



Sun Ray Server Software 1.3 Administrator's Guide

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900 U.S.A.
650-960-1300

Part No. 806-7712-10
July 2001, [Revision 01](#)

[Send comments about this document to: docfeedback@sun.com](mailto:docfeedback@sun.com)

Copyright 2001 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, CA 94303-4900 U.S.A. All rights reserved.

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

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, ShowMe TV, Sun Camera, Java, JDK, 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.

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.

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 2001 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, CA 94303-4900 Etats-Unis. Tous droits réservés.

Ce produit ou document est 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 logo Sun, ShowMe TV, Sun Camera, Java, JDK, 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.

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

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	xi
Before You Read This Book	xi
How This Book Is Organized	xii
Using UNIX Commands	xii
Typographic Conventions	xiii
Shell Prompts	xiii
Related Documentation	xiv
Accessing Sun Documentation Online	xiv
Ordering Sun Documentation	xiv
Sun Welcomes Your Comments	xv
1. Sun Ray System Overview	1
Part 1—The Sun Ray System	1
Sun Ray Server Software	2
Sun Ray Appliance	3
Power Cycling	3
Firmware Module	3
Server Ports	4
Device Emulation Capabilities	4

Interoperability	4
Sun Ray Interconnect Fabric	5
Workgroup Scenario	5
Department Scenario	5
Failover Scenario	6
Part 2—The System Functions	7
Authentication Manager	8
Alternate Server List	9
Token Readers	9
Mobility—Hot Desking	11
Sessions and Services	11
Session Manager	11
Changes in a Session	12
Sun Ray Appliance Settings	13
▼ To Change the Sun Ray Settings	13
Part 3—Security Considerations	14
2. Non-Smart Card Mobile Sessions	15
NSCM Session	15
Sun Ray Mobile Session Login Dialog Box	15
▼ To Log In to an NSCM Session	17
Disconnecting an Active NSCM Session	19
Hot Key	19
▼ To Disconnect the Current Session	19
▼ To Terminate the Current Session	19
▼ To Create a utdetach Alias	19
▼ To Customize the Short Cut for Disconnecting an NSCM Session	19
▼ To Terminate the Current NSCM Session	20

NSCM and Failover Groups	20
Load Balancing Between Servers	21
Connecting to Existing Sessions	21
Switching Between Servers	21
Pseudo-Token Sessions	22
Considerations	22
Configuring the Authentication Manager for NSCM Sessions	22
▼ To Enable NSCM Sessions From the Administration Tool	23
▼ To Enable NSCM Sessions From a Command Line	25
3. Administration Tool	27
Administration Data	27
Logging In	28
▼ To Log Into the Administration Tool	28
▼ To Change the Administrator's Password	30
Changing Policies	31
▼ To Change the Policy	31
Resetting and Restarting Sun Ray Services	33
▼ To Reset Sun Ray Services	33
▼ To Restart Sun Ray Services	33
Token Readers	34
Creating a Token Reader	34
▼ To Create a Token Reader	34
▼ To Locate Token Readers	35
Managing Desktops	36
▼ To List All Desktops	36
▼ To Display a Desktop's Current Properties	37
▼ To List Currently Connected Desktops	38

- ▼ To View the Properties of the Current User 39
- ▼ To Search for Desktops 40
- ▼ To Edit a Single Desktop's Properties 41
- Multihead 42
 - ▼ To View All Multihead Groups 43
- Viewing Failover Group Status 44
 - ▼ To View Failover Group Status 45
 - Sun Ray Failover Group Status Icons 46
- Examining Log Files 47
 - ▼ To View a Log File 47
- Managing Smart Cards From Different Vendors 48
 - ▼ To View or List Configured Smart Cards 49
 - ▼ To View The Smart Card Probe Order 50
 - ▼ To Change the Smart Card Probe Order 51
 - ▼ To Add a Smart Card 51
 - ▼ To Delete a Smart Card 52
- Sun Ray System Status 53
 - ▼ To View the Sun Ray System Status 53
- Administering Users 55
 - ▼ To View Users by ID 56
 - ▼ To View Users by Name 56
 - ▼ To Delete a User 56
 - ▼ To View Current Users 57
 - ▼ To Display a User's Current Properties 57
 - ▼ To View the User's Sessions 59
 - ▼ To Edit a User's Properties 59
 - ▼ To Add a Token ID to a User's Properties 60

▼	To Delete a Token ID From a User's Properties	60
▼	To Enable or Disable a User's Token	60
▼	To Add a User	61
▼	To Find a User	62
▼	To Get a Token ID From a Token Reader	62
	Controlled Access Mode	63
▼	To Configure Controlled Access Mode	63
▼	To Select Additional Applications	64
▼	To Add or Edit Applications	65
	Managing Sessions	67
▼	To View Sun Ray Sessions	67
▼	To Find Sun Ray Sessions	68
	Accessing Online Documentation	69
▼	To Access Online Documentation	69
4.	Using the Command-Line Interface	71
	Supported Commands	71
▼	To Stop Sun Ray Services	74
▼	To Start Sun Ray Services	75
	Changing Policies	75
	Configuring Interfaces on the Sun Ray Interconnect Fabric	75
▼	To Add an Interface	76
▼	To Delete an Interface	76
▼	To Remove All Interfaces	76
▼	To Print the Sun Ray Interconnect Configuration	77
	Managing PROM Versions	77
▼	To Update All of the Appliances on an Interface	78
▼	To Update an Appliance Using the Ethernet (MAC) Address	79

Restarting Sun Directory Services	79
▼ To Restart Sun Directory Services	79
Solaris Lock Screen for Detached Sessions	80
▼ To Lock a Screen Using CDE	80
▼ To Lock an OpenWindows Session	80
▼ To Create a System-Wide Default for Screen Locking	80
▼ To Get a Token ID From a Token Reader	81
Configuring Sun Ray Settings	81
Setting Hot Key Values	83
▼ To Change the Hot Key Setting System-Wide	83
▼ To Change the Hot Key Setting for a Single User	84
Smart Card Vendor Configuration Files	84
▼ To Load a Configuration File Into the Directory	85
▼ To Configure a Token Reader	85
5. Peripherals for Sun Ray Appliances	87
Device Nodes and USB Peripherals	87
Device Nodes	88
Device Links	89
Device Node Ownership	89
Hot Desking and Device Node Ownership	89
Attached Printers	90
Printer Setup	90
▼ To Set Up a Printer	90
Printers Other Than PostScript™ Printers	92
PDA Synchronization	92
PDASync for Solaris™ Application on Sun Ray Appliances	93
▼ To Set Up the PDASync Application on a Sun Ray Appliance	93

Adapters 94

A. Troubleshooting 95

- ▼ To Restart DHCP 96
- ▼ To Activate the Redirection Library 100
- ▼ To Identify and Unconfigure the `dtlogin` Session 108
- ▼ To Determine the Integrity of the Configuration Files 109
- ▼ To Replace the `Xservers` and `Xconfig` Files 110

Glossary 115

Preface

The *Sun Ray Server Software 1.3 Administrator's Guide* provides instructions for setting up, administering, and monitoring a system of Sun Ray™ appliances. These instructions are designed for an experienced system administrator with networking knowledge.

Before You Read This Book

This guide assumes that you have installed the Sun Ray server software 1.3 on your server and that you have added any required patches.

In order to fully use the information in this document, you must have thorough knowledge of the topics discussed in these books:

- *Sun Ray Server Software 1.3 Readme*
- *Sun Ray Server Software 1.3 Installation Guide*

How This Book Is Organized

Chapter 1 describes the Sun Ray system.

Chapter 2 describes the Administration Tool.

Chapter 3 describes the command-line interface.

Chapter 4 describes peripherals for Sun Ray appliances.

Appendix A provides troubleshooting information, including error messages from the Authentication Manager.

This manual also contains a glossary.

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 contain information about unique Sun Ray system commands.

See one or more of the following for this information:

- AnswerBook2[™] online documentation for the Solaris[™] operating environment
- Other software documentation that you received with your system

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 1.3 Installation Guide</i>	806-7711-10
Software	<i>Sun Ray Server Software 1.3 Advanced Administrator's Guide</i>	806-7713-10
	<i>Sun Ray Server Software 1.3 Readme</i>	

Accessing Sun Documentation Online

The `docs.sun.com`SM web site enables you to access a select group of Sun technical documentation on the Web. You can browse the `docs.sun.com` archive or search for a specific book title or subject at:

<http://docs.sun.com>

For Sun Ray specific documentation:

<http://www.sun.com/products/sunray/docs>

Ordering Sun Documentation

Fatbrain.com, an Internet professional bookstore, stocks select product documentation from Sun Microsystems, Inc.TM

For a list of documents and how to order them, visit the Sun Documentation Center on Fatbrain.com at:

<http://www.fatbrain.com/documentation/sun>

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 (806-7712-10) of your document in the subject line of your email.

Sun Ray System Overview

This chapter provides a three-part overview of the Sun Ray system:

- “Part 1—The Sun Ray System” on page 1
- “Part 2—The System Functions” on page 7
- “Part 3—Security Considerations” on page 14

Part 1—The Sun Ray System

The Sun Ray system consists of:

- one or more Sun servers running the Sun Ray server software on the Solaris operating environment
- Sun Ray appliances
- an *interconnect fabric* (network) that ties the server and appliances together (FIGURE 1-1).

The software is installed on a server running the Solaris 2.6, Solaris 7, or Solaris 8 operating environment.

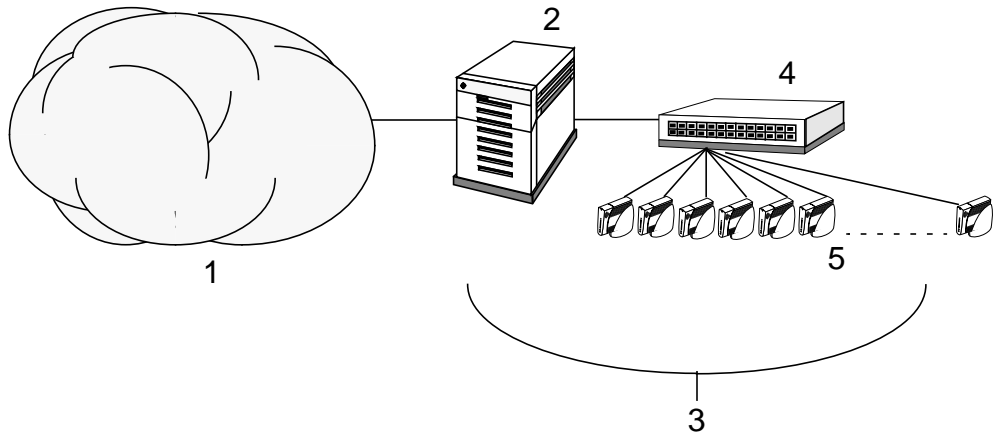


FIGURE 1-1 Example Sun Ray System

Legend:

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

Sun Ray Server Software

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

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

The Sun Ray server software provides the user with access to all Solaris applications and a variety of X Windows and legacy (mainframe) applications, which are currently third-party emulations. The installation of third-party applications enables the user to access Microsoft Windows NT applications.

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

Sun Ray Appliance

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

- 24-bit, 2-D accelerated graphics up to 1280x1024 resolution at 85 Hz (640 x 480 at 60 Hz is the lowest resolution)
- Multichannel audio input and output capabilities
- Composite video input
- Smart card reader
- USB ports that support hot-pluggable peripherals

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

All Sun Ray appliances are identical except for the Ethernet MAC address. If an appliance ever fails, simply replace it with another appliance. Sun Ray appliance IP addresses are leased to each Sun Ray appliance when it is connected and can be reused when the appliance is disconnected. IP address leasing is managed by the Dynamic Host Configuration Protocol (DHCP).

Power Cycling

A Sun Ray appliance can be power cycled by disconnecting the power cord, waiting 15 seconds, and reconnecting the power cord.

Firmware Module

A small firmware module in each Sun Ray appliance is updated from the server. This module checks the hardware with a power-on self test (POST) and boots the appliance. The Sun Ray appliance also contacts the server to authenticate the user

and handles low-level input (such as keyboard, mouse, and display information) and output. If there is a problem with the appliance, the module displays an on-screen display (OSD) icon.

Server Ports

Do not assign other services to the Sun Ray server ports. The following list details the port usage in the `/etc/inet/services` file.

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

Device Emulation Capabilities

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

The emulated audio device follows the user session during Hot Desking. The device name appears in the `$AUDIODEV` environment variable but is transparently interpreted by audio programs for Sun systems. Device nodes 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.

Interoperability

The Interoperability white paper is available at the following website:

<http://www.sun.com/products/sunray/whitepapers/index.html>

Further information about Citrix is available at the Citrix website:

<http://www.citrix.com>

Further information about Tarantella is available at the Tarantella website:

<http://www.tarantella.com>

Further information about HOblink is available at the HOBsoft website:

<http://www.HOBsoft.com>

Sun Ray Interconnect Fabric

The recommended Sun Ray interconnect is implemented with a physically dedicated Ethernet network. Deployments using Virtual Local Area Network (VLAN) technology to implement a logically dedicated network are also supported. The dedicated interconnect is the recommended environment for Sun Ray appliances.

Sun Ray appliances are connected to the server over this network using an application-specific protocol. This network is based on 10/100BASE-T Ethernet technology, using layer-2 or layer-3 switches and *Category 5* wiring. Each Sun Ray appliance is attached to the interconnect fabric through its built-in 10/100BASE-T interface.

Note – Using Category 3 wiring with 10BASE-T equipment reduces performance.

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

- “Workgroup Scenario” on page 5
- “Department Scenario” on page 5
- “Failover Scenario” on page 6

Workgroup Scenario

For small workgroups with between 5 and 50 Sun Ray appliances, 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 appliances.

For example, in FIGURE 1-1 a Sun Enterprise™ 220R server with a Sun card 10/100BASE-T card and a 24-port 10/100BASE-T switch can easily support 23 users.

Department Scenario

For departments with groups consisting of 100 or more Sun Ray appliances, the Sun Ray server uses one or more gigabit Ethernet cards to connect to large 10/100BASE-T switches.

A 100-user departmental system, for example, consisting of a Sun Enterprise 420R server, one gigabit Ethernet card, and two large (48-port and 80-port) 10/100BASE-T switches delivers services to the 100 Sun Ray appliances (FIGURE 1-2).

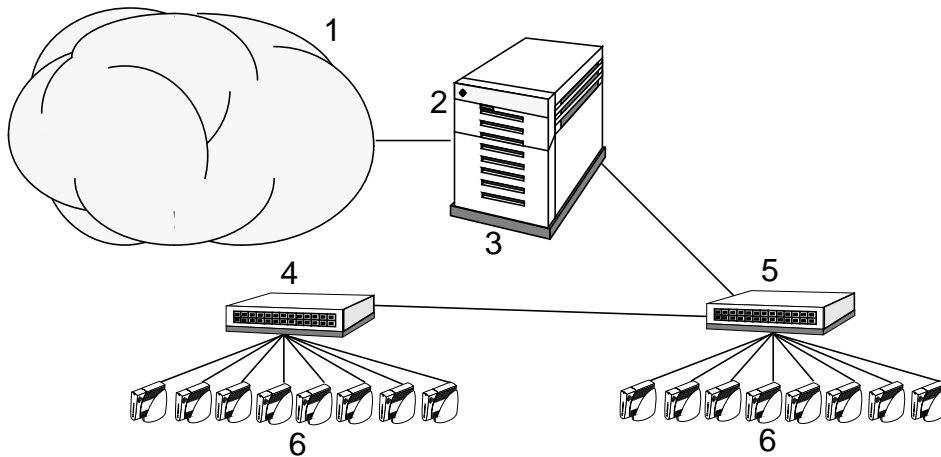


FIGURE 1-2 Department Scenario

Legend:

1. Local area network (LAN)—Existing connection to Intranet/Internet
2. Sun Enterprise 420R server
3. Gigabit Ethernet card
4. 80-port, 10/100BASE-T switch with gigabit uplink and downlink ports
5. 48-port 10/100BASE-T switch with gigabit uplink
6. Sun Ray appliances

Failover Scenario

A failover group, comprising two or more servers, provides users with a higher level of availability should one of those servers become unavailable due to a network or system failure.

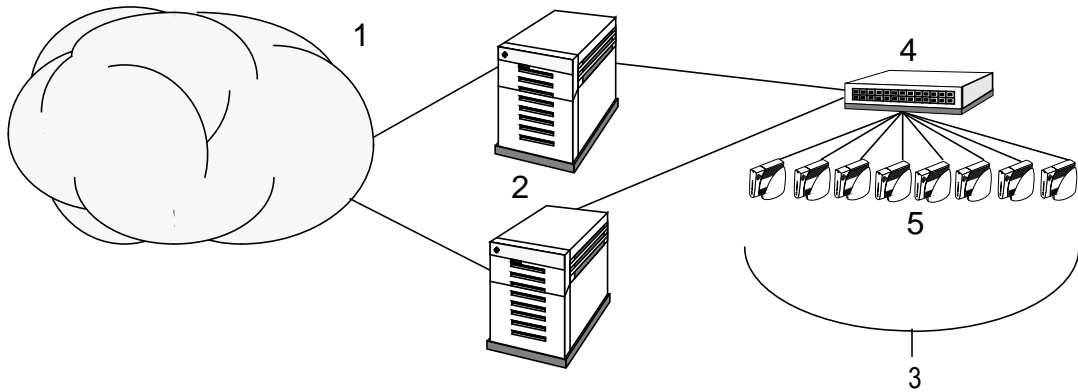


FIGURE 1-3 Failover Group

Legend:

1. Public network—Existing connection to intranet or Internet
2. Sun Ray servers
3. Interconnect
4. Switches
5. Sun Ray appliances

Should a server fail in a failover group, each Sun Ray appliance that was using that server reconnects to another server in the failover group. The appliance connects to a previously existing session for that token if there is one on another server. If there is no existing session, the appliance connects to a server selected by the load-balancing algorithm. This server presents a login screen to the user, and the user must relogin to create a new session. The session on the failed server is lost.

Part 2—The System Functions

Two unique system functions are crucial to the proper and continued operation of the Sun Ray system:

- Authentication Manager
- Session Manager

Authentication Manager

The Authentication Manager implements the chosen policies for identifying and authenticating users on Sun Ray appliances. The Authentication Manager also verifies user identities and implements site access policies. The Authentication Manager is not visible to the user.

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

1. A user accesses an appliance.
2. The appliance (item 2 in FIGURE 1-4) sends the user's token information to the Authentication Manager (item 3) and requests access. If a smart card is presented to the appliance, the smart card's type and ID are the token. If not, the appliance's Ethernet address is sent.
3. If the Authentication Manager runs through the entire list of modules and no module takes responsibility for the request, the user is denied.
4. If the user is accepted, the Authentication Manager starts an X Windows session (item 5) for the user, which takes the user to the `dtlogin` screen.

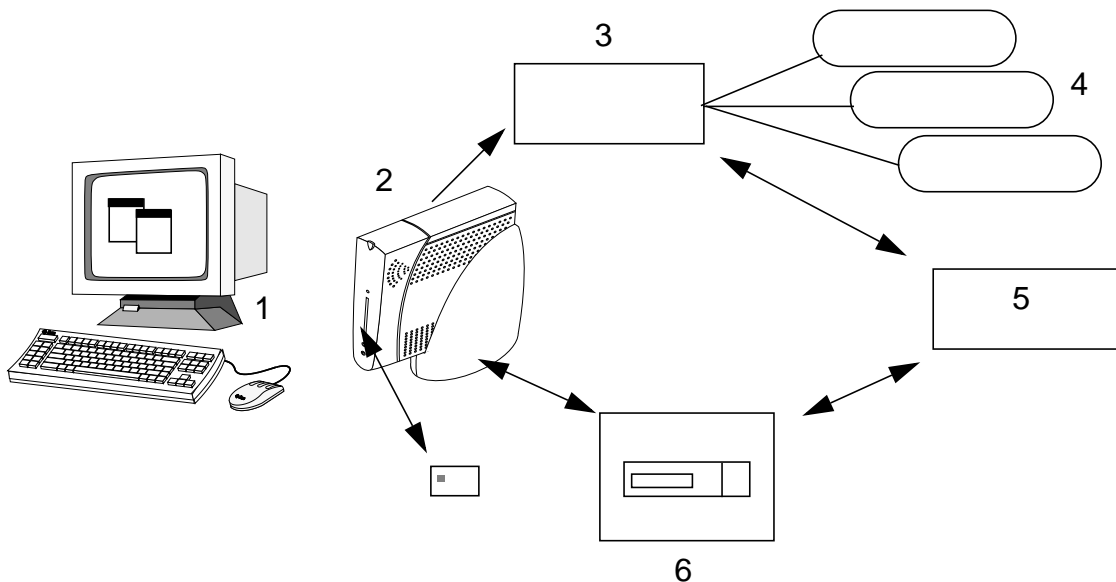


FIGURE 1-4 Authentication and Session Manager Interaction

Alternate Server List

When the server list is defined, it disables the normal authentication discovery protocol.

Normally, the Sun Ray appliance looks for the Authentication Manager DHCP option and contacts that address. If that field hasn't been supplied or the server does not respond, it sends a broadcast request for any authentication manager on the subnet.

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. If you want the broadcast feature enabled, then the broadcast address (255.255.255.255) must be the last one in the list. Any addresses after the broadcast address are ignored.

Note – If the local server is not in the list, Sun Ray appliances will not attempt to contact it.

Token Readers

When you enable an authentication policy with registered users, specify smart card IDs. Some manufacturers print the smart card ID on the card itself, but many do not. Since all of the administrative functions refer to this token ID, the Sun Ray server software provides a way to designate one or more specific appliances as dedicated token readers. Site administrators can use these dedicated appliances to administer Sun Ray users.

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

See FIGURE 1-5 for an example of a configuration that includes a token reader. The second appliance (item 2) acts as a token reader.

Note – The token reader is not used for normal Sun Ray services, so it does not need a keyboard, mouse, or monitor connected to it.

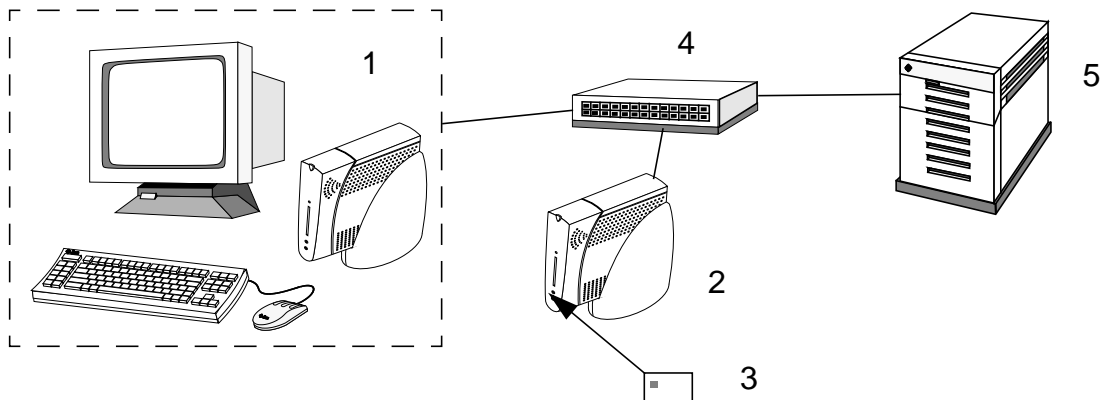


FIGURE 1-5 Using a Token Reader to Register Smart Cards

Legend:

1. Sun Ray appliance
2. Token reader appliance
3. Smart card
4. Switch
5. Server

Once the Sun Ray server software has been configured so that this extra appliance is designated as a token reader, you can configure the administration applications to read smart cards.

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

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

Users can be registered in two ways:

- Central Registration—You assign smart cards and/or appliances to authorized users and register users' tokens in the Sun Ray administration database.
- Self-Registration—Users register themselves in the Sun Ray administration database. If this mode is enabled and the Authentication Manager is presented with an unregistered token, the user is prompted with a registration window. The user provides information a site administrator would request.

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

Mobility—Hot Desking

Depending on the authentication policy selected, users can be *mobile* within the workgroup; that is, if a user starts a session on one appliance and moves to another, the session follows the user to the new appliance. In previous versions of the Sun Ray server software, mobile sessions were possible only with smart cards.

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 directly connect to the Sun Ray appliance. This can include audio, video, X servers, and device control of the appliance. For example, `dtmail` is not a service because it is accessed through an X server.

Session Manager

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

The steps below describe how the process starts and ends:

1. After a user's token is authenticated, the Authentication Manager determines if a session exists for the token. If 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 its policy. This usually involves starting an X server for the session.
2. When services are started, they explicitly join the session by contacting the Session Manager.
3. The Authentication Manager informs the Session Manager that the session associated with the token is to be connected to a specific Sun Ray appliance. The Session Manager then informs each service in the session that it should connect directly to the appliance.
4. The Authentication Manager determines that the session associated with a token should be disconnected from an appliance. The Authentication Manager notifies the Session Manager which, in turn, notifies all the services in the session to disconnect.
5. The Session Manager mediates control of the screen real-estate between competing services in a session and notifies the services of clip region changes.



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

Changes in a Session

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 an appliance (for example, when a card is removed), the Session Manager disconnects the services from the appliance but the services remain active on the server. For example, programs attached to the X server continue to run although their output is not visible.



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

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

If the Session Manager is disrupted, it automatically restarts. Each service contacts the Session Manager to request reattachment to a particular session.

Sun Ray Appliance Settings

Sun Ray Settings is an interactive GUI that allows the user to view and change the settings for the Sun Ray appliance that the user is currently logged into.

The Sun Ray Settings GUI contacts the Session Manager to determine which appliance 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 appliance by removing the smart card and inserting it into another appliance.

▼ To Change the Sun Ray Settings

1. Press the hot key (by default Shift-Props).

The Sun Ray Settings window is displayed. See FIGURE 1-6.

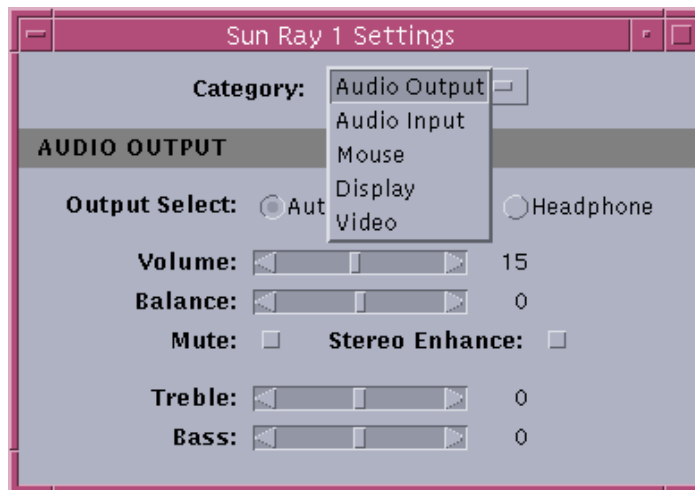


FIGURE 1-6 Settings Screen

2. Use the **Category pull-down menu** to access **Audio Output, Audio Input, Mouse, Display, and Video settings**.
3. To change a setting, move the appropriate scroll bar, checkbox, or pull-down menu.

The appliance 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 appliance.

4. Press the hot key to close the window.

Note – Only one instance of Sun Ray Settings runs in hot key mode per session.

Part 3—Security Considerations

Using switched network gear for the last link to the appliances makes it very difficult for a malicious PC user or network snooper at one of the network ports to obtain unauthorized information. Because switches only send packets 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 appliance is plugged directly into the wall jack, then it is virtually impossible to intercept the communications between the server and the appliance.

The Sun Ray system does not encrypt its communications. Anyone who gains access to the data has access to what is typed and displayed at each Sun Ray appliance.

Non-Smart Card Mobile Sessions

Configuring the Sun Ray server software 1.3 with non-smart card mobile (NSCM) sessions provides the benefits of Hot Desking without the use of smart cards. This chapter explains NSCM sessions and how to configure them.

This chapter contains the following sections:

- “NSCM Session” on page 15
- “NSCM and Failover Groups” on page 20
- “Configuring the Authentication Manager for NSCM Sessions” on page 22

NSCM Session

In an NSCM session, the user types a user name and password instead of inserting a smart card. The user types the `utdetach` command instead of removing the smart card.

Sun Ray Mobile Session Login Dialog Box

When the Sun Ray server software 1.3 is configured for NSCM sessions, the Sun Ray Mobile Session Login dialog box is displayed on the Sun Ray appliance. See FIGURE 2-1.

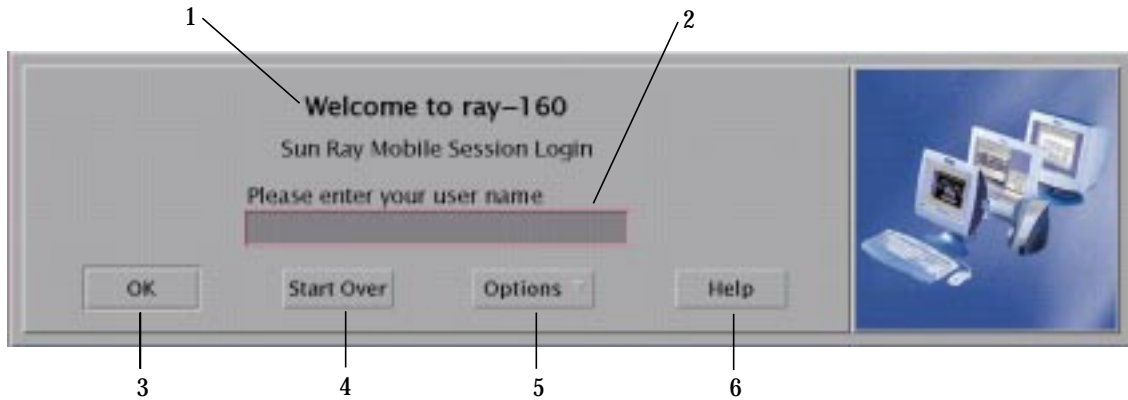


FIGURE 2-1 Sun Ray Mobile Session Login Dialog Box

Legend:

1. Sun Ray server hostname—The hostname of the Sun Ray server where the NSCM session is connected.
2. User entry field—The user types a user name and then a password into this field.
3. OK button—Clicking this button accepts the typed data.
4. Start Over button—Clicking this button clears and resets the dialog box.
5. Options button—Right clicking this button opens a panel where the user can select:
 - QuickLogin—Only used when creating a new session. Selecting Off enables the user to login with the same options available through `dtlogin`. Selecting On enables the user to bypass the option selection phase. QuickLogin is on by default.
 - Exit—Selecting Exit temporarily disables the NSCM session. A pseudo-token session is started, and the dialog box is replaced by the `dtlogin` screen. Users without a valid username for this server group can exit so as to make a remote login to a server where their user name is valid.
6. Help button—Clicking this button opens a pop-up window that provides information about the Sun Ray Mobile Session Login dialog box.

Note – If you don't want to use the NSC mobile session, insert a smart card. The NSCM session is disconnected and replaced by a smart card session.

▼ To Log In to an NSCM Session

1. Type a user name and then a password into the user entry field.

See FIGURE 2-2 and FIGURE 2-3.



FIGURE 2-2 User Name Entry



FIGURE 2-3 User Password Entry

2. If an NSCM session for this user does not exist:
 - a. The Authentication Manager creates an NSCM session token for the user.
The token has the following format:
`mobile.username`
where *username* is the user's identification.
 - b. Under the Solaris 2.6 and Solaris 7 operating environments, the `dtlogin` screen is displayed, and the user types a user name and password a second time.

c. If the Sun Ray server is configured to be part of a failover group, the load-balancing algorithm might redirect the user to another Sun Ray server where the user types a username and password again.

d. An NSCM session is created.

3. If an NSCM session exists on a different Sun Ray server in a failover group, the user is redirected to the server where the most current NSCM session is located.

The Sun Ray Mobile Session Login dialog box is redisplayed with the host name of the new Sun Ray server, and the user must retype the user name and password.

Note – The user is redirected either for server load balancing or because there is a disconnected session on another server. For added security, each redirection requires re-authentication, so the user must re-enter a user name and password. The Sun Ray administrator can prevent this re-authentication behavior by setting the `acceptRedirectToken` property in the `/etc/opt/SUNWut/auth.props` file to `true`. After restarting Sun Ray services, users do not need to re-authenticate when redirected.

4. If an NSCM session exists on the current Sun Ray server, the session is displayed to the user.

5. If a user wants to move to another location, there are two methods of disconnecting an NSCM session:

- Type the `utdetach` command in a shell window:

```
% /opt/SUNWut/bin/utdetach
```

- Press the Shift and Pause keys simultaneously.

The Sun Ray Mobile Session Login dialog box is redisplayed, and the user moves to another Sun Ray appliance.

6. Repeat Step 1 at the second Sun Ray appliance.

The session becomes active.

7. The user can terminate the session by clicking the Exit button in the CDE panel or by pressing the key combination `Ctrl+Alt+Bksp`, `Bksp`.

Note – In Step 5, the user may decide not to disconnect the session before moving to another Sun Ray appliance. Upon repeating Step 1, the user's session is disconnected from the previous appliance and connected to the current appliance.

Disconnecting an Active NSCM Session

There are two ways to disconnect an NSC mobile session:

- Hot Key combination
- `utdetach`

Hot Key

The NSC mobile session can also be disconnected by pressing the key combination Shift-Pause.

▼ To Disconnect the Current Session

The `utdetach` command enables the user to disconnect only the current NSCM session.

- **Type:**

```
% /opt/SUNWut/bin/utdetach
```

▼ To Terminate the Current Session

- **To terminate the current NSCM session, click the Exit button on the CDE panel.**

▼ To Create a `utdetach` Alias

You can create an alias for the `utdetach` command, such as `pause`, to make the command easier to use.

- **When executed as `superuser`, the following command line creates an alias for all users:**

```
# /usr/bin/ln -s /opt/SUNWut/bin/utdetach /usr/bin/alias
```

More information about the `utdetach` command is available in the `utdetach` man page.

▼ To Customize the Short Cut for Disconnecting an NSCM Session

You can disconnect the current session using the key combination (hot key) in the `/etc/opt/SUNWut/utslaunch.properties` file.

1. **To reconfigure the hot key combination, edit the file and find the line with the `utdetach.hotkey` property.**
2. **Change the string after the equals sign to the keystrokes desired.**

For example:

```
utdetach.hotkey=Alt Esc
```

configures the key combination of Alt-Esc.

More information about the `utdetach.hotkey` property is available in the `utslaunch.properties` man page.

▼ To Terminate the Current NSCM Session

- **Press the `Ctrl+Alt+Bksp+Bksp` key combination.**

The disconnect key combination (hot key) is changed by the Sun Ray administrator in the `/etc/opt/SUNWut/utslaunch_defaults.properties` file. This file is for site-wide default configuration of the hotkey key combination. Individual users can override the default key combination by configuring the `~/utslaunch.properties` file located in their home directory.

To reconfigure the hotkey key combination, edit the respective file and find the line with the `utdetach.hotkey` property. Change the string after the equals sign to the keystrokes desired. For example:

```
utdetach.hotkey=Alt Esc
```

configures the key combination of Alt + Esc.

More information about the `utdetach.hotkey` property is available in the `utlaunch.properties` man page.

NSCM and Failover Groups

The user's log in experience for NSCM sessions might be different than expected when logging into a system configured as a failover group.

The Sun Ray Authentication Manager uses a properties file:

`/etc/opt/SUNWut/auth.props`. When the system is initially configured, the `acceptRedirectToken` property in this file is set to `false`. This is done to support a model of high security by default. Because the property is set to `false`, unfamiliar behavior is seen in the following situations:

- Load Balancing Between Servers
- Connecting to Existing Sessions
- Switching Between Servers

■ Pseudo-Token Sessions

Note – The following behaviors are only experienced when the `acceptRedirectToken` property is set to `false`.

Load Balancing Between Servers

If a user logs into server A using the NSCM GUI but this server is heavily loaded, the user is redirected to server B. The user must log in again using the NSCM GUI. Because server B is running the Solaris 7 operating environment, the user enters a username and password a third time. The user gets a session, but it required three log ins. To disconnect from server B, the user types `utdetach`.

If the user is accustomed to smart card ease of use, the user might be confused by this repetitious behavior.

Connecting to Existing Sessions

A user's session exists on server B. The user returns to server A and logs in. Because the user's session is on server B, the user is redirected and must log in a second time using the NSCM GUI.

Unlike the simple task of inserting a smart card, NSCM sessions require the user to log in.

Switching Between Servers

The user is has a session on server A and wants to switch to a session on server B. The user invokes the `utselect` GUI to access the other session. In doing so, the user is required to log in using the NSCM GUI.

Users familiar with the ease of the `utselect` GUI might be discouraged that another log in is necessary.

Pseudo-Token Sessions

The user bypasses the NSCM GUI by clicking the Exit button and, using `dtlogin`, logs into server A. The user has a standard pseudo-token session. The user invokes the `utselect` GUI to switch to server B and, in doing so, is presented with the NSCM GUI. The user must click Exit again to get to the pseudo-token session on server B.

Users accustomed to a quick switch might be annoyed that they must interact with the NSCM GUI a second time.

Considerations

You, as the system administrator, must consider the options and consequences of increased security versus ease of use. If you wish to maintain a highly secure and regulated environment, set the `acceptRedirectToken` to `false`. If you want a more open and user friendly network, set the property to `true`.

Configuring the Authentication Manager for NSCM Sessions

The Authentication Manager in the Sun Ray server software 1.3 already has the code that provides NSCM sessions. The Sun Ray administrator has two methods of enabling the NSC mobile session feature:

- Sun Ray Administration Tool
- Command-line interface

▼ To Enable NSCM Sessions From the Administration Tool

1. **Before changing the Authentication Manager policy, inform your users that all active and detached sessions will be lost.**

You can use the `utwall` command to send the notice of policy change. For example:

```
# /opt/SUNWut/sbin/utwall -d -t 'System policy will change in 10
minutes.\nAll active and detached sessions will be lost.\nPlease
save all data and terminate your session now.' ALL
```

The following message is seen by all users in a pop-up window:

```
System policy will change in 10 minutes.
All active and detached sessions will be lost.
Please save all data and terminate your session now.
```

2. **Log in to the Administration Tool.**
3. **From the task list, select Admin and click the Policy link.**
The Change Policy window is displayed.
4. **In the Non-Card Users column, check the Enable Mobile Sessions box.**
See FIGURE 2-4.

Change Policy		Server: nomad-101
To change the Group Policy , select the desired settings and press Apply .		
<p>Card Users</p> <p><input type="checkbox"/> Controlled Access Mode</p> <p>Access:</p> <p><input type="radio"/> None</p> <p><input checked="" type="radio"/> All Users</p> <p><input type="radio"/> Registered Users</p> <p><input type="checkbox"/> Allow Self Registration</p> <p><input type="checkbox"/> Self Registration Requires Solaris Authentication</p>	<p>Non-Card Users</p> <p><input type="checkbox"/> Controlled Access Mode</p> <p><input checked="" type="checkbox"/> Enable Mobile Sessions</p> <p>Access:</p> <p><input type="radio"/> None</p> <p><input checked="" type="radio"/> All users</p> <p><input type="radio"/> Registered Users</p> <p><input type="checkbox"/> Allow Self Registration</p>	
Multihead feature enabled: <input type="radio"/> Yes <input checked="" type="radio"/> No		
<input type="button" value="Apply"/> <input type="button" value="Reset"/>		

FIGURE 2-4 Change Policy Window

5. Click the Apply button.

As the policy is being changed, you are shown a status window..

Change Policy		Server: nomad-100
Confirmation		
Policy change in progress, please wait		
1 of 2 hosts updated.		
nomad-100 : Succeeded		
nomad-101 : Incomplete		

FIGURE 2-5 Change Policy in Process Window

When the policy change is complete, you are shown a confirmation window

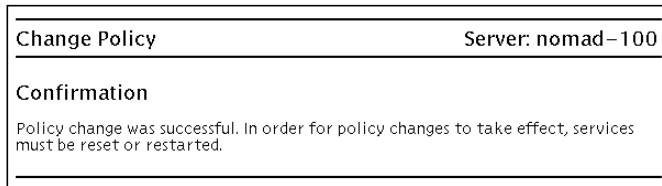


FIGURE 2-6 Change Policy Confirmation Window

- 6. From the task list, select Admin and click the Reset Services link.**
The Sun Ray Services panel is displayed.
- 7. Select Group if this is a failover group or Local if there is a single Sun Ray server.**
- 8. Click Restart to restart Sun Ray services and terminate all users' sessions.**
The NSC mobile sessions are enabled in a moment.

▼ To Enable NSCM Sessions From a Command Line

The Sun Ray administrator can toggle the NSCM session capability by including or excluding the `-M` argument in the `utpolicy` (or `utglpolicy` for failover groups) command. More information about the `utpolicy` and `utglpolicy` commands is available in the respective man pages.

- 1. Before changing the Authentication Manager policy, inform your users that all active and detached sessions will be lost.**

You can use the `utwall` command to provide them the notice of policy change. For example:

```
# /opt/SUNWut/sbin/utwall -d -t 'System policy will change in 10
minutes.\nAll active and detached sessions will be lost.\nPlease
save all data and terminate your session now.' ALL
```

The following message is seen by all users in a pop-up window:

```
System policy will change in 10 minutes.
All active and detached sessions will be lost.
Please save all data and terminate your session now.
```

2. **As superuser, type the `utpolicy` (`utglpolicy`) command for your authentication policy with the addition of the `-M` argument.**

For example:

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

This example configures the Authentication Manager to allow self-registration of users both with or without smart cards and NSC mobile sessions are enabled.

3. **Initialize Sun Ray services.**

- a. **Type this command to restart the Authentication Manager:**

This command clears all active and detached sessions.

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

- b. **Repeat Step a on each secondary Sun Ray server if in a failover group.**

Administration Tool

This chapter describes a standalone server. Failover is discussed in the *Sun Ray Server Software 1.3 Advanced Administration Guide*.

You can use the Administration Tool to administer Sun Ray users and appliances. This chapter is divided into the following sections:

- “Logging In” on page 28
- “Changing Policies” on page 31
- “Resetting and Restarting Sun Ray Services” on page 33
- “Token Readers” on page 34
- “Managing Desktops” on page 36
- “Multihead” on page 42
- “Viewing Failover Group Status” on page 44
- “Examining Log Files” on page 47
- “Managing Smart Cards From Different Vendors” on page 48
- “Sun Ray System Status” on page 53
- “Administering Users” on page 55
- “Controlled Access Mode” on page 63
- “Managing Sessions” on page 67
- “Accessing Online Documentation” on page 69

Administration Data

Sun Ray administration data comes from two sources: an internal database that keeps persistent administration data and the Authentication Manager, which is queried as needed for dynamic data. Sun Ray administration data is kept in its own

internal database that grants read access to all internal database clients but only allows changes by internal database clients that connect as the privileged `utadmin` user. Sun Ray administration data is accessible through standard database interfaces and applications.

Note – To avoid operational errors, only modify data using the Administration Tool.

Logging In

The Administration Tool allows you to administer your Sun Ray users and appliances from a Web browser.

This section includes the following procedures:

- “To Log Into the Administration Tool” on page 28
- “To Change the Administrator’s Password” on page 30
- “To Change the Policy” on page 31

▼ To Log Into the Administration Tool

1. **Log in to your Sun Ray server’s console or any appliance attached to it.**
2. **Start a browser.**
3. **Type the following URL:**

`http://hostname:1660`

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

The Login window is displayed.



FIGURE 3-1 Login Window

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

- You are running a browser on the Sun Ray server or one of its appliances.
 - The browser is not using a different machine as an HTTP proxy server to proxy the connection to the Web server.
4. **Enter the administrator user name `admin` and the administration password you specified when you configured the Sun Ray server software.**

For information on configuring the Sun Ray server software, see *Sun Ray Server Software 1.3 Installation Guide*.

Note – Only `admin` can be entered in the User text box.

5. **Click the Log In button.**

The Summary Status window is displayed. See FIGURE 3-2.

The navigation bar to the left of the window allows you to navigate through the Administration Tool.

Note – Due to security considerations, if the session is inactive for 30 minutes, you must log in again.



FIGURE 3-2 Summary Status Window

▼ To Change the Administrator's Password

The password allows you to use the Administration Tool to access and change Sun Ray administration data.

1. In the navigation menu, click the arrow to the left of Admin to view the options.
2. Click the Password link.

The Change Admin Password window is displayed.

Change Admin Password Server: nomad-100

Current password:

New password:

Reenter new password:

FIGURE 3-3 Change Admin Password Window

3. Enter your current password.

4. Enter a new password.
5. Re-enter the new password.

Note – If you make a mistake, click the Reset Fields button to clear the fields and start again.

6. Click the Change button.

The new password takes affect and the internal database hierarchy is updated.

Changing Policies

Changing policies involves changing the policy scope. The scope is either local or group (default). For a normal configuration (Group), which is discussed in the *Sun Ray Server Software 1.3 Advanced Administrator's Guide*, all policies are the same on all Sun Ray servers. If you need to override the default setting, choose the local setting. The local setting binds the policy to the current Sun server and is not applied to other Sun Ray servers.

Note – Set the same policies on all of the Sun Ray servers in the same failover group. For example, if all of the servers are configured to use the same policies and a failover occurs, all policies remain consistent.

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

▼ To Change the Policy

1. Select the arrow to the left of Admin in the navigation bar to expand the menu.
2. Click the Policy link.

The Change Policy window is displayed (see FIGURE 3-4).

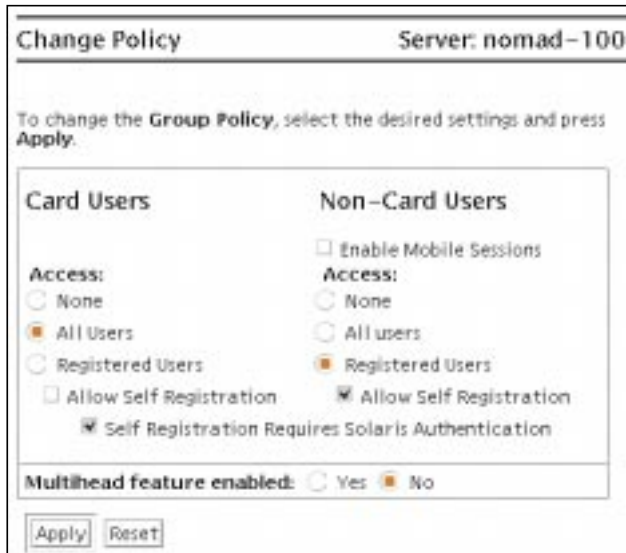


FIGURE 3-4 Change Policy Window

3. Under Card Users, select None, All Users, or Registered Users.

4. Under Access, select either None, All Users, or Registered Users.

Registered users are those registered by you. Selecting Allow Self Registration includes users who are prompted to self-register when they inserted their card. All Users encompasses all types of users.

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

6. To enable multihead, click the Yes radio button next to Multihead feature enabled.

For additional information on Multihead, see the *Sun Ray Server Software 1.3 Advanced Administrator's Guide*.

7. Notify users to log off.

If users do not log off and you restart, user sessions can be lost.

8. Restart services.

When changing the Multihead feature only, you can reset Sun Ray services. All other changes require restarting Sun Ray services.

Resetting and Restarting Sun Ray Services

▼ To Reset Sun Ray Services

If policy changes have been made, reset services to implement those changes.

1. **From the expanded navigation menu under Admin, click the Reset Services link.**

The Sun Ray Services window is displayed. See FIGURE 3-5.

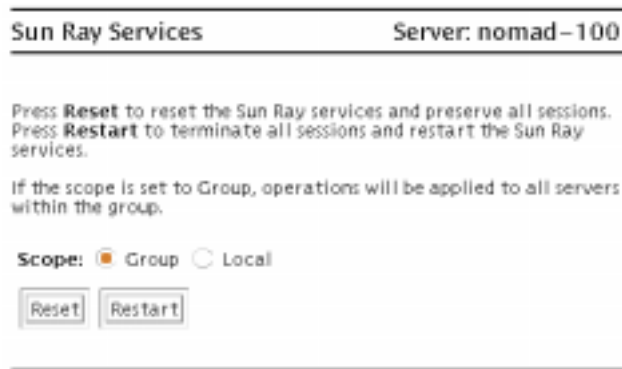


FIGURE 3-5 Sun Ray Services Window

2. **Click Reset.**

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

▼ To Restart Sun Ray Services

- **To restart Sun Ray Services, click Restart.**

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

Token Readers

Using the Administration Tool you can create token readers and can locate Sun Ray appliances designated as token readers.

Creating a Token Reader

A token reader is a Sun Ray appliance that reads a smart card and returns the ID, allowing you to add a user.

▼ To Create a Token Reader

- 1. Click the arrow in front of Desktops to expand the navigation menu.**
- 2. Click the View Current link.**
- 3. Select the desktop of the appliance you want to use as a token reader.**
The Current Properties window is displayed.
- 4. Click the Edit Properties button.**
The Edit Desktop Properties window is displayed.

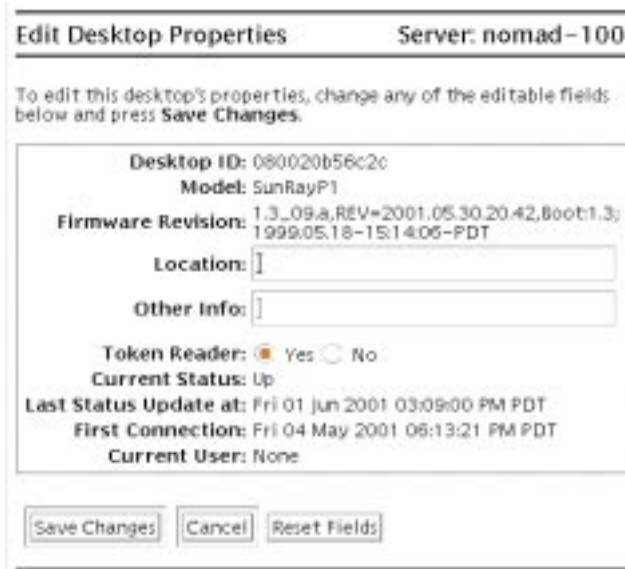


FIGURE 3-6 Edit Desktop Properties Window

5. Next to **Token Reader**, select the radio button **Yes**.
6. Click the **Save Changes** button.

The appliance you have selected now reads smart cards.

▼ To Locate Token Readers

- From the expanded navigation menu under **Admin**, click the **Token Readers** link. The Token Readers window is displayed. In FIGURE 3-7 only one Sun Ray appliance is listed as a token reader. If more than one page of information is displayed, use the following links to navigate:
 - Previous—returns to the previous page
 - Next—goes to the next page of data
 - Home—returns to first page

Token Readers		Server: nomad-100		
Desktop ID	Server	Location	Other Info	Current User
080020b56c2c	nomad-101			

FIGURE 3-7 Token Readers Window

Managing Desktops

This section includes the following procedures:

- “To List All Desktops” on page 36
- “To Display a Desktop’s Current Properties” on page 37
- “To List Currently Connected Desktops” on page 38
- “To View the Properties of the Current User” on page 39
- “To Search for Desktops” on page 40
- “To Edit a Single Desktop’s Properties” on page 41

▼ To List All Desktops

1. In the navigation menu, click the directional arrow to the left of Desktops to view the options.
2. To view all desktops, click View all.

The View All Desktops window is displayed. This window contains the complete list of desktops in the administration database.

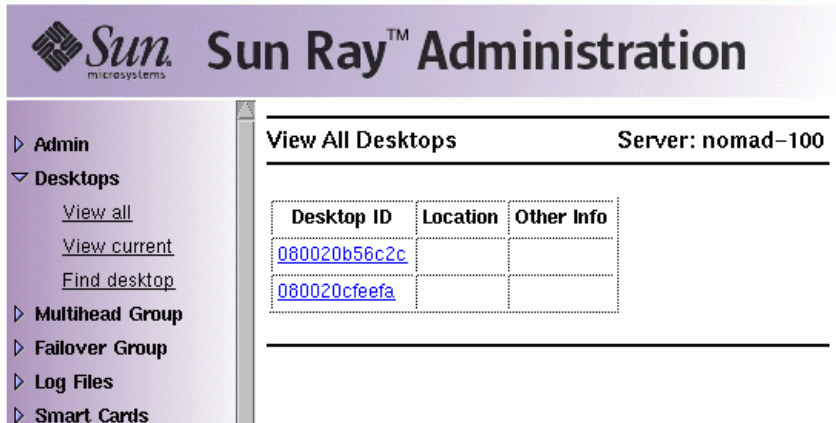


FIGURE 3-8 View All Desktops Window

3. Use the navigation buttons at the bottom of the page to view additional pages of results.

Each page lists up to 20 desktops.

▼ To Display a Desktop's Current Properties

1. Click a Desktop ID link.

The Desktops Current Properties window is displayed.



FIGURE 3-9 Desktops Current Properties Window

The page shows information about the appliance (desktop) as obtained from the administration database and the Authentication Manager.

▼ To List Currently Connected Desktops

1. In the navigation menu, click the directional arrow to the left of Desktops to view the options.
2. Click View current.

The View Current Desktops window is displayed, listing only the desktops that are currently connected to this Sun Ray server and communicating with the Authentication Manager or any other Sun Ray server in the same failover group.

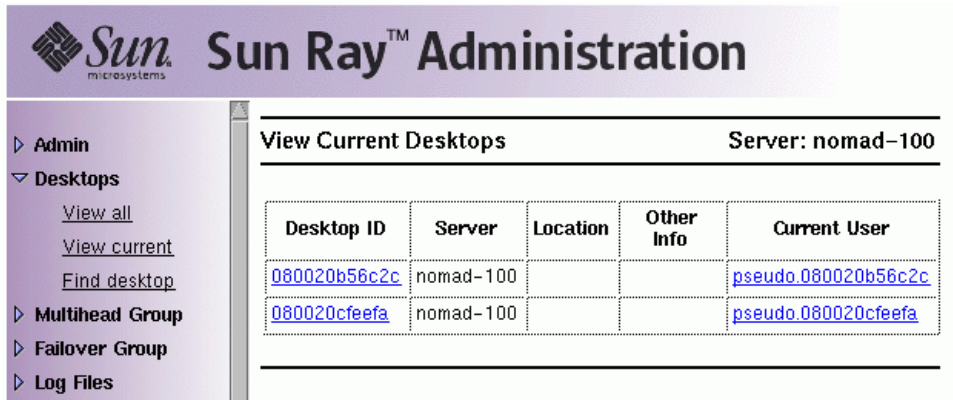


FIGURE 3-10 View Current Desktops Window

▼ To View the Properties of the Current User

- From either the View Current User window or the Desktops Current Properties window, click the link for Current User.

The Properties window for the Current User is displayed.



FIGURE 3-11 Properties Page for the Current User

▼ To Search for Desktops

1. In the navigation menu, click the directional arrow to the left of Desktops to view the options.
2. Click Find desktop.

The Find Desktop window is displayed.

The screenshot shows the Sun Ray Administration interface. The top header features the Sun Microsystems logo and the text "Sun Ray™ Administration". On the left, a navigation menu is visible with the following items: Admin, Desktops (expanded), Multihead Group, Failover Group, Log Files, Smart Cards, Status, and Users. Under the "Desktops" section, there are three links: "View all", "View current", and "Find desktop". The main content area is titled "Find Desktop" and displays "Server: nomad-100". Below this, there is a search criteria section: "Search for All Desktops that Contain:". This section includes three input fields: "Desktop ID:", "Location:", and "Other Info:". Each field is followed by the word "and". At the bottom of the search section, there are two buttons: "Search" and "Reset Fields".

FIGURE 3-12 Find Desktop Window

3. From the Find Desktop page, enter data into the Desktop ID, Location, and Other Info fields.
4. Click the Search button.

The Find Desktop window is redisplayed with all matches in the administration database.

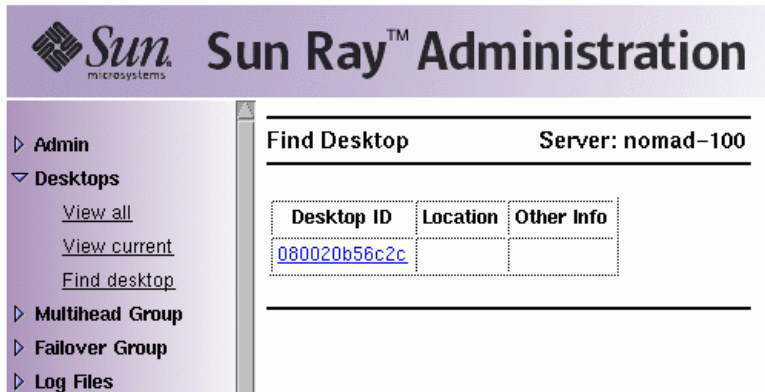


FIGURE 3-13 Find Desktop Search Results Window

▼ To Edit a Single Desktop's Properties

1. **To display the Desktop Properties page for the desktop you want to edit, click the Desktop ID.**

The Desktops Current Properties window is displayed.

2. **Click the Edit Properties button.**

The Edit Desktop Properties window is displayed. See FIGURE 3-14.



FIGURE 3-14 Edit Desktop Properties Window

3. Change the data in the text boxes as appropriate.
4. Click the Save Changes button to save the changes to the administration database.

Multihead

For further information on multihead, see the *Sun Ray Server Software 1.3 Advanced Administrator's Guide*.

The multihead feature on Sun Ray appliances allows users to control separate applications on multiple screens using a single keyboard and pointer device attached to the primary appliance. Users can also display and control a single application, such as a spreadsheet, on multiple screens. System administrators create multihead groups that may be accessed by users. A multihead group, consisting of two or more appliances controlled by one keyboard and mouse, can consist of Sun Ray 1, Sun Ray 100, and Sun Ray 150 appliances.

▼ To View All Multihead Groups

1. From the navigation menu, select the arrow to the left of Multihead Group to expand the menu.
2. Click the View All link.

The Multihead Groups window is displayed. See FIGURE 3-15.



FIGURE 3-15 The Multihead Groups Window

3. To view the properties for this group, click the Multihead Group Name link.

The Multihead Group Properties window is displayed. See FIGURE 3-16.

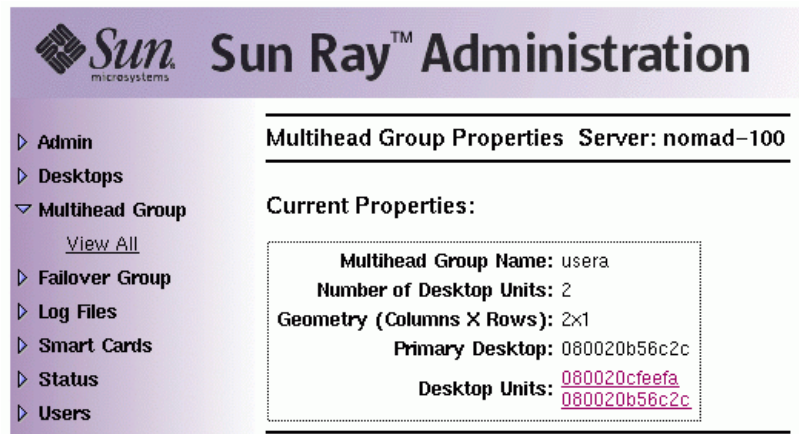


FIGURE 3-16 The Multihead Group Properties Window

4. To display the Desktops Current Properties for the appliances that are part of this group, click the Desktop Units links.

The Desktops Current Properties window for the link selected is displayed. See FIGURE 3-17.

Desktops	Server: nomad-100
-----------------	--------------------------

Current Properties:

Desktop ID:080020cfeefa
Model:SunRayP3
Firmware1.3_06.a,REV=2001.04.17.19.55,Boot:1.4;
Revision:2000.05.11-16:42:52-PDT
Multihead
Group name:[usera](#)
Location:
Enabled?:no value
Other Info:

Token Reader:No
Current Status:Up
Last Status
Update at:Mon 23 Apr 2001 03:06:18 PM PDT
First
Connection:Wed 18 Apr 2001 11:09:08 AM PDT
Current User:[IEEE802.080020cfeefa](#)

FIGURE 3-17 Desktops Current Properties Window for a Member of the Usera Multihead Group

The Multihead Group name is displayed as a property of this desktop.

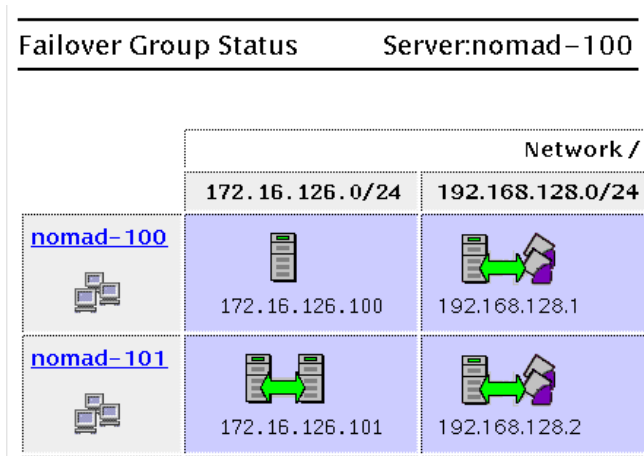
Viewing Failover Group Status

A failover group is a set of Sun Ray servers all running the same release of the Sun Ray server software and all having access to all the Sun Ray appliances on the interconnect.

▼ To View Failover Group Status

1. From the navigation menu, select the arrow to the left of **Failover Group** to expand the menu.
2. Click the **Status** link.

The Failover Group Status window is displayed. See FIGURE 3-18.



The screenshot shows a window titled "Failover Group Status" for "Server: nomad-100". It contains a table with the following structure:





	Network / IP	
	172.16.126.0/24	192.168.128.0/24
nomad-100	 172.16.126.100	 192.168.128.1
nomad-101	 172.16.126.101	 192.168.128.2

FIGURE 3-18 Failover Group Status Table

The Failover Group Status window describes the health and current state of multiple Sun Ray servers within your failover group. This window also describes the health of any Sun Ray servers that have responded to a Sun Ray broadcast.







The Failover Group Status window provides information on group membership and network connectivity. The servers are listed by name in the first column. Failover Group Status only displays public networks and Sun Ray interconnect fabrics.

In FIGURE 3-18 the information provided is from the point of view of the server in the upper left hand of the table. In this example the server is nomad-100.

Note – Sun Ray server broadcasts do not traverse over routers or servers other than Sun Ray servers.

Sun Ray Failover Group Status Icons

TABLE 3-1 Status Icons

Icons	Description
	It indicates that the displayed information is from the perspective of the system performing the Failover status.
	A failover group is established and functioning properly. The trusted hosts are members of this failover group because they share the same group signature.
	A Sun Ray interconnect fabric is established and functioning properly.
	This Sun Ray interconnect fabric is unreachable from the server performing the Failover Group Status. This may indicate a failure in the interconnect fabric between Sun Ray servers if they are supposed to be on the same interconnect. In the past, this host was reachable but is no longer from the point of view of the system performing failover status.
	The servers are unreachable. This network is unreachable from the server performing the Failover Group Status. This could be an alert situation. Over a public network the conditions could be normal, except for the Sun Ray broadcast information, which cannot traverse over routers.
	Servers that appear in the same group use this icon. The signature files, <code>/etc/opt/SUNWut/gmSignature</code> , on those two machines are identical. This icon identifies systems as trusted hosts. Failover occurs for any Sun Ray appliances connected between these systems. The <code>utgroupsig</code> utility is used to set the <code>gmSignature</code> file. Refer to the <i>Sun Ray Server Software 1.3 Advanced Administrator's Guide</i> for information regarding the <code>gmSignature</code> file and <code>utgroupsig</code> utility.

For further information on failover, see the Failover chapter in the *Sun Ray Server Software 1.3 Advanced Administrator's Guide*.

Examining Log Files

Significant activity concerning files retrieved from the Sun Ray server is recorded. The server stores this information in text files. TABLE 3-2 describes the log files that are maintained.

TABLE 3-2 Log Files

Log File	Path	Description
Messages	<code>/var/opt/SUNWut/log/messages</code>	Lists events from the server's appliances, including details of registering, inserting, or removing smart cards. This file is updated daily, and archived files are stored on the server for one week and are annotated using numeric extensions (for example, from <code>messages.0</code> to <code>messages.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>).
Administration	<code>/var/opt/SUNWut/log/admin_log</code>	Lists operations performed when administering the server. This log is updated daily. Archived files which are stored on the system for up to one week are annotated using numeric extensions (for example, from filename <code>admin_log.0</code> to <code>admin_log.5</code>).

▼ To View a Log File

1. From the navigation menu, select the arrow to the left of Log Files to expand the menu.
2. Click the Log link.

The Log File window is displayed. See FIGURE 3-19. Use the scroll bar to access data to the right and bottom of the window.



FIGURE 3-19 Log File Window

Managing Smart Cards From Different Vendors

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; for example, `acme_card.cfg`.

For certain vendors, the smart card might require additional software to enable the Sun Ray server software to probe for it. If required, this optional software must be supplied as Java classes in a Jar file. This file must end with a `.jar` suffix and must have the same pre-suffix filename as the `.cfg` file that contains its configuration information.

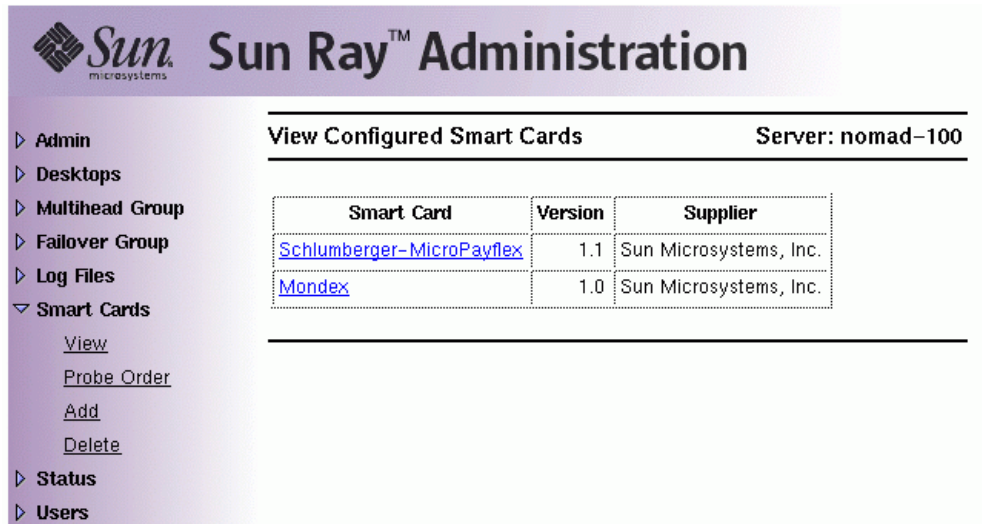
This section contains the following procedures:

- “To View or List Configured Smart Cards” on page 49
- “To View The Smart Card Probe Order” on page 50
- “To Change the Smart Card Probe Order” on page 51
- “To Add a Smart Card” on page 51
- “To Delete a Smart Card” on page 52

▼ To View or List Configured Smart Cards

1. From the navigation menu, select the arrow to the left of Smart Cards to extend the menu.
2. Click the View link.

The View Configured Smart Cards window is displayed with the smart cards listed in alphabetical order (see FIGURE 3-20).



The screenshot shows the Sun Ray Administration interface. The title bar reads "Sun Ray™ Administration" with the Sun Microsystems logo. The navigation menu on the left is expanded to show "Smart Cards" with sub-options: "View", "Probe Order", "Add", and "Delete". The main content area is titled "View Configured Smart Cards" and "Server: nomad-100". Below this is a table with the following data:

Smart Card	Version	Supplier
Schlumberger-MicroPayflex	1.1	Sun Microsystems, Inc.
Mondex	1.0	Sun Microsystems, Inc.

FIGURE 3-20 The View Configured Smart Cards Window

From this window an administrator can see the current list of smart cards in alphabetical order, the smart card supplier, and version number.

3. From the the View Configured Smart Cards window, select the link for the smart card.

The main properties for the selected smart card are displayed in FIGURE 3-21.

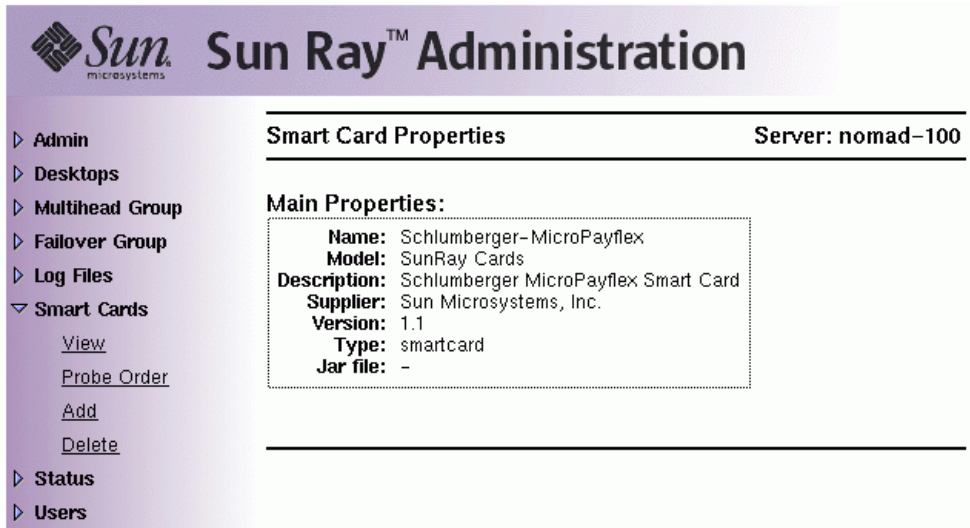


FIGURE 3-21 Smart Card Properties Window

▼ To View The Smart Card Probe Order

- From the navigation menu under Smart Cards, click the Probe Order link. The Smart Card Probe Order window is displayed.



FIGURE 3-22 Smart Card Probe Order Window

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

▼ To Change the Smart Card Probe Order

- **Select a smart card and press the appropriate up and down button.**

Clicking on the first and last (from top to bottom) buttons moves the selected card to either the top or bottom of the list.

▼ To Add a Smart Card

1. **From the expanded navigation menu under Smart Cards click the Add link.**

The Add Smart Cards to Probe List window is displayed. See FIGURE 3-23.

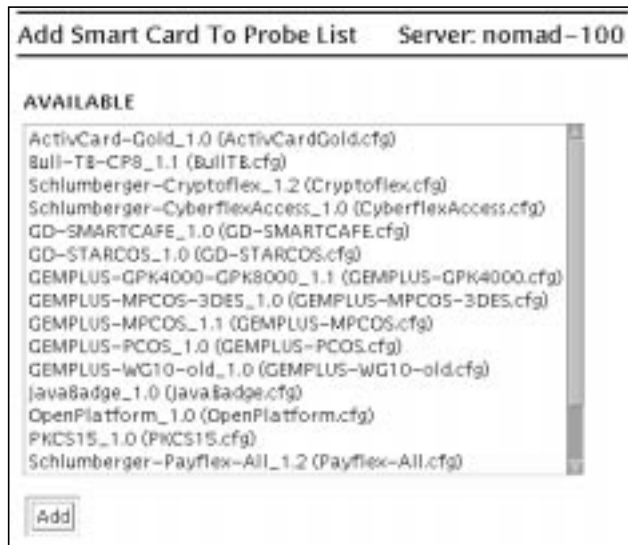


FIGURE 3-23 Add Smart Card to Probe List Window

2. **Select a smart card and click the Add button.**

▼ To Delete a Smart Card

1. **From the expanded navigation menu under Smart Cards, click the Delete link.**
The Delete Smart Card From Probe List window is displayed (see FIGURE 3-24).



FIGURE 3-24 Delete Smart Card From Probe List Window

2. **Select a smart card.**
3. **Click the Delete button.**

Sun Ray System Status

▼ To View the Sun Ray System Status

1. Click the directional arrow to the left of Status to expand the navigation menu.
2. Click the Summary Status link.

The Summary Status window is displayed. See FIGURE 3-25.

Sun Ray Administration Server: nomad-100

Summary Status

Desktop Summary Status				User Summary Status	
Units Connected:			0	Users in database:	0
Units Disconnected:			2	Users logged in:	0
Token card readers:			1	Enabled cards:	0
System Information				Disabled cards:	0
Description	kbytes	Used	Available	Users logged in with cards:	0
Root File System	288556	58934	229622	Users logged in without cards:	0
Swap Space	527544	32	527512		

Refresh

FIGURE 3-25 Summary Status Window

TABLE 3-3 Summary Status Field Descriptions

Options	Description
Desktop Summary Status	
Units Connected	Number of Sun Ray appliances currently active or available on the interconnect fabric.
Units Disconnected	Number of Sun Ray appliances no longer available.
Token card readers	Number of Sun Ray appliances designated as token card readers attached to the interconnect fabric.
User Summary Status	
Users in database	Number of Sun Ray users in the internal database.
Users logged in	Number of Sun Ray users logged in to the system.
Enabled cards	Number of enabled smart cards.
Disabled cards	Number of disabled smart cards.
Users logged in with cards	Number of Sun Ray users logged in with smart cards or using non-smart card mobility.
Users logged in without cards	Number of Sun Ray users logged in using a pseudo token.
System Information	
Root File System	Total, used, and available disk space available for the Sun Ray server.
Swap Space	Total, used, and available swap space available for the Sun Ray server.

Administering Users

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

TABLE 3-4 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 appliances, this is the type "pseudo" and the appliance's Ethernet address. Examples: mondex.9998007668077709 pseudo.080020861234
Server Name	Name of the Sun Ray server that the user is using.
Server Port	Sun Ray server's communication port. This field should generally be set to 7007.
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.

This section includes the following procedures:

- "To View Users by ID" on page 56
- "To View Users by Name" on page 56
- "To Delete a User" on page 56
- "To View Current Users" on page 57
- "To Display a User's Current Properties" on page 57
- "To Edit a User's Properties" on page 59
- "To Add a Token ID to a User's Properties" on page 60
- "To Delete a Token ID From a User's Properties" on page 60
- "To Enable or Disable a User's Token" on page 60
- "To Add a User" on page 61
- "To Find a User" on page 62
- "To Get a Token ID From a Token Reader" on page 62

▼ To View Users by ID

- From the expanded Users navigation menu, click the View by ID link.

The View Users by ID window is displayed. See FIGURE 3-26. The list of all the users in the administration database is sorted by the Token ID field. If a user has multiple tokens, they are listed separately.




Token ID	Server	Port	User Name	Other Info
MicroPayflex.00005d9565000100	localhost	7007	test1	

FIGURE 3-26 View Users by ID Window

▼ To View Users by Name

- From the the expanded Users navigation menu, click the View by name link.

The View Users by Name window is displayed, listing all the users in the administration database sorted by the User Name field. If a user has multiple tokens, they are grouped together with the name. See FIGURE 3-27.



User Name	Token ID(s)	Server	Port	Other Info
test1	MicroPayflex.00005d9565000100	localhost	7007	

FIGURE 3-27 View Users by Name Window

▼ To Delete a User

Caution – This operation deletes the user and all associated tokens.

1. From the View by name window, click the name for the user you want to delete.
2. Press the Delete This User button.

The Delete User page is displayed.



FIGURE 3-28 Delete User Window

3. To proceed with deleting the user, press the YES - Delete User Now button.

To cancel this delete operation, press the NO - Cancel Delete button.

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

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

▼ To View Current Users

- From the expanded navigation menu under Users, click the View current link.

The View Current Users window is displayed, listing only the registered users that are currently logged into an appliance connected to this Sun Ray server.

View Current Users		Server: nomad-100		
Token ID	User Name	Server	Desktop ID	Desktop Location
cstudio.080020b56c2c	???	nomad-101	080020b56c2c	???
cstudio.080020cfeefa	???	nomad-100	080020cfeefa	???

FIGURE 3-29 View Current Users Window

▼ To Display a User's Current Properties

- Click on the Token ID or User Name hyperlink for the user.

The Current Properties page for the user is displayed. See FIGURE 3-30.

Current Properties:

User Name: test1
 Other Info:
 Server Name: localhost
 Server Port: 7007
 User Created: Mon 04 Jun 2001 11:42:17 AM PDT

Token ID	Enabled?
MicroPayflex,00005d9565000100	Yes

Currently Logged In:

Current Desktop: 080020b0ed1f
 Desktop Location:
 Logged In Since: Tue 05 Jun 2001 01:47:53 AM PDT

FIGURE 3-30 User's Current Properties Page

FIGURE 3-30 displays the user's information contained in the administration database. Information about the user's current login status is displayed. The possible states are:

- Never Logged In
- Currently Logged In
- Logged Off

For the last two states, the following fields are also displayed:

TABLE 3-5 Login Status Fields

Option	Description
Current Desktop/ Last Desktop	Current/last appliance (desktop) the user is or was logged in to.
Desktop Location	Location of the appliance (desktop).
Logged In Since/ Logged Off At	Date and time the user logged in or off the appliance (desktop).

▼ To View the User's Sessions

- If the user is currently logged in, the user's session can be viewed by clicking the **View This User's Session** button.

The Sessions for User window is displayed.

▼ To Edit a User's Properties

1. From the user's **Current Properties** page, press the **Edit Properties** button.

The Edit User Properties page is displayed.

Edit User Properties Server: springcreek

To add a Token ID to this user, select a token reader and press **Get Token ID** below to fill in the new token ID field. Then, make any other changes and press **Save Changes**.

User Name: test1
Other Info:
Server Name: localhost
Server Port: 7007
User Created: Mon 04 Jun 2001 11:42:17 AM PDT

Token ID	Enabled?	
MicroPayflex.00005d9565000100	<input checked="" type="checkbox"/>	<input type="checkbox"/> Remove
	<input type="checkbox"/>	<input type="checkbox"/> Add

Token Reader: (None Available)

FIGURE 3-31 Edit User Properties Page

2. Make changes to any of the text boxes.

You can also add or remove tokens from a user at the same time.

3. When finished, press the **Save Changes** button.

The changes are saved to the administration database.

▼ To Add a Token ID to a User's Properties

1. **From the Edit User Properties page, type the new Token ID into the empty Token ID text field.**
2. **If you do not know the new Token ID and have configured a token reader:**
 - a. **Insert the user's new card into the selected token reader.**
 - b. **Choose the selected token reader from the pull-down menu of available readers.**
 - c. **Press the Get Token ID button.**

The application queries the token reader and, if successful, redisplay the form with the Token ID text field filled out.
3. **Check the Enabled checkbox next to the new Token ID.**
4. **Check the Add checkbox next to the new Token ID.**

You can also make any other edits to the user at the same time.
5. **Press the Save Changes button.**

The changes are then added to the administration database.

▼ To Delete a Token ID From a User's Properties

1. **From the Edit User Properties page, check the Remove checkbox for any Token IDs you want to remove.**
2. **Press the Save Changes button.**

The changes are then added to the administration database.

▼ To Enable or Disable a User's Token

1. **From the Edit User Properties page, check the Enabled checkbox for any Token IDs you want to enable.**
2. **Uncheck the Enabled checkbox for any Token IDs you want to disable.**
3. **Press the Save Changes button.**

The changes are saved to the administration database.

▼ To Add a User

1. From the expanded menu under Users, click the Add user link.

The Add User window is displayed.

Add User Server: nomad-100

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

Token Reader: 080020b56c2c

Token ID:

Server Name: localhost

Server Port: 7007

User Name:

Other Info:

FIGURE 3-32 Add User Window

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

- a. Insert the user's new card into the selected token reader.
- b. Choose the selected token reader from the pull-down menu of available readers.
- c. Press the Get Token ID button.

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

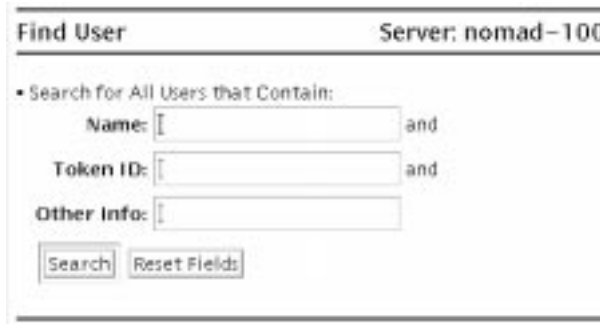
3. Enter data in the required fields.

4. Press the Add User button.

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

▼ To Find a User

1. **From the expanded menu under Users, click the Find link.**
The Find User window is displayed.



Find User Server: nomad-100

• Search for All Users that Contain:

Name: and

Token ID: and

Other Info:

FIGURE 3-33 Find User Window

2. **Enter data in the required fields.**
3. **Press the Search button.**

▼ To Get a Token ID From a Token Reader

1. **From the expanded Users menu, click the Get token ID link.**
The Get Token ID window is displayed.



Get Token ID Server: nomad-100

To get a token's ID, select a reader from the pull-down list below, insert the token in that reader and press **Get Token ID**.

Token Reader:

Token ID:

FIGURE 3-34 Get Token ID Window

2. **Insert the new card into the selected token reader.**
3. **Choose the selected token reader from the pull-down menu of available readers.**

4. Press the Get Token ID button.

The application queries the token reader and redisplay the page with the Token ID field filled out.

Controlled Access Mode

For more information on controlled access mode, see the *Sun Ray Server Software 1.3 Advanced Administration Guide*.

▼ To Configure Controlled Access Mode

1. Select the arrow to the left of Controlled Access Mode to expand the navigation menu.

The Controlled Browser menu item is displayed only if the Controlled Browser package is installed. See the *Sun Ray Server Software 1.3 Installation Guide*.

2. Click the Controlled Access Mode link.

The Controlled Access Mode Configuration Window is displayed. See FIGURE 3-35.

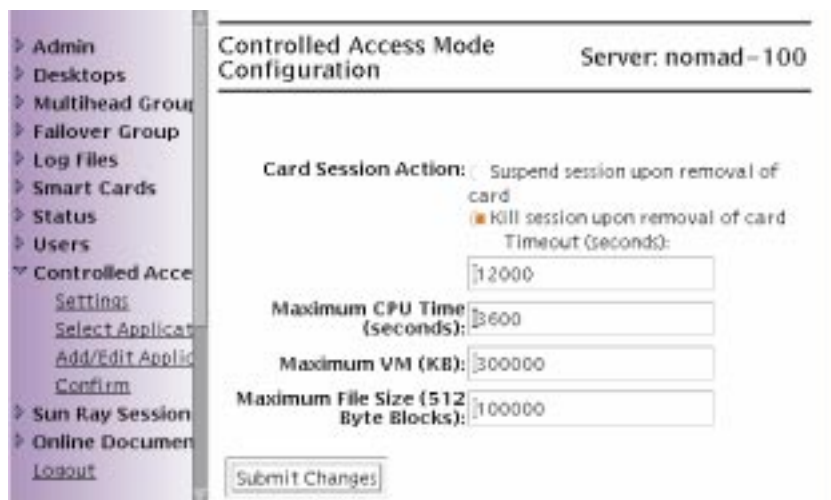


FIGURE 3-35 Controlled Access Mode Configuration Window

From this window the administrator can determine the length of session timeout under Kill session upon removal of card if selected.

3. Click the Submit Changes button.

Note – You must confirm by using the link in the navigation bar before activating any changes.

▼ To Select Additional Applications

- 1. Select the arrow to the left of Controlled Access Mode to expand the navigation menu.**
- 2. Click the Select Applications link.**

The Select Additional Applications Window is displayed. See FIGURE 3-36.

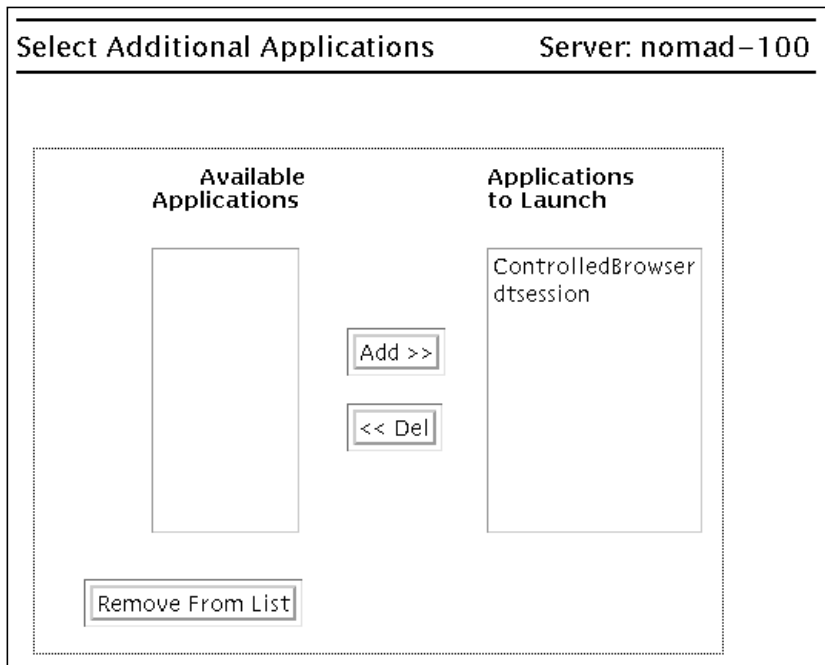


FIGURE 3-36 Select Additional Applications Window

From this window the administrator can configure browser behavior, home page, and proxy to work in the Controlled Access Mode.

- 3. Highlight the applications in the Available Applications scroll box.**

4. Click the Add button.

The application moves to the Applications to Launch scroll box. An application must be in the Applications to Launch box to be executable.

5. To delete an application, follow this process in reverse by selecting an application in the Applications to Launch scroll box and clicking the Del button.

The application moves to the Available Applications scroll box.

6. The remove an application from the list of available applications, click the Remove From List button.

7. Click the Confirm link.

▼ To Add or Edit Applications

1. Select the arrow to the left of Controlled Access Mode to expand the navigation menu.

2. Click the Add/Edit Applications link.

The Add/Edit Apps Window is displayed. See FIGURE 3-37.

The screenshot shows a window titled "Add/Edit Apps" with "Server: nomad-100" in the top right corner. On the left, under "All Available Applications", there is a scroll box containing "ControlledBrowser dtsession" and an "Edit >>" button. On the right, there are three input fields: "Application Profile Name:", "Application Menu Label:", and "Path of Application:". Below these is a "Set Attribute:" section with three radio button options: "critical (automatically launch and restart session on exit)", "menu (launch from menu only)", and "default (launch automatically and in menu, but don't restart on exit)". At the bottom, there are three buttons: "Add New", "Update", and "Reset".

FIGURE 3-37 Add/Edit Apps Window

Applications can be edited or added from this window.

Note – If you are adding a new application, the Reset button clears the fields. If you are updating an existing application, the Reset button resets the fields to the original configuration.

3. To edit an application, highlight the application in the All Available Applications scroll box.

4. Click the Edit button.

The information for the application is displayed in the text fields.

5. When you have edited the text fields and selected the radio button for your preferred launch attribute, click the Update button.

6. To add an application, fill in the text fields.

7. Click the Add New button.

8. To confirm the new application configuration, click the Confirm link in the expanded navigation menu under Controlled Access Mode.

The Confirmation window is displayed. See FIGURE 3-38.



FIGURE 3-38 Confirmation Window

9. Click the Confirm Configuration button.

Managing Sessions

A Sun Ray session is created when the user logs in to a Sun Ray appliance. A Sun Ray session has three possible states as shown in TABLE 3-6.

TABLE 3-6 Sun Ray Session States

State	Description
Connected/disconnected	A session is currently displayed on an appliance.
Idling	The session is waiting at the Solaris login prompt.
Running/suspended	The session is running unless the startup process and its descendents are stopped.

▼ To View Sun Ray Sessions

1. From the navigation menu, click the expansion arrow for Sun Ray Sessions.
2. From the expanded navigation menu, click the View by Server link.

The Search User Sessions by Server window is displayed. See FIGURE 3-39.

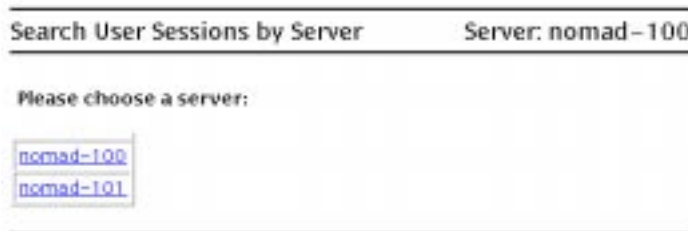


FIGURE 3-39 Search User Sessions by Server Window

3. Click the server link.

The current running sessions for that server are displayed. See FIGURE 3-40.

Sessions on Sun Ray Server: nomad-100					Server: nomad-100
Wed 06 Jun 2001 04:55:15 PM PDT					
Running Sessions:					
Token ID	User Name	Unix ID	Connection	Display No	Action
pseudo.080020cfeefa	???	???	Connect	2	None ▾
<input type="button" value="Apply"/> <input type="button" value="Reset"/>					

FIGURE 3-40 Current Running Sessions Window

- To change the state of any of the displayed sessions, use the Action pull-down menu button to display your choices.**

There are three possible actions: None, Terminate, and Suspend.

- To apply your changes, click the Apply button.**

Click the Reload button to update, and click the Back button in the browser to go back to the previous page.

▼ To Find Sun Ray Sessions

- From the expanded navigation menu, click the Find Sun Ray Sessions link.**

The Find Sun Ray Sessions window is displayed. See FIGURE 3-41.

Find Sun Ray Sessions		Server: nomad-100
• Search for All Sun Ray Sessions that contain:		
User Name:	<input type="text"/>	
Token ID:	<input type="text"/>	
Unix Login Name:	<input type="text"/>	
<input type="button" value="Search"/> <input type="button" value="Clear"/>		

FIGURE 3-41 The Find Sun Ray Sessions Window

- In the text fields, enter the Sun Ray Name, Token ID, or UNIX Login Name.**

3. Click the Search button.

If you enter data in error, press the Clear button to clear entered data. The Sun Ray Sessions window is displayed with the Sun Ray search results. See FIGURE 3-42.

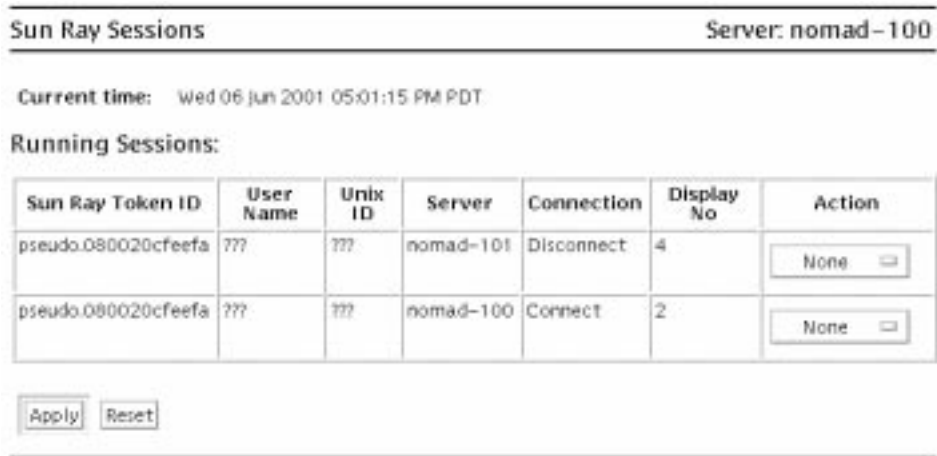


FIGURE 3-42 Sun Ray Sessions Window Containing the Search Results

Accessing Online Documentation

Online Documentation is available in English only.

▼ To Access Online Documentation

1. From the navigation menu, click the navigation arrow to expand the menu for Online Documents.

The menu is expanded to display Admin Guide, Advanced Admin Guide, and Installation Guide.

2. Select a document from the list.

The documentation is displayed in a separate window.

Using the Command-Line Interface

This chapter contains the following information:

- “Supported Commands” on page 71
- “Changing Policies” on page 75
- “Configuring Interfaces on the Sun Ray Interconnect Fabric” on page 75
- “Managing PROM Versions” on page 77
- “Configuring Sun Ray Settings” on page 81

Supported Commands

Commands that can be executed from the command line are listed in TABLE 4-1. For further information on executing these commands, see the appropriate man page.

Note – 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
```

followed by

```
% man command
```

TABLE 4-1 Supported Commands

Command	Definition
<code>utaction</code>	The <code>utaction</code> program provides a way to execute commands when a Sun Ray appliance session is connected or disconnected.
<code>utadm</code>	The <code>utadm</code> command manages the private network and DHCP configuration for the Sun Ray interconnect.
<code>utcapture</code>	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 appliances.
<code>utcard</code>	The <code>utcard</code> command allows configuration of different types of smart cards in the Sun Ray administration database.
<code>utconfig</code>	The <code>utconfig</code> command performs the initial configuration of the Sun Ray server and supporting administration framework software.
<code>utdesktop</code>	The <code>utdesktop</code> command allows the user to manage Sun Ray appliance desktop units connected to the Sun Ray server that the command is run on.
<code>utdetach</code>	The <code>utdetach</code> command disconnects the current non-smart card mobile session from its respective Sun Ray appliance. The session is not destroyed but put into a detached state. The session can be accessed if the same user token (user name) is presented to the Sun Ray server.
<code>utfwadm</code>	The <code>utfwadm</code> command manages firmware upgrades to Sun Ray appliances.
<code>utfwsync</code>	The <code>utfwsync</code> command refreshes the firmware level on the Sun Ray appliances to what is available on the Sun Ray servers in an HA group. It then forces all the Sun Ray appliances within the group to restart.
<code>utglpolicy</code>	The <code>utglpolicy</code> command gets or sets group <code>utpolicy</code> options. Normally, setting group policies is accomplished by using the Sun Ray Web-based Administration Tool.
<code>utgroupsig</code>	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 Directory Services rootpw used by Sun Ray to a value based on the group signature.
<code>utgstatus</code>	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.

TABLE 4-1 Supported Commands (*Continued*)

Command	Definition
<code>utinstall</code>	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, any patches required by the framework, and Solaris operating environment patches.
<code>utkiosk</code>	The <code>utkiosk</code> script is used to export kiosk configuration information into the LDAP database.
<code>utload</code>	The <code>utload</code> command sends a request to a Sun Ray appliance to initiate a firmware download. As an option, the downloaded firmware can be written to the appliance's flash memory.
<code>utmhadm</code>	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 Sun Ray administration database.
<code>utmhconfig</code>	The <code>utmhconfig</code> tool allows an administrator to list, add, or delete multiheaded groups easily.
<code>utmhscreen</code>	The <code>utmhscreen</code> tool draws a window displaying the current session on each screen, with the current screen highlighted for easy identification. This tool is automatically launched for users during the X server startup process (session creation).
<code>utpolicy</code>	The <code>utpolicy</code> command writes 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 according to the file, <code>/cdrom/cdrom0/.upgrade/utpreserve_list</code> .
<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>utrcmd</code>	The <code>utrcmd</code> program provides a way to run Sun Ray administrative commands remotely. The <code>utrcmd</code> program contacts the <code>in.utrcmdd</code> daemon on the remote <i>hostname</i> and executes the specified <i>command</i> with the specified arguments, <i>args</i> (if any).
<code>utreplica</code>	The <code>utreplica</code> command performs the configuration of the Sun Ray LDAP server to enable replication of administered data from a designated Primary server to each Secondary server in a failover group.
<code>utselect</code>	The <code>utselect</code> command presents the output of <code>utswitch -l</code> in a window and allows mouse-based selection of a Sun Ray server to which the Sun Ray appliance in use is reconnected.

TABLE 4-1 Supported Commands (*Continued*)

Command	Definition
utsession	The <code>utsession</code> command lists and manages Sun Ray sessions on the local Sun Ray server.
utsettings	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 appliance.
utsummc	The <code>utsummc</code> command adds the Sun Ray server software 1.3 module to the Sun Management Center (SunMC) and loads it to permit monitoring of the Sun Ray server software. The <code>utsummc</code> command can also remove the Sun Ray server software 1.3 module from SunMC.
utswitch	The <code>utswitch</code> command allows switching a Sun Ray appliance among Sun Ray servers in a failover group. It can also list the existing sessions for the current token.
utsvc	The <code>utsvc</code> script restarts the Sun Ray server software and, due to its location in <code>/etc/init.d</code> , is executed upon startup of the actual server.
utuser	The <code>utuser</code> command allows the user to manage Sun Ray users registered on the Sun Ray server that this command is run on.
utwall	The <code>utwall</code> utility sends a message or an audio file to users having an Xsun (X server unique to Sun Ray) process. The messages can be sent in email and displayed in a pop-up window.
utxconfig	The <code>utxconfig</code> program provides X server configuration parameters for users of Sun Ray appliance sessions.
utxset	The <code>utxset</code> command changes mouse acceleration and screen blank characteristics of the Sun Ray appliance. It is generally used internally by an X11 server to implement changes initiated by the <code>xset(1)</code> command.

▼ To Stop Sun Ray Services

- **Type:**

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

▼ To Start Sun Ray Services

- Type:

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

Changing Policies

When you run the `utpolicy` command with certain operands, messages are returned that indicate what operands to use. For example, if you make significant policy changes, run the `utpolicy` command with the `clear` option. See TABLE 4-2.

Use the `utpolicy -i clear` command instead of rebooting the server.

TABLE 4-2 `utpolicy` (clear and soft) Commands

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

Configuring Interfaces on the Sun Ray Interconnect Fabric

Use the `utadm` command to manage the Sun Ray interconnect fabric. This section contains the following procedures:

- “To Add an Interface” on page 76
- “To Delete an Interface” on page 76
- “To Remove All Interfaces” on page 76
- “To Print the Sun Ray Interconnect Configuration” on page 77

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

Note – For information on configuring interfaces, IP addresses, and DHCP data for failover, refer to the *Sun Ray Server Software 1.3 Advanced Administrator's Guide*. If the IP addresses and DHCP configuration data are not set up properly at the time that the interfaces are configured, the failover feature will not work properly.

▼ To Add an Interface

- **Type:**

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

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

You can use any valid Solaris network interface. For example:

```
hme[0-9], qfe[0-9]
```

▼ To Delete an Interface

- **Type:**

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

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

▼ To Remove All Interfaces

Use the `utadm -r` command to prepare for removal of the Sun Ray server software.

- **Type:**

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

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

▼ To Print the Sun Ray Interconnect Configuration

- **Type:**

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

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

Managing PROM Versions

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

- “To Update All of the Appliances on an Interface” on page 78
- “To Update an Appliance Using the Ethernet (MAC) Address” on page 79
- “Restarting Sun Directory Services” on page 79

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

You must have superuser privileges to run `utfwadm`. Use this command to select the appliances for upgrading. Select appliances one at a time or all appliances on a subnet.

TABLE 4-3 Options for the `utfwadm` Command

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

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

▼ To Update All of the Appliances on an Interface

- **Type:**

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

Note – Reboot the server. You must power cycle the appliance to force a firmware upgrade.

▼ To Update an Appliance Using the Ethernet (MAC) Address

- **Type:**

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

Restarting Sun Directory Services

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

▼ To Restart Sun Directory Services

1. **Stop the Sun Ray services:**

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

2. **Stop the SunDS daemon:**

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

3. **Start the SunDS daemon:**

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

4. **Restart the Sun Ray services:**

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

Solaris Lock Screen for Detached Sessions

The following commands are used to lock the screen when a user detaches the session; for example, by removing a smart card.

▼ To Lock a Screen Using CDE

1. Type the following command to lock the screen for the current session:

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

2. To make this feature the default, add the command to the end of the `.dtprofile` file in the user's home directory.

▼ To Lock an OpenWindows Session

1. Type the following command to lock the screen for the current session:

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

2. To make this feature the default, add the command to the end of the `.xinitrc` file in the user's home directory.

▼ To Create a System-Wide Default for Screen Locking

- Place the following script in `/etc/dt/config/Xsession.d` as an executable file (named, for example, `/etc/dt/config/Xsession.d/0999.screenlock`).

```
#!/bin/ksh
#
# Turn on screen-lock on disconnect for Sun Ray sessions
#
if [ "$DTUSERSESSION" != "" -a "$SESSIONTYPE" != "altDt" ]
then
    /opt/SUNWut/lib/utaction -d '/usr/dt/bin/dtaction LockDisplay' \
    2>/dev/null >/dev/null &
else
    /opt/SUNWut/lib/utaction -d \
    '/usr/openwin/bin/xlock -delay 1000000 -mode blank' \
    2>/dev/null >/dev/null &
fi
```


▼ To Get a Token ID From a Token Reader

- Type the following command:

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

Where *Token Reader* is the reader that you want to read the ID from. You are prompted to insert the token into the Token Reader when the command is ready. The command queries the Token Reader for the token's ID and, if successful, displays it. For example:

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

Configuring Sun Ray Settings

A hot key can be configured to display and hide the Sun Ray Settings GUI. This customization can be done on three levels:

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

To support these levels of customization, the Sun Ray Settings GUI looks for the following Java properties files at startup in the following order:

TABLE 4-4 Java Properties Files

File	Defaults	Description
<code>/etc/opt/SUNWut/utslaunch_defaults.properties</code>	System - wide	This file is read in first and contains helpful default properties. Any properties specified here override any defaults built into the application itself.
<code>/home/<i>anyuser</i>/.utslaunch.properties</code>	User	This file is read in second and contains the user's preferred values for the properties. Properties specified here override any application or sitewide defaults.
<code>/etc/opt/SUNWut/utslaunch_mandatory.properties</code>	System - wide mandatory	This file is read in last and contains sitewide mandatory settings that cannot be overridden by the user. Any properties specified here override any application, sitewide, or user defaults.

If you have a mandatory policy that all appliances use a standard hot key (perhaps for ease of training and support), use the system-wide mandatory defaults file to specify this standard key. In this case, users would not be allowed to specify their own preferences.

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

```
utsettings.hotkey=value
```

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

TABLE 4-5 Sun Ray Server Software 1.3 Specific Hot Key Values

Example Value	Notes
Shift-Props	This brings up the Settings GUI.
Ctrl+Alt+Backspace twice	This kills a session.
Ctrl+Alt+Del twice	This kills the process that has taken control of the X server.
Shift-Pause	This suspends a non-smart card session.
Mute+Louder+Softer	This displays the appliance's MAC address.
Ctrl+Power Key	This cycles power.

Both Shift-Props and Shift-Pause are configurable by users.

Setting Hot Key Values

If you do not want to use the Sun Props key as your default hot key, use the system-wide defaults file to specify a function key instead. Users can still specify their preferences (through the user defaults file), if so desired.

▼ To Change the Hot Key Setting System-Wide

1. As superuser, open the

`/etc/opt/SUNWut/utslaunch_defaults.properties` **file in a text editor.**

Note – 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 and place a # in front of that statement.

The # comments out the first hot key property.

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

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

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

4. **Save the `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 that were logged in prior to changing the hot key use the old value.

▼ To Change the Hot Key Setting for a Single User

1. **In your home directory, create the `.utslaunch.properties` 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.**

Smart Card Vendor Configuration Files

Note – Use the Administration Tool to add additional smart card vendor configuration files.

The configuration files are available from each smart card vendor. You might receive a `vendor.cfg` file.

This section contains the following procedures:

- “To Load a Configuration File Into the Directory” on page 85
- “To Configure a Token Reader” on page 85

▼ To Load a Configuration File Into the Directory

- Copy the vendor configuration file to the following location:

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

The additional vendor cards are displayed under the Available column in the Add page in the Administration Tool.

▼ To Configure a Token Reader

This command specifies an appliance for registering smart cards.

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

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

Where `nnnnnnnnnnnn` is the full Ethernet address (for example, `0800204c121c`) of the appliance that you want to use as a smart card reader.

Peripherals for Sun Ray Appliances

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

- “Device Nodes and USB Peripherals” on page 87
- “Attached Printers” on page 90
- “PDA Synchronization” on page 92
- “Adapters” on page 94

There are two kinds of peripherals: serial and parallel. Serial peripherals enable RS-232-style serial connections to the Sun Ray appliance. Parallel peripherals enable printing and come in two types: adapters and direct USB-connected printers.

Support for legacy serial and parallel devices is achieved using third-party adapters. In the case of a serial device such as a personal digital assistant (PDA), the adapter maps serial protocol to USB protocol. The Sun Ray server interprets USB protocol as serial protocol and directs it to the appropriate device node.

The Sun Ray server software 1.3 recognizes a parallel printer with an adapter as a USB printer.

Note – The printer naming conventions in the Sun Ray server software differ from those in a Solaris operating environment.

Device Nodes and USB Peripherals

The Sun Ray server software creates a device directory named `IEEE802.MACID` in the `/tmp/SUNWut/units` directory. This directory contains the MAC address for each appliance on the interconnect. The `IEEE802.MACID` directory for each appliance contains `dev` and `devices` directories, analogous to the `/dev` and `/devices` directories in the Solaris operating environment. The Sun Ray `dev`

directory contains a representation of the logical topology of the devices connected to the appliance. The Sun Ray `devices` directory contains a representation of the physical topology of the devices connected to the appliance.

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.

A typical device node path is as follows:

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

TABLE 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,</i> <i>terminal name 1</i>	The printer and terminal name in the Sun Ray <code>devices</code> directory is <i>manufacturer, model@port</i> with a colon separating the numerical index when the string just described is not unique in the directory.
<i>printer name 2,</i> <i>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

All device nodes are owned by the user whose session is active on the appliance. Only that user and superuser have permission to use the attached device. If there is no user with an active session, superuser owns the device nodes.

Hot Desking and Device Node Ownership

Changing the active session on an appliance changes the ownership of the device nodes to the user associated with the new session. A session change occurs whenever a user inserts a smart card into or removes one from an appliance or logs in to a session or detaches from one using non-smart card mobility. In a failover environment, a session can also be changed using the `utselect` or `utswitch` commands. 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. Any devices currently open by the superuser are not affected by the session change. This includes normal Solaris printing.

Caution – Any input or output in progress on a device node opened by a non-superuser user when a session is changed is cancelled after 15 seconds. For example, PDA synchronizing should be completed before changing sessions.

Note – If the original session is restored within 15 seconds, the ownership is not relinquished and input and output continue uninterrupted.

Attached Printers

Sun Ray server software 1.3 supports PostScript™ printers connected directly to a USB port on the Sun Ray appliance or connected through a USB-to-parallel port adapter. For non-PostScript™ printer support, refer to “Printers Other Than PostScript™ Printers” on page 92.

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

For more information on Solaris Ready™ printers, go to:

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

Printer Setup

Starting a print queue on a printer attached to a Sun Ray appliance, either directly or through an adapter, is identical to starting a print queue in the Solaris operating environment.

▼ To Set Up a Printer

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

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

3. To locate the Sun Ray appliance, 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 appliance 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. Start the Administration Tool by typing:

```
# admintool &
```

7. Go to Browse -> Printers -> Edit -> Add -> LocalPrinter.

8. Type in:

a. Printer name: *printername*

b. Description (optional)

c. Printer Port

Choose **Other** to enter the printer port path name, using the resulting directory from Step 4.

```
/tmp/SUNWut/units/IEEE802.MACID/dev/printers/printer-node-name
```

Note – Do not use the port name under the devices directory.

d. Click OK.

e. If you are using a PostScript printer, under **Printer Type** choose **PostScript** unless your printer is listed.

Select the printer type according to your printer model. If no option matches, select **other**; then type your printer type or **unknown**.

f. If you are using a PostScript printer, under **File Contents** choose **PostScript and ASCII**.

g. **Options: Default Printer (optional)**

h. Click **OK**.

Note – Do not click OK more than one time. If you do, a failure message is displayed.

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

```
# lpstat -d printername
```

Printers Other Than PostScript™ Printers

PostScript™ printers are the native Solaris operating environment printing solution. 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.

PDA Synchronization

You can synchronize PDAs that use the Palm OS to a Sun Ray appliance using a USB-to-serial adapter. Hot Desking gives the user the ability to synchronize a PDA as it moves with the user from appliance-to-appliance, provided each appliance has a cradle or the user moves the cradle. For PDA synchronization, the PDASync for Solaris™ application is included in the Solaris 7 11/99 and Solaris 8 operating environments.

In the Solaris 8 operating environment, PDASync is compatible with Java 1.2 software. In the Solaris 7 operating environment, PDASync is compatible with Java 1.1 software. To run PDASync for Solaris™ under Java 1.2 software in the Solaris 7 operating environment, the PDASync for Solaris™ patch is required. This patch is available at the following Web site:

<http://www.sun.com/software/solaris/pdasync/index.html>

PDASync for Solaris™ Application on Sun Ray Appliances

PDASync for Solaris™ requires Java Communications API 2.0.2 or a later version to run on the Sun Ray appliance. The Java Communications API 2.0.2 is provided in the Sun Ray Server Software 1.3 CD's Supplemental directory.

Certain components of the Java Communications API 2.0.2 package must be installed in specific directories for PDASync for Solaris™ to run.

▼ To Set Up the PDASync Application on a Sun Ray Appliance

1. **Log in as superuser.**
2. **Insert the Sun Ray Server Software 1.3 CD-ROM.**
3. **Copy the `comm.tar.Z` file from the Supplemental directory on the CD into a directory you created on your system by typing:**

```
# cp /cdrom/cdrom0/Supplemental/comm.tar.Z /var/tmp
```

4. **Change to the directory you created on your system by typing:**

```
# cd /var/tmp
```

5. **Uncompress the `comm.tar.Z` file located in the Supplemental top-level directory on the Sun Ray Server Software 1.3 CD.**

```
# uncompress comm.tar.Z
# tar -xvf comm.tar
```

6. To change directories to the `commapi` directory, type:

```
# cd commapi
```

7. Copy the `comm.jar` file by typing:

```
# cp comm.jar /usr/dt/appconfig/sdtpdasync/classes
```

8. Copy the `libSolarisSerialParallel.so` file by typing:

```
# cp libSolarisSerialParallel.so /usr/dt/appconfig/sdtpdasync/lib
```

9. Run the PDASync application by going to Application Manager -> Desktop_Apps->PDASync or typing:

```
# /usr/dt/bin/sdtpdasync
```

Adapters

A list of verified adapters, serial and parallel, is available by following the links on the Sun Ray appliance third-party peripherals Web site:

http://www.sun.com/io_technologies/sunray/usb/sunray-usb.html

Troubleshooting

This appendix contains the following sections:

- “Appliance Questions” on page 95
- “User Questions” on page 101
- “Server Questions” on page 103
- “Green Newt Cursor” on page 106
- “Errors From the Authentication Manager” on page 111

Appliance Questions

Q: What action is required when the OSD (on-screen display) is displayed?

A: Perform the following steps listed for each icon shown:

Startup Icon

There are three possible startup modes:



Waiting for the Interconnect

Definition: The appliance has passed the power-on self test but has not detected an Ethernet signal yet. This icon is displayed as part of the normal startup phase and is usually displayed for only a few seconds.

Actions to take if this icon stays on for more than 10 seconds:

1. Check that the Ethernet cable is correctly plugged in to the back of the appliance and the other end is plugged in to the correct hub, switch, or network outlet.
2. If the appliance is connected through a hub or a switch, make sure that the hub or switch is powered on and configured correctly.
3. Check that the Sun Ray server is up and running.



DHCP Pending

Definition: The appliance has detected the Ethernet carrier but has not received its initial parameters from DHCP yet. This icon is displayed as part of the normal startup phase and is usually displayed for only a few seconds.

Actions to take if this icon stays on for more than 10 seconds:

- Make sure that DHCP on the Sun Ray server is configured correctly, is up and running, and has not run out of IP addresses to assign to clients.

▼ To Restart DHCP

- as superuser, type:

```
# /etc/init.d/dhcp stop  
# /etc/init.d/dhcp start
```



Waiting to Connect to Authentication Manager

Definition: The appliance has received its initial parameters from DHCP but has not connected to the Sun Ray Authentication Manager yet. This icon is displayed as part of the normal startup phase and is usually displayed for only a few seconds. Once this icon disappears, the connection has been made and the user can insert his or her smart card and log in.

Actions to take if the icon displays for more than a few seconds:

- Make sure that the Sun Ray services, including the Authentication Manager are up and running on the Sun Ray server.

Appliance Failure



This icon is called **Hardware Failure** in the Sun Ray Troubleshooting Guides.

Definition: The appliance tried to load new PROM software from the Sun Ray server but failed in its attempt.

Actions to take if this icon displays for more than a few seconds:

1. Examine the Sun Ray server software logs for any error messages that might indicate the cause.
2. Check that DHCP on the Sun Ray server is configured correctly and is up and running.
3. Check that the TFTP service is enabled on the server.
4. Check `/tftpboot` on the Sun Ray server to see if the new PROM software exists and is ready to be downloaded to the appliance.
5. Once any problems are corrected, power cycle the appliance so that it can try to reload the PROM software.

No Ethernet



Check to see if the Ethernet cable is plugged in correctly.

The last six hexadecimal digits of the Ethernet address are shown in the icon.

Definition: The appliance has lost the Ethernet signal. This icon is only displayed after the appliance has successfully booted and then lost its Ethernet signal.

Actions to take:

1. Check that the Ethernet cable is correctly plugged in to the back of the appliance and the other end is plugged into the correct switch or network outlet.
2. If the appliance is connected through a hub or switch, make sure that the hub or switch is on and configured correctly.

Software Failure



Definition: The appliance has lost its connection to the Sun Ray Authentication Manager or DHCP was unable to renew its lease for an IP address.

Actions to take:

1. Check that the Sun Ray server is up and running.
2. Check that the Sun Ray services, including the Authentication Manager are up and running on the Sun Ray server.
3. Check that DHCP on the Sun Ray server is configured correctly, is up and running, and has not run out of IP addresses to assign to clients.

Firmware Download

The number of dashes under the machines indicate progress:



Downloading PROM Software

Definition: The appliance is currently downloading new flash PROM software from the Sun Ray server.

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 appliance has to download new PROM software the next time it reboots.



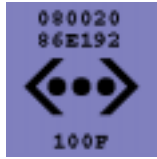
Saving PROM Software

Definition: The appliance has just downloaded new PROM software from the Sun Ray server and is saving it to the appliance's PROM.

Actions to take:

- Wait until the download is done. Downloading and saving the new PROM software usually takes less than a minute. If you interrupt the download, the appliance has to download new PROM software the next time it reboots.

Ethernet Address



Definition: When the three audio volume control keys are pressed simultaneously, the Ethernet address, which uniquely identifies the appliance, is displayed. This icon is displayed from 5 to 15 seconds. If the user has a non-Sun keyboard, the user should disconnect and reconnect the Ethernet wire. Link speed is also indicated below the symbol (for example, 10F, 10H, 100F, 100H). The F stands for full duplex; H stands for half duplex. The 10 stands for 10 Mbps, and 100 for 100 Mbps.

Card Read Error OSD



Definition: The Card Read Error OSD icon appears whenever the firmware is unable to read the card due to one of the following causes:

- The appliance 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:

- Upgrade the firmware.
- Replace the card.

Prompt for Card Insertion OSD



Definition: If the current authentication policy allows access only by card, this OSD icon appears and prompts the user to insert a card.

Access Denied OSD



Definition: 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 an appliance.

LEDs

TABLE A-1 Power LED

State of LED	Action to take
Off	Check to see if the appliance is plugged in. Replace the appliance.
Yellow	Hardware fault. Replace the appliance.
Blinking	PROM is corrupted. Check that firmware downloads are properly configured and enabled. Then power cycle the appliance.

Q: How can a user check to see if the Sun Ray appliance can play audio files (*.au)?

A: Ask the user to type:

```
% cat /usr/demo/SOUND/sounds/whistle.au >/$AUDIODEV
```

Some applications are hardcoded to send files to `/dev/audio`. Sun Ray provides a redirection library that can be used to correct this behavior.

▼ To Activate the Redirection Library

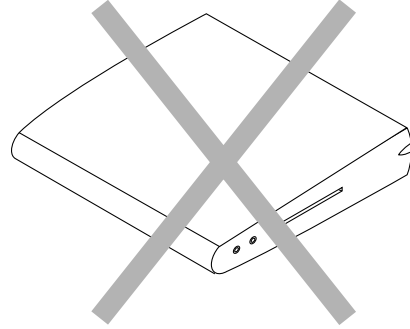
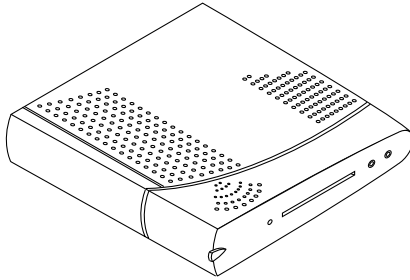
1. Set the environment variable `LD_PRELOAD` to `libc_ut.so` in the shell or wrapper from which you started the audio player:

```
# setenv LD_PRELOAD libc_ut.so
```

2. Relaunch the application.

Q: What if a user has broken or misplaced the Sun Ray 1 appliance's base?

A: The appliance must lie on a desk speaker-side up. It overheats if it is placed speaker-side down.



User Questions

Q: The user's screen locked up. What do I do?

A: There are two possible problems that have occurred. Their symptoms and solutions are as follows:

- Problem: The window manager `dtwm` or `olwm` has died.
- Symptom: All the windows that had been iconified are restored, and the user cannot move or resize them but can move the mouse pointer.
- Solution: Use a terminal window if available or remotely log in using the `DISPLAY` variable set correctly to restart `dtwm` or `olwm`. For example:

```
% rlogin machine_name -l user_name
% setenv DISPLAY xxxx
% /usr/dt/bin/dtwm &
```

- Problem: The user's last application has locked the server and will not release it.
- Symptom: The server freezes, and the user cannot resize or move any window. The user can move the mouse but cannot activate a window.
- Solution:
 1. Determine the last application used by the user and kill it.
 2. Try power cycling the appliance using the hot key sequence `ctrl+alt+backspace`.
 3. If the user is using a smart card, ask the user to remove the smart card.
 4. If the user removes the smart card and the screen does not go blank, you need to replace the Sun Ray appliance.

5. As a last resort, you can kill the X server.

a. To identify the X server's PID, type:.

```
# ps -ef | grep Xsun | grep username
```

b. Kill the process associated with the X server by typing:

```
% kill pid
```

Q: What does it mean when a user gets one of the following (or similar) errors when starting an application?

```
/usr/openwin/bin/xcolor: unable create colormap (8)
Application initialization failed: couldn't find an appropriate visual
could not get visual
X Error of failed request: BadValue (integer parameter out of range for operation)
Major opcode of failed request: 91 (X_QueryColors)
Value in failed request: 0xc3b2ae
Serial number of failed request: 82
```

A: These types of errors indicate that the application can be written to use only 8-bit PseudoColor graphics. Many older programs require an 8-bit PseudoColor visual.

Sun Ray server software supports an 8-bit visual, but enabling it requires more memory for the X server and causes some graphics-performance degradation. The general use of the 8-bit visual support reduces the scalability of the Sun Ray server.

If an important application fails for a user or set of users, you can use the `utxconfig(1M)` command to enable the 8-bit support or make it the default visual for them.

As a rule, you should disable 8-bit visuals. Try to enable the 8-bit support before making it the default visual. Using the 8-bit visual as the default visual causes a greater negative impact on performance and scalability than enabling it for a few users. However, some applications do not search for the visual that they require and blindly assume that the default visual is what they should use. For such programs, using the 8-bit visual as the default visual is the only choice.

To allow the 8-bit PseudoColor visual to be enabled, as superuser, type:

```
# utxconfig -d $DISPLAY -p on
```

To make 8-bit PseudoColor visual the default, as superuser, type:

```
# utxconfig -d $DISPLAY -p default
```

Note – See the `utxconfig` command man pages for more information about this command.

A user can run the `utxconfig` command for a session as long as he or she has access to the X display for the session. Only superuser can make a change for someone else or change the default values.

Although the display specification is used to identify the X server configuration that should be changed, `utxconfig` stores the configuration based on the token that provides access to the session. Therefore, the configuration stays with the user (for smart card tokens) or the appliance (for default tokens) even if a different display number is allocated in the future.

Q: A user can start commands from menus and the CDE bar but cannot start them from terminal windows. What is wrong?

A: The user's startup scripts (`.cshrc`, `.login`, `.profile`, or `.dtprofile`) probably set the `DISPLAY` variable. The scripts should be changed to only set `DISPLAY` if it is not already set or to retain the display number (the part after the `:`). For example:

```
% echo $DISPLAY
yoyodata:62.0
```

Server Questions

Q: The server's hard drive is constantly being accessed. Why is the Sun Ray server swapping so often?

A: You might need to increase your server's memory. At least 256MB of RAM is recommended for most network environments with 40 to 60MB per user. If you have less, your server relies upon any available swap space on your hard drive. Use the `swap` command to review your system's resources:

```
% /usr/openwin/bin/swap -s
```

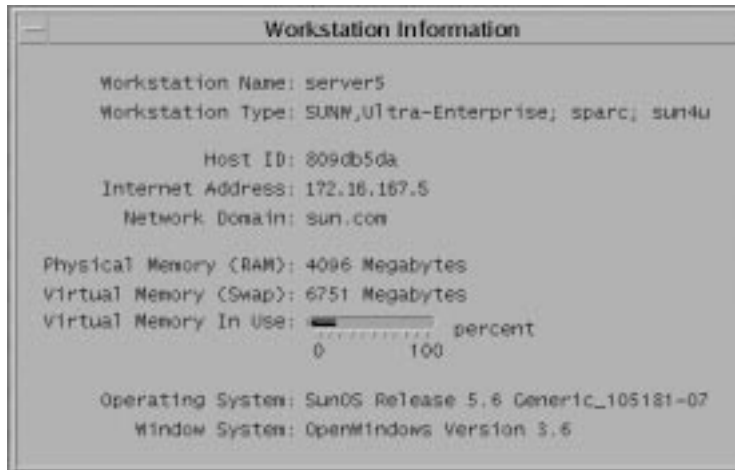


FIGURE A-1 Accessing Workstation Resource Information

To determine if the server is swapping, type:

```
% vmstat 5
```

The output is displayed in the terminal window.


```

proc  memory      page      disk      faults      cpu
r b e  swpd  free   re   wf  pi  ps  fr  de  sr  fo  so  st  si  in  sy  cs  us  sy  id
0  0  0  19528  8794   0  1386  22  16  23  1136  3  0  4  1  0  1261  835  1996  26  20  54
7  0  0  24930912  62296  1  2526  544  1161  1699  336  328  0  57  8  10  2423  27333  8691  40
22  38
0  0  0  24929376  64360  0  2247  16  246  318  0  43  0  8  2  1  1729  23553  7383  47  16  38
2  0  0  24926960  63408  0  2727  3  323  472  0  80  0  2  1  2  1728  33794  9126  40  24  36
1  0  0  24926182  63464  1  2975  1132  654  905  0  137  0  39  41  35  2544  28658  7906  56  24  20
3  0  0  24920352  62288  3  3080  174  1158  1612  0  247  0  15  6  4  2340  23643  9530  54  23  24
2  0  0  24916176  63820  5  2589  147  1059  1062  27400  338  0  19  9  6  2176  27236  7688  56  23  20
3  0  0  24917680  70152  1  2461  289  179  179  16200  0  0  39  22  10  2315  24438  8807  52  33  13
13  0  0  24913760  65808  1  3290  43  1  1  9578  0  0  1  6  1  2384  48328  8701  52  41  7
0  0  0  24918144  68136  1  2451  476  0  0  5672  0  0  3  3  1  2345  32262  9344  36  24  40
1  0  0  24917224  65808  0  1991  240  184  280  3376  42  0  3  1  1  2023  23744  7174  55  17  20
3  0  0  24924568  73224  1  2538  44  6  6  2008  0  0  3  2  1  2218  32810  9113  46  23  31
1  0  0  24929144  77320  0  2011  51  0  0  1152  0  0  1  2  1  1900  28752  7856  48  19  33
1  0  0  24928376  76488  0  2353  32  0  0  352  0  0  26  4  0  2770  31567  10589  42  23  35
8  0  0  24925376  73860  0  2239  27  0  0  0  0  0  1  2  0  2343  30338  8929  48  19  33

```

FIGURE A-2 Output of the `vmstat 5` Command

If the column marked `sr` is larger than 10 (a noticeable amount of time), you should consider adding memory.

Q: A user is receiving an `Unable to get pty error message`. What is wrong?

A: The Sun Ray server has exhausted the number of pseudo terminals defined. If a system does not have enough pseudo terminals defined, users cannot bring up a shell window and cannot login. For example, a network consists of 50 Sun Ray appliances and the `pty` entry is set to 40. When the 41st user tries to open a shell window, this error message is displayed. As superuser, edit the `/etc/system` file `pt_cnt` value to increase the number of available pseudo terminals. Change the `pt_cnt` entry to a higher number (at least four or five times the number of users). You must reboot:

```
# set pt_cnt=40
set pt_cnt=200
```

Q: Does the Sun Ray server software support the Direct Graphics Access (DGA) extension to X11?

A: No. The Sun Ray server software does not support the SunDGA (Direct Graphics Access) extension to X11. The Sun Ray server software correctly reports that DGA is not supported to any application that initiates an inquiry. Normally applications make use of DGA through libraries (for example, XIL) that deal with the inability to use DGA and use an alternate path.

Q: A user is working in a CAD program with complex graphics. When the user is scrolling the graphic, it is jerky. Is there anything that I can do?

A: Make sure that the appliance is using a 100-Mbyte full-duplex link. Also check the system's configuration and the application's requirements. Possible remedies on the server include: adjusting process priorities, adding more memory, adding a CPU, or adding more disk space.

Q: Why is my ShowMe TV™ session running slow?

A: For best performance with the Sun Ray server, use the latest version of ShowMe TV. You can download this application from the following URL:

<http://www.sun.com/desktop/products/software/ShowMeTV/>

Q: If I am using AutoCAD, what settings should be enabled?

A: AutoCAD is an 8-bit only program and requires the 8-bit visual to be enabled. You can enable this setting (for the current user) by typing:

```
# /opt/SUNWut/lib/utxconfig -p on
```

The `utxconfig(1M)` manual page provides more information including the steps to make this the system-wide default. The users need to log out and log in for the change to take effect.

Green Newt Cursor

The green newt cursor is the transitional cursor for the Sun Ray appliance. The cursor remains a green newt until an application, typically the X Window server (`Xsun`), changes the cursor to an X, an hourglass, or an arrow. The green newt cursor does not necessarily mean that the Sun Ray appliance is hung or in an error condition but that it is ready and awaiting display-rendering commands from `Xsun`.

If the green newt cursor is displayed for an extended period, there is no X Window server running.

To troubleshoot a green newt cursor, you need to consider:

- “Is There Really a Problem?” on page 107
- “Is the Problem Caused by Hardware?” on page 107
- “Is the `dtlogin` Daemon Up-to-Date?” on page 108
- “Is the `dtlogin` Session Hung?” on page 108
- “Are the Configuration Files Corrupt?” on page 109

Is There Really a Problem?

The Sun Ray administration model has six user session types:

- Default—normal user login
- Register—user self-registration
- Kiosk—anonymous user operation
- Insert card—user smart card required
- Card error—unrecognized user smart card type
- No entry—user’s smart card token is blocked

The first three session types have normal login processes. The last three session types do not have a login process at all but display an icon on the Sun Ray appliance monitor along with the green newt cursor. The icons indicate that the user must take other steps before a successful login is possible. If the user were to immediately remove and reinsert the smart card, the icon would disappear but the green newt cursor would remain.

These last three session types, their icons, and the appearance of the green newt cursor are not cause for alarm. The user can:

- Insert a recognized smart card in the correct orientation
- Ask the Sun Ray administrator to grant access

Is the Problem Caused by Hardware?

Sluggish Sun Ray server performance or excessive disk swapping is an indication that the Sun Ray server is under provisioned. Under these circumstances, there is not enough virtual memory available to start an X Window server instance for a user’s session. With no X Window server running, the cursor remains a green newt.

The solution in this situation is to add more memory or increase the size of the swap partition. See the *Sun Ray Server Software 1.3 Installation Guide* for information regarding Sun Ray server sizing requirements.

Green Newt Cursor for Default Session Type

This section applies to a normal `dtlogin` session.

The `Xsun` server is indirectly started by the `dtlogin` daemon. In the process of starting the `Xsun` server, the `dtlogin` daemon reads two configuration files:

- `/etc/dt/config/Xservers`
- `/etc/dt/config/Xconfig`

If, after several retries, the `Xsun` process does not start, the `dtlogin` daemon just gives up. The problem can usually be traced back to an older version of the `dtlogin` daemon or the configuration files for the `dtlogin` daemon.

Is the `dtlogin` Daemon Up-to-Date?

The `dtlogin` daemon is part of the Solaris operating environment and has existed long before the Sun Ray server software. The Sun Ray administration model uses the `dtlogin` daemon in new ways, such that certain bugs in the `dtlogin` daemon have become apparent. Patches to fix these bugs in the `dtlogin` daemon are available.

For the latest information regarding Sun Ray server software bugs and patches, check the following URL:

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

Solaris operating environment patches and other software patches are available at the following URL:

<http://access1.sun.com>

Is the `dtlogin` Session Hung?

Under certain circumstances, the `dtlogin` daemon might not be able to start the `Xsun` server. Without an X Window server running, the cursor remains a green `newt`. In this case, the `dtlogin` daemon has given up and has marked the user's session as bad. Consequently, this action prevents any further X Window server start-up attempts for the user's session.

To resolve this situation, you must manually unconfigure the `dtlogin` session. The system then reconfigures the session automatically.

▼ To Identify and Unconfigure the `dtlogin` Session

1. **On the keyboard of the Sun Ray appliance displaying the green `newt` cursor, press all three audio keys at the same time.**

An icon with the Sun Ray appliance Ethernet address is displayed.

2. **Record the Ethernet address.**

Note – Do not remove the smart card.

3. **On another Sun Ray appliance or the Sun Ray server, log in as superuser and open a shell window.**

4. Execute the following command:

```
# basename `grep -li Ethernet_address /var/opt/SUNWut/displays/*`
```

Record the output, which is the display number assigned to the session experiencing the Green Newt Cursor.

5. Execute the following command:

```
# /opt/SUNWut/sbin/utuser -k -xdisplay display_number
```

Are the Configuration Files Corrupt?

There are two configuration files susceptible to corruption:

- /etc/dt/config/Xservers
- /etc/dt/config/Xconfig

These files are used by the `dtlogin` daemon. When they are corrupt, the `dtlogin` daemon cannot properly start the `Xsun` server. Without an X Window server running, the cursor remains a green newt.

▼ To Determine the Integrity of the Configuration Files

1. As a user of the Sun Ray server, open a shell window and compare the `/usr/dt/config/Xservers` and `/etc/dt/config/Xservers` files:

```
% diff /usr/dt/config/Xservers /etc/dt/config/Xservers
```

This command compares a known good file with the suspect file. The output should be similar to the following example:

```
106a107,130
> # BEGIN SUNRAY CONFIGURATION
> :8 SunRay local@none /usr/openwin/bin/Xsun :8 -nobanner
.
.
> :9 SunRay local@none /usr/openwin/bin/Xsun :9 -nobanner
> # END SUNRAY CONFIGURATION
```

Note – This is a simplified example. Your output might have tens of lines between the `BEGIN SUNRAY CONFIGURATION` and `END SUNRAY CONFIGURATION` comments.

In the first line of output, there is `106a107,130`. The `106` means that the two files are identical to the 106th line of the files. The `a107,130` means that the information on lines 107 through 130 of the second file would have to be added to the first file to make it the same as the second.

If your output shows the first three digits to be a number less than 100, the `/etc/dt/config/Xservers` file is corrupt.

2. Compare the `/usr/dt/config/Xconfig` and `/etc/dt/config/Xconfig` files:

```
% diff /usr/dt/config/Xconfig /etc/dt/config/Xconfig
```

The output should be similar to the following example:

```
156a157,180
> # BEGIN SUNRAY CONFIGURATION
> Dtlogin.*_8.environment:
SUN_SUNRAY_TOKEN=ZeroAdmin.ml.at88sc1608.6d0400aa
.
.
> Dtlogin.*_9.environment:
SUN_SUNRAY_TOKEN=ZeroAdmin.ml.at88sc1608.a10100aa
> # END SUNRAY CONFIGURATION
```

Note – Again, this is a simplified example. Your output may have tens of lines between the `BEGIN SUNRAY CONFIGURATION` and `END SUNRAY CONFIGURATION` comments.

If your output shows the first three digits to be a number less than 154, the `/etc/dt/config/Xconfig` file is corrupt.

▼ To Replace the `Xservers` and `Xconfig` Files

Note – Replacing the `Xservers` file requires shutting down all Sun Ray appliance services. Remember to inform users of the outage.

1. As superuser, open a shell window and stop the Sun Ray server:

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

2. Replace the `Xservers` and `Xconfig` files as appropriate:

```
# /bin/cp -p /usr/dt/config/Xservers /etc/dt/config/Xservers
```

```
# /bin/cp -p /usr/dt/config/Xconfig /etc/dt/config/Xconfig
```

3. Re-initialize the authentication policy:

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

The `utpolicy` command will wait for a full minute to insure that all Sun Ray appliance X Window servers have exited.

The extra lines within the previous `Xservers` and `Xconfig` files are automatically rebuilt.

Errors From the Authentication Manager

Message Format

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 appliance authentication, access control, and session monitoring. These threads are named “Client” plus number. The Client# thread names are reused when a connection terminates. Other threads are:

- `SessionManager#`—Communicate with `utsessiond` on behalf of a Client# thread.
- `AdminJobQ`—Used in the implementation to wrap a library that would not otherwise be thread-safe.
- `CallBack#`—Communicate with applications such as `utload`.
- `Control`—Listens for connections from `utsessiond` as well as the initial communications with applications such as `utload`.

- `message_class`

Messages with the same thread name are related. The exception occurs when a Client# thread disconnects an appliance and then purges the connection information from memory. After a Client# DESTROY message, the next use of that Client# thread name has no relation to previous uses of the thread name (in other words, the thread names are reused).

- `CLIENT_ERROR`—Indicates unexpected behavior from an appliance. These messages can be generated during normal operation if an appliance is rebooted.
- `CONFIG_ERROR`—Indicates a system configuration error. The Authentication Manager generally exits after one of these errors is detected.
- `NOTICE`—Logs normal events.
- `UNEXPECTED`—Logs events or conditions that were not anticipated for normal operation but are generally not fatal. Some of these errors should be brought to the attention of the Sun Ray product development team.

- **DEBUG**—Only occurs if explicitly enabled. Beneficial to developers. Debug messages can reveal session IDs, which must be kept secret to ensure proper security.

TABLE A-2 Error Message Examples

Error class	Message	Description
CLIENT_ERROR	...Exception ... : cannot send keepAliveInf	Error encountered while attempting to send a keep-alive message to an appliance.
	...keepAlive timeout	An appliance has failed to respond within the allotted time. The session is being disconnected.
	duplicate key:	Appliance does not properly implement the authentication protocol.
	invalid key:	Appliance does not properly implement the authentication protocol.
CONFIG_ERROR	attempt to instantiate CallBack 2nd time.	Program error.
	AuthModule.load	Problem encountered while loading configuration module.
	Cannot find module	Program or installation error.
NOTICE	"discarding response: " + param	No controlling application is present to receive appliance response.
	"NOT_CLAIMED PARAMETERS: " + param	A token was not claimed by any authentication module.
	...authentication module(s) loaded.	Notification that authentication modules have loaded.
	...DISCONNECT ...	Normal notification of disconnection.
UNEXPECTED	"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 appliance.
	.../... protocolError: ...	Various protocol violations are reported with this message. This is also a way for utauthd to force the appliance to reset.

Glossary

B

bpp Bits per pixel.

C

CAM Controlled access mode.

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.

D

DHCP Dynamic Host Configuration Protocol, which is a means of distributing IP addresses and initial parameters to the appliances.

E

- 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.
- FTP** File Transfer Protocol. The name of the Internet protocol and the program used to transfer files between hosts.

H

- Hot Desking** The ability for a user to remove a smart card, insert it into any other appliance 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 appliances.
- hot key** A pre-defined key that causes something to appear on your screen. A hot key is used to bring up the Settings screen on the Sun Ray appliance.
- hot-pluggable** A property of a hardware component that can be inserted into or removed from a system that is powered on. USB devices connected to Sun Ray appliances are hot-pluggable.

I

- Interconnect fabric** All the cabling and switches that connect a Sun Ray server's network interface cards to the Sun Ray appliances.
- internet** A collection of networks interconnected by a set of routers that enable them to function as a single, large virtual network.
- Internet** The largest internet in the world consisting of large national backbone nets (such as MILNET, NSFNET, and CREN) and a myriad of regional and local campus networks all over the world. It is a global collection of networks connecting a wide range of computers using a common protocol to communicate and share services.
- intranet** Any network that provides similar services within an organization to those provided by the Internet but which is not necessarily connected to the Internet.
- IP address** A unique number that identifies each host or other hardware system on a network. An IP address is composed of four integers separated by periods. Each decimal integer must be in the range 0-255 (for example, 129.144.0.0).
- IP address lease** The assignment of an IP address to a computer system for a specified length of time, rather than permanently. IP address leasing is managed by the Dynamic Host Configuration Protocol (DHCP). Sun Ray appliance IP addresses are leased.

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 client's perspective, the most immediate server in the LAN.

- login** The process of gaining access to a computer system.
- login name** The name by which the computer system knows the user.
-

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.
- mobility** For the purposes of the Sun Ray server software, the property of a session that allows it to follow a user from one appliance 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.
- multiplexing** The process of transmitting multiple channels across one communications circuit.
-

N

- namespace** A set of names in which a specified ID must be unique.
- network** The hardware connecting various computer systems that enables them to communicate and the systems so connected.
- network address** The IP address used to specify a network.
- network interface** An access point to a computer system on a network. Each interface is associated with a physical device. However, a physical device can have multiple network interfaces.
- network interface card** NIC. The hardware that links a workstation or server to a network device.

- network latency** The time delay associated with moving information through a network. Interactive applications such as voice, video displays and multimedia applications are sensitive to these delays.
- network mask** A number used by software to separate the local subnet address from the rest of a given Internet protocol address. An example of a network mask for a class C network is 255.255.255.0.
- network protocol stack** A network suite of protocols, organized in a hierarchy of layers called a stack. TCP/IP is an example of a Sun Ray protocol stack.
- non-smart card mobility** A mobile session on a Sun Ray appliance that does not rely on a smart card.
-

O

- OSD** On-screen display. The Sun Ray appliance uses small OSD icons to alert the user of potential start-up problems.
-

P

- patch** A collection of files and directories that replace or update existing files and directories that prevent proper execution of the software on a computer system. The patch software is derived from a specified package format and can only be installed if the package it fixes is already present.
- policies** Authentication Manager, using the selected authentication modules, decides what tokens are valid and which users have access.
- port** (1) A location for passing data in and out of a computer system. (2) The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host.
- power cycling** Using the power cord to restart an appliance.

S

- 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 appliance. It can include audio, video, X servers, access to other machines, and device control of the appliance.
- session** A group of services associated with a single user.
- smart card** A plastic card containing a microprocessor capable of making calculations.
- subnet** A working scheme that divides a single logical network into smaller physical networks to simplify routing.

T

- token** In the Sun Ray system, a token must be presented by the user. It is required by the Authentication Manager to consider allowing a user to access the system. It consists of a type and an ID. If the user inserted a smart card, the smart card's type and ID are used as the token. If the user is not using a smart card, the appliance's built-in type (pseudo) and ID (the unit's Ethernet address) are supplied as the token.
- thin client** Thin clients remotely access some resources of a computer server, such as compute power and large memory capacity. The Sun Ray appliances rely on the server for all computing power and storage.
- time-out value** The maximum allowed time interval between communications from an appliance to the Authentication Manager.
- TCP/IP** Transmission Control Protocol/Internet Protocol (TCP/IP) is a networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and operating systems.

U

- URL** Uniform Resource Locator. A standard for writing a textual reference to an arbitrary piece of data in the World Wide Web (WWW). The syntax of a URL is `protocol://host/localinfo` where `protocol` specifies a protocol to use to fetch the object (like HTTP or FTP), `host` specifies the Internet name of the host on which to find it, and `localinfo` is a string (often a file name) passed to the protocol handler on the remote host.
- 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). The first character must be a letter.

V

- 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.

W

- work group** A collection of associated users who exist in near proximity to one another. A set of Sun Ray appliances that are connected to a Sun Ray server provides computing services to a work group.

X

X server A process which controls a bitmap display device in an X window system. It performs operations on request from client applications.

Index

A

adapters, 94

Administration Group

viewing failover group status, 44

Administration Tool, 23, 28

changing policies, 31

changing the admin password, 30

controlled access mode, 63

adding or editing applications, 65

selecting additional applications, 64

desktops

displaying current properties, 37

editing a single desktop's properties, 41

searching for, 40

viewing, 36

viewing properties of current user, 39

examining log files, 47

finding Sun Ray sessions, 68

locating token readers, 34

log files

viewing messages logs, 47

logging in, 28

managing Sun Ray sessions, 67

resetting Sun Ray Services, 33

restarting Sun Ray Services, 33

smart card

adding, 51

changing the probe order, 51

deleting, 52

viewing or listing configured, 49

viewing the probe order, 50

users

adding a token ID, 60

adding a user with token ID, 61

deleting, 56

deleting a token ID, 60

displaying current properties, 57

editing properties, 59

enabling or disabling a token ID, 60

finding a user, 62

getting a token ID from token reader, 62

viewing by ID, 56

viewing by name, 56

viewing current, 57

viewing all multihead groups, 43

viewing Sun Ray sessions, 67

AUDIODEV environment variable, 4

Authentication Manager, 8, 27

interacting with Session Manager, 11

C

CDE

locking the screen, 80

central registration, 11

Citrix, 4

commands

utadm, 75

utadm -r, 76

utaudio, 4

utdetach, 18, 19

utfwadm, 77

utglpolicy, 25, 26

utpolicy, 25, 26

utpolicy -i clear, 75

- utslaunch.properties, 20
- utwall, 23, 25
- controlled access mode
 - adding or editing applications, 65
 - configuring, 63
 - selecting additional applications, 64

D

- departments, 5
- desktops
 - displaying current properties, 37
 - editing a single desktop's properties, 41
 - searching for, 40
 - viewing, 36
 - viewing properties of current user, 39
- device
 - directory, 87
 - links, 89
 - node ownership, 89
 - nodes, 88
 - USB, 88
- device emulation, 4
- dsserv, 79
- dtlogin
 - unconfiguring, 108
- dtlogin screen, 8, 16
- dtprofile file, 80
- Dynamic Host Configuration Protocol (DHCP), 3
 - data for failover, 76

F

- failover group, 6, 7
 - viewing status, 44
- firmware module, 3
 - PROM version management, 77

H

- Help, 16
- HOBsoft, 5
- Hot Desking, 4, 15, 89
- hot key, 81, 101

- changing setting, 84
- changing setting site-wide, 83
- detaching a mobile session, 19
- entry, 82
- values, 83

I

- IEEE802.MACID directory, 87
- interconnect fabric, 1, 5
 - adding an interface, 76
 - deleting an interface, 76
 - departments, 5
 - failover group, 6
 - managing, 75
 - printing configuration, 77
 - removing an interface, 77
 - workgroups, 5
- Interoperability, 4
- interoperability
 - Citrix, 4
 - HOBlink, 5
 - Tarantella, 4
 - white paper, 4

K

- key combination, 19

L

- log files
 - examining, 47
 - viewing messages logs, 47

M

- modules, 10
 - Registered, 10
 - ZeroAdmin, 10
- multihead groups
 - viewing all, 43

N

network

- adding an interface, 76
- deleting an interface, 76
- interconnect fabric, 1
- removing an interface, 77

NSC mobile session, 15, 26

NSC mobile session login, 16

NSCM session, 16

- disconnecting, 19
- enabling from Administration Tool, 23
- enabling from command line, 25
- logging in to, 17
- terminating, 19

O

online documentation

- accessing, 69

P

parallel peripherals, 87

PDA synchronization, 92

peripherals

- parallel, 87
- serial, 87

policies, 10

- changing, 31
- removing old, 75

power cycle, 3

power-on self test (POST)

- firmware module, 3

printer

- printing to attached, 90

printers

- non-PostScript, 92
- setting up, 90

Q

QuickLogin, 16

R

Registered module, 10

S

self-registration, 11, 26

serial peripherals, 87

service, 11

session, 11

- changes, 12
- finding, 68
- managing, 67
- viewing, 67

Session Manager, 11

Short Cut, 19

smart card

- adding, 51
- changing the probe order, 51
- deleting, 52
- viewing or listing configured, 49
- viewing the probe order, 50

Sun Directory Services (SunDS) daemon, 79

Sun Ray administration data, 27

- changing, 30

Sun Ray administration database

users

- adding a token ID, 60
- adding a user with token ID, 61
- deleting, 56
- deleting a token ID, 60
- displaying current properties, 57
- editing properties, 59
- enabling or disabling a token ID, 60
- finding, 62
- getting a token ID from a token reader, 62
- viewing by ID, 56
- viewing by name, 56
- viewing current, 57

Sun Ray appliance, 3

- finding sessions, 68
- firmware module, 3
- locking the screen, 80
- managing sessions, 67
- starting a print queue, 90
- updating and upgrading, 78
- viewing sessions, 67

- Sun Ray server
 - device directory, 87
 - ports, 4
 - software, 2
 - viewing all multihead groups, 43
- Sun Ray Services
 - resetting, 33
 - restarting, 33
- Sun Ray Settings
 - changing, 13
 - configuring, 81
- Sun Ray system, 1
 - example of, 2
 - security, 14

T

- Tarantella, 4
- token reader, 9
 - creating, 34
 - getting a token ID from, 62, 81
 - locating, 34

U

- utadm command, 75
- utadm -r command, 76
- utaudio command, 4
- utdetach command, 18, 19
- utfwadm command, 77
- utglpolicy command, 25, 26
- utpolicy command, 25, 26
- utpolicy -i clear command, 75
- utslaunch.properties command, 20
- utwall command, 23, 25

V

- virtual frame buffer, 3

W

- workgroups, 5

X

- xinitrc file, 80

Z

- ZeroAdmin module, 10