performing the Failover Group Status. This appears in two scenarios: an alert and a failover situation. The administrator must investigate this situation.
	No-connect: the servers are unreachable. This network is unreachable from the server performing the Failover Group Status. This could be an alert situation. Over a public network the conditions could be normal, except for the Sun Ray broadcast information, which can not traverse over routers.
	Server Up: represents an unconnected server within the group. This icon only occurs in a (row) public network display. It reinforces the fact that the displayed information is from the perspective of the system performing the Failover status.
	Group: Servers that appear in the same group use this icon. The signature files, <code>/etc/opt/SUNWut/gmSignature</code> , on those two machines are identical. Also identifies systems as trusted hosts. Failover will occur for any Sun Ray appliances connected between these systems. The <code>utgroupsig</code> utility is used to set the <code>gmSignature</code> file. Refer to the <i>Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide</i> for information regarding the <code>gmSignature</code> file and <code>utgroupsig</code> utility.

▼ To View Failover Group Status

1. **Starting at the Main Administration page select Failover►Status.**

The Failover Group Status frame appears (FIGURE 8-9).

Sunray F/O Group Status		Server: Sunray5		
(d)				
Sunray5 Group Status				
Network / Netmask				
	129.144.167.0 / 24	192.168.128.0 / 24	192.168.140.0 / 24	
Sunray5 (a)	129.144.167.5	192.168.128.2	192.168.140.1	(c)
Sunray11 (b)	129.144.167.11	192.168.128.1		
Sunray41	129.144.167.41	192.168.128.1		(c)
Sunray55	129.144.167.55	192.168.128.2		

FIGURE 8-9 Failover Group Status Frame

Interpreting Failover Group Status Information

The status screen displays all of the Sun Ray servers that it sees and identifies group members. It identifies trusted hosts with a group icon (refer to TABLE 8-5), which indicates the server is in a failover group. It also displays, in column format, all of the identified networks (on a per server basis) and whether those networks are public networks or Sun Ray interconnect fabrics. It also lists each server's IP address.

For example, in FIGURE 8-9 there is one public network and two Sun Ray interconnect fabrics. Sun Ray 5 (a) has the potential for failover for all of the Sun Ray appliances that its on the 192.168.128.1 network. On the 192.168.140.0 network (e) they are not intended for failover and considered completely private to Sun Ray 5 (a).

Note – The Sun Ray server performing the Failover Group Status should also be reflected in the header of the status frame. For example, notice that Sun Ray 5 is called out in both (a) and (d) locations.

The Sun Ray 5 server can currently communicate with those IP addresses shown in the Failover Group Status frame. Out of all of those addresses, Sun Ray 11 (b) is the only server in the same group as Sun Ray 5. They share the same “Group icon.”

Established connections to servers appear in the upper-left hand quadrant of the frame and propagate outward from that location. It is normal to have open cells in the frame.

Note – The /24 in the IP addresses is Common InterDomain Routing (CIDR) notation for the subnet mask. This represents the number of bits that are significant as part of the netmask. For example, /24 is the same as 255.255.255.0.

The network/netmask headings (xxx.xxx.xxx.x/24) refer to all of the networks that are observed. Group Membership is represented by the group Icon. Other Sun Ray servers that are visible on the screen, may also be members of another group. That information is not visible until you select a different server, to change the point of view, which refreshes the broadcasted information and reveals other groups. It is possible that multiple groups may be using the same network IDs for their private interconnect fabrics and this is considered a legitimate configuration. For example, the group Sun Ray 5 and Sun Ray 11 are using a specific network. The connection only exist between those two servers. However, at the same time Sun Ray 41 and Sun Ray 55.

From the Sun Ray 41 point of view, the 192.168.128.1 interconnect fabric is functional. However, from Sun Ray 5's point of view, the Sun Ray 41's 192.168.128.0 network is unreachable (the address space is the same). This means that since two failover groups are using the same network, it could be considered a legitimate configuration. The important note to remember is that they are not sharing a common physical network, just the name for the network.

TABLE 8-6 Icon Background Definitions

Background Color	Description
Dark Blue	Connected
Light Blue/Grey	Alert. Network connection status has changed recently.

Example Configurations

An administrator could have several servers (in separate groups) and two of the servers are in one group and two others in another group. They may be connected to the public network, but also have private networks that span between the two servers (in separate groups).

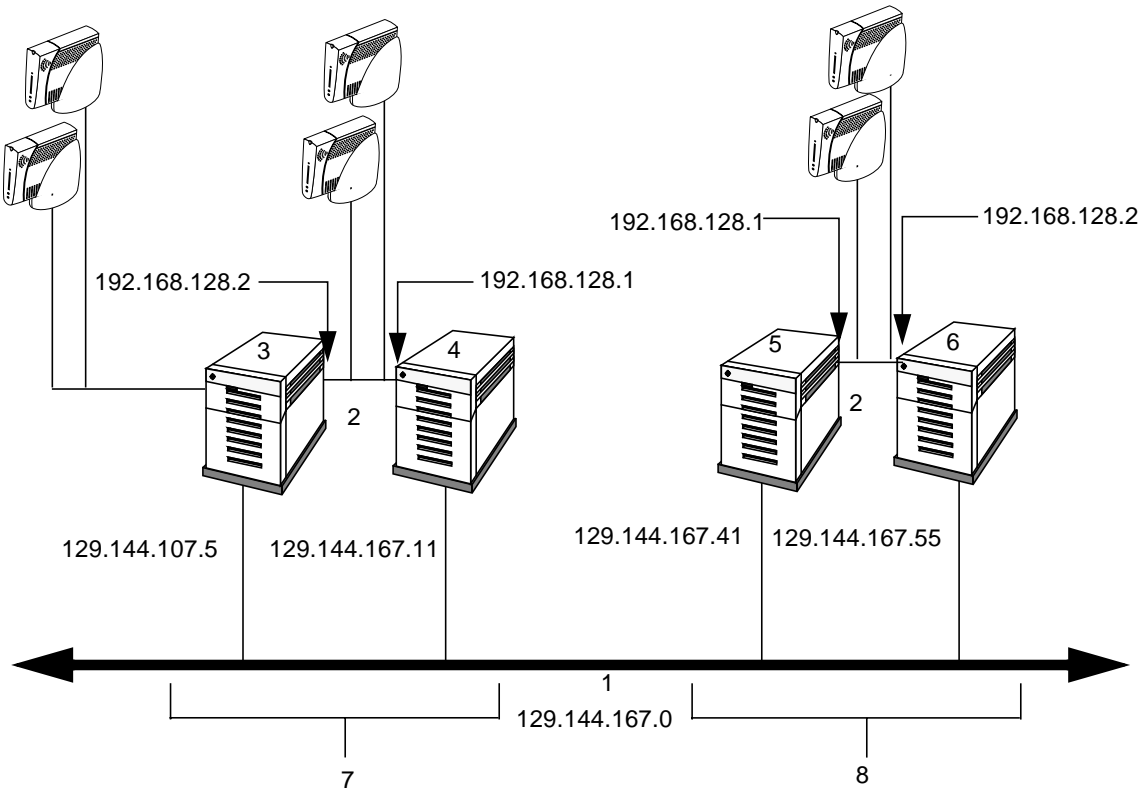


FIGURE 8-10 Sample Network Configuration

Legend:

1. Public Network (129.144.167.0)
2. A= private network (192.168.128.0)
3. Sun Ray 5 Sun Ray enterprise server
4. Sun Ray 11 Sun Ray enterprise server
5. Sun Ray 41 Sun Ray enterprise server
6. Sun Ray 55 Sun Ray enterprise server
7. Failover Group 1
8. Failover Group 2

In FIGURE 8-10, both networks are classified as private networks and are connected to a public network. Sun Ray 5 also uses a private network. Notice that Sun Ray 5 and Sun Ray 41 use the same IP address, but are not physically connected. This is the same situation for Sun Ray 11 and 55. Both private networks, in both segments, have exactly the same amount of address space. Consequently, they never connect and since this is a private network there are no address conflicts.

Examining Log Files

Every time a file is retrieved from the Sun Ray server, it is recorded. The server stores this information in text files. Both the authentication log and the message log files have a numeral as an extension. Many administration activities are logged (including).

- Policy changes
- Login/logout
- Timeout
- Failed login
- Modifying a policy
- Changing a password
- Interrupting a service, user or desktop

Log files which can be viewed from the SunRay server include:

Messages Log File (`/var/opt/SUNWut/log/messages`) - Lists events from the server's appliances including detail of registration, insertion or removal of smart card. The messages log file is aged daily and archived files are stored on the server for 1 week and are annotated using numeral extensions (for example, from `messages.0` to `messages.5`). Refer to FIGURE 8-11.

Authentication Log File (`/var/opt/SUNWut/log/auth_log`). Lists events logged from the authentication manager. The `auth_log` file is aged (up to a limit of 10) every time the server's authentication policy is changed and whenever it is started. The archived authentication files are annotated using numeral extensions (for example, from `auth_log.0` to `auth_log.9`).

Administration Log File (`/var/opt/SUNWut/log/admin_log`). Lists operations performed when administering the server. This log is aged daily and archived files which are stored on the system for up to one week are annotated using numerical extensions (for example, from filename `admin_log.0` to `admin_log.5`).

The following sections describe how to access a log file.

Viewing Message Logs

▼ To View Messages Logs

1. Starting at the Main Administration page select **Users**►**Messages Log**.

The Message Log File frame appears. Use the slider bar to access data to the right of the frame.

Message Log File

Size: 12 KB

Date last modified: Wed Jan 5 16:56:24 2000

```
Jan 5 16:10:54 netraj118 utauthd: Worker1 NOTICE: Read a byte after a
Jan 5 16:10:55 [192.168.128.51.2.2] 0x0.0x4fcd2 8:0:20:b6:d:30 Applicat
Jan 5 16:10:55 netraj118 utauthd: Worker1 UNEXPECTED: 192.168.128.
Jan 5 16:10:55 netraj118 utauthd: Worker2 NOTICE: whichServer monde
Jan 5 16:10:55 netraj118 utauthd: Worker2 NOTICE: CLAIMED by Zero/
Jan 5 16:10:55 netraj118 utauthd: Worker2 NOTICE: SessionManager.ge
Jan 5 16:10:55 netraj118 utauthd: Worker2 NOTICE: SessionManager.in
Jan 5 16:10:55 [192.168.128.52.2.2] 0x0.0x4fcb8 8:0:20:b5:65:3c Applic
Jan 5 16:10:55 netraj118 utauthd: Worker2 NOTICE: SESSION_OK Zerc
Jan 5 16:10:55 netraj118 utauthd: Worker2 NOTICE: CONNECT Coronal
Jan 5 16:10:58 [192.168.128.53.2.2] 0x0.0x4fca9 8:0:20:b5:65:13 Applic
Jan 5 16:10:58 netraj118 utauthd: Worker2 NOTICE: whichServer pseud
Jan 5 16:10:58 netraj118 utauthd: Worker2 NOTICE: CLAIMED by Zero/
Jan 5 16:10:58 netraj118 utauthd: Worker2 NOTICE: SESSION_OK Zerc
Jan 5 16:10:58 netraj118 utauthd: Worker2 NOTICE: CONNECT Coronal
Jan 5 16:11:01 netraj118 utauthd: Worker2 NOTICE: whichServer at88s
Jan 5 16:11:01 netraj118 utauthd: Worker2 NOTICE: CLAIMED by Zero/
Jan 5 16:11:01 netraj118 utauthd: Worker2 NOTICE: SESSION_OK Zerc
Jan 5 16:11:01 netraj118 utauthd: Worker2 NOTICE: CONNECT Coronal
Jan 5 16:11:01 netraj118 utauthd: Worker2 NOTICE: Read a byte after a
Jan 5 16:11:01 [192.168.128.51.2.2] 0x0.0x24f 8:0:20:b6:d:30 Applicati
Jan 5 16:12:41 netraj118 UTPOLICY: Any command line option other th
Jan 5 16:12:41 netraj118 UTPOLICY: Waiting 60+ seconds to insure tha
Jan 5 16:12:41 netraj118 UTPOLICY: Restarting SunRay services
```

FIGURE 8-11 Message Log File Frame

Viewing Authentication Logs

▼ To View Authentication Logs

1. Start at the Main Administration page select **Log Files**►**Authenticated Logs**.

The Authentication Log frame appears.

Auth Log File

Size: 911 KB

Date last modified: Mon Jan 24 20:03:34 2000

```
socket open failed
get_system_capacity:kstat_open: Too many open files
Error obtaining system capacity
socket open failed
get_system_capacity:kstat_open: Too many open files
Error obtaining system capacity
socket open failed
get_system_capacity:kstat_open: Too many open files
Error obtaining system capacity
socket open failed
get_system_capacity:kstat_open: Too many open files
Error obtaining system capacity
socket open failed
get_system_capacity:kstat_open: Too many open files
Error obtaining system capacity
socket open failed
get_system_capacity:kstat_open: Too many open files
Error obtaining system capacity
socket open failed
```

FIGURE 8-12 Authentication Log File Frame

Viewing Administration Logs

▼ To View Administration Logs

1. Start at the Main Administration page select Log Files►Admin Log.

The Administration Log frame appears.

Administration Log File

Size: 2 KB

Date last modified: Wed Jan 19 16:06:07 2000

```
Jan 19 09:49:30 netraj118 admincgi[8167]: User logged in from 129.146.48.201.
Jan 19 09:50:46 netraj118 corona_cgi[8188]: Login attempt failed from 129.146.48.201
Jan 19 09:50:52 netraj118 admincgi[8191]: User logged in from 129.146.48.201.
Jan 19 11:05:53 netraj118 admincgi[8272]: User logged in from 129.144.50.128.
Jan 19 11:06:10 netraj118 user[8299]: Attempting to delete user 'Erik Seilnacht'.
Jan 19 11:06:10 netraj118 user[8299]: Successfully deleted token id 'MicroPayflex.0000b37d6
Jan 19 11:06:10 netraj118 user[8299]: Successfully deleted user for token id 'MicroPayflex.000
Jan 19 11:06:10 netraj118 user[8299]: User 'Erik Seilnacht' deleted.
Jan 19 12:59:07 netraj118 admincgi[8370]: User logged out from 129.144.50.128.
Jan 19 12:59:24 netraj118 admincgi[8376]: User logged in from 129.144.50.128.
Jan 19 12:59:47 netraj118 corona_cgi[8382]: User session timed out for 129.144.50.128.
Jan 19 13:01:24 netraj118 admincgi[8413]: User logged in from 129.144.50.128.
Jan 19 13:05:08 netraj118 admincgi[8444]: User logged in from 129.144.50.128.
Jan 19 13:09:42 netraj118 corona_cgi[8459]: Login attempt failed from 129.144.50.128
Jan 19 13:11:30 netraj118 admincgi[8463]: User logged in from 129.144.50.128.
Jan 19 13:11:41 netraj118 admincgi[8484]: User logged in from 129.144.50.128.
Jan 19 13:12:22 netraj118 corona_cgi[8497]: Login attempt failed from 129.144.50.128
Jan 19 13:12:26 netraj118 admincgi[8500]: User logged in from 129.144.50.128.
Jan 19 13:24:22 netraj118 admincgi[8521]: User logged in from 129.144.50.128.
Jan 19 13:24:41 netraj118 admincgi[8545]: User logged out from 129.144.50.128.
Jan 19 13:24:46 netraj118 admincgi[8552]: User logged in from 129.144.50.128.
Jan 19 13:27:06 netraj118 admincgi[8574]: User logged out from 129.144.50.128.
Jan 19 13:27:11 netraj118 admincgi[8580]: User logged in from 129.144.50.128.
Jan 19 14:21:23 netraj118 admincgi[8625]: User logged in from 129.144.167.5.
Jan 19 15:15:23 netraj118 admincgi[8711]: User logged out from 129.144.167.5.
Jan 19 15:15:33 netraj118 admincgi[8717]: User logged in from 129.144.167.5.
Jan 19 15:19:30 netraj118 corona_cgi[8745]: User session timed out for 129.144.50.128.
Jan 19 15:19:37 netraj118 admincgi[8751]: User logged in from 129.144.50.128.
Jan 19 16:02:32 netraj118 admincgi[8879]: User logged in from 129.146.1.171.
Jan 19 16:06:07 netraj118 admincgi[8924]: User logged in from 129.144.167.5.
```

FIGURE 8-13 Administration Log File Frame

Viewing Archived Logs

▼ To View Archived Logs

1. Start at the Main Administration page select Log Files►Archived Logs.
2. Select the archived file (message log, authentication log, or administration log) you wish to view from the main frame.

The Archived Log frame appears.

Archived Log File

Size: 3 KB
Date last modified: Wed Jan 19 00:14:48 2000

```
Jan 17 10:22:16 netraj110 corona_cg[4025]: Login attempt failed from 129.144.167.5
Jan 17 10:22:23 netraj110 admincg[4029]: User logged in from 129.144.167.5
Jan 17 12:24:50 netraj110 corona_cg[4152]: User session timed out for 129.144.167.5
Jan 17 12:24:56 netraj110 admincg[4158]: User logged in from 129.144.167.5
Jan 17 12:32:47 netraj110 admincg[4182]: User logged in from 129.144.167.5
Jan 17 12:34:32 netraj110 admincg[4233]: User logged out from 129.144.167.5
Jan 18 10:48:28 netraj110 corona_cg[4373]: Login attempt failed from 129.144.167.5
Jan 18 10:48:39 netraj110 corona_cg[4376]: Login attempt failed from 129.144.167.5
Jan 18 10:48:45 netraj110 admincg[4379]: User logged in from 129.144.167.5
Jan 18 10:49:35 netraj110 admincg[4421]: User logged out from 129.144.167.5
Jan 18 10:49:42 netraj110 corona_cg[4427]: Login attempt failed from 129.144.167.5
Jan 18 10:49:54 netraj110 corona_cg[4430]: Login attempt failed from 129.144.167.5
Jan 18 10:50:02 netraj110 corona_cg[4433]: Login attempt failed from 129.144.167.5
Jan 18 10:50:10 netraj110 admincg[4438]: User logged in from 129.144.167.5
Jan 18 12:22:10 netraj110 admincg[4770]: User logged in from 127.0.0.1
Jan 18 12:34:35 netraj110 corona_cg[5960]: User session timed out for 129.144.50.128
Jan 18 12:34:39 netraj110 admincg[5967]: User logged in from 129.144.50.128
Jan 18 13:54:35 netraj110 admincg[6417]: User logged out from 129.144.50.128
Jan 18 13:54:39 netraj110 admincg[6424]: User logged in from 129.144.50.128
Jan 18 14:03:53 netraj110 admincg[6464]: Attempt to change ldap password succeeded
Jan 18 14:03:53 netraj110 admincg[6464]: Attempt to update password file succeeded
Jan 18 14:03:53 netraj110 admincg[6464]: Password successfully changed
Jan 18 14:04:03 netraj110 admincg[6464]: <2> cgi elapsed time = 0.1774 sec
Jan 18 14:04:03 netraj110 admincg[6484]: Attempt to change ldap password succeeded
Jan 18 14:04:03 netraj110 admincg[6484]: Attempt to update password file succeeded
Jan 18 14:04:03 netraj110 admincg[6484]: Password successfully changed
Jan 18 14:04:03 netraj110 admincg[6484]: <2> cgi elapsed time = 0.1352 sec
Jan 18 14:33:03 netraj110 admincg[6829]: User logged in from 129.144.52.77
Jan 18 14:44:13 netraj110 admincg[6982]: User logged in from 129.144.167.5
Jan 18 16:07:58 netraj110 corona_cg[7150]: User session timed out for 129.144.50.128
Jan 18 16:08:01 netraj110 admincg[7156]: User logged in from 129.144.50.128
Jan 18 16:08:10 netraj110 admincg[7170]: Attempt to change ldap password succeeded
Jan 18 16:08:10 netraj110 admincg[7170]: Attempt to update password file succeeded
Jan 18 16:08:18 netraj110 admincg[7178]: Password successfully changed
Jan 18 16:08:18 netraj110 admincg[7178]: <2> cgi elapsed time = 0.1523 sec
Jan 18 16:08:29 netraj110 admincg[7193]: Attempt to change ldap password succeeded
Jan 18 16:08:29 netraj110 admincg[7193]: Attempt to update password file succeeded
Jan 18 16:08:29 netraj110 admincg[7193]: Password successfully changed
Jan 18 16:08:29 netraj110 admincg[7193]: <2> cgi elapsed time = 0.1470 sec
Jan 18 17:31:34 netraj110 corona_cg[7277]: User session timed out for 129.144.52.77
Jan 18 17:31:44 netraj110 admincg[7283]: User logged in from 129.144.52.77
Jan 18 22:04:41 netraj110 admincg[7597]: User logged in from 129.144.52.77
Jan 18 22:34:20 netraj110 admincg[7660]: User logged in from 129.144.52.77
Jan 19 00:14:48 netraj110 policy[7633]: Enter modifying group policy '-a -g -z both'
```

FIGURE 8-14 Archived Log File Frame

Reset/Restart Sun Ray Services

▼ To Reset Sun Ray Services

1. **Starting at the Main Administration page select Admin►Reset Services.**

The Sun Ray Services frame appears (FIGURE 8-15).

Sun Ray Services

Press **Reset** to reset the Sun Ray services and preserve all sessions.
Press **Restart** to terminate all sessions and restart the Sun Ray services.



FIGURE 8-15 Sun Ray Services Reset/Restart Frame

2. **Select Reset.**

The Sun Ray services are reset and the sessions are preserved.

▼ To Restart Sun Ray Services

1. **Starting at the Main Administration page select Admin►Reset Services.**

The Sun Ray Services frame appears (FIGURE 8-15).

2. **Select Restart.**

All sessions are immediately terminated and the Sun Ray services are restarted.

Locating Token Readers

The Administration application can locate Sun Ray appliances that have been designated as token readers. These dedicated appliances can be used by site administrators to administer Sun Ray users. Token readers use the smart card ID to register users. Some manufacturers print the smart card ID on the card itself, but many do not. Since all of the administrative functions refer to this token ID, the Sun Ray server software provides a way to designate one or more specific enterprise appliances as dedicated token readers. If you enable an authentication policy with registered users, you need to identify smart card IDs.

▼ To Locate Token Readers

- Starting at the Main Administration page select Admin►Token Readers.

The Token Readers frame appears. In FIGURE 8-16 only one Sun Ray 1 appliance is listed as a token reader. If more than one page of information is displayed, use the Previous (previous page of data), Next (next page of data) or Home (returns to first page) links to navigate.

Token Readers

Desktop ID	Location	Other Info	Current User
080020b5653c			

Home Previous Next

FIGURE 8-16 Token Readers Frame

Restarting Sun Directory Services

If you restart the Sun™ Directory Services daemon (`dsserv`), you need to restart the Sun Ray Authentication Manager. The Sun Directory Services (SunDS) daemon might need to be restarted if you change one of its configuration parameters. The following procedure shows the correct order of steps to take if you need to restart SunDS.

▼ To Restart Sun Directory Services

1. Stop the Sun Ray services:

```
# /etc/init.d/utsvc stop
```

2. Stop the SunDS daemon:

```
# /etc/init.d/dsserv stop
```

3. Start the SunDS daemon:

```
# /etc/init.d/dsserv start
```

4. Restart the Sun Ray services:

```
# /etc/init.d/utsvc start
```

Changing Policies

Changing policies involves changing the policy scope. The scope is either local or group (default). For a normal configuration (Group) all policies are the same on all Sun Ray servers (FIGURE 8-17). If the administrator needs to override the default setting, they can choose the Local setting. The local setting binds the policy to the current server and is not applied to other Sun Ray servers.

Note – It is recommended to have the same policies on all of the Sun Ray servers in the same failover group. For example, if all of the servers are configured to use the same policies, then when a failover occurs, all policies are remain consistent.

Changing group policies affects all Sun Ray servers in the same group.

Solaris Authentication Considerations

If users are registered you can then indicate whether they need to be authenticated by solaris by entering valid username and password. The administrator can ensure that this happens by selecting the Self Registration Requires Solaris Authentication radio button in the Change Policy frame (FIGURE 8-17). This is separate from the standard `dtlogin`. For example, if the admin chooses registered, you can have both registered non-smart card users or registered smart card users, or both. But when the admin selects Solaris authentication it refers to any registered user. Non-card users can be defined as psuedo-terminals. Card users are registered users.

Changing the Local/Group Policy

▼ To Change the Local/Group Policy

1. **Starting at the Main Administration page select Admin►Policy.**
The Change Policy frame appears (FIGURE 8-17).

Change Policy

To change the active policy, select the desired settings and press **Apply**.
If the policy scope is set to Group (default), policy changes will be applied to all corona servers within the group.

Card Users	Non-Card Users
Access: <input checked="" type="radio"/> All Users <input type="radio"/> Registered Users <input type="checkbox"/> Allow Self Registration <input checked="" type="checkbox"/> Self Registration Requires Solaris Authentication	Access: <input type="radio"/> All users <input checked="" type="radio"/> Registered Users <input checked="" type="checkbox"/> Allow Self Registration
Policy Scope: <input type="radio"/> Group <input checked="" type="radio"/> Local	
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

FIGURE 8-17 Sun Ray Change Policy Frame (Local Policy)

2. Select Card Users or Non-Card Users.

Card users can be defined as registered users. Non-card users can be defined as pseudo-terminals.

3. Select either All Users, Registered Users, or Allow Self Registration.

Registered users were originally registered by the system administrator. Selecting Allow Self Registration includes users who were prompted to self register when they inserted their card. All Users encompasses all types of users.

4. Select Self Registration Requires Solaris Authentication, if applicable.

Refer to “Solaris Authentication Considerations” on page 129 for additional information.

5. Select a Policy Scope to change.

Choose Group to affect all Sun Ray servers in the same group. Choose Local to affect the local (same server) policy.

Accessing Online Documentation

Online documentation is available from within the Administration application. When the system administrator logs into the Administration application a locale is selected. This action determines which language is selected for the online documentation (HTML-based). After a successful login, the following (locales-specific) documents are accessible:

- *Sun Ray Enterprise Server Software 1.1 Installation Guide*
- *Sun Ray Enterprise Server Software 1.1 Administrator's Guide* (this book)
- *Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide*

Note – The Administration application links all languages (locales) to the English HTML documentation. However, the Japanese documentation is provided in HTML format.

▼ To Access Online Documentation

1. **Starting at the Main Administration page select Online Documents.**
2. **Select a document from the list.**

The documentation appears in the body frame.

Smart Card Usage and Solaris Lock Screen

The following commands are used to lock the screen when a user removes the smart card.

End Users Using CDE

End users can type this command to lock the screen for the current session.

```
% /opt/SUNWut/lib/utaction -d '/usr/dt/bin/dtaction LockDisplay' &
```

If the user wants to make this feature the default, the command needs to be placed at the end of the `.dtprofile` file in the user's home directory.

End Users Using OpenWindows

The end users can type this command to lock the screen for the current session. This command needs to be typed on one line.

```
% /opt/SUNWut/lib/utaction -d '/usr/openwin/bin/xlock -delay 1000000 -mode blank'
```

If the user wants to make this feature the default, the command needs to be placed at the end of the `.xinitrc` file in the user's home directory.

System Wide Default

The system administrator can make this the system default by placing this script in `/etc/dt/config/Xsession.d` as an executable file (named, for example, `/etc/dt/config/Xsession.d/0999.screenlock`).

```
#!/bin/ksh
#
# Turn on screen-lock on disconnect for Sun Ray sessions
#

if [ "$DTUSERSESSION" != "" -a "$SESSIONTYPE" != "altDt" ]
then
    /opt/SUNWut/lib/utaction -d '/usr/dt/bin/dtaction LockDisplay' \
    2>/dev/null >/dev/null &
else
    /opt/SUNWut/lib/utaction -d \
    '/usr/openwin/bin/xlock -delay 1000000 -mode blank' \
    2>/dev/null >/dev/null &
fi
```

Ordering Sun Ray 1 Smart Cards

Full commercial orders of smart cards can be placed with your Solaris-Ready vendor. Custom smart cards will bear your company's logo or the vendor's logo. For more information on Sun Ray 1 smart cards, go to the following URL:

<http://www.sun.com/sunray1>

Managing Sun Ray Users

This chapter describes how to use the Sun Ray web-based and command-line administration application to manage your Sun Ray users. The following procedures for managing users are covered:

- “User Fields” on page 136
- “Adding and Deleting Users” on page 136
- “Finding Users” on page 144
- “User Properties” on page 152
- “Administering Tokens” on page 159
- “Managing Smart Cards From Different Vendors” on page 165
- “Smart Card Vendor Configuration Files” on page 175

See “Administration Application” on page 87, for background about Sun Ray users and the administration application. For the web-based interface, this chapter assumes you have already launched a browser, accessed the web-based application and logged in. All of the functionality detailed in this chapter can be reached from the Users page. For the command-line interface, this chapter assumes you are logged into the Sun Ray server as superuser, have `/opt/SUNWut/sbin` in your path, and are at a shell prompt (refer to FIGURE 9-1).

From the Initial Administration page select Users to select an option.

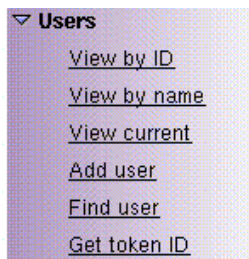


FIGURE 9-1 Users Selection List

User Fields

You can specify the following user fields in the Sun Ray administration database:

TABLE 9-1 Key User Fields

Field	Description
Token ID	The user's unique token type and ID. For smart cards, this is a manufacturer type and the card's serial ID. For enterprise appliances, this is the type "pseudo" and the appliance's Ethernet address. Examples: mondex.9998007668077709 pseudo.080020861234
Server Name	The name of the Sun Ray server the user is using.
Server Port	The Sun Ray server's communication port. This field should generally be set to 7007.
User Name	The user's name.
Other Info	Any additional information you want to associate with the user (for example, an employee or department number). This field is optional.

Adding and Deleting Users

Note – Token Readers: To add a user, insert the user's token into the desired reader and click Get Token ID.

Adding a Single User

▼ To Add a Single User From the Web-Based Interface

To add a user, insert the user's token into the desired reader and click Get Token ID.

1. Starting at the Main page, click on Users►Add User.

A frame similar to the following displays.

Add User

To add a user, insert the user's token in the desired reader and press **Get Token ID** to fill in the Token ID field below. Then fill out the rest of the fields and press **Add User**.

Token Reader:

Token ID:

Server Name:

Server Port:

User Name:

Other Info:

FIGURE 9-2 Add a Single User

2. If you do not know the user's Token ID and have configured a token reader (see "To Configure a Token Reader" on page 73):

- a. Insert the user's token into the selected token reader.**
- b. Choose the selected token reader from the pulldown list of available readers.**
- c. Press the Get Token ID button.**

The application queries the token reader and, if successful, redisplay the form with the Token ID field filled out.

3. Fill out the required fields.

The Other Info field is optional.

4. Press the Add User button.

The user and associated token are created in the administration database.

▼ To Add a Single User From the Command-Line Interface

● Type the appropriate `utuser` command.

a. If you already know the user's Token ID, type:

```
# utuser -a "<Token ID>,<Server Name>,<Server Port>,<User Name>,<Other Info>"
```

This command creates the user and associated token in the administration database. For example:

```
# utuser -a "mondex.9998008800007658,localhost,7007,Eric Seilnacht,C987"
Added 1 user.
```

b. If you do not know the user's Token ID and have configured a token reader, type:

```
# utuser -a "x,<Server Name>,<Server Port>,<User Name>,<Other Info>" -r <Token Reader>
```

where the "x" that is specified instead tells the command to query `<Token Reader>` for the Token ID. You will be prompted to insert the user's token into the Token Reader when the command is ready. Then, the user and the associated token (using the ID obtained from the reader) will be created in the administration database. For example:

```
# utuser -a "x,localhost,7007,Eric Seilnacht,C987" -r 08002086e18f
Insert token into token reader '08002086e18f' and press return.
Read token ID 'mondex.9998008800007658'
Added 1 user.
```

Note – The `<Other Info>` argument is optional.

Adding Multiple Users

There is no web-based interface for this operation.

▼ To Add Multiple Users From the Command-Line Interface

1. Prepare a file with the user information. Each user should be on a separate line:

```
<Token ID>, <Server Name>, <Server Port>, <User Name>, <Other Info>
```

If you do not know the Token ID for a user and have configured a Token Reader, specify an “x” for the Token ID. This tells the command to query a Token Reader for the Token ID (see “To Configure a Token Reader” on page 73).

2. Type the appropriate `utuser` command:

a. If you already specified all Token IDs (and so you do not need to use a token reader), type:

```
# utuser -af <filename>
```

where *<filename>* is the user file you created in Step 1. For each line in the specified file, the command adds the user and associated token to the administration database

For example:

```
# cat users
mondex.9998008800007658,localhost,7007,Eric Seilnacht,C987
mondex.9998008458700965,localhost,7007,John Stone,C2310
mondex.9998007300058900,localhost,7007,Ethan Williams,E1049

# utuser -af users
Added Eric Seilnacht
Added John Stone
Added Ethan Williams

3 users added, 0 lines skipped due to errors.
```

b. If you had to specify “x” for at least one Token ID (in other words, if you need to use a Token Reader), type the following command:

```
# utuser -af <filename> -r <Token Reader>
```

where <filename> is the user file you created in Step 1 and <Token Reader> is the enterprise appliance that you have configured as a Token Reader.

For each line that has an “x” specified, you will be prompted to insert the user’s token into the reader and press return. Lines that have a Token ID already specified will not require prompting. As each line is completed, the command will add the user and associated token to the administration database.

For example:

```
# cat users
x,localhost,7007,Eric Seilnacht,C987
mondex.9998008458700965,localhost,7007,John Stone,C2310
x,localhost,7007,Ethan Williams,E1049

# utuser -af users -r 08002086e18f
Insert token for 'Eric Seilnacht' into token reader '08002086e18f'
and press return.
Read token ID 'mondex.9998008800007658'
Added Eric Seilnacht
Added John Stone
Insert token for 'Ethan Williams' into token reader '08002086e18f'
and press return.
Read token ID 'mondex.9998007300058900'
Added Ethan Williams

3 users added, 0 lines skipped due to errors.
```

Deleting a Single User

▼ To Delete a Single User From the Web-Based Interface

1. Starting at the Main Administration page select **Users>View by name** and click on the name (see FIGURE 9-9) for the user you want to delete.
2. Press the **Yes-Delete This User** button.

A confirmation frame similar to the following appears.

Delete User

Confirm Delete

Are you sure you want to delete user 'Erik Seilnacht' and all tokens associated with this user?

FIGURE 9-3 Confirm Deletion of a User



Caution – This operation deletes the user and all associated tokens. To delete a single token from a user, please see “To Delete a Token From a User from the Web-Based Interface” on page 161.

3. To proceed with deleting the user, press the **YES - Delete User Now** button. To cancel this delete operation, press the **NO - Cancel Delete** button.

If you press YES, the user and all associated tokens are deleted from the administration database and a confirmation of your delete operation will be displayed.

If you press NO, you are returned to the Current Properties frame.

Delete User

Confirmation

User 'Erik Seilnacht' has been deleted.

FIGURE 9-4 Confirmation Frame

▼ To Delete a Single User From the Command-Line Interface

- Type the following command:

```
# utuser -d <Token ID>
```

Where <Token ID> is any one of the token IDs held by the user you want to delete.

Caution – This operation deletes the user and all associated tokens. To delete a single token from a user, please see “To Delete a Token From a User From the Command-Line Interface” on page 161.

For example:

```
# utuser -d mondex.9998008800007658  
  
Deleted 1 user.
```

Deleting Multiple Users

There is no web-based interface for this procedure.

▼ To Delete Multiple Users From the Command-Line Interface

1. Prepare a file with the users you want to delete and their new information. Each user should be on a separate line:

```
<Token ID>
```

Note – You can use the output of `utuser -o` as input for this command since this command ignores everything after the first comma.



Caution – This operation deletes each user and all associated tokens. To delete a single token from a user, please see “To Delete a Token From a User From the Command-Line Interface” on page 161.

2. Type the following command:

```
# utuser -df <filename>
```

Where *<filename>* is the user file you created in Step 1. For each line in the specified file, the command deletes a user from the administration database.

For example:

```
# cat users
mondex.9998008800007658,localhost,7007,Eric Seilnacht,C987
mondex.9998008458700965,localhost,7007,John Stone,C2310
mondex.9998007300058900,localhost,7007,Ethan Williams,E1049

# utuser -df users
Deleted mondex.9998008800007658
Deleted mondex.9998008458700965
Deleted mondex.9998007300058900

3 users deleted
```

Finding Users

Listing All Users by ID

▼ To List All Users by ID From the Web-Based Interface

1. Starting at the Main Administration page select Users►View by ID.

A frame like the following displays (FIGURE 9-5), listing all the users in the administration database, sorted by the Token ID field. If a user has multiple tokens, they are listed separately.

View Users by ID

Token ID	Server	Port	User Name	Other Info
mondex.9998008800007658	localhost	7007	Erik Seilnacht	

Home Previous Next

FIGURE 9-5 Results of List All Users by ID Frame

2. Use the navigation buttons at the bottom of the frame to view additional frames of more than 20 users or more.

The buttons allow you to view the next 20 users, previous 20 users, or to go back to the first frame of 20 users.

▼ To List All Users by ID From the Command-Line Interface

1. Type the following command:

```
# utuser -l
```

This command displays the complete list of users in the administration database. For example:

```
# utuser -l
```

Token ID	User Name	Other Info
mondex.9998008800007658	Eric Seilnacht	C987
mondex.9998008458700965	John Stone	C2310
mondex.9998007300058900	Ethan Williams	E1049
mondex.9998006885500934	Trevor Young	C3303
mondex.9998007668000076	Richard Parker	C4501
mondex.9998007587333001	Helen Anderson	C987
mondex.9998007777965800	Cecilia Brown	C4501

```
7 tokens total.
```

2. Or you can get a longer listing by typing the following command:

```
# utuser -L
```

The longer listing displays the same information as the normal listing, but adds the Server and Port columns.

Viewing All Users by Name

There is no command-line interface for this procedure.

▼ To View All Users by Name From the Web-Based Interface

1. Starting at the Main Application page, select Users>View by name.

A frame similar to the following displays, listing all the users in the administration database, sorted by the User Name field. If a user has multiple tokens, they are grouped together with the name.

View Users by Name

User Name	Token ID(s)	Server	Port	Other Info
Erik Seilnacht	mondex.9998008800007658	localhost	7007	

[Home](#) [Previous](#) [Next](#)

FIGURE 9-6 Results of List All Users by Name Frame

2. Use the navigation buttons at the bottom of the frame to view additional frames of more than 20 users or more.

The buttons allow you to view the next 20 users, previous 20 users, or to go back to the first frame of 20 users.

Searching for Desktops (Users)

▼ To Find a Desktop (User) From the Web-Based Interface

1. Starting at the Main Administration page select **Desktops**►**Find desktop**. Fill out the **Desktop ID**, **Location**, and **Other Info** fields with the values you want to search.
2. Press the **Search** button.

A results frame similar to the following is shown, displaying all matches from the administration database. If more than one search value is entered, the search performs a logical AND. Only those results that match all the specified values are returned.

If Token ID was specified as a search value, the results are sorted by Token ID. Otherwise, they are sorted by User Name.

Find Desktop

▪ Search for All Desktops that Contain:

Desktop ID: and

Location: and

Other Info:

FIGURE 9-7 Results of Search by Value Frame

3. Use the navigation buttons at the bottom of the frame to view additional frames of more than 20 users or more.

The buttons allow you to view the next 20 users, previous 20 users, or to go back to the first frame of 20 users.

▼ To Search for Users from the Command-line Interface

1. To search by User Name, type the following command:

```
# utuser -ln <substring>
```

Where *<substring>* is the full or partial User Name you want to search for. This command displays the list of users in the administration database whose names match this substring. For example:

```
# utuser -ln anderson

Token ID                               User Name                               Other Info
-----
mondex.9998007587333001                Helen Anderson                           C987

2 tokens, 1 user total.
```

2. Type the following command to search by User Name and get a longer listing:

```
# utuser -Ln <substring>
```

The longer listing displays the same information as the normal listing, but adds the Server and Port columns.

3. To search by Token ID, type the following command:

```
# utuser -li <substring>
```

Where *<substring>* is the full or partial Token ID you want to search for. This command displays the list of users in the administration database whose Token IDs match this substring. For example:

```
# utuser -li 0934

Token ID                               User Name                               Other Info
-----
mondex.9998006885500934                Trevor Young                             C3303

1 token total.
```

Listing Current Users

Note – The Authentication Manager must be operating to perform these procedures.

▼ To List Currently Logged In Users From the Web-Based Interface

1. Starting at the Main Administration page, select **Users**►**View current**.

A frame similar to the following displays, listing only the registered users that are currently logged into an appliance (desktop) connected to this Sun Ray server. This also applies to any Sun Ray server in the same failover group as this Sun Ray server.

View Current Users

Token ID	User Name	Desktop ID	Desktop Location
at88sc1608_a70100aa	???	080020b60d30	???
pseudo_080020b56513	???	080020b56513	???

[Home](#) [Previous](#) [Next](#)

FIGURE 9-8 Currently Logged in Users Frame

2. Use the navigation buttons at the bottom of the frame to view additional frames of more than 20 users or more.

The buttons allow you to view the next 20 users, previous 20 users, or to go back to the first frame of 20 users.

▼ To List Currently Logged In Users From the Command-Line Interface

1. Type the following command:

```
# utuser -lc
```

This command lists only the registered users that are currently logged in to an appliance connected to the Sun Ray server. This also applies to any Sun Ray server in the same failover group as this Sun Ray server. For example:

```
# utuser -lc

Token ID                               User Name                               Desktop ID
-----
mondex.9998006885500934                Trevor Young                             C3303
1 user currently logged in.
```

2. To get a longer listing type the following command:

```
# utuser -Lc
```

The longer listing displays the same information as the normal listing, but adds the Desktop Location column.

3. Or to view currently logged in users and the servers they are connected to, type the following command:

```
# utuser -G
```

Listing Users in Dump Format

There is no web-based interface for this procedure.

▼ To Output the User List in Dump Format From the Command-Line Interface

- Type the following command:

```
# utuser -o
```

The command outputs the full list of users from the administration database in comma-delimited format. For example:

```
# utuser -o
mondex.9998008800007658,localhost,7007,Eric Seilnacht,C987
mondex.9998008458700965,localhost,7007,John Stone,C2310
mondex.9998007300058900,localhost,7007,Ethan Williams,E1049
mondex.9998006885500934,localhost,7007,Trevor Young,C3303
mondex.9998007668000076,localhost,7007,Richard Parker,C4501
mondex.9998007587333001,localhost,7007,Helen Anderson,C987
mondex.999800777965800,localhost,7007,Cecilia Brown,C4501
```

The format of each line is:

```
<Token ID> , <Server> , <Server Port> , <User Name> , <Other Info>
```

This output can be saved to a file and used later to perform batch add, edit or delete operations.

User Properties

This section covers the following topics:

- “Displaying Properties” on page 152
- “Editing a Single User’s Properties” on page 155
- “Editing Multiple Users’ Properties” on page 157

Displaying Properties

▼ To Display a User’s Current Properties From the Web-Based Interface

- 1. Starting at the Users page, perform a list (see FIGURE 9-5, FIGURE 9-6, or FIGURE 9-8) or search operation (see FIGURE 9-7).**
- 2. Click on the Token ID or User Name hyperlink for the user of interest.**

A frame similar to the following displays.

Erik Seilnacht

Current Properties:

User Name: Erik Seilnacht
Other Info:
Server Name: localhost
Server Port: 7007
User Created: Fri 07 Jan 2000 02:50:00 PM PST

Token ID	Enabled?
mondex.9998008800007658	Yes

Never Logged In

Edit Properties	Delete This User
---------------------------------	----------------------------------

FIGURE 9-9 User's Current Properties Frame

FIGURE 9-9 shows information about the user as obtained from the administration database. The following core fields are displayed:

TABLE 9-2 User Properties Fields

Option	Description
User Name	The user's name.
Other Info	An optional field that administrators can fill out to display any additional information associated with the user.
Server Name	The name of the Sun Ray server the user is registered on.
Server Port	The communication port used on the Sun Ray server.

TABLE 9-2 User Properties Fields

Option	Description
User Created	The date and time that the user was created (registered) on this server.
Token ID	The IDs of one or more tokens currently associated with the user.
Enabled?	Displays “Yes” if a token is enabled, “No” otherwise. Disabled tokens are not allowed to log into Sun Ray 1 enterprise appliances that require registered tokens.

Additionally, information about the user’s current login status is displayed. The possible states are:

- Never Logged In
- Currently Logged In
- Logged Off

Of the last two states, the following fields also are displayed:

TABLE 9-3 Login Status Fields

Option	Description
Current Desktop/ Last Desktop	The current/last appliance (desktop) the user is/was logged into.
Desktop Location	The location of the appliance (desktop).
Logged In Since/ Logged Off At	The date and time the user logged in/off the appliance (desktop).

▼ To Display a User's Current Properties From the Command-Line Interface

- Type the following command:

```
# utuser -p <Token ID>
```

Where *<Token ID>* is any one of the token IDs held by a user you want to get properties for. This command shows information about the user as obtained from the administration database. For example:

```
# utuser -p MicroPayflex.00004f9165000100
Current Properties:
  User Name           = Richard Parker
  Other Info          = C4501
  Server Name         = localhost
  Server Port         = 7007
  User Created        = 04/29/1999 16:06:20

  Token                                     Enabled?
  -----
  mondex.9998007668000076                   Yes
  mondex.9998007668077709                   Yes

Last Login:
  Last Desktop       = 08002086e18f
  Desktop Location   = SFO12-2103
  Logged Off At      = 04/29/1999 16:33:09
```

See TABLE 9-2 and TABLE 9-3 for descriptions of the fields displayed.

Editing a Single User's Properties

▼ To Edit a Single User's Properties From the Web-Based Interface

1. Starting at the User Properties frame for the user you want to edit, press the **Edit Properties** button.

A frame similar to the following displays.

Edit User Properties

To add a Token ID to this user, select a token reader and press **Get Token ID** below to fill in the new token ID field. Then, make any other changes and press **Save Changes**.

User Name: Erik Seilnacht
Other Info:
Server Name: localhost
Server Port: 7007
User Created: Fri 07 Jan 2000 02:50:00 PM PST

Token ID	Enabled?	
mondex.99980068800007658	<input checked="" type="checkbox"/>	<input type="checkbox"/> Remove
	<input type="checkbox"/>	<input type="checkbox"/> Add

Token Reader: 080020b5653c	<input type="button" value="Get Token ID"/>
-----------------------------------	---

FIGURE 9-10 Edit Properties Frame

2. Make change to any of the editable fields.

You can also add or remove tokens from a user at the same time. See “To Add a Token to a User From the Web-Based Interface” on page 159 and “To Delete a Token From a User from the Web-Based Interface” on page 161 for details.

3. When done, press the Save Changes button.

The changes are then made to the administration database.

▼ To Edit a Single User's Properties From the Command-Line Interface

- Type the following command:

```
# utuser -e "<Token ID>,<Server>,<Server Port>,<User Name>,<Other Info>"
```

Where *<Other Info>* can be left empty if you want to clear the field. The command updates the user's information in the administration database. For example:

```
# utuser -e "mondex.9998007668000076,localhost,7007,Richard Parker,D0001"
1 User Modified.
```

To clear the *<Other Info>* field, put no text after the comma. The following example clears the Other Info field:

```
# utuser -e "mondex.9998007668000076,localhost,7007,Richard Parker,"
1 User Modified.
```

Tip – You can use the output of the `utuser -o` command as input to this command. Remember to put quotes around the data.

Editing Multiple Users' Properties

There is no web-based interface for this procedure.

▼ To Edit Multiple Users' Properties From the Command-Line Interface

1. Prepare a file listing users you want to edit and their changed information. Each user should be on a separate line of the form:

```
<Token ID> , <Server Name> , <Server Port> , <User Name> , <Other Info>
```

Tip – You can use the output of `utuser -o`, edit it and then use the resulting file as input to this command.

Note – The Token ID must match an existing Token ID, so this field cannot be changed. To change a user’s Token ID, add a new token (see “To Add a Token to a User From the Command-Line Interface” on page 159) and then delete the old token (see “To Delete a Token From a User From the Command-Line Interface” on page 161).

2. Type the following command:

```
# utuser -ef <filename>
```

where <filename> is the user file you created in Step 1. For each line in the specified file, the command checks for any modifications, and if any are found, saves the changes to the administration database.

For example:

```
# cat users
mondex.9998007300058900,localhost,7007,Ethan Williams,D0002
mondex.9998006885500934,localhost,7007,Trevor Young,C3303
mondex.9998007777965800,localhost,7007,Cecilia Brown,D0003

# utuser -ef users
Modified Ethan Williams
No modifications necessary for Trevor Young.
Modified Cecilia Brown

2 users modified
1 user did not require changes
```

Administering Tokens

Adding a Token to a Single User

▼ To Add a Token to a User From the Web-Based Interface

1. **Starting from the User Properties frame for the user for whom you want to add a token, press the Edit Properties button.**

The Edit Properties frame displays. See FIGURE 9-10.

2. **If you know the new Token ID, type it into the empty Token ID text field.**
3. **If you do not know the new Token ID and have configured a token reader (see “To Configure a Token Reader” on page 73):**
 - a. **Insert the user’s token into the selected token reader.**
 - b. **Choose the selected token reader from the pulldown list of available readers.**
 - c. **Press the Get Token ID button.**

The application queries the token reader and, if successful, redisplay the form with the Token ID text field filled out.

4. **Check the Enabled checkbox next to the new Token ID.**
5. **Check the Add checkbox next to the new Token ID.**

You can also make any other edits to the user at the same time. See “To Edit a Single User’s Properties From the Web-Based Interface” on page 155.

6. **Press the Save Changes button.**

The changes are then made to the administration database.

▼ To Add a Token to a User From the Command-Line Interface

- **Type the appropriate `utuser` command:**

a. If you already know the user's new Token ID, type the following command:

```
# utuser -ai <Current Token ID> <New Token ID>
```

where <Current Token ID> is any of the user's existing Token IDs and <New Token ID> is the ID of the token you want to add. The command adds the new token to the user in the administration database.

For example:

```
# utuser -ai mondex.9998007668000076 mondex.9998007668077709
1 Token ID added to user.
```

b. If you do not know the user's new Token ID and have configured a token reader, type the following command:

```
# utuser -ai <Current Token ID> x -r <Token Reader>
```

Where <Current Token ID> is any of the user's existing Token IDs. The "x" that is specified instead of the new Token ID tells the command to query <Token Reader> for the Token ID. You will be prompted to insert the user's token into the token reader when the command is ready. Then, the command will add the new token to the user in the administration database. For example:

```
# utuser -ai mondex.9998007668000076 x -r 08002086e18f
Insert token into token reader '08002086e18f' and press return.
Read token ID 'mondex.9998007668077709'
1 Token ID added to user.
```

Deleting a Token From a Single User

▼ To Delete a Token From a User from the Web-Based Interface

1. **Starting from the User Properties frame for the user from whom you want to remove a token from, press the Edit Properties button.**

The Edit Properties frame displays. See FIGURE 9-10.

2. **Check the Remove checkbox for any Token IDs you want to remove.**

Note – You cannot remove all of a user’s tokens. If you want to delete the user and all associated tokens, see “To Delete a Single User From the Web-Based Interface” on page 141.

3. **Press the Save Changes button.**

The changes are then made to the administration database.

▼ To Delete a Token From a User From the Command-Line Interface

- **Type the following command:**

```
# utuser -di <Token ID>
```

where *<Token ID>* is the token you want to remove from the user that currently holds it. The command deletes the token from the user in for the administration database.

Note – You cannot remove all of a user’s tokens. If you want to delete the user and all associated tokens, see “To Delete a Single User From the Command-Line Interface” on page 142.

For example:

```
# utuser -di mondex.9998007668077709

1 Token ID removed from user.
```

Enabling or Disabling a User's Token

▼ To Enable or Disable a User's Token From the Web-Based Interface

1. **Starting from the User Properties frame for the user whose token you want to enable or disable, press the Edit Properties button.**

The Edit Properties frame displays. See FIGURE 9-10.

2. **Check the Enabled checkbox for any Token IDs you want to enable.**
3. **Uncheck the Enabled checkbox for any Token IDs you want to disable.**
4. **Press the Save Changes button.**

The changes are then made to the administration database.

▼ To Enable or Disable a User's Token From the Command-Line Interface

1. **To enable a user's token, type the following command:**

```
# utuser -ei <Token ID> enable
```

where <Token ID> is the ID of the token you want to enable. This command updates the token's information in the administration database.

2. **To disable a user's token, type the following command:**

```
# utuser -ei <Token ID> disable
```

where <Token ID> is the ID of the token you want to disable. This command updates the token's information in the administration database.

Getting a Token ID From a Token Reader

▼ To Get a Token ID from a Token Reader From the Web-Based Interface

1. **Starting at the Users frame, click on the Get Token ID From Token Reader (see “To Configure a Token Reader” on page 73).**

A frame similar to the following displays.

Get Token ID

To get a token's ID, select a reader from the pulldown list below, insert the token in that reader and press **Get Token ID**.

Token Reader: 080020b5653c

Token ID: mondox.9998008800007858

FIGURE 9-11 Get Token ID Frame

2. **Insert the token you want to read into the selected token reader.**
3. **Choose the selected token reader form the pulldown list of available readers.**
4. **Press the Get Token ID button.**

The application queries the token reader and, if successful, redisplay the frame with the Token ID field filled out.

▼ To Get a Token ID From a Token Reader From the Command-Line Interface

- Type the following command:

```
# utuser -r <Token Reader>
```

Where *<Token Reader>* is the reader you want to read the ID from. You will be prompted to insert the token into the Token Reader when the command is ready. The command will then query the Token Reader for the token's ID and, if successful, display it. For example:

```
# utuser -r 08002086e18f
Insert token into token reader '08002086e18f' and press return.
Read token ID 'mondex.9998007668077709'
```

Managing Smart Cards From Different Vendors

The Sun Ray enterprise server software supports the use of different smart cards from different vendors. This is in contrast to managing individual cards that end users are assigned. Additionally, viewing and adding smart cards is also possible through the Administration application. The order in which the smart cards are probed by the authentication daemon is also adjustable. The information provided about the smart cards is extracted from a vendor-supplied configuration file. These configuration files are located in the directory: `/etc/opt/SUNWut/smartcard`. The configuration file must be formatted correctly and the filename must end with a `.cfg` suffix.

For example: `acme_card.cfg`

For certain vendors, the smart card may require additional software to enable the Sun Ray to probe for it. If required, this optional software must be supplied as Java classes in a Jar file. This file must end with a `.jar` suffix and must have the same pre-suffix filename as the `.cfg` file that contains its configuration information.

▼ To View/List The Configured Smart Cards

1. Starting at the Main Administration page select Smart Cards►View.

The configured smart cards listed in alphabetical order (FIGURE 9-12).

View Configured Smart Cards

Smart Card	Version	Supplier
iButton	1.0	Sample Industries, Inc.
iButton	1.3	Sample Industries, Inc.
JavaCard	2.1	Sample Industries, Inc.
MicroFlexCard	5.3	Sample Industries, Inc.
Mondex	1.1	Sample Industries, Inc.
SampleCard	4.0	Sample Industries, Inc.

FIGURE 9-12 Smart Card View Frame

From this frame an administrator can see the current list of smart cards in alphabetical order. The smart card supplier and version number is also shown (FIGURE 9-12)

TABLE 9-4 View Configured Smart Card Fields

Option	Description
Smart Card	Smart card name.
Version	Smart card version.
Supplier	Smart card supplier.

▼ To View/List The Configured Smart Cards From the Command-Line Interface

- To list the configured smart cards, type the following command:

```
# /opt/SUNWut/sbin/utcard -l
```

For example:

```
# /opt/SUNWut/sbin/utcard -l
Card Name           Ver.  Probe
-----
iButton             1.0   1
iButton             1.3   2
JavaCard            2.1   3
MicroFlexCard       5.3   4
Mondex              1.1   5
SampleCard          4.0   6
```

▼ To View the Properties for a Particular Smart Card

- **Starting at the Main Administration page select Smart Cards>View and click on any smart card under the Smart Card column.**

FIGURE 9-13 displays the main properties for the selected smart card. All smart card configuration files are required to have values for these properties. If the Jar file property contains a hyphen (-), the card can be probed in a standard method using properties in the file, and does not require auxiliary software classes supplied in the form of a Jar file.

Smart Card Properties

Main Properties:

Name: MicroFlexCard
Model: MP1
Description: The XXX Cryptographic Do-All Smart Card
Supplier: XXX Industries, Inc.
Version: 5.3
Type: smartcard
Jar file: -

FIGURE 9-13 Smart Card Properties Frame

▼ To View The Properties of Smart Cards From the Command-Line Interface

- **To view the properties of smart cards, type the following command:**

```
# /opt/SUNWut/sbin/utcard -p "<name>,<version>"
```

Where *<name>* is the name of the smart card and *<version>* is the version number.

Smart Cards Probe Order

▼ To View The Smart Card Probe Order

1. **Starting at the Main Administration page select Smart Cards>Probe Order.**

The Smart Card Probe Order frame appears (FIGURE 9-14).

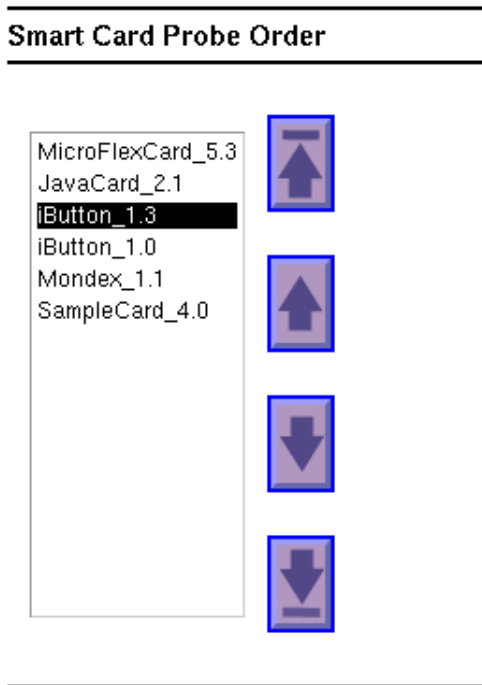


FIGURE 9-14 Smart Card Probe Order Frame

Changing the Smart Card Probe Order

▼ To Change the Smart Card Probe Order

1. **Starting at the Main Administration page select Smart Cards>Probe Order.**

The Smart Card Probe Order frame appears. The probe order may be changed by selecting a card and pressing the appropriate button.

Smart Card Probe Order

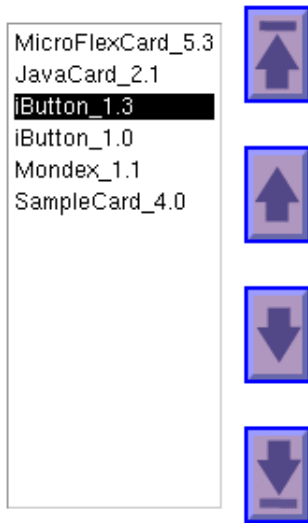


FIGURE 9-15 Smart Card Probe Order Frame

2. Click on a smart card selection to highlight it (see above).
3. Click on the up or down arrow button to maneuver the card's location in the probe order.

Clicking on the first and last (from top to bottom) buttons moves the selected card to either the top or bottom of the list.

▼ To Change The Smart Card Probe Order From the Command-Line Interface

1. To change the smart card probe order, type the following command:

```
# /opt/SUNWut/sbin/utcard -l
```

The current probe order is indicated in the Probe column.

2. To specify a new position for a smart card in the Probe Order, type the following command:

```
# /opt/SUNWut/sbin/utcard -r <name>,<version>,<new position>
```

Where *<name>* is the name of the smart card, *<version>* is the version and *<new position>* specifies the new position for the card.

Note – When a new position is specified for a card, the existing order is shifted up or down to accommodate the change.

Adding Smart Cards

▼ To Add a Smart Card

1. Starting at the Main Administration page select Smart Cards►Add.

The Add Smart Cards to Probe List frame appears (FIGURE 9-16).

Add Smart Card To Probe List

AVAILABLE

OtherCard_1.3 (filename_a.cfg)
SampleCard_3.0 (filename_b.cfg)
JavaButton_4.0 (filename_g.cfg)
JavaRolex_5.8 (filename_h.cfg)
ThumbReader_1.1 (filename_i.cfg)
SmartButton_1.1 (filename_l.cfg)
MicroPayflex_1.1 (filename_m.cfg)



FIGURE 9-16 Add Smart Card Frame

- 2. Highlight a smart card and click the Add button.**

▼ To Add a Smart Card From the Command-Line Interface

1. To list the files containing details for cards that are not currently configured in the probe order, type the command:

```
# /opt/SUNWut/sbin/utcard -u
```

For example:

```
# /opt/SUNWut/sbin/utcard -u
Filename          Name           Ver.
-----
filename_a.cfg    OtherCard      1.3
filename_b.cfg    SampleCard     3.0
filename_g.cfg    JavaButton    4.0
filename_h.cfg    JavaRolex     5.8
filename_i.cfg    ThumbReader   1.1
filename_l.cfg    SmartButton   1.1
filename_m.cfg    MicroPayflex  1.1
```

2. To add one of the listed (see above) cards, type:

```
# /opt/SUNWut/sbin/utcard -a <filename>
```

Where *<filename>* is one of the files listed in the Filename column above.

Deleting Smart Cards

▼ To Delete a Smart Card

1. Starting at the Main Administration page select **Smart Cards**►**Delete**.
The Delete Smart Cards From the Probe List frame appears (FIGURE 9-17).

Delete Smart Card From Probe List

CONFIGURED

```
iButton_1.0  
iButton_1.3  
JavaCard_2.1  
MicroFlexCard_5.3  
Mondex_1.1  
SampleCard_4.0
```

Delete

FIGURE 9-17 Delete Smart Card Frame

2. Select a smart card and click the Delete button.

▼ To Delete a Smart Card From the Command-Line Interface

1. To delete one of the cards, type the command:

```
# /opt/SUNWut/sbin/utcard -d <name>,<version>
```

Where *<name>* and *<version>* are those as listed by
`/opt/SUNWut/sbin/utcard -l`.

Smart Card Vendor Configuration Files

Use the Administration application to add additional smart card vendor configuration files. The configuration files are available from each smart card vendor. You may receive both a `vendor.jar` file and a `vendor.cfg` file.

▼ To Load A Configuration File Into the Directory

- Copy the vendor configuration file(s) to the following location:

```
# cp vendor.cfg /etc/opt/SUNWut/smartcard
# cp vendor.jar /etc/opt/SUNWut/smartcard
```

The additional vendor card(s) should now appear under the Available column in the Add frame. Refer to FIGURE 9-16 or FIGURE 9-17.

▼ To Load/Add A Configuration File Into the Database

1. Starting at the Main Administration page select Smart Cards►Add.

The Add Smart Card To Probe List appears. The new smart cards and their corresponding configuration file(s) appear.

Add Smart Card To Probe List

AVAILABLE

OtherCard_1.3 (filename_a.cfg)
SampleCard_3.0 (filename_b.cfg)
JavaButton_4.0 (filename_g.cfg)
JavaRolex_5.8 (filename_h.cfg)
ThumbReader_1.1 (filename_i.cfg)
SmartButton_1.1 (filename_l.cfg)
MicroPayflex_1.1 (filename_m.cfg)



FIGURE 9-18 Adding A Smart Card to the Probe List

2. Highlight a smart card and click the Add button.

The smart card is now added to the datastore. Proceed to the next step to verify this action.

▼ To Verify the Configuration File Addition

1. Starting at the Main Administration page select Smart Cards►View.

The View Configured Smart Cards frame appears.

View Configured Smart Cards

Smart Card	Version	Supplier
iButton	1.0	Sample Industries, Inc.
iButton	1.3	Sample Industries, Inc.
JavaCard	2.1	Sample Industries, Inc.
MicroFlexCard	5.3	Sample Industries, Inc.
Mondex	1.1	Sample Industries, Inc.
SampleCard	4.0	Sample Industries, Inc.

FIGURE 9-19 Verifying the File Addition

2. Verify that the new vendor appears on the list.

This step ensures that the configuration file was properly entered into the datastore.

OpenWindows Considerations

For end users running OpenWindows™ on their enterprise appliances, certain preferences must be set. For example, if a CD is inserted into the Sun Ray server, the File Manager application appears on all monitors of the appliances running OpenWindows. To prevent this from occurring, each OpenWindows user should follow these instructions. Essentially, this procedure needs to be performed on every end user's configuration in their /home directory (it has no involvement with the appliance). This procedure only needs to be performed once.

Note – If the end user clicks the Apply button without clicking Save As Defaults, the end user will have to perform the procedure (shown below) repeatedly.

▼ To Alter OpenWindows Properties

1. **Choose File Manager.**
2. **Choose Edit.**
3. **Click on Properties.**
The Properties panel appears.
4. **Click on Category ►Advanced Settings.**
5. **Click No as the selection for “Open File Manager Window upon insertion of: CDROM:.”**
6. **Click Apply.**
7. **Save as default.**

Removing the Sun Ray Software

This chapter explains how to remove the Sun Ray software from your server. Both script-based and manual removal procedures are provided. This chapter is organized as follows:

- “Using Scripts to Uninstall the Software” on page 179
- “Manually Uninstalling the Software” on page 186

Using Scripts to Uninstall the Software

A system administrator can use an unconfiguration script and an uninstall script to remove the Sun Ray server software.

This section describes how to unconfigure and uninstall the Sun Ray server software.

Note – You must unconfigure the Sun Ray server software before you can use `uninstall -u` to remove the server software.

In the following instructions you will need to take the values you chose in the worksheet and substitute in the appropriate places. Refer to “Collecting Key Configuration Parameters” on page 40. For example, if you chose `@(WEBSERVER_NAME)` to be `utadmin`, when substituting into this partial command:

```
# htserver stop @(WEBSERVER_NAME)
```

the result would be:

```
# htserver stop utadmin
```

▼ To Unconfigure the Sun Ray Server Software

1. As superuser, type:

```
# cd /etc/init.d
```

2. Stop the Sun Ray services:

```
# ./utsvc stop
```

The services are stopped.

3. Type:

```
# htserver stop @(WEBSERVER_NAME)
```

The Sun WebServer instance is stopped. *@(WEBSERVER_NAME)* is the name of the WebServer instance that supports the administration application. Refer to the value you chose on your worksheet (see “Configuration Worksheet” on page 40).

4. Stop SunDS:

```
# ./dsserv stop
Stopping SunDS daemon
SunDS daemon stopped
```

5. Type:

```
# /opt/SUNWut/sbin/utadm -r
```

All of the entries and all of the structure relating to all of the Sun Ray interfaces are removed. This command prepares the system for the removal of the Sun Ray server software.

```
### Removing interface "<interface>"
```

6. Begin the unconfiguration process:

```
# /opt/SUNWut/sbin/utconfig -u  
Un-configuration of Sun Ray enterprise server Software
```

7. Answer the question: Unconfigure Sun Web Server 2.1 ([y]/n)?

This script gives you the option of unconfiguring the Sun Web Server 2.1 or not. Yes is the default.

```
Unconfigure Sun Web Server 2.1 ([y]/n)y
```

8. Answer the question as follows:

Note – The web server instance name, @(WEBSERVER_NAME), and the CGI username, @(CGI_USER), in this example, use the default values: utadmin and www). If you entered different values, enter them here. Refer to your configuration worksheet for your original values (see “Configuration Worksheet” on page 40).

```
Enter UT admin web server instance name [utadmin]:

Delete CGI username account ([y]/n)y
# Enter CGI username [www]): utadmin

About to un-configure the following software products:

Sun Directory Services 3.1
Sun Web Server 2.1
Sun Ray enterprise server 1.1

Continue ([y]/n)y
```

The Sun Ray server unconfiguration process begins. The following message is displayed.

```
Removing Sun Ray enterprise server Configuration ...

Removing Sun Web Server 'utadmin' instance ...
utadmin : Not running.
utadmin : Deleted.

Deleting user account for 'utadmin' ...
www:x:130001:10:ut admin web server cgi user:/tmp:/bin/sh

Unloading Sun Directory Services Datastore ...

Removing Sun Directory Services Datastore ...

Downdating Sun Directory Services ACL's ...

Downdating Sun Directory Services schema ...
Starting SunDS daemon .
Tue Apr 20 16:58 : dsservd starting

Un-configuration of Sun Ray enterprise server has completed.
Please check the log file, /var/tmp/utconfig.xxxxx.log, for
errors.
```

9. After the script has completed check in `/var/tmp/utconfig.xxx.log` to see if there were any errors, where `xxx` is the process ID of the script.

▼ To Uninstall the Sun Ray Software

This section describes how to use the `utinstall -u` command to remove the Sun Ray server software.

Note – Your current working directory must not be within any of the directories to be removed. Perform a `cd /` to your working directory for verification.

1. Change to your working directory:

```
# cd /
```

2. Start the removal process:

```
# /opt/SUNWut/sbin/utinstall -u  
Removal of Sun Ray enterprise server Software
```

3. Answer the questions as follows:

```
Remove Sun Directory Services 3.1 ([y]/n)? y
```

```
About to remove the following software products:
```

```
Sun Ray enterprise server 1.1
```

```
Sun Web Server 2.1
```

```
Sun Directory Services 3.1
```

```
In addition, any running Sun Ray enterprise server services will  
be stopped. All existing sessions will also be cleared out.
```

```
Continue ([y]/n)y
```

The packages are removed. The following message is displayed:

```
Removing Sun Ray enterprise server version 1.0 ...

Removal of <SUNWuta> was successful.

Removal of <SUNWutj> was successful.

Removal of <SUNWutm> was successful.

Removal of <SUNWuto> was successful.

Removal of <SUNWutr> was successful.
### successfully removed Sun Ray audio pseudo driver (utadem)
### successfully removed Sun Ray pseudo driver

Removal of <SUNWutk> was successful.

Removal of <SUNWutu> was successful.

Removing Sun Web Server version 2.1 ...
No running servers found.

Removing SWS does not remove your websites or configurations.
Server instances and websites are typically found in /var/http,
although they may be placed anywhere you choose. See "/etc/http/
httpd-instances.conf" for the master list of server
configurations.

Checking installed packages and patches...
...Removal of <SUNWsds> was successful.

Removal of <SUNWsdsc> was successful.

Removal of Sun Ray enterprise server has completed, see /var/tmp/
utinstall.xxxxx.log
#
```

- 4. After the script has completed, check in `/var/tmp/utconfig.xxx.log` to see if there were any errors, where `xxx` is the process ID of the script.**

Manually Uninstalling the Software

Use these procedures to uninstall the Sun Ray server software by using `pkgrm`. For procedures on how to remove the software using a script, see “Using Scripts to Uninstall the Software” on page 179.

Note – It is highly recommended that you use the `utinstall` script to remove the Sun Ray server software. Refer to “Using Scripts to Uninstall the Software” on page 179 for additional information.

▼ To Remove the Sun Ray Server Software

1. **Become superuser and stop the Sun Ray services:**

```
# /etc/init.d/utsvc stop
```

2. **Remove all of the network interconnects:**

```
# /opt/SUNWut/sbin/utadm -r
```


3. Remove the software packages:

```
# pkgrm SUNWuta SUNWutm SUNWuto SUNWutr SUNWutux SUNWutu SUNWutkx SUNWutk SUNutj
```

Respond **y** to each package removal query. The output is similar to the following:

```
The following package is currently installed:
  SUNWuto      Sun Ray enterprise server Core Software
                (sun4m,sun4u,sun4d) Alpha4

Do you want to remove this package? y

## Removing installed package instance <SUNWuto>
## Verifying package dependencies.
## Processing package information.
## Removing pathnames in class <none>
/tftpboot/view
/tftpboot/tftpboot
/tftpboot <non-empty directory not removed>
/opt/SUNWut/lib/tftpboot
/opt/SUNWut/lib <shared pathname not removed>
/opt/SUNWut/bin/utfwupgrade
/opt/SUNWut/bin/esdl
/opt/SUNWut/bin <shared pathname not removed>
/opt/SUNWut <shared pathname not removed>
## Updating system information.

Removal of <SUNWuto> was successful.
```

SunDS 3.1 and Sun WebServer 2.1

Refer to the supporting software's documentation (included on the Sun Ray enterprise server software 1.1 CD) for uninstall and unconfigure information.

Troubleshooting

This chapter has three sections:

- “Appliance Questions” on page 189
- “User Questions” on page 196
- “Server Questions” on page 201

Appliance Questions

Q: A user calls and describes the OSD (on-screen display). What do I do for each one?

A: Take the following steps for each of the following icons.

Startup Icon



Startup icon: under the hourglass there are dashes to indicate progress.

- Waiting for interconnect
- DHCP pending
- Waiting to connect to the Authentication Manager

- Startup 1—Waiting for the Interconnect

Meaning: The appliance has passed the power-on self test but has not detected an Ethernet signal yet. This icon is displayed as part of the normal startup phase and usually is displayed for only a few seconds.

Actions to take if this icon stays on for more than 10 seconds:

- Check that the Ethernet cable is correctly plugged into the back of the appliance and the other end into the correct hub, switch, or network outlet.
- If the appliance is connected via a hub or switch, make sure that the hub or switch is powered on and configured correctly.
- Check that the Sun Ray server is up and running.
- Startup 2—DHCP Pending

Meaning: The appliance has detected the Ethernet carrier but has not received its initial parameters from DHCP yet. This icon is displayed as part of the normal startup phase and usually is displayed for only a few seconds.

Actions to take if this icon stays on for more than 10 seconds:

- Make sure that DHCP on the Sun Ray server is configured correctly, is up and running and has not run out of IP addresses to assign to clients.
- To restart DHCP as superuser type:
 - `# /etc/init.d/dhcp stop`
 - `# /etc/init.d/dhcp start`
- Startup 3—Waiting to Connect to Authentication Manager

Meaning: The appliance has received its initial parameters from DHCP but has not connected to the Sun Ray Authentication Manager yet. This icon is displayed as part of the normal startup phase and usually is displayed for only a few seconds. Once this icon disappears, the connection has been made and the user can insert their smart card and/or log in.

Actions to take if the icon displays for more than a few seconds:

- Make sure that the Sun Ray services, including the Authentication Manager are up and running on the Sun Ray server.

Appliance Failure



Appliance failure: This icon is called hardware failure in the *Sun Ray 1 Troubleshooting Guide*.

Meaning: The appliance tried to load new PROM software from the Sun Ray server, but failed.

Actions to take if icon displays for more than a few seconds:

1. Examine the Sun Ray server software logs for any error messages that might indicate the cause.
2. Check that DHCP on the Sun Ray server is configured correctly and is up and running.

3. Check `/tftpboot` on the Sun Ray server to see if the new PROM software exists and is ready to be downloaded to the appliance.
4. Once any problems are corrected, power cycle the appliance so it can try to reload the PROM software.

No Ethernet



No Ethernet: check to see if the Ethernet cable is plugged in correctly.

The last six hexadecimal digits of the Ethernet address are shown.

Meaning: The appliance has lost the Ethernet signal. This icon will only be displayed after the appliance has successfully booted and then loses its Ethernet signal.

Actions to take:

1. Check that the Ethernet cable is correctly plugged into the back of the appliance and the other end into the correct hub, switch, or network outlet.
2. If the appliance is connected via a hub or switch, make sure that the hub or switch is on and configured correctly.
3. Check that the Sun Ray server is up and running.

Software Failure



Software or server failure:

Meaning: The appliance has lost its connection to the Sun Ray Authentication Manager or DHCP was unable to renew its lease for an IP address.

Actions to take:

1. Check that the Sun Ray server is up and running.
2. Check that the Sun Ray services, including the Authentication Manager are up and running on the Sun Ray server.
3. Check that DHCP on the Sun Ray server is configured correctly, is up and running and has not run out of IP addresses to assign to clients.

Firmware Download



Firmware download: the dashes under the machines indicate progress.

- downloading PROM software
- saving PROM software

■ Firmware 1—Downloading PROM Software

Meaning: The appliance is currently downloading new flash PROM software from the Sun Ray server.

Actions to take:

- Please wait until the download is done. Downloading and saving the new PROM software usually takes less than a minute. If you interrupt the download, the appliance will have to download new PROM software the next time it reboots.
- Firmware 2— Saving PROM Software

Meaning: The appliance has just downloaded new PROM software from the Sun Ray server and is saving it to the appliance's PROM.

Actions to take:

- Please wait until the download is done. Downloading and saving the new PROM software usually takes less than a minute. If you interrupt the download, the appliance will have to download new PROM software the next time it reboots.

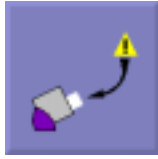
Ethernet Address



Ethernet address:

When the three audio volume control keys are pressed simultaneously, the last six hexadecimal digits of the Ethernet address are shown. This uniquely identifies the appliance. This icon displays from 5-15 seconds. If the user has a non-Sun keyboard, have the user disconnect and reconnect the Ethernet wire. Link speed is also indicated below the symbol (for example, 10F, 10H, 100F, 100H). The F stands for full duplex; H represents for half duplex.

Card Read Error OSD



The Card Read Error OSD appears whenever the firmware is unable to read the card. The cause is one of the following:

- The appliance is an old hardware revision that is unable to read this particular card.
- The appliance is running old firmware and should be upgraded.
- The card contacts are dirty, the contacts on the card reader are dirty, or the card is not properly inserted.
- The card is malfunctioning and needs to be replaced.
- The card is of a type which the firmware is not configured to read. Refer to “Managing Smart Cards From Different Vendors” on page 165.
- There is an error in the configuration for reading this type of card (see also “Smart Card Vendor Configuration Files” on page 175).

Prompt for Card Insertion OSD



If the current authentication policy allows access only by card, then this OSD appears and prompts the end user to insert a card.

Access Denied OSD



The Access Denied OSD appears when the current authentication policy denies access to the presented token. Specifically, this icon is displayed if a disabled card has been inserted into an appliance.

LEDs

TABLE A-1 Power LED

State of LED	Action to take
Off	Check to see if the appliance is plugged in. Replace the appliance.
Yellow	Hardware fault. Replace appliance.
Blinking	PROM is corrupted. Use <code>utadm</code> to restore the firmware.

Q: Where do I look if an appliance is not working?

A: There are log files in `/var/opt/SUNWut/log`. For example, if the appliance is in Authentication mode, there may be log messages in `/var/opt/SUNWut/log/messages`.

1. Check the onscreen display (OSD).
2. If there is no Ethernet connection, check all of the connectors.
3. Verify that DHCP is running on the server.

```
% ps -ef | grep dhcp
```

4. If there is still a problem contacting the Authentication Manager, check for the Session Manager.

```
% ps -ef | grep utsessiond
```

5. Check to see if the Authentication Manager is running.

```
% /usr/ucb/ps -axww | grep utauthd
```

The Authentication Manager creates log files in `/var/opt/SUNWut/log/messages`.

Q: How can a user check to see if the Sun Ray 1 appliance can play audio files (*.au)?

A: Ask the user to type:

```
% cat /usr/demo/SOUND/sounds/whistle.au >/dev/audio
```


The Sun Ray software is designed to work with `$AUDIODEV`. Some applications use `/dev/audio`. There is a Sun Ray preloaded library that translates access to `/dev/audio` and `/dev/audioct/` to the appropriate filenames for the audio device on the Sun Ray 1 appliance. To determine if this feature is enabled, type:

```
% echo $LD_PRELOAD
```

The output should contain a file name such as `libc_ut.so`. This translation is enabled by default.

Note – The un-patched ShowMe TV 1.2.1 is known not to work properly with this workaround. Upgrade to ShowMe TV 1.3 properly.

Q: I want to use the Sun Ray 1 appliance in a kiosk. What options do I have?

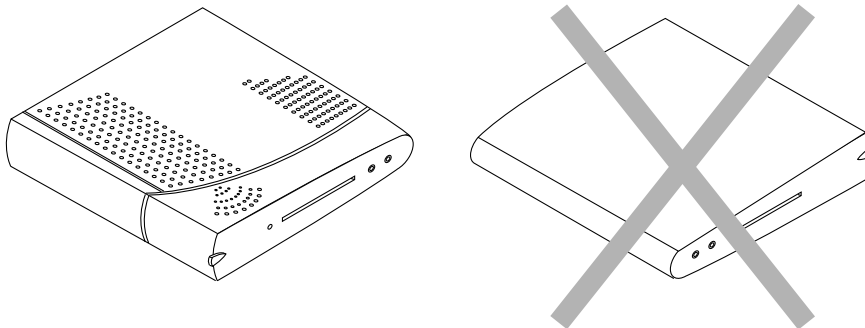
A: For information on kiosk mounting for the Sun Ray 1 appliance see:

<http://www.sun.com/sunray1>

For additional information kiosks, no-admin user mode, see the *Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide*.

Q: What if a user has broken or misplaced the Sun Ray 1 appliance's base?

A: The appliance must lie on a desk speaker-side up. It will overheat if it is placed speaker-side down.



Q: All (or most of) the monitors at our site can only support 1152x900 resolution. The X server comes up in 1280x1024 resolution, so users have to scroll around the larger screen. What can I do?

A: The user can use the Settings screen.

The `utxconfig(1M)` command can be used to set the default X server resolution to match the majority of monitors attached to the appliances. For individual users with different requirements, `utxconfig(1M)` can create specific parameters for one user. (This is based on the user's authentication token. In workstation replacement mode, the token is the Ethernet address of the appliance itself. Otherwise, it is based on the smart card ID.)

To set the resolution, as superuser type:

```
# utxconfig -a -r 1152x900
```

Q: Is there any way to reset an appliance? How does a user power cycle the appliance?

A: To reset the appliance, power cycle it.

▼ To Power Cycle a Sun Ray 1 Appliance

1. Ask the user to press the Control key simultaneously with the power key.

If the user has a Sun USB keyboard or has a keyboard with a power control key, the user can press the Control key simultaneously with the power key to reset the appliance. The power key on Sun USB keyboards is typically marked with a crescent moon and is in the upper right corner of the keyboard (see FIGURE 1-4 on page 11).

2. The other way to power cycle an appliance is to have the user disconnect and reconnect the power cord.

Q: The users at my company work from 8am - 5pm. Is there any way I can ping the appliances at 7:45am to see if they are all functional?

A: Ping the appliances in the usual manner using their IP addresses. Get the active IP addresses from the DHCP table.

Use the Sun Ray administration application to list currently connected appliances (see "Listing Currently Connected Desktops" on page 107).

User Questions

Q: The user's screen locked up. What do I do?

A: There are two possibilities:

1. Symptom: All the windows that had been iconified are restored and the user cannot move or resize them, but can move the mouse pointer.

Cause: The window manager `dtwm` or `olwm` has died.

Solution: Use a terminal window if available or `rlogin` with the `DISPLAY` variable set correctly to restart `dtwm` or `olwm`. For example:

```
% rlogin machine_name -l user_name
% setenv DISPLAY xxxxx
% /usr/dt/bin/dtwm &
```

2. Symptom: The server freezes and the user cannot resize or move any window. The user can move the mouse, but none of the windows highlight.

Cause: Usually the user's last application has locked the server and will not release it.

Solution:

- a. Determine the last application used by the user and kill it.
- b. Try power cycling the appliance. If the user is using a smart card, ask the user to remove the smart card. If the user removes the smart card and the screen does not go blank, the Sun Ray 1 enterprise appliance needs to be replaced.
- c. As a last resort you can kill the X server.
 - i. To identify the X server's PID, type:.

```
% ps -ef | grep xsun | grep <username>
```

- ii. Next, kill the process associated with the X server. Type:

```
% kill <pid>
```

Q: A user gets one of the following (or similar) errors when starting an application.

```
/usr/openwin/bin/xcolor: unable create colormap (8)

Application initialization failed: couldn't find an appropriate visual

could not get visual

X Error of failed request: BadValue (integer parameter out of range for operation)
Major opcode of failed request: 91 (X_QueryColors)
Value in failed request: 0xc3b2ae
Serial number of failed request: 82
```

A: The application may be written to use only 8-bit PseudoColor graphics. Many older programs require an 8-bit PseudoColor visual.

Sun Ray software supports an 8-bit visual, but enabling it requires more memory for the X server and causes some graphics performance degradation. The general use of the 8-bit visual support reduces the scalability of the Sun Ray server.

If an important application fails for a user or set of users, the `utxconfig(1M)` command can be used to enable the 8-bit support and/or make it the default visual for them.

Unless needed, 8-bit visuals should be disabled. Try enabling the 8-bit support before making it the default visual, because using the 8-bit visual as the default visual causes a greater negative impact on performance and scalability than enabling it for a few users. However, some applications do not search for the visual they require and blindly assume that the default visual is what they should use. For such programs, using the 8-bit visual as the default visual is the only choice.

To allow 8-bit PseudoColor visual to be enabled, as superuser type:

```
# utxconfig -d $DISPLAY -p on
```

To make 8-bit PseudoColor visual the default, as superuser type:

```
# utxconfig -d $DISPLAY -p default
```

Note – See the `utxconfig` command man pages for more information about this command.

A normal user can run the `utxconfig` command for a session as long as they have access to the X display for the session. Only `root` can make a change for someone else or change the default values.

Although the display specification is used to identify the X server configuration that should be changed, `utxconfig` stores the configuration based on the token that provides access to the session. Therefore, the configuration will stay with the user (for smart card tokens) or the appliance (for default tokens) even if a different display number is allocated in the future.

Q: A user can start commands from menus and the CDE bar, but cannot start them from terminal windows. What is wrong?

A: The user's startup scripts (`.cshrc`, `.login`, `.profile`, or `.dtprofile`) probably set the `DISPLAY` variable. The scripts should be changed to only set `DISPLAY` if it is not already set or to retain the display number (the part after the `:`). For example:

```
% echo $DISPLAY
% yoyodata:62.0
```

Q: I have a non-smart card user whose appliance just failed in the middle of a session. I replaced the appliance. How do I get the user reconnected to their session?

A: Find and kill the users X server and have the user login again. For this release, there is no mechanism available to save the data.

Q: A user's session is timing out and not connecting. What do I do?

A: Change the time-out value.

If your server is under a heavy load, increasing the amount of time the Authentication Manager waits to receive a request from the Sun Ray 1 appliance will keep the session from timing out.

The *time-out* value is the maximum allowed time interval between communications from an appliance to the Authentication Manager. The Authentication Manager waits the prescribed time as defined in the `auth.props` file (60 seconds). If 60 seconds passes and no message is received, the Authentication Manager queries the appliance. If there is still no response after another 60 seconds, the Authentication Manager closes the TCP connection to the appliance.

Tip – If you have a server that is highly loaded, you can change the time-out value to a much higher number than the default of 60 seconds.

▼ To Modify the Time-Out Value

1. As superuser, open the `/etc/opt/SUNWut/auth.props` file with a text editor.

```
# Copyright (c) 04/03/99 Sun Microsystems, Inc. All Rights Reserved
# @(#)auth.props.txt1.22 99/04/03

# Timeout
# Terminals are required to send a message to the authentication manager
# at least once every {timeout} seconds.
timeout = 60

# Workers
# This is the target number of spare threads to maintain to handle
# new terminal connections.
workers = 3
      :
      :
      :

# Service port
# The authentication manager listens on this port for connections from
# terminals.
port = 7009

# Admin/LDAP configuration file.
# Uncomment the following line to
# enable raw to logical token name mapping, logical token record lookup,
# and desktop status reporting.
# The "RegisteredDistributed" authentication policy depends on a
# properly configured LDAP database.
# This property has no default value.
#
#adminConfigFile = utadmin.conf

# Module Directory
# All authentication modules must be located in the following directory
moduleDir = /opt/SUNWut/lib/modules

# Policy
# The active authentication policy determines which tokens and terminals
# are accepted and granted access to system services.
policy = ZeroAdmin
# policy = RegisteredDistributed
      :
      :
      :
```

2. Locate the default time out value (near the beginning of the code listing).

```
timeout=60
```

3. Comment out the default value and enter a new value, better suited to your server conditions. (The value must be in seconds.)

```
#timeout=60  
timeout=120
```

4. Save the file and reboot the Sun Ray server.

Note – The `/etc/opt/SUNWut/auth.props` file also contains authentication policy information

Server Questions

Q: Which files are added, removed, or modified by the installation process?

A: The following files are affected by the Sun Ray software installation:

```
/etc/nsswitch.conf  
/etc/hostname.{hme,qfe,gem}[0-9]  
/etc/inet/hosts  
/etc/inet/netmasks  
/etc/inet/networks  
/var/dhcp  
/var/dhcp/dhcptab  
/etc/default/dhcp  
/etc/init.d/dhcp  
/etc/default/sys-suspend  
/usr/dt/config/sessionetc
```

Changes are marked with a project identification string (at this writing the strings are: “SUNRAY ADD”, “SUNRAY DEL”, “SUNRAY BEGIN”, and “SUNRAY END”).

Q: The server’s hard drive is constantly being accessed. Why is the Sun Ray server swapping so often?

A: You may need to increase your server's memory. At least 256MB of RAM is recommended for most network environments with 40-60MB per user. If you have less, your server relies upon any available swap space on your hard drive. Use the `wsinfo` command to review your system's resources.

```
% /usr/openwin/bin/wsinfo &
```

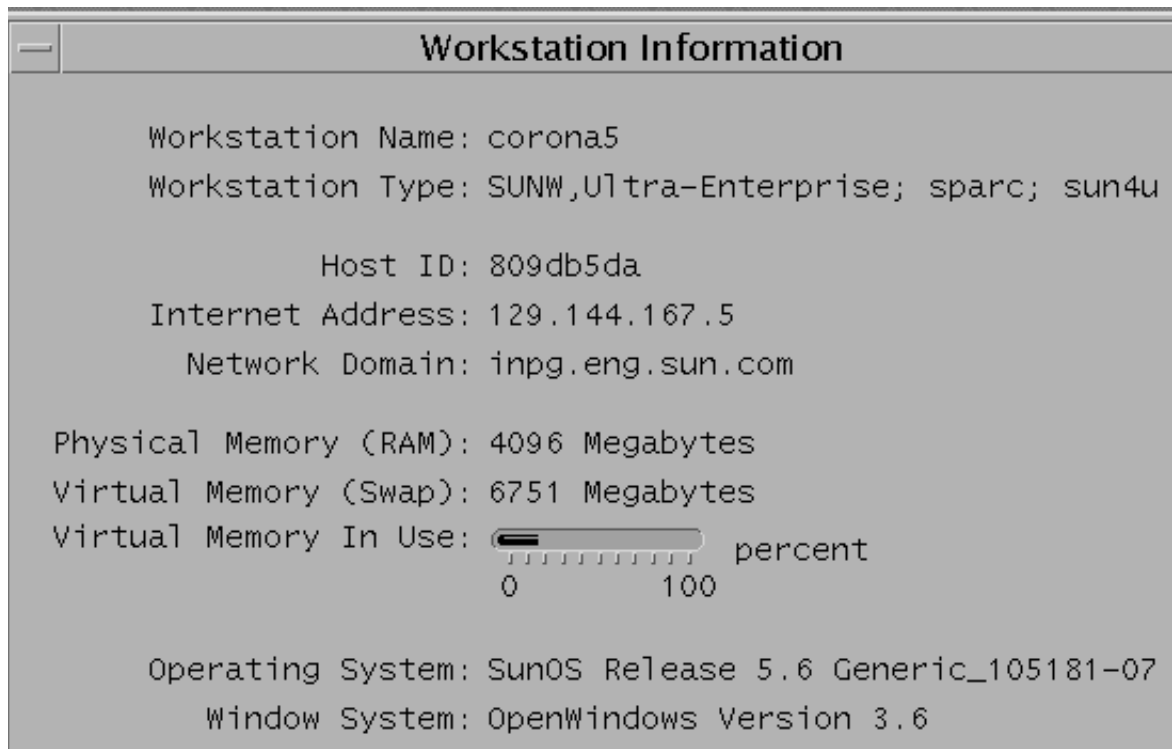


FIGURE A-1 Accessing Workstation Resource Information

To determine if the server is swapping, type:

```
% vmstat 5
```

If the column marked `sr` is larger than 10 (a noticeable amount of time), you should consider adding memory.

Q: A user is receiving an Unable to get pty error message. What is wrong?

A: The Sun Ray server has exhausted the number of pseudo terminals defined. If a system does not have enough pseudo terminals defined, users can not bring up a shell window and will not be able to login. For example, a network consists of 50 Sun Ray 1 appliances and the `pty` entry is set to 40. When the 41st user tries to open a shell window, this error message displays. As `root`, edit the `/etc/systems` file `pt_cnt` value to increase the number of available pseudo terminals. Change the `pt_cnt` entry to a higher number (at least four or five times the number of users). You must reboot. For example:

```
# set pt_cnt=40
set pt_cnt=100
```

For additional information see “Setting System Parameters” on page 62.

Q: Does the Sun Ray software support the Direct Graphics Access (DGA) extension to X11?

A: No. The Sun Ray server software does not support the SunDGA (Direct Graphics Access) extension to X11. The Sun Ray server software correctly reports that DGA is not supported to any application that initiates an inquiry. Normally applications make use of DGA through libraries (for example, XIL) that deal with the inability to use DGA and use an alternate path.

Q: A user is working in a CAD program with complex graphics. When the user is scrolling the graphic, it is jerky. Is there anything I can do?

A: Make sure the enterprise desktop is using a 100 Mbyte full duplex link. Also check the system’s configuration and the application’s requirements. Possible remedies on the server include: Adjust process priorities, add more memory, add a CPU, or add more disk space.

Q: Why is my ShowMe TV™ session running slow?

A: For best performance with the Sun Ray server, use the latest version of ShowMe TV. It is recommended that you use ShowMe TV 1.3 or later. This application can be downloaded from the following URL:

<http://www.sun.com/>

Q: If I am using AutoCAD, what settings should be enabled?

A: AutoCAD is an 8-bit only program and requires the 8-bit visual to be enabled. This setting can be enabled (for the current user) by typing:

```
# /opt/SUNWut/lib/utxconfig -p on
```

The `utxconfig(1M)` manual page gives more information, including how to make this the system-wide default. The end users need to log out and log in for the change to take effect.

The Green Newt Cursor

The green newt cursor is the default cursor for the Sun Ray 1 appliance. The cursor remains as a green newt until an application, typically the X Window server (`Xsun`), changes the cursor to an “X”, hourglass, or arrow. The green newt cursor does not necessarily mean the Sun Ray 1 appliance is hung or in an error condition, but rather that the Sun Ray 1 appliance is ready and awaiting display rendering commands from `Xsun`.

The `Xsun` server is started by the `dtlogin` daemon. In the process of starting the `Xsun` server, the `dtlogin` daemon reads two configuration files:

- `/etc/dt/config/Xservers`
- `/etc/dt/config/Xconfig`

If the green newt cursor is displayed for an extended period, there is no X Window server running. The problem can usually be traced back to an older version of the `dtlogin` daemon or the configuration files for the `dtlogin` daemon.

To troubleshoot a green newt cursor, you need to consider:

- Is There Really a Problem?
- Is the Problem Caused by Hardware?
- Is the `dtlogin` Daemon Up-to-Date?
- Is the `dtlogin` Session Hung?
- Are the Configuration Files Corrupt?

Is There Really a Problem?

The Sun Ray administration model has six user session types:

- Default — normal user login
- Register — user self-registration
- Kiosk — anonymous user operation

- Insert card — user smart card required
- Card error — unrecognized user smart card type
- No entry — user's smart card token is blocked

The first three session types have normal login processes. The last three session types do not have a login process at all, but display an icon on the Sun Ray 1 appliance monitor along with the green newt cursor. The icons indicate that the user must take other steps before successful login is possible. If the user were to immediately remove and reinsert the smart card, the icon would disappear, but the green newt cursor would remain.

These last three session types, their icons, and the appearance of the green newt cursor are not cause for alarm. The user can:

- Insert a recognized smart card in the correct orientation
- Ask the Sun Ray administrator to grant access

See the *Sun Ray 1 Quick Reference* and *Sun Ray 1 Troubleshooting Guide* for more information regarding Sun Ray 1 appliance startup and the icons displayed.

Is the Problem Caused by Hardware?

Sluggish Sun Ray server performance or excessive disk swapping is an indication that the Sun Ray server is under-provisioned. Under these circumstances, there is just not enough virtual memory available to start an X Window server instance for a user's session. If after several retries the `Xsun` process does not start, the `dtlogin` daemon just gives up. With no X Window server running, the cursor remains a green newt.

The solution in this situation is to add more memory or increase the size of the swap partition. See the *Sun Ray Server Software 1.0 Administrator's Guide* and the *Sun Ray Server Software 1.0 Installation Guide* for information regarding Sun Ray server sizing requirements.

Is the `dtlogin` Daemon Up-to-Date?

The `dtlogin` daemon is part of the Solaris™ operating environment and has existed long before the Sun Ray software. The Sun Ray administration model uses the `dtlogin` daemon in new ways, such that certain bugs in the `dtlogin` daemon have become apparent. Patches to fix these bugs in the `dtlogin` daemon are available.

At the time of this writing, the following patches were available:

- For CDE:
 - 105703-17 (Solaris 2.6 SPARCstation™)
 - 107180-12 (Solaris 7 SPARCstation)
- For the X Window server:
 - 105633-29 (Solaris 2.6 SPARCstation)
 - 107078-18 (Solaris 7 SPARCstation)

For the latest information regarding Sun Ray software bugs and patches, check this URL:

<http://www.sun.com/products/sunray1/patches.html>

Solaris operating environment patches and other software patches are available at this URL:

<http://access1.sun.com>

Note – An additional patch, 108303-xx, is available to correct a bug in the `utdtsession` command at <http://access1.sun.com>. This patch helps prevent corruption of the `/etc/dt/config/Xservers` and `/etc/dtconfig/Xconfig` files.

Is the `dtlogin` Session Hung?

Under certain circumstances, the `dtlogin` daemon may not be able to start the `Xsun` server. Without an X Window server running, the cursor remains a green newt. In this case, the `dtlogin` daemon has given up and has marked the user's session as bad. Consequently, this action prevents any further X Window server start-up attempts for the user's session.

To resolve this situation, the `dtlogin` session must be manually unconfigured. After which, the system will automatically reconfigure the session.

Caution – If patch 108303-xx has *not* been applied, Step 6 of this procedure could corrupt the `/etc/dt/config/Xservers` or `/etc/dtconfig/Xconfig` files. Verify the integrity of these files after conducting this procedure. See the next section, “Are the Configuration Files Corrupt?” on page 209.

▼ To Identify and Unconfigure the dtlogin Session

1. **On the keyboard of the Sun Ray 1 appliance displaying the green newt cursor, press all three audio keys at the same time.**

An icon with the last six digits of the Sun Ray 1 appliance Ethernet address is displayed.

2. **Record the six hexadecimal digits.**

For example, B05E25.

3. **Keep the smart card inserted in the Sun Ray 1 appliance that is hung.**

4. **On another Sun Ray 1 appliance or the Sun Ray server, log in as superuser and open a shell window.**

5. **Create a server status file.**

Be sure to press the Return key after typing `sunraystatus`.

```
# telnet localhost 7010 > /tmp/sunraystatus
status
```

The file is created and Telnet is exited.

6. **Edit the file using `vi`:**

```
# vi /tmp/sunraystatus
```

The following is an excerpt of a `sunraystatus` file. This example illustrates the information used from Step 1 through Step 4:

```
.
.
begin
terminalId=CoronaP1.080020b05e25(Step 7)
.
.
tokenName=ZeroAdmin.m1.MicroPayflex.00005bca65000100(Step 9, 10)
.
.
end (Step 8)
.
.
```

7. Search for the Ethernet address:

```
:set ic  
:/address
```

Where *address* is the Ethernet address from Step 1. For example, B05E25.

In the example, the cursor is moved to the line:

```
terminalId=CoronaP1.080020b05e25.
```

8. Scan down the listing until the word `end` is encountered.

9. Scan back up for the word `tokenName`.

In the example:

```
tokenName=ZeroAdmin.m1.MicroPayflex.00005bca65000100.
```

10. Record the text following the `= sign`.

In the example: `ZeroAdmin.m1.MicroPayflex.00005bca65000100.`

11. Exit `vi`:

```
:q!
```

12. Unconfigure the `dtlogin` session:

```
# /opt/SUNWut/lib/utdtssession -t text delete
```

Where *text* is the text recorded in Step 4. For example,

```
ZeroAdmin.m1.MicroPayflex.00005bca65000100.
```

13. Reboot the hung Sun Ray 1 appliance by pressing the Control and Power keys simultaneously. Alternatively, remove and reinsert the smart card.

The `dtlogin` session is automatically reconfigured and presented on the Sun Ray 1 appliance.

Are the Configuration Files Corrupt?

These two configuration files are susceptible to corruption:

- `/etc/dt/config/Xservers`
- `/etc/dt/config/Xconfig`

These files are used by the `dtlogin` daemon. When they are corrupt, the `dtlogin` daemon cannot properly start the `Xsun` server. Without an X Window server running, the cursor remains a green newt.

▼ To Determine the Integrity of the Configuration Files

1. As a user of the Sun Ray server, open a shell window and compare the `/usr/dt/config/Xservers` and `/etc/dt/config/Xservers` files:

```
% diff /usr/dt/config/Xservers /etc/dt/config/Xservers
```

This command compares a known good file with the suspect file. The output should be similar to the following example:

```
106a107,130
> # BEGIN SUNRAY CONFIGURATION
> :8 SunRay local@none /usr/openwin/bin/Xsun :8 -nobanner
.
.
> :9 SunRay local@none /usr/openwin/bin/Xsun :9 -nobanner
> # END SUNRAY CONFIGURATION
```

Note – This is a simplified example. Your output may have tens of lines between the `BEGIN SUNRAY CONFIGURATION` and `END SUNRAY CONFIGURATION` comments.

In the first line of output, there is `106a107,130`. The `106` means that the two files are identical to the 106th line of the files. The `a107,130` means the information on lines 107 through 130 of the second file would have to be added to the first file to make it the same as the second.

If in your output the first three digits are a number less than 100, the `/etc/dt/config/Xservers` file is corrupt.

2. Compare the `/usr/dt/config/Xconfig` and `/etc/dt/config/Xconfig` files:

```
% diff /usr/dt/config/Xconfig /etc/dt/config/Xconfig
```

The output should be similar to the following example:

```
156a157,180
> # BEGIN SUNRAY CONFIGURATION
> Dtlogin.*_8.environment: CORONA_TOKEN=ZeroAdmin.m1.at88sc1608.6d0400aa
.
.
> Dtlogin.*_9.environment: CORONA_TOKEN=ZeroAdmin.m1.at88sc1608.a10100aa
> # END SUNRAY CONFIGURATION
```

Note – Again, this is a simplified example. Your output may have tens of lines between the `BEGIN SUNRAY CONFIGURATION` and `END SUNRAY CONFIGURATION` comments.

If in your output the first three digits are a number less than 154, the `/etc/dt/config/Xconfig` file is corrupt.

▼ To Replace the `Xservers` and `Xconfig` Files

Note – Replacing the `Xservers` file requires shutting down all Sun Ray 1 appliance services. Remember to inform the users of the outage.

1. As superuser, open a shell window and stop the Sun Ray server:

```
# /etc/init.d/utsvc stop
```

2. Replace the `Xservers` and `Xconfig` files as appropriate:

```
# /bin/cp -p /usr/dt/config/Xservers /etc/dt/config/Xservers
```

```
# /bin/cp -p /usr/dt/config/Xconfig /etc/dt/config/Xconfig
```

3. Re-initialize the authentication policy:

```
# /opt/SUNWut/sbin/utpolicy -i clear
```

The `utpolicy` command will wait for a full minute to insure that all Sun Ray 1 appliance X Window servers have exited.

The extra lines within the previous `Xservers` and `Xconfig` files are automatically rebuilt.

Security

The Sun Ray system does not encrypt its communications. This means if someone gains access to the data, they have access to what is typed and displayed at the Sun Ray 1 enterprise appliance. The primary forms of protection available are to physically secure the shared resources (uplinks, server, etc.) and to use switched network equipment for the last link to the Sun Ray 1 appliances.

Note – The Sun Ray system consists of a server connected to the Sun Ray 1 appliances by a dedicated, private network (interconnect). The appliances and server communicate over this private switched network.

Using switched network gear for the last link to the appliances makes it very difficult for a malicious user using a PC or network snoopers at one of the network ports to obtain unauthorized information. That is because switches only send packets to the proper output port, so a snoopers plugged into another port will receive no unauthorized data. If the server and wiring closet are secure, the last hop is switched, and the appliance is plugged directly into the wall jack, then it is virtually impossible to intercept the communications between the server and the appliance.

This appendix covers the following security topics:

- “Physical Access” on page 214
- “Superuser Access” on page 214
- “Sun Ray User” on page 214
- “Non-Sun Ray Clients on the Interconnect” on page 215
- “Switches” on page 215

Physical Access

There should be physical security on all shared uplinks and switches. This means that the server, the cables to the switch, and the switch are in locked areas where only trusted personnel have access.

Someone with physical access to the network can monitor authentication and all keystrokes that travel across the network.

The network traffic is formatted by the Sun Ray software, so an inexperienced user will have difficulty understanding the information. However, a determined user will be able to decode the information. When challenge/response tokens are available, the authentication challenge and response portions of the messages will be hashed or encrypted. With this added security, even if authentication traffic is monitored, it will not reveal any useful information.

Superuser Access

If someone has superuser access to the Sun Ray server, that person can gain access to every user's smart card ID, password, and any user's Internet business. By using the `snoop` command, all authentication information and keystrokes are available to read. In addition, superuser can read or modify any file, erase disk contents, or crash the server. Therefore, access to the superuser account should be controlled and only provided to trusted personnel.

Sun Ray User

A normal Sun Ray user can access the user's own information, and any other user's information only in the regular Solaris manner (for example, through the other user's home directory).

Non-Sun Ray Clients on the Interconnect

DHCP default configuration will assign an IP address to any client that plugs into the switch, which means someone with physical access to the interconnect can plug in a computer. That person may be able to copy files from other servers and could possibly cause performance degradation.

Note – The quality of service assumptions that the Sun Ray system depends on cannot be guaranteed when non-Sun Ray 1 appliances (computers) are used on the private interconnect. Do NOT connect non-Sun Ray devices to the Sun Ray interconnect.

The information available to a PC user plugged into a switch is limited to just that one port.

If a PC is plugged into a hub, all of the traffic going through that hub is available to the PC user. This situation is of greater concern because using a hub means that there is more opportunity for snooping keystrokes to get a login name and password. When challenge/response tokens are available, the system will be configurable such that merely knowing a login name and password is not enough to gain access to the system.

Switches

Some switches support remote monitoring features where all the traffic going to or from an identified port can be silently copied to another port. With this feature, someone can see every IP packet to or from a Sun Ray 1 appliance.

Another security concern present on almost all switches: after gaining access to the switch, it is possible and fairly easy to disable a specific port on the switch, thereby denying service to a user. It is therefore important to secure your switches and prevent unauthorized access to control functions by setting passwords and turning off remote access to switch control functions.

Tips for Using Non-Sun Web Servers

The web-based interface of the Sun Ray administration application is designed to run with the Sun WebServer 2.1. However, if you want to run it under a different web server, the following general tips are provided.

- Make sure that your web server's document root is either set to `/opt/SUNWut/lib/locale/html` or is a symbolic link to it (the preferred option).
- Make sure that your web server's `cgi-bin` directory contains copies of the executables in `/opt/SUNWut/cgi-bin` or contains individual symbolic links to them (the preferred option).
- If you use symbolic links for the document superuser or CGI executables, make sure your web server is configured to allow symbolic links.
- Set up your web server's mappings so all requests for the top-level document (the `/` document) are mapped to `/cgi-bin/main`. You can do this through HTTP redirects, aliases, or similar mechanisms.
- Set up your web server so it only accepts connections from the local host unless you have installed additional security software that encrypts connections between the browser and server.
- Set up your web server so CGI applications are run as the `@(CGI_USER)` you specified on your worksheet (see "Configuring the Software" on page 39) and that the `/var/opt/SUNWut/cgitokens` subdirectory is owned by this same user and is only readable, writable, and executable by this user.

Tips for Language Selection

This section describes all the interfaces where the language (locale) can be changed in the Sun Ray server software as well as specific language issues.

This appendix covers the following topics:

- “Language Selection for System Administrators” on page 219
- “Language Selection for Users” on page 221
- “Using Solaris admintool(1m) in non-English locales” on page 221
- “Henkan Key or Hangul Key” on page 222

Language Selection for System Administrators

Sun Ray Web-based Interface of the Administration Application

The web-based administration application is localized in the following four languages:

- English—en_US
- French—fr
- Japanese—ja
- Simplified Chinese—zh

When you log in to the web-based administration application, the login page (see FIGURE 7-2 on page 92) defaults to the server’s default locale as specified in the Sun Ray configuration file `/etc/opt/SUNWut/utadmin.conf`.

You can override this default locale for your current administration login session by selecting a different locale from the Language pulldown menu on the login page (see FIGURE 7-2 on page 92). For more detail, see the `utadmin.conf(4)` man page.

Self-Registration GUI

When the Sun Ray server is configured with an authentication policy that enables self-registration, the self-registration GUI that is displayed to the user is localized in the following 10 languages:

- English—en_US
- French—fr
- German—de
- Spanish—es
- Italian—it
- Swedish—sv
- Japanese—ja
- Korean—ko
- Simplified Chinese—zh
- Traditional Chinese—zh_TW

The self-registration GUI detects the locale to use from the operating system's default locale via some environment variables. To change the locale that is displayed, edit the `/etc/default/init` file and specify the desired locale using the `LC_ALL` or `LC_CTYPE`, or `LANG` variable. Setting the `LANG` variable is the preferred method. Rebooting the server is not necessary. See the `init(1M)` man page for the default values and more information.

Note – Note that this file specifies the default environment variables that are passed to any process started on this server.

Input to the Self-Registration GUI

The Self-registration GUI only supports the input of ASCII characters. It does not support input of non-ASCII characters (for example, Asian characters or European letters that use diacritic marks). Contact your site system administrator to input these characters via the administration application (GUI or the command-line interface).

Note – The language selection that is done for the self-registration GUI is so that the GUI and related messages are presented in the selected language.

Language Selection for Users

Users can choose in which language to view the Sun Ray 1 Settings GUI.

The Sun Ray 1 Settings GUI is localized in the following 10 languages:

- English—en_US
- French—fr
- German—de
- Spanish—es
- Italian—it
- Swedish—sv
- Japanese—ja
- Korean—ko
- Simplified Chinese—zh
- Traditional Chinese—zh_TW

When the user starts an X windows session on the `dtlogin` page, the user can select a different language from Options►Language pulldown menu. The selection the user makes here is automatically detected by the Sun Ray 1 Settings GUI. See the `utsettings(1)` man page for more information.

Using Solaris `admintool(1m)` in non-English locales

If you use `admintool(1m)` to create a new user account whose login shell is not the C shell, `admintool` copies `/etc/skel/local.profile` as the `.profile` file for the user in the users's home directory. This `.profile` file has the following line that disables the user's input of 8-bit characters on a terminal:

```
stty istrip
```

If the users need to have 8-bit character input, delete this line from their `.profile` file or modify the `/etc/skel/local.profile` file before creating new user accounts with `admintool`.

Note – C-shell user's have 8-bit character input on a terminal by default.

Henkan Key or Hangeul Key

If the Henkan key for traditional Chinese or Hangeul key for Korean (multiple key mode toggle switch) does not work and you want it to, then use the properties setting for the `htt(1)` to select the toggle of your choice.

Errors From the Authentication Manager

This appendix lists the errors you can receive from the Authentication Manager and their meaning.

This appendix covers the following Authentication Manager topics:

- “Message Format” on page 223
- “Error Messages” on page 225

Message Format

The general format of the log messages is:

```
timestamp    thread_name    message_class    message
```

For example:

```
1999.04.15 21:46:33.909 PDT Client6 NOTICE: SESSION_OK user.924231680-8477
```

In this example, a session was successfully initialized for the authentication token “user.924231680-8477”.

Message components are defined as follows:

- `timestamp` is of the form:
year.month.day hours:minutes:seconds.milliseconds timezone
- `thread_name`

There are several different types of threads. The most common is the thread that handles appliance authentication, access control and session monitoring. These threads are named “Client” plus number. The Client# thread names are reused when a connection terminates. Other threads are:

- `SessionManager#`—Communicate with `utsessiond` on behalf of a `Client#` thread.
- `AdminJobQ`—Used in the implementation to wrap a library that would not otherwise be thread safe.
- `CallBack#`—Communicate with applications such as `utload`.
- `Control`—Listens for connections from `utsessiond` as well as the initial communications with applications such as `utload`.

Note – Messages with the same thread name are related. The exception to this is when a `Client#` thread disconnects an appliance and then purges the connection information from memory. After a `Client# DESTROY` message, the next use of that `Client#` thread name will have no relation to previous uses of the thread name (in other words the thread names are reused).

- `message_class`
 - `CLIENT_ERROR`—Indicates unexpected behavior from an appliance. These messages can be generated during normal operation if an appliance is rebooted.
 - `CONFIG_ERROR`—Indicates a system configuration error. The Authentication Manager generally exits after one of these errors is detected.
 - `NOTICE`—Logs normal events.
 - `UNEXPECTED`—Logs events or conditions that were not anticipated for normal operation but are generally not fatal. Some of these errors should be brought to the attention of the Sun Ray product development team.
 - `DEBUG`—Beneficial to developers and only occur if they are explicitly enabled. Debug messages can reveal session IDs, which must be kept secret to ensure proper security.

Error Messages

TABLE F-1 Possible Errors

Error class	Message	Description
CLIENT_ERROR	...Exception ... : cannot send keepAliveInf	Error encountered while attempting to send a keep alive message to an appliance.
	...keepAlive timeout	An appliance has failed to respond within the allotted time. The session is being disconnected.
	duplicate key:	Appliance does not properly implement the authentication protocol.
	invalid key:	Appliance does not properly implement the authentication protocol.
CONFIG_ERROR	attempt to instantiate CallBack 2nd time.	Program error.
	AuthModule.load	Problem encountered while loading configuration module.
	Cannot find module	Program or installation error.
	Cannot get AdminImpl methods:	Installation error.
	Cannot open call back socket on port ...	Runtime error. Is cbport busy?
	Cannot read properties file: ...	Installation or configuration error.
	cannot read properties file: ...	Installation or configuration error, check file.
	Cannot read session types	Check file, usually /etc/opt/SUNWut/ sessionTypes.props
	during status:	Program error or Java VM error.
	Error while reading policy file ...	Installation or configuration error.
Invalid configuration. Exiting	Check value of auth.props:policy and the contents of the file indicated by the policy property.	

TABLE F-1 Possible Errors (Continued)

Error class	Message	Description
	Invalid option	Program error in the <code>/opt/SUNWut/lib/utauthd</code> script.
CONFIG_ERROR	No policy specified	A policy must be specified using the <code>utpolicy</code> command. Check the "policy" keyword in the <code>/etc/opt/SUNWut/auth.props</code> file.
	Policy file does not exist: ...	Installation or configuration error.
	refreshProperties: file non-existent: ...	Installation or configuration error, check file name.
	refreshProperties: no filename	Configuration error, check the <code>/etc/opt/SUNWut/auth.props</code> file.
	SessionManager.initiat eCallback: ... claims to be already connected	Possible configuration error.
	sessionTypesFile not specified	The required parameter "sessionTypesFile" is missing from / <code>etc/opt/SUNWut/auth.props</code> file.
	UNCONFIGUED MODULE	An authentication module is not configured and will not be offered a token. This can be a serious problem and should probably be a fatal error. However, none of the currently implemented authentication modules should ever fail this test.
	utjadmin.so or configuration error in ...	Check installation.
	XXX CANNOT instantiate module instance=	Program, configuration, or installation error.
NOTICE	"discarding response: " + param	No controlling application is present to receive appliance response.
	"NOT_CLAIMED PARAMETERS: " + param	A token was not claimed by any authentication module.
	...authentication module(s) loaded.	Notification that authentication modules have loaded.
	...DISCONNECT ...	Normal notification of disconnection.

TABLE F-1 Possible Errors (Continued)

Error class	Message	Description
	...finalize lifetime=	An authentication record has been garbage collected by the Java Virtual Machine.
	...null session in redirect	Not seen in normal operation.
	CLAIMED by	A token has been claimed by an authentication module.
	CONNECT ...	Normal indication of session connection.
NOTICE	Control established on ...	Normal notification that a program has been granted control over a session.
	DESTROY ... lifetime= ...	Normal cleanup of disconnected session.
	DISCONNECT ...	Normal notification of disconnection.
	Invalid call back attempt: ...	Bad call back attempt from a utsessiond.
	Loaded module	Notification of authentication module loading.
	SESSION_OK	Normal startup of a new session or verification of an existing session.
	SessionManager.getSessionManager: Initiate callback to utsessiond at ...	Normal.
	SessionManager.initiateCallback... established communication	Normal.
	TERMINATE ...	Normal notification of session termination.

TABLE F-1 Possible Errors (Continued)

Error class	Message	Description
	TERMINATE: empty session cleanup is disabled	The <code>auth.props:terminateEnable</code> feature is not fully functional in this release and is not enabled by default. This message indicates that <code>utsessiond</code> notified <code>utauthd</code> that a session has no members. Future releases may use this information to cleanup empty sessions. It is normal to receive this message when a user exits their X session. <code>Dtlogin</code> normally will restart the session and present a login screen.
	TERMINATE: inactive session	Terminate message received from <code>utsessiond</code> on a session that has already been purged from <code>utauthd</code> .
	TIMEOUT connection dropped ...	An appliance is not responding.
UNEXPECTED	"CallBack: malformed command"	Bad syntax from a user application such as <code>utload</code> or <code>utidle</code> .
	.../ ... read/0:" + ie	Possible program error.
	.../ ... read/1: ... Exception ...	Error encountered while reading messages from appliance.
	.../... protocolError: ...	Various protocol violations are reported with this message. This is also a way for <code>utauthd</code> to force the appliance to reset.
UNEXPECTED	cannot send <code>connInf</code> , disconnecting session	Session was disconnected during connection due to a problem in communicating with the appliance.
	Cannot set socket timeout: ... Exception ...	Program error.
	connect failed: ...	Problem encountered while attempting to connect appliance to a session.
	Error while closing socket: ... Exception ...	Possible program error.
	Error while processing protocolError: ...	An error was encountered while attempting to send a <code>protocolError</code> message to an appliance.
	Exception ... on ... / ...	Error while trying to read input from appliance.

TABLE F-1 Possible Errors (*Continued*)

Error class	Message	Description
	null session in disconnect	Possible program error.
	adminEvent strange event=	Program error.
	attempt to instantiate Callback()	Program error.
	AuthReader: "	Java runtime error or normal IO error due to appliance reboot.
	AuthRecord.connect: ... already connected"	Possible program error.
	AuthRecord.disconnect: Null Client	Possible program error.
	AuthRecord.send: no connection.	Possible program error.
	Callback.attach: cookie NOT consumed	Bad call back attempt from a utsessiond.
	Callback.control: cannot begin: ...	Possible program error while trying to start a thread to handle a program such as utload.
	Callback.print: ...	IO error while trying to send an appliance response back to the controlling application.
	Callback.run init in: ...	IO error.
	Callback: malformed command	Syntax error from program attempting to control a session.
	Callback: malformed session id	Syntax error from program attempting to control a session.
	Cannot accept on socket: ...	Runtime error. Is cbport busy?
UNEXPECTED	Cannot accept on socket: ... Exception ...	Possible program error.
	Cannot connect on port change	Check utsessiond log file.
	Cannot derive BufferedOutputStream: ... Exception ...	Program error.

TABLE F-1 Possible Errors (Continued)

Error class	Message	Description
	Cannot derive BufferedReader: ... Exception ...	Program error.
	cannot get socket InputStream from ... / ...	Error while trying to read input from appliance.
	Cannot open socket: ... Exception ...	Cannot open the socket specified by auth.props:port. Is there another utauthd running? utauthd should only be started by running /etc/ init.d/utsvc.
	cannot pushback	Possible program error.
	Cannot send protocolError to terminal on failed port change	IO problem encountered while trying to reset appliance.
	Cannot set socket timeout: ... Exception ...	Program error.
	Control.annotate: bad key: ...	Annotations are not allowed in the /etc/opt/SUNWut/auth.props file.
	Control.annotate: bad value: ...	Only true or false are allowed as values for this parameter.
	Control.destroy: unable to clear controller: " + e	Session has already disconnected.
	Control.load: extraneous parameters: ...	Syntax error from controlling application.
	Control.load: invalid file param ...	File might not be present and readable in /tftpboot.
	Control.load: invalid flash param	Syntax error from controlling application.
	Control.parse: invalid parameter	Syntax error from controlling application.
	Control.response: out=null"	No controlling application is present to receive appliance response.

TABLE F-1 Possible Errors (Continued)

Error class	Message	Description
UNEXPECTED	Control.run: ar: " + arex	Only one controlling application allowed or session not connected.
	Control.setParam failed: ...	Only one controller allowed or session is not connected.
	Control.setParam null ar	Possible program error.
	Control.setParam null in/out	Possible program error or early exit of controlling command.
	Control: ...	Possible program error or early exit of controlling command.
	Control: input error: ...	Syntax or IO error from controlling application.
	Control: recv	Error while reading input from controlling application.
	Control: unknown command: ...	Syntax error from controlling application.
	Control: unknown command: ...	Syntax error from controlling application.
	createClient:	Program, installation or runtime error.
	desktopExists	Likely program error.
	destroy error: " + e	Error while trying to tell utsessiond to destroy a session.
	during send to:	Loss of connection to appliance.
	Error ...\nwhile instantiating module. instance=	Program, configuration, or installation error.
	exception in async job:	Program error.
	Impossible error in putCanonical	Possible program error.
	JobQueue.run:	Program or installation error.
	JobQueue.submit:	If auth.props:terminateEnable is true then this can occur in normal operation, otherwise it may occur due to a program error.
logicalTokenExists	Likely program error.	

TABLE F-1 Possible Errors (*Continued*)

Error class	Message	Description
	No controller available to handle message:	Normal if controlling application (utload, etc.) exited before results were received.
	rawTokenExists	Likely program error.
UNEXPECTED	Resolve error on	Program or installation error.
	revoke error: ... Exception ...	Error while trying to disconnect an appliance from a session.
	SESSION_ERROR	Possible program error.
	SESSION_ERROR ... exitCode=	It was not possible to start the first program in a session. The exitCode is helpful in determining the exact cause.
	SessionManager.confirmation: ... Exception ...	If auth.props.terminateEnable is true then this can occur in normal operation, otherwise it may occur due to a program error or a problem in utsessiond.
	SessionManager.getSessionManager: ... InterruptedException	Possibly normal message.
	SessionManager.initiateCallback: ... is not configured to talk to this utauthd	The configuration file /etc/opt/SUNWut/auth.permit does allow this utauthd to talk to utsessiond.
	SessionManager.initiateCallback: ... unknown response: ...	Program error.
	SessionManager.initiateCallback: ... was not able to talk to this utauthd	Possible configuration error.
	SessionManager.initiateCallback: during send: ...	Error while communicating to utsessiond.
	SessionManager.permit: ... Exception ...	Error while attempting to connect an appliance to a session.
	SessionManager.permit: line="..."	utsessiond did not allow the appliance to session connection.

TABLE F-1 Possible Errors (Continued)

Error class	Message	Description
	SessionManager.run: ... Exception ...	Error while reading input from utsessiond.
	SessionManager.run: No job to match with "... " ... Exception ...	Program error.
	SessionManager.run: readLine returns null	Error while reading input from utsessiond.
	SessionManager.session Factory: ... Exception ...	Possible program error.
UNEXPECTED	SessionManager.session Factory: Cannot send create: ... Exception ...	Communication problem with utsessiond.
	SessionManager.session Factory: Empty file: ...	Possible program error.
	SessionManager.session Factory: unable to create new session: ...	utsessiond did not create a new session ID as requested.
	SessionManager.session Factory:invalid SID from utsessiond: ...	Program error in utsession.
	SessionManager.termina te: bad argument: "... "	Could not parse message from utsessiond. Possible program error.
	SessionManager.termina te: invalid SessionId	Possible program error.
	socket + "Handleclient, AuthRecord: ... Exception ...	Possible program error.
	Terminal sent "... " as first message after TcpOpen, reports connected	Appliance and utauthd are out of sync. This situation should correct itself.

TABLE F-1 Possible Errors *(Continued)*

Error class	Message	Description
	userExists	Likely program error.
	utauthd: ... Exception ...	Error encountered while listening for appliances.
	Worker: ... Exception ...	Possible program error.

Glossary

- AP** Sun Enterprise Alternate Pathing (AP) 2.0.1 enables Sun Enterprise 10000 server customers who run Solaris 2.5.1 11/97 on their domain(s) to use all of the features of the AP 2.1 release. AP 2.1 runs only on Solaris 2.6 5/98 domains and AP 2.2 runs only on Solaris 7 5/99 domains. AP 2.0.1 also includes integrated fixes for many bugs that were patched in AP 2.1
- bpp** Bits per pixel.
- category 5** The most common type of wiring used in LANs. It is approved for both voice and data (at up to 100Mhz). Also called cat 5.
- CIDR** Common InterDomain Routing (CIDR) is a protocol which allows the assignment of Class C IP addresses in contiguous blocks.
- client-server** A common way to describe network services and the user processes (programs) of those services.
- composite video** Refers to a type of video signal in which all of the information is transmitted on the same wire.
- DDC** This standard defines I²C-based communication protocol with various levels of complexity which operate over the DDC channel for the purpose of controlling the monitor and optional annex devices. Also, see EDID.
- DHCP** Dynamic Host Configuration Protocol. DHCP is a means of distributing IP addresses and initial parameters to the appliances.
- EDID** The EDID data format as a compact method to specify the capabilities of various types of monitors as well as integrated displays. This standard defines data formats to carry configuration information to allow optimum use of displays.
- Ethernet** Physical and link-level communications mechanism defined by the IEEE 802.3 family of standards.
- Ethernet address** The unique hardware address assigned to a computer system or interface board when it is manufactured. See MAC address.

Ethernet switch	A unit that redirects packets from input ports to output ports. Can be a component of the Sun Ray interconnect fabric.
failover	The process of transferring processes from a failed server to a functional server automatically.
fan out	Connections that radiate out from a hub or switch.
FTP	File Transfer Protocol. The name of the Internet protocol and the program used to transfer files between hosts.
hot desking	The ability for a user to remove a smart card, insert it in any other enterprise appliance connected to the same Sun Ray server, and have the user's session "follow" the user, thus allowing the user to have instantaneous access to the user's windowing environment and current applications from multiple appliances
hot key	A pre-defined key that causes something to appear on your screen. A hot key is used to bring up the Settings screen on the Sun Ray enterprise appliance.
hot-pluggable	A property of a hardware component that can be inserted into or removed from a system that is powered on. USB devices connected to Sun Ray appliances are hot-pluggable.
Interconnect fabric	All the cabling, switches, or hubs that connect Sun Ray server's network interface cards to the Sun Ray appliances.
internet	A collection of networks interconnected by a set of routers that enable them to function as a single, large virtual network.
Internet	(Note the capital "I") The largest internet in the world consisting of large national backbone nets (such as MILNET, NSFNET, and CREN) and a myriad of regional and local campus networks all over the world. It is a global collection of networks connecting a wide range of computers using a common protocol to communicate and share services.
intranet	Any network that provides similar services within an organization to those provided by the Internet outside it but which is not necessarily connected to the Internet.
IP address	A unique number that identifies each host or other hardware system on a network. An IP address is composed of four integers separated by periods. Each decimal integer must be in the range 0-255 (for example, 129.144.0.0).
IP address lease	The assignment of an IP address to a computer system for a specified length of time, rather than permanently. IP address leasing is managed by the Dynamic Host Configuration Protocol (DHCP). Sun Ray appliance IP addresses are leased.
LAN	Local area network. A group of computer systems in close proximity that can communicate with one another via some connecting hardware and software.

layer 2	The data link layer. In the OSI (Open Standards Interconnection) model, there are a total of seven layers. Layer 2 is concerned with procedures and protocols for operating the communication lines between networks as well as clients and servers. Layer 2 also has the ability to detect and correct message errors.
local host	The CPU or computer on which a software application is running.
local server	From the client's perspective, the most immediate server in the LAN.
login	The process of gaining access to a computer system.
login name	The name by which the computer system knows the user.
MAC address	Media Access Control. A MAC address is a 48-bit number programmed into each local area network interface card (NIC) at the time of manufacture. LAN packets contain destination and source MAC names and can be used by bridges to filter, process, and forward packets. 8:0:20:9e:51:cf is an example of a MAC address. See also Ethernet address.
mobility	For the purposes of the Sun Ray software, the property of a session that allows it to follow a user from one appliance to another within a work group. On the Sun Ray system, mobility requires the use of a smart card or other identifying mechanism.
modules	Authentication modules are used to implement various site-selectable authentication policies.
multiplexing	The process of transmitting multiple channels across one communications circuit.
namespace	A set of names in which a specified ID must be unique.
network	Technically, the hardware connecting various computer systems enabling them to communicate. Informally, the systems so connected.
network address	The IP address used to specify a network.
network interface	An access point to a computer system on a network. Each interface is associated with a physical device. However, a physical device can have multiple network interfaces.
network interface card	NIC. The hardware that links a workstation or server to a network device.
network latency	The time delay associated with moving information through a network. Interactive applications such as voice, video displays and multimedia applications are sensitive to these delays.
network mask	A number used by software to separate the local subnet address from the rest of a given Internet protocol address. An example of a network mask for a class C network is 255.255.255.0.

network protocol

- stack** A network suite of protocols, organized in a hierarchy of layers called a stack. TCP/IP is an example of a Sun Ray protocol stack.
- OSD** On-screen display. The Sun Ray appliance uses small OSD icons to alert the user of potential start-up problems.
- patch** A collection of files and directories that replace or update existing files and directories that prevent proper execution of the software on a computer system. The patch software is derived from a specified package format and can only be installed if the package it fixes is already present.
- policies** Authentication Manager, using the selected authentication modules, decides what tokens are valid and which users have access.
- port** (1) A location for passing data in and out of a computer system. (2) The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host.
- root user** A user name that grants special privileges to the person who logs in with that ID.
- server** A computer system that supplies computing services or resources to one or more clients.
- service** For the purposes of the Sun Ray software, any application that can directly connect to the Sun Ray appliance. It can include audio, video, X servers, access to other machines, and device control of the appliance.
- session** A group of services associated with a single user.
- subnet** A working scheme that divides a single logical network into smaller physical networks to simplify routing.
- token** In the Sun Ray system, a token must be presented by the user. It is required by the Authentication Manager to consider allowing a user to access the system. It consists of a type and an ID. If the user inserted a smart card, the smart card's type and ID are used as the token. If the user is not using a smart card, the enterprise appliance's built-in type (pseudo) and ID (the unit's Ethernet address) are supplied as the token.
- thin client** Thin clients remotely access some resources of a computer server, such as compute power and large memory capacity. The Sun Ray appliances rely on the server for all computing power and storage.
- time-out value** The maximum allowed time interval between communications from an appliance to the Authentication Manager.
- TCP/IP** Transmission Control Protocol/Internet Protocol (TCP/IP) is a networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and operating systems.

- URL** Uniform Resource Locator. A standard for writing a textual reference to an arbitrary piece of data in the World Wide Web (WWW). The syntax of a URL is `protocol://host/localinfo` where `protocol` specifies a protocol to use to fetch the object (like HTTP or FTP), `host` specifies the Internet name of the host on which to find it, and `localinfo` is a string (often a file name) passed to the protocol handler on the remote host.
- user name** The name a computer system uses to identify a particular user. Under UNIX this is a text string of up to eight characters composed of letters (a-z and A-Z), digits (0-9), hyphens (-), and underscores (_) (for example, jpmorgan). The first character must be a letter.
- virtual frame buffer** A region of memory on the Sun Ray server that contains the current state of a user's display.
- work group** A collection of associated users who exist in near proximity to one another. A set of Sun Ray appliances that are connected to a Sun Ray server provides computing services to a work group.

Index

SYMBOLS

\$AUDIODEV, 195
/dev/audio, 195
@(CGI_USER), 43, 182
@(HOSTNAME), 41
@(ROOTENTRY), 41
@(ROOTNAME), 41
@(UTPASSWD), 42
@(WEBSERVER_NAME), 42, 182
@(WEBSERVER_PORT), 42

NUMERICS

10 BASE-T, 33
10/100BaseT, 14
 built-in interface, 14
100 BASE-T, 16
100BaseT
 cable receptacle, 9
 link speed, 16
10BaseT
 bandwidth limitations, 33
24-bit, 6, 24
2-D, 6
8-bit, 24
 determining status, 25
8-bit color, 198

A

access1.sun.com, 33
active sessions
 memory requirements, 32
administration
 desktops, 97
administration application, 87, 219
 browser, 92
 command-line interface, 91
 login screen, 91
 web-based graphical interface, 91
administration database, 157
administrator's guide
 accessing online, 131
admintool
 non-English locales, 221
Adobe FrameMaker
 RAM requirements, 32
Adobe PhotoShop
 RAM requirements, 32
Alternate Pathing (AP), 59
API (application programming interface)
 modifying
 changing, 24
 rendering, 17
appliance
 authentication, 224
 default system configuration, 57
 power cycle, 62
 revealing information about, 110
 state, 88
 token readers, 89, 127

- applications
 - recording sound, 13
 - using `/dev/audio`, 12, 13
 - using AutoCAD, 203
- audio
 - audio volume down key, 11
 - audio volume up key, 11
 - input, 7
 - line-out, 13
 - mixing, 12
 - monaural signal, 8
 - multichannel, 7
 - mute audio key, 11
 - recording, 13
 - redirecting device emulator, 13
 - rerouting the audio signal, 13
 - sample rates, 10
 - SunMicrophone II, 37
- `auth.permit`, 232
- `auth.props`, 226, 228, 230, 231
- authentication
 - enabling a policy, 71
 - example policies, 71
 - policy, 63, 88
- authentication manager, 22, 70, 88, 107
 - communicating with desktops, 108
 - error messages, 223
 - message format, 223
 - obtaining desktop properties, 111
 - restarting considerations, 72
- authentication policy
 - self-register, 70
 - self-registration, 88
 - zero admin, 70
- AutoCAD
 - visual settings, 203

B

- bandwidth
 - environment considerations, 34
 - full bisectional, 35
 - hubs, 35
- batch edit
 - listing desktops, 109
- batch operations, 95

- blending, 24
- buffer
 - frame, 7
 - switch, 35
 - unbuffered switches, 35
 - virtual frame, 7
- buffering, 35

C

- cables
 - requirements, 34
- calendar, 32
 - response time, 32
- callback address, 24
- camcorders
 - video capabilities, 10
- camera, 37
 - using the SunCamera II, 37
- cards
 - specifications for smart cards, 37
- category 3 wire, 33
 - using 10BASE-T equipment, 14
- category 5 wire, 14, 33
 - for use with 10BaseT, 33
- CGI username, 182
- Citrix
 - using third-party applications, 5
- command
 - `utdesktop`, 113
 - `utuser`, 143
- command-line interface, 135, 146
- composite video, 37
- compositing, 24
- computing nodes, 34
- configuration
 - by hand, 40
 - key parameters, 40
 - modify interconnect fabric, 34
 - prompted values, 44
- configuration files
 - `dtlogin`, 209
- configuration worksheet, 40, 182
- configuring SSL
 - `crca` script, 52

- on failover server, 54
- on primary Sun Ray server, 51
- removal, 55
- required information, 51
- sslgencred script, 53
- troubleshooting, 55

congestion

- preventing, 34

crca script, 52

cursor

- green newt, 205

D

daemon

- dtlogin, 206
- session manager, 81
- SunDS, 180

database, 19

- administration, 88, 103
- default directory, 31
- disk space requirements, 31
- token associated with, 138

DDC (Display Data Channel), 24

DDC data

- making use of, 37

debug

- error message, 224

default visual type, 24

desktop

- ID, 105, 106
- location, 154
- managing, 97
- properties, 76
- searching for location, 105

device drivers

- virtual, 17, 24

device emulation, 13

- script, 13

device files

- interface, 58

device nodes, 13

devices

- video input, 37

DGA

- support, 203

DHCP

- compatibility with other products, 58
- dhtadm command, 85
- leasing, 7
- parameters for logging, 83
- service, 58
- setting version variable, 68
- table, 85
- unsetting version variable, 67

dhtadm command, 83

Direct Graphics Access

- support, 203

disk space

- requirements, 31

display information, 7

display rates

- typical, 36

distinguished name, 50

- attributes, 50
- example, 50

distribution

- server software, 18

documentation

- accessing online, 131

dtlogin

- configuration files
 - checking integrity, 210
 - replacing, 211

dtlogin, 77, 88

- configuration files, 209
- patches, 206
- screen, 58
- unconfiguring, 208

duplex

- using full duplex, 34
- using half-duplex switches, 35

dynamic library, 13

E

email, 32

Enterprise 10000

- considerations, 59

Enterprise 2, 15

enterprise appliance, 6

- problems, 7

- replacement, 7
- environment variable
 - \$AUDIODEV, 13
 - LD_PRELOAD, 13
- error message
 - application uses 8-bit graphics, 25
 - message classes, 224
- Ethernet, 16
 - address, 7
 - compatible cards, 33
 - dedicated card, 33
 - gigabit, 14
 - gigabit Ethernet card, 17, 33
 - installing controller card, 58
 - lance Ethernet card, 33
 - QEC/MACE Ethernet card, 33
 - quad FastEthernet card, 33
 - required interface, 29
 - Sun FastEthernet card, 33
 - technology, 14

F

- failover
 - configuring interconnect fabric, 58, 66
- failover server
 - configuring SSL, 54
- fiber optic
 - extending cable length, 35
- files affected by installation, 201
- firmware, 57, 58
 - changing version, 57
 - forcing an update/upgrade, 68
 - management, 67
 - module, 7
 - prevent user from downloading, 69
 - updating, 7
 - version information, 110
- frame buffer, 7
 - virtual, 7
- full duplex
 - network considerations, 34
 - switching considerations, 35

G

- gem0, 33
- gem1, 17
- graphics
 - accelerated, 6
- green newt cursor, 205
- guidelines
 - network, 34

H

- half-duplex
 - hubs, 35
 - switches, 35
- Hangul key, 222
- hardware
 - requirements, 29
- headphone
 - connectors, 7
 - output, 7, 8
 - sensing presence, 10
- Henkan key, 222
- hme2, 33
- hostname
 - value, 41
- hosts
 - interface configuration, 58
- hot desking
 - mobility, 21
- Hot Java browser, 91
- hot key, 79
 - values, 80
- hot-pluggable support, 7
- http
 - //access1.sun.com
 - web site for patches, 33
- HTTP proxy server, 92
- hubs, 14, 15, 34
 - 100BaseT, 14
 - appliance considerations, 35
 - half-duplex, 35
 - specifications, 35
 - verified components list, 36
 - with more than 12 ports, 35

I

- icons, 189
- indexed color, 24
- installation
 - testing, 47
- interactive applications
 - test results, 32
- interconnect fabric, 5
 - composition, 34
 - configure, 58
 - description, 14
 - managing, 65
 - scenarios, 14
 - traffic tests, 32
- interface
 - command-line, 135, 146
 - entries, 181
 - hme2, 33
 - le1, 33
 - qe0, 33
- internet
 - connecting to LAN, 15
- intranet
 - connecting to LAN, 15
- IP address, 7
 - leasing, 7

J

- jar file
 - smart card usage, 168
- Java
 - rendering, 24
 - runtime error, 229
 - supported version, 28
 - VM error message, 227
- JDK
 - disk space requirements, 31

K

- keyboard
 - hardware requirements, 29
 - specifications
 - non-Sun keyboards, 37

- type 6, 37
 - using non-Sun keyboards, 79
- kiosk mounting, 195

L

- LAN
 - example interconnect system, 5
- language selection, 219
- latency
 - minimizing, 34
- LDAP
 - administration, 89
 - client libraries
 - disk space requirements, 31
 - clients, 89
 - data design
 - administration, 40, 41
 - data store, 89
 - interface, 89
- le0, 33
- le1, 33
- line-in
 - sensing presence, 10
- line-out
 - speaker connector, 8
- link speed, 16
- locale, 219
- log files, 31, 83
 - utssessiond, 229
- log management, 58
- login status, 154
 - currently logged in, 154
 - logged off, 154
 - never logged in, 154
- login status fields, 154, 166
- loopback, 84
- low impedance
 - headphones, 8
- low-level input
 - keyboard, 7

M

- MAC address, 68, 69

- man page
 - audio(7i), 13
 - fwadm(1m), 68
 - xset, 12
- management
 - authentication, 22
 - device, 17
 - network, 34
 - session, 17, 22
 - user, 135
- managing
 - desktops, 95
 - users, 95
- memory needed, 32
- messages
 - informative, 48
- metanetwork
 - Alternate Pathing (AP), 59
- mice, 6, 29
 - using USB type, 37
- microkernel, 87
- microphone, 37
 - adjusting volume, 7
 - input, 7, 8
 - non-powered, 7
 - self-powered, 7
 - sensing presence, 10
 - using SunMicrophone II, 37
 - volume adjustment, 8
- Microsoft Windows NT
 - using applications, 5
- mobility
 - hot desking, 21
 - sessions, 21
- module
 - authentication, 226
 - firmware, 7
- monaural
 - signal, 8
- monitor
 - hardware requirements, 29
 - multi-sync, 36
 - specifications, 36
 - using DDC data, 37
- monitor resolution, 195
- monitoring tools, 83
- mouse, 7, 29
 - Crossbow USB, 37
- multimedia PC
 - functionality comparison, 6
- multiplexing
 - network considerations
 - safe ratios, 34
- mute
 - audio, 11
 - muting audio through keyboard, 11

N

- netmasks
 - files, 66
- Netscape
 - Communicator, 32
 - RAM requirements, 32
- netstat command, 83
- network
 - connector, 9
 - considerations, 34
 - management, 34
- network interface card (NIC), 15
 - configure, 58
 - gem0, 17
- nodes, 34
- non-blocking
 - switches, 35
- non-negotiating
 - switches, 35
- NTSC
 - compatible standards, 10, 37

O

- object class, 41
- on screen display, 189
- On-Screen Display (OSD), 7
- OpenGL
 - considerations, 25
- OpenWindows
 - user considerations, 178
- OSD, 189
- output, 7

overlays, 24

P

packages

SUNWqfed, 33

PAL

compatible standards, 10, 37

password

administration (worksheet), 42

changing, 99

patches

acquiring latest

URL, 33

dtlogin, 206

software requirements, 27

SUNWqfed package, 33

performance issues

applications being used, 32

connecting other devices, 14

memory, 32

peripherals

hot-pluggable, 6

keyboards, 6

USB, 9

permission

denied on web server, 48

PhotoShop, 32

pixels, 24

platforms

4u, 30

policies

example authentication, 71

port

autonegotiate, 35

session manager, 24

power

LED, 8

receptacle, 9

power amps, 13

power cycle, 196

power-on self test (POST), 7

printer

adding, 76

properties fields

user, 153

protocol

authentication, 17

native, 24

proxy server, 48, 92

pseudo terminals, 203

pseudo user

smart cards, 70

pt_cnt, 203

pty, 203

publications

accessing online, 131

Q

quad FastEthernet

interface, 14

recommended cards, 33

R

ratio

enterprise appliances to servers, 5

reader

token, 73, 160, 163

removing

SSL configuration, 55

rendering

fonts, 24

replacement

enterprise appliance, 7

reset, 196

response time

applications

number of sessions, 32

RJ-45

connector, 9

root

certificate authority, 50

entry, 41

router, 34

S

safe ratio

- statistical multiplexing, 34
- sample rates, 10
- script
 - configuration, 39, 43
 - locating errors, 45, 183, 185
 - unconfig, 179
 - unconfiguring Sun WebServer, 181
 - uninstall, 179
- search
 - user name, 148
- security
 - @(UTPASSWD) value, 42
 - standard root issue, 43
 - unauthorized access, 22
- self-registration GUI, 220
- server, 19
 - booting, 58
 - extending length to switch, 35
 - hardware requirements, 30
 - hardware systems, 30
 - name, 136
 - port, 136
 - processors required, 32
- server software
 - distribution, 18
- session ID, 22
 - revealing, 224
- session manager, 22, 81
 - changing default settings, 81
 - settings screen, 78
- sessions
 - active, 32
 - active session memory requirements, 32
 - appliance connections per interface, 57
 - mapping, 82
 - roving smart cards, 88
 - user, 58
- settings GUI, 221
- settings screen, 18
 - adjusting volume, 7
 - command line options, 78
 - default key sequence, 58
 - hot key, 77
 - launching another instance, 77
 - moving to another appliance, 78
 - number of instances allowed, 78
 - remaining hidden, 77
 - resolution/refresh rate exception, 78
 - sitewide default setting, 79
 - sitewide mandatory setting, 79
 - user default setting, 79
 - using PC-style keyboards, 79
- smart card
 - ID, 89, 127
 - LED, 8
 - ordering additional, 133
 - protocol, 58
 - questions, 70
 - reader, 7, 8, 73
 - registering, 73
 - specifications, 37
 - users, 70, 88
- snoop command, 83
- software
 - requirements, 27
- Solaris
 - network interface, 66
- Solaris 2.6, 6, 27, 30
- Solaris 7, 6, 27, 30
- speaker
 - internal, 12
 - location, 8
 - using powered (external), 13
- SSL certificate, 49
- sslgencred script, 53
- sslstore script, 53
- stereo
 - mini-plug, 9
- strict cut-through
 - switches, 35
- subnet
 - upgrading, 67
 - using private numbers, 66
- Sun Directory Services
 - disk space requirements, 31
- Sun props key, 79
- Sun Ray server
 - configuring SSL, 51
- Sun WebServer, 180, 181
 - configure, 39
 - disk space requirements, 31
 - instance name, 182
- SunCamera II

- specifications, 37
- SunDS
 - configure, 39
 - LDAP server, 40
- SUNWgfred, 33
- superuser
 - configuration script, 43
- supporting users, 14
- swap space, 202
 - active sessions, 32
 - Sun Directory Services, 31
- switches, 16, 17, 19, 34
 - compatible, 34
 - extending length to server, 35
 - non-blocking, 35
 - non-negotiating, 35
 - ports, 35
 - selecting, 35
 - specifications, 34
 - strict cut-through, 35
 - using full bandwidth, 35
 - using unmanaged (level 2), 14
- system administrator
 - duties, 6

T

- terminal window, 203
- text editing, 32
- tftpbboot, 230
- thin client, 6
- time-out value, 199
- timestamp, 223
- token, 22
 - claimed by authentication module, 227
 - configuring as a reader, 73
 - deleting, 141
 - disabled, 88
 - disconnected, 22
 - enabled, 88
 - ID, 106, 138, 139, 155
 - ID field, 144
 - matching IDs, 158
 - reader, 137, 160, 163
 - readers, 89, 127
 - removing, 161

- tools
 - system administration, 17
- traffic
 - average, 32
 - monitoring, 84
- troubleshooting
 - SSL configuration, 55
- Type 6
 - keyboard, 37

U

- Ultra 2
 - server, 15
- unauthorized access
 - revealing session ID, 22
- unbuffered
 - switches, 35
- unconfiguration
 - process, 181
- uninstall, 179
- UNIX
 - nobody user, 43
 - user account, 88
 - username, 43
- uplink
 - gigabit, 17
- URL
 - administration application, 91
 - administration application default port, 42
 - compatible switches, 35
 - patches, 33
- USB, 6
 - keyboards, 10
 - mice, 10
 - ports, 7
 - ports 1 and 2, 9
 - ports 3 and 4, 9
- user
 - listing, 149
 - property fields, 153
 - session types, 205
- user account
 - isolated (security), 43
- user statistics, 88
- utauthd, 228

- utload, 224, 229
- utpolicy, 75
 - enabling a policy, 71
- utsessiond
 - threads, 224

V

- VCR
 - video capabilities, 10
- VGA
 - monitor output, 9
- video
 - bandwidth issues (10BaseT), 33
 - compatible cameras, 10
 - compatible standards, 10
 - composite, 7, 9
 - conferencing, 10
 - current support for video input, 37
 - display rates, 36
 - editing, 10
 - input, 9
 - monitor output (15-pin SVGA), 9
 - output, 9
 - video input devices
 - specifications, 37
- video disc players
 - video capabilities, 10
- virtual device drivers, 17
- visual type
 - default, 24
- volume
 - adjusting, 10
 - application levels, 12
 - control, 12
 - master, 12

W

- web pages
 - overtaxing bandwidth, 33
- web server
 - default port, 42
 - instance, 182
 - public port designation, 42
- web site

- compatible switches, 34
- specifications for smart cards, 37
- web-based administration application, 43
- Win32
 - interface, 24
- WinFrame
 - using third-party applications, 5
- workgroup
 - scenarios, 14
- worksheet, 40, 182
 - configuration, 40

X

- X server, 22, 24, 82
- X Window, 205
- X11, 24
- X11 bell, 12
- xhost +, 22
- xprop(1), 22