



Sun Ray™ Server Software 4.1 Administrator's Guide

for the Linux Operating System

Beta Draft

Sun Microsystems, Inc.
www.sun.com

Part No 820-3769-05
July 2008 Revision A

Copyright 2002—2008, Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

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

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this 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.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Sun Ray, Sun WebServer, Sun Enterprise, Ultra, UltraSPARC, SunFastEthernet, Sun Quad FastEthernet, HotJava, Java, JDK, JavaServer Pages, 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 is a trademark or registered trademark of Netscape Communications Corporation.

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.

Federal Acquisitions: Commercial Software—Government Users Subject to Standard License Terms and Conditions.

Use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth in the Sun Microsystems, Inc. license agreements and as provided in DFARS 227.7202-1(a) and 227.7202-3(a) (1995), DFARS 252.227-7013(c)(1)(ii) (Oct. 1998), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable.

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 2002—2008, Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

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

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 des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le Sun logo, Sun Ray, Sun WebServer, Sun Enterprise, Ultra, UltraSPARC, SunFastEthernet, Sun Quad FastEthernet, HotJava, Java, JDK, JavaServer Pages, 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 est une marque de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays.

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 licenciées de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

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

Contents

Preface	xxi
1. Sun Ray System Overview	1
Computing Model	1
The Sun Ray System	2
Sun Ray DTU	3
Multihead Displays	3
Firmware Module	4
Sun Ray Server Software	4
Authentication Manager	5
Sessions and Services	7
Session Manager	7
Xserver	8
Multimedia Support	8
CLI and Admin GUI	9
Data Store	9
Kiosk (Controlled Access) Mode	9
Network Components	10
Physical Connections	10
Deployment Examples	11

Small Deployments	11
Medium to Large Deployments	11
Failover Group Scenario	12
Regional Hotdesking	13
Security Considerations	13
2. Command-Line Interface	15
Supported Commands	15
▼ To Stop Sun Ray Services	20
▼ To Start Sun Ray Services	20
Session Redirection	20
▼ To Redirect to a Different Server	20
▼ To Redirect a DTU Manually	21
▼ To List Available Hosts	22
▼ To Select a Server with the Latest Session	22
Managing User Data in the Sun Ray Data Store	22
Changing Authentication Policies	23
Enabling Multiple Administration Accounts	23
PAM Entries	24
▼ To Configure UNIX Users	24
▼ To Revert to the Old admin User	24
Administration GUI Audit Trail	25
Enabling and Disabling Device Services	26
▼ To Determine the Current State of Device Services	26
▼ To Enable USB Service	27
▼ To Disable USB Service	27
▼ To Perform a Cold Restart	27
Configuring Interfaces on the Sun Ray Interconnect Fabric	27
▼ To Configure a Private Sun Ray Network	28

- ▼ To Configure a Second Private Sun Ray Network 28
- ▼ To Delete an Interface 28
- ▼ To Print the Sun Ray Private Interconnect Configuration 29
- ▼ To Add a LAN Subnet 29
- ▼ To Delete a LAN Subnet 29
- ▼ To List the Current Network Configuration 29
- ▼ To Remove All Interfaces and Subnets 30

Managing Firmware Versions 30

- ▼ To Update All the DTUs on an Interface 30
- ▼ To Update a DTU Using the Ethernet (MAC) Address 31

Restarting the Sun Ray Data Store (SRDS) 31

- ▼ To Restart Sun Ray Data Store 31

Smart Card Configuration Files 32

- ▼ To Load a Configuration File Into the Directory 32

Configuring and Using Token Readers 32

Token Reader Icon 34

- ▼ To Configure a Token Reader 34
- ▼ To Get a Token ID From a Token Reader 35

Using the utcapture Tool 35

- ▼ To Start utcapture 37

Examining Log Files 38

3. Administration Tool 39

Login Page 40

Servers Tab 42

Sessions Tab 43

Desktop Units Tab 44

- ▼ To Display Properties for a DTU 44
- ▼ To Edit a DTU's Properties 45

Multihead Groups	45
Token Readers	45
▼ To Set Up a Token Reader	45
▼ To Locate a Token Reader	46
▼ To Get Information on a Token Reader	46
Tokens Tab	47
▼ To Register a Token	48
▼ To Register a Pseudo-Token	49
▼ To Enable, Disable, or Delete a Token	50
Advanced Tab	51
Security Settings	52
System Policy	52
Kiosk Mode Configuration	54
Smart Card Probe Order	55
Data Store Password	56
Log Files Tab	57
4. Peripherals for Sun Ray DTUs	59
Device Nodes and USB Peripherals	59
Device Nodes	60
Device Links	61
Device Node Ownership	61
Hotdesking and Device Node Ownership	61
Mass Storage Devices	62
Device Nodes and Links	62
Mount Points	62
Device Ownership and Hotdesking	63
Common Disk Operations	63
Attached Printers	64

Printer Setup	64
▼ To Set Up a Printer	64
Non-PostScript Printers	66
libusb	66
5. Hotdesking (Mobile Sessions)	67
Regional Hotdesking	67
Functional Overview	68
Site Requirements	68
Providing Site Integration Logic	69
▼ To Configure a Site-specific Mapping Library	69
Token Readers with Regional Hotdesking	70
▼ To Configure the Sample Data Store	70
▼ To Disable Regional Hotdesking	71
Remote Hotdesk Authentication (RHA)	71
▼ To Disable or Re-enable RHA Using the Admin GUI	72
▼ To Disable RHA from a Command Line	72
▼ To Re-enable RHA from a Command Line	72
6. Encryption and Authentication	73
Introduction	73
Security Configuration	74
Security Mode	74
Session Security	75
Security Status	76
7. Deployment on Shared Networks	77
Sun Ray DTU Initialization Requirements	78
DHCP Basics	78
DHCP Parameter Discovery	79

DHCP Relay Agent	80
Network Topology Options	80
Directly-Connected Dedicated Interconnect	82
Directly-Connected Shared Subnet	82
Remote Shared Subnet	82
Network Configuration Tasks	83
Preparing for Deployment	83
Deployment on a Directly-Connected Dedicated Interconnect	84
Directly-Connected Dedicated Interconnect: Example	85
Deployment on a Directly-Connected Shared Subnet	87
Directly-Connected Shared Subnet: Example 1	88
Directly-Connected Shared Subnet: Example 2	90
Deployment on a Remote Subnet	92
Remote Shared Subnet: Example 1	93
Remote Shared Subnet: Example 2	96
Network Performance Requirements	99
Packet Loss	100
Latency	100
Out-of-Order Packets	100
Encapsulated Options	101
Troubleshooting Tools	102
utcapture	102
utquery	102
OSD Icons	102
Remote Configuration	103
Firmware	104
Generic DHCP Parameters	105
.parms Lookup	106

Routerless VPN Capability	107
Pop-up GUI	108
Access Control	108
Features and Usage	108
Remote Loading of Configuration Data	114
Ports and Protocols	116
8. Gnome Display Manager	119
Installation	119
Uninstallation	120
Configuration	120
Gnome Display Manager Privileges	120
Bundled Greeter	121
9. Multihead Administration	123
Multihead Groups	124
Multihead Screen Configuration	124
Multihead Screen Display	125
Multihead Administration Tool	126
▼ To Enable Multihead Policy From the Command Line	126
▼ To Enable Multihead Policy Using the Admin GUI	126
▼ To Create a New Multihead Group	128
XINERAMA	130
Session Groups	131
Authentication Manager	131
10. Kiosk Mode	135
Enabling Kiosk Mode	135
Enabling Kiosk Mode Using the CLI	136
▼ To Enable Kiosk Mode for All Users (Card and Non-card)	136

- ▼ To Enable Kiosk Mode for Card Users Only 136
- ▼ To Enable Kiosk Mode for Non-card Users Only 137
- ▼ To Enable Both Card and Non-Card Sessions 137
- ▼ To Allow Only Card Sessions in Kiosk Mode 137
- ▼ To Enable Regular Sessions for Registered Cards and Kiosk Sessions for Non-Card Users 137
- ▼ To Enable Kiosk Sessions for Registered Cards and Regular Sessions on Registered DTUs 137

Enabling Kiosk Mode Using the Admin GUI 138

- ▼ To Enable Kiosk Mode Using the Admin GUI 138

Overriding Kiosk Mode Policy 140

- ▼ To Override Kiosk Mode Policy Using the CLI 140
- ▼ To Override Kiosk Mode Policy Using the Admin GUI 141

Building the Kiosk Mode Environment 142

- ▼ To Configure Kiosk Mode Settings 143
- ▼ To Add an Application 144

Security and Failover Considerations 146

11. Failover Groups 147

Overview 147

Setting Up IP Addressing 150

Setting Up Server and Client Addresses 150

Server Addresses 151

Configuring DHCP 152

Coexistence of the Sun Ray Server With Other DHCP Servers 152

Administering Other Clients 153

- ▼ To Set Up IP Addressing on Multiple Servers, Each with One Sun Ray Interface 153

Group Manager 155

Redirection 156

Group Manager Configuration	156
▼ To Restart the Authentication Manager	157
Load Balancing	157
▼ To Turn Off the Load Balancing Feature	158
Setting Up a Failover Group	158
Primary Server	158
▼ To Specify a Primary Server	159
▼ To Specify a Dedicated Primary Server	159
Secondary Server	159
▼ To Specify Each Secondary Server	160
▼ To Add Additional Secondary Servers	160
Removing Replication Configuration	160
▼ To Remove the Replication Configuration	160
Viewing Administration Status	161
▼ To Show Current SRDS Replication Configuration	161
▼ To View Network (Failover Group) Status	161
Recovery Issues and Procedures	162
Primary Server Recovery	163
▼ To Rebuild the Primary Server's Administration Data Store	163
▼ To Replace the Primary Server with a Secondary Server	164
Secondary Server Recovery	165
Setting Up a Group Signature	165
▼ To Change the Group Manager Signature File	165
Taking Servers Offline	166
▼ To Take a Server Offline	166
▼ To Bring a Server Online	166
A. User Settings	167
Supported Devices and Libraries	167

Supported Mass Storage Devices	167
Sun Ray DTU Settings	168
▼ To Change the Sun Ray Settings	168
Monitor Settings	169
Non-Sun Keyboard Settings	170
Hot Key Preferences	170
Hot Key Values	172
▼ To Change the Hot Key for the Settings GUI	172
▼ To Change the Hot Key Setting for a Single User	172
Power Cycling a Sun Ray DTU	173
▼ To Power Cycle a Sun Ray DTU	173
▼ To Perform a Soft Reset	173
▼ To Kill a User's Session	173
B. Troubleshooting and Tuning Tips	175
Understanding OSD	175
OSD Icon Topography	175
Sun Ray Desktop Unit Startup	180
▼ If this icon stays on for more than 10 seconds	180
▼ If this icon stays on for more than 10 seconds	181
▼ Actions to Take	182
▼ If the icon displays for more than a few seconds or if the DTU continues to reset after the icon is displayed	182
▼ To Identify a Hung Session	184
▼ To Kill a Hung Session	184
▼ Actions to Take	184
▼ Actions to Take	185
Session Connection Failures	187
▼ Actions to Take	188

Firmware Download Diagnostics	189
Firmware Download OSD	190
▼ Actions to Take	190
▼ Actions to Take	191
Token Reader Icons	192
▼ Actions to Take	193
Authentication Manager Errors	195
Troubleshooting USB Mass Storage Devices	197
Device Nodes Are Not Created	198
Device Is Not Automatically Mounted	198
Device Is Not Automatically Unmounted	198
Audio	198
Audio Device Emulation	199
Audio Malfunction	199
▼ To Activate the Redirection Library	199
Performance Tuning	200
Applications	200
Sluggish Performance	200
JDS Tuning	201
Screensaver Resource Consumption	201
▼ To Disable Screensaver Hacks on Linux Systems	201
Network Switches	201
Multihead Displays	202
Monitor Display Resolution Defaults to 640 x 480	202
▼ To Correct or Reset the Screen Resolution	203
Old Icons (Hourglass with Dashes Underneath) Appear on Display	203
Port Currently Owned by Another Application	203
Design Tips	204

Glossary 205

Index 219

Figures

FIGURE 1-1	Authentication and Session Manager Interaction	5
FIGURE 1-2	Typical Medium to Large Deployment Scenario	12
FIGURE 1-3	Simple Failover Group	13
FIGURE 2-1	The Server Selection (<code>utselect</code>) GUI	21
FIGURE 2-2	Using a Token Reader to Register Smart Cards	33
FIGURE 2-3	Token Reader (Card Reader) Icon	34
FIGURE 3-1	Admin GUI Navigation Hierarchy	39
FIGURE 3-2	User Name Challenge Screen	41
FIGURE 3-3	Top-level Servers Tab	42
FIGURE 3-4	Sessions Tab Displays Active and Idle Sessions	43
FIGURE 3-5	Desktop Units Tab	44
FIGURE 3-6	Setting Up a Token Reader	46
FIGURE 3-7	Tokens Tab	47
FIGURE 3-8	Edit Token Properties	48
FIGURE 3-9	Add New Token Page	49
FIGURE 3-10	Pseudo-token Properties	50
FIGURE 3-11	The Security Tab	51
FIGURE 3-12	System Policy Tab	53
FIGURE 3-13	Kiosk Mode Tab	54
FIGURE 3-14	Edit Smart Card Probe Order	55

FIGURE 3-15	Use the Data Store Password Tab to Change the Admin Password	56
FIGURE 3-16	Sample Administration Log	57
FIGURE 6-1	Sun Ray Security Configuration Tab	75
FIGURE 7-1	Network Topologies for Sun Ray DTU Deployment	81
FIGURE 7-2	Sun Ray Network Topology	84
FIGURE 7-3	Pop-up GUI Main Menu (Part I)	110
FIGURE 7-4	Pop-up GUI Main Menu (Part II)	110
FIGURE 7-5	Setup TCP/IP Menu	111
FIGURE 7-6	Enable VPN Configuration Policy Toggle	111
FIGURE 7-7	Advanced Menu (Part I)	113
FIGURE 7-8	Advanced Menu (Part II)	114
FIGURE 7-9	Sample VPN Configuration File	116
FIGURE 9-1	The Multihead Screen Display	126
FIGURE 9-2	Multihead Feature Enabled	127
FIGURE 9-3	<code>utmhconfig</code> GUI Lists Multihead Groups and Details	128
FIGURE 9-4	Create New Multiheaded Group Pop-up Dialog Box	129
FIGURE 9-5	Setup Display for the New Multihead Group	129
FIGURE 9-6	Completed Multihead Group List With Active Finish Button	130
FIGURE 9-7	Authentication Manager Flowchart for the Primary DTU	132
FIGURE 9-8	Authentication Manager Flowchart for the Secondary DTU	133
FIGURE 10-1	Kiosk Mode Enabled for Non-Card Users	139
FIGURE 10-2	Edit Token Properties	142
FIGURE 10-3	Edit Kiosk Mode	143
FIGURE 11-1	Simple Failover Group	148
FIGURE 11-2	Redundant Failover Group	149
FIGURE 11-3	Network Status Screen	162
FIGURE A-1	Settings Screen	168
FIGURE B-1	Layout of Old (left) and New (right) OSD Icons	176
FIGURE B-2	DTU Startup OSD	180
FIGURE B-3	Network Connection Verified	181

FIGURE B-4	Waiting to Connect to Authentication Manager	182
FIGURE B-5	Redirection OSD	183
FIGURE B-6	Wait for Session OSD	183
FIGURE B-7	Bus Busy	184
FIGURE B-8	No Ethernet Signal	185
FIGURE B-9	Ethernet Address	186
FIGURE B-10	Ethernet Address OSD with Different Encryption and Authentication States	187
FIGURE B-11	Session Refused by DTU	187
FIGURE B-12	DHCP Broadcast Failure	188
FIGURE B-13	Establishing a VPN Connection	189
FIGURE B-14	VPN Connection Established	189
FIGURE B-15	OSD Icon 4 Displays Firmware Download Error Messages	190
FIGURE B-16	Firmware Download in Progress	190
FIGURE B-17	Saving PROM Software	191
FIGURE B-18	Firmware Download Failed	192
FIGURE B-19	Card Reader OSD	193
FIGURE B-20	Card Read Error OSD	193
FIGURE B-21	Prompt for Card Insertion OSD	194
FIGURE B-22	Access Denied OSD	194

Tables

TABLE 2-1	Supported Commands	16
TABLE 2-2	Key User Fields	22
TABLE 2-3	<code>utrestart</code> Commands	23
TABLE 2-4	Data Elements Displayed	36
TABLE 2-5	<code>utcapture</code> Options	36
TABLE 2-6	Log Files	38
TABLE 4-1	Definitions of Naming Conventions	60
TABLE 4-2	Commands for Common Disk Operation on Linux Platforms	63
TABLE 7-1	DHCP Service Parameters Available	79
TABLE 7-2	Vendor-specific DHCP Options	98
TABLE 7-3	<code>.parms</code> Key/Value Pairs	106
TABLE 7-4	Prompt Mode Key Codes	109
TABLE 7-5	Pop-up GUI Menu Configuration Values	115
TABLE 7-6	Sun Ray DTU-to-Server Ports and Protocols	117
TABLE 7-7	Sun Ray Server-to-Server Protocols	118
TABLE 10-1	Kiosk Mode Settings	144
TABLE 11-1	Configuring Five Servers for 100 DTUs	150
TABLE 11-2	Available Options	155
TABLE A-1	Alternate Key Sequences for Non-Sun Keyboards	170
TABLE A-2	Sun Ray Settings Properties Files	171

TABLE A-3	Specific Hot Key Values	171
TABLE B-1	Icon Messages	176
TABLE B-2	DCHP State Codes	178
TABLE B-3	Power LED	179
TABLE B-4	Firmware Download Error Codes and Messages	179
TABLE B-5	Error Message Examples	196

Preface

The *Sun Ray Server Software 4.0 Administrator's Guide* provides instructions for setting up, administering, monitoring, and troubleshooting a system of Sun Ray™ Desktop Units (DTUs) and their server or servers. It is written for system administrators who are already familiar with the Sun Ray™ computing paradigm and have substantial networking knowledge. This guide may also be useful for those interested in customizing Sun Ray systems.

Before You Read This Book

This guide assumes that you have installed the Sun Ray Server Software on your server from the Sun Ray Server Software 4.0 CD or the Electronic Software Download (ESD).

How This Book Is Organized

[Chapter 1](#) gives an overview of the Sun Ray system.

[Chapter 2](#) describes the command-line interface.

[Chapter 3](#) describes the Administration Tool.

[Chapter 4](#) describes peripherals for Sun Ray DTUs.

[Chapter 5](#) describes mobile sessions, also known as Hotdesking.

[Chapter 6](#) gives a brief description of traffic encryption between Sun Ray clients and servers and server-to-client authentication.

[Chapter 7](#) discusses network requirements, such as LAN, VLAN, and dedicated interconnect options, switch requirements, and other network-related issues, such as downloading firmware and (optional) local configuration capabilities for Sun Ray DTUs.

[Chapter 8](#) outlines issues pertinent to the Gnome Display Manager.

[Chapter 9](#) describes how to implement multihead and XINERAMA on a Sun Ray system.

[Chapter 10](#) presents Kiosk Mode, for controlled access to applications.

[Chapter 11](#) discusses failover groups.

[Appendix A](#) addresses user settings and concerns.

[Appendix B](#) provides troubleshooting information, including error messages from the Authentication Manager.

This manual also contains a glossary and an index.

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. This document does, however, contain information about specific Sun Ray system commands.

Typographic Conventions

Typeface	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	Read Chapter 6 in the <i>User's Guide</i> . These are called <i>class</i> options. You <i>must</i> be superuser to do this.
	Command-line variable; replace with a real name or value	To delete a file, type <code>rm filename</code> .

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	#

Related Documentation

Application	Title	Part Number
Installation	<i>Sun Ray Server Software 4.0 Installation and Configuration Guide for the Linux Operating System</i>	820-0414
Release Notes	<i>Sun Ray Server Software 4.0 Release Notes for the Linux Operating System</i>	820-0418

Accessing Sun Documentation

You can view, print, or purchase a broad selection of Sun documentation, including localized versions, at:

<http://docs.sun.com>

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Sun at:

docfeedback@sun.com

Please include the part number (820-3769) of your document in the subject line of your email.

Sun Ray System Overview

The Sun Ray computing model, originally developed for Sun's Solaris™ Operating System, is historically the first thin client implementation to offer both workstation-like user functionality and sufficient speed and reliability for mission-critical applications. Sun Ray Server Software supports Sun Ray thin clients on two flavors of Linux—Red Hat Enterprise Linux 5 and SuSE Linux Enterprise Server 10—as well as Solaris 10, including Solaris Trusted Extensions.

Sun Ray Server Software supports LAN and low-bandwidth WAN deployment, integrated [VPN](#) capability, and many USB peripheral devices, even when the Sun Ray DTU is located behind a [NAT](#) gateway.

The Sun Ray Connector for Windows offers easy-to-manage connections from Sun Ray DTUs to user sessions running on Microsoft Windows Terminal Servers, including media extensions for improved video playback. It is described in the *Sun Ray Connector for Windows Operating Systems 2.1 Installation and Administration Guide*.

When used in conjunction with the Sun Ray Connector for Windows and the Sun Virtual Desktop Connector, Sun Ray Server Software helps to enable the use of multiple, virtualized desktops from Sun Ray DTUs. This capability is described in the *Sun Virtual Desktop Connector 1.0 Installation and Administration Guide*.

Computing Model

In contrast to other client-server models, which typically utilize combinations of remote and local operating systems, applications, memory, and storage, the Sun Ray computing model moves *all* computing to a server. Instead of storing data and doing computation on the desktop, the Sun Ray model simply passes input and output data between Sun Ray thin clients, also known as virtual display terminals and desktop terminal units (DTUs), and the Sun Ray server, where the operating system and applications are located.

Nearly any Sun server with sufficient capacity can be configured as a Sun Ray server so long as it runs a supported version of the Solaris operating system or one of the supported flavors of Linux. (See the *Sun Ray Server Software 4.1 Release Notes* for the most up-to-date list of supported operating systems and versions.)

Every Sun Ray DTU includes a smart card reader.

Sun Ray DTUs have no local disks, operating systems, or applications; they are therefore considered *stateless*. This is what makes them true thin clients. Stateless devices are inexpensive to maintain because they require no hands-on service by administrators or technicians to install, upgrade, or configure software or to replace mechanical components on the desktop. They are also extremely secure. Central administration of USB mass storage devices, at the server or group level, allows sites with particular security or intellectual property concerns to eliminate many risks imposed by PCs and other fat clients. Because fat clients rely on local operating systems and applications, critical data can easily be lost or compromised when physical devices are stolen.

Most large implementations include at least one failover group or to ensure uninterrupted service whenever a server goes off-line. Once a *failover group* is set up, Sun Ray Server Software provides automatic load balancing to optimize performance by spreading the computing load among the servers in the group. Failover groups and related concepts are addressed in [Chapter 11](#) and in the *Sun Ray Server Software 4.1 Installation and Configuration Guide*.

Sun Ray *sessions*—groups of services controlled by the Session Manager and associated with a user through an authentication token—reside on a server rather than on the desktop. Because Sun Ray DTUs are stateless, a session can be directed, or redirected, to any Sun Ray DTU on the appropriate network or subnetwork when a user logs in or inserts a smart card. While the session continues to reside on a server, it appears to follow the user to the new DTU. This functionality, called *session mobility*, enables *hotdesking*—the ability of users to access their sessions from any DTU on their network. Hotdesking, including non-smart card session mobility (*NSCM*), is discussed in [Chapter 5](#). In addition, *regional hotdesking* promotes hotdesking among server groups, letting users access their sessions across a wider domain. A new security enhancement, called Remote Hotdesk Authentication (*RHA*), requires SRSS-based authentication before users can reconnect to existing sessions.

The Sun Ray System

The Sun Ray system consists of Sun Ray DTUs, servers, server software, and the physical networks that connect them.

Sun Ray DTU

The Sun Ray desktop unit (DTU) delivers and may exceed the full functionality of a workstation or a multimedia PC. The key features include:

- 24-bit, 2-D accelerated graphics up to 1920 x 1200 resolution at 70 Hz (640 x 480 at 60 Hz is the lowest resolution)
- Multichannel audio input and output capabilities
- Smart card reader
- USB ports that support hot-pluggable peripherals
- Serial port (for the Sun Ray 170 and later models)
- [NAT](#) gateway device support
- Integrated, routerless [VPN](#) capability on Sun Ray 2, 2 FS, 270 and later models)
- EnergyStar™ compliance
 - No fan, switch, or disk
 - Very low power consumption

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

From the point of view of network servers, Sun Ray DTUs are identical except for their Ethernet [MAC address](#). If a DTU ever fails, it can easily be replaced.

An IP addresses is leased to each Sun Ray DTU when it is connected and can be reused when the DTU is disconnected. IP address leasing is managed by the Dynamic Host Configuration Protocol ([DHCP](#)). In cases where they already exist on a network that will support Sun Ray DTUs, separate DHCP servers may be useful for tasks such as assigning IP addresses and network parameters to the DTUs. The use of separate DHCP servers is not required; however, because they require static IP addresses, Sun Ray Servers cannot be DHCP clients. These considerations are discussed in [Chapter 7](#).

Multihead Displays

Sun Ray Server Software supports the use of multiple displays connected to a single keyboard and mouse. This functionality is important for users who need to monitor many applications or systems simultaneously or to accommodate a single application, such as a large spreadsheet, across multiple screens. To use multiple screens, the administrator sets up multihead groups, consisting of two or more DTUs, for those users who need them. Administration of multihead groups is explained in [Chapter 9](#).

Firmware Module

A small firmware module in each Sun Ray DTU can be updated from the server. The firmware module checks the hardware with a power-on self test (POST) and initializes the DTU. The DTU contacts the server to authenticate the user, and it also handles low-level input and output, such as keyboard, mouse, and display information. If there is a problem with the DTU, the module displays an on-screen display (OSD) icon to make it easier to diagnose. OSD icons are described in [Appendix B](#).

An enhanced version of the DTU firmware allows configuration parameters to be entered and modified locally through a Pop-up user interface (see [“Pop-up GUI” on page 108](#)). This new functionality can be especially useful in implementations such as Sun Ray at Home, which allows employees to connect remotely to the same sessions they use in their offices. Because it is not suitable for certain other implementations, however, such as public libraries or secure government sites, this feature must be downloaded explicitly and enabled by the administrator. The default version of the DTU firmware cannot be configured locally.

Sun Ray Server Software

The administrator can configure network connections, select an authentication protocol, administer authentication tokens, define desktop properties, and perform troubleshooting.

Sun Ray server software includes:

- User authentication and access control
- Encryption between the Sun Ray server and DTUs
- System administration tools
- Session management
- Device management, including application-level USB access
- Virtual device drivers for audio and serial, parallel, and mass storage USB devices

Sun Ray server software enables direct access to all Linux X11 applications. The Sun Ray Connector for Windows enables Sun Ray users to access applications running on remote Windows Terminal Servers (see the *Sun Ray™ Connector for Windows Operating Systems 2.1 Installation and Administration Guide*). Third-party applications running on the Sun Ray server can also provide access to Microsoft Windows applications and a variety of legacy (mainframe) applications.

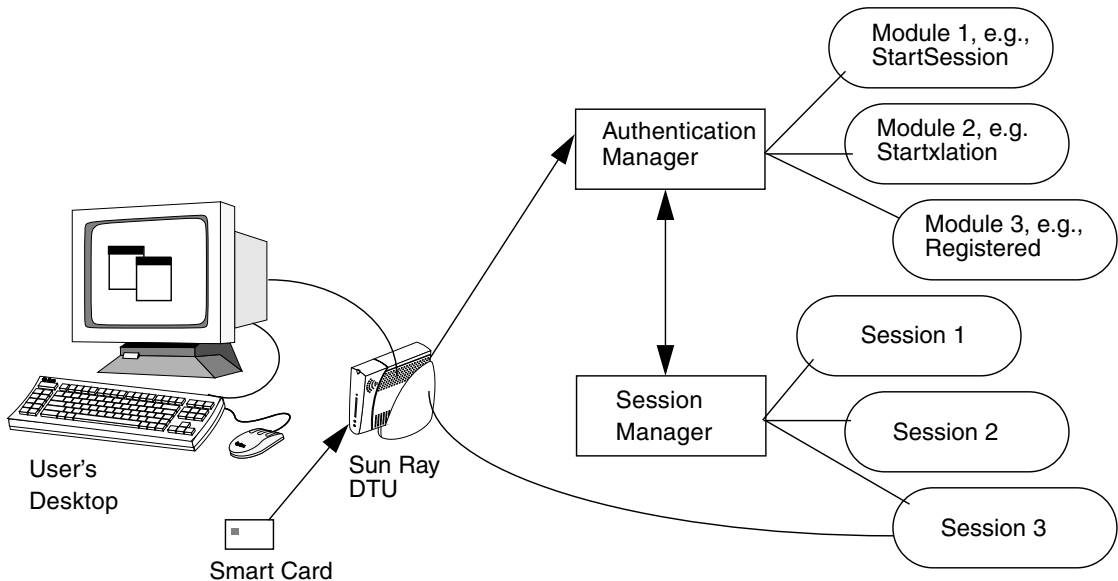
Authentication Manager

The Authentication Manager implements the chosen *policies* for identifying and authenticating users on Sun Ray DTUs, using pluggable components called *modules* to verify user identities and implements site access policies defined by the administrator. It also supplies an audit trail of the actions of users who have been granted administrative privileges over Sun Ray services. The Authentication Manager is not visible to users.

The interaction between the Authentication Manager and the DTU is depicted in [FIGURE 1-1](#). It works as follows:

1. A user accesses a DTU.
2. The DTU sends the user's *token* information to the Authentication Manager and requests access. If the user inserts a smart card in the DTU, the card's type and ID are used as the token. If not, the DTU's Ethernet address is used as a *pseudo-token*.
3. Based on the policy defined by the system administration, the Authentication Manager accepts or denies the access request.
4. If the user's access request is accepted, the Authentication Manager tells the Session Manager to start an X Windows session, which takes the user to the login screen. Solaris implementations use the `dtlogin` screen. Linux implementations use the Gnome Display Manager (GDM).

FIGURE 1-1 Authentication and Session Manager Interaction



Normally, the Sun Ray DTU looks for the `AuthSrvr` DHCP option and contacts that address. If that field has not been supplied, or if the server does not respond, the DTU sends a broadcast request for any Authentication Manager on its subnet.

As an alternative, the administrator can supply a list of servers. If the authentication list is specified, only addresses on the list are checked. The Authentication Manager addresses are tried in order until a connection is made.

The site administrator can construct a combination of the different modules and their options to implement a policy tailored to the site's needs.

Commonly used modules include:

- **StartSession**

Any type of token is accepted. Users are automatically passed through to the login window. This module is designed primarily for implementations in which Sun Ray DTUs replace workstations or PCs.

- **StartxlationSession**

Any type of token is accepted. A temporary, transitional session is created for authentication purposes. This is used for login and hotdesking with Non-SmartCard Mobility (*NSCM*) and for hotdesking when a Remote Hotdesk Authentication (*RHA*) policy is used.

- **Registered**

The token is accepted *only* if the token has been registered in the Sun Ray data store *and* the token is enabled. If the token does not meet these conditions, it is rejected. If the token is accepted, the user is passed through to the login window. This module is designed for sites that want to restrict access to only certain users or DTUs.

Users can be registered in two ways, reflecting two possible policy decisions for the administrator:

- **Central Registration**

The administrator assigns smart cards and/or DTUs to authorized users and registers users' tokens in the Sun Ray data store.

- **Self-Registration**

Users register themselves in the Sun Ray data store. If this mode is enabled and the Authentication Manager is presented with an unregistered token, the user is prompted with a registration window. In this case, the user provides the same information a site administrator would request.

If self-registration is enabled, users can still be registered centrally. If a token has been registered but disabled, the user *cannot* re-register the token; the user must contact the site administrator to re-enable the token.

Sessions and Services

A *session* consists of a group of services controlled by the Session Manager.

The session is associated with a user through an *authentication token*. A *service* is any application that can connect directly to the Sun Ray DTU. This can include audio, video, Xservers, and device control of the DTU. For example, `dtmail` is not a service because it is accessed through an Xserver.

Session Manager

The Session Manager (see [FIGURE 1-1](#)) interacts with the Authentication Manager and directs services to the 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 Session Manager keeps track of sessions and services by mapping services to sessions and binding and unbinding related services to or from a specific DTU. The Session Manager takes authentication only from authorized Authentication Managers listed in the `/etc/opt/SUNWut/auth.permit` file.

The sequence below describes how the process starts, ends, and restarts:

1. After a user's token is authenticated, the Authentication Manager determines whether a session exists for that token. If a session does not exist, the Authentication Manager asks the Session Manager to create a session and then starts the appropriate service(s) for the session according to the authentication policy decisions taken by the administrator. Creating a session usually involves starting an *Xserver* process for the session.
2. When services are started, they join the session explicitly 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 DTU. The Session Manager then informs each service in the session that it should connect directly to the DTU.
4. At this point, the user can interact with the session. The Session Manager mediates control of the screen real estate between competing services in a session and notifies the services of changes in screen real estate allocation.
5. When the user removes the smart card, or presses Shift-Pause in an *NSCM* session, or power cycles the DTU, the Authentication Manager determines that the session associated with that token should be disconnected from that DTU. The Authentication Manager notifies the Session Manager which, in turn, notifies all the services in the session to disconnect.

6. When the user inserts the smart card again, or logs in again for access to an NSCM session, the Authentication Manager's default behavior is to ask the Session Manager to create a temporary new session and use it to authenticate the user. This is known as Remote Hotdesk Authentication (*RHA*). After the user has been successfully authenticated, the Sun Ray DTU is connected directly to the user's session.

Note – RHA does not apply to anonymous Kiosk Mode or to token readers. Sun Ray Server Software can be configured to turn this security policy feature off if desired. See “[Remote Hotdesk Authentication \(RHA\)](#)” on page 71.

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

To verify that the Session Manager daemon is running, use the `ps` command and look for `utsessiond`.

If the Authentication Manager quits, the Session Manager disconnects all the sessions it authorized and tells them that they have to be re-authenticated. These services are disconnected but still active. If the Session Manager is disrupted, it restarts automatically. Each service contacts the Session Manager to request reattachment to a particular session.

Xserver

SRSS 4.1 now includes a new Xserver process, *Xnewt*, as the default Xserver. *Xnewt*, which supports all the latest multimedia enhancements below, is based on the release 7.2 of the Xorg Community source. For information on how to configure different Xservers, see the `utxconfig(1)` man page.

Multimedia Support

Sun Ray media extensions improve playback of certain kinds of video by adding support for *H.264* and *VC-1 codec* directly in Sun Ray 2 DTUs. H.264 is the video compression standard used by MPEG-4 part 10. VC-1 is the common video compression standard used by Windows Media Player 9 and 10. Not all profiles and levels of each *codec* format are supported, so videos need to be properly encoded to be able to play. Further information is available in the *Sun Ray Connector for Windows Operating Systems 2.1 Installation and Administration Guide*.

An accelerated path for *YUV* video delivery enables improved playback of video formats such as MPEG-1 and MPEG-2 by reducing the bandwidth required to deliver the decoded video to the Sun Ray DTU. The accelerated YUV path is used automatically so long as the correct software decoders are available for the video format required and the software is configured to make use of the Xvideo extension. For example, RealPlayer on Solaris supports the XVideo extension to utilize the accelerated YUV path. The following YUV formats are supported:

- Planar: YV12, I420
- Packed: UYVY, YUY2

H.264 or VC-1 video playback on a Sun Ray 1 DTU, which does not have a hardware decoding capability, uses software decoding and the accelerated YUV path.

Note – Chapter 8 is scheduled to be updated during Beta.

CLI and Admin GUI

Sun Ray Server Software has both a command-line interface (CLI—see [Chapter 2](#)) and a graphical user interface (GUI) for administrative functions. The Sun Ray Administration Tool (Admin GUI) was completely rewritten for the 4.0 release to present a clearer view of administrative functions, with a tab-based navigational model and context-sensitive help. It is described in [Chapter 3](#).

Data Store

Sun Ray Server Software 4.1 provides a private data store service, the Sun Ray Data Store (SRDS), for access to SRSS administration and configuration data, useful for maintaining consistency across failover groups.

Kiosk (Controlled Access) Mode

Sun Ray DTUs are becoming increasingly popular in settings where it is desirable to provide anonymous users with limited access to specific applications. Sun Ray Kiosk mode software, revised and improved for the 4.0 release, is described in [Chapter 10](#). Instructions for migrating configuration data from the previous Controlled Access Mode (CAM) can be found in the *Sun Ray Software 4.1 Installation and Configuration Guide*.

Network Components

In addition to the servers, server software, DTUs, smart cards, and peripheral devices, such as local printers, the Sun Ray system needs a well-designed network, configured in one of several possible ways, including:

- Dedicated interconnect
- LAN (Local Area Network), with or without network routers
- VLAN (Virtual Local Area Network)
- VPN (Virtual Private Network)
- WAN (Wide Area Network), low-bandwidth (less than 2 Mbps)

Various types of network configuration are discussed in depth in [Chapter 7](#). For basic instructions on configuring different types of networks for Sun Ray implementation, see [“Basic Network Topology” on page 36](#) of the *Sun Ray Server Software 4.1 Installation and Configuration Guide*.

Physical Connections

The physical connection between the Sun Ray server and Sun Ray clients relies on standard switched Ethernet technology. To boost the power of the interconnect and shield Sun Ray DTU users from the network interaction taking place at every display update, 100 Mbps switches are preferred.

There are two basic types of 100 Mbps switches:

- Low-capacity switches—These switches have 10/100 Mbps interfaces for each port.
- High-capacity switches—These switches have 10/100 Mbps interfaces for each terminal port, but one or more gigabit interfaces to attach to the server.

Either type of switch can be used in the interconnect. They can be managed or unmanaged; however, some managed switches may require basic configuration in order to be used on a Sun Ray network.

Server-to-switch bandwidth should be scaled based on end-user multiplexing needs so that the server-to-switch link does not become overly saturated. Gigabit uplink ports on the switch provide high-bandwidth connections from the server, thus increasing the number of supportable clients. The distance between the server and the switch can also be extended using gigabit fiber-optic cabling.

The interconnect may be completely dedicated and private, or a VLAN, or it may be part of the corporate LAN. For private interconnects, the Sun Ray server uses at least two network interfaces: one for the corporate LAN, the other for the Sun Ray interconnect.

Even in a LAN deployment, two server network interfaces are recommended: one to connect to the general LAN and one to connect the server to back-end services, such as file servers, compute grids, and large databases.

Deployment Examples

There is no physical or logical limit to the ways that a Sun Ray system can be configured. The following sections offer some elementary examples. In addition, detailed discussions of actual deployment scenarios can be found on blogs such as <http://blogs.sun.com/ThinkThin>, <http://blogs.sun.com/ThinGuy>, and <http://blogs.sun.com/bobd>.

Small Deployments

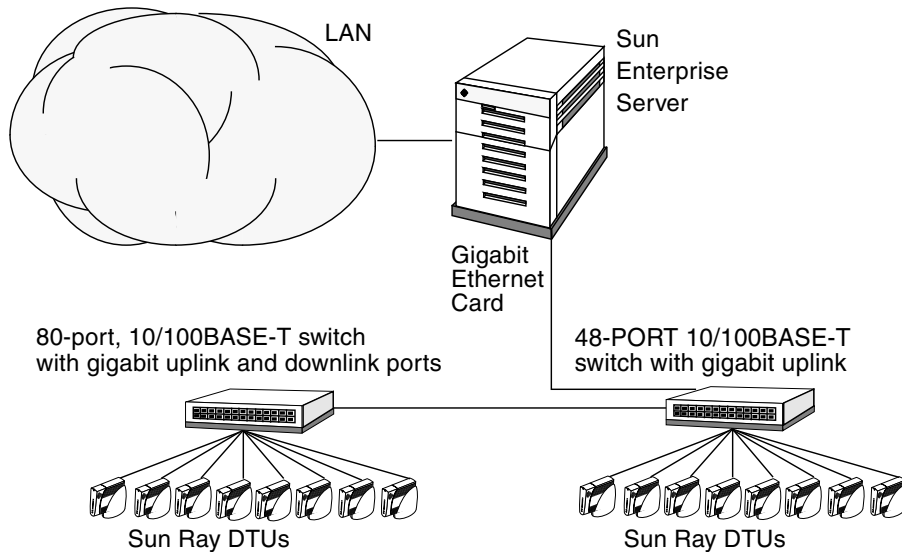
For smaller deployments, such as those with between five and 50 Sun Ray DTUs, the Sun Ray server uses a single 100BASE-T card to connect to a 100BASE-T switch. This switch, in turn, connects to the Sun Ray DTUs. With five or fewer DTUs, a wireless interconnect works acceptably at 10 Mbytes.

Medium to Large Deployments

For larger departments with groups consisting of hundreds or thousands of Sun Ray DTUs, the Sun Ray server uses a gigabit Ethernet card to connect to large 10/100BASE-T switches. Especially with recent low-bandwidth enhancements, there is no performance need to have more than one gigabit link from the server to the Sun Ray DTU's network.

A 100-user departmental system, for example, consisting of a Sun Enterprise server, one gigabit Ethernet card, and two large (48-port and 80-port) 10/100BASE-T switches delivers services to the 100 Sun Ray DTUs (see [FIGURE 1-2](#)).

FIGURE 1-2 Typical Medium to Large Deployment Scenario



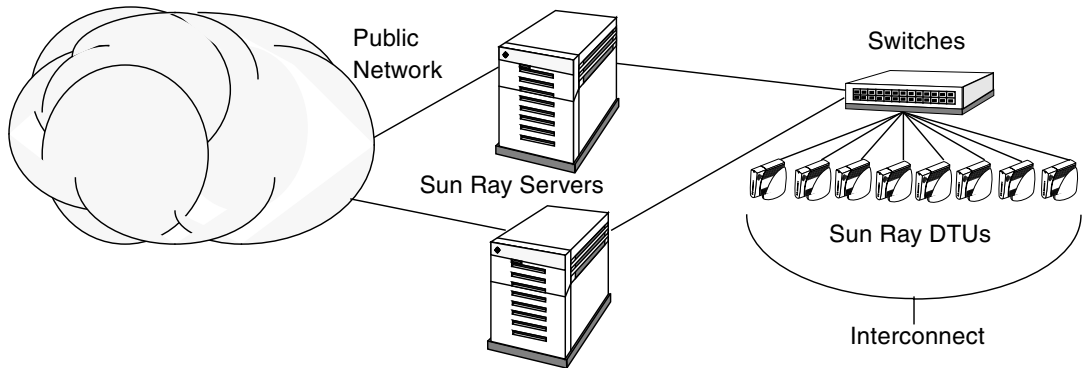
For example, a Sun Enterprise™ server with a Sun 10/100BASE-T card and a 24-port 10/100BASE-T switch can easily support 23 users performing standard desktop activities.

Failover Group Scenario

Sun Ray servers are often bound together to create failover groups. A failover group, comprising two or more servers, provides users with a higher level of availability in case one server become unavailable due to a network or system failure.

When a server in a failover group goes down, whether for maintenance, a power outage, or any other reason, each Sun Ray DTU connected to it reconnects to another server in the failover group and to a previously existing session for the current token, if there is one, on that server. If it can find no existing session for the current token, the DTU connects to a server selected by the load balancing algorithm. This server presents a login screen to the user, who then logs in to create a new session. The session on the failed server is lost. Failover groups are discussed in [Chapter 11](#) as well as in the *Sun Ray Server Software 4.1 Installation and Configuration Guide*.

FIGURE 1-3 Simple Failover Group



Regional Hotdesking

Enterprises with multiple failover groups and users who move from one location to another—such as between corporate headquarters and various branch offices—may wish to configure regional hotdesking. This feature provides users with access to their sessions across a wider domain and longer distance than a single failover group. It is described in [Chapter 5](#).

Security Considerations

Using switched network gear for the last link to the DTUs makes it difficult for a malicious PC user or network snooper at one of the network ports to obtain unauthorized information. Because switches send packets only to the proper output port, a snooper plugged into another port receives no unauthorized data. If the server and wiring closet are secure, the last step is switched, and the DTU is plugged directly into the wall jack, then it is very difficult to intercept communications between the server and the DTU. Sun Ray Server Software encryption features also help to protect sensitive data by providing options to encode keyboard input and display traffic. In addition, Remote Hotdesk Authentication (*RHA*), requires SRSS-based authentication before users can reconnect to existing sessions.

Command-Line Interface

The Command-Line Interface (CLI) is the recommended interface for enabling assistive technologies.

This chapter contains the following information:

- “Supported Commands” on page 15
- “Session Redirection” on page 20
- “Changing Authentication Policies” on page 23
- “Managing User Data in the Sun Ray Data Store” on page 22
- “Enabling Multiple Administration Accounts” on page 23
- “Enabling and Disabling Device Services” on page 26
- “Configuring Interfaces on the Sun Ray Interconnect Fabric” on page 27
- “Managing Firmware Versions” on page 30
- “Restarting the Sun Ray Data Store (SRDS)” on page 31
- “Smart Card Configuration Files” on page 32
- “Using the `utcapture` Tool” on page 35
- “Examining Log Files” on page 38

Supported Commands

Commands that can be executed from the command line are listed in [TABLE 2-1](#), and a few of the most important commands are documented in this chapter. For further information on executing these commands, see the man page for the command in question.

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

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

or type:

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

TABLE 2-1 Supported Commands

Command	Definition
utaction	The <code>utaction</code> program provides a way to execute commands when a Sun Ray DTU session is connected, disconnected, or terminated.
utadm	The <code>utadm</code> command manages the private network, shared network, and DHCP (Dynamic Host Configuration Protocol) configuration for the Sun Ray interconnect.
utadminuser	The <code>utadminuser</code> command is used to add, list, and delete UNIX user names from the list of users authorized to administer Sun Ray services. The list is stored in the Sun Ray data store.
utamghadm	The <code>utamghadm</code> command is used to configure or disable regional hotdesking, which enables users to access their sessions across multiple failover groups.
utcapture	The <code>utcapture</code> command connects to the Authentication Manager and monitors packets sent and packets dropped between the Sun Ray server and the Sun Ray DTUs.
utcard	The <code>utcard</code> command allows configuration of different types of smart cards in the Sun Ray data store.
utconfig	The <code>utconfig</code> command performs the initial configuration of the Sun Ray server and supporting administration framework software.
utcrypto	The <code>utcrypto</code> command is a utility for security configuration.
utdesktop	The <code>utdesktop</code> command allows the user to manage Sun Ray DTUs connected to the Sun Ray server that the command is run on.
utdetach	The <code>utdetach</code> command disconnects the current non-smart card mobile session or authenticated smart card session from its respective Sun Ray DTU. The session is not destroyed but put into a detached state. The session can be accessed again only after authentication. When Remote Hotdesk Authentication (RHA) is disabled (via <code>utpolicy</code> or the Admin GUI), <code>utdetach</code> affects only authenticated smart card sessions and non-smart card mobile sessions.

TABLE 2-1 Supported Commands (*Continued*)

Command	Definition
utdevadm	The <code>utdevadm</code> command is used to enable/disable Sun Ray device services. This includes USB devices connected through USB ports, embedded serial ports, and internal smart card reader in the Sun Ray DTU.
utdiskadm	The <code>utdiskadm</code> utility is a tool for Sun Ray mass storage administration.
utdssync	The <code>utdssync</code> command converts the port number for the Sun Ray Data Store service to the new default port on servers in a failover group, then forces all servers in the group to restart Sun Ray services.
uteject	The <code>uteject</code> command is used to eject media from a removable storage media device.
utfwadm	The <code>utfwadm</code> command manages firmware versions on the Sun Ray DTUs.
utfwload	The <code>utfwload</code> command is used primarily to force the download of new firmware to a DTU running older firmware than its server.
utfwsync	The <code>utfwsync</code> command refreshes the firmware level on the Sun Ray DTUs to what is available on the Sun Ray servers in a failover group. It then forces all the Sun Ray DTUs within the group to restart.
utgmtarget	The <code>utgmtarget</code> command manages a group-wide list of explicit destinations for Sun Ray group membership announcements
utgroupsig	The <code>utgroupsig</code> command sets the failover group signature for a group of Sun Ray servers. The <code>utgroupsig</code> command also sets the Sun Data Store <code>rootpw</code> used by Sun Ray to a value based on the group signature. Although <code>utgroupsig</code> sets the <code>rootpw</code> in the <code>utdsd.conf</code> file, it does <i>not</i> set the admin password, which is a separate entity, in the data store.
utgstatus	The <code>utgstatus</code> command allows the user to view the failover status information for the local server or for the named server. The information that the command displays is specific to that server at the time the command is run.
utinstall	The <code>utinstall</code> utility installs, upgrades, and removes Sun Ray Server Software. All software required to support the Sun Ray server is installed, including the administration framework.
utkiosk	The <code>utkiosk</code> tool is used to import/export kiosk configuration information into the data store. It also supports storage of multiple named kiosk session configurations in the data store.
utkioskoverride	The <code>utkioskoverride</code> command provides a way to set the session type associated with a token, to select a kiosk session configuration for a token associated with a kiosk session, or to query the session type and kiosk session currently associated with a token.
utmhadm	The <code>utmhadm</code> command provides a way to administer Sun Ray server multihead terminal groups. The information that <code>utmhadm</code> displays and that is editable is stored in the data store.

TABLE 2-1 Supported Commands (*Continued*)

Command	Definition
<code>utmhconfig</code>	The <code>utmhconfig</code> tool allows an administrator to list, add, or delete multiheaded groups easily.
<code>utmount</code>	The <code>utmount</code> command is used to mount a file system on a Sun Ray mass storage device.
<code>utpolicy</code>	The <code>utpolicy</code> command sets and reports the policy configuration of the Sun Ray Authentication Manager, <code>utauthd(1M)</code> .
<code>utpreserve</code>	The <code>utpreserve</code> command saves existing Sun Ray Server Software configuration data to the <code>/var/tmp/SUNWut.upgrade</code> directory.
<code>utpw</code>	The <code>utpw</code> command changes the Sun Ray administrator password (also known as the UT admin password) used by the Web-based and command-line administration applications.
<code>utquery</code>	The <code>utquery</code> command collects DHCP information from the Sun Ray DTUs.
<code>utreader</code>	The <code>utreader</code> command is used to add, remove, and configure token readers.
<code>utreplica</code>	The <code>utreplica</code> command configures the Sun Ray Data Store server to enable replication of administered data from a designated primary server to each secondary server in a failover group. The data stores of the secondary servers remain synchronized automatically unless there is a power outage. The <code>-z</code> option is useful for updating the port number.
<code>utresadm</code>	The <code>utresadm</code> command allows an administrator to control the resolution and refresh rate of the video monitor signal (persistent monitor settings) produced by the Sun Ray unit.
<code>utresdef</code>	The <code>utresdef</code> command allows an administrator to create, delete, and view resolution definitions (actually monitor signal timing definitions) for monitors attached to Sun Ray DTUs.
<code>utrestart</code>	The <code>utrestart</code> command is used to start Sun Ray services.
<code>utselect</code>	The <code>utselect</code> command presents the output of <code>utswitch -l</code> as a list of servers in the current host group, to be used for reconnection of the current DTU. A user can either select a server from this list or specify a server not in the current host group by typing its full name in the <code>utselect</code> text box.
<code>utsession</code>	The <code>utsession</code> command lists and manages Sun Ray sessions on the local Sun Ray server.
<code>utset</code>	Use <code>utset</code> to view and change Sun Ray DTU settings.
<code>utsettings</code>	The <code>utsettings</code> command opens a Sun Ray Settings dialog box that allows the user to view or change audio, visual, and tactile settings for the Sun Ray DTU.
<code>utswitch</code>	The <code>utswitch</code> command allows a Sun Ray DTU to be switched among various Sun Ray servers. <code>utswitch</code> can also list existing sessions for the current token.
<code>utumount</code>	The <code>utumount</code> command is used to unmount a file system from a Sun Ray mass storage device.

TABLE 2-1 Supported Commands (*Continued*)

Command	Definition
<code>utuser</code>	The administrator can manage Sun Ray user tokens registered on a Sun Ray server by running the <code>utuser</code> command on it. The <code>utuser</code> command also provides information on the currently inserted token (smart card) for a specified DTU that is configured as a token reader.
<code>utwall</code>	The <code>utwall</code> utility sends a message or an audio file to users having an Xnewt (Xserver unique to Sun Ray) process. The messages can be sent in email and displayed in a pop-up window.
<code>utwho</code>	The <code>utwho</code> script assembles information about display number, token, logged-in user, etc., in a compact format.
<code>utxconfig</code>	The <code>utxconfig</code> program provides Xserver configuration parameters for users of Sun Ray DTU sessions.

▼ To Stop Sun Ray Services

- Type:

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

▼ To Start Sun Ray Services

- Type:

```
# utrestart
```

This procedure, known as a *warm restart*, starts Sun Ray services without clearing existing sessions.

Or

- Type:

```
# utrestart -c
```

This procedure, known as a *cold restart*, starts Sun Ray services and clears existing sessions.

Session Redirection

After a user's token has been authenticated, whether via smart card token or direct login, it is automatically redirected to the appropriate server. To redirect a session to a different server manually, use the `utselect` graphical user interface (GUI) or the `utswitch` command.

▼ To Redirect to a Different Server

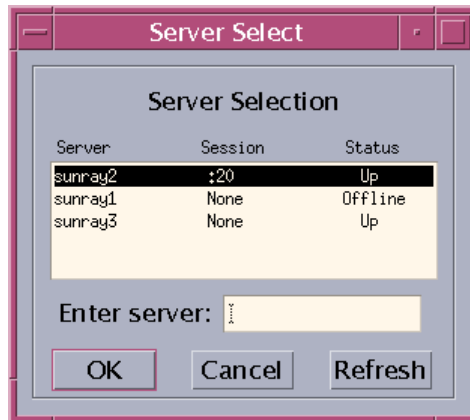
- From a shell window on the DTU, type:

```
% utselect
```

The selections in the window are sorted in order of the most current to least current active sessions for the token ID.

In [FIGURE 2-1](#), the Server column lists the servers accessible from the DTU. The Session column reports the DISPLAY variable X session number on the server if one exists. In the Status column, Up indicates that the server is available. The first server in the list is highlighted by default. Select a server from the list or enter the name of a server in the Enter server: field. If a server without an existing session is selected, a new session is created on that server.

FIGURE 2-1 The Server Selection (`utselect`) GUI



The OK button commits the selection of the highlighted or manually entered server. The Cancel button dismisses the GUI without making any changes to the session. The Refresh button reloads the window with the most current information.

▼ To Redirect a DTU Manually

- From a shell window on the DTU, type:

```
% utswitch -h host [ -k token]
```

where *host* is the host name or IP address of the Sun Ray server to which the selected DTU is redirected, and *token* is the user's token ID.

▼ To List Available Hosts

- From a shell window, type:

```
% utswitch -l
```

Hosts available from the Sun Ray DTU are listed.

▼ To Select a Server with the Latest Session

- In a shell window, type:

```
% utswitch -t
```

The DTU is redirected to the server with the latest session connect time.

Managing User Data in the Sun Ray Data Store

You can specify the following user fields in the Sun Ray data store:

TABLE 2-2 Key User Fields

Field	Description
Token ID	User's unique token type and ID. For smart cards, this is a manufacturer type and the card's serial ID. For DTUs, this is the type "pseudo" and the DTU's Ethernet address. Examples: mondex.9998007668077709 pseudo.080020861234
Server Name	Name of the Sun Ray server that the user is using. Server Name is optional.
Server Port	Sun Ray server's communication port. This field should generally be set to 7007. This setting is optional.
User Name	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.

Note – Sun Ray Server Software now supports multiple administration accounts. This feature is described in “[Enabling Multiple Administration Accounts](#)” on [page 23](#).”

Changing Authentication Policies

Setting an authentication policy with `utpolicy`, automatically sets the failover group policy, so all you need to do after making a policy change is to reset or restart services. You can also modify policy settings with the Admin GUI System Policy tab (see [FIGURE 3-12](#)).

TABLE 2-3 `utrestart` Commands

Command/Option	Result
<code>utrestart</code>	Use this option if a minor policy change was made, such as changing from soft to hard security mode. With minor changes, it is not necessary to terminate existing sessions. This is a warm restart.
<code>utrestart -c</code>	Use this option if a significant policy change has been made, such as enabling or disabling access to mass storage devices. All existing sessions are terminated. This is a cold restart.

Enabling Multiple Administration Accounts

Early releases of Sun Ray Server Software allowed only one user account, `admin`, to modify entries in the Sun Ray Data Store. Now, however, the administrator can allow any valid UNIX user ID in the authorized user list to administer Sun Ray services. An audit trail of activity on these accounts is provided. See the man page for `utadminuser(1M)`.

Authentication for accounts with administrative privileges is based on the PAM authentication framework.

PAM Entries

In order to support the old Data Store authentication, a PAM module, `/opt/SUNWut/lib/pam_sunray_admingui.so.1`, is included in the Sun Ray product.

▼ To Configure UNIX Users

To configure the Sun Ray Admin GUI to use UNIX user names instead of the default admin account:

- **Copy the auth entries from `/etc/pam.d/login` file into `/etc/pam.d/utadmingui`:**
 - On RHEL 5, the PAM entries are:

```
# added to utadmingui by Sun Ray Server Software -- utadmingui
auth required pam_stack.so service=system-auth
auth required pam_nologin.so
```

- On SLES 10, the PAM entries are:

```
# added to utadmingui by Sun Ray Server Software -- utadmingui
auth required pam_unix2.so
auth required pam_nologin.so
```

Note – Make sure to include the comment line, which is needed for the cleanup to work properly.

▼ To Revert to the Old admin User

To return to the old Sun Ray Admin GUI authentication scheme:

- **Replace the PAM entries in the `/etc/pam.d/utadmingui` file with the `pam_sunray_admingui.so.1` module:**

```
# added to utadmingui by Sun Ray Server Software -- utadmingui
auth sufficient /opt/SUNWut/lib/pam_sunray_admingui.so.1
```

Note – Make sure to include the comment line, which is needed for the cleanup to work properly.

Administration GUI Audit Trail

The administration framework provides an audit trail of the Admin GUI. The audit trail is an audit log of the activities performed by multiple administration accounts. All events that modify system settings are logged in the audit trail.

SRSS 4.1 uses the `syslog` implementation. Events are logged into `/var/opt/SUNWut/log/messages` file, where audit events are prefixed with the keyword `utadt::` so that administrator can filter events from the messages file.

For example, session termination from the Admin GUI generates the following audit event:

```
Jun  6 18:49:51 sunrayserver usersession[17421]: [ID 521130 user.info] utadt::
username={demo} hostname={sunrayserver} service={Sessions}
cmd={/opt/SUNWut/lib/utrcmd sunrayserver /opt/SUNWut/sbin/utsession -x -d
Cyberflex_Access_FullCrypto.1047750b1e0e -k 2>&1}
message={terminated User "Cyberflex_Access_FullCrypto.1047750b1e0e" with
display number="4" on "sunrayserver"}
status={0} return_val={0}
```

where

<i>username</i>	=	User's Unix ID
<i>hostname</i>	=	Host on which the command is executed
<i>service</i>	=	Name of the service being executed
<i>cmd</i>	=	Name of the command being executed
<i>message</i>	=	Details about the action being performed

Enabling and Disabling Device Services

Sun Ray device services can be enabled and disabled with the `utdevadm` command line tool or with the Admin GUI. Sun Ray device services include USB devices connected through USB ports, internal serial ports, and internal smart card readers on the Sun Ray DTU. Device services can also be administered from the Security tab on the Admin GUI Advanced tab (see [FIGURE 3-11](#)).

The Sun Ray 2 and Sun Ray 2FS each have one embedded serial port; the Sun Ray 170 and Sun Ray 270 each have two embedded serial ports. When internal serial service is disabled, users cannot access embedded serial ports on the Sun Ray DTU.

When internal smart card reader service is disabled, users cannot access the internal smart card reader through the PC/SC or SCF interfaces for reading or writing; however, this does not affect session access or hotdesking with unauthenticated smart cards.

When USB service is disabled, users cannot access any devices connected to USB ports. This does not, however, affect HID devices such as the keyboard, mouse, or barcode reader.

After installation of Sun Ray Server Software, all device services are enabled by default. You can use the `utdevadm` command to enable or disable device services only in the configured mode, that is, *after* the Sun Ray Data store is activated.

This configuration affects all the servers in a group and all the DTUs connected to that group.

The following example shows how to enable or disable USB service. The other device services can be enabled or disabled with the same syntax.

▼ To Determine the Current State of Device Services

- Use the `utdevadm` command:

```
# utdevadm
```

This displays enabled or disabled state of the devices.

▼ To Enable USB Service

- Use the `utdevadm` command as below:

```
# utdevadm -e -s usb
```

▼ To Disable USB Service

- Use the `utdevadm` command as below:

```
# utdevadm -d -s usb
```

▼ To Perform a Cold Restart

- Use the `utrestart` command as below:

```
# utrestart -c
```

Configuring Interfaces on the Sun Ray Interconnect Fabric

Use the `utadm` command to manage the Sun Ray interconnect fabric.

Note – If the IP addresses and DHCP configuration data are not set up properly when the interfaces are configured, then the failover feature will not work as expected. In particular, configuring the Sun Ray server’s interconnect IP address as a duplicate of any other server’s interconnect IP address may cause the Sun Ray Authentication Manager to generate “Out of Memory” errors.

Note – If you make manual changes to your DHCP configuration, you will have to make them again whenever you run `utadm` or `utfwadm`.

▼ To Configure a Private Sun Ray Network

- To add an interface, type:

```
# utadm -a interface_name
```

This command configures the network interface *interface_name* as a Sun Ray interconnect. 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.

Note – If you choose to specify your own subnet, make sure it is not already in use.

After an interconnect is selected, appropriate entries are made in the *hosts*, *networks*, and *netmasks* files. (These files are created if they do not exist.) The interface is activated.

Any valid network interface can be used. For example:

```
eth0, eth1, eth2
```

▼ To Configure a Second Private Sun Ray Network

- To add another interface, type, for example:

```
# utadm -a hme1
```

▼ To Delete an Interface

- Type:

```
# utadm -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 Print the Sun Ray Private Interconnect Configuration

- Type:

```
# utadm -p
```

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

Note – Sun Ray servers require static IP addresses; therefore, they cannot be DHCP clients.

▼ To Add a LAN Subnet

- Type:

```
# utadm -A subnet_number
```

▼ To Delete a LAN Subnet

- Type:

```
# utadm -D subnet_number
```

▼ To List the Current Network Configuration

- Type:

```
# utadm -l
```

`utadm -l` lists all the currently configured networks.

▼ To Remove All Interfaces and Subnets

Use the `utadm -r` command to prepare for removal of the Sun Ray Server Software.

- **Type:**

```
# utadm -r
```

This command removes all of the entries and structures relating to all of the Sun Ray interfaces and subnets.

Managing Firmware Versions

Use the `utfwadm` command to keep the firmware version in the PROM on Sun Ray DTUs synchronized with that on the server. See also [“Firmware” on page 104](#).

Note – If the DHCP *version* variable is defined, then when a new DTU is plugged in, its firmware is changed to the firmware version on the server.

Note – If you make manual changes to your DHCP configuration, you will have to make them again whenever you run `utadm` or `utfwadm`.

▼ To Update All the DTUs on an Interface

- **Type:**

```
# utfwadm -A -a -n interface
```

Tip – To force a firmware upgrade, power-cycle the DTUs.

▼ To Update a DTU Using the Ethernet (MAC) Address

- Type:

```
# utfwadm -A -e MAC_address -n interface
```

Restarting the Sun Ray Data Store (SRDS)

If you restart the Sun Ray Data Store daemon (`utdsd`), you must also restart the Sun Ray Authentication Manager. The Sun Ray Data Store daemon may need to be restarted if you change one of its configuration parameters. The following procedure shows the correct order of the steps to take if you need to restart SRDS.

▼ To Restart Sun Ray Data Store

1. Stop the Sun Ray services:

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

2. Stop the Sun Ray Data Store daemon:

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

3. Restart the Sun Ray services:

```
# utrestart
```

Smart Card Configuration Files

Use the Admin GUI or the `utcard` command to add additional smart card vendor configuration files.

Smart card configuration files are available from a variety of sources, including Sun and various of smart card manufacturers.

▼ To Load a Configuration File Into the Directory

- Copy the vendor configuration file containing the vendor tags to the following location:

```
# cp vendor.cfg /etc/opt/SUNWut/smartcard
```

The additional vendor cards are displayed under the Available Smart Cards column in the Card Probe Order tab in the Admin GUI.

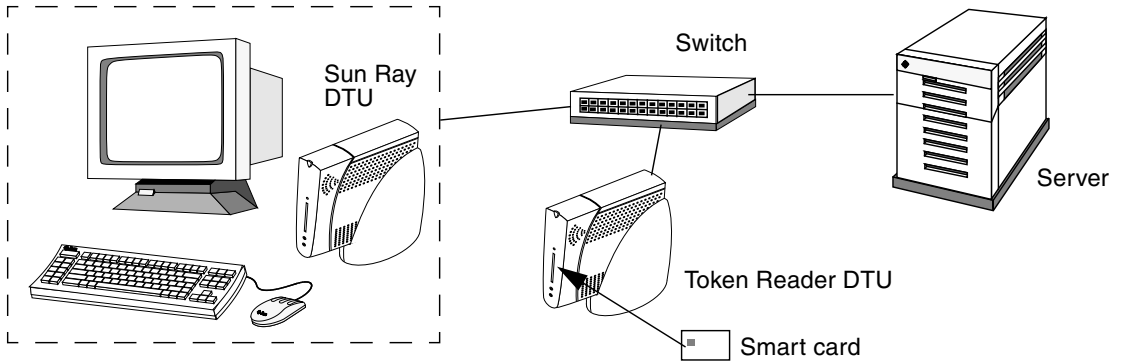
Configuring and Using Token Readers

Some manufacturers print the smart card ID on the card itself, but many do not. Since all the administrative functions refer to this token ID, Sun Ray Server Software provides a way to designate one or more specific DTUs as dedicated token readers. Site administrators can use a dedicated token reader to administer Sun Ray users through their tokens. A token reader is not used for normal Sun Ray services, so it does not need a keyboard, mouse, or monitor.

In the example configuration in [FIGURE 2-2](#), the second DTU acts as a token reader.

When you enable an authentication policy with registered users, or token owners, be sure to specify smart card IDs for them. To utilize token readers with regional hotdesking based on Sun Ray *pseudo-tokens*, use the Site-specific Mapping Library to produce the desired behavior for them. See [“To Configure a Site-specific Mapping Library” on page 69](#) and [“Token Readers with Regional Hotdesking” on page 70](#).

FIGURE 2-2 Using a Token Reader to Register Smart Cards



Token Reader Icon

When a site policy disallows pseudo-sessions, DTUs configured as token readers display the token reader icon instead of the Login Dialog box. The token reader is also called the card reader. (See [“Token Reader Icons”](#) on page 192.)

FIGURE 2-3 Token Reader (Card Reader) Icon



▼ To Configure a Token Reader

The `utreader` command allows a DTU to be used as a token reader, for registering smart cards. When a DTU is configured as a token reader, inserting or removing a smart card does not initiate session mobility; any session connected to that DTU remains connected to it regardless of card movement events.

Token reader mode is useful when you want to determine the raw token ID of a smart card.

- For instance, to configure the DTU with MAC address `0800204c121c` as a token reader, type the following command:

```
# utreader -a 0800204c121c
```

- To re-enable the DTU with MAC address `0800204c121c` to recognize card movement events and perform session mobility based on the smart card inserted into the DTU:

```
# utreader -d 0800204c121c
```

- To unconfigure all token readers on this server:

```
# utreader -c
```

▼ To Get a Token ID From a Token Reader

In releases prior to SRSS 3, access to the token card reader was limited to the server to which it was connected; the `utuser` command had to be invoked from that server. Beginning with SRSS 3.1, however, you can access the token card reader by invoking `utuser -r` from any server in the relevant failover group. The procedure otherwise remains as it was in earlier releases.

- Type the following command:

```
# utuser -r Token Reader
```

where *Token Reader* is the MAC address of the DTU containing the smart card whose ID you want to read. Insert the smart card into the DTU and run the `utuser` command. This command queries the DTU for the smart card token's ID and, if successful, displays it. For example:

```
# /opt/SUNWut/sbin/utuser -r 08002086e18f
Insert token into token reader '08002086e18f' and press return.
Read token ID 'mondex.9998007668077709'
```

Using the `utcapture` Tool

The `utcapture` tool connects to the Authentication Manager and collects data about the packets sent and packets dropped between the Sun Ray server and the DTU. The data in [TABLE 2-4](#) is then displayed on the screen in the following format:

TABLE 2-4 Data Elements Displayed

Data Element	Description
TERMINALID	The MAC address of the DTU
TIMESTAMP	The time the loss occurred in year-month-day-hour-minute-second format. Example: 20041229112512
TOTAL_PACKET	Total number of packets sent from server to DTU
TOTAL_LOSS	Total number of packets reported as lost by DTU
BYTES_SENT	Total number of bytes sent from server to DTU
PERCENT_LOSS	Percentage of packets lost between the current and previous polling interval
LATENCY	Time in milliseconds for a round trip from DTU to server.

Tip – Sun Ray DTU traffic loss of more than .1%, may indicate a network problem. You may want to allocate higher priority to the VLAN that carries Sun Ray DTU traffic. For more information on how to change the priority, see the manufacturer’s documentation for your switch.

The following `utcapture` options are supported:

TABLE 2-5 `utcapture` Options

Option	Definition
-h	Help for using the command.
-r	Dump output to <code>stdout</code> in raw format. By default, data is dumped when there is a packet loss. With this option, the data is always dumped to <code>stdout</code>
-s <i>server</i>	Name of server on which the Authentication Manager is running. By default, it is the same host that is running <code>utcapture</code> .
-i <i>filename</i>	Process raw data from a file specified by file name and dump to <code>stdout</code> only the data for those DTUs that had packet loss.
<i>desktopID</i>	Collects the data for the specified DTUs only. DTUs are specified on the command line by their desktop IDs separated by a space. By default, data for all currently active desktops is collected.

▼ To Start utcapture

- From a command line, enter one of the following commands:

```
% utcapture -h
```

This command lists the help commands for the `utcapture` tool.

```
% utcapture
```

This command captures data every 15 seconds from the Authentication Manager running on the local host and then writes it to `stdout` if there is any change in packet loss for a DTU.

```
% utcapture -r > raw.out
```

This command captures data every 15 seconds from the Authentication Manager running on the local host and then writes it to `stdout`.

```
% utcapture -s sunray_server5118.eng 080020a893cb 080020b34231
```

This command captures data every 15 seconds from the Authentication Manager running on `server5118.eng` and then writes the output to `stdout` if there is any change in packet loss for the DTU with ID `080020a893cb` or `080020b34231`.

```
% utcapture -i raw-out.txt
```

This command processes the raw data from the input file `raw-out.txt` and then writes to `stdout` the data only for those DTUs that had packet loss.

Examining Log Files

Significant activity concerning files retrieved from the Sun Ray server is logged and saved. The server stores this information in text files. [TABLE 2-6](#) describes the log files that are maintained.

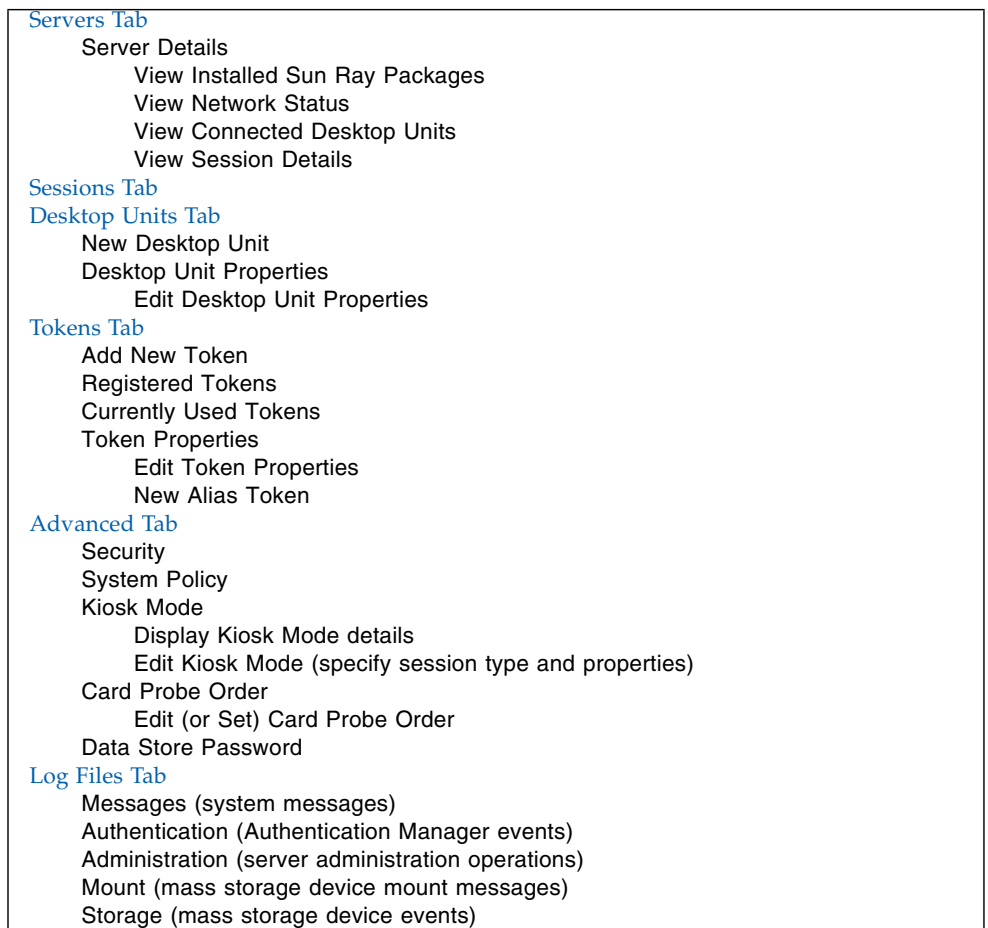
TABLE 2-6 Log Files

Log File	Path	Description
Administration	<code>/var/opt/SUNWut/log/admin_log</code>	Lists operations performed during server administration. This log is updated daily. Archived files are stored on the system for up to one week and are annotated using numeric extensions (for example, from file name <code>admin_log.0</code> to <code>admin_log.5</code>).
Authentication	<code>/var/opt/SUNWut/log/auth_log</code>	Lists events logged from the Authentication Manager. The <code>auth_log</code> file is updated (up to a limit of 10) every time the server's authentication policy is changed or started. The archived authentication files are annotated using numeric extensions (for example, from <code>auth_log.0</code> to <code>auth_log.9</code>).
Automatic Mounting	<code>/var/opt/SUNWut/log/utmountd.log</code>	Lists mount messages for mass storage devices. The archived <code>mountd</code> files are annotated using numeric extensions (for example, from <code>utmountd.log.0</code> to <code>utmountd.log.9</code>).
Mass Storage Devices	<code>/var/opt/SUNWut/log/utstoraged.log</code>	Lists mass storage device events. The archived storage files are annotated using numeric extensions (for example, from <code>utstoraged.log.0</code> to <code>utstoraged.log.9</code>).
Messages	<code>/var/opt/SUNWut/log/messages</code>	Lists events from the server's DTUs, including details of registering, inserting, or removing smart cards. This file is updated daily. Archived files are stored on the server for one week annotated with numeric extensions (for example, from <code>messages.0</code> to <code>messages.5</code>).
Web Administration	<code>/var/opt/SUNWut/log/utwebadmin.log</code>	Lists web administration-related messages. The archived log files are annotated with numeric extensions.

Administration Tool

The Sun Ray Administration Tool (Admin GUI) is organized around primary Sun Ray objects, such as servers, sessions, desktop units, and tokens.

FIGURE 3-1 Admin GUI Navigation Hierarchy



The tab navigation model is easier to use than the previous navigation tree, and context-sensitive help makes it easier to manage a Sun Ray installation with little need for official documentation. Search functionality has been integrated into the main GUI tabs, and all tables can be sorted by clicking on the column headers.

Login Page

The default user name for the Admin GUI administration account is `admin`. The initial password is set at configuration time (see [“Configure Sun Ray Server Software” on page 47](#) of the *Sun Ray Server Software 4.1 Installation and Configuration Guide for Linux*).

To allow another user account or accounts to perform administrative functions, see [“Enabling Multiple Administration Accounts” on page 23](#) of this manual.

To access the Admin GUI, log in to your Sun Ray server’s console or to any DTU attached to it, start a browser, and type the following URL:

```
http://<localhost>:1660
```

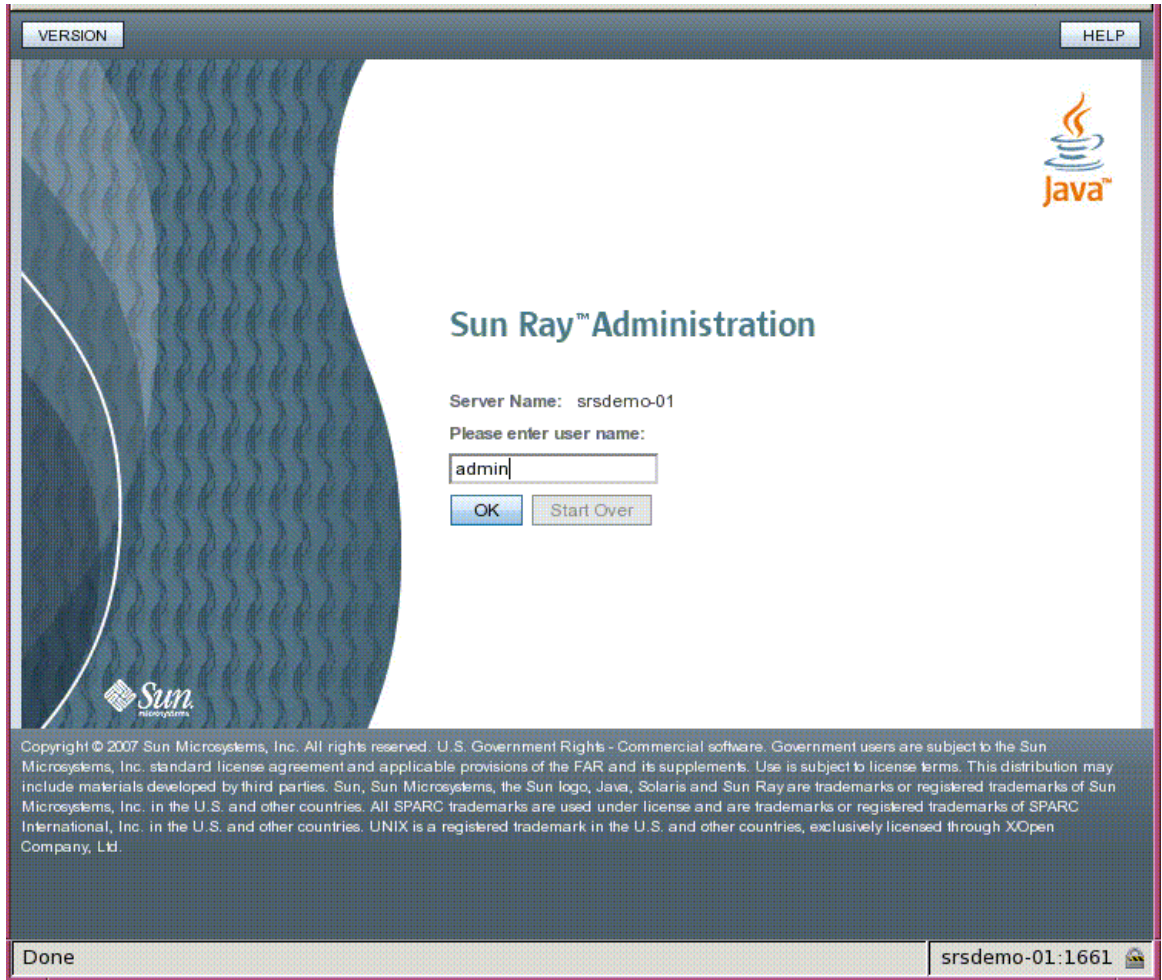
Note – If you chose a different port number when you configured the Sun Ray Server Software, substitute that number for 1660 in the URL above. If secure communication was enabled during SRSS configuration, the browser may be redirected to a secure port (default 1661).

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

- You are running a browser on a Sun Ray server or one of its DTUs.
- The browser is not using a different machine as an HTTP proxy server (to proxy the connection to the HTTP server (Web server)).

All actions performed within the Admin GUI that modify system settings are logged in an audit trail.

FIGURE 3-2 User Name Challenge Screen



To log in, enter the administrator user name `admin` on the user name challenge screen and click the OK button. On the password challenge screen, enter the administration password and click the OK button.

If the session is inactive for 30 minutes, you must log in again.

Note – To change the administration password, use the Advanced tab. See [“Data Store Password” on page 56](#).

Servers Tab

This tab provides the capability to list all the servers in the *failover group*. Clicking on a server name displays additional details for the selected server and offers links to display the host group's network connectivity status (that is, failover group status) or to list installed Sun Ray packages. It also simplifies restart options by offering buttons for *warm restart* or *cold restart* of Sun Ray services on a local or failover group-wide basis.

Note – A cold restart terminates all sessions on the selected server or servers before restarting; a warm restart does not terminate sessions.

FIGURE 3-3 Top-level Servers Tab

The screenshot shows the Sun Ray Administration web interface. At the top, there's a header with 'VERSION', 'LOG OUT', and 'HELP' buttons. Below that, it says 'User: admin Server: srsdemo-01' and 'Sun Ray Administration' with the Java logo. A navigation bar contains tabs for 'Servers', 'Sessions', 'Desktop Units', 'Tokens', 'Advanced', and 'Log Files'. The 'Servers' tab is active, showing a title 'Servers' and a description: 'This page lists all Sun Ray servers with the same group signature. Click on the server names to display additional details. >> More on Servers.' Below this is a 'Servers (2)' section with a toolbar containing checkboxes, a 'Warm Restart' button, a 'Cold Restart' button, and a refresh icon. A table lists the servers:

	Name	IP Address	Mode	LAN Connections	Start Time
<input type="checkbox"/>	srsdemo-01	10.6.133.148	Online	Enabled	Tue Jul 17 00:56:14 PDT 2007
<input type="checkbox"/>	srsdemo-02	10.6.133.171	Online	Enabled	Tue Jul 17 00:53:02 PDT 2007

At the bottom, the browser address bar shows 'https://srsdemo-01:1661/ut/faces/jsp/server/Servers.jsp#' and the page title is 'srsdemo-01:1661'.

Sessions Tab

This tab lists all the sessions, sorted by *user sessions* and *idle sessions*.

FIGURE 3-4 Sessions Tab Displays Active and Idle Sessions

The screenshot shows the Sun Ray Administration web interface. At the top, there is a navigation bar with 'VERSION', 'LOG OUT', and 'HELP' buttons. Below this, the user information 'User: admin Server: srsdemo-01' is displayed. The main title is 'Sun Ray Administration' with the Java logo and 'Sun Microsystems, Inc.' on the right. A secondary navigation bar contains tabs for 'Servers', 'Sessions', 'Desktop Units', 'Tokens', 'Advanced', and 'Log Files'. The 'Sessions' tab is active, showing a sub-header 'Sessions' and a brief description of the search functionality. Below the description is a search form with a dropdown menu set to 'All Servers', a text input field with an asterisk, and a 'Search' button. The main content area is titled 'Sessions (4)' and features a toolbar with checkboxes, a 'Terminate' button, and a refresh icon. A table lists the sessions with columns for Token, Owner, Unix ID, Server, Display, Status, and Desktop Unit. The table is divided into 'User Sessions' and 'Login Greeter/Idle Sessions' sections. The 'User Sessions' section contains four rows of data, all with a 'Connected' status. The 'Login Greeter/Idle Sessions' section shows 'No idle sessions found.' At the bottom of the interface, a status bar displays 'Done' and 'srsdemo-01:1661'.

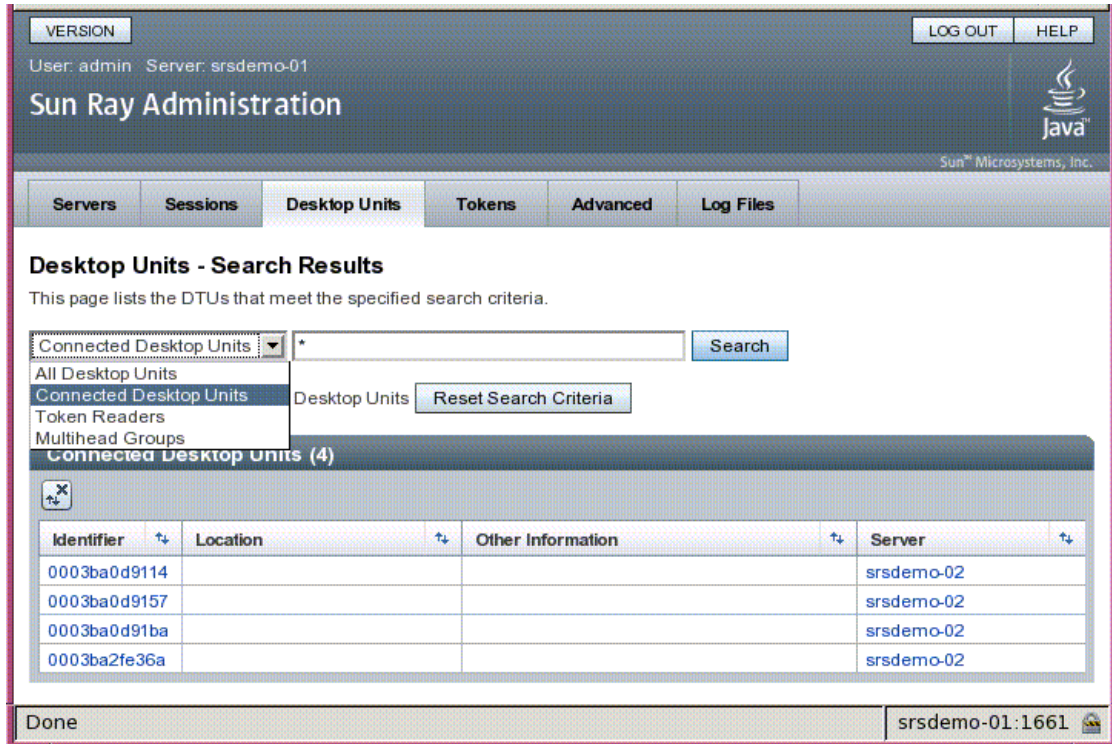
Token	Owner	Unix ID	Server	Display	Status	Desktop Unit
<input type="checkbox"/> MicroPayflex.5001430700130100		user02	srsdemo-02	2	Connected	0003ba0d9157
<input type="checkbox"/> MicroPayflex.5001be4a00130100		user01	srsdemo-02	5	Connected	0003ba0d91ba
<input type="checkbox"/> pseudo.0003ba0d9114	Sun Ray Tech Pubs	utku19	srsdemo-02	4	Connected	0003ba0d9114
<input type="checkbox"/> pseudo.0003ba2fe36a		utku20	srsdemo-02	3	Connected	0003ba2fe36a

The search functionality allows lookup of specific sessions, such as those running on a single server or sessions where a specific user is logged in. This tab also allows you to drill down for more information on any server or DTU as well as to select and terminate sessions.

Desktop Units Tab

The new desktop unit (DTU) management tab consolidates several DTU-related screens from the old Admin GUI.

FIGURE 3-5 Desktop Units Tab



The search drop-down menu provides access to the choices of listing all registered DTUs, listing all connected DTUs, displaying DTUs configured as token readers, or DTUs participating in multihead groups (see “Multihead Groups” on page 124). As on other tabs in the new Admin GUI, clicking on the identifier (MAC address) displays additional details for each DTU. All fields can be sorted by clicking their column headers.

▼ To Display Properties for a DTU

- Click any Desktop Identifier link on the Desktop Units tab.

▼ To Edit a DTU's Properties

1. Click any **Desktop Identifier** link on the **Desktop Units** tab, then click the **Edit** button.
2. Enter or modify data in the text boxes, and click the **OK** button to save the changes to the data store.

Multihead Groups

The multihead feature allows users to control separate applications on multiple Sun Ray displays with a single keyboard and mouse, attached to the primary DTU. The multihead feature also allows users to display and control a single application, such as a spreadsheet, on multiple displays (see [Chapter 9](#)).

Token Readers

A token reader is a Sun Ray DTU that is dedicated to reading a smart card and returning the card's ID, which you can associate with a user (card owner). Sun Ray DTUs configured as token readers display the token reader icon (see [“Token Reader Icons” on page 192](#)) instead of a login dialog box and do not support hotdesking when cards are inserted or removed. To manage token readers with the CLI, see [“Configuring and Using Token Readers” on page 32](#).

▼ To Set Up a Token Reader

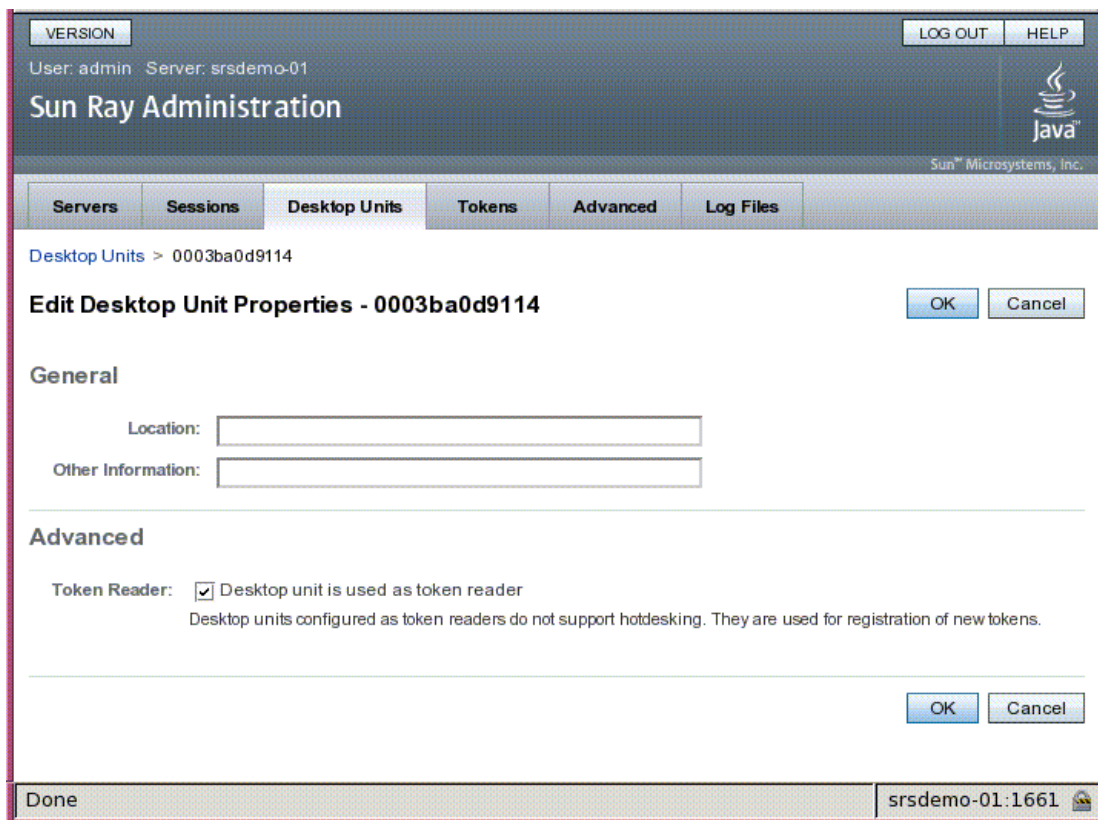
1. On the **Desktop Units** tab, click the **Identifier** of the DTU you want to use as a token reader.
2. On the **Desktop Unit Properties** tab, click **Edit**.
3. On the **Edit Desktop Unit Properties** tab, click the **Token Reader** checkbox.
4. Click the **OK** button.

The DTU you have selected is now set up to read smart card tokens.

5. **Restart Sun Ray services.**

The DTU is now a token reader.

FIGURE 3-6 Setting Up a Token Reader



▼ To Locate a Token Reader

- On the Desktop Units tab, select Token Readers from the drop-down list and click the Search button.

The default is to search for all possible matches. You may specify other search criteria in the Search text box.

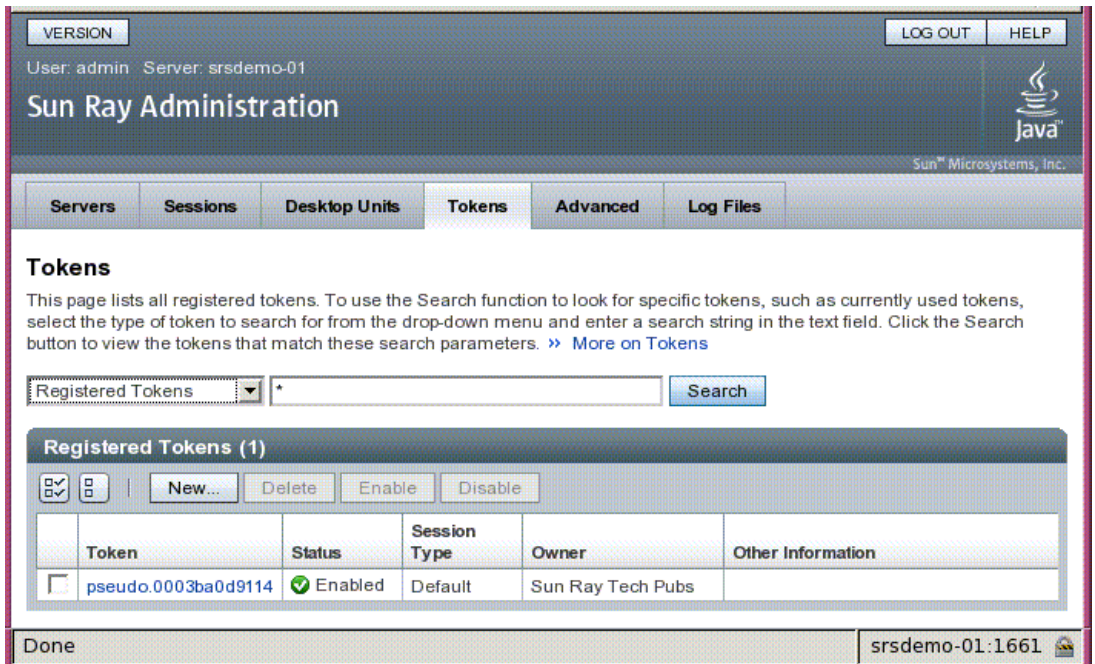
▼ To Get Information on a Token Reader

- Click the Token Readers Identifier link after searching for token readers on the Desktop Units tab.

Tokens Tab

The Admin GUI manages *tokens* associated with users and *pseudo-tokens* associated with DTUs through the Tokens tab. Smart cards can be registered to specific users, considered as *token owners*. *Alias tokens* allow a token owner to use more than one token for access to the same session.

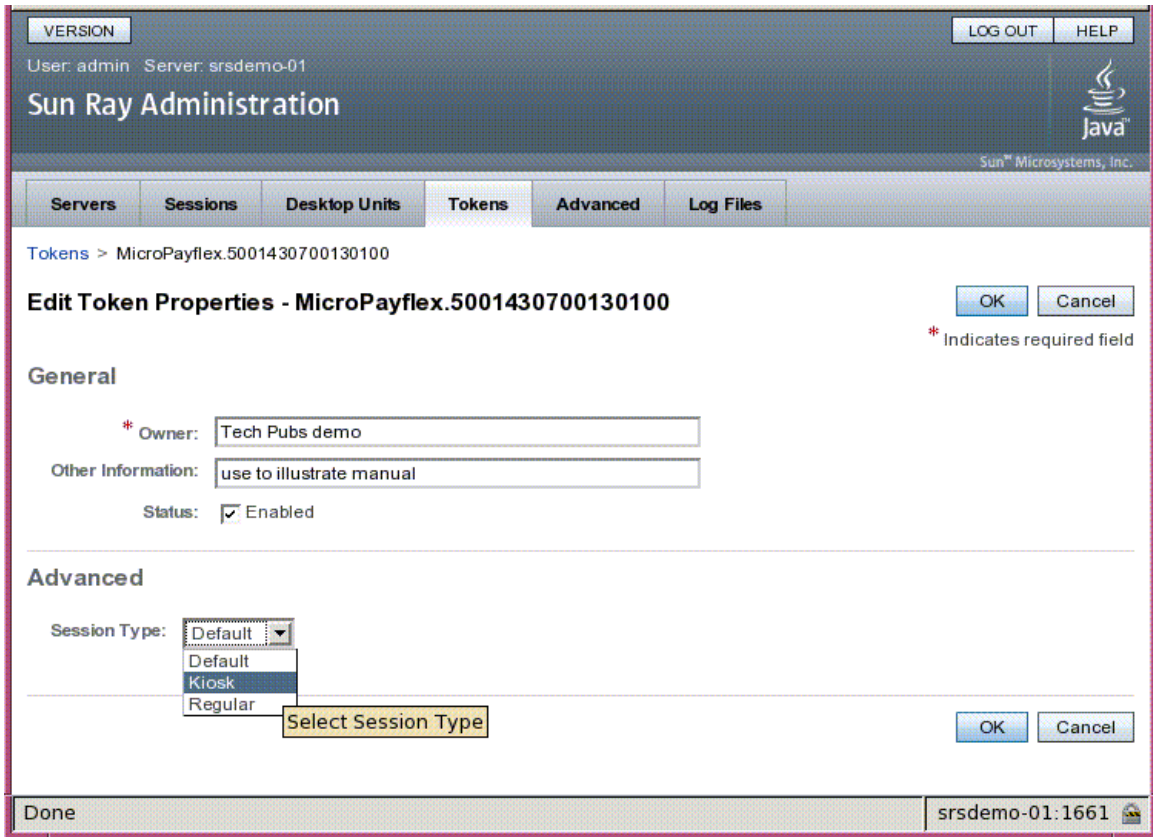
FIGURE 3-7 Tokens Tab



Note – The Tokens tab is not used to administer *token readers*, which are DTUs set up to read smart cards and retrieve their token IDs. See “[Token Readers](#)” on page 45.

The Edit Token Properties page (see [FIGURE 3-8](#)) and the Add New Token page (see [FIGURE 3-9](#)) can be used to enable session types, such as Kiosk or regular desktop sessions, to control what type of desktop is displayed for each user token or class of user token.

FIGURE 3-8 Edit Token Properties



▼ To Register a Token

1. Click on any token on the **Tokens** tab to display that token's properties (see [FIGURE 3-8](#)).
2. To register a token, click the **New** button on the **Tokens** tab to display its properties (see [FIGURE 3-9](#)).

You can now enter an identifier or select a token reader.

FIGURE 3-9 Add New Token Page

VERSION LOG OUT HELP

User: admin Server: srsdemo-01

Sun Ray Administration

Sun Microsystems, Inc.

Servers Sessions Desktop Units **Tokens** Advanced Log Files

Add New Token

Specify the details of the new token. The token identifier can either be entered manually or retrieved automatically from a configured token reader. Select a token reader from the drop-down list below, then insert a smart card, and click OK.

Identifier: Read Identifier from Token Reader:

Enter Token Identifier Manually:

Owner:

Other Information:

Advanced

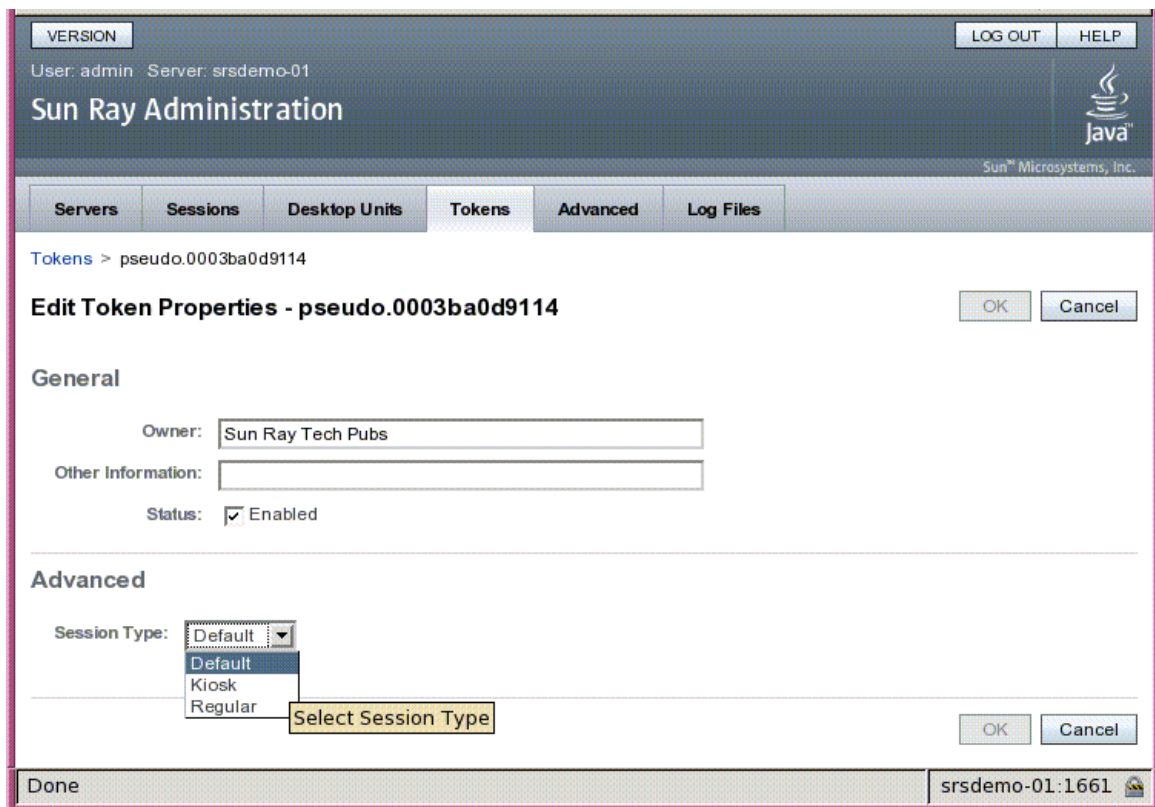
Session Type:

Done srsdemo-01:1661

▼ To Register a Pseudo-Token

1. Click on any Identifier on the Desktop Units tab to view properties for that DTU.
2. On the Desktop Unit Properties page, click View Token Details.
3. Click the Edit button to enter details such as ownership and to specify a session type: Default, Kiosk, or Regular (see [FIGURE 3-10](#)).

FIGURE 3-10 Pseudo-token Properties



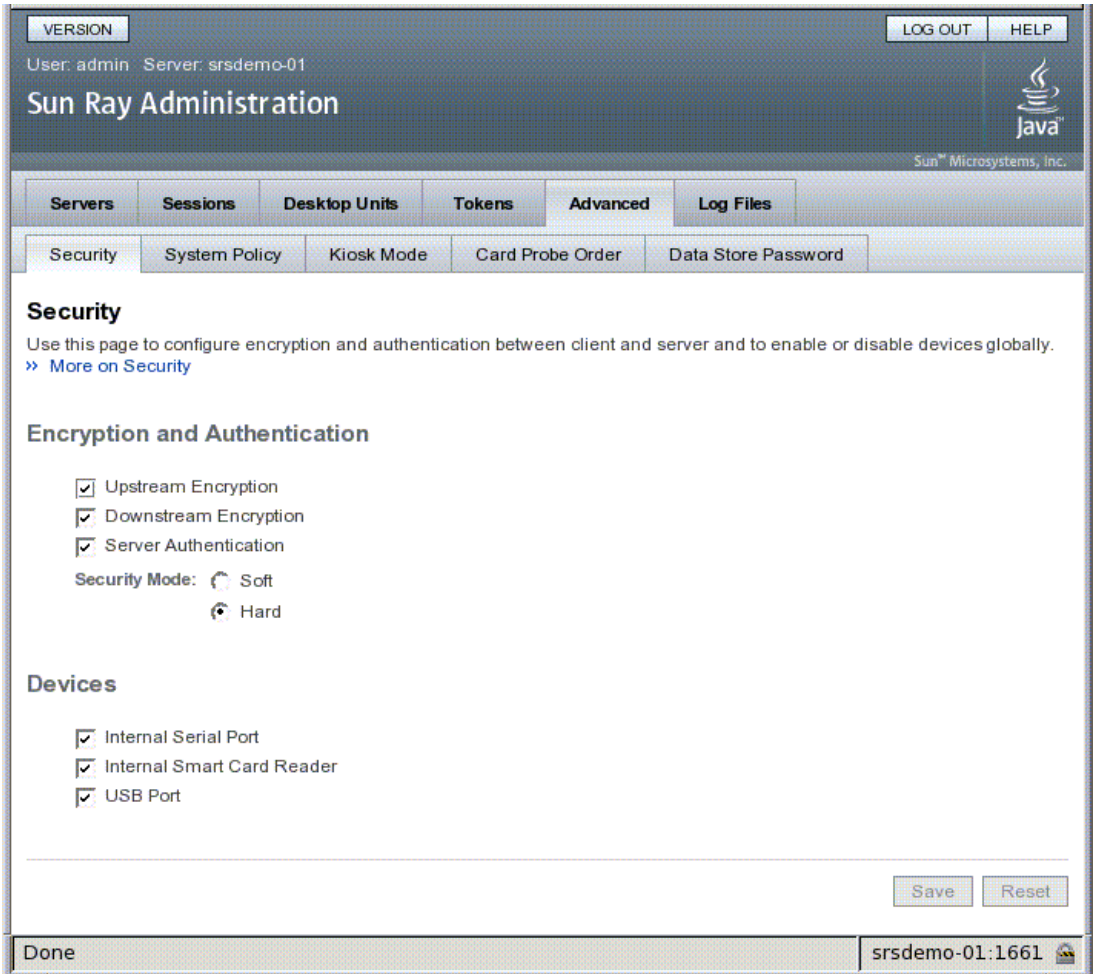
▼ To Enable, Disable, or Delete a Token

1. Click the check box next to the token's identifier on the Token Properties page.
2. Click the Enable, Disable, or Delete button.

Advanced Tab

This tab provides sub-tabs for group-wide settings, described below.

FIGURE 3-11 The Security Tab



Security Settings

Security settings include encryption of communication between DTU and server, server authentication, security mode, and device access, as shown in [FIGURE 3-11](#).

All Sun Ray device services are enabled by default. Sun Ray device services include USB devices connected through USB ports, internal serial ports, and internal smart card readers on the Sun Ray DTU. To enable or disable these services, use the `utdevadm` command line tool (see [“Enabling and Disabling Device Services”](#) on [page 26](#)) or the Admin GUI as shown in this section.

For a description of encryption and authentication options, see [“Encryption and Authentication”](#) on [page 73](#). For devices, see [“Peripherals for Sun Ray DTUs”](#) on [page 59](#).

System Policy

Use this tab to regulate authentication manager policy settings, such as access for card users and non-card users, and enabling Kiosk mode and the multihead feature, for each Sun Ray server, or system. An additional checkbox at the bottom of this tab enables users to access sessions directly while hotdesking. Checking this box effectively bypasses the Remote Hotdesking Authentication (RHA) feature and may present a security risk under some circumstances, so the default is to leave RHA enabled.

FIGURE 3-12 System Policy Tab

The screenshot shows the Sun Ray Administration interface. At the top, there is a header with 'VERSION', 'LOG OUT', and 'HELP' buttons. Below the header, the user is identified as 'admin' on server 'srsdemo-01'. The main navigation bar includes tabs for 'Servers', 'Sessions', 'Desktop Units', 'Tokens', 'Advanced', and 'Log Files'. A secondary navigation bar contains 'Security', 'System Policy', 'Kiosk Mode', 'Card Probe Order', and 'Data Store Password'. The 'System Policy' section is active, showing a 'Save' and 'Reset' button. The page content is divided into three sections: 'Card Users', 'Non-Card Users', and 'Multihead'. Each section has radio buttons for 'Access' and checkboxes for 'Kiosk Mode' and 'Mobile Sessions'. The 'Multihead' section has a checked checkbox for 'Multihead Feature'.

VERSION LOG OUT HELP

User: admin Server: srsdemo-01

Sun Ray Administration

Sun Microsystems, Inc.

Servers Sessions Desktop Units Tokens Advanced Log Files

Security System Policy Kiosk Mode Card Probe Order Data Store Password

System Policy Save Reset

This page allows you to configure group-wide policies. Some policy settings combinations are not allowed, and the settings are disabled accordingly to enforce these rules. For example, it is not possible to completely disable access for smart card and non-smart card users at the same time. [» More on System Policy](#)

Card Users

Access: None
 All Users
 Users with Registered Tokens
 Self-Registration Allowed
 User Account Authentication Required

Kiosk Mode: Enabled

Non-Card Users

Access: None
 All Users
 Users with Registered Tokens
 Self-Registration Allowed
 User Account Authentication Required

Kiosk Mode: Enabled

Mobile Sessions: Enabled
For convenience, enabling mobile sessions automatically activates the exit option for mobile sessions.
 Exit from Mobile Sessions Allowed

Multihead

Multihead Feature: Enabled

Save Reset

Kiosk Mode Configuration

To use Kiosk Mode, enable it on the System Policy tab (see [FIGURE 3-12](#)) and use the Kiosk Mode tab for setup. For a more detailed description, see “[Kiosk Mode](#)” on [page 135](#) of this manual

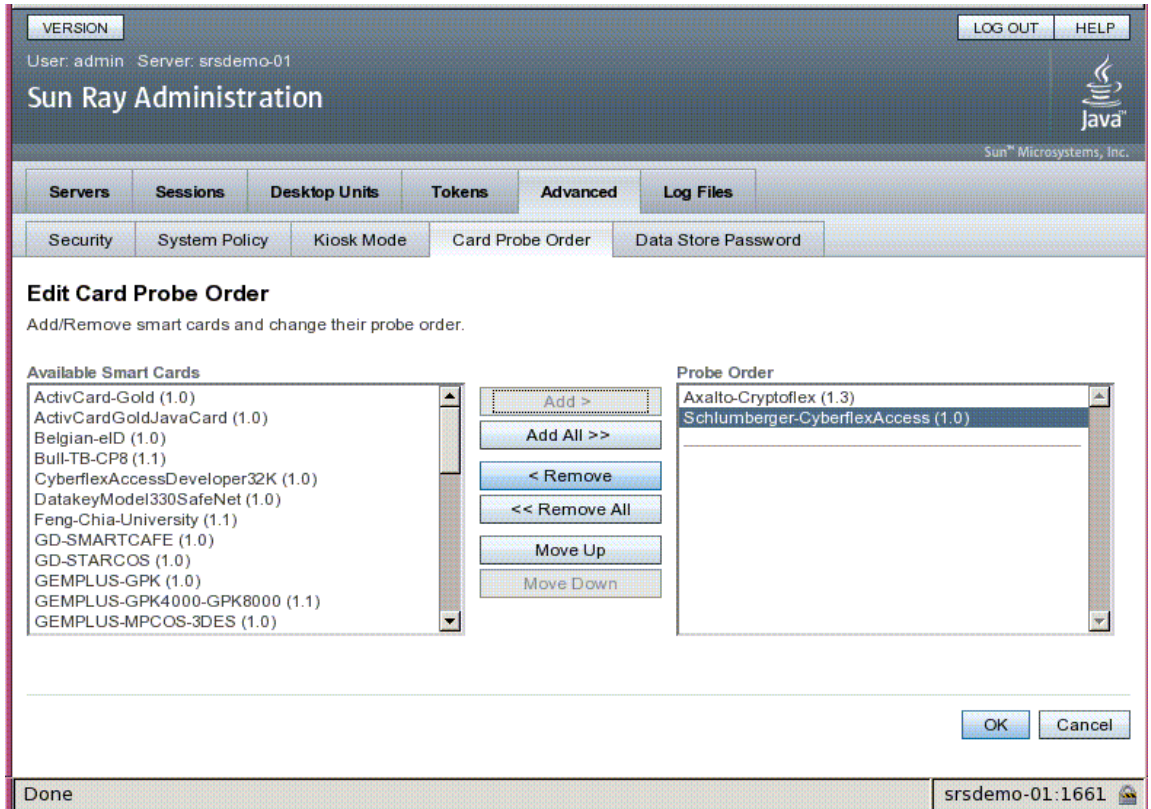
FIGURE 3-13 Kiosk Mode Tab

The screenshot shows the Sun Ray Administration web interface. At the top, there is a header with 'VERSION', 'LOG OUT', and 'HELP' buttons. Below this, the user information 'User: admin Server: srsdemo-01' is displayed. The main title is 'Sun Ray Administration' with the Java logo and 'Sun Microsystems, Inc.' on the right. A navigation menu contains tabs for 'Servers', 'Sessions', 'Desktop Units', 'Tokens', 'Advanced', 'Log Files', 'Security', 'System Policy', 'Kiosk Mode', 'Card Probe Order', and 'Data Store Password'. The 'Kiosk Mode' tab is selected and highlighted. The main content area is titled 'Kiosk Mode' and includes 'Edit' and 'Delete' buttons. A descriptive paragraph states: 'This page allows you to limit the user's desktop to certain session types (for example, full-screen Windows Connector session, JDS or CDE desktop session) or applications. >> [More on Kiosk Mode.](#)' Below this, several configuration parameters are listed: 'Session: Sun Ray Connector for Windows OS', 'Timeout: 12000 seconds', 'Maximum CPU Time:', 'Maximum VM Size:', 'Maximum number of Files:', 'Maximum File Size:', 'Locale:', and 'Arguments: tswin2003'. At the bottom of the configuration area, there are 'Edit' and 'Delete' buttons. The status bar at the very bottom shows 'Done' on the left and 'srsdemo-01:1661' on the right.

Smart Card Probe Order

The information provided about smart cards is extracted from vendor-supplied configuration files. These configuration files are located in the directory: `/etc/opt/SUNWut/smartcard`. Configuration files must be formatted correctly, and file names must end with a `.cfg` suffix, such as `acme_card.cfg`.

FIGURE 3-14 Edit Smart Card Probe Order



Smart cards are probed in the order in which they appear in this list. As you add more cards, you can move those used most often to the top of the list.

Data Store Password

The administrator's password allows you to use the Admin GUI to access and change Sun Ray administration data.

FIGURE 3-15 Use the Data Store Password Tab to Change the Admin Password

The screenshot shows the Sun Ray Administration web interface. At the top, there is a header with 'VERSION', 'LOG OUT', and 'HELP' buttons. Below this, it displays 'User: admin Server: srsdemo-01' and the 'Sun Ray Administration' title. A navigation menu includes 'Servers', 'Sessions', 'Desktop Units', 'Tokens', 'Advanced', and 'Log Files'. The 'Data Store Password' tab is selected. The main content area is titled 'Data Store Password' and contains the following text: 'This page allows you to change the password of the administrative user for privileged access to the Sun Ray data store. >> [More on Data Store Password](#)'. There are three password input fields, each with an asterisk indicating it is required: '* Current Password:', '* New Password:', and '* Confirm New Password:'. A legend indicates '* Indicates required field'. Below the fields is a 'Confirm New Administration Password' button, and 'Save' and 'Reset' buttons are at the bottom right. The footer shows 'Done' and 'srsdemo-01:1661'.

The Data Store Password tab allows you to change the password for the admin account. The password was set at configuration time (see “Configure Sun Ray Server Software” in the *Sun Ray Server Software 4.1 Installation and Configuration Guide for Linux*).

This tab does not allow you to change UNIX user passwords.

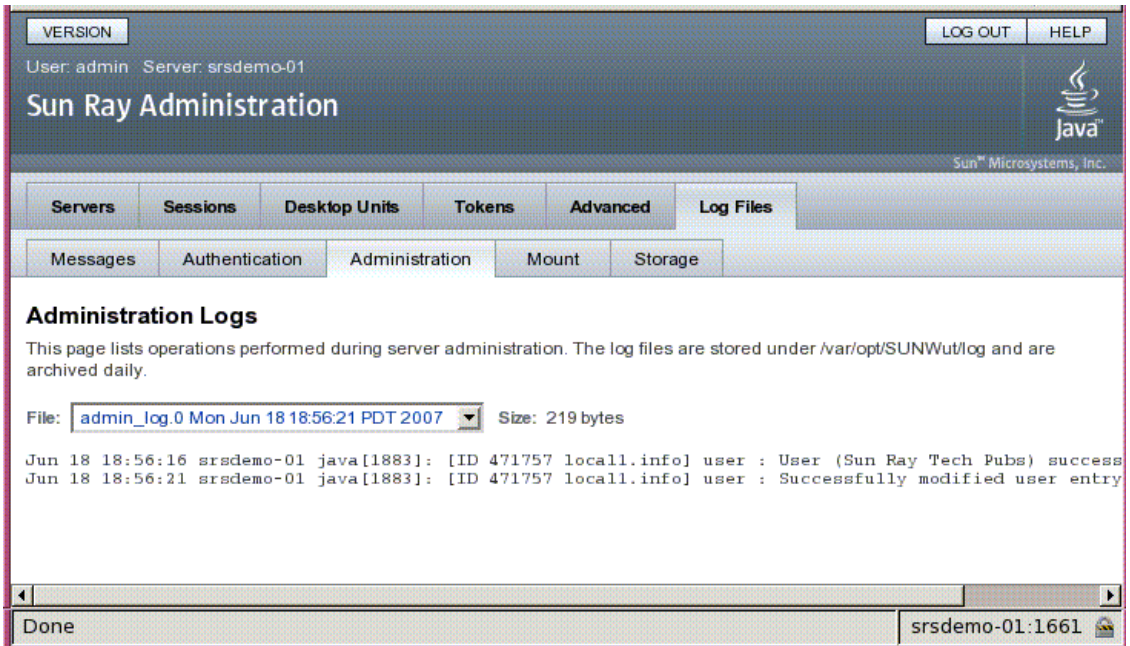
Note – Every server in a failover group must use the same password for the admin account.

The layout of the data store is described in “Managing User Data in the Sun Ray Data Store” on page 22. To allow other UNIX accounts to perform administrative functions, see “Enabling Multiple Administration Accounts” on page 23.

Log Files Tab

This tab provides sub-tabs for displaying the various log files recording events such as system messages, authentication logs, server administration events, mount logs, and storage related actions. To locate Sun Ray log files from the command line, see “Examining Log Files” on page 38.

FIGURE 3-16 Sample Administration Log



Peripherals for Sun Ray DTUs

This chapter contains information about selected USB, parallel, and serial devices and printing setup from Sun Ray DTUs.

- “Device Nodes and USB Peripherals” on page 59
- “Mass Storage Devices” on page 62
- “Attached Printers” on page 64
- “libusb” on page 66

Serial peripherals enable RS-232-style serial connections to the Sun Ray DTU. Parallel peripherals enable printing and come in two types: adapters and direct USB-connected printers. Third-party adapters are useful for supporting legacy serial and parallel devices. Sun Ray Server Software recognizes parallel printers with adapters as USB printers.

For a list of supported serial and parallel devices and adapters, see:
http://www.sun.com/io_technologies/sunray/sunray0.html

Device Nodes and USB Peripherals

Sun Ray Server Software creates a device directory called `IEEE802.MACID` in the `/tmp/SUNWut/units` directory. This directory contains the MAC address for each DTU on the interconnect. The `IEEE802.MACID` directory for each DTU contains `dev` and `devices` directories. The Sun Ray `dev` directory contains a representation of the logical topology of the devices connected to the DTU. The Sun Ray `devices` directory contains a representation of the physical topology of some of the devices connected to the DTU.

Note – Sun Ray Server Software does not create device nodes for every USB device. Some USB device drivers export their device interfaces through other mechanisms than a traditional UNIX device node.

Directories correspond to buses and hubs, and files correspond to ports. Hub directories are named according to the port on the upstream hub into which they are attached.

Device Nodes

In Sun Ray `devices`, device nodes are created for each serial or printer port on an attached USB device. The device nodes are created in the `hub` directory corresponding to the hub to which they are attached. They are named:

```
manufacturer_name, model_name@upstream_hub_port
```

If the USB device has multiple identical ports (for example, two serial ports), the name is followed by `:n` where `n` is a numerical index, starting at 1.

The following is a typical device node path:

```
/tmp/SUNWut/units/IEEE802.MACID/devices/usb@1/hub@1/\nmanufacturer_name, model_name@3:1
```

TABLE 4-1 Definitions of Naming Conventions

Term	Definition
<i>physical topology</i>	The <i>physical topology</i> is <code>hub@port/hub@port</code> and so on. The <i>port</i> refers to the port on the parent hub into which the device or child hub is plugged.
<i>printer name 1, terminal name 1</i>	The printer and terminal name in the Sun Ray <code>devices</code> directory is <code>manufacturer, model@port</code> with a colon separating the numerical index when the string just described is not unique in the directory.
<i>printer name 2, terminal name 2</i>	The printer and terminal name in the Sun Ray <code>dev</code> directory is the manufacturer and serial number concatenated with an alphabetic index when the serial number is not unique.

Device Links

Device links are created under the `dev` directory. A link to each serial node is created in `dev/term`, and a link to each parallel node is created in `dev/printers`.

Typical device links are:

```
/tmp/SUNWut/units/IEEE802.080020cf428a/dev/term/manufacturer_name-67a  
/tmp/SUNWut/units/IEEE802.080020cf428a/dev/printers/1608b-64
```

```
manufacturer_name-serial_numberindex
```

where *index* is an increasing alphabetical character, starting at a.

If the manufacturer name is not available, the USB vendor and product ID numbers are used for the name of the device link.

Device Node Ownership

Some device nodes are owned by the user whose session is active on the DTU, while others may be owned by root or by other users that may have had previously active sessions on the DTU. Device permissions, access controls and ownership rules are determined by the class of device. For serial and parallel devices, only the user whose session is active on the DTU or the superuser have permission to use the attached device. If there is no user with an active session, superuser owns the serial and parallel device nodes. This rule may not hold for other classes of USB devices connected to the DTU.

Hotdesking and Device Node Ownership

The following description of the behavior of USB devices when sessions are connected and disconnected from a DTU applies only to USB serial and USB parallel devices. Other device classes may have different semantics regarding ownership and device lease times.

Changing the active session on a DTU changes the ownership of the device nodes to the user associated with the new session. A session change occurs whenever a user:

- Inserts or removes a smart card from a DTU
- Logs into a session

In a failover environment, you can use the `utselect` or `utswitch` command to change a session. A session change causes all devices currently open by a non-root user to be closed after 15 seconds. Any input or output to or from any affected device results in an error. Devices currently opened by the superuser remain unaffected by the session change.

Note – When a session is changed, any input or output in progress on a device node opened by a non-root user is cancelled after 15 seconds. If the original session is restored within 15 seconds, the ownership is not relinquished, and input and output continue uninterrupted.

Mass Storage Devices

Device Nodes and Links

Mass storage device nodes are block special nodes. They are created in the `dev/dsk` directory. Note that for mass storage devices, device nodes are not created in the devices directory and no device links are created.

Device nodes are named with a partition identifier suffix. The device node representing the whole disk does not have such a suffix. For example:

- `disk3p2` represents partition 2 of `disk3`.
- `disk3` represents the whole disk.

Disk operations such as `eject` should be directed at the whole disk. Partition operations such as `mount` should be directed at individual partitions. See [TABLE 4-2](#) for examples.

Mount Points

When a mass storage device is plugged into the DTU, if it has an OS-recognizable file system, it is automatically mounted on a directory under the user's mount parent directory. The mount parent directory is located in `$DTDEVROOT/mnt/`. The user can also locate mount points by using the `-l` option to the `utdiskadm` command:

```
% utdiskadm -l
```

Device Ownership and Hotdesking

When the user's session disconnects from the DTU, the user loses access rights to the mass storage device, and all pending I/O to the device is aborted. This can cause the data on the device to be corrupted. Users should use `utdiskadm -r` to unmount all filesystems safely before hotdesking or unplugging the disk from the DTU. They should also close all references to files and directories in the mount point to ensure that the device in question is not busy.



Caution – Linux does not immediately write data to disks. Failure to run `utdiskadm -r` before unplugging mass storage devices will cause loss of data. Make sure your users run `utdiskadm -r` before they unplug any mass storage device.

```
% utdiskadm -r device_name
```

Common Disk Operations

TABLE 4-2 is a summary of common disk operations and the commands used to perform them. Refer to the man pages for more information on the individual commands.

TABLE 4-2 Commands for Common Disk Operation on Linux Platforms

OPERATION	COMMAND	DEVICE NAME ARGUMENT EXAMPLES
create file system	<code>mkfs (8)</code>	path of partition <code>\$UTDEVROOT/dev/dsk/disk3p1</code>
mount	<code>utdiskadm -m</code>	partition name <code>disk3p1</code>
unmount	<code>utdiskadm -u</code>	mount point <code>\$DTDEVROOT/mnt/label1</code>
prepare to unplug	<code>utdiskadm -r</code>	device alias <code>disk3</code>
eject media	<code>utdiskadm -e</code>	device alias <code>disk3</code>
check for media	<code>utdiskadm -c</code>	device alias <code>disk3</code>

TABLE 4-2 Commands for Common Disk Operation on Linux Platforms (*Continued*)

OPERATION	COMMAND	DEVICE NAME ARGUMENT EXAMPLES
create fdisk table	<code>fdisk(8)</code>	path of whole disk <code>\$UTDEVROOT/dev/dsk/disk3</code>
repair file system	<code>fsck(8)</code>	path of partition <code>\$UTDEVROOT/dev/dsk/disk3p1</code>
display file system capacity	<code>df -k</code>	mount point <code>\$DTDEVROOT/mnt/label1</code>
list devices	<code>utdiskadm -l</code>	none

Attached Printers

Sun Ray Server Software supports PostScript™ printers connected directly to a USB port on the Sun Ray DTU or connected through a USB-to-parallel port adapter. For non-PostScript printer support, refer to [“Non-PostScript Printers” on page 66](#).

Note – The `lp` subsystem opens the device node as superuser for each print request, so print jobs are not affected by hotdesking.

Printer Setup

The following generic instructions may vary slightly from one operating system implementation to another but should provide enough information to enable an administrator to set up basic printing services.

▼ To Set Up a Printer

1. **Log in as superuser on a Sun Ray DTU.**
2. **To determine the MAC address of the DTU, press the three audio option keys to the left of the power key in the upper right corner of the keyboard.**

The alphanumeric string displayed above the connection icon is the MAC address.

3. To locate the Sun Ray DTU, type:

```
# cd /tmp/SUNWut/units/*MAC_address
# pwd
/tmp/SUNWut/units/IEEE802.MACID/
```

The path to the extended MAC address for your particular Sun Ray DTU is displayed.

4. Locate the port for the printer by typing:

```
# cd dev/printers
# pwd
/tmp/SUNWut/units/IEEE802.MACID/dev/printers
#ls
printer-node-name
```

5. In the directory, locate the printer node.

6. Use the Linux administration tools to set up the printer.

Make sure to choose Other so that you can enter the device node from [Step 4](#) above.

7. To verify that the printer has been set up correctly, type:

```
# lpstat -d printername
```

Note – For SLES 10, perform the following additional steps:

8. Create a soft link to the Sun Ray printer node in /dev/usb.

For example, if the device node is
/tmp/SUNWut/units/IEEE802.<mac-address>/dev/printers/<device node>,
then use the following command:

```
# ln -s \  
/tmp/SUNWut/units/IEEE802.<mac-address>/dev/printers/<device node> \  
/dev/usb/sunray-printer
```

Use this soft link (/dev/usb/sunray-printer) as the Device URI while creating the print queue.

9. Update /etc/cups/cupsd.conf to set the RunAsUser property to No.

10. Restart the cups daemon.

```
# /etc/init.d/cups restart
```

Non-PostScript Printers

Printers that do not use PostScript, such as engineering plotters, are best supported by third-party software. Low-cost inkjet printers require third-party software such as:

- Easy Software's ESP PrintPro, available from <http://www.easysw.com>
- Ghostscript, available from <http://www.ghostscript.com>
- Vividata PShop, available from <http://www.vividata.com>

Check with the vendors for pricing and the precise printer models supported.

libusb

libusb is an Open Source user space USB API that enables applications to access USB devices. It has been implemented for a number of operating environments including Linux, BSD Unix, and Solaris.

The Sun Ray libusb plugin `libusb.so.1` provides Sun Ray-specific support for libusb in Linux environments.

The `SUNWlibusb` RPM delivers the Sun Ray libusb plugin `libusb.so.1` in `/opt/SUNWut/lib`. To build applications, use the `usb.h` header file from the existing server-side Linux libusb RPM.

The `libusb` man page provided with SRSS 4.1 for Linux discusses options available for using the Sun Ray libusb plugin alongside the Linux server-side libusb support.

The Open Source libusb-based applications provided with the standard Linux distributions can be used to drive USB-based devices attached to Sun Ray DTUs. For example, for Sane, see www.sane-proj.org; for Gphoto, see www.gphoto.org.

Note – Sane can be used in Sun Ray implementations if built with threads enabled. Sane binaries with threads enabled are available at the Sun Download Center (SDLC), or they can be built from source.

Hotdesking (Mobile Sessions)

- The Sun Ray system is designed to enable session mobility, or hotdesking, with or without smart cards. Every Sun Ray DTU is equipped with a smart card reader. Remote Hotdesk Authentication

Note – Non-Smart Card Mobility is implemented only on Solaris platforms.

Regional Hotdesking

Regional hotdesking can be enabled by means of multiple failover groups. Multiple failover groups are useful for various reasons, such as:

- Availability
It is sometimes advantageous to have multiple, geographically-separate locations, each with a failover group, so that if an outage occurs at one location, another location can continue to function.
- Organizational Policies
Some sites have different administrative policies at different locations. It can be advantageous to keep separate failover groups at these locations.

Regional hotdesking, sometimes referred to as Automatic Multi-Group Hotdesking (AMGH), is useful when an enterprise has multiple failover groups and users who move from one location to another who wish to gain access to their existing session wherever they roam. The following sections describe regional hotdesking. For further technical detail, please refer to the `utamghadm(8)`, `ut_amgh_get_server_list(3)`, and `ut_amgh_script_interface(3)` man pages.

Note – Regional hotdesking is not enabled for multihead groups.

Functional Overview

Once regional hotdesking is configured, user login information and sessions are handled as follows:

1. When a smart card is inserted or removed from the system or a user logs in via the greeter GUI, parameters such as the user name (if known at the time), smart card token, and terminal identifier are passed to a piece of site integration logic.
2. The site-integration software uses these parameters to determine to which Sun Ray servers it should direct the Sun Ray DTU.
3. If the smart card token is associated with a local session, then that session gets preference, and regional hotdesking is not invoked.
4. Otherwise, the regional hotdesking software redirects the Sun Ray DTU to connect to the appropriate Sun Ray server.

Thus, if the user has an existing session, the DTU connects to that session; if not, the regional hotdesking software creates a new session for that user.

Site Requirements

To utilize regional hotdesking, a site must provide some site integration logic that can utilize enterprise data to determine which users or Sun Ray DTUs should connect to which failover groups. This is ordinarily provided through the use of a dynamic C library or a shell script that implements a particular interface used by regional hotdesking software. SRSS provides some reference code that a site administrator can use as an example or adapt as required. An administrator must configure the regional hotdesking software to utilize a specified library or shell script, then implement the PAM stack of the login applications, as described below.

Note – To ensure continuous operation, be sure to include enough servers in the target group to provide availability for session location and placement in the event that a particular server becomes unavailable. Two servers should be minimally sufficient for most sites; three servers provide a conservative margin of error.

Providing Site Integration Logic

To determine where given Sun Ray DTUs or users should be connected when creating or accessing sessions, the administrator must utilize enterprise data. Sun Ray Server Software 4.1 includes for this purpose:

- man pages, such as `ut_amgh_get_server_list(3)`, which describe the appropriate C API for a shared library implementation
- A shell-script API, `ut_amgh_script_interface(3)`, which can be used as an alternative.
- Reference C code and script code, located at `/opt/SUNWutref/amgh`. This code can serve as example or be directly adapted for use.
- A functional Makefile.

▼ To Configure a Site-specific Mapping Library

The administrator for each site must determine what mapping library to use. It may be a site-specific implementation, as described above, or one of the sample implementations provided with the SRSS software.

Use the `/opt/SUNWut/sbin/utamghadm` command to configure the regional hotdesking software to use this library.

1. To configure the token-based mapping implementation provided as a sample, execute the following:

```
# /opt/SUNWut/sbin/utamghadm -l /opt/SUNWutref/amgh/libutamghref_token.so
```

2. To configure the user name-based mapping implementation provided as a sample, execute the following:

```
# /opt/SUNWut/sbin/utamghadm -l /opt/SUNWutref/amgh/libutamghref_username.so
```

3. To configure a script-based back-end mapping (for example, the token-and-user name-combination-based mapping sample), use the `-s` option to this command:

```
# /opt/SUNWut/sbin/utamghadm -s /opt/SUNWutref/amgh/utamghref_script
```

4. Do a cold restart of the SRSS services using either the `utrestart` CLI or the Admin GUI.

Token Readers with Regional Hotdesking

To utilize token readers with regional hotdesking based on Sun Ray *pseudo-tokens*, use the Site-specific Mapping Library to produce the desired behavior for them.

Configured token readers should have the following value formats:

*Key	*Value
insert_token	pseudo.<MAC_address>
token	TerminalId.<MAC_address>

If a registered policy is in place, use the `insert_token` key instead of the `token` key, which is not globally unique.

Note – The RHA security feature does not affect token readers. It is assumed that token readers are deployed in physically secure environments.

▼ To Configure the Sample Data Store

Each site must configure a data store to contain site-specific mapping information for regional hotdesking. This data store is used by the site mapping library to determine whether regional hotdesking should be initiated for the parameters presented. The data store can be a simple flat file. The sample implementations included with the SRSS require a simple flat file configuration.

- **Create the back-end database file under**

`/opt/SUNWutref/amgh/back_end_db` on the Sun Ray server:

- a. For a token-based mapping, use entries of the form:**

```
token=XXXXXXX [username=XXXXX] host=XXXXX
```

- Comments (lines beginning with #) are ignored.
- User name is optional. If the same token is associated with more than one non-null user name, an error is returned.

- b. For a user name-based mapping, use entries of the form:**

```
username=XXXXX host=XXXXX
```

- Comments (lines beginning with #) are ignored,
- Key/value pairs other than those mentioned above are ignored.

- The order of key/value pairs is not significant.

c. For a combined mapping, use entries of the form:

```
Any combination of TOKEN BASED and USERNAME BASED lines.
```

- Comments (lines beginning with #) are ignored,
- A token match is attempted first.
- If none is made (or if no user name is included in the matches) the user is prompted for a user name.
- A lookup is made for this user name. If there is no match, a local session is created; otherwise, the Sun Ray DTU is forwarded to the first host reported as available.

A sample line for this file would look like the following:

```
token=MicroPayflex.5001436700130100 username=user1 host=ray-207
```

▼ To Disable Regional Hotdesking

1. To disable AMGH configuration for a group, run the following command:

```
% /opt/SUNWut/sbin/utamghadm -d
```

2. Do a cold restart of the SRSS services using either the utrestart CLI or the Admin GUI.

Remote Hotdesk Authentication (RHA)

The default behavior of the SRSS Authentication Manager now requires users to be authenticated when hotdesking, i.e., upon reconnection to an existing session.

The Authentication Manager asks the Session Manager to create a temporary new session for this purpose. After the user has been successfully authenticated, the Sun Ray DTU is connected directly to the user's session. This authentication does not apply to anonymous Kiosk Mode, and Sun Ray Server Software can be configured to turn this security policy feature off if desired.

Note – The RHA security feature does not affect token readers. It is assumed that token readers are deployed in physically secure environments.

▼ To Disable or Re-enable RHA Using the Admin GUI

See “[System Policy](#)” on page 52 for a description illustration of the RHA check box.

▼ To Disable RHA from a Command Line

1. To disable RHA from a command line, use the **-D** option to **utpolicy**.

For example, if your policy allows smartcards and non-smartcard logins and FOGs, use the following command and options to disable RHA:

```
# utpolicy -a -z both -g -D
```

2. Do a cold restart of the SRSS services:

```
# utrestart -c
```

▼ To Re-enable RHA from a Command Line

1. To re-enable RHA from a command line, restate your policy using **utpolicy** without the **-D** option.

For example, to reinstate a policy that allows smartcards and non-smartcard logins and FOGs with RHA, use the following command and options:

```
# utpolicy -z both -g
```

2. Do a cold restart of the SRSS services:

```
# utrestart -c
```


Encryption and Authentication

Sun Ray Server Software provides interconnect security. Two main aspects of this feature are:

- Traffic encryption between the Sun Ray client and server
- Sun Ray server-to-client authentication

Introduction

In earlier versions of Sun Ray Server Software, data packets on the Sun Ray interconnect were sent “in the clear”. This made it easy to “snoop” the traffic and recover vital and private user information, which malicious users might misuse. To avoid this type of attack, Sun Ray Server Software allows administrators to enable traffic encryption. This feature is optional; the system or network administrator can configure it based on site requirements.

The ARCFOUR encryption algorithm, selected for its speed and relatively low CPU overhead, supports a higher level of security between Sun Ray services and Sun Ray desktop units. In the Sun Ray Server Software 2.0 and later releases, only the Xserver traffic was encrypted.

Encryption alone does not provide complete security. It is still possible, if not necessarily easy, to spoof a Sun Ray server or a Sun Ray client and pose as either. This leads to the man-in-the-middle attack, in which an impostor claims to be the Sun Ray server for the clients and pretends to be client for the server. It then goes about intercepting all messages and having access to all secure data.

Client and server authentication can resolve this type of attack. This release offers server-side authentication only, through the pre-configured public-private key pairs in Sun Ray Server Software and firmware. The Digital Signature Algorithm (DSA) is used to verify that clients are communicating with a valid Sun Ray server. This

authentication scheme is not completely foolproof, but it mitigates trivial man-in-the-middle attacks and makes it harder for attackers to spoof Sun Ray Server Software.

Security Configuration

When configuring the security for a Sun Ray system, you should evaluate the security requirements. You may choose:

- to enable encryption for upstream traffic only
- to enable encryption for downstream traffic only
- to enable bidirectional encryption
- to enable server authentication (client authentication is not currently available)

Additionally, you must decide whether to enable hard security mode. To configure your site, you can use the `utcrypto` command or the Sun Ray Administration Tool (Admin GUI).

Security Mode

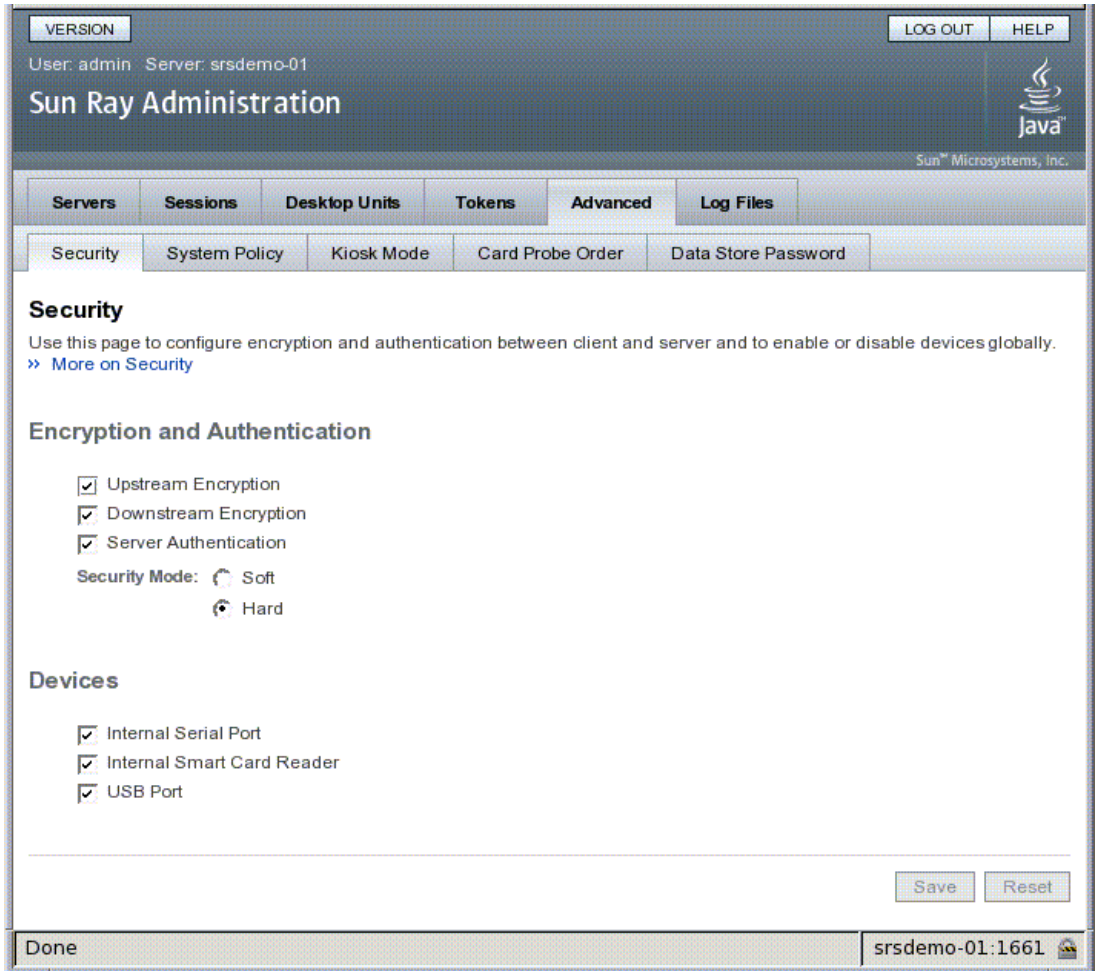
Hard security mode ensures that every session is secure. If security requirements cannot be met, the session is refused. Soft security mode ensures that every client that requests a session gets one; if security requirements cannot be met, the session is granted but not secure.

For example, in hard security mode, if any Sun Ray DTU that does not support security features (for instance, because of old firmware) connects to a Sun Ray server, the server denies the session.

In soft security mode, given the above situation, the Sun Ray server grants the DTU a non-secure session. It is now up to the user to decide whether to continue using a non-secure session.

For more information, please see the man page for `utcrypto` or [“Security Settings” on page 52](#).

FIGURE 6-1 Sun Ray Security Configuration Tab



Session Security

Use the `utsession` command to display session status. Its output has been modified to include security status for a session. The State column in `utsession -p` output now displays the encrypted/authenticated state of the session by using *E* for encrypted and *A* for authenticated session types. This information is not displayed for any session in the disconnected state.

In a multihead environment, there may be a case where the primary and the secondary servers have different firmware. For instance, if the secondary has version 1.3 or earlier firmware, it cannot support any of the security features. In this case, the lowest security setting is displayed. In other words, if the secondary server is configured with 1.3 firmware and the primary server with SRSS 2.0, 3.0, 3.1, 4.0, or 4.1 firmware, and encryption and authentication are configured, then neither an *E* or an *A* is displayed.

```
# utsession -p
Token ID Registered NameUnix IDDispState
Payflex.0000074500000202 ??? ??? 2IEA
Micropayflex.000003540004545??????3D
```

Security Status

Once a connection has been successfully established between a client and a server, the user can determine whether the connection is secure at any time by pressing the three volume keys simultaneously to display a status icon, which also shows the DTU's MAC. For a description of OSD icons and their respective codes, see ["Understanding OSD" on page 175](#).

Deployment on Shared Networks

This chapter describes the process of deploying DTUs on shared network segments. It covers the following topics:

- “Sun Ray DTU Initialization Requirements” on page 78
- “Network Topology Options” on page 80
- “Network Configuration Tasks” on page 83
- “Network Performance Requirements” on page 99
- “Troubleshooting Tools” on page 102
- “Remote Configuration” on page 103
- “Firmware” on page 104
- “Routerless VPN Capability” on page 107
- “Pop-up GUI” on page 108
- “Remote Loading of Configuration Data” on page 114
- “Ports and Protocols” on page 116

When first introduced, Sun Ray DTUs could be deployed only on dedicated, directly-connected interconnect subnets. Although dedicated interconnects provide reliable service and are easy to configure, they require the full-time commitment of networking equipment, cabling, and host interfaces. This constraint has been removed from SRSS 2.0 and later releases, allowing network administrators to deploy Sun Ray DTUs nearly anywhere on an enterprise intranet. The most important advantages of intranet deployment are:

- Sun Ray can be deployed on any existing network infrastructure that meets Sun Ray Quality of Service (QoS) requirements.
- Sun Ray DTUs can be deployed at a greater distance from their Sun Ray server.

Sun Ray DTU Initialization Requirements

Because Sun Ray DTUs are stateless, they rely entirely on network services to provide the configuration data they need to complete their initialization.

- Each DTU must first acquire basic network parameters, such as a valid IP address, on the network to which it is connected.
- The DTU can also be supplied with additional configuration information to support advanced product features, such as the ability to update the DTU firmware and to report exception conditions to a syslog service.
- The DTU must locate and contact a Sun Ray server that can offer desktop services to the Sun Ray user.

The Sun Ray DTU uses the Dynamic Host Configuration Protocol (DHCP) to obtain this information.¹

DHCP Basics

The DTU is a DHCP client that solicits configuration information by broadcasting DHCP packets on the network. The requested information is supplied by one or more DHCP servers in response to the client's solicitations. DHCP service may be provided by a DHCP server process executing on a Sun Ray server, by DHCP server processes executing on other systems, or by some combination of the two. Any conforming implementation of a DHCP service can be used to satisfy the DHCP requirements of the DTU. Sun's Solaris DHCP service is one such implementation. Third-party implementations executing on non-Sun platforms can also be configured to deliver information to Sun Ray DTUs.

The DHCP protocol defines a number of *standard options* that can be used to inform the client of a variety of common network capabilities. DHCP also allows for a number of *vendor-specific options* (see [TABLE 7-2](#)), which carry information that is meaningful only to individual products.

The Sun Ray DTU depends on a small number of standard options to establish its basic network parameters. It depends on several standard and vendor-specific options to provide the additional information that constitutes a complete DTU configuration. If these additional configuration parameters are not supplied, the DTU cannot perform certain activities, the most important of which is the downloading of new DTU firmware. [TABLE 7-2](#) lists the vendor-specific options.

1. DHCP is an Internet Engineering Task Force (IETF) protocol described in Requests for Comments (RFC) *RFC 2131* and *RFC 2132*.

Note – If an administrator chooses not to make this additional configuration information available to the Sun Ray DTUs, a procedure must be established to deliver firmware updates to them. One solution would be a small, dedicated interconnect on one Sun Ray server. Then, the administrator can transfer the DTUs one-by-one when new firmware becomes available on the server, for instance, through a patch or Sun Ray product upgrade.

The location of the Sun Ray server is usually conveyed to the DTU through one of a pair of DHCP vendor-specific options, *AuthSrvr* and *AltAuth* (see [TABLE 7-2](#)).

If the DTU does not receive this information, it uses a broadcast-based discovery mechanism to find a Sun Ray server on its subnet. The DTU firmware now goes one step further. If the broadcast-based discovery mechanism fails, the DTU interprets the DHCP standard option (option 49) of the *X Window Display Manager* as a list of Sun Ray server addresses where it attempts to contact Sun Ray services (see [“Configure the external DHCP service.” on page 97](#)). This can simplify the DHCP configuration of LAN-deployed Sun Rays by removing the need for a DHCP vendor option to carry this information (see [TABLE 7-1](#)).

TABLE 7-1 DHCP Service Parameters Available

Parameters	Sun Ray Server DHCP Service	External DHCP service with vendor-specific options	External DHCP service without vendor-specific options	No DHCP service
Basic network parameters	Yes	Yes	Yes	No
Additional parameters (for firmware download, etc.)	Yes	Yes	No	No
Sun Ray server location	Yes	Yes	Yes, through broadcast discovery or the <i>X Display Manager</i> standard option	Yes, through broadcast discovery

DHCP Parameter Discovery

DHCP enables two stages of parameter discovery. The initial DHCPDISCOVER stage discovers basic network parameters. This stage may be followed by a DHCPINFORM, which finds additional information that was not provided during DHCPDISCOVER.

All Sun Ray DTUs must have access to at least one DHCP service, which provides network parameters in response to a DHCPDISCOVER request from the DTU. DTUs containing firmware delivered with Sun Ray Server Software 2.0 or later can exploit the DHCPINFORM feature. They enable full configuration of the DTU, even when an external DHCP service that is not capable of providing complete configuration data provides the network parameters of the DTU.

DTUs that contain pre-2.0 firmware require all of their configuration information in the initial DHCPDISCOVER phase. They do not attempt a DHCPINFORM step. If the deployment strategy requires a two-step DHCP interaction, such DTUs must be upgraded with Sun Ray Server Software firmware version 2.0 or later before being deployed on a shared subnet.

DHCP Relay Agent

The DTU sends DHCP requests as broadcast packets that propagate only on the local LAN segment or subnet. If the DTU resides on the same subnet as the DHCP server, the DHCP server can see the broadcast packet and respond with the information the DTU needs. If the DTU resides on a different subnet than the DHCP server, the DTU must depend on a local DHCP Relay Agent to collect the broadcast packet and forward it to the DHCP server. Depending on the physical network topology and DHCP server strategy, the administrator may need to configure a DHCP Relay Agent on each subnetwork to which Sun Ray clients are connected. Many IP routers provide DHCP Relay Agent capability. If a deployment plan requires the use of a DHCP Relay Agent, and the administrator decides to activate this capability on a router, the appropriate instructions can be found in the router documentation, usually under the heading of “DHCP Relay” or “BOOTP forwarding.”²

In certain cases, an existing enterprise DHCP service provides the DTU with its IP address while a Sun Ray server provides it with firmware version details and Sun Ray server location. If a deployment plan calls for DHCP parameters to be provided to the DTU by multiple servers, and none of those servers is connected to the subnet where the DTU resides, the DHCP Relay Agent should be configured so that the DTUs subnet can deliver broadcasts to all the DHCP servers. For example, in routers controlled by a Cisco® IOS Executive (see [“Deployment on a Remote Subnet” on page 92](#)), the `ip helper-address` command activates a DHCP Relay Agent. Specifying multiple arguments to the `ip helper-address` command enables relaying to multiple DHCP servers.

Network Topology Options

There are three basic topology options for Sun Ray deployment. DTUs can be deployed on:

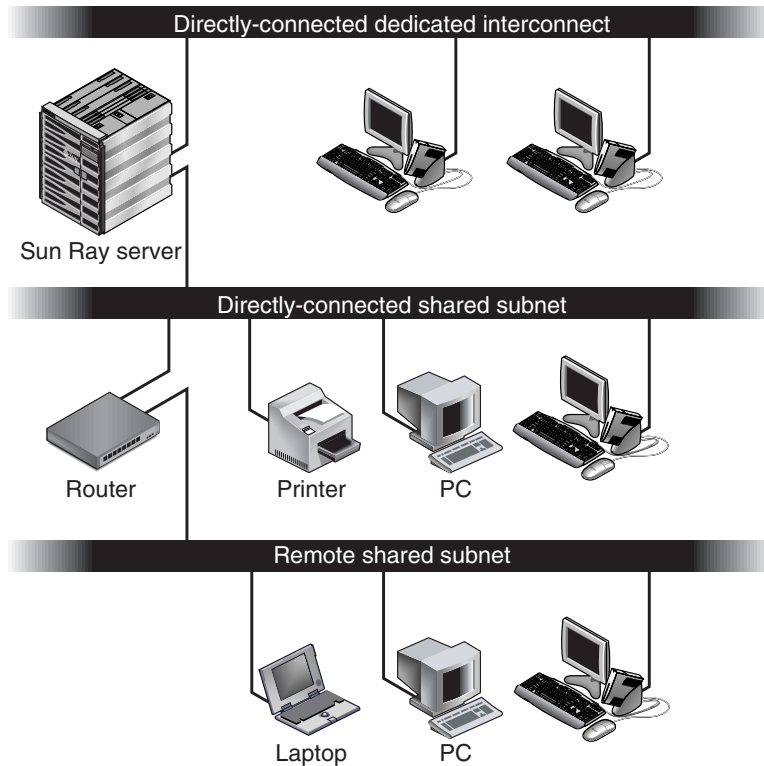
- a directly-connected dedicated interconnect.
- a directly-connected shared subnet.

2. DHCP is derived from an earlier protocol called BOOTP. Some documentation uses these names interchangeably.

- a remote shared subnet.

A Sun Ray server can support any combination of these topologies, which are shown in [FIGURE 7-1](#).

FIGURE 7-1 Network Topologies for Sun Ray DTU Deployment



Note – Sun Ray traffic on shared networks is potentially more exposed to an eavesdropper than traffic on a dedicated Sun Ray interconnect. Modern switched network infrastructures are far less susceptible to snooping activity than earlier shared technologies, but to obtain additional security the administrator may choose to activate Sun Ray’s encryption and authentication features. These capabilities are discussed in [“Encryption and Authentication”](#) on page 73.

Directly-Connected Dedicated Interconnect

The *directly-connected dedicated interconnect*—often referred to simply as an interconnect—places DTUs on subnets that are:

- directly connected to the Sun Ray server (that is, the server has a network interface connected to the subnet).
- devoted entirely to carrying Sun Ray traffic. Prior to the release of Sun Ray Server Software 2.0, this was the only officially supported Sun Ray topology.

The Sun Ray server, which guarantees the delivery of the full set of DTU configuration parameters, is always used to provide DHCP service for a dedicated interconnect.

Directly-Connected Shared Subnet

Sun Ray Server Software now supports DTUs on a *directly-connected shared subnet*, in which:

- the Sun Ray server has a network interface connected to the subnet.
- the subnet may carry a mix of Sun Ray and non-Sun Ray traffic.
- the subnet is generally accessible to the enterprise intranet.

On a directly-connected shared subnet, DHCP service can be provided by the Sun Ray server, or some external server, or both. Since the Sun Ray server can see broadcast DHCP traffic from the DTU, it can participate in DTU initialization without requiring a DHCP Relay Agent.

Remote Shared Subnet

Sun Ray Server Software now also supports DTUs on a *remote shared subnet*. On a remote shared subnet:

- a Sun Ray server does not have a network interface connected to the subnet.
- the subnet can carry a mix of Sun Ray and non-Sun Ray traffic.
- all traffic between the server and the DTU flows through at least one router.
- the subnet is generally accessible to the enterprise intranet.

On a remote shared subnet, DHCP service can be provided by the Sun Ray server, by some external server, or by both. For DHCP service on the Sun Ray server to participate in DTU initialization, a DHCP Relay Agent must be configured on the remote subnet, where it collects DHCP broadcast traffic and forwards it to the Sun Ray server.

Network Configuration Tasks

The addition of directly-connected and remote shared subnet support allows DTUs to be deployed virtually anywhere on the enterprise intranet, subject only to the provision of DHCP service and a sufficient quality of service between the DTU and the Sun Ray server.

The following sections explain how to configure a network to support these scenarios:

- [Deployment on a Directly-Connected Dedicated Interconnect](#)
- [Deployment on a Directly-Connected Shared Subnet](#)
- [Deployment on a Remote Subnet](#)

FIGURE 7-2 shows the overall topology and configuration tasks.³

Preparing for Deployment

Before deploying a DTU onto any subnet, the administrator must answer three questions:

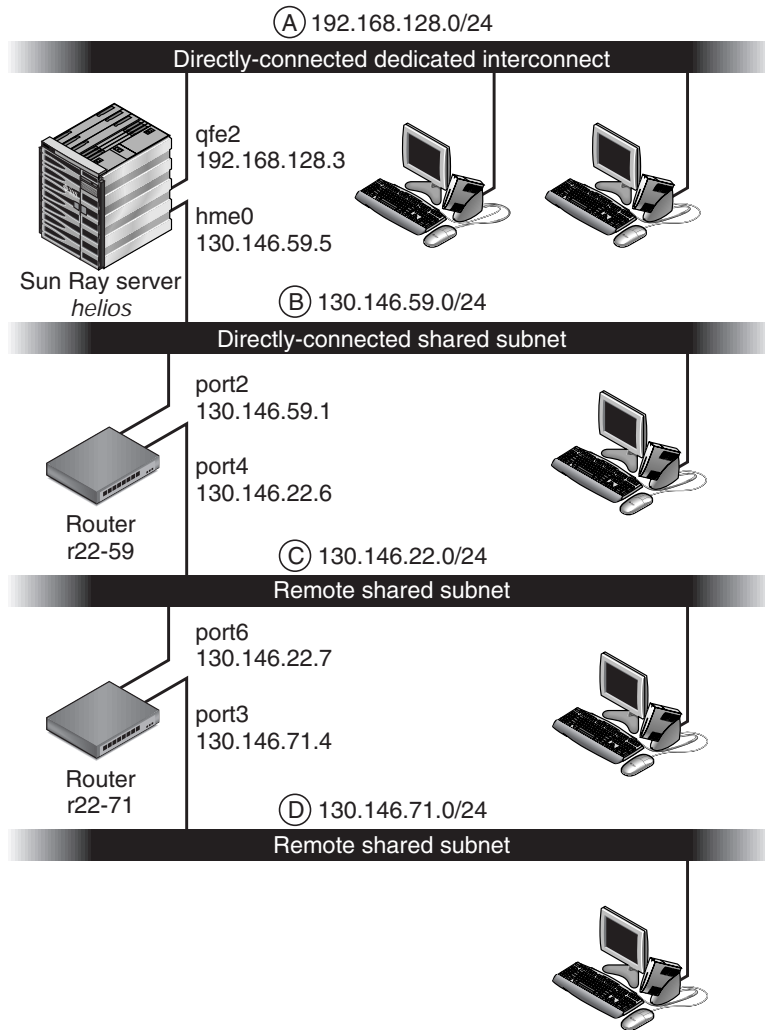
1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?
2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?
3. How will DTUs on this subnet locate their Sun Ray server?

The answers to these questions determine what configuration steps will let DTUs placed on this subnet initialize themselves and offer Sun Ray sessions to users.

The following sections present examples of DTU deployment on the directly-connected dedicated interconnect A, the directly-connected shared subnet B, and the remote shared subnets C and D shown in [FIGURE 7-2](#).

3. The /24 suffix in IP addresses indicates the use of Classless Inter Domain Routing (CIDR) notation, which is documented in IETF RFCs 1517, 1518, and 1519

FIGURE 7-2 Sun Ray Network Topology



Deployment on a Directly-Connected Dedicated Interconnect

Subnet A in [FIGURE 7-2](#) is a directly-connected dedicated interconnect. Its subnet will use IP addresses in the range 192.168.128.0/24. The Sun Ray server named *helios* is attached to the interconnect through its *qfe2* network interface, which will be assigned the IP address 192.168.128.3.

In an interconnect scenario, the DHCP service on the Sun Ray server always provides both basic networking parameters and additional configuration parameters to the DTU. The answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

On a directly-connected dedicated interconnect, basic networking parameters are always supplied by the DHCP service on the Sun Ray server.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

On a directly-connected dedicated interconnect, additional configuration parameters are always supplied by the DHCP service on the Sun Ray server.

3. How will DTUs on this subnet locate their Sun Ray server?

On a directly-connected dedicated interconnect, the DTU is always notified of the location of the Sun Ray server through an additional configuration parameter supplied in Step 2.

Directly-Connected Dedicated Interconnect: Example

This is an example of DHCP service for the directly-connected dedicated interconnect A shown in [FIGURE 7-2](#).

- 1. Configure the Sun Ray server to provide both basic and additional parameters to the interconnect.**

Use the `utadm -a ifname` command to configure DHCP service for DTUs on an interconnect. In this example, the interconnect is attached through interface `qfe2`, so the appropriate command is:

CODE EXAMPLE 7-1

```
# /opt/SUNWut/sbin/utadm -a qfe2
### Configuring /etc/nsswitch.conf
### Configuring Service information for Sun Ray
### Disabling Routing
### configuring qfe2 interface at subnet 192.168.128.0
Selected values for interface "qfe2"
  host address:          192.168.128.1
  net mask:              255.255.255.0
  net address:           192.168.128.0
  host name:             helios-qfe2
  net name:              SunRay-qfe2
  first unit address:    192.168.128.16
  last unit address:     192.168.128.240
  auth server list:      192.168.128.1
  firmware server:       192.168.128.1
```

CODE EXAMPLE 7-1

```
router: 192.168.128.1
Accept as is? ([Y]/N): n
new host address: [192.168.128.1] 192.168.128.3
new netmask: [255.255.255.0]
new host name: [helios-qfe2]
Do you want to offer IP addresses for this interface? ([Y]/N):
new first Sun Ray address: [192.168.128.16]
number of Sun Ray addresses to allocate: [239]
new auth server list: [192.168.128.3]
To read auth server list from file, enter file name:
Auth server IP address (enter <CR> to end list):
If no server in the auth server list responds, should an
auth server be located by broadcasting on the network? ([Y]/N):
new firmware server: [192.168.128.3]
new router: [192.168.128.3]
Selected values for interface "qfe2"
host address: 192.168.128.3
net mask: 255.255.255.0
net address: 192.168.128.0
host name: helios-qfe2
net name: SunRay-qfe2
first unit address: 192.168.128.16
last unit address: 192.168.128.254
auth server list: 192.168.128.3
firmware server: 1 192.168.128.3
router: 192.168.128.3
Accept as is? ([Y]/N):
### successfully set up "/etc/hostname.qfe2" file
### successfully set up "/etc/inet/hosts" file
### successfully set up "/etc/inet/netmasks" file
### successfully set up "/etc/inet/networks" file
### finished install of "qfe2" interface
### Building network tables - this will take a few minutes
### Configuring firmware version for Sun Ray
    All the units served by "helios" on the 192.168.128.0
    network interface, running firmware other than version
    "2.0_37.b,REV=2002.12.19.07.46" will be upgraded at their
    next power-on.
### Configuring Sun Ray Logging Functions
DHCP is not currently running, should I start it? ([Y]/N):
### started DHCP daemon
#
```

In this example, the default values initially suggested by `utadm` were not appropriate. (Specifically, the suggested value for the server's IP address on the interconnect was not the desired value.) The administrator replied `n` to the first `Accept as is?` prompt and was given the opportunity to provide alternative values for the various parameters.

2. Restart Sun Ray services on the Sun Ray server.

Once the `utadm` command has completed, issue a `utrestart` command to fully activate Sun Ray services on the newly-defined interconnect:

```
# /opt/SUNWut/sbin/utrestart
A warm restart has been initiated... messages will be logged to
/var/opt/SUNWut/log/messages.
```

Deployment on a Directly-Connected Shared Subnet

Subnet B in [FIGURE 7-2](#) is a directly-connected shared subnet that uses IP addresses in the range `130.146.59.0/24`. The Sun Ray server *helios* is attached to the interconnect through its `hme0` network interface, which has been assigned the IP address `130.146.59.5`. The answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

In a shared subnet scenario, you must choose whether a DHCP service on the Sun Ray server or some external DHCP service will provide the DTU with basic network parameters. If the enterprise already has a DHCP infrastructure that covers this subnet, it probably supplies basic network parameters. If no such infrastructure exists, configure the Sun Ray server to provide basic network parameters.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

The administrator must choose whether to supply additional configuration parameters to the DTU and, if so, whether to use a DHCP service on the Sun Ray server or some external DHCP service for this purpose. On a directly connected shared subnet, it is possible to deploy DTUs without providing additional parameters at all, but since this deprives the DTU of a number of features, including the ability to download new firmware, it is generally undesirable.

Administrators of an already established DHCP infrastructure may be unable or unwilling to reconfigure that infrastructure to provide additional Sun Ray configuration parameters, so it is usually more convenient to have the Sun Ray server provide these parameters. Even when the established infrastructure is capable of delivering the additional parameters, it may be desirable to have the Sun Ray server provide them. This

enables SRSS commands to be used to manage the values of the additional configuration parameters when those values need to be changed in response to software upgrades or patch installations on the Sun Ray server. For instance, a patch that delivers new DTU firmware could automatically update the firmware version string that is delivered to the DTU. However, if the firmware version parameter is supplied by some external DHCP service, an administrator must manually edit the firmware version parameter string in the external DHCP configuration rules to reflect the new firmware version delivered by the patch. This activity is time-consuming and error-prone, as well as unnecessary.

3. How will DTUs on this subnet locate their Sun Ray server?

Use one of the optional additional configuration parameters to report the location of the Sun Ray server to the DTU. If additional configuration parameters are not supplied to the DTU at all, the DTU has no indication of the location of any Sun Ray server. In these circumstances, the DTU attempts to discover the location of a Sun Ray server by using a broadcast-based mechanism. However, the DTUs broadcast packets propagate only on the local subnet, so, in the case of a remote subnet, the broadcast cannot reach the Sun Ray server, and contact cannot be established.

The following examples illustrate two configurations of the directly connected shared subnet. In the first example, the Sun Ray server delivers both basic networking parameters and additional parameters. In the second example, an external DHCP service supplies basic networking parameters, and no additional parameters are provided to the DTU, which must establish contact with the Sun Ray server through its local subnet broadcast discovery mechanism.

The most likely case, where an external DHCP service provides basic networking parameter and the Sun Ray server provides additional parameters, is illustrated by an example in “Deployment on a Remote Subnet.”

Directly-Connected Shared Subnet: Example 1

In this example, the answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

From the Sun Ray server.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

From the Sun Ray server.

3. How will DTUs on this subnet locate their Sun Ray server?

The DTUs will be informed of the location of the Sun Ray server through an additional configuration parameter delivered in Step 2.

1. Configure the Sun Ray server to provide both basic and additional parameters to the shared subnet.

DHCP service for DTUs on a shared subnet is configured through the `utadm -A subnet` command. In this example, the shared subnet has network number 130.146.59.0, so the appropriate command is `utadm -A 130.146.59.0`:

CODE EXAMPLE 7-2

```
# /opt/SUNWut/sbin/utadm -A 130.146.59.0
Selected values for subnetwork "130.146.59.0"
  net mask:                255.255.255.0
  no IP addresses offered
  auth server list:       130.146.59.5
  firmware server:       130.146.59.5
  router:                 130.146.59.1
Accept as is? ([Y]/N): n
netmask: 255.255.255.0 (cannot be changed - system defined netmask)
Do you want to offer IP addresses for this subnet? (Y/[N]): y
new first Sun Ray address: [130.146.59.4] 130.146.59.200
number of Sun Ray addresses to allocate: [55] 20
new auth server list:     [130.146.59.5]
To read auth server list from file, enter file name:
Auth server IP address (enter <CR> to end list):
If no server in the auth server list responds, should an
auth server be located by broadcasting on the network? ([Y]/N):
  new firmware server:   [130.146.59.5]
  new router:            [130.146.59.1]
Selected values for subnetwork "130.146.59.0"
  net mask:                255.255.255.0
  first unit address:     130.146.59.200
  last unit address:     130.146.59.219
  auth server:           130.146.59.5
  firmware server:       130.146.59.5
  router:                130.146.59.1
  auth server list:      130.146.59.5
Accept as is? ([Y]/N):
### Building network tables - this will take a few minutes
### Configuring firmware version for Sun Ray
All the units served by "helios" on the 130.146.59.0
network interface, running firmware other than version
"2.0_37.b,REV=2002.12.19.07.46" will be upgraded at
their next power-on.
### Configuring Sun Ray Logging Functions
### stopped DHCP daemon
### started DHCP daemon
#
```

The default values initially suggested by `utadm` were not appropriate. Specifically, this server would not have offered any IP addresses on the `130.146.59.0` subnet because `utadm` assumes that basic networking parameters, including IP addresses, are provided by some external DHCP service when the DTU is located on a shared subnet. In this example, however, the Sun Ray server is required to provide IP addresses, so the administrator replied `n` to the first `Accept as is?` prompt and was given the opportunity to provide alternative values for the various parameters. Twenty IP addresses, starting at `130.146.59.200`, were made available for allocation to DHCP clients on this subnet.

2. Restart Sun Ray services on the Sun Ray server.

Once the `utadm` command has completed, issue a `utrestart` command to fully activate Sun Ray services on the shared subnet:

```
# /opt/SUNWut/sbin/utrestart
A warm restart has been initiated... messages will be logged to
/var/opt/SUNWut/log/messages.
```

Directly-Connected Shared Subnet: Example 2

In this example, the answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

From an external DHCP service.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

The DTUs will not be supplied with additional parameters.

3. How will DTUs on this subnet locate their Sun Ray server?

By using the local subnet broadcast discovery mechanism.

In this example, the Sun Ray server does not participate in DTU initialization at all. Why, then, are configuration steps required on the Sun Ray server? The Sun Ray server responds by default only to DTUs located on directly connected dedicated interconnects. It responds to DTUs on shared subnets only if the `utadm -L on` command has been executed. Running the `utadm -A subnet` command to activate DHCP on the Sun Ray server for a shared subnet, as in this example, implicitly executes `utadm -L on`. If `utadm -A subnet` has not been run, the administrator must run `utadm -L on` manually to allow the server to offer sessions to DTUs on the shared subnet.

1. Configure the external DHCP service.

Determining how to configure the external DHCP infrastructure to provide basic networking parameters to the DTUs on this subnet is beyond the scope of this document. Bear in mind:

- If the external DHCP service does not have its own direct connection to this subnet, the administrator must configure a DHCP Relay Agent to deliver DHCP traffic on this subnet to the external DHCP service. The most likely location for such a Relay Agent would be on a router in this subnet, in this case the router named r22-59 in [FIGURE 7-2](#). For a brief introduction to this topic refer to “[DHCP Relay Agent](#)” on page 80.
- An existing external DHCP service may need to have its IP address allocation for this subnet increased in order to support the new DTUs. (This applies whenever additional DHCP clients are placed on a subnet.) It might also be desirable to reduce the lease time of addresses on this subnet so that addresses become eligible for reuse quickly.

2. Configure the Sun Ray server to accept DTU connections from shared subnets.

Run `utadm -L` on:

```
# /opt/SUNWut/sbin/utadm -L on
### Turning on Sun Ray LAN connection
NOTE: utrestart must be run before LAN connections will be allowed
```

3. Restart Sun Ray services on the Sun Ray server.

Once the `utadm` command has completed, issue a `utrestart` command to fully activate Sun Ray services on the shared subnet::

```
# /opt/SUNWut/sbin/utrestart
A warm restart has been initiated... messages will be logged to
/var/opt/SUNWut/log/messages.
```

Deployment on a Remote Subnet

Subnets C and D in [FIGURE 7-2](#) are remote shared subnets.

Subnet C uses IP addresses in the range 130.146.22.0/24. Subnet D uses IP addresses in the range 130.146.71.0/24. The Sun Ray server named *helios* has no direct attachment to either of these subnets; it is this characteristic that defines them as remote. The answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

In a shared subnet scenario, the administrator must choose whether a DHCP service on the Sun Ray server or some external DHCP service will provide the DTU with basic network parameters.

If the enterprise already has a DHCP infrastructure that covers this subnet, it probably supplies basic network parameters. If no such infrastructure exists, configure the Sun Ray server to provide basic network parameters.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

The administrator must choose whether additional configuration parameters will be supplied to the DTU, and if so whether they will be supplied by a DHCP service on the Sun Ray server or by some external DHCP service.

Administrators of an established DHCP infrastructure may be unable or unwilling to reconfigure it to provide additional Sun Ray configuration parameters, so it is usually more convenient to have the Sun Ray server provide them.

Even when the established infrastructure is capable of delivering the additional parameters, it may be desirable to have the Sun Ray server provide them. This enables you to use Sun Ray Server Software commands to manage the values of the additional configuration parameters, when those values need to be changed in response to software upgrades or patch installations on the Sun Ray server. For instance, a patch that delivers new DTU firmware could automatically update the firmware version string delivered to the DTU. However, if the firmware version parameter is supplied by some external DHCP service, an administrator must manually edit the firmware version parameter string in the external DHCP configuration rules to reflect the new firmware version delivered by the patch. This kind of activity is time-consuming and error-prone as well as unnecessary.

3. How will DTUs on this subnet locate their Sun Ray server?

Use one of the optional additional configuration parameters to report the location of the Sun Ray server to the DTU. If additional configuration parameters are not supplied to the DTU at all, the DTU cannot locate a Sun Ray server, so it tries to discover the location of a Sun Ray server by using a broadcast-based mechanism. However, the DTUs broadcast packets propagate only on the local subnet; they cannot reach a Sun Ray server located on a remote subnet, and cannot establish contact.

The next two examples illustrate representative remote shared subnet configurations. In the first example, an external DHCP service provides basic networking parameters, and the Sun Ray server provides additional parameters. This is by far the most likely configuration for a Sun Ray deployment in an enterprise that has an established DHCP infrastructure.

In the second example, basic networking parameters and a bare minimum of additional parameters—just enough to enable the DTU to contact a Sun Ray server—are supplied by an external DHCP. In this case, it is the DHCP service in a Cisco router. This scenario is less than ideal.

No firmware parameters are delivered to the DTU, so it cannot download new firmware. The administrator must make some other arrangement to provide the DTU with new firmware, for instance, by rotating it off this subnet periodically onto an interconnect or onto some other shared subnet where a full set of additional configuration parameters is offered.

Note – For examples of shared subnet deployments in which both basic networking parameters and additional parameters are delivered by the Sun Ray server and basic networking parameters are supplied by an external DHCP service (with no additional DTU parameters provided), see [“Directly-Connected Shared Subnet” on page 82](#).

Remote Shared Subnet: Example 1

In this example, in which DTUs are deployed on subnet C in [FIGURE 7-2](#), the answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

From an external DHCP service.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

From the Sun Ray server.

3. How will DTUs on this subnet locate their Sun Ray server?

The DTUs will be informed of the location of the Sun Ray server through an additional configuration parameter delivered in Step 2.

Use the `utadm -A subnet` command as follows to configure DHCP service for DTUs on a shared subnet.

1. Configure the external DHCP service.

Determining how to configure the external DHCP infrastructure to provide basic networking parameters to the DTUs on this subnet is beyond the scope of this document. Bear in mind:

- If the external DHCP service does not have its own direct connection to this subnet, the administrator must configure a DHCP Relay Agent to deliver DHCP traffic on this subnet to the external DHCP service. The most likely location for such a Relay Agent would be on a router in this subnet, in this case the router named `r22-59` in [FIGURE 7-2](#). For a brief introduction to this topic refer to [“DHCP Relay Agent” on page 80](#).
- An existing external DHCP service may need to have its IP address allocation increased for this subnet to support the new DTUs. (This applies whenever additional DHCP clients are placed on a subnet.) It might also be desirable to reduce the lease time of addresses on this subnet so that addresses become eligible for re-use quickly.

2. Arrange to deliver DHCP traffic to the Sun Ray server.

Because the Sun Ray server does not have its own direct connection to this subnet, the administrator must configure a DHCP Relay Agent to deliver the subnet’s DHCP traffic to the Sun Ray server. The most likely location for such a Relay Agent would be on a router in this subnet, in this case the router named `r22-59` in [FIGURE 7-2](#). For a brief introduction to this topic refer to [“DHCP Relay Agent” on page 80](#).

If `r22-59` is running the Cisco IOS, the `ip helper-address` command can be used to activate its DHCP Relay Agent to relay DHCP broadcasts from its 10/100 Ethernet port number 4 to the Sun Ray server at `130.146.59.5`.

```
r22-59> interface fastethernet 4
r22-59> ip helper-address 130.146.59.5
r22-59>
```

If the external DHCP service also lacks a connection to this subnet, configure a DHCP Relay Agent to forward requests from the DTU to:

- The external DHCP service (so that the DTU can obtain basic networking parameters)
- The DHCP service on the Sun Ray server (so that the DTU can obtain additional parameters)

The Cisco IOS `ip helper-address` command accepts multiple relay destination addresses, so if, for instance, the external DHCP service could be contacted at `130.146.59.2` on subnet B in [FIGURE 7-2](#), the appropriate sequence would be:

```
r22-59> interface fastethernet 4
r22-59> ip helper-address 130.146.59.2 130.146.59.5
r22-59>
```

Note – Details of the IOS interaction vary according to the specific release of IOS, the model of the router, and the hardware installed in the router.

3. Configure the Sun Ray server to provide additional parameters to the shared subnet.

Use the `utadm -A subnet` command to configure DHCP service for DTUs on a shared subnet. In this example, the shared subnet has network number 130.146.22.0, so the appropriate command is `utadm -A 130.146.22.0`.

CODE EXAMPLE 7-3

```
# /opt/SUNWut/sbin/utadm -A 130.146.22.0
Selected values for subnetwork "130.146.22.0"
  net mask:                255.255.255.0
  no IP addresses offered
  auth server list:        130.146.59.5
  firmware server:         130.146.59.5
  router:                  130.146.22.1
Accept as is? ([Y]/N): n
new netmask:[255.255.255.0]
Do you want to offer IP addresses for this subnet? (Y/[N]):
new auth server list:      [130.146.59.5]
To read auth server list from file, enter file name:
Auth server IP address (enter <CR> to end list):
If no server in the auth server list responds, should an
auth server be located by broadcasting on the network? ([Y]/N):
new firmware server:       [130.146.59.5]
new router: [130.146.22.1] 130.146.22.6
Selected values for subnetwork "130.146.59.0"
  net mask:                255.255.255.0
  no IP addresses offered
  auth server list:         130.146.59.5
  firmware server:          130.146.59.5
  router:                  130.146.22.6
Accept as is? ([Y]/N):
### Building network tables - this will take a few minutes
### Configuring firmware version for Sun Ray
All the units served by "helios" on the 130.146.22.0
network interface, running firmware other than version
"2.0_37.b,REV=2002.12.19.07.46" will be upgraded at their
next power-on.
### Configuring Sun Ray Logging Functions
### stopped DHCP daemon
### started DHCP daemon
#
```

In this example, the default values initially suggested by `utadm` were not appropriate. Specifically, the default router address to be used by DTUs on this subnet was not correct because `utadm` guesses that the address of the default router for any shared subnet will have a host part equal to 1. This was a *great* guess for the directly-connected subnet B in [FIGURE 7-2](#), but it is not correct for subnet C.

The appropriate router address for DTUs on this subnet is 130.146.22.6 (port 4 of router `r22-59`), so the administrator replied **n** to the first `Accept as is?` prompt and was given the opportunity to provide alternative values for the various parameters.

4. Restart Sun Ray services on the Sun Ray server.

Once the `utadm` command has completed, issue a `utrestart` command to fully activate Sun Ray services on the shared subnet:

```
# /opt/SUNWut/sbin/utrestart
A warm restart has been initiated... messages will be logged to
/var/opt/SUNWut/log/messages.
```

Remote Shared Subnet: Example 2

In this example, deploying DTUs on subnet D in [FIGURE 7-2](#), the answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

From an external DHCP service.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

The DTUs will not be supplied with the additional parameters required to support firmware download or to activate other advanced DTU features.

3. How will DTUs on this subnet locate their Sun Ray server?

The external DHCP service will supply a single additional parameter to inform the DTU of the location of a Sun Ray server.

In this example, the Sun Ray server does not participate in DTU initialization at all. Why, then, are configuration steps required on the Sun Ray server? The Sun Ray server responds by default only to DTUs located on directly connected dedicated interconnects. It responds to DTUs on shared subnets only if the `utadm -L on` command has been executed. Running the `utadm -A subnet` command to activate DHCP on the Sun Ray server for a shared subnet, as in this example, implicitly executes `utadm -L on`. If `utadm -A subnet` has not been run, the administrator must run `utadm -L on` manually to allow the server to offer sessions to DTUs on the shared subnet.

1. Configure the external DHCP service.

Determining how to configure the external DHCP infrastructure to provide basic networking parameters to the DTUs on this subnet is beyond the scope of this document. However, for this example, assume that DHCP service is provided by Cisco IOS-based router r22-71 in [FIGURE 7-2](#), attached to the 130.146.71.0 subnet through its 10/100 Ethernet port 3. This router can be configured to provide basic networking parameters and the location of a Sun Ray server as follows:

```
r22-71> interface fastethernet 3
r22-71> ip dhcp excluded-address 130.146.71.1 130.146.71.15
r22-71> ip dhcp pool CLIENT
r22-71/dhcp> import all
r22-71/dhcp> network 130.146.71.0 255.255.255.0
r22-71/dhcp> default-router 130.146.71.4
r22-71/dhcp> option 49 ip 130.146.59.5
r22-71/dhcp> lease 0 2
r22-71/dhcp> ^Z
r22-71>
```

Note – Details of the IOS interaction vary according to the specific release of IOS, the model of router and the hardware installed in the router.

DHCP option 49, the standard option of the *X Window Display Manager*, identifies 130.146.59.5 as the address of a Sun Ray server. In the absence of AltAuth and Auth-Srvr vendor-specific options, the DTU tries to find a Sun Ray server by broadcasting on the local subnet. If the broadcasts evoke no response, the DTU uses the address supplied in t option of the *X Window Display Manager*—provided that the DTU contains firmware at Sun Ray Server Software 2.0 patch level 114880-01 or later.

Note – This is an unorthodox use of the option of the *X Window Display Manager*, but in a remote subnet deployment where vendor-specific options can not be delivered, it may be the only way of putting a DTU in touch with a server.

2. Configure the Sun Ray server to accept DTU connections from shared subnets by running `utadm -L on`.

```
# /opt/SUNWut/sbin/utadm -L on
### Turning on Sun Ray LAN connection
NOTE: utrestart must be run before LAN connections will be allowed
#
```

3. Restart Sun Ray services on the Sun Ray server.

Once the `utadm` command has completed, issue a `utrestart` command to fully activate Sun Ray services on the shared subnet:

```
# /opt/SUNWut/sbin/utrestart
A warm restart has been initiated... messages will be logged to
/var/opt/SUNWut/log/messages.
```

TABLE 7-2 lists the vendor-specific DHCP options that Sun Ray defines and uses.

TABLE 7-2 Vendor-specific DHCP Options

Option Code	Parameter Name	Client Class	Data Type	Optional/Mandatory	Granularity	Max Count	Comments
21	AuthSrvr	SUNW.NewT.SUNW	IP	Mandatory	1	1	Single Sun Ray server IP addresses
22	AuthPort	SUNW.NewT.SUNW	NUMBER	Optional	2	1	Sun Ray server port
23	NewTVer	SUNW.NewT.SUNW	ASCII	Optional	1	0	Desired firmware version
24	LogHost	SUNW.NewT.SUNW	IP	Optional	1	1	Syslog server IP address
25	LogKern	SUNW.NewT.SUNW	NUMBER	Optional	1	1	Log level for kernel
26	LogNet	SUNW.NewT.SUNW	NUMBER	Optional	1	1	Log level for network
27	LogUSB	SUNW.NewT.SUNW	NUMBER	Optional	1	1	Log level for USB
28	LogVid	SUNW.NewT.SUNW	NUMBER	Optional	1	1	Log level for video
29	LogAppl	SUNW.NewT.SUNW	NUMBER	Optional	1	1	Log level for firmware application
30	NewTBW	SUNW.NewT.SUNW	NUMBER	Optional	4	1	Bandwidth cap
31	FWSrvr	SUNW.NewT.SUNW	IP	Optional	1	1	Firmware TFTP server IP address
32	NewTDispIndx	SUNW.NewT.SUNW	NUMBER	Optional	4	1	Obsolete. Do not use.
33	Intf	SUNW.NewT.SUNW	ASCII	Optional	1	0	Sun Ray server interface name
34	NewTFlags	SUNW.NewT.SUNW	NUMBER	Optional	4	1	Obsolete. Do not use.
35	AltAuth	SUNW.NewT.SUNW	IP	Optional	1	0	List of Sun Ray server IP addresses
36	BarrierLevel	SUNW.NewT.SUNW	NUMBER	Mandatory	4	1	Firmware Download: barrier level

The DTU can perform its basic functions even if none of these options are delivered during initialization, but some advanced DTU features do not become active unless certain options are delivered to the DTU. In particular:

- `AltAuth` and `AuthSrvr` indicate the IP addresses of Sun Ray servers. Addresses in the `AltAuth` list are tried in order until a connection is established. Current firmware ignores `AuthSrvr` if `AltAuth` is provided, but it is good practice always to specify `AuthSrvr` for the benefit of old (pre Sun Ray Server Software 1.3) firmware, which does not understand the `AltAuth` option. If neither of these options is supplied, the DTU tries to locate a Sun Ray server by sending broadcasts on the local subnet. If the DTU contains firmware at Sun Ray Server Software 2.0 patch level 114880-01 or later, it resorts to trying to contact a Sun Ray server at the address supplied in the option of the *X Window Display Manager* if that option has been provided.
- `NewTVer` and `FWSrvr` must both be provided in order for the DTU to attempt a firmware download. `NewTVer` contains the name of the firmware version that the DTU should use. If this name does not match the name of the firmware version that the DTU is actually running, the DTU tries to download the desired firmware from a TFTP server at the address given by `FWSrvr`.
- `LogHost` must be specified in order for the DTU to report messages through the syslog protocol. Reporting thresholds for major DTU subsystems are controlled by the `LogKern`, `LogNet`, `LogUSB`, `LogVid`, and `LogAppl` options.

Note – The message formats, contents, and thresholds are intended for use only by service personnel and are not documented intentionally.

The DHCP Client Class name for all Sun Ray vendor-specific options is `SUNW.NewT.SUNW`. The DTU cites this name in DHCP requests so that the server can respond with the appropriate set of vendor-specific options. This mechanism guarantees that the DTU is not given vendor options defined for some other type of equipment and that other equipment is not given options that are meaningful only to the DTU.

Network Performance Requirements

This section describes the minimal network infrastructure needed to support a Sun Ray implementation.

Packet Loss

Before version 2.0, Sun Ray Server Software was intolerant of packet losses, so it was recommended that packet loss not exceed 0.1 percent over any extended period. However, because this is often an impractical requirement in local area (LAN) and wide area (WAN) network Sun Ray deployments, the Sun Ray Server Software has been made much more robust in the face of packet loss. The first version of this improved software was released with the first 2.0 patch, with additional improvements in releases supporting low-bandwidth WAN Sun Ray deployments.

In earlier versions, the server tried to avoid packet loss by severely limiting its use of available bandwidth whenever it encountered packet loss. Because random losses are inevitable in a non-dedicated LAN or WAN network environment, this approach put unnecessary limits on performance.

Sun Ray Server Software has always had the capability to detect and recover quickly from such losses, so avoiding them was a matter of policy more than necessity. The new software is less timid and avoids operating at bandwidth levels that create packet losses. Instead, it tries to send data at the highest possible rate that it can without incurring large losses. By design, it sometimes sends data at a rate that is too great for the capacity of the connection between the server and the client, and thus discovers what that capacity is. With very high demand, sustained packet losses of up to 10 percent may sometimes be seen, but the software continues to operate and update the contents of the screen correctly nevertheless.

Latency

Network latency between any Sun Ray client and its server is an important determinant of the quality of the user experience. The lower the latency, the better; latencies under 50 milliseconds for round trip delay are preferred. However, like familiar network protocols such as TCP, the Sun Ray DTU does tolerate higher latencies, but with degraded performance. Latencies up to 150 milliseconds provide usable, if somewhat sluggish, performance.

Out-of-Order Packets

DTUs that contain Sun Ray Server Software 2.0 firmware or later can tolerate small occurrences of out-of-order packet delivery, such as might be experienced on an Internet or wide-area intranet connection. Current Sun Ray firmware maintains a reordering queue that restores the correct order to packets when they are received out of order. In releases prior to Sun Ray Server Software 2.0, out-of-order packets were simply discarded.

The next byte is 0x1f=31, which represents the `FWSrvr` parameter, whose function is to indicate the IP address of the firmware TFTP server. The next byte is the length, 4, which is always be true for an IP address. The hexadecimal value is 0x81 0x92 0x3a 0x88, which corresponds to the IP address 129.146.58.136.

Troubleshooting Tools

`utcapture`

The `utcapture` utility connects to the Sun Ray Authentication Manager and reports packet loss statistics and round-trip latency timings for each DTU connected to this server. See the `utcapture man` page to learn more about this command.

`utquery`

The `utquery` command interrogates a DTU and displays the DTUs initialization parameters along with the IP addresses of the DHCP services that supplied those parameters. It can be helpful in determining whether a DTU was able to obtain the parameters that were expected in a particular deployment and in determining specific DHCP servers that contributed to the DTUs initialization. See the `utquery man` page to learn more about this command.

OSD Icons

Sun Ray DTU on-screen display (OSD) icons contain information that can help the administrator understand and debug network configuration problems. The amount of information encoded into the icons has been significantly expanded in the firmware delivered with Sun Ray Server Software. The icon structure and progression are described in detail in [Appendix B](#). Recent updates to Sun Ray DTU firmware include OSD icons that are larger and easier to read than previous versions. The icon message codes and DHCP states they display, however, remain the same and are listed in [Table B-1 on page 176](#) and [Table B-2 on page 178](#) respectively.

Remote Configuration

You can simplify the DHCP configuration of Sun Ray DTUs at remote sites by using the *X Window System Display Manager* option to supply a list of available Sun Ray servers. This eliminates the need for Sun Ray vendor options as well as the need to forward DHCPINFORM requests to a Sun Ray server.

For a more complete treatment of network configuration, including DHCP and vendor-specific options, see [TABLE 7-1](#) and [TABLE 7-2](#).

A sample DHCP configuration for a Cisco IOS-based router is shown below:

```
ip dhcp excluded-address 129.149.244.161

ip dhcp pool CLIENT

    import all network 129.149.244.160 255.255.255.248

    default-router 129.149.244.161

    option 26 hex 0556

    option 49 ip 10.6.129.67 129.146.58.136

    lease 0 2
```

Option 49, the *X Window System Display Manager* option, lists IP addresses 10.6.129.67 and 129.146.58.136 as Sun Ray servers. The Sun Ray DTU tries to connect to those servers when it receives a DHCP response from the router. Option 26 sets the Maximum Transmission Unit (MTU), which defines the maximum packet size for the Sun Ray connections, in this case 1366 bytes rather than the default Ethernet MTU of 1500 bytes. This is necessary to allow space for the IPsec headers to implement a virtual private network (VPN) connection.

DHCP service, either directly from an ISP or from a home firewall, is also required, to give the router its IP address behind the firewall.

The router's WAN port either plugs directly into the DSL/Cable modem⁴ or into the home firewall/gateway. The Sun Ray DTU then plugs into one of the four LAN ports on the router. If the router has been configured to supply DHCP parameters to the Sun Ray DTU, it will tell the DTU to try to connect to the appropriate Sun Ray server.

4. A VPN router plugged directly into the DSL or cable modem can be connected only to a Sun Ray DTU.

The router should bring up a VPN tunnel when it is plugged in; it should always be on. Each router should be connected to the VPN gateway and programmed with a user name based on an employee's ID and a random password. The VPN gateway should be configured to allow only Sun Ray traffic to pass, and only to a limited number of hosts, so that users cannot connect anything else to the LAN side of the router and then connect into the corporate network. However, users may connect more than one Sun Ray DTU.

Whenever a VPN or other tunnel is being used, you need to take account of the IP MTU across the path between the server and the Sun Ray DTU. The VPN typically packs additional control data into each packet, which reduces the available space for application data.

The latest Sun Ray firmware attempts to compensate for this reduction automatically, but it cannot do that in all situations. Make sure that the Sun Ray DTU has the latest firmware. Simply installing the latest patch on the server is not sufficient: you must also make sure that the DTU is told to update its firmware and then check that it has been able to do so.

If the DTU has the latest firmware but the problem still occurs, then you should explicitly inform the DTU that it is going to be working with a reduced MTU. You can do this through whatever mechanism you use to give the Sun Ray its basic configuration data, such as DHCP, TFTP or, if the DTU is running GUI-capable firmware, local configuration on the Sun Ray DTU itself.

The site should know what the effective MTU is across the VPN. If not, see any available technical archives or the ThinkThin blog on blogs.sun.com. If a precise MTU is not important, then a low estimate, such as 1350 (the standard value is 1500), should be sufficient to let you verify that MTU is the cause of the problem.

After you do this and restart the Sun Ray DTU, the DTU reports the new MTU value to the server, and the server adjusts its packet-construction strategy to fit within that MTU. It should no longer send Sun Ray traffic that is too big to be delivered in one piece through the VPN tunnel.

Firmware

Local settings on the Sun Ray DTU generally override values obtained from other sources, such as `.parms` files or DHCP. As such, the ability to clear a setting must be provided so that the value from a `.parms` file is not overridden and can be used for configuration. For numeric values, enter an empty field; for switch settings, select the `Clear` button when modifying a setting. The `utquery` output from a DTU faithfully reflects the values that are defined in the local configuration.

Generic DHCP Parameters

A set of Sun Ray DTUs can now be brought up with nothing more than generic DHCP parameters, shifting the burden of defining the server list to the Domain Name Service (DNS) and firmware management to TFTP.

If `sunray-config-servers` and `sunray-servers` are defined appropriately by the DNS serving a set of remote Sun Rays DTUs, no extra DHCP parameters are required other than basic network information.

A DNS client incorporated in the firmware allows many values to be names rather than IP addresses. DHCP option 66 (TFTP server name) is supported as an alternative to the `FWSrvr` vendor option. This can resolve to a list of IP addresses, one of which is chosen randomly.

A firmware maintenance mechanism creates `*.parms` files in `/tftpboot` (one for each model type), which are read in lieu of using the `NewTVer` DHCP vendor option. Thus, remote firmware upgrades are possible without DHCP access to the `NewTVer` value. The `*.parms` files contain the version, hardware revision, and barrier levels, eliminating unnecessary file reads in cases where the barrier would have prevented writing the firmware to flash. For details on options that can be used to configure the `.parms` files, see `utfwadm(8)`.

A default DNS name for the firmware server, `sunray-config-servers`, is used when neither option 66 nor `FWSrvr` is given. Defining it in DNS gives a way to provide the firmware server address without DHCP options, just DNS servers and domain name.

Inclusion of `servers=<server name list>` and `select=<inorder|random>` in the `*.parms` files allow specification of a list of server names and specification of whether the names should be used in order, or at random. If a name resolves to multiple addresses, then an IP address is chosen according to the `select` keyword.

When neither a server list nor an `AltAuth` list is given, the default name `sunray-servers` is looked up in DNS, and the list of IP addresses is used in place of the `AltAuth` list.

In the event of an error in the firmware download, a new set of error messages provides additional information that can be useful in diagnosing and correcting the problem. See [“Firmware Download Diagnostics” on page 189](#).

Also, during DNS lookups, a status line in the OSD icon shows the name being looked up and, if one is found, the IP address.

.parms Lookup

There are four ways to specify where to find the firmware server to read both .parms files and actual firmware: the DHCP Sun Ray vendor option `FWSrvr`, the Firmware Server local configuration value, the generic DHCP option 66 (`TFTPSrvr`) value, and the default host name `sunray-config-servers`.

Previous versions of firmware would use these values in this order of priority:

1. Local configuration value (host name or IP address)
2. `FWSrvr` vendor option (IP address)
3. Option 66 (host name or IP address)
4. `sunray-config-servers` (default host name)

However, the old behavior was such that only the highest priority value was used, and if the lookup of .parms files failed, the attempt was aborted. The new behavior attempts each of these values in order until it finds one that succeeds. The exception is that if the local configuration value is used and fails, none of the others is attempted. This prevents the overwriting of custom-configured firmware in a situation where the controlling firmware server happens to be temporarily unresponsive.

Additional key/value pairs included in the .parms files are in `<key>=<value>` format, with case sensitivity and no spaces allowed. Options which take values of 0 or 1 have a default value of 0 if not specified. The following options are allowed:

TABLE 7-3 .parms Key/Value Pairs

Key	Value
<code>servers=</code>	Specifies a comma-separated mixture hostnames and/or IP addresses. This is a generalization and replacement for the <code>AltAuth</code> list.
<code>select=</code>	Allows either <code>in order</code> or <code>random</code> , and selects a server from the server list either starting at the beginning, or at random, respectively.
<code>MTU=</code>	Gets the network MTU. The value used is the minimum of those supplied from various sources.
<code>LogXXX=</code>	Gets the logging level for various classes of logging events, where <code>XXX</code> is one of <code>Appl</code> , <code>Vid</code> , <code>USB</code> , <code>Net</code> , or <code>Kern</code> . These correspond to the equivalent DHCP vendor options.
<code>LogHost=</code>	A dotted-decimal IP address used as the logging host, equivalent to the corresponding DHCP vendor option.
<code>bandwidth= 6</code>	Sets the bandwidth limit used by the Sun Ray, in bits per second.
<code>compress=[0 1]</code>	When set to 1, forces compression on.

TABLE 7-3 .parms Key/Value Pairs

Key	Value																																		
lossless=[0 1]	When set to 1, does not permit lossy compression to be used.																																		
stopqon=[0 1]	When set to 1, enables the <code>STOP-Q</code> key sequence to be used to disconnect a Sun Ray from a server, in particular, if it's using a VPN connection.																																		
utloadoff=[0 1]	When set to 1, disables the ability to use the <code>utload</code> program to force a Sun Ray to load firmware.																																		
kbcountry=code	Forces the keyboard country code number for a non-U.S. keyboard that reports a country code value of 0. This value can also be set on the Advanced menu of the Sun Ray configuration GUI. Some possible values for the country code, from USB keyboard maps, are: <table><tbody><tr><td>6</td><td>Danish</td></tr><tr><td>7</td><td>Finnish</td></tr><tr><td>8</td><td>French</td></tr><tr><td>9</td><td>German</td></tr><tr><td>14</td><td>Italian</td></tr><tr><td>15</td><td>Roman/Kana</td></tr><tr><td>16</td><td>Korean</td></tr><tr><td>18</td><td>Dutch</td></tr><tr><td>19</td><td>Norwegian</td></tr><tr><td>22</td><td>Portuguese</td></tr><tr><td>25</td><td>Spanish</td></tr><tr><td>26</td><td>Swedish</td></tr><tr><td>27</td><td>Swiss French</td></tr><tr><td>28</td><td>Swiss German</td></tr><tr><td>30</td><td>Taiwanese</td></tr><tr><td>32</td><td>UK English</td></tr><tr><td>33</td><td>U.S. English</td></tr></tbody></table>	6	Danish	7	Finnish	8	French	9	German	14	Italian	15	Roman/Kana	16	Korean	18	Dutch	19	Norwegian	22	Portuguese	25	Spanish	26	Swedish	27	Swiss French	28	Swiss German	30	Taiwanese	32	UK English	33	U.S. English
6	Danish																																		
7	Finnish																																		
8	French																																		
9	German																																		
14	Italian																																		
15	Roman/Kana																																		
16	Korean																																		
18	Dutch																																		
19	Norwegian																																		
22	Portuguese																																		
25	Spanish																																		
26	Swedish																																		
27	Swiss French																																		
28	Swiss German																																		
30	Taiwanese																																		
32	UK English																																		
33	U.S. English																																		

For a current list of configured keyboards, see the `keytable.map` file in `/opt/SUNWut/lib/keytables`.

Routerless VPN Capability

Sun Ray Server Software and the most recent firmware provide a VPN solution for remote users that does not require a separate VPN router. The IPsec capability in the Sun Ray firmware allows the Sun Ray DTU to act as a standalone VPN device. The most commonly used encryption, authentication, and key exchange mechanisms are supported, along with Cisco extensions that allow a Sun Ray DTU to interoperate with Cisco gateways that support the Cisco EzVPN protocol.

Although digital certificates are not supported, the security model is identical to that of the Cisco software VPN client. Using a common group name and key for the initial (IKE phase one) authentication exchange, the DTU authenticates the user individually with the Cisco `xauth` protocol, either by presenting a fixed user name and password stored in flash or by requiring the entry of a user name and one-time password generated by a token card. See [“Download Configuration” on page 112](#).

Pop-up GUI

Sun Ray Server Software provides optional functionality, called the Pop-up Graphical User Interface (Pop-up GUI), which allows the entry of configuration parameters for a Sun Ray DTU from the attached keyboard. Most of these configuration parameters are stored in the DTU's flash memory. Certain control key combinations are used to invoke this new facility, which provides a tree of menus that can be navigated to set and examine configuration values.

Access Control

To accommodate customers with differing requirements with respect to flexibility and security, two versions of the DTU software are provided.

Note – The default version of Sun Ray DTU firmware installed at `/opt/SUNWut/lib/firmware` does *not* enable the Pop-up GUI.

The Pop-up GUI-enabled version of the firmware is installed at: `/opt/SUNWut/lib/firmware_gui`. To make the Pop-up GUI available, the administrator must run `utfwadm` to install the firmware, using the `-f` option.

Features and Usage

The Pop-up GUI enables several features that require the ability to set and store configuration information on the Sun Ray DTU itself, including:

- Non-DHCP network configuration for standalone operation, when it is impossible to configure local DHCP operation
- Local configuration of Sun Ray specific parameters, such as server list, firmware server, MTU, and bandwidth limits
- DNS servers and domain name for DNS bootstrapping

- IPsec configuration
- Wireless network configuration (used in Tadpole laptops)

To protect the use of stored authentication information, the VPN configuration includes a PIN entry. This enables two-factor authentication for Sun Ray at Home VPN deployments.

The key combinations used to enter this prompt model are unlikely to be used for other purposes. On a regular Sun keyboard, the key combinations are of the form `Stop-<x>`, where `<x>` is one of the keys listed in [TABLE 7-4](#). On non-Sun (PC) keyboards, use the key combination `Ctrl-Pause-<x>`. For hot key values, see [TABLE A-3](#).

TABLE 7-4 Prompt Mode Key Codes

Code	Meaning
A	Soft reset (Ctrl-Moon)
C	Clear configuration
M or S	Enter main configuration menu
N	Show status (3 audio keys)
Right arrow	Volume up (right arrow)
Left arrow	Volume down (left arrow)
Down arrow	Mute/Unmute
V	Show model, <i>MAC address</i> , and firmware version
Ctrl-u	Clear the contents of an existing entry
Stop-M	Invoke the main configuration menu.

FIGURE 7-3 Pop-up GUI Main Menu (Part I)



The arrow at the lower right corner indicates that the menu can be scrolled with the Up and Down arrow keys.

FIGURE 7-4 Pop-up GUI Main Menu (Part II)



The configuration tree for the Main Menu has the following components:

- Servers
 - Auth list
A list of comma-separated server names or IP addresses
 - Firmware Server
Name or IP address of firmware/config server
 - Loghost
IP address of syslog host
- TCP/IP

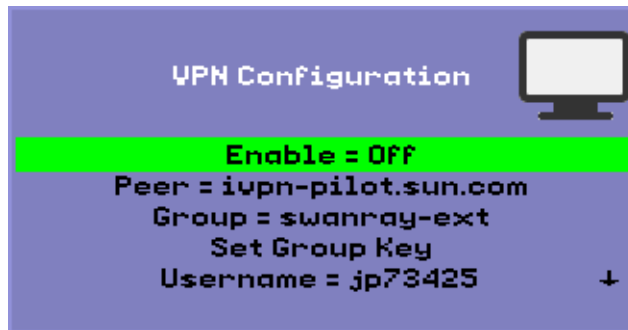
FIGURE 7-5 Setup TCP/IP Menu



- Type
DHCP or Static

- DHCP
 - MTU only
- Static
 - IP address, netmask, router, broadcast address, MTU
- DNS
 - Domain name
 - One only
 - DNS Server list
 - List of IP addresses
- VPN/IPsec (Cisco 3000/EzVPN semantics)

FIGURE 7-6 Enable VPN Configuration Policy Toggle



- Enable/Disable switch (toggles with Return key (CR))
- Gateway peer (name or IP address)
- Group name
- Group key
- Xauth user name (if static)
- Xauth password (if static)
- Set PIN
 - If the PIN has been set, the user is prompted for it before a locally stored Xauth user name and password are used.
- Diffie-Hellman group
- IKE Phase 1 lifetime
 - Session timeout (idle timeout, after which VPN connection is dropped)
- Authentication (for HTTP authentication)
 - Enable/Disable switch
 - Port number
- Security

- Set password (lock configuration under password control)
- Status
 - Version (equivalent to *STOP-V*)
- Advanced
 - Download Configuration
 - Keyboard Country Code
 - Bandwidth Limit (in bits per second)
 - Session Disconnect (*STOP-Q*)
 - Force Compression
 - Lossless Compression
 - Disallow utload
 - Force Full Duplex
 - Video (set blanking timeout)
- Clear Configuration (also available with *STOP-C*)

FIGURE 7-7 Advanced Menu (Part I)



The Download Configuration entry on the Advanced Menu prompts for a server name and file name of a file to be downloaded from the server, in the form `<server>:<filename>`. The default server is the TFTP server value if defined, and the default file name is `config.<MAC>`, where `<MAC>` is the unit's *MAC address* in upper-case hexadecimal. This field can be overwritten when selected. Pressing Enter causes the corresponding file to be read and the configuration values parsed and set. For configuration values, see [TABLE 7-5](#).

On success, the user is prompted to save the values, otherwise the previous menu is displayed. No other error indications are given.

Some of the menus have an `Exit` entry, but the `Escape` key always invokes one level higher than the current menu. `Escape` at the top level prompts for any changes to be saved or discarded. If changes have been written to the flash, the `Escape` key resets the DTU.

The `Keyboard Country Code` value is a keyboard country code that is applied to a keyboard that returns a country code of 0, for use with non-U.S. keyboards that do not report a country code.

The `Session Disconnect` setting enables or disables the ability to terminate a session by entering `STOP-Q` from the keyboard. This is useful when it's desired to terminate a VPN connection and leave the Sun Ray in a quiescent state. Hitting the `Escape` key after the session has terminated will cause a reboot of the Sun Ray DTU.

The `Force Compression` setting sets a tag sent from the Sun Ray DTU to the Xserver telling it to enable compression, regardless of available bandwidth.

FIGURE 7-8 Advanced Menu (Part II)



The `Lossless Compression` setting disables the use of lossy compression for image data.

The `Disallow utload` setting disables the ability to explicitly force a firmware load into a DTU. In this way, firmware can be tightly controlled using `.parms` files or DHCP parameters.

The `Force Full Duplex` setting allows the DTU to operate correctly when the network port that it is connected to does not auto-negotiate. In that case, the auto-negotiation results in the Sun Ray running at half duplex, which significantly impacts network performance. This setting allows the Sun Ray to operate with better performance in this situation.

Note – Support for the `Force Full Duplex` setting may not be available in the network device driver.

Remote Loading of Configuration Data

To help avoid error-prone manual entry of configuration data for deployments where pre-configuration is required, you can use the Pop-up GUI to download a configuration to a Sun Ray DTU from a file on a server via TFTP, as indicated in [FIGURE 7-7](#).

The following keywords correspond to configuration values that can be set from Pop-up GUI menus (see [“Pop-up GUI” on page 108](#)). To group items that are logically related, some of the keywords take the form *<family>.<field>*.

TABLE 7-5 Pop-up GUI Menu Configuration Values

VPN/IPsec Submenu	Comment
vpn.enabled	Enable toggle
vpn.peer	Remote gateway name/IP address
vpn.group	VPN group
vpn.key	VPN key
vpn.user	Xauth user
vpn.passwd	Xauth password
vpn.pin	PIN lock for use of user/passwd
vpn.dhgroup	Diffie-Hellman group to use
vpn.lifetime	Lifetime of IKE connection
vpn.killtime	Idle timeout value to drop VPN connection.
DNS Submenu	
dns.domain	Domain name
dns.servers	Server list (comma-separated IP addresses)
Servers Submenu	
servers	Sun Ray server
tftpserver	TFTP server
loghost	Syslog host
Security Submenu	
password	Set administrator password
TCP/IP Submenu	
ip.ip	Static IP

TABLE 7-5 Pop-up GUI Menu Configuration Values

ip.mask	Static netmask
ip.bcast	Static broadcast address
ip.router	Static router
ip.mtu	MTU
ip.type	Type of network (“DHCP” “Static”)
Advanced Submenu	
kbcountry	Keyboard country code
bandwidth	Bandwidth limit in bits
stopqon	Enable (1) or Disable (0) STOP-Q for disconnect
compress	Force compression on when 1
lossless	Force use of lossless compression when 1
utloadoff	Disallow use of utload to force firmware download when 1

The format of the file is a set of `<key>=<value>` lines, each terminated by a newline character, which are parsed and the corresponding configuration items set (see the sample file below). No whitespace is permitted. Key values are case-sensitive, always lower case, as listed above. Setting a keyword to have a null value results in the configuration value being cleared in the local configuration.

FIGURE 7-9 Sample VPN Configuration File

```
vpn.enabled=1
vpn.peer=vpn-gateway.sun.com
vpn.group=homesunray
vpn.key=abcabcabc
vpn.user=johndoe
vpn.passwd=xyzzyzxyzy
dns.domain=sun.com
tftpserver=config-server.sun.com
servers=sunray3,sunray4,sunray2
```

Ports and Protocols

TABLE 7-6 and TABLE 7-7 summarize Sun Ray port and protocol usage. In TABLE 7-6, a double-headed arrow in the Flow column indicates the direction of the initial packet. In most cases the DTU initiates the interaction.

The range of dynamic/UDP ports on the server is constrained to the range defined by the `utservices-low` and `utservices-high` UDP service definitions, whose default values in `/etc/services` are 40000 and 42000 respectively.

- Dynamic/TCP ports on the DTU are in the range 32768-65535.
- Dynamic/UDP ports on the DTU are in the range 4096-65535.
- ALP rendering traffic (ALP-RENDER) always uses a UDP port number greater than 32767 at the DTU.

TABLE 7-6 Sun Ray DTU-to-Server Ports and Protocols

DTU Port	Flow	Protocol	Flow	Server Port	Peer	Importance	Comments
66/UDP (BOOTPC/ DHCP)	--broadcast->> --unicast->>	DHCP	<-broadcast-- <-unicast--	67/UDP (BOOTPS/DH CPS)	DHCP Service	Mandatory	Network and configuration parameter discovery
Dynamic/ UDP	--unicast->>	TFTP	<-unicast--	69/UDP (TFTP)	TFTP Service	Recommended	Firmware download (Since SRSS 3.1: configuration parameter download)
Dynamic/ UDP	--unicast->>	DNS	<-unicast--	53/UDP (domain)	DNS Service	Optional	Introduced in SRSS 3.1 for server name lookups.
514/ UDP (syslog)	--unicast->>	Syslog	(none)	514/UDP (syslog)	Syslog Service	Optional	Event reporting
Dynamic/ UDP	--broadcast->>	ALP- DISCOVERY	<-unicast--	7009/UDP (utauthd-gm)	Sun Ray Server	Optional	On-subnet Sun Ray Server discovery
Dynamic/ TCP	--unicast->>	ALP- AUTH	<-unicast--	7009/TCP (utauthd)	Sun Ray Server	Mandatory	Presence, control, status

TABLE 7-6 Sun Ray DTU-to-Server Ports and Protocols

DTU Port	Flow	Protocol	Flow	Server Port	Peer	Importance	Comments
Dynamic/UDP with port number >= 32768	--unicast-> or --unicast->> when NAT is in use	ALP-RENDER	<<-unicast-- or <-unicast-- when NAT is in use	Dynamic/UDP constrained by utservices-low and utservices-high	Sun Ray Server	Mandatory	On-screen drawing, user input, audio
Dynamic/TCP	-unicast->>	ALP-DEVMGR	<-unicast--	7011/TCP (utdevmgr)	Sun Ray Server	Optional	Device management
7777/TCP	--unicast->	ALP-DEVDATA	<<-unicast--	Dynamic/TCP	Sun Ray Server	Optional	Device data transfer
7013/UDP (utquery)	--unicast->	ALP-QUERY	<<-unicast-- <<-broadcast--	Dynamic/UDP	Any	Optional	utquery support

TABLE 7-7 Sun Ray Server-to-Server Protocols

Sun Ray Server Port	Protocol	Port	Peer	Notes
	<<-ARP->>		All on subnet	IP-to-MAC mapping
Transient	--SYSLOG/UDP unicast->>	514 (SYSLOG)	Syslog Server	Status reporting, if required
7009 (UTAUTHD)	<<-UTAUTHD-GM/UDP->> broadcast or multicast	7009 (UTAUTHD)	Sun Ray Server	Group discovery, if required
7011 (UTDEVMGRD)	<<-UTDEVMGRD/TCP->>	7011 (UTDEVMGR)	SR Group Member	Device control and status
7008 (UTRCMD)	<<-UTDEVMGRD/TCP->	Privileged	SR Group Member	Remote execution
	<<-ICMP ECHO->		Any	Admin: presence (a bug)
7010 (UTAUTH-CB)	<<-UTAUTH-CB/TCP->	Transient	Any	Admin: control and status
7012 (UTDS)	<<-UTDS/TCP->	Transient	Any	Data store, if required
7007 (UTSESSIOND)	<<-UTSESSION/TCP->	Transient	Any	Session members
7011 (UTDEVMGR)	<<-UTDEVMGR/TCP->	Transient	Any	Device clients
1660 (HTTPS)	<<-HTTPS/TCP->	Transient	Localhost	Web GUI, if configured
1660 (HTTP)	<<-HTTP/TCP->	Transient	Localhost	Web GUI, if configured
7007 (UTSESSIOND)	<<-UTSESSION/TCP->	Privileged	Localhost	Session management

Gnome Display Manager

The Gnome Display Manager (GDM) is responsible for logging users into your system and starting their sessions (X11 server plus applications). It is typically used to manage the console on a system that is configured with a graphics device, but it may also be used to manage other displays attached to a system.

Note – The default version of the GDM supplied with your system does not work in a Sun Ray environment. Therefore, Sun Ray Server Software includes a GDM that has been enhanced with the ability to manage Sun Ray devices. This enhanced GDM is otherwise identical to the GDM it replaces, and can still be used to manage the console and/or other displays.

Installation

During the SRSS installation process, you are asked whether the installation script should remove the existing GDM from your system. Answer Yes to this question to continue with the SRSS installation, remove the old GDM from your system and install the Sun Ray-enhanced version. If you answer No, the SRSS install process aborts.

Since the existing GDM is removed during SRSS installation, do not use a GDM-controlled display to do the install. Use either a telnet session into the server or a virtual terminal.



Caution – Sun Ray Server Software requires its own Sun Ray-enhanced Gnome Display Manager. If you update your system with a newer GDM, SRSS will not be able to run, and DTUs with 2.0 or newer firmware will display the 26D icon.

Tip – If you are using an automatic update system, such as Red Hat’s `up2date`, you may wish to alter your configuration files to ignore GDM.

Uninstallation

If you need to remove the SRSS software, you will be asked whether the Sun Ray-enhanced GDM should remain on your system. If you answer No, you may have to install the original GDM RPM if you want non-Sun Ray displays, such as the console, to be managed.

Configuration

The Sun Ray GDM is based on version 2.4.4.7. If you have already upgraded your system to a newer version of GDM, the Sun Ray version may not have all the features you expect.

Sun Ray installation will remove the current GDM from your system, including its configuration file, `/etc/X11/gdm/gdm.conf` (or `/etc/gnome2/gdm/gdm.conf` on SuSE systems)

Therefore, if you have modified to your `gdm.conf` configuration, back the file up before installing SRSS. You may wish to reapply your changes to the `gdm.conf` that SRSS installs.

Tip – Do not simply put your old `gdm.conf` in place of the SRSS-installed one, Sun Ray Server Software will not work correctly.

The default configuration for GDM is to manage `DISPLAY 0` (zero) on the console. If you do not wish to start an X11 server on the console, edit `/etc/X11/gdm/gdm.conf` and remove `DISPLAY 0` from the servers section.

Gnome Display Manager Privileges

Many Linux systems come configured with liberal administrative privileges for non-root users. You most likely do *not* want these privileges offered to users who login using a Sun Ray DTU. Please review the man pages for `pam_console`, `console.perms`, and `console.apps`. It is also a good idea to edit the `/etc/security/console.perms` file to remove display numbers from the definition of `console`. If a definition exists for `xconsole`, it should be removed entirely.

For example, a line that reads:

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]* :[0-9]`[0-9] :[0-9]
```

should instead read:

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]*
```

And a line such as:

```
<xconsole>=: [0-9]`[0-9] : [0-9]
```

should be removed altogether.

Bundled Greeter

If you are using Kiosk mode, please see the `kiosk` man page for details on the bundled `gtmgreeter`. See also [“Kiosk Mode” on page 135](#) of this manual and [“Kiosk Session” on page 31](#) in the *Sun Ray Connector for Windows OS, Version 2.0 Installation and Administration Guide*.

Multihead Administration

The multihead feature on Sun Ray™ DTUs enables users to control separate applications on multiple displays, also called screens, or *heads*, using a single keyboard and pointer device attached to the primary DTU. Users can also display and control a single application, such as a spreadsheet, on multiple screens. System administrators create multihead groups that can be accessed by users. A multihead group, consisting of between two and 16 DTUs controlled by one keyboard and mouse may be composed of virtually any mix of Sun Ray DTUs, such as Sun Ray 1, Sun Ray 100, Sun Ray 150, Sun Ray 170, and Sun Ray 270, for instance. Each DTU other than the Sun Ray 2FS¹ presents an X screen of the multihead X display.

For the multihead feature to function properly:

1. You must be in administered mode; therefore, you must run `utconfig` before you run `utmhconfig` or `utmhadm`.
2. You must enable the multihead policy using either `utpolicy` or the Admin GUI.
3. Always run `utmhconfig` from a Sun Ray DTU.

Note – Regional hotdesking is not enabled for multihead groups.

1. The Sun Ray 2FS is designed to run a single display across two screens without additional configuration. It utilizes a single frame buffer for two displays, always treating two attached heads as a single, unified display surface to be controlled with a single mouse and keyboard, and always presenting itself to the Xserver as a single screen.

Multihead Groups

A multihead group is comprised of a set of associated Sun Ray DTUs controlled by a primary DTU to which a keyboard and pointer device, such as a mouse, are connected. This group, which can contain a maximum of 16 DTUs, is connected to a single session.

The primary DTU hosts the input devices associated with the session. The remaining DTUs, called the secondaries, provide the additional displays. All peripherals are attached to the primary DTU, and the group is controlled from the primary DTU.

Multihead groups can be created easily by using a smart card to identify the terminals with the `utmhconfig` GUI utility.

However, if you disconnect the secondary DTUs without deleting the multihead group to which they belong, the screens are not displayed on the single primary DTU. The primary DTU is still part of the multihead group, and the mouse seems to get lost when it goes to the disconnected secondary DTU. To recover from this situation, you can either reconnect the missing DTU, or delete the multihead group using the `utmhconfig` or `utmhadm` command, or you can delete the multihead group, replace the missing DTU, and create a new multihead group that incorporates the replacement DTU.

Multihead Screen Configuration

A multihead group can have its screens arranged in various configurations. For example, a user can arrange a multihead group of four screens as two rows of two screens (2x2) or as a single row of four screens (4x1). By default, when a user logs into a multihead group, the session uses the number of screens available; the layout, or geometry of these displays is generated automatically. You can use the `-R` option to `utxconfig` to manipulate the automatic geometry, as in the following examples:

- **To override the automatic geometry, where geometry is expressed as *columns x rows*:**

```
% utxconfig -R geometry
```

- **To restore the automatic geometry on the next login:**

```
% utxconfig -R auto
```

When the mouse pointer is moved past the edge between two screens, it moves from one screen to the next. The geometry of the multihead group determines which screen is displayed at that moment.

Screen dimensions for the multihead group are automatically set, by default, to the largest supported by the primary DTU. The primary DTU is the one that controls the other DTUs in the group and to which all peripherals are attached.

To override the automatic sizing of screen dimensions, use the `-r` option to `utxconfig`:

- To override automatic sizing, where dimensions are expressed as *width x height* (for example, 1280 x 1024):

```
% utxconfig -r dimensions
```

- To restore automatic sizing behavior on the next login:

```
% utxconfig -r auto
```

- To explicitly choose not to use multiple displays for a session, type:

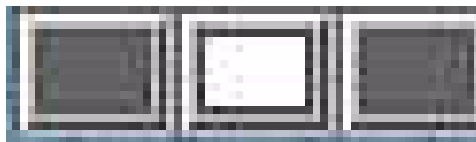
```
% utxconfig -m off
```

Note – If explicit screen dimensions are chosen, or if the resolutions of the monitors differ, you may have problems with unwanted on-screen movement called *panning*, or large *black bands* around the visible screen area.

Multihead Screen Display

When the multihead feature is used, a small window indicating the current session on each screen is displayed with the current screen highlighted for easy identification. This window is automatically displayed for users during session creation. For example, the display in [FIGURE 9-1](#) indicates that the user is on the second screen of a three-screen display.

FIGURE 9-1 The Multihead Screen Display



Multihead Administration Tool

The administration tool for the multihead feature displays the current multihead groups and enables you to create new groups.

▼ To Enable Multihead Policy From the Command Line

- On the command-line interface, type:

```
# /opt/SUNWut/sbin/utpolicy -a -m -g your_policy_flags  
# /opt/SUNWut/sbin/utrestart
```

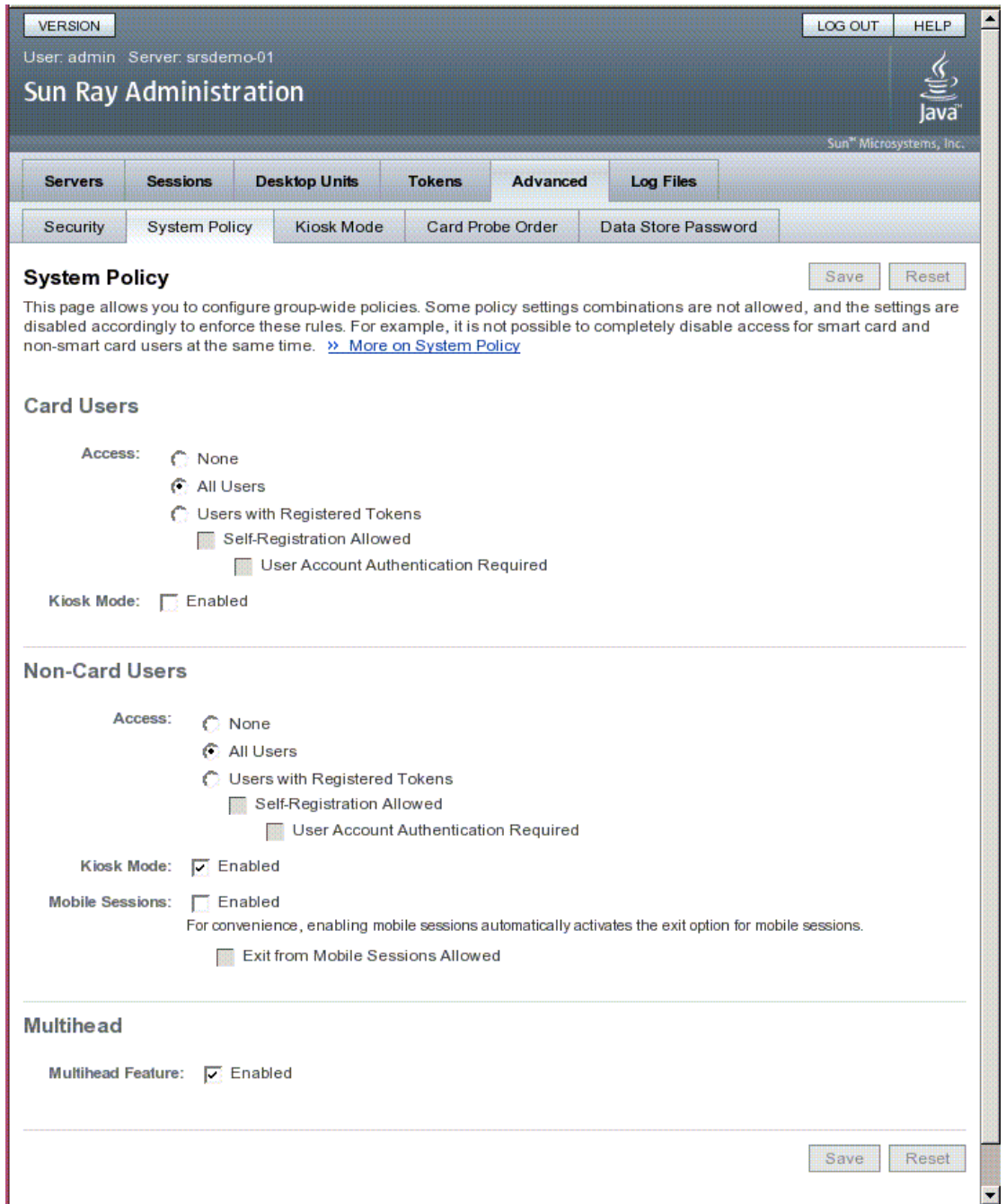
This enables the multihead policy for the failover group and restarts Sun Ray Server Software with the new policy on the local server without disrupting existing sessions.

Tip – Issue the `utrestart` command on every server in the failover group.

▼ To Enable Multihead Policy Using the Admin GUI

1. Start the Admin GUI.
2. Select the Advanced tab.

FIGURE 9-2 Multihead Feature Enabled



3. Select the System Policy tab (see [FIGURE 9-2](#)).
4. Select (or deselect) the Multihead Feature Enabled check box.
5. Click the Save button.

If a system restart is needed, an advisory message will appear.

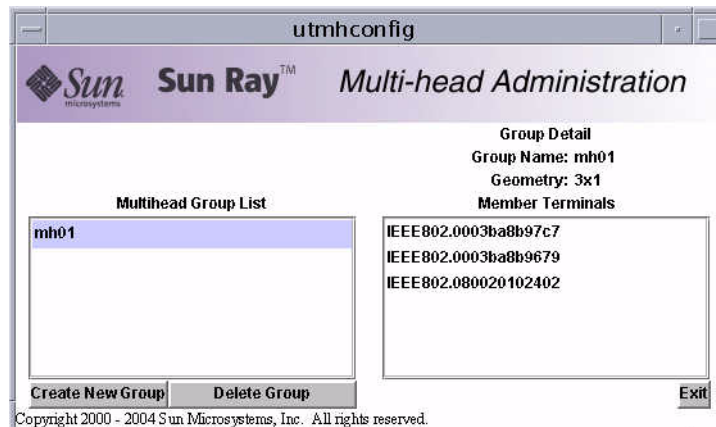
▼ To Create a New Multihead Group

1. On the command-line interface, type:

```
# /opt/SUNWut/sbin/utmhconfig
```

2. On the initial screen, click Create New Group.

FIGURE 9-3 utmhconfig GUI Lists Multihead Groups and Details



The Create New Multiheaded Group pop-up dialog box is displayed. The number of rows and the number of columns you enter are displayed as the group geometry when the group has been created.

FIGURE 9-4 Create New Multiheaded Group Pop-up Dialog Box



3. Enter the information for the group.

Enter a name for the group and the number of rows and columns.

4. Click the Next button.

A third screen is displayed.

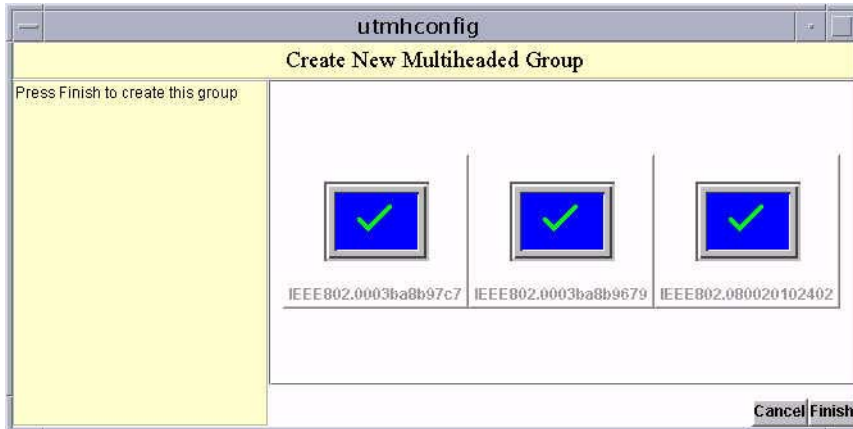
FIGURE 9-5 Setup Display for the New Multihead Group



5. Select the DTUs within the multihead group and insert a smart card in each Sun Ray DTU in turn to establish the order of the group.

The Finish button, which was previously grayed out, is now active.

FIGURE 9-6 Completed Multihead Group List With Active Finish Button



6. Click the Finish button.
7. Exit the session or disconnect by removing your card.

XINERAMA

The XINERAMA extension to X11 creates a single large screen displayed across several monitors. With XINERAMA, only one toolbar is displayed, and a window can be moved smoothly from one part of the screen to the next.

Tip – XINERAMA tends to consume a lot of CPU, memory, and network bandwidth, so for reasonable performance, set the `shmsys:shminfo_shmmax` parameter in the `/etc/system` file to at least $LARGEST_NUMBER_OF_HEADS * width * height * 4$.

Users can enable or disable XINERAMA as part of their X preferences. The `utxconfig` command handles this on an individual token basis; however, the user must log off for this changes to take effect.

The XINERAMA feature is enabled using the following command:

```
% utxconfig -x on
```

The XINERAMA feature is disabled using the following command:

```
% utxconfig -x off
```

To enable as default for a single system or failover group, as superuser, type the following command:

```
% utxconfig -a -x on
```

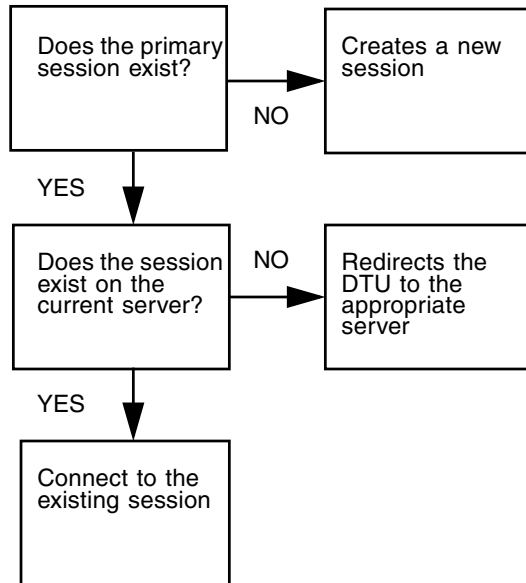
Session Groups

If you hotdesk from a multihead group to a DTU that is not part of a multihead group—that is, a DTU with a single head—you can view all the screens created in the original multihead group on the single screen, or head by panning to each screen in turn. This is called *screen flipping*.

Authentication Manager

The TerminalGroup policy module extends the Authentication Manager to support multihead groups. When a DTU connects to the Authentication Manager or a new smart card is inserted, the TerminalGroup module queries its database to determine whether the DTU is part of a multihead group and, if so, whether the DTU is a primary or secondary DTU of that group. If it is not identified as part of a multihead group, the DTU is treated normally.

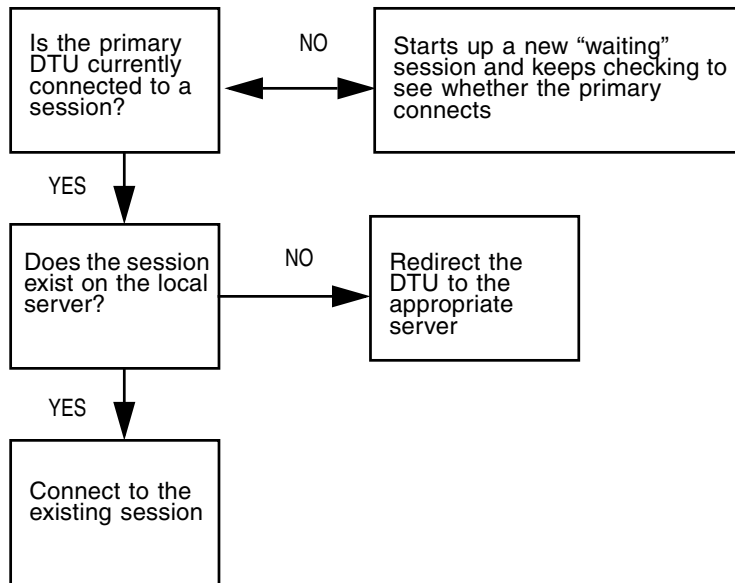
FIGURE 9-7 Authentication Manager Flowchart for the Primary DTU



If the DTU is determined to be part of a multihead group and it is the multihead group's primary DTU, a normal session placement occurs. If a session does not exist on the current server, but there is a preexisting session for the DTU or smart card on another server in the failover group, the primary DTU will be redirected to that server. If there is no session on any server, the request for a session is directed to the least-loaded server and a session is created there.

If a DTU is determined to be part of a multihead group, and it is a multihead group secondary DTU, the TerminalGroup module determines whether the multihead group primary DTU is locally attached to a session. If so, it tells the Session Manager to allow the secondary DTU to attach to that session also. If the primary DTU is not attached locally, the TerminalGroup module determines whether the primary DTU is attached to another server in the failover group (if any), and if it is, it redirects the secondary DTU to that server.

FIGURE 9-8 Authentication Manager Flowchart for the Secondary DTU



If the primary DTU is determined to not be attached to any server in the failover group at that moment, a Waiting for Primary icon is displayed on the DTU, and further activity is blocked on that DTU until the primary is discovered. The secondary DTU is redirected to the server to which the primary is attached.

Kiosk Mode

This chapter describes Kiosk Mode, which enables controlled, simplified access to anonymous users without compromising the security of the Sun Ray server. For a detailed explanation of Kiosk Mode functionality, see `kiosk(5)`.

In earlier releases of Sun Ray Server Software, Kiosk Mode was known as Controlled Access Mode (CAM).

Topics include:

- [“Enabling Kiosk Mode” on page 135](#)
- [“Overriding Kiosk Mode Policy” on page 140](#)
- [“Building the Kiosk Mode Environment” on page 142](#)
- [“Security and Failover Considerations” on page 146](#)



Caution – Sun Ray Server Software and NIS (Network Information System) store user names and groups in the same system file (`/etc/passwd`). Be sure to use unique user names when setting up a Kiosk Mode application if the same physical server is used to host both the Sun Ray Server Software and the NIS software. If both systems use the same user names, then the `utconfig -u` command can overwrite the NIS entries.

Enabling Kiosk Mode

Kiosk Mode allows the administrator to specify what types of sessions are available to users, based on policy choices for different types of user and usage scenario. For instance, settings can differ for smart card users as opposed to non-smart card users, for those with registered as opposed to unregistered tokens, and for other characteristics.

Kiosk Mode functionality can be enabled and disabled from the System Policy section of the Advanced tab, and administered from the Kiosk Mode section, which provides check boxes to enable Kiosk Mode for smart card users, non-smart card users, or both. Enabling and disabling Kiosk Mode for individual tokens is described in the [“Overriding Kiosk Mode Policy” on page 140](#).

Note – Before enabling Kiosk Mode, you must configure it with the `utconfig` utility.

Enabling Kiosk Mode Using the CLI

As superuser, type the `utpolicy` command for your authentication policy with the addition of the `-k` argument. Some examples are suggested below.

Note – The following options determine access to the Sun Ray server:

`-z both/pseudo/card`

or

`-r both/pseudo/card [-s both/pseudo/card]`

The `-k both/pseudo/card` option determines whether some or all of the granted sessions are Kiosk sessions.

▼ To Enable Kiosk Mode for All Users (Card and Non-card)

```
# /opt/SUNWut/sbin/utpolicy -a -M -s both -r both -k both
```

All users are directed to Kiosk sessions.

▼ To Enable Kiosk Mode for Card Users Only

```
# /opt/SUNWut/sbin/utpolicy -a -M -s both -r both -k card
```

Only card users are directed to Kiosk sessions.

▼ To Enable Kiosk Mode for Non-card Users Only

```
# /opt/SUNWut/sbin/utpolicy -a -M -s both -r both -k pseudo
```

Only non-card users are directed to Kiosk sessions.

▼ To Enable Both Card and Non-Card Sessions

```
# /opt/SUNWut/sbin/utpolicy -z both -k pseudo
```

Card sessions are non-Kiosk (ordinary login) sessions. Non-card sessions are Kiosk sessions.

▼ To Allow Only Card Sessions in Kiosk Mode

```
# /opt/SUNWut/sbin/utpolicy -z card -k card
```

All sessions are in Kiosk Mode and available only to card users unless you specify overrides.

▼ To Enable Regular Sessions for Registered Cards and Kiosk Sessions for Non-Card Users

```
# /opt/SUNWut/sbin/utpolicy -r card -z pseudo -k pseudo
```

Non-card sessions are Kiosk sessions. Non-Kiosk card sessions are allowed only for registered tokens.

▼ To Enable Kiosk Sessions for Registered Cards and Regular Sessions on Registered DTUs

```
# /opt/SUNWut/sbin/utpolicy -r both -s both -k card
```

Card sessions are Kiosk sessions, non-card sessions are non-Kiosk (ordinary login) sessions. Users can self-register card tokens and DTUs.

Enabling Kiosk Mode Using the Admin GUI

The Admin GUI presents a set of choices that may be more convenient to use than the CLI.

▼ To Enable Kiosk Mode Using the Admin GUI

1. **Start the Admin GUI.**
2. **Select the Advanced tab.**
3. **Select the System Policy tab (see [FIGURE 10-1](#)).**
4. **Select the Kiosk Mode checkbox in the Card Users section, the Non-Card Users section, or both, depending on whether you wish to enable Kiosk Mode for card users, non-card users, or both.**
5. **Click the Save button.**
6. **Select the Servers tab**
7. **Select the relevant server(s) from the list of servers.**
8. **Click the Cold Restart button.**

FIGURE 10-1 Kiosk Mode Enabled for Non-Card Users

The screenshot shows the Sun Ray Administration interface. At the top, there is a header with 'VERSION', 'LOG OUT', and 'HELP' buttons. Below the header, the user is identified as 'admin' on server 'srsdemo-01'. The main navigation bar includes 'Servers', 'Sessions', 'Desktop Units', 'Tokens', 'Advanced', and 'Log Files'. A secondary navigation bar shows 'Security', 'System Policy', 'Kiosk Mode', 'Card Probe Order', and 'Data Store Password'. The 'System Policy' section is active, displaying a 'Save' and 'Reset' button. The 'System Policy' text explains that some settings are disabled. The 'Card Users' section has 'Access' set to 'All Users' and 'Kiosk Mode' set to 'Disabled'. The 'Non-Card Users' section has 'Access' set to 'All Users', 'Kiosk Mode' set to 'Enabled', and 'Mobile Sessions' set to 'Disabled'. The 'Multihead' section has 'Multihead Feature' set to 'Enabled'. 'Save' and 'Reset' buttons are at the bottom right.

VERSION LOG OUT HELP

User: admin Server: srsdemo-01

Sun Ray Administration

Sun Microsystems, Inc.

Servers Sessions Desktop Units Tokens Advanced Log Files

Security System Policy Kiosk Mode Card Probe Order Data Store Password

System Policy

Save Reset

This page allows you to configure group-wide policies. Some policy settings combinations are not allowed, and the settings are disabled accordingly to enforce these rules. For example, it is not possible to completely disable access for smart card and non-smart card users at the same time. [More on System Policy](#)

Card Users

Access:

- None
- All Users
- Users with Registered Tokens
 - Self-Registration Allowed
 - User Account Authentication Required

Kiosk Mode: Enabled

Non-Card Users

Access:

- None
- All Users
- Users with Registered Tokens
 - Self-Registration Allowed
 - User Account Authentication Required

Kiosk Mode: Enabled

Mobile Sessions: Enabled

For convenience, enabling mobile sessions automatically activates the exit option for mobile sessions.

- Exit from Mobile Sessions Allowed

Multihead

Multihead Feature: Enabled

Save Reset

Overriding Kiosk Mode Policy

It may be desirable to use a different authentication policy setting or kiosk session configuration for a particular smart card or DTU, or subset of smart cards or DTUs, than for other smart cards or DTUs. You can override Kiosk Mode policy with `utkioskoverride` or with the GUI. You can override the default Kiosk session selection with `utkioskoverride`.

For more detailed information on overriding Kiosk Mode policy and Kiosk session selection, see the `utkioskoverride(1m)` man page.

Note – Overriding the Kiosk session selection and administration of non-default Kiosk session configurations are not supported by the Admin GUI in this release. Use the `utkioskoverride` and `utkiosk` commands to access these features.

▼ To Override Kiosk Mode Policy Using the CLI

Use the `utkioskoverride` command to override Kiosk Mode policy or assign a non-default kiosk session for a user’s smart card token or for a DTU’s pseudo-token. Several usage examples are listed below.

Note – Only registered tokens—those that have already been registered—can be assigned policy overrides.

- To enable Kiosk sessions regardless of Kiosk Mode policy for the registered smart card `MicroPayFlex.12345678`:

```
# /opt/SUNWut/sbin/utkioskoverride -s kiosk -r \  
MicroPayFlex.12345678
```

- To disable Kiosk sessions regardless of Kiosk Mode policy for the registered smart card `MicroPayFlex.12345678`:

```
# /opt/SUNWut/sbin/utkioskoverride -s regular -r \  
MicroPayFlex.12345678
```

- To disable Kiosk sessions regardless of Kiosk Mode policy for the logical token `user.12345678`:

```
# /opt/SUNWut/sbin/utkioskoverride -s regular -t user.12345678
```

- To assign and enable the non-default kiosk session `MySession2`, stored using `utkiosk`, to the logical token `user.12345678`, regardless of Kiosk Mode policy:

```
# /opt/SUNWut/sbin/utkioskoverride -s kiosk -c MySession2 \  
-t user.123456-78
```

▼ To Override Kiosk Mode Policy Using the Admin GUI

1. Select the Tokens tab.

2. Select the token of interest from the list of tokens.

This token can be a card owner's smart card token or a pseudo-token associated with a DTU's *MAC address*. However, only tokens that have been registered in the Sun Ray data store can be overridden. To register a smart card token, see [“To Register a Token” on page 48](#). To register a pseudo-token, see [“To Register a Pseudo-Token” on page 49](#).

3. Click the Edit button.

4. Select the desired Session Type from the list of available session types.

The available session types are Default, Kiosk, and Regular.

- a. Select Default to prevent Kiosk Mode policy from being overridden for this token.

or

- b. Select Kiosk to use a Kiosk session for this token regardless of Kiosk Mode policy.

or

- c. Select Regular to ensure that a Kiosk session is not used for this token, regardless of Kiosk Mode policy.

5. Click the OK button.

FIGURE 10-2 Edit Token Properties

VERSION LOG OUT HELP

User: admin Server: srsdemo-01

Sun Ray Administration

Sun Microsystems, Inc.

Servers Sessions Desktop Units Tokens Advanced Log Files

Tokens > MicroPayflex.5001430700130100

Edit Token Properties - MicroPayflex.5001430700130100

OK Cancel

* Indicates required field

General

* Owner: Tech Pubs demo

Other Information: use to illustrate manual

Status: Enabled

Advanced

Session Type: Default

- Default
- Kiosk
- Regular

Select Session Type

OK Cancel

Note – The Edit Token Properties page does not show whether a non-default Kiosk session has been assigned to a token. If you use the Admin GUI to assign a Kiosk session type to a token, the default Kiosk session configuration is used for this token.

Building the Kiosk Mode Environment

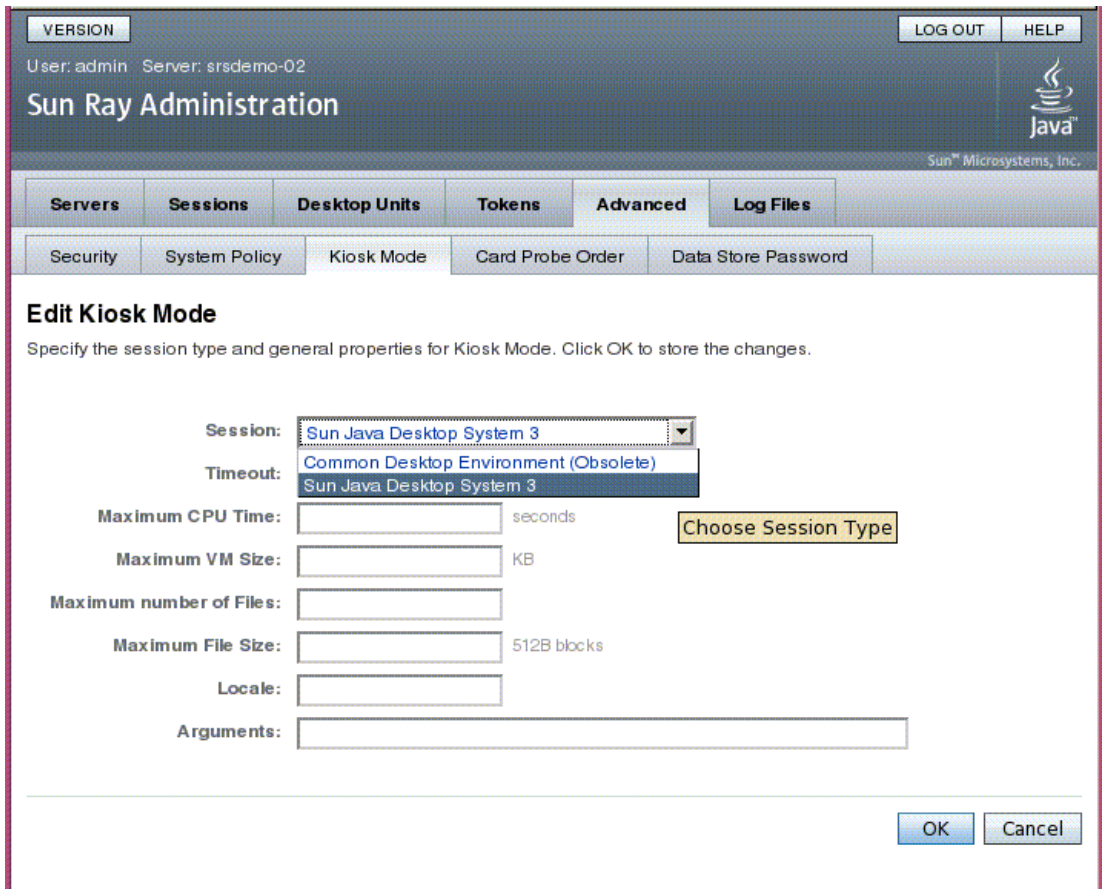
Once you have selected a Kiosk session, that session is launched by default to provide basic Kiosk Mode functionality. Some Kiosk sessions will support the addition of applications to extend this basic functionality.

Note – Kiosk session and application configuration data created with the Admin GUI is stored as the default Kiosk session under the name `session`. To store non-default Kiosk session configurations, use the `utkiosk` command.

▼ To Configure Kiosk Mode Settings

1. Select the **Advanced** tab.
2. Select the **Kiosk Mode** tab.
3. Click the **Edit** button.

FIGURE 10-3 Edit Kiosk Mode



The screenshot displays the Sun Ray Administration web interface. At the top, it shows the user 'admin' on server 'srsdemo-02'. The main navigation bar includes tabs for Servers, Sessions, Desktop Units, Tokens, Advanced, and Log Files. The 'Advanced' tab is selected, and within it, the 'Kiosk Mode' sub-tab is active. The 'Edit Kiosk Mode' dialog box is open, prompting the user to specify session type and general properties. The dialog includes a dropdown menu for 'Session' (currently set to 'Sun Java Desktop System 3'), a 'Timeout' dropdown (with 'Common Desktop Environment (Obsolete)' and 'Sun Java Desktop System 3' visible), and input fields for 'Maximum CPU Time' (in seconds), 'Maximum VM Size' (in KB), 'Maximum number of Files', 'Maximum File Size' (in 512B blocks), 'Locale', and 'Arguments'. A 'Choose Session Type' button is highlighted in yellow. At the bottom right, there are 'OK' and 'Cancel' buttons.

4. Select your preferred Kiosk Session from the drop-down list, as shown in [FIGURE 10-3](#).
5. Provide appropriate values for the remaining settings. See [TABLE 10-1](#) for descriptions of individual settings.
6. Click the OK button.

Changes to Kiosk Mode Settings are applied automatically to Kiosk sessions that start after the changes have been saved. Thus, there is no need to restart Sun Ray services for changes to take effect.

TABLE 10-1 Kiosk Mode Settings

Setting	Description
Timeout	Indicates the number of seconds after which a disconnected session will be terminated. If you provide no value for this setting, termination of disconnected sessions will be disabled.
Maximum CPU Time	Indicates the maximum number of CPU seconds per process for Kiosk sessions. By default, the system default is applied to all Kiosk sessions. For more information see <code>ulimit(1)</code> .
Maximum VM Size	Indicates the maximum Virtual Memory size per process for Kiosk sessions. By default, the system default is applied to all Kiosk sessions. For more information see <code>ulimit(1)</code> .
Maximum Number of Files	Indicates the maximum number of open files per process for Kiosk sessions. By default, the system default is applied to all Kiosk sessions. For more information see <code>ulimit(1)</code> .
Maximum File Size	Indicates the maximum file size per process for Kiosk sessions. By default, the system default is applied to all Kiosk sessions. For more information see <code>ulimit(1)</code> .
Locale	Indicates the locale to be used by the Kiosk session. By default, the system default is applied to all Kiosk sessions.
Arguments	Indicates a list of arguments that should be passed to Kiosk sessions as they start. This is a Kiosk session-specific setting. For more information on supported arguments, consult the session-specific documentation for your selected session.



Caution – Choosing unsuitable values for `ulimit(1)` settings may cause Kiosk sessions to start incorrectly or to crash due to lack of resources.

▼ To Add an Application

1. Select the **Advanced** tab.

2. Select the Kiosk Mode tab.

If the currently selected Kiosk session supports the addition of applications, there is an Applications setting at the bottom of the page.

3. Click the New button.

a. To use one of the predefined Kiosk application descriptors:

i. Select Predefined Descriptor.

ii. Choose the relevant descriptor from the drop-down menu.

b. To define a custom Kiosk application descriptor:

i. Select Custom Path to use your own custom Kiosk application descriptor or a system application.

ii. Enter the path to your custom Kiosk application descriptor or executable.

If you choose Custom Path, indicate whether the path refers to a custom Kiosk application descriptor or an executable by choosing either Descriptor or Executable.

4. Select your preferred Start Mode for the application.

a. Choose USER to allow users to start the application themselves, for instance from a menu or launcher item.

b. Choose AUTO to make the application start automatically when the Kiosk session starts.

c. Choose CRITICAL to make the application start automatically when the Kiosk session starts, to allow users to start the application themselves, and to force the Kiosk session to restart if the application terminates.

5. Enter any application specific arguments.

Note – Individual Kiosk sessions may handle the various application start modes and arguments differently. For precise details on these, consult the session-specific documentation of your selected Kiosk session.

Security and Failover Considerations

Since Kiosk Mode bypasses the system login mechanism, you must consider the security of the applications added to the user environment. Many custom applications provide built-in security; however, other applications do not and are therefore not suitable for Kiosk Mode.

For example, adding an application such as `xterm` provides users with access to a command-line interface from a Kiosk Mode session. This is not desirable in a public environment and is not advised. However, using a custom application for a call center would be perfectly acceptable.

In a failover environment, the Kiosk Mode administrative settings are copied to the failover (i.e., secondary) servers. Be sure that all application descriptors and executable paths added to the Kiosk Mode sessions are copied across the servers in the failover group. For example, if the Mozilla application is added to the sessions with the executable path `/usr/sfw/bin/mozilla`, make sure that the path to the binary is available to all servers in the failover group. One way to ensure that sessions and applications are available on all servers in a failover group is to put them into a shared network directory, which is available on all hosts in the failover group.

Failover Groups

Sun Ray servers configured in a *failover group* (FOG) provide users with a high level of availability when one of those servers becomes unavailable because of a network or system failure. This chapter describes how to configure failover groups.

For a discussion on how to utilize multiple failover groups to utilize *regional hotdesking*, see “Hotdesking (Mobile Sessions)” on page 67.

This chapter covers these topics:

- “Overview” on page 147
- “Setting Up IP Addressing” on page 150
- “Group Manager” on page 155
- “Load Balancing” on page 157
- “Setting Up a Failover Group” on page 158
- “Viewing Administration Status” on page 161
- “Recovery Issues and Procedures” on page 162
- “Setting Up a Group Signature” on page 165
- “Taking Servers Offline” on page 166

Overview

A failover group consists of two or more Sun Ray servers grouped together to provide highly-available and scalable Sun Ray service for a population of Sun Ray DTUs. Releases earlier than 2.0 supported DTUs available to the servers only on a common, dedicated interconnect. Beginning with the 2.0 release, this capability was expanded to allow access across the LAN to either local or remote Sun Ray devices. However, the servers in a failover group must still be able to reach one another, using multicast or broadcast, over at least one shared subnet. Servers in a group

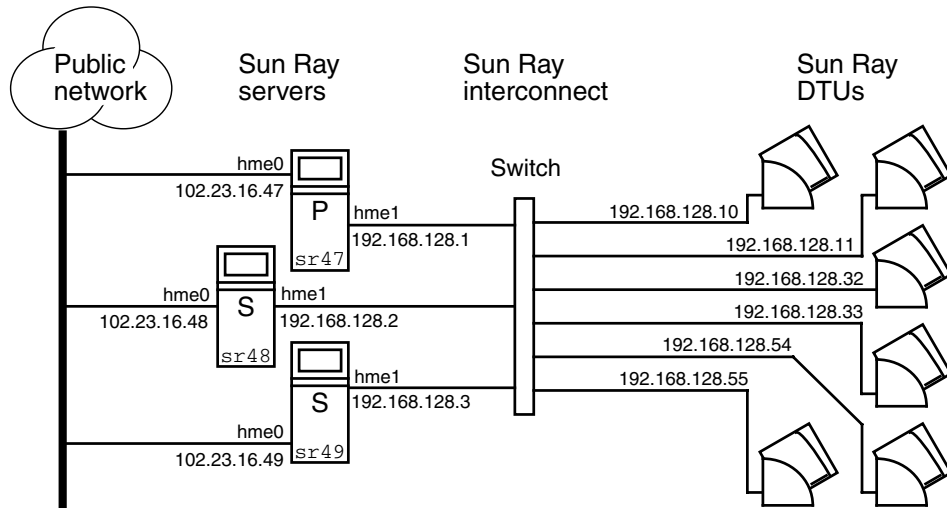
authenticate (or “trust”) one another using a common group signature. The group signature is a key used to sign messages sent between servers in the group; it must be configured to be identical on each server.

Failover groups that use more than one version of Sun Ray Server Software will be unable to use all the features provided in the latest releases. On the other hand, the failover group can be a heterogeneous group of Sun servers.

When a dedicated interconnect is used, all servers in the failover group should have access to, and be accessible by, all the Sun Ray DTUs on a given sub-net. The failover environment supports the same interconnect topologies that are supported by a single-server Sun Ray environment; however, switches should be multicast-enabled.

FIGURE 11-1 illustrates a typical Sun Ray failover group. For an example of a redundant failover group, see FIGURE 11-2.

FIGURE 11-1 Simple Failover Group



When a server in a failover group fails for any reason, each Sun Ray DTU connected to that server reconnects to another server in the same failover group. The failover occurs at the user authentication level: the DTU connects to a previously existing session for the user’s token. If there is no existing session, the DTU connects to a server selected by the load-balancing algorithm. This server then presents a login screen to the user, and the user must relogin to create a new session. The state of the session on the failed server is lost.

The principal components needed to implement failover are:

- Group Manager

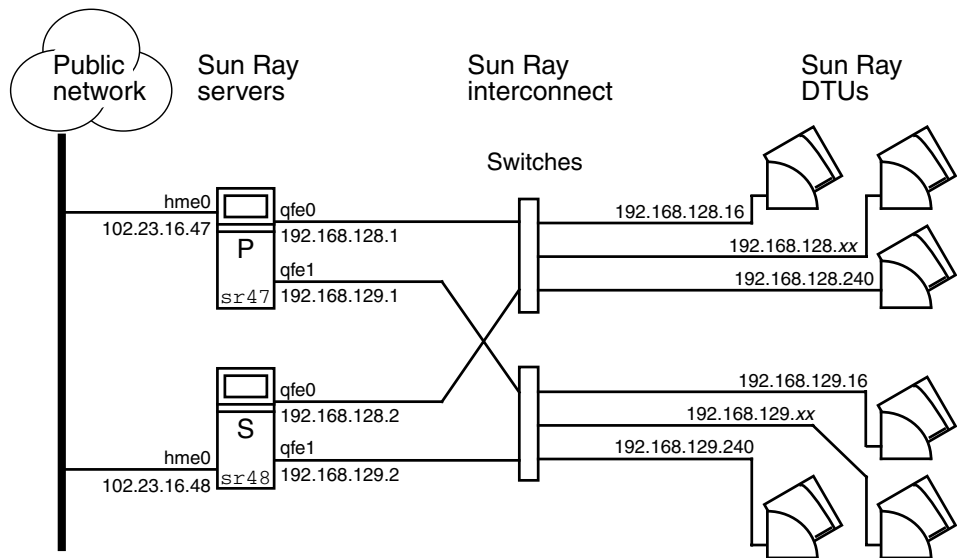
A module that monitors the availability (liveness) of the Sun Ray servers and facilitates redirection when needed.

- Multiple, coexisting Dynamic Host Configuration Protocol (DHCP) servers

All DHCP servers configured to assign IP addresses to Sun Ray DTUs have a non-overlapping subset of the available address pool.

Note – The failover feature cannot work properly if the IP addresses and DHCP configuration data are not set up properly when the interfaces are configured. In particular, if any Sun Ray server’s interconnect IP address is a duplicate of any other server’s interconnect IP address, the Sun Ray Authentication Manager throws “Out of Memory” errors.

FIGURE 11-2 Redundant Failover Group



The redundant failover group illustrated in [FIGURE 11-2](#) can provide maximum resources to a few Sun Ray DTUs. The server `sr47` is the primary Sun Ray server, and `sr48` is the secondary Sun Ray server; other secondary servers (`sr49`, `sr50` . . . are not shown).

Setting Up IP Addressing

The `utadm` command assists you in setting up a DHCP server. The default DHCP setup configures each interface for 225 hosts and uses private network addresses for the Sun Ray interconnect. For more information on using the `utadm` command, see the man page for `utadm`.

Before setting up IP addressing, you must decide upon an addressing scheme. The following examples discuss setting up class C and class B addresses.

Setting Up Server and Client Addresses

The loss of a server usually implies the loss of its DHCP service and its allocation of IP addresses. Therefore, more DHCP addresses must be available from the address pool than there are Sun Ray DTUs. Consider the situation of five servers and 100 DTUs. If one of the servers fails, the remaining DHCP servers must have enough available addresses so that every “orphaned” DTUs gets a new working address.

[TABLE 11-1](#) lists configuration settings used to configure five servers for 100 DTUs, accommodating the failure of two servers (class C) or four servers (class B).

TABLE 11-1 Configuring Five Servers for 100 DTUs

Servers	Class C (2 Servers Fail)		Class B (4 Servers Fail)	
	Interface Address	DTU Address Range	Interface Address	DTU Address Range
serverA	192.168.128.1	192.168.128.16 to 192.168.128.49	192.168.128.1	192.168.128.16 to 192.168.128.116
serverB	192.168.128.2	192.168.128.50 to 192.168.128.83	192.168.129.1	192.168.129.16 to 192.168.129.116
serverC	192.168.128.3	192.168.128.84 to 192.168.128.117	192.168.130.1	192.168.130.16 to 192.168.130.116
serverD	192.168.128.4	192.168.128.118 to 192.168.128.151	192.168.131.1	192.168.131.16 to 192.168.131.116
serverE	192.168.128.5	192.168.128.152 to 192.168.128.185	192.168.132.1	192.168.132.16 to 192.168.132.116

The formula for address allocation is: address range (AR) = number of DTUs/(total servers - failed servers). For example, in the case of the loss of two servers, each DHCP server must be given a range of $100/(5-2) = 34$ addresses.

Ideally, each server would have an address for each DTU. This would require a class B network. Consider these conditions:

- If AR multiplied by the total number of servers is *less than or equal to 225*, configure for a class C network
- If AR multiplied by the total number of servers is *greater than 225*, configure for a class B network

Tip – If all available DHCP addresses are allocated, it is possible for a Sun Ray DTU to request an address yet not find one available, perhaps because another unit has been allocated IP addresses by multiple servers. To prevent this condition, give each DHCP server enough addresses to serve the all the DTUs in a failover group.

Server Addresses

Server IP addresses assigned for the Sun Ray interconnect should all be unique. Use the `utadm` tool to assign them.

When the Sun Ray DTU boots, it sends a DHCP broadcast request to all possible servers on the network interface. One (or more) server responds with an IP address allocated from its range of addresses. The DTU accepts the first IP address that it receives and configures itself to send and receive at that address.

The accepted DHCP response also contains information about the IP address and port numbers of the Authentication Managers on the server that sent the response.

The DTU then tries to establish a TCP connection to an Authentication Manager on that server. If it is unable to connect, it uses a protocol similar to DHCP, in which it uses a broadcast message to ask the Authentication Managers to identify themselves. The DTU then tries to connect to the Authentication Managers that respond in the order in which the responses are received.

Note – For the broadcast feature to be enabled, the broadcast address (255.255.255.255) must be the last one in the list. Any addresses after the broadcast address are ignored. If the local server is not on the list, Sun Ray DTUs cannot attempt to contact it.

Once a TCP connection to an Authentication Manager has been established, the DTU presents its token. The token is either a pseudo-token representing the individual DTU (its unique Ethernet address) or a smart card. The Session Manager then starts an X window/Xserver session and binds the token to that session.

The Authentication Manager then sends a query to all the other Authentication Managers on the same subnet and asks for information about existing sessions for the token. The other Authentication Managers respond, indicating whether there is a session for the token and the last time the token was connected to the session.

The requesting Authentication Manager selects the server with the latest connection time and redirects the DTU to that server. If no session is found for the token, the requesting Authentication Manager selects the server with the lightest load and redirects the token to that server. A new session is created for the token.

The Authentication Manager enables both implicit (smart card) and explicit switching. For explicit switching, see [“Group Manager” on page 155](#).

Configuring DHCP

In a large IP network, a DHCP server distributes the IP addresses and other configuration information for interfaces on that network.

Coexistence of the Sun Ray Server With Other DHCP Servers

The Sun Ray DHCP server can coexist with DHCP servers on other subnets, provided you isolate the Sun Ray DHCP server from other DHCP traffic. Verify that all routers on the network are configured not to relay DHCP requests. This is the default behavior for most routers.

Caution – If the IP addresses and DHCP configuration data are not set up correctly when the interfaces are configured, the failover feature cannot work properly. In particular, configuring the Sun Ray server’s interconnect IP address as a duplicate of any other server’s interconnect IP address may cause the Sun Ray Authentication Manager to throw “Out of Memory” errors.

Administering Other Clients

If the Sun Ray server has multiple interfaces, one of which is the Sun Ray interconnect, the Sun Ray DHCP server should be able to manage both the Sun Ray interconnect and the other interfaces without cross-interference.

▼ To Set Up IP Addressing on Multiple Servers, Each with One Sun Ray Interface

1. Log in to the Sun Ray server as superuser and, open a shell window. Type:

```
# /opt/SUNWut/sbin/utadm -a <interface_name>
```

where *<interface_name>* is the name of the Sun Ray network interface to be configured; for example, *hme[0-9]*, *qfe[0-9]*, or *ge[0-9]*. You must be logged on as superuser to run this command. The *utadm* script configures the interface (for example, *hme1*) at the subnet (in this example, 128).

The script displays default values, such as the following:

```
Selected values for interface "hme1"
host address:      192.168.128.1
net mask:         255.255.255.0
net address:      192.168.128.0
host name:        serverB-hme1
net name:         SunRay-hme1
first unit address: 192.168.128.16
last unit address: 192.168.128.240
auth server list: 192.168.128.1
firmware server:  192.168.128.1
router:           192.168.128.1
```

The default values are the same for each server in a failover group. Certain values must be changed to be unique to each server.

2. When you are asked to accept the default values, type **n**:

```
Accept as is? ([Y]/N): n
```

3. Change the second server's IP address to a unique value, in this case **192.168.128.2**:

```
new host address: [192.168.128.1] 192.168.128.2
```

4. Accept the default values for netmask, host name, and net name:

```
new netmask: [255.255.255.0]
new host name: [serverB-hme1]
```

5. Change the DTU address ranges for the interconnect to unique values. For example:

```
Do you want to offer IP addresses for this interface? [Y/N]:
new first Sun Ray address: [192.168.128.16] 192.168.128.50
number of Sun Ray addresses to allocate: [205] 34
```

6. Accept the default firmware server and router values:

```
new firmware server: [192.168.128.2]
new router: [192.168.128.2]
```

The utadm script asks if you want to specify an authentication server list:

```
auth server list:      192.168.128.1
To read auth server list from file, enter file name:
Auth server IP address (enter <CR> to end list):
If no server in the auth server list responds, should an auth server
be located by broadcasting on the network? ([Y]/N):
```

These servers are specified by a file containing a space-delimited list of server IP addresses or by manually entering the server IP addresses.

The newly selected values for interface hme1 are displayed:

```
Selected values for interface "hme1"
  host address:      192.168.128.2
  net mask:         255.255.255.0
  net address:      192.168.128.0
  host name:        serverB-hme1
  net name:         SunRay-hme1
  first unit address: 192.168.128.50
  last unit address: 192.168.128.83
  auth server list: 192.168.128.1
  firmware server:  192.168.128.2
  router:           192.168.128.2
```

7. If these are correct, accept the new values:

```
Accept as is? ([Y]/N): y
```

8. Stop and restart the server and power cycle the DTUs to download the firmware.

TABLE 11-2 lists the options available for the `utadm` command. For additional information, see the `utadm` man page.

TABLE 11-2 Available Options

Option	Definition
-c	Create a framework for the Sun Ray interconnect.
-r	Remove all Sun Ray interconnects.
-A <subnetwork>	Configure the subnetwork specified as a Sun Ray sub-network. This option only configures the DHCP service to allocate IP address and/or to provide Sun Ray parameters to Sun Ray clients. It also will automatically turn on support for LAN connections from a shared subnetwork.
-a <interface_name>	Add <interface_name> as Sun Ray interconnect.
-D <subnetwork>	Delete the subnetwork specified from the list of configured Sun Ray subnetworks.
-d <interface_name>	Delete <interface_name> as Sun Ray interconnect.
-l	Print the current configuration for all the Sun Ray subnetworks, including remote subnetworks.
-p	Print the current configuration.
-f	Take a server offline
-n	Bring a server online
-x	Print the current configuration in a machine-readable format

Group Manager

Every server has a group manager module that monitors availability and facilitates redirection. It is coupled with the Authentication Manager.

In setting policies, the Authentication Manager uses the selected authentication modules and decides what tokens are valid and which users have access.

Warning – The same policy must exist on every server in the failover group or undesirable results might occur.

The Group Managers create maps of the failover group topology by exchanging `keepalive` messages among themselves. These `keepalive` messages are sent to a well-known UDP port (typically 7009) on all of the configured network interfaces. The `keepalive` message contains enough information for each Sun Ray server to construct a list of servers and the common subnets that each server can access. In addition, the Group Manager remembers the last time that a `keepalive` message was received from each server on each interface.

The `keepalive` message contains the following information about the server:

- Server's host name
- Server's primary IP address
- Elapsed time since it was booted
- IP information for every interface it can reach
- Machine information (number and speed of CPUs, configured RAM, and so on)
- Load information (CPU and memory utilization, number of sessions, and so on)

Note – The last two items are used to facilitate load distribution. See [“Load Balancing” on page 157](#).

The information maintained by the Group Manager is used primarily for server selection when a token is presented. The server and subnet information is used to determine the servers to which a given DTU can connect. These servers are queried about sessions belonging to the token. Servers whose last `keepalive` message is older than the timeout are deleted from the list, since either the network connection or the server is probably down.

Redirection

In addition to automatic redirection at authentication, you can use the `utselect` or `utswitch` command for manual redirection.

Note – The `utselect` GUI is the preferred method to use for server selection. For more information, see the `utselect` man page.

Group Manager Configuration

The Authentication Manager configuration file, `/etc/opt/SUNWut/auth.props`, contains properties used by the Group Manager at runtime. The properties are:

- gmport
- gmKeepAliveInterval
- enableGroupManager
- enableLoadBalancing
- enableMulticast
- multicastTTL
- gmSignatureFile
- gmDebug
- gmTarget

Note – These properties have default values that are rarely changed. Only very knowledgeable Sun support personnel should direct customers to change these values to help tune or debug their systems. If any properties are changed, they must be changed for all servers in the failover group, since the `auth.props` file must be the same on all servers in a failover group.

▼ To Restart the Authentication Manager

Property changes do not take effect until the Authentication Manager is restarted.

- As superuser, open a shell window and type:

```
# /opt/SUNWut/sbin/utrestart
```

The Authentication Manager is restarted.

Load Balancing

At the time of a server failure, the Group Manager on each remaining server attempts to distribute the failed server's sessions evenly among the remaining servers. The load balancing algorithm takes into account each server's capacity (number and speed of its CPUs) and load so that larger or less heavily loaded servers host more sessions.

When the Group Manager receives a token from a Sun Ray DTU and finds that no server owns an existing session for that token, it redirects the Sun Ray DTU to whichever server in the group has the lightest load. A Sun Ray DTU may appear to connect twice, once on the server that answered its DHCP request and a second time on a server that was less loaded than the first.

▼ To Turn Off the Load Balancing Feature

- In the `auth.props` file set:

```
enableLoadBalancing = false
```

Setting Up a Failover Group

A failover group is one in which two or more Sun Ray servers use a common policy and share services. It is composed of a primary server and one or more secondary servers. For such a group, you must configure a Sun Ray Data Store to enable replication of the Sun Ray administration data across the group. Configure the secondary servers so that they serve users directly in addition to serving the Data Store. For best results in groups of four or more servers, configure the primary server so that it serves only the Sun Ray Data Store.

The `utconfig` command sets up the data store for a single system initially, and enables the Sun Ray servers for failover. The `utreplica` command then configures the Sun Ray servers as a failover group.

Log files for Sun Ray servers contain time-stamped error messages which are difficult to interpret if the time is out of sync. To make troubleshooting easier, all secondary servers should periodically synchronize with their primary server.

Tip – Use `rdate <primary-host>`, preferably with `crontab`, to synchronize secondary servers with their primary server.

Primary Server

Layered administration of the group takes place on the primary server, where the master copy of SRDS resides. The `utreplica` command designates a primary server, advises the server of its Administration Primary status, and tells it the host names of all the secondary servers.

The term primary server reflects the replication relationship, not failover order.

Adding or removing secondary servers requires services to be restarted on the primary server. In large failover groups, and significant loads may be pushed onto the primary server from various sources. In addition, runaway processes from user applications on the primary can degrade the health of the entire failover group. Failover groups of more than four servers should have a dedicated primary server devoted to solely serving the Sun Ray Data Store, i.e., not hosting any Sun Ray sessions.

Tip – Configure the primary server before you configure the secondary servers.

▼ To Specify a Primary Server

- As a superuser, open a shell window on the primary server and type:

```
# /opt/SUNWut/sbin/utreplica -p secondary-server1 [secondary-server2 ...]
```

where *secondary_server1 [secondary_server2...]* is a space-separated list of unique host names of the secondary servers.

▼ To Specify a Dedicated Primary Server

The purpose of a dedicated primary server is to serve the Sun Ray Data Store; however, specifying a dedicated primary server allows secondary servers to be added or removed without disturbing user sessions.

- Follow the procedure to specify a primary server, as above; however, do not run `utadm` on this server.

Secondary Server

The secondary servers in the group store a replicated version of the primary server's administration data. Use the `utreplica` command to advise each secondary server of its secondary status and also the host name of the primary server for the group.

▼ To Specify Each Secondary Server

- As superuser, open a shell window on the secondary server and type:

```
# /opt/SUNWut/sbin/utreplica -s primary-server
```

where *primary-server* is the hostname of the primary server.

▼ To Add Additional Secondary Servers

To include an additional secondary server in an already configured failover group:

1. **On the primary server, rerun `utreplica -p -a` with a list of additional secondary servers.**

```
# /opt/SUNWut/sbin/utreplica -p -a secondary-server1, secondary-server2,...
```

2. **Run `utreplica -s primary-server` on the new secondary server.**

```
# /opt/SUNWut/sbin/utreplica -s primary-server
```

Removing Replication Configuration

▼ To Remove the Replication Configuration

- As superuser, open a shell window and type:

```
# /opt/SUNWut/sbin/utreplica -u
```

This removes the replication configuration.

Viewing Administration Status

▼ To Show Current SRDS Replication Configuration

- As superuser, open a shell window and type:

```
# /opt/SUNWut/sbin/utreplica -l
```

The result indicates whether the server is standalone, primary (with the secondary host names), or secondary (with the primary host name).

▼ To View Network (Failover Group) Status

A failover group is a set of Sun Ray servers all running the same release of Sun Ray Server Software and all having access to all the Sun Ray DTUs on the interconnect.

1. **From the Servers tab in the Admin GUI, click on a server name to display its Server Details screen.**
2. **Click View Network Status.**

FIGURE 11-3 Network Status Screen

VERSION [LOG OUT] [HELP]

User: admin Server: srsdemo-01

Sun Ray Administration

Sun Microsystems, Inc.

Servers Sessions Desktop Units Tokens Advanced Log Files

All Servers > srsdemo-01 > Network Status

srsdemo-01 - Network Status

This page lists the network status of all trusted servers from the perspective of the selected server.

Network Status (2)

Server Name	10.6.133.0/24			192.168.128.0/24		
	Address	Status	Type	Address	Status	Type
srsdemo-01	10.6.133.148	✓ Up	LAN	192.168.128.1	✓ Up	Interconnect
▼ Trusted Servers						
srsdemo-02	10.6.133.171	✓ Up	LAN	192.168.128.2	✓ Up	Interconnect

Done srsdemo-01:1661

The Network Status screen provides information on group membership and network connectivity for *trusted servers*—those in the same failover group.

Note – Sun Ray server broadcasts do not traverse routers or servers other than Sun Ray servers.

Recovery Issues and Procedures

If one of the servers of a failover group fails, the remaining group members operate from the administration data that existed prior to the failure. The recovery procedure depends on the severity of the failure and whether a primary or secondary server has failed.

Note – When the primary server fails, you cannot make administrative changes to the system. For replication to work, all changes succeed on the primary server.

Primary Server Recovery

There are several strategies for recovering the primary server. The following procedure is performed on the same server that was the primary after it is fully operational again.

▼ To Rebuild the Primary Server's Administration Data Store

Use this procedure to rebuild the primary server's data store from a secondary server. This procedure uses the same hostname for the replacement server.



Caution – Be sure to set `umask` appropriately before running `utldbmc`, otherwise, unprivileged users can gain access to the `utadmin` password.

1. On one of the secondary servers, capture the current data store to a file called `/tmp/store`:

```
# /opt/SUNWut/srds/lib/utldbmc \
/var/opt/SUNWut/srds/dbm.ut/id2entry.dbb > /tmp/store
```

This provides an LDIF format file of the current data store.

2. FTP this file to the `/tmp` directory on the primary server.
3. Follow the directions in the *Sun Ray Server Software 4.1 Installation and Configuration Guide* to install Sun Ray Server Software.
4. After running `utinstall`, configure the server as a primary server for the group. Make sure that you use the same admin password and group signature.

```
# utconfig
:
# utreplica -p <secondary-server1> <secondary-server2> ...
```

5. Shut down the Sun Ray services, including the data store:

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

6. Restore the data:

```
# /opt/SUNWut/srds/lib/utldif2l1dbm -c -j 10 -i /tmp/store
```

This populates the primary server and synchronizes its data with the secondary server. The replacement server is now ready for operation as the primary server.

7. Restart Sun Ray services:

```
# utrestart -c
```

8. (Optional) Confirm that the data store is repopulated:

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

9. (Optional) Perform any additional configuration procedures.

▼ To Replace the Primary Server with a Secondary Server

Note – This procedure is also known as promoting a secondary server to primary.

1. Choose a server in the existing failover group to be promoted and configure it as the primary server:

```
# utreplica -u
# utreplica -p <secondary-server1> <secondary-server2> ...
```

2. Reconfigure each of the remaining secondary servers in the failover group to use the new primary server:

```
# utreplica -u
# utreplica -s <new-primary-server>
```

This resynchronizes the secondary server with the new primary server.

Note – This process may take some time to complete, depending on the size of the data store. Since Sun Ray services will be offline during this procedure, you may want to schedule your secondary servers’ downtime accordingly. Be sure to perform this procedure on each secondary server in the failover group.

Secondary Server Recovery

Where a secondary server has failed, administration of the group can continue. A log of updates is maintained and applied automatically to the secondary server when it has recovered. If the secondary server needs to be reinstalled, repeat the steps described in the *Sun Ray Server Software 4.1 Installation and Configuration Guide*.

Setting Up a Group Signature

The `utconfig` command asks for a group signature if you chose to configure for failover. The signature, which is stored in the `/etc/opt/SUNWut/gmSignature` file, must be the same on all servers in the group.

The location can be changed in the `gmSignatureFile` property of the `auth.props` file.

To form a fully functional failover group, the signature file must:

- be owned by root with only root permissions
- contain at least eight characters, in which at least two are letters and at least one is not

Tip – For slightly better security, use long passwords.

▼ To Change the Group Manager Signature File

1. As superuser of the Sun Ray server, open a shell window and type:

```
# /opt/SUNWut/sbin/utgroupsig
```

You are prompted for the signature.

2. Enter it twice identically for acceptance.

3. For each Sun Ray server in the group, repeat the steps, starting at step 1.

Note – It is important to use the `utgroupsig` command, rather than any other method, to enter the signature. `utgroupsig` also ensures proper internal replication.

Taking Servers Offline

Being able to take servers offline makes maintenance easier. In an offline state, no new sessions are created. However, old sessions continue to exist and can be reactivated unless Sun Ray Server Software is affected.

▼ To Take a Server Offline

- At the command-line interface, type:

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

▼ To Bring a Server Online

- At the command-line interface, type:

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

User Settings

This appendix covers topics that users as well as administrators may find useful. There are sections for:

- [“Supported Devices and Libraries” on page 167](#)
 - [“Sun Ray DTU Settings” on page 168](#)
 - [“Monitor Settings” on page 169](#)
 - [“Hot Key Preferences” on page 170](#)
 - [“Hot Key Values” on page 172](#)
 - [“Power Cycling a Sun Ray DTU” on page 173](#)
-

Supported Devices and Libraries

Sun Ray Server Software supports a wide variety of end-user devices, including mass storage and end-user peripherals that can be connected to a Sun Ray DTU’s serial, parallel, or USB ports; however, because of the growing number of USB devices available, it has not been possible to test all of them on Sun Ray DTUs.

Supported Mass Storage Devices

Sun Ray Server Software 4.1 supports the use of flash disks, memory card readers, Zip drives, and hard drives on Sun Ray DTUs. It allows data CDs and DVDs to be read but not written. It does *not* support floppy drives. Most devices claiming USB 2.0 compliance are backwards compatible and should work with Sun Ray Mass Storage.

For troubleshooting tips, see [“Troubleshooting USB Mass Storage Devices” on page 197](#).

Sun Ray DTU Settings

Sun Ray Settings is an interactive GUI that allows the user to view and change the settings for the Sun Ray DTU that the user is currently logged into.

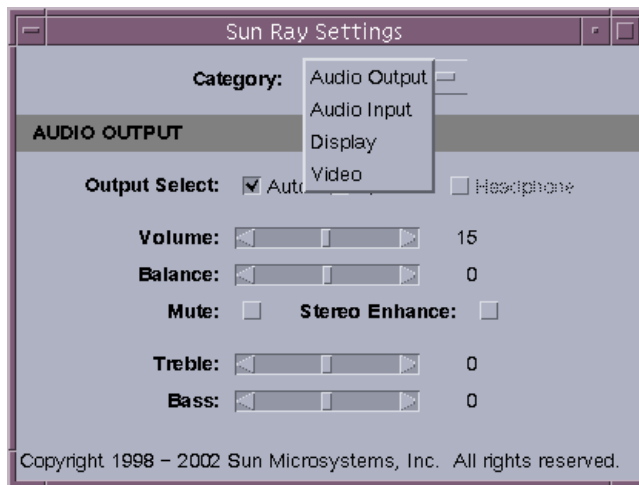
The Sun Ray Settings GUI contacts the Session Manager to determine which DTU is currently being used and connects to that unit to get the current values. The GUI maintains a connection to the Session Manager so that the Session Manager can notify the GUI if the user moves to another DTU by removing the smart card and inserting it into another DTU.

▼ To Change the Sun Ray Settings

1. Press the hot key (by default Shift-Props).

On a non-Sun keyboard, you can use the `utsettings` CLI as an alternative. In either case, the Sun Ray Settings window is displayed.

FIGURE A-1 Settings Screen



2. Use the Category pull-down menu to access Audio Output, Audio Input, Display, and Video settings.

3. **To change a setting, move the appropriate scroll bar, checkbox, or pull-down menu.**

The DTU is updated immediately. The only exception is the “Resolution/Refresh Rate” setting, which prompts the user with confirmation dialog boxes before and after the change is made on the DTU.

4. **Press the hot key to close the window.**

Note – Only one instance per session of Sun Ray Settings runs in hot key mode.

Monitor Settings

Sun Ray users can modify their screen resolution settings by invoking `utsettings`.

Any resolution selection made within a session remains effective whenever the session is displayed on that particular DTU. The selection is not lost if the unit goes into power-save mode or is power-cycled; however, the resolution settings selected through `utsettings` apply *only* to the DTU where `utsettings` is run.

When a user moves to another DTU, the resolution settings do not accompany the user to the new DTU, but the settings remain effective for the user’s session on the original DTU if the user returns to the session via hotdesking.

If the session is associated with a personal mobile token, then `utsettings` offers to make the selected timing permanent. If a user accepts that offer, then the timing is retained and reused on that user’s subsequent personal mobile token sessions on the same DTU.

In addition, the administrator can use the `utresadm` command to:

- Arrange for a particular monitor timing to be used whenever a specific token is presented on a specific DTU.
- Arrange for a particular monitor timing to be used on a specific DTU, regardless of the token that is presented at the DTU.
- Arrange for a particular monitor timing to be used on all DTU’s regardless of the token that is presented at the DTU.

Any conflict among settings is resolved in favor of the most specific configuration rule. That is, a configuration record for a specific token at a specific DTU takes precedence over a record for *any token* at that specific DTU, and a configuration record for *any token* at a specific DTU takes precedence over a record for *any token* at *any DTU*.

For further details, see the `utsettings` and `utresadm` man pages.

Non-Sun Keyboard Settings

For customers using non-Sun USB keyboards, controls such as volume and reset can be accessed using alternate key sequences. Use the key combination `Ctrl-Pause-<x>`, where `<x>` is one of the keys listed in [TABLE A-2](#).

TABLE A-1 Alternate Key Sequences for Non-Sun Keyboards

Code	Meaning
A	Soft reset (equivalent of Ctrl-Moon on a Sun keyboard)
N	Show status (3 audio keys)
Right arrow	Volume up (right arrow)
Left arrow	Volume down (left arrow)
Down arrow	Mute/Unmute
V	Show model, <i>MAC address</i> , and firmware version

Hot Key Preferences

Hot keys can be configured for various Sun Ray utilities. The scope for these hot keys can be:

- System-wide default setting
- User default setting
- System-wide mandatory setting

To support these levels of customization, the utilities look for the properties files in [TABLE A-2](#), in the following order, at startup:

TABLE A-2 Sun Ray Settings Properties Files

File	Scope	Description
/etc/opt/SUNWut/utslaunch_defaults.properties	System	This file contains helpful default properties. Any properties specified here override any defaults built into the application itself.
\$HOME/.utslaunch.properties	User	This file contains the user's preferred values, which override any application or site-wide defaults.
/etc/opt/SUNWut/utslaunch_mandatory.properties	Mandatory	This file contains site-wide mandatory settings that cannot be overridden by the user. These properties override any application, site-wide, or user defaults.

If your policy is for all DTUs to use a standard hot key, use the system-wide mandatory defaults file to specify this standard key. This prevents users from specifying their own hot key preferences.

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

```
<utility_name>.hotkey=value
```

where *<utility_name>* is the name of the utility, such as *utsettings* or *utdetach*, and *value* is a valid X keysym name preceded by one or more of the supported modifiers (*Ctrl*, *Shift*, *Alt*, *Meta*) in any order. Values are shown in [TABLE A-3](#).

TABLE A-3 Specific Hot Key Values

Example Value	Notes
Shift+Props	Invoke the Settings GUI.
Stop+S	Invoke the Pop-up GUI
Ctrl+Alt+Backspace	Press this key sequence twice to kill a session.
Ctrl+Alt+Del	Press this key sequence twice to kill the process that has taken control of the Xserver.
Mute+Softer+Louder	Display the DTU's <i>MAC address</i> .
Ctrl+Moon	Power cycle the DTU.

Hot Key Values

▼ To Change the Hot Key for the Settings GUI

If you do not want to use `Shift Props` as your default hot key, use the system-wide defaults file to specify a function key. Users can still specify their preferences in the user defaults file.

Use this procedure to modify the settings GUI for all users on a server.

1. As superuser, open the

`/etc/opt/SUNWut/utslaunch_defaults.properties` **file in a text editor.**

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

2. Locate the original hot key entry for the `utdetach` utility and place a # in front of that statement.

The # comments out the first hot key property.

```
# utdetach.hotkey=Shift Pause
```

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

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

4. Save the `utslaunch_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 Settings screen. Users who were logged in before you changed the hot key continue to use the old value.

▼ To Change the Hot Key Setting for a Single User

1. In the user's home directory, create the `.utslaunch.properties` file.

Note – Make sure that the user owns and can read this file.

2. Add a line to the `.utslaunch.properties` file with the value for the hot key.
For example:

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

3. Save the `.utslaunch.properties` file.
4. Log out and log back in to enable the new hot key.

Note – You can modify other hot keys in a similar fashion.

Power Cycling a Sun Ray DTU

▼ To Power Cycle a Sun Ray DTU

- Disconnect then reconnect the power cord.

▼ To Perform a Soft Reset

- Use the key sequence `Ctrl-Power`. The Power key at the right side of the top row of a Sun Type 6 or Type 7 keyboard has a crescent moon icon; the soft reset key sequence is often called `Ctrl-Moon`.

▼ To Kill a User's Session

- Use the key sequence `Ctrl-Alt-Backspace` twice.

This kills the Xserver process, alerting the current session's parent process to start another session.

Troubleshooting and Tuning Tips

This appendix contains the following sections:

- “Understanding OSD” on page 175
- “Authentication Manager Errors” on page 195
- “Troubleshooting USB Mass Storage Devices” on page 197
- “Audio” on page 198
- “Performance Tuning” on page 200

Note – For the latest information regarding Sun Ray Server Software patches, check: <http://www.sun.com/software/sunray/patches.xml>

Understanding OSD

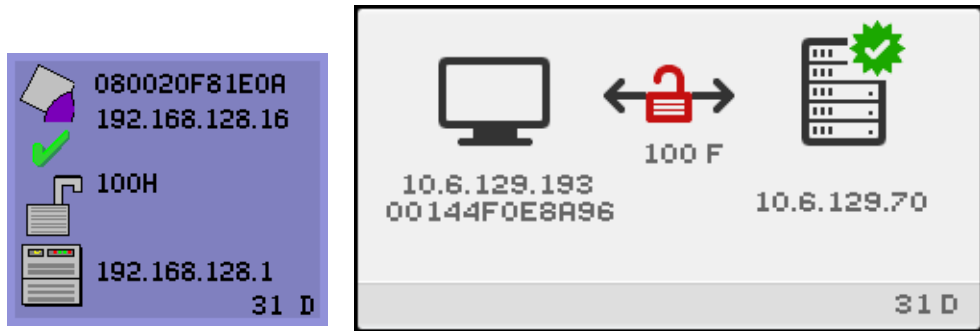
Sun Ray Server Software on-screen displays (OSD) to help administrators and others identify problems visually. The most important information about the Sun Ray DTU and its current state is displayed on the screen.

OSD Icon Topography

The original OSD supplied with earlier versions of Sun Ray Server Software and DTU firmware have now been replaced with larger icons that provide the same information in an easier to read format. It is always a good idea to make sure that you are using the latest firmware. See “[Managing Firmware Versions](#)” on page 30.

Both sets of OSD icons are composited live, based on the current state of connectivity at a given moment. Examples of the original OSD are shown at left in the figures below, with equivalent or similar examples of the newer OSD at the right.

FIGURE B-1 Layout of Old (left) and New (right) OSD Icons



The OSD icons display:

- Ethernet address
- Currently assigned IP address of the DTU
- Link status of the currently connected Sun Ray server
- Authentication Server IP address
- Icon code and DHCP state

To help you locate problems, the OSD icons display a numeric icon code followed by an alphabetic DHCP state code. You can look up the meaning of the numeric OSD message codes in [TABLE B-1](#) and the alphabetic DHCP state codes in [TABLE B-2](#), and firmware download error codes in [TABLE B-4](#). Encryption and authentication information is also displayed when appropriate.

Sun Ray DTUs can function in a private interconnect or in a simple LAN environment with only an IP address, but additional basic parameters and Sun Ray-specific vendor options are needed for more complex LAN operations, such as when a DTU is located several hops away from the Sun Ray Server's subnet.

OSD icon messages and codes are summarized in the following tables:

TABLE B-1 Icon Messages

Icon Code	Meaning
1	Sun Ray DTU is starting up and is waiting for ethernet link
2	Sun Ray DTU is downloading new firmware
3	Sun Ray DTU is storing new firmware in its flash memory

TABLE B-1 Icon Messages

Icon Code	Meaning
4	Either the download or storage of new firmware has failed
5	There is no session to connect with the Sun Ray
6	The server is denying access to the Sun Ray
7	Local pin entry to the smart card has failed
8	In local smart card pin entry mode
9	There is an over current condition on the USB bus, i.e., the total number of devices draws too much current. Consider using a powered hub.
11	Server is authenticated by the Sun Ray DTU and the graphic/keyboard network connection is encrypted
12	The Sun Ray DTU cannot authenticate the server but the graphic/keyboard network connection is still being encrypted
13	Server authenticated to the Sun Ray; network connection between Sun Ray and server not encrypted
14	Server not authenticated to the Sun Ray; graphic/keyboard network connection is not encrypted
15	the Sun Ray DTU is refusing to talk to the server due to the server's refusal or inability to authenticate or encrypt the network connection
16	The Sun Ray USB bus is temporarily busy servicing a high-speed device, and the keyboard or mouse may not be responsive to user input.
21	The Sun Ray DTU is booting up and is waiting on DHCP IP address and parameter assignment.
22	The Sun Ray DTU is booting up and is now waiting for the initial connection to a Sun Ray server.
23	The connection between the Sun Ray DTU and the network is down. Check the network drop cable and (if the network drop cable is okay) the network switch.
24	The Sun Ray DTU has disconnected from the previous server.
25	The Sun Ray DTU is being redirected to a new server.
26	The Sun Ray DTU has connected to the server and is waiting for graphics traffic.
27	The Sun Ray DTU is broadcasting to locate a Sun Ray server since either it was not provided with Sun Ray specific DHCP parameters or all of the specified servers are not responding.
28	VPN connection being attempted
29	VPN connection established
30	VPN connection error
	Icons 31 through 34 display network status when the three audio keys are pressed simultaneously.
31	The network link is up, the server is authenticated, and graphics/keyboard network connections are not encrypted.
32	The network link is up, the server is not authenticated, and graphics/keyboard network connections are encrypted.

TABLE B-1 Icon Messages

Icon Code	Meaning
33	The network link is up, the server is authenticated and graphics/keyboard are encrypted.
34	The network link is up, the server is not authenticated and graphics/keyboard are not encrypted.
35	The DTU has been disconnected from its server, either by a STOP-Q session disconnect event or by the VPN session timeout value having been set and exceeded.
50	The server is refusing to talk to the Sun Ray DTU due to the Sun Ray's refusal or inability to authenticate or encrypt the network connection

TABLE B-2 DHCP State Codes

DCHP State Code	Meaning
A	DCHP only provided IP address with no additional parameters.
B	DCHP provided IP address, subnet mask, and router, but Sun Ray vendor-specific parameters are missing.
C	DHCP provided IP address and Sun Ray vendor-specific parameters, but subnet mask and router are missing.
D	DHCP provided all expected parameters.
	Codes E, F, H, and I are valid only with OSD icon 28
E	VPN Phase 1 IKE initiated.
F	VPN Phase 1 IKE complete.
H	VPN Phase 2 initiated.
I	VPN Phase 2 complete.

TABLE B-3 Power LED

DTU Hardware State	Action to Take
Off	Check to see if the DTU is plugged in. Replace the DTU.
Amber	Hardware fault. Replace the DTU.
Blinking	PROM is corrupted. Check that firmware downloads are properly configured and enabled, then power cycle the DTU.
Card reader LED remains on even when smart card is removed	Card reader hardware problem. Replace the DTU.

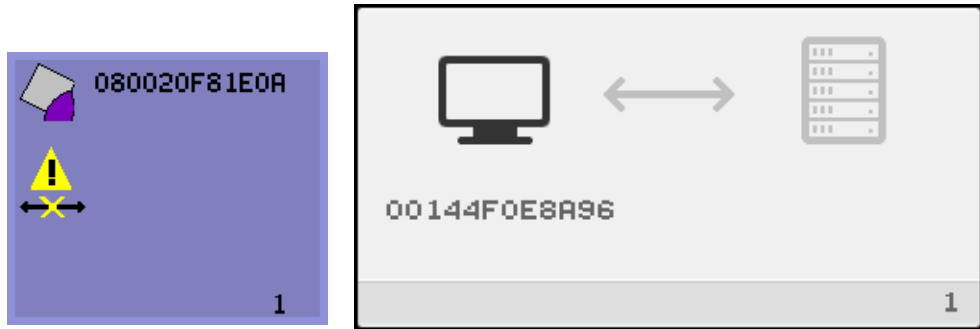
TABLE B-4 Firmware Download Error Codes and Messages

Error Code	Error Message
E	FW Load: No server
F	FW Load: Name too long
G	FW Load: Bad read
H	FW Load: Bad signature
I	FW Load: Failed decompression
J	FW Load: Invalid module type
K	FW Load: Version mismatch
L	FW Load: Not enough memory
M	FW Load: Prevented by barrier
N	FW Load: Invalid HW version
O	FW Load: Flash write error

Sun Ray Desktop Unit Startup

The first display a user should see is depicted below:

FIGURE B-2 DTU Startup OSD



This icon indicates that the DTU 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 is usually displayed for only a few seconds.

▼ If this icon stays on for more than 10 seconds

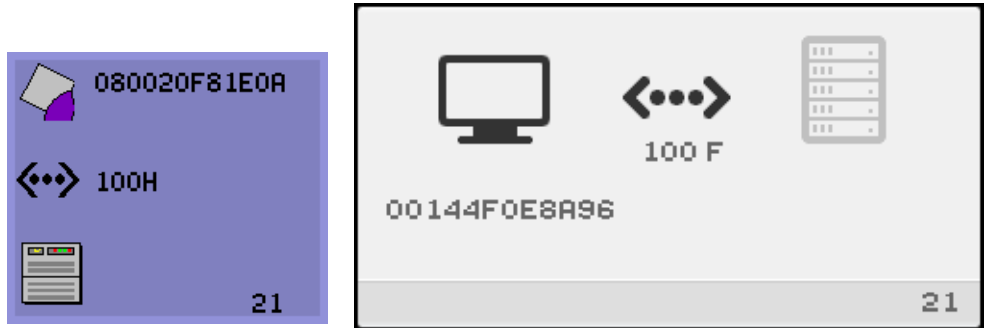
1. Check that the Ethernet cable is correctly plugged into the DTU and the other end is plugged in to the correct hub, switch, or network outlet.

A link light on the switch or hub indicates that the connection is alive.

2. If the DTU is connected through a hub or a switch, make sure that the hub or switch is powered on and configured correctly.

After the Sun Ray DTU has verified its network connection, the user should see this OSD:

FIGURE B-3 Network Connection Verified



This icon indicates that the DTU has detected the Ethernet carrier but has not yet received its initial parameters or IP address from DHCP. This icon is displayed as part of the normal startup phase and is usually displayed for only a few seconds.

▼ If this icon stays on for more than 10 seconds

1. **Make sure that the DHCP server is configured correctly, is up and running, and has not run out of IP addresses to assign to clients.**
2. **Verify that your DHCP server is configured properly for network parameters.**

After the DHCP server has allocated an IP address, the icon is updated with the unit's IP address; if the response is inadequate, the Sun Ray DTU issues a DHCP `inform` request to attempt to obtain the Sun Ray vendor-specific parameters. The Sun Ray DTU continues all the way through booting with just a DHCP-supplied IP address but usually functions better with some additional parameters.

At this point, depending on whether you have configured your Sun Ray servers to run on a LAN or a dedicated interconnect, OSD 21A or 21B may display.

Code 21 A indicates that the DTU got an IP address and is waiting for a DHCP `inform` response to other parameters.

Code 21 B indicates that the DTU got an IP address and IP router and is waiting for Sun Ray vendor-specific options from DHCP `inform`.

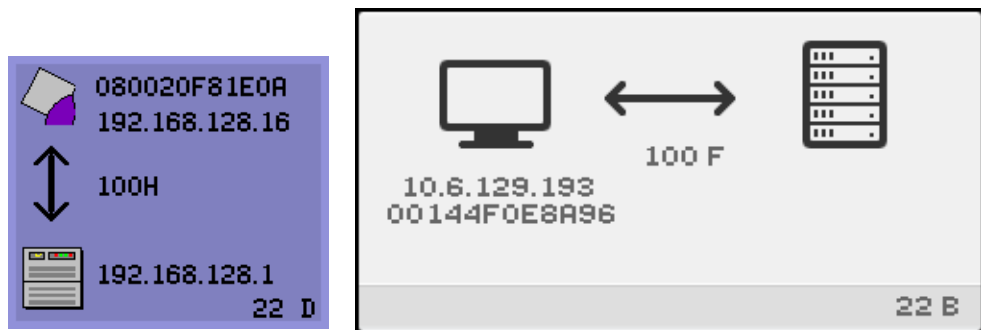
Note – If you see a 21 A or 21 B with a DTU IP address in a LAN deployment, the Sun Ray DTU is trying to use DHCP `INFORM` to get Sun Ray-specific parameters.

▼ Actions to Take

1. For LAN configurations with other (non-Sun Ray) DHCP services but no `bootp` proxy agent, verify the DHCP server and the Sun Ray vendor tags.
2. For routed configurations, verify that the `bootp` proxy agent is configured correctly in the Sun Ray DTU's subnet and that it points to one of the Sun Ray servers in the failover group.
3. For non-routed private interconnect configurations, the Sun Ray server also performs the functions of a DHCP server. Verify that it is configured properly for DHCP services.

When DHCP finishes, the Sun Ray DTU tries to connect to a Sun Ray server and the Authentication Manager running on it.

FIGURE B-4 Waiting to Connect to Authentication Manager



This icon indicates that the DTU has received its initial parameters from DHCP but has not yet connected to the Sun Ray Authentication Manager. This icon is displayed as part of the normal startup phase and is usually displayed for only a few seconds.

▼ If the icon displays for more than a few seconds or if the DTU continues to reset after the icon is displayed

1. Make sure that Sun Ray services, including the Authentication Manager, are up and running on the Sun Ray server.

In a LAN configuration or other routed environment:

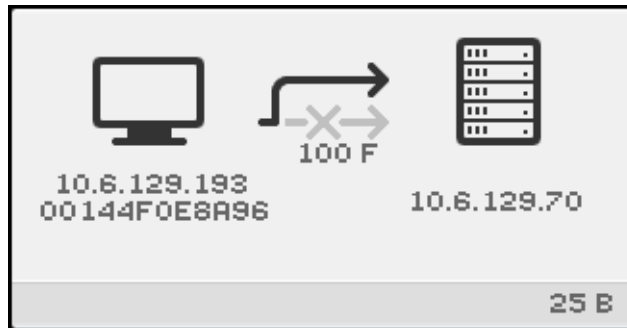
2. Make sure that the Authentication Manager can be reached from the IP address assigned to the DTU.
3. Verify that the routing information the DTU receives is correct.

4. Run `utquery` for the DTU's IP address.

The `utquery` command displays the parameters a Sun Ray DTU has received. If `utquery` fails to display an `AuthSrvr` parameter, the DHCP server for Sun Ray parameters may not be reachable or may not be configured properly. Confirm that the `DHCPServer` and `INFORMServer` values are appropriate. If not, look at your `bootp` relay configurations and DHCP server configurations for network and Sun Ray parameters. For details of these parameters, see the `utquery` man page.

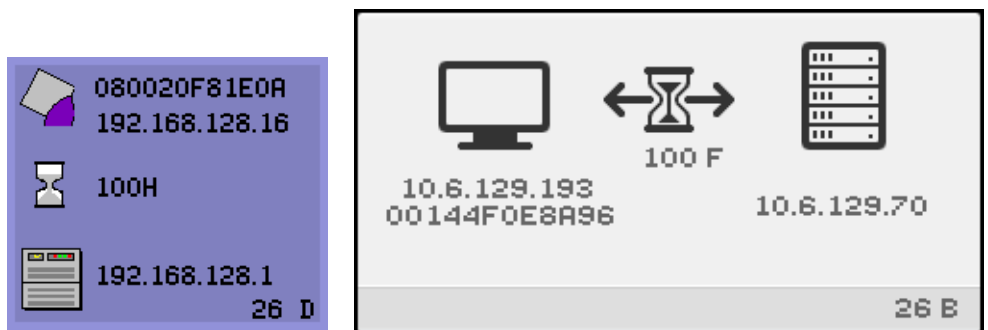


FIGURE B-5 Redirection OSD



This OSD indicates that the DTU is being redirected to a new server. This can occur for any of several reasons, including load balancing.

FIGURE B-6 Wait for Session OSD



This OSD represents the transition state for the Sun Ray DTU. If it is displayed for an extended period, there is probably no X Window server running.

The current wait icon is a white “X” cursor. In earlier releases, the wait icon was displayed as a green newt cursor.

▼ To Identify a Hung Session

- As superuser, type:

```
# /opt/SUNWut/sbin/utdesktop -l -w
```

▼ To Kill a Hung Session

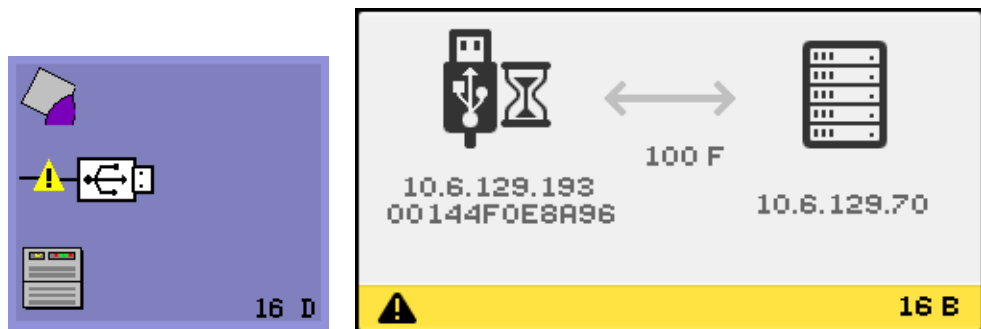
- As superuser, type:

```
# /opt/SUNWut/sbin/utsession -k -t token
```

▼ Actions to Take

1. Check the messages file `/var/opt/SUNWut/log/messages` to verify the version number.
2. Correct, if necessary, with `utadm -l`.

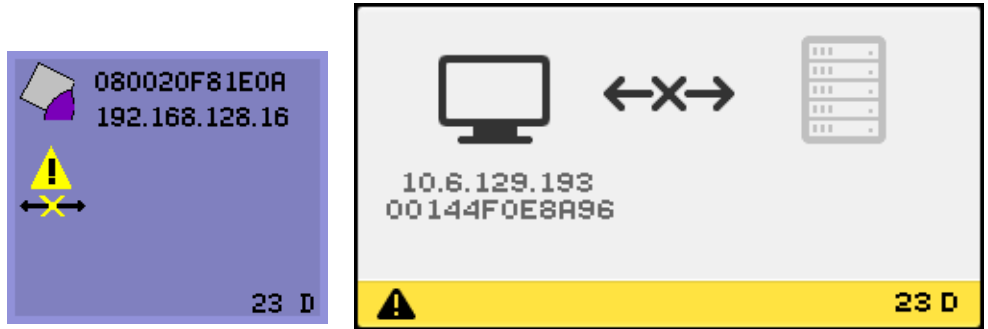
FIGURE B-7 Bus Busy



This icon indicates that the Sun Ray USB bus is temporarily busy servicing a high-speed device, and the keyboard or mouse may not be responsive to user input.

This icon typically appears only during an unusually long print job and disappears when the job is done. This is an informational OSD; there is no particular action to take unless it is necessary to kill the print job.

FIGURE B-8 No Ethernet Signal

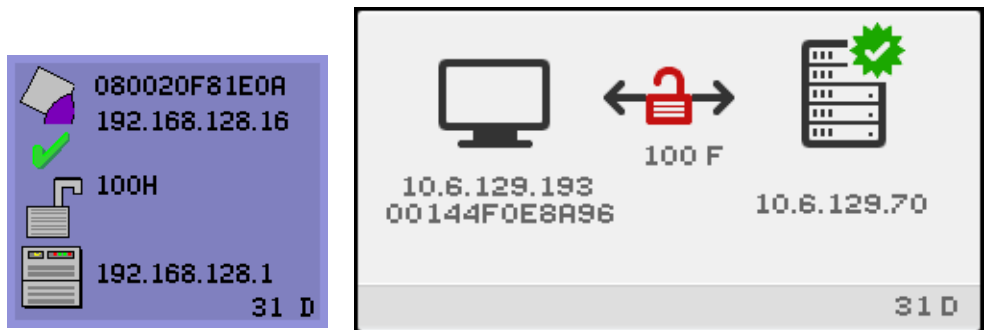


This icon indicates that the DTU has an Ethernet address and an IP address but has lost the Ethernet signal. This icon is displayed only after the DTU successfully boots and receives an IP address, but then loses its Ethernet signal.

▼ Actions to Take

1. Check that the Ethernet cable is correctly plugged in to the back of the DTU and the other end is plugged into the correct switch or network outlet.
2. If the DTU is connected through a hub or switch, make sure that the hub or switch is on and configured correctly.

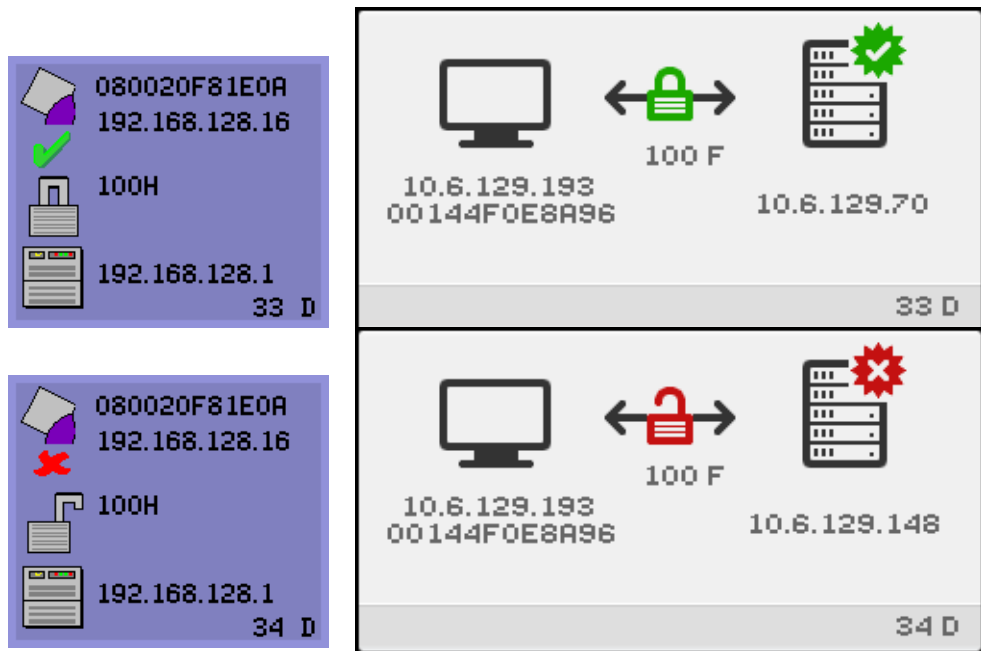
FIGURE B-9 Ethernet Address



This OSD shows the Ethernet address, currently assigned IP address, currently connected server, encryption status, DHCP state, and link speed and mode. 10 stands for 10 Mbps, and 100 for 100 Mbps. F stands for full duplex, H stands for half-duplex mode. To display this OSD with current information, press the three audio volume keys simultaneously.

Tip – To get the same effect on non-Sun keyboard, disconnect and reconnect the Ethernet cable.

FIGURE B-10 Ethernet Address OSD with Different Encryption and Authentication States



Session Connection Failures

The following icons are displayed in the event of a possible security breach.

FIGURE B-11 Session Refused by DTU



Icon 15D indicates that the DTU is refusing to connect to a server because it is unable to verify the validity of the Sun Ray server. This error can occur only if an unknown Sun Ray server intercepts the messages and tries to emulate a valid Sun Ray server. This is a session security breach.

A graphically similar icon displaying the number 50 indicates that the server is refusing to grant a session to the DTU because the DTU is unable to fulfill the server's security requirements.

▼ Actions to Take

1. Check the DTU's firmware version.

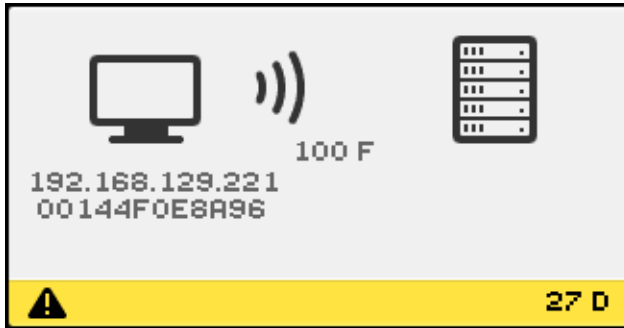
This error may occur with firmware versions earlier than 2.0 if the server is configured for hard security mode.

2. Upgrade the firmware.

As an alternative, confirm whether your site requires hard security mode. If not, the session can be enabled with soft security mode.

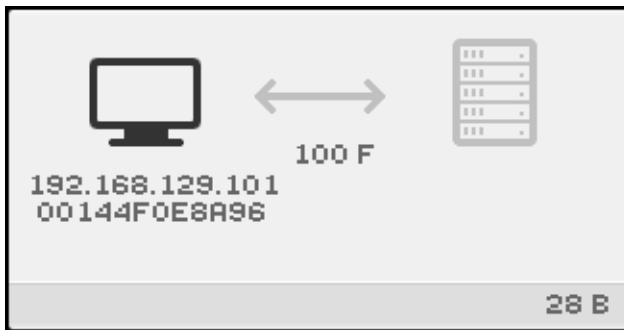
The following icon is displayed if the DTU is broadcasting to locate a server and either no servers respond or Sun Ray specific DHCP parameters have not been supplied correctly.

FIGURE B-12 DHCP Broadcast Failure



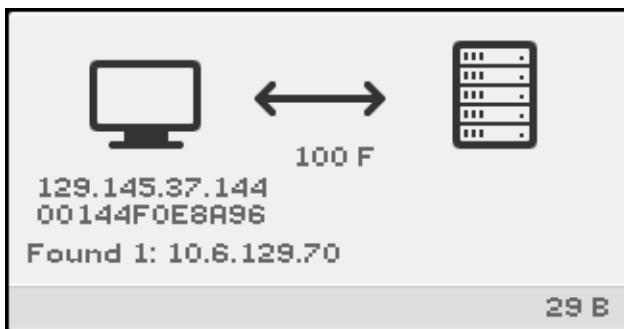
The following icon is displayed while a DTU is trying to establish a VPN connection.

FIGURE B-13 Establishing a VPN Connection



When the VPN connection is established, the following icon is displayed.

FIGURE B-14 VPN Connection Established



Firmware Download Diagnostics

When firmware download error occurs, OSD icon 4 (see [FIGURE B-15](#)) displays the appropriate error code and a descriptive text string. These error codes are listed in [TABLE B-4](#).

Note – These error messages appear in English even in localized versions of Sun Ray Server Software.

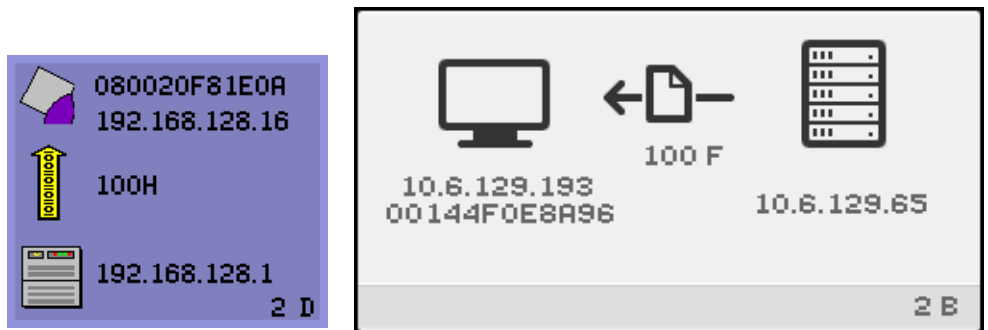
FIGURE B-15 OSD Icon 4 Displays Firmware Download Error Messages



Firmware Download OSD

The following OSD are typical of those that may display when new firmware is downloaded to a DTU from a Sun Ray server.

FIGURE B-16 Firmware Download in Progress



This icon indicates that the DTU is currently downloading new flash PROM software from the Sun Ray server.

▼ Actions to Take

1. Wait until the download is complete.

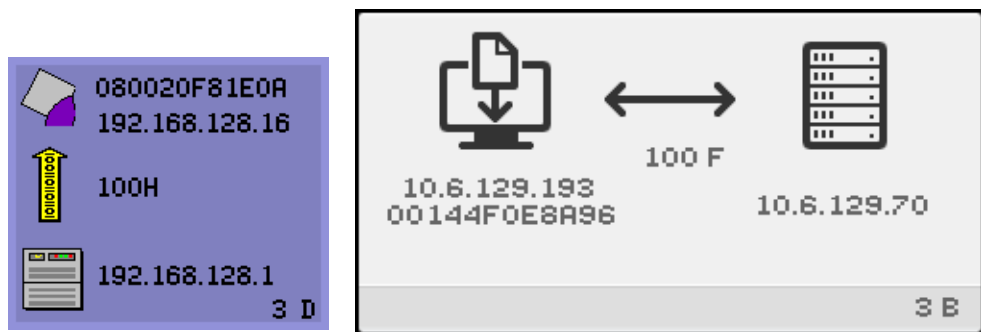
Downloading and saving the new PROM software usually takes less than a minute. If you interrupt the download, the DTU has to download new PROM software the next time it reboots.

If the firmware download fails, the following syslog message indicates that the barrier level has been set to prevent Sun Ray DTUs with SRSS 4.1 firmware from automatically downloading an earlier version of the firmware:

```
Firmware upgrade/downgrade not allowed! Barrier is 310 Firmware level is 0
```

2. Check `/var/opt/SUNWut/log/messages` to confirm that your configuration is set up properly.

FIGURE B-17 Saving PROM Software



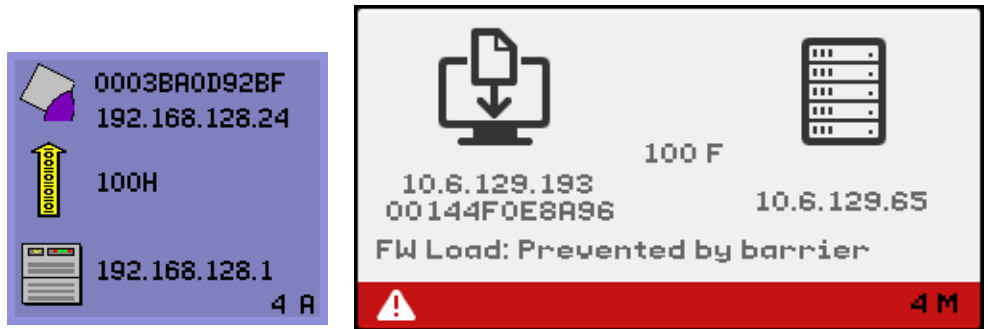
This icon indicates that the DTU has just downloaded new PROM software from the Sun Ray server and is saving it to the DTU's PROM.

▼ Actions to Take

● 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 DTU has to download new PROM software the next time it reboots.

FIGURE B-18 Firmware Download Failed



This icon indicates that the DTU has failed to download new firmware. OSD 4 now includes error code text, as shown above.

Token Reader Icons

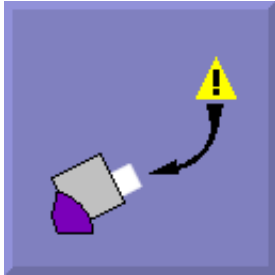
When a site policy disallows pseudo-sessions, DTUs configured as token readers display the Card Reader icon instead of the Login Dialog box card.

Note – The token reader was called the card reader in earlier releases. The smart card token itself is an integrated circuit embedded in or printed on the card, and it is data on the token that is read when a user inserts a card. In practice, the terms *card reader* and *token reader* are used interchangeably.

FIGURE B-19 Card Reader OSD



FIGURE B-20 Card Read Error OSD



This icon indicates that the Card Read Error OSD icon appears whenever the firmware is unable to read the card due to one of the following causes:

- The DTU is running old firmware.
- The card contacts are dirty, the contacts on the card reader are dirty, or the card is not properly inserted.
- The card is malfunctioning.
- The card is of a type that the firmware is not configured to read.
- There is an error in the configuration for reading this type of card.

▼ Actions to Take

1. Upgrade the firmware.
2. Replace the card.

FIGURE B-21 Prompt for Card Insertion OSD



If the current authentication policy allows access only by card, this OSD icon appears and prompts the user to insert a card.

FIGURE B-22 Access Denied OSD



This icon indicates that the Access Denied OSD icon 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 a DTU.

The Sun Ray administration model has seven 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
- Session Refused—The server refuses to grant a session to a DTU that does not meet the server’s security requirements

The first three session types have normal login processes. When there is a problem, the administrator should examine:

- Sun Ray Server configuration files

Caution – Sun Ray Server Software modifies certain system configuration files. In most cases, these changes are identified with SRSS-specific comments. Please do not change these modifications.

- Any locally modified Xserver startup files

Although the last four session types display icons on the Sun Ray DTU, they do not have login processes at all. The icons indicate that the user must take steps before a successful login is possible. If the user immediately removes and reinserts the smart card, the icon disappears, but the Wait for Session OSD remains.

These last four session types and their OSDs should not cause alarm. The user can:

- Insert a recognized smart card in the correct orientation
- Ask the Sun Ray administrator to grant access

- Ask the Sun Ray administrator to download the correct firmware

Authentication Manager Errors

Authentication Manager errors can be found in the following error logs:

- Installation log:
 - `/var/opt/SUNWut/log`
- General log files:
 - `/var/opt/SUNWut/srds/log`
 - `/var/opt/SUNWut/srds/replug`

The general format of the log messages is:

```
timestamp    thread_name    message_class    message
```

For example:

```
May  7 15:01:57 e47c utauthd: [ID 293833 user.info] Worker3
NOTICE: SESSION_OK pseudo.080020f8a5ee
```

Message components are defined as follows:

- timestamp format:
year.month.day hours:minutes:seconds
- thread_name
There are several different types of threads. The most common thread handles DTU authentication, access control, and session monitoring. These threads are named “worker” plus number. The Worker# thread names are reused when a connection terminates. Other threads are:
 - SessionManager#—Communicate with `utsessiond` on behalf of a Worker# thread.
 - AdminJobQ—Used in the implementation to wrap a library that would not otherwise be thread-safe.
 - CallBack#—Communicate with applications such as `utload`.
 - WatchID—Used to poll data/terminals from connections
 - Terminator—Cleans up terminal sessions
 - Group Manager—Main group manager thread
- message_class

Messages with the same thread name are related. The exception occurs when a Worker# thread disconnects a DTU and then purges the connection information from memory. After a Worker# DESTROY message, the next use of that Worker# thread name has no relation to previous uses of the thread name (in other words, the thread names are reused).

- CLIENT_ERROR—Indicates unexpected behavior from a DTU. These messages can be generated during normal operation if a DTU 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—Only occurs if explicitly enabled. Beneficial to developers. Debug messages can reveal session IDs, which must be kept secret to ensure proper security.

TABLE B-5 Error Message Examples

Error class	Message	Description
CLIENT_ERROR	...Exception ... : cannot send keepAliveInf	Error encountered while attempting to send a keep-alive message to a DTU.
	...keepAlive timeout	A DTU has failed to respond within the allotted time. The session is being disconnected.
	duplicate key:	DTU does not properly implement the authentication protocol.
	invalid key:	DTU 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.
NOTICE	"discarding response: " + param	No controlling application is present to receive DTU response.
	"NOT_CLAIMED PARAMETERS: " + param	A token was not claimed by any authentication module.
	...authentication module(s) loaded.	Notification that authentication modules have loaded.

TABLE B-5 Error Message Examples (*Continued*)

Error class	Message	Description
UNEXPECTED	...DISCONNECT ...	Normal notification of disconnection.
	"CallBack: malformed command"	Bad syntax from a user application such as utload or utidle.
	.../ ... read/0:" + ie	Possible program error.
	.../ ... read/1: ... Exception ...	Error encountered while reading messages from the DTU.
	.../... protocolError: ...	Various protocol violations are reported with this message. This is also a way for utauthd to force the DTU to reset.

Troubleshooting USB Mass Storage Devices

The most common problems encountered with USB mass storage devices on Sun Ray DTUs are described in the following sections.

Device Nodes Are Not Created

Some mass storage device types are not supported on Sun Ray. Inspect the log file `/var/opt/SUNWut/log/utstoraged.log` for an indication as to why device nodes were not created.

Device Is Not Automatically Mounted

If the storage medium does not have a OS-recognizable file system, it will not get automatically mounted. An error message will be logged to:
`/var/opt/SUNWut/log/utmountd.log`

Device Is Not Automatically Unmounted

If the device is unplugged, or if the user's session is disconnected from the DTU, all mount points for that DTU are automatically unmounted unless the user has open references to the mount point. In that case, the mount point becomes stale. A stale mount point persists until the administrator unmounts it manually or until the system is rebooted.

Run the following command to find stale mount points.

```
# utdiskadm -s
```

Note – Close all references to the mount point or terminate all processes that refer to the mount before running the `umount` command.

Audio

Each time a user logs in to a Sun Ray DTU, a script automatically assigns the `$AUDIODEV` environment variable to that session. One `utaudio` process is assigned to each session. Refer to the `utaudio(1)` and `audio(7i)` man pages for more information.

Audio Device Emulation

The emulated audio device follows the user session during hotdesking. The device name appears in the `$AUDIODEV` environment variable but is transparently interpreted by audio programs for Sun systems. Device nodes are created in the `/tmp/SUNWut/dev/utaudio` directory. The directory tree is completely recreated at boot time.



Caution – Do not remove the `/tmp/SUNWut/dev/utaudio` directory. Deleting this directory prevents existing users with `utaudio` sessions from using their audio pseudo device nodes.

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

Audio Malfunction

If audio features are malfunctioning:

1. To confirm whether audio is working, run the following command on the DTU:

```
% cat <audio file> >/$AUDIODEV
```

2. Bring up `utsettings`:

```
% utsettings
```

3. Verify that audio output is selected properly, for example, for headphones or speakers.
4. Check the volume level.
5. Verify that Mute is not selected.

Some applications are hard-coded to use `/dev/audio` for output. Sun Ray System Software provides a redirection library that you can use to correct this behavior.

▼ To Activate the Redirection Library

1. Set the environment variable `LD_PRELOAD` to `libc_ut.so` in the shell or wrapper from which you started the audio player:

```
# setenv LD_PRELOAD libc_ut.so
```

2. Restart the application.

Performance Tuning

Some applications, such as intensive 3-D visual simulations, may run very slowly on Sun Ray. Other applications, such as pseudo-stereo viewers using double-buffering, or high-frequency dynamic color table flips on 8-bit visuals, do not produce the expected visual result. Turning off antialiasing can help to save screen resources.

Applications

Placing the user's interactive applications, such as Web browsers or StarOffice, or PC interoperability tools, such as Citrix or Sun Secure Global Desktop (SGD), on the Sun Ray server usually helps performance by reducing network load. The applications benefit from faster transport of commands to the Sun Ray's Xserver.

Applications that can be configured to use shared memory instead of DGA or openGL usually perform better on Sun Ray when they used shared memory.

Sluggish Performance

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 not enough virtual memory available to start an X Window server instance for a user's session.

The solution in this situation is to add more memory or increase the size of the swap partition. In other situations, network load or packet loss may be too high. In very rare cases, network cables or switch equipment may be defective.

1. **To determine whether there is excessive swapping, use `vmstat 5`.**

```
# vmstat 5
```

If there is excessive swapping, the system may be undersized or overutilized.

2. **Verify that network connections are 100F.**
3. **Use `utcapture` to assess network latency and packet loss.**

As latency and packet loss increase, performance suffers.

JDS Tuning

Useful hints for tuning desktop performance, for instance, to use solid backdrops and wireframe window moves, can be found in Java Desktop System

documentation. See, for instance, docs.sun.com/app/docs/doc/817-5099.

Additional tips for Gnome tuning can be found at:

http://www.sun.com/bigadmin/content/submitted/gnome_on_solaris.html

http://www.sun.com/bigadmin/jsp/descFile.jsp?url=descAll/gnome_performance_s

Screensaver Resource Consumption

Many graphics-intensive screensaver programs consume large amounts of CPU, memory, and network bandwidth. To avoid excessive resource consumption, they should be disabled on Sun Ray servers.

▼ To Disable Screensaver Hacks on Linux Systems

It is slightly more complicated to perform the equivalent procedure on Linux systems because the screensaver hacks all reside in one RPM with the `xscreensaver` executables. Thus, instead of removing all the hacks with a single command, it may be necessary to rename the directory or directories that contain the screensavers or restrict their permissions.

Network Switches

There are some network switches that do not work well with Sun Ray DTUs when the server side connection is configured to run at 1 Gbps. Because the DTUs run at 100 Mbps, these switches are required to buffer a certain amount of data, because data are sent from the X Windows server in periodic bursts. This can happen even when the average data rate from the Xserver is well under 100 Mbps. The Xserver is programmed in such a way that a certain allowed amount of data are sent at *tick* intervals. In the original implementation, there were 50 ticks per second, and the Xserver is allowed to send at a certain specific rate granted by the Sun Ray. For example, if the DTU's grant is 40 Mbps, that means that it can send 5 MB per second, in bursts that are sent every 1/50th of a second. That is, at each tick, the server can send 100 KB of data at a rate of 1 Gbps. This would cause a queue buildup in the switch of close to 100 KB, which would then drain out at 100 Mbps over the next 1/50th of a second.

The first thing done to mitigate this issue was to increase the number of ticks per second to 100 per second from 50. Thus, in the example above, the Xserver would send 50 KB every 10 ms, rather than 100 KB every 20 ms. This improved the situation considerably, but did not solve it completely. The 100 ticks per second was chosen since it corresponded to the normal resolution of the timer in Solaris and Linux.

To improve the situation further requires increasing the ticks per second again, but that is only effective if the timer resolution of the underlying system is also increased. On Solaris, this can be accomplished by adding the following line to the `/etc/system` file and rebooting the system:

```
set hires_tick = 1
```


This setting increases the system timer resolution to 1000 ticks per second. The 4.1 Xserver code sets the number of ticks dependent on the system setting, so in the case of setting `hires_tick`, this results in an Xserver ticks per second of 1000, which now means that in the above example, the Xserver sends only 5 KB at each 1 ms tick. This change decreases the amount of buffering required on the switch, so that the behavior of Sun Rays should improve.

Multihead Displays

For information on multihead displays, please see [“Multihead Administration” on page 123](#).

Note – The Sun Ray 2FS is designed to run a single display across two screens without additional configuration. It utilizes a single frame buffer for two displays, and always treats two attached heads as a single, unified display surface to be controlled with a single mouse and keyboard. It always presents itself to the Xserver as a single screen.

Monitor Display Resolution Defaults to 640 x 480

First, eliminate the most obvious possible causes:

- An older monitor
- A bad cable
- Monitor was off when the Sun Ray DTU was started

If the Sun Ray DTU is unable to read DDC data from the monitor, then it defaults to 640 x 480 pixels.

▼ To Correct or Reset the Screen Resolution

1. **Replace the cable**
2. **Restart the Sun Ray DTU after powering the monitor on**
3. **Replace the monitor**
4. **Use the `utresadm` to set persistent display setting to override the default.**

Old Icons (Hourglass with Dashes Underneath) Appear on Display

If the old icons appear on the display, either the DTU's firmware has not been upgraded or it is failing.

1. **Upgrade the firmware to SRSS 4.1.**
2. **Follow the procedure to upgrade the firmware. See the *Sun Ray Software 4.1 Installation and Configuration Guide*.**

Port Currently Owned by Another Application

If this message displays, use the following procedure to correct it:

1. **Download the latest Java Communications API (javax.comm API version 2.0.2 and above)**
2. **Make sure that the supported USB-Serial Adapter is used.**

The supported USB devices list is available at

http://www.sun.com/io_technologies/sunray/usb/

3. **Click the Change Synchronization Settings icon and select the appropriate port (to which the Palm cradle should be connected), then click OK.**
4. **If the ports are not correctly shown in the Serial Port drop down menu, close the application and hot plug the device.**
5. **Start the application again.**

Design Tips

- Avoid drawing into off-screen memory and then copying large areas to the screen. This technique produces slow Sun Ray performance.
- GXcopy mode is usually the fastest drawing mode.
- To display large images, use shared memory pixmaps, if possible.
- Opaque stipple patterns are faster than transparent stipples.
- Opaque (image) text is faster than other text.

Glossary

A

- AAC** Advanced Audio Coding, a “lossy” compression format capable of delivering relatively high quality at relatively low bit rates.
- alias token** An *alias token* enables a card owner to access the same Sun Ray session with more than one physical token. This can be useful, for example, when a user needs a duplicate smart card.
- ALP** The Sun Appliance Link Protocol, a suite of network protocols that enable communication between Sun Ray servers and DTUs.
- AMGH** Automatic Multigroup Hotdesking. See [regional hotdesking](#).
- AH** Authentication headers, used as part of an IPSec implementation.
- authentication policy** The Authentication Manager, using the selected authentication modules, decides what tokens are valid and which users, as token owners, have access to the system and sessions.
- authentication token** Although all tokens are used by the Authentication Manager to grant or deny access to Sun Ray sessions, this term usually refers to a user’s smart card token.

B

- backplane bandwidth** Sometimes also referred to as switch fabric. A switch's backplane is the pipe through which data flows from an input port to an output port. Backplane bandwidth usually refers to the aggregate bandwidth available amongst all ports within a switch.
- barrier mechanism** To prevent clients from downloading firmware that is older than the firmware they already have, the administrator can set a barrier mechanism. The barrier mechanism symbol `BarrierLevel` is defined by default in the DHCP table of Sun Ray servers running version 2.0 or later of Sun Ray Server Software.
- bpp** Bits per pixel.

C

- CABAC** Context-adaptive binary arithmetic coding, a "lossless" entropy coding technique used in H.264/MPEG-4 AVC video encoding.
- CAM** Controlled Access Mode, also known as *kiosk mode*. As of SRSS 4.0, the CAM module was replaced by a rewritten Kiosk module.
- card reader** See *token reader*.
- 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.
- client-server** A common way to describe network services and the user processes (programs) of those services.
- codec** A device or program capable of encoding and/or decoding a digital data stream or signal.
- cold restart** Pressing the Cold Restart button terminates all sessions on a given server before restarting Sun Ray services. See *restart*.
- cut-through switches** The switch begins forwarding the incoming frame onto the outbound port as soon as it reads the MAC address, while it continues receiving the remainder of the frame.

D

- DHCP** Dynamic Host Configuration Protocol, which is a means of distributing IP addresses and initial parameters to the DTUs.
- domain** A set of one or more system boards that acts as a separate system capable of booting the OS and running independently of any other board.
- DTU** Sun Ray desktop units were originally known as Desktop Terminal Units.

E

- ESP** Encapsulating Security Payloads, used as part of *IPSec*.
- 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. It can be a component of the Sun Ray interconnect fabric.

F

- failover** The process of transferring processes from a failed server to a functional server
- failover group** Two or more Sun Ray servers configured to provide continuity of service in the event of a network or system failure. Sometimes abbreviated as FOG or HA (for *high availability*). The term *high availability* refers to the benefit of this type of configuration; the term *failover group* refers to the functionality.
- filling station** When a DTU's firmware is downgraded to an earlier version because it connects to a server running the earlier version, it needs to be connected to a filling station so that it can download newer firmware. For this purpose, a filling station can be any private network configured for Sun Ray services or any shared network in which the Sun Ray DHCP server is the only DHCP server.

firmware barrier See *barrier mechanism*.

FOG See *failover group*.

FTP File Transfer Protocol. The name of the Internet protocol and the program used to transfer files between hosts.

G

GEM Gigabit Ethernet.

group-wide Across a failover group.

H

H.264 A standard for video compression developed by MPEG and VCEG for a wide range of bit rates and resolutions. Also known as MPEG-4 AVC (Advanced Video Coding) and MPEG-4 Part 10.

HA High availability. Sun Ray HA groups have traditionally been called *failover groups*.

head Colloquial term for a screen, or display, or monitor, especially in a context where more than one is used in conjunction with the same keyboard and mouse, as in “multihead” feature.

high availability See *failover*. The term *high availability* refers to the benefit of this type of configuration; the term *failover group* refers to the functionality.

hotdesking The ability for a user to remove a smart card, insert it into any other DTU within a server group, 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 DTUs.

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 DTU.

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 DTUs are hot-pluggable.

I

- idle session** A session that is running on a Sun Ray server but to which no user (identified by a smart card token or a pseudo-token) is logged in.
- IKE** Internet Key Exchange, a component of *IPSec*.
- interconnect fabric** All the cabling and switches that connect a Sun Ray server's network interface cards to the Sun Ray DTUs.
- internet** A collection of networks interconnected by a set of routers that enable them to function as a single, large virtual network.
- Internet** The largest internet in the world, consisting of large national backbone nets (such as MILNET, NSFNET, and CREN) and myriad 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 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). The IP addresses of Sun Ray DTUs are leased.
- IPSec** The Internet Protocol (Security) set of protocols seeks to secure IP communications by encoding data packets through authentication headers (*AH*) and encapsulating security payloads (*ESP*) and by providing a key exchange mechanism (*IKE*).

K

- kiosk mode** A facility to run sessions without UNIX login under an anonymous user account. Kiosk sessions provide a preconfigured, usually restricted, software environment. The term kiosk mode was used interchangeably with *CAM* in

earlier versions of SRSS. As of SRSS 4.0, however, this module was completely rewritten and is now officially called kiosk mode. The term CAM is meant to refer to implementations in SRSS 3.1 and earlier.

L

- LAN** Local Area Network. A group of computer systems in close proximity that can communicate with one another through 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 DTU'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.

M

- 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.
- mobile token** If mobile sessions are enabled, a user can log into an existing session from different locations without a smart card, in which case the user name is associated with the session. This type of *pseudo-token* is called a mobile token.

- mobility** For the purposes of the Sun Ray Server Software, the property of a session that allows it to follow a user from one DTU to another within a server 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.
- MPPC** Microsoft Point-to-Point Compression protocol.
- MTU** Maximum Transmission Unit, used to specify the number of bytes in the largest packet a network can transmit.
- multicasting** The process of enabling communication between Sun Ray servers over their Sun Ray network interfaces in a failover environment.
- multihead** See [head](#).
- multiplexing** The process of transmitting multiple channels across one communications circuit.

N

- NAT** See [network address translation](#).
- 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 address translation** NAT. Network address translation typically involves the mapping of port numbers to allow multiple machines (Sun Ray DTUs in this case, but not Sun Ray servers) to share a single IP address.
- 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.
- NIC** Network interface card.
- non-smart card mobility** A mobile session on a Sun Ray DTU that does not rely on a smart card. NSCM requires a policy that allows *pseudo-tokens*.
- NSCM** See *non-smart card mobility*.

O

- OSD** On-screen display. The Sun Ray DTU uses OSD icons to alert the user of potential start-up or connectivity problems.

P

- PAM** Pluggable Authentication Module. A set of dynamically loadable objects that gives system administrators the flexibility of choosing among available user authentication services.
- PAM session** A single PAM handle and run time state associated with all PAM items, data, etc.
- 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.
- PCM** Pulse Code Modulation.

policy	See <i>authentication policy</i> .
Pop-up GUI	A mechanism that allows the entry of configuration parameters for a Sun Ray DTU from the attached keyboard.
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.
POST	Power-on self test.
power cycling	Using the power cord to restart a DTU.
pseudo-session	A Sun Ray session associated with a <i>pseudo-token</i> rather than a smart card token.
pseudo-token	A user accessing a Sun Ray session without a smart card is identified by the DTU's built-in type and MAC address, known as a pseudo-token. See <i>token</i> .

R

regional hotdesking	Originally known as Automatic Multigroup Hotdesking (AMGH), this SRSS feature allows users to access their sessions across wider domains and greater physical distances than was possible in earlier versions of SRSS. Administrators enable this feature by defining how user sessions are mapped to an expanded list of servers in multiple failover groups.
RHA	Remote Hotdesk Authentication, a security enhancement that requires SRSS authentication before users can reconnect to an existing session. RHA does not apply to Kiosk sessions, which are designed for anonymous access without authentication. RHA policy can be administered either with a GUI checkbox or with the <code>utpolicy</code> command.
restart	Sun Ray services can be restarted either from the <code>utrestart</code> command or with the Warm Restart or Cold Restart buttons on the GUI. A cold restart terminates all Sun Ray sessions; a warm restart does not.

S

screen flipping	The ability to pan to individual screens on a DTU with a single head that were originally created by a multihead group.
------------------------	---

- server** A computer system that supplies computing services or resources to one or more clients.
- service** For the purposes of the Sun Ray Server Software, any application that can directly connect to the Sun Ray DTU. It can include audio, video, Xservers, access to other machines, and device control of the DTU.
- session** A group of services associated with an authentication token. A session may be associated with a token embedded on a smart card. See *token*.
- session mobility** The ability for a session to “follow” a user’s login ID or a token embedded on a smart card.
- smart card** Generically, a plastic card containing a microprocessor capable of making calculations. Smart cards that can be used to initiate or connect to Sun Ray sessions contain identifiers, such as the card type and ID. Smart card tokens may also be registered in the Sun Ray Data Store, either by the Sun Ray administrator or, if the administrator chooses, by the user.
- smart card token** An authentication token contained on a smart card. See *token*.
- SNMP** Simple Network Management Protocol
- spanning tree** The spanning tree protocol is an intelligent algorithm that allows bridges to map a redundant topology and eliminates packet looping in Local Area Networks (LAN).
- store-and-forward switches** The switch reads and stores the entire incoming frame in a buffer, checks it for errors, reads and looks up the MAC addresses, and then forwards the complete good frame out onto the outbound port.
- subnet** A working scheme that divides a single logical network into smaller physical networks to simplify routing.
- SUNWut** The naming convention for the earliest incarnation of the Sun Ray thin client used the stock symbol for Sun Microsystems (SUNW) plus the letters “ut” to stand for Unix Terminal. Similarly, Sun Ray-specific commands begin with the characters “ut”.

T

- 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.

- thin client** Thin clients remotely access some resources of a computer server, such as compute power and large memory capacity. The Sun Ray DTUs rely on the server for all computing power and storage.
- tick** The time interval since some network event. Early versions of SRSS defined a tick as 1/50th of a second. It is now defined as 1/100th of a second, which is the usual *SNMP* convention.
- timeout value** The maximum allowed time interval between communications from a DTU to the Authentication Manager.
- token** The Sun Ray system requires each user to present a token, which the Authentication Manager uses to allow or deny access to the system and to sessions. A token consists of a type and an ID. If the user uses 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 DTU's built-in type and ID (the unit's Ethernet, or MAC, address) are used instead as a *pseudo-token*. If mobile sessions are enabled, a user can log into an existing session from different locations without a smart card, in which case the user name is associated with the session. A pseudo-token used for mobile sessions is called a *mobile token*. *Alias tokens* can also be created to enable users to access the same session with more than one physical token.
- token reader** A Sun Ray DTU that is dedicated to reading smart cards and returning their identifiers, which can be associate with card owners (i.e. with users).
- trusted server** Servers in the same failover group "trust" one another.

U

- URI** Uniform Resource Identifier, the generic term for all types of names and addresses that refer to objects on the World Wide Web.
- 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 (such as 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.
- USB** Universal Serial Bus.
- 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*, *jp_morg*, *jpm-888*. The first character must be a letter.

user session A session that is running on a Sun Ray server and to which a user (identified by a smart card token or a pseudotoken) is logged in.

ut... See *SUNWut*.

V

VC-1 Informal name of the SMPTE 421M video codec standard, now a supported standard for Blu-ray Discs and Windows Media Video 9.

virtual frame buffer A region of memory on the Sun Ray server that contains the current state of a user's display.

VLAN Virtual Local Area Network.

VPN Virtual Private Network.

W

warm restart See *restart*.

WMA Windows Media Audio data compression file format and codec developed by Microsoft.

work group A collection of associated users who exist in near proximity to one another. A set of Sun Ray DTUs that are connected to a Sun Ray server provides computing services to a work group.

X

Xnewt The new default Xserver for Sun Ray Server Software 4.1 and later on Solaris.

Xserver A process which controls a bitmap display device in an X window system. It performs operations on request from client applications.

Y

YUV Simple, lossless mechanism to store images or a sequence of images.

Index

Symbols

.parms files, 105

A

Admin GUI, 56

admin password, 18

Administration Tool

 changing the admin password, 56

 desktops

 displaying current properties, 44

 editing a single desktop's properties, 45

 examining log files, 38

AdminJobQ, 196

AltAuth, 79, 98, 99

AMGH, 67

appliance

 hotdesking to a multihead group, 131

 multihead feature, 123

 multihead group, 124

ARCFOUR, 73

attacks

 man-in-the-middle, 74

AUDIODEV environment variable, 198

authentication, 73

 server, 74

Authentication Manager, 5, 35, 131, 151, 155

 configuration file, 156

 flowchart for primary appliance, 132, 133

 interacting with Session Manager, 7

 restarting, 157

AuthPort, 98

AuthSrvr, 6, 79, 98, 183

B

barrier

 firmware, 191

BarrierLevel, 98

bidirectional encryption, 74

BOOTP forwarding, 80

BYTES SENT, 36

C

Cabling

 fiber-optic, 10

CallBack#, 196

central registration, 6

Cisco IOS Executive, 80

Cisco IOS-based router, 97

Cisco router, 103

Citrix, 200

client

 authentication, 73

CLIENT_ERROR, 196

code

 DHCP option, 101

command

 utadm, 150, 155

 utcapture

 data elements, 35

 utconfig, 123, 158, 165

 utmhconfig, 124

 utreplica, 158

- utswitch, 22
- commands
 - utadm, 27
 - utadm -r, 30
 - utaudio, 198
 - utfwadm, 30
- CONFIG_ERROR, 196
- configuration
 - security, 74, 75
- configuration data
 - DHCP, 27, 149, 152
- crontab, 158
- Ctrl-Moon, 173
- Ctrl-Power, 173
- cursor
 - green newt, 184
 - X, 184

D

- daemon
 - data store, 31
- Data Store, 158
- data store, 9
 - primary server, 163
 - regional hotdesking
 - to configure, 70
- DCHP
 - state codes, 178
- DCHP State Code, 178
- DEBUG, 196
- dedicated interconnect, 82
- departments, 11
- desktopID, 36
- desktops
 - displaying current properties, 44
 - editing a single desktop's properties, 45
- device
 - directory, 59
 - links, 61
 - node ownership, 61
 - nodes, 60
 - USB, 60
- DHCP, 150, 182
 - configuring for failover, 152
- DHCP Client Class, 99
- DHCP configuration data, 27, 149, 152

- DHCP option 49, 97
- DHCP options
 - vendor-specific, 98
- DHCP Relay Agent, 80
- DHCP relay agent, 91
- DHCP server, 153
- DHCP servers, 149
- DHCPACK, 101
- DHCPDISCOVER, 80
- DHCPINFORM, 80, 101
- DHCPServer, 183
- directly-connected dedicated interconnect, 85
- directly-connected shared subnet, 82, 87, 88, 90
- DNS, 105
- Domain Name Service, 105
- DSA, 73
- dtlogin, 5
- DTU, 35
- DTU Hardware State, 179
- DTU initialization, 78
- duplicate IP addresses, 27, 149, 152
- Dynamic Host Configuration Protocol (DHCP), 3

E

- e, 148
- each, 148
- encapsulated options, 101
- encryption
 - algorithm, 73
 - bidirectional, 74
 - downstream only, 74
 - upstream only, 74
- environment variables
 - LD_PRELOAD, 199
- errors
 - out of memory, 27, 149, 152

F

- failover
 - address allocation formula, 150
 - configuring DHCP, 152
 - group, 147
 - primary server, 158
 - removing replication configuration, 160
 - secondary server, 159

- Group Manager module, 149
 - principle components needed, 149
 - server IP addresses, 151
 - setting up group, 158
 - taking servers offline, 166
- failover group, 12
 - administration status, 161
 - recovery procedures, 162
- failover groups, 148
- firmware download, 190
- firmware module, 4
 - PROM version management, 30
- frame buffer, 3
- FWSrvr, 98, 99, 102

G

- GDM, 5, 119
- GDM installation, 119
- GDM privileges, 120
- gmSignature, 165
- Gnome Display Manager, 5
- green newt cursor, 183
- green newt icon, 184
- Group Manager
 - keepalive message, 156
 - load balancing, 157
 - redirection, 20, 156
 - using Authentication Manager properties, 156
- Group manager, 155
- group manager
 - keepalive message, 156
- group manager module, 155
- group signature, 17
 - setting up, 165
- GXcopy, 204

H

- hacking
 - man-in-the-middle attacks, 74
- hard security mode, 74
- hexadecimal values, 101
- hot key, 170
 - changing setting, 172
 - changing setting site-wide, 172
 - entry, 171

- values, 171
- Hotdesking, 61
- hotdesking, 131, 199
 - regional, 67

I

- Icon Codes, 176
- icon messages
 - OSD, 176
- IEEE802.MACID directory, 59
- ifname, 85
- INFORMServer, 183
- Interconnect, 10
- interconnect
 - boost power of, 10
 - dedicated, 82
- interconnect fabric
 - adding an interface, 28
 - deleting an interface, 28
 - departments, 11
 - failover group, 12
 - managing, 27
 - printing configuration, 29
 - removing an interface, 30
- interconnect IP address, 27, 149, 152
- Internal database, 158
- Intf, 98
- IOS, 97
- IP address
 - duplicate, 27, 149, 152

K

- keepalive message, 156

L

- LATENCY, 36
- LD_PRELOAD environment variable, 199
- LDIF, 163
- LED signals, 179
- libusb, 66
- load balancing, 157
 - turning off, 158
- log files
 - examining, 38
- LogAppl, 98, 99

- LogHost, 98, 99
- login screen, 5
- LogKern, 98, 99
- LogNet, 98, 99
- LogUSB, 98, 99
- LogVid, 98, 99
- low-bandwidth deployment, 1, 100

M

- man-in-the-middle attack, 74
- mass storage, 167
- Maximum Transfer Unit (MTU), 103
- message_class, 196
- modules, 5
 - Registered, 6
 - StartSession, 6
- mount point
 - stale, 198
- MTU, 103
- multihead
 - administration tool, 126
 - creating a new group, 128
 - group, 124, 132
 - hotdesking to an appliance, 131
 - screen display, 125
 - turning on policy from command line, 126
 - turning on policy with administration tool, 126
- multihead feature, 123

N

- NAT, 3
- Netscape, 200
- network
 - adding an interface, 28
 - deleting an interface, 28
 - removing an interface, 30
- NewTBW, 98
- NewTDispIdx, 98
- NewTFlags, 98
- NewTVer, 98, 99
- non-secure session, 74
- NOTICE, 196

O

- openGL, 200

- option 49, 79, 97
- option code, 101
- options
 - encapsulated, 101
- OSD
 - icon messages, 176
 - understanding, 175
- out of memory error, 27, 149, 152

P

- packet loss
 - utcapture, 35
- packets, 100
 - out-of-order, 100
- PAM
 - stack, 68
- panning, 125
- parallel peripherals, 59
- PERCENT LOSS, 36
- peripherals, 167
 - parallel, 59
 - serial, 59
- persistent settings (monitor), 18
- policies, 5
- POST, 4
- power cycle, 173
- Power LED, 179
- power-on self test (POST)
 - firmware module, 4
- Primary server, 158
- printers
 - non-PostScript, 66
 - setting up, 64
- PROM, 30
- ps, 8

R

- rdate, 158
- redirection
 - Group Manager, 20, 156
- redundant failover group, 149
- regional hotdesking, 67
- Registered module, 6
- Relay Agent
 - DHCP, 80

- remote shared subnet, 82
- remote subnet, 92
- Remove replication, 160
- restart, 126
- RHA, 8, 16, 52, 70, 71
 - disable, 72
 - re-enable, 72

S

- screen flipping, 131
- Secondary server, 158
- secure session, 74
- security
 - configuration, 74, 75
 - interconnect, 73
 - session, 75
- security mode
 - hard, 74
 - soft, 74
- security status, 76
- self-registration, 6
- serial peripherals, 59
- server
 - authentication, 73, 74
- Server addresses, 151
- Server-to-switch bandwidth, 10
- session, 7
 - changes, 8
 - secure vs non-secure, 74
- session change, 62
- Session Manager, 2, 7
- session timeout, 112
- session types, 194
- SessionManager#, 196
- settings
 - monitor
 - persistent, 18
- shared memory, 200
- simple failover group, 148
- soft security mode, 74
- spoofing, 74
- SRDS, 9
- StarOffice, 200
- StartSession module, 6
- state codes

- DHCP, 178
- status
 - security, 76
- storage
 - devices
 - supported, 167
 - USB
 - mass, 167
- subnet
 - directly-connected
 - shared, 87, 88, 90
 - remote
 - deployment on, 92
- Sun Data Store, 17
- Sun Ray
 - Data Store, 158
- Sun Ray administration data
 - changing, 56
- Sun Ray appliance, 1, 3
 - firmware module, 4
 - multihead feature, 123
 - multihead group, 124
 - shield users, 10
- Sun Ray data store daemon, 31
- Sun Ray DTU
 - updating and upgrading, 30
- Sun Ray DTU (appliance), 35
- Sun Ray interconnect
 - server IP addresses, 151
- Sun Ray server, 1, 35
 - device directory, 59
 - network interfaces, 10
 - software, 4
- Sun Ray Settings
 - changing, 168
- Sun Secure Global Desktop, 200
- SUNW.NewT.SUNW, 98, 99
- Switch
 - high-capacity, 10
 - low-capacity, 10
- switch
 - basic types of 100 Mbps, 10
- syslog, 191

T

- TCP, 151

- TerminalGroup policy, 131
- TERMINALID, 36
- Terminator, 196
- TFTP, 102
- thread_name, 195
- threads, 196
- timeout
 - idle, 112
 - keepalive, 156, 196
 - kiosk, 144
 - video, 112
 - VPN, 112, 115, 178
- TIMESTAMP, 36
- TOTAL LOSS, 36
- TOTAL PACKET, 36

U

- UNEXPECTED, 196
- Uplink ports, 10
- utaction, 16
- utadm, 16
- utadm -A, 90
- utadm command, 27, 150
 - available options, 155
- utadm -L, 91
- utadm -r command, 30
- utadminuser, 16
- utamghadm, 69, 71
- utaudio command, 198
- utauthd, 197
- utcapture, 16, 102
- utcapture command
 - data elements, 35
- utcard, 16, 32
- utconfig, 16
- utconfig command, 123, 158, 165
- utcrypto, 16, 74
- utdesktop, 16
- utdetach, 16, 171
- utdevadm, 26
- utdiskadm, 17
- utdsd daemon, 31
- utdssync, 17
- uteject, 17
- utfwadm, 17
- utfwadm command, 30
- utfwload, 17
- utfwsync, 17
- utgroupsig, 17, 165, 166
- utgstatus, 17
- utidle, 197
- utinstall, 17
- utkiosk, 17
- utload, 197
- utmhadm, 17, 123
- utmhconfig, 18, 123
- utmhconfig command, 124
- utmount, 18
- utpolicy, 18
- utpreserve, 18
- utpw, 18
- utquery, 18, 102, 183
- utreader, 18
- utreplica, 18
- utreplica command, 158
- utresadm, 18, 169, 170
- utresdef, 18
- utrestart, 18, 126
- utselect, 18, 20, 62, 156
- utsession, 18
- utsessiond, 8, 196
- utset, 18
- utsettings, 18, 169, 171
- utswitch, 18, 20, 62
- utswitch command, 22
- utumount, 18
- utuser, 19, 35
- utwall, 19
- utwho, 19
- utxconfig, 19

V

- v, 17
- vendor-specific DHCP options, 98
- vendor-specific options, 99
- video timeout, 112
- virtual frame buffer, 3

VLAN, 10
VPN timeout, 112, 115

W

WAN, 1, 100
WatchID, 196

X

X cursor, 184
X Window Display Manager, 79, 97, 99
XINERAMA, 130
Xnewt, 8, 19

