



# Sun Ray™ Server Software 2.0 Administrator's Guide

---

Sun Microsystems, Inc.  
4150 Network Circle  
Santa Clara, CA 95054 U.S.A.  
650-960-1300

Part No. 816-6753-10  
February 2003, Revision A

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

Copyright 2002, 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

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

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

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

Sun, Sun Microsystems, the Sun logo, Sun Ray, Sun WebServer, Sun Enterprise, Ultra, UltraSPARC, SunFastEthernet, Sun Quad FastEthernet, Java, JDK, HotJava, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

Netscape is a trademark or registered trademark of Netscape Communications Corporation.

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

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

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

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

---

Copyright 2002, 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.

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

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

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

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

Sun, Sun Microsystems, le logo Sun, Sun Ray, Sun WebServer, Sun Enterprise, Ultra, UltraSPARC, SunFastEthernet, Sun Quad FastEthernet, Java, JDK, HotJava, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

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

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

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

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



Adobe PostScript

# Contents

---

**Preface**   xiii

**1. Sun Ray System Overview**   1

Computing Model   1

The Sun Ray System   2

    Sun Ray Appliance   2

    Sun Ray Server Software   3

    Network Components   8

    Physical Connections   11

    Deployment Examples   12

Security Considerations   14

**2. Command-Line Interface**   15

Supported Commands   15

    ▼ To Stop Sun Ray Services   19

    ▼ To Start Sun Ray Services   19

Session Redirection   19

    ▼ To Redirect to a Different Server   19

    ▼ To Redirect an Appliance Manually   20

    ▼ To List Available Hosts   21

- ▼ To Select a Different Server 21
- Changing Policies 21
  - ▼ To Configure CAM Using the CLI 22
- Configuring Interfaces on the Sun Ray Interconnect Fabric 22
  - ▼ To Add an Interface 23
  - ▼ To Delete an Interface 23
  - ▼ To Print the Sun Ray Private Interconnect Configuration 24
  - ▼ To Add a LAN Subnet 24
  - ▼ To Delete a LAN Subnet 24
  - ▼ To Print Public LAN Subnets 24
  - ▼ To Remove All Interfaces and Subnets 24
- Managing Firmware Versions 25
  - ▼ To Update All the Appliances on an Interface 25
  - ▼ To Update an Appliance Using the Ethernet (MAC) Address 25
- Restarting the Sun Ray Data Store 26
  - ▼ To Restart Sun Ray Data Store 26
- Solaris Lock Screen for Detached Sessions 26
  - ▼ To Lock a Screen Using CDE 27
  - ▼ To Lock an OpenWindows Session 27
  - ▼ To Create a System-Wide Default for Screen Locking 27
- Managing Monitor Settings 28
- Configuring Hot Key Preferences 28
- Setting Hot Key Values 30
  - ▼ To Change the Hot Key for the Settings GUI 30
  - ▼ To Change the Hot Key Used to Detach NSCM Sessions 31
  - ▼ To Change the Hot Key Setting for a Single User 31
- Smart Card Configuration Files 32
  - ▼ To Load a Configuration File Into the Directory 32

Configuring and Using Token Readers 32

- ▼ To Configure a Token Reader 33
- ▼ To Get a Token ID From a Token Reader 34

Using the `utcapture` Tool 34

- ▼ To Start `utcapture` 35

### **3. Administration Tool 37**

Administration Data 38

Logging In 38

- ▼ To Log Into the Administration Tool 38
- ▼ To Change the Administrator's Password 40

Changing Policies 41

- ▼ To Change the Policy 42

Resetting and Restarting Sun Ray Services 43

- ▼ To Reset Sun Ray Services 43
- ▼ To Restart Sun Ray Services 43

Token Readers 44

Creating a Token Reader 44

- ▼ To Locate Token Readers 46
- ▼ To Get Information on a Token Reader 47

Managing Desktops 48

- ▼ To List All Desktops 48
- ▼ To Display a Desktop's Current Properties 48
- ▼ To List Currently Connected Desktops 48
- ▼ To View the Properties of the Current User 49
- ▼ To Search for Desktops 49
- ▼ To Edit a Single Desktop's Properties 50

Sun Ray Appliance Settings 51

- ▼ To Change the Sun Ray Settings 51

Managing Multihead Groups	52
▼ To View All Multihead Groups	52
Examining Log Files	55
▼ To View a Log File	56
Managing Smart Cards	56
▼ To View or List Configured Smart Cards	57
▼ To View The Smart Card Probe Order	58
▼ To Change the Smart Card Probe Order	59
▼ To Add a Smart Card	59
▼ To Delete a Smart Card	60
Sun Ray System Status	60
▼ To View the Sun Ray System Status	60
Administering Users	62
▼ To View Users by ID	62
▼ To View Users by Name	63
▼ To Delete a User	63
▼ To View Current Users	65
▼ To Display a User's Current Properties	65
▼ To Add a User	66
▼ To View the User's Sessions	67
▼ To Edit a User's Properties	67
▼ To Add a Token ID to a User's Properties	68
▼ To Delete a Token ID From a User's Properties	69
▼ To Enable or Disable a User's Token	69
▼ To Find a User	69
▼ To Get a Token ID From a Token Reader	70
Controlled Access Mode	71
▼ To Configure Controlled Access Mode	71

- ▼ To Select Additional Applications 72
- ▼ To Add or Edit Applications 73
- Managing Sessions 75
  - ▼ To Find Sun Ray Sessions 75
  - ▼ To View Sun Ray Sessions 77
- 4. Peripherals for Sun Ray Appliances 79**
  - Device Nodes and USB Peripherals 79
    - Device Nodes 80
    - Device Links 81
    - Device Node Ownership 81
    - Hot Desking and Device Node Ownership 81
  - Attached Printers 82
    - Printer Setup 82
    - Printers Other Than PostScript Printers 84
  - PDA Synchronization 84
    - PDASync for Solaris Application on Sun Ray Appliances 85
  - Adapters 86
- 5. Mobile Sessions (Hot Desking) 87**
  - NSCM Session 87
    - Sun Ray Mobile Session Login Dialog Box 88
      - ▼ To Log In to an NSCM Session 88
    - Disconnecting an Active NSCM Session 90
  - NSCM and Failover Groups 92
    - Load Balancing Between Servers 92
    - Connecting to Existing Sessions 92
    - Switching Between Servers 92
    - Escape Token Sessions 93

Considerations	93
Configuring the Authentication Manager for NSCM Sessions	93
▼ To Enable NSCM Sessions From the Administration Tool	94
▼ To Enable NSCM Sessions From a Command Line	96
<b>6. Encryption and Authentication</b>	<b>97</b>
Introduction	97
Security Configuration	98
Security Mode	98
Session Security	99
Security Status	100
Session Connection Failures	101
<b>7. Network Configuration</b>	<b>103</b>
Introduction	103
Network Infrastructure Requirements	104
Packet Loss	104
Latency	104
Out-of-Order Packets	104
DHCP Services	104
Network Topology	105
DHCP Configuration	106
<b>8. Monitoring the Sun Ray System</b>	<b>113</b>
Sun Management Center (SunMC) Software Features	113
SunMC Software Requirements	115
Installing the SunMC Software	116
Additional Sun Management Center Modules	119
Setting Up the Monitoring Environment	119
Setting Alarms	120



Setting Monitoring Guidelines	126
Sun Ray System Panel	126
Sun Ray Services Panel	128
Failover Group Panel	129
Interconnect Panel	130
Desktops Panel	131
Using Other Monitoring Programs	132
Removing the Sun Ray Module from SunMC	134
<b>9. Multihead Administration</b>	<b>135</b>
Multihead Groups	136
Multihead Screen Display	136
Display Resolution	137
Multihead Administration Tool	137
XINERAMA	141
Session Groups	142
Authentication Manager	142
<b>10. Controlled Access Mode</b>	<b>145</b>
Controlled Access Mode Functionality	145
Enabling Controlled Access Mode	145
Building the Controlled Access Mode Environment	148
Advanced Application Setup	153
Enabling Prototypes	153
Using Wrapper Scripts to Customize Controlled Access Mode Applications	154
Security and the Controlled Access Mode Environment	154
Failover	155
Localization	155

<b>11. Failover Groups</b>	<b>157</b>
Failover Group Overview	158
Setting Up IP Addressing	160
Setting Up Server and Client Addresses	160
Configuring DHCP	162
Group Manager	166
Redirection	167
Group Manager Configuration	167
Load Balancing	168
Setting Up a Failover Group	169
Primary Server	169
Secondary Server	170
Removing Replication Configuration	170
Viewing the Administration Status	171
Viewing Failover Group Status	171
▼ To View Failover Group Status	171
Sun Ray Failover Group Status Icons	172
Recovery Issues and Procedures	173
Primary Server Recovery	173
Secondary Server Recovery	176
Setting Up a Group Signature	176
Taking Servers Offline	177
<b>A. Troubleshooting</b>	<b>179</b>
Understanding OSD	179
OSD Icon Topography	179
Sun Ray Desktop Unit Startup	182
Firmware Download	185
Firmware Download Failed	186

Bus Busy	186
No Ethernet	187
Ethernet Address	187
Session Connection Failures	188
Card Read Error OSD	188
Prompt for Card Insertion OSD	189
Access Denied OSD	189
Wait for Session OSD	190
Wait Icon Cursor for Default Session Type	190
Patches	191
Authentication Manager Errors	191
Audio	194
Audio Device Emulation	194
Audio Malfunction	194
PDA Synchronization Issues	195
Performance Tuning	196
General Configuration	196
Applications	196
Sluggish Performance	197
Monitor Display Resolution Defaults to 640 x 480	197
Old Icons (Hourglass with Dashes Underneath) Appear on Display	198
Port Currently Owned by Another Application	198
Design Tips	198
Troubleshooting the Sun Management Center	199
No Sun Ray Object	199
▼ To Load the Sun Ray Module	199
No Sun Ray Module	200
▼ To Activate the Sun Ray Module	200

<b>B. Controlled Browser</b>	<b>201</b>
Controlled Browser Installation	201
▼ To Install the Controlled Browser	202
▼ To Remove the Controlled Browser	202
Controlled Browser Functionality	203
▼ To Setup the Controlled Browser in Control Access Mode Administration	204
Browser Printing	206
▼ To Print from the Browser	206
Adding Plug-ins to the Controlled Browser	208
Set Up Considerations	209
General Requirements and Other Considerations	210
Sample Plug-In Setup	211
<b>C. Sun Ray and Network Parameter Delivery (DHCP)</b>	<b>217</b>
Encapsulated Options	219
<b>Index</b>	<b>231</b>

# Preface

---

The *Sun Ray Server Software 2.0 Administrator's Guide* provides instructions for setting up, administering, monitoring, and troubleshooting a system of Sun Ray™ appliances and their server or servers. It is written for system administrators who are already familiar with the Sun Ray™ computing paradigm and have substantial networking knowledge. This guide may also be useful for those interested in customizing their Sun Ray systems.

---

## Before You Read This Book

This guide assumes that you have installed the Sun Ray Server Software on your server from the Sun Ray Server Software 2.0 CD or the Electronic Software Download (ESD) and that you have added the required patches.

---

## How This Book Is Organized

Chapter 1 gives an overview of the Sun Ray system.

Chapter 2 describes the command-line interface.

Chapter 3 describes the Administration Tool.

Chapter 4 describes peripherals for Sun Ray appliances.

Chapter 5 describes mobile sessions, also known as Hot Desking.

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

Chapter 7 discusses network requirements, including LAN, VLAN, and dedicated interconnect options, switch requirements, and other network topology issues.

Chapter 8 describes how to monitor the Sun Ray system using Sun<sup>TM</sup> Management Center software.

Chapter 9 describes how to implement multihead and XINERAMA on a Sun Ray system.

Chapter 10 describes how to customize Sun Ray Server Software for controlled access mode.

Chapter 11 discusses failover groups.

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

Appendix B shows how to install a controlled browser.

Appendix C contains a listing of Sun Ray parameter symbol values defined in the DHCP table and a brief discussion of encapsulated options.

This manual also contains a glossary and an index.

---

## Using UNIX Commands

This document does not contain information on basic UNIX<sup>®</sup> commands and procedures, such as shutting down the system, booting the system, or configuring devices. This document does, however, contain information about specific Sun Ray system commands.

---

# Typographic Conventions

Typeface	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. % You have mail.
<b>AaBbCc123</b>	What you type, when contrasted with on-screen computer output	% <b>su</b> 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 2.0 Installation and Configuration Guide</i>	816-7396-10
Release Notes	<i>Sun Ray Server Software 2.0 Release Notes</i>	816-7398-10

---

## Accessing Sun Documentation

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

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

---

## 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](mailto:docfeedback@sun.com)

Please include the part number (816-6753-10) of your document in the subject line of your email.



# Sun Ray System Overview

---

The current generation of Sun Ray thin-client appliances and server software represents the highest evolution to date of client-server computing. Although the idea of thin client computing has been considered interesting for many years, Sun Ray is the first implementation to offer both workstation-like user functionality and sufficient speed and reliability to be suitable for mission-critical applications. With the addition of LAN deployment, Sun Ray is now gaining acceptance in large-scale, distributed enterprises in addition to the schools, universities, research laboratories, and business units of large companies where it has been developed and tested.

---

## Computing Model

The Sun Ray system employs a network-dependent computing model in which all computing is performed on a server, with input and output data passed back and forth between the Sun Ray server and the Sun Ray appliances.

User sessions—groups of services controlled by the Session Manager and associated with a user through an authentication token—reside on a server and are directed to a Sun Ray appliance. Because Sun Ray appliances are stateless, a user's session can be redirected to any Sun Ray appliance on the appropriate network or subnetwork when that user logs in or inserts a smart card; that is, the session follows the user to the new appliance. This *session mobility* is the key architectural feature that enables *hot desking*—the ability of users to access their sessions from any appliance on their network.

In previous versions of Sun Ray Server Software, mobile sessions were possible only with smart cards. Beginning with version 1.3, it became possible to enable hot desking with or without smart cards.

Because effective client-server network traffic often relies on the rapid movement of large numbers of packets, an optimal Sun Ray implementation requires a well-designed network. Most large implementations include at least one *failover group* to ensure uninterrupted service whenever a server goes off-line.

Once a failover group is set up, Sun Ray Server Software provides automatic load balancing to optimize performance by spreading the computing load among the servers in the group. Whenever a server fails, the Group Manager on each remaining server tries to distribute the failed server's sessions evenly among the remaining servers. The load balancing algorithm takes into account each server's load and capacity (number and speed of its CPUs) so that larger or less heavily loaded servers host more sessions. These concepts are addressed in Chapter 11 and in the *Sun Ray Server Software 2.0 Installation and Configuration Guide*.

---

## The Sun Ray System

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

### Sun Ray Appliance

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

- 24-bit, 2-D accelerated graphics up to 1280x1024 resolution at 85 Hz (640 x 480 at 60 Hz is the lowest resolution)
- Multichannel audio input and output capabilities
- Smart card reader
- USB ports that support hot-pluggable peripherals
- EnergyStar™ compliance
  - No fan, switch, or disk
  - Very low power consumption

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

From the point-of-view of network servers, Sun Ray appliances are identical except for their Ethernet MAC addresses. If an appliance ever fails, it can easily be replaced.

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

To power cycle a Sun Ray appliance, disconnect the power cord, wait 15 seconds, then reconnect the power cord.

## Multihead

Sun Ray Server Software supports the use of multiple displays connected to a single keyboard and pointer. This functionality is important for users who need extra screen real estate, for instance, to monitor many applications or systems simultaneously or to accommodate a single application, such as a large spreadsheet, across multiple screens. The fact that each DTU has a single frame buffer does not limit the use of multiple screens; the administrator can set up multihead groups, consisting of two or more DTUs, for those users who need them. Administration of multihead groups is explained in Chapter 9.

## Firmware Module

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

## Sun Ray Server Software

Sun Ray server software allows the administrator to configure network connections, select an authentication protocol, administer users, define desktop properties, monitor the system, and troubleshoot a wide variety of administration problems.

Sun Ray server software includes:

- User authentication and access control
- Encryption between the Sun Ray server and appliances
- Session management
- Device management

- System administration tools
- Virtual device drivers for all supported or optimized rendering APIs

Sun Ray server software enables user 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 also permits users to access Microsoft Windows NT applications.

## Authentication Manager

The Authentication Manager implements the chosen policies for identifying and authenticating users on Sun Ray appliances. The Authentication Manager uses pluggable components called *modules* to implement various site-selectable authentication *policies*.

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 sends the user's token information to the Authentication Manager 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 for the user, which takes the user to the `dtlogin` screen.

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

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

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

The modules are:

- StartSession

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

- Registered

The token is accepted *only* 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

The administrator assigns 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 registered centrally. If a token has been registered but disabled, the user cannot re-register the token; the user must contact the site administrator to re-enable the token.

## Sessions and Services

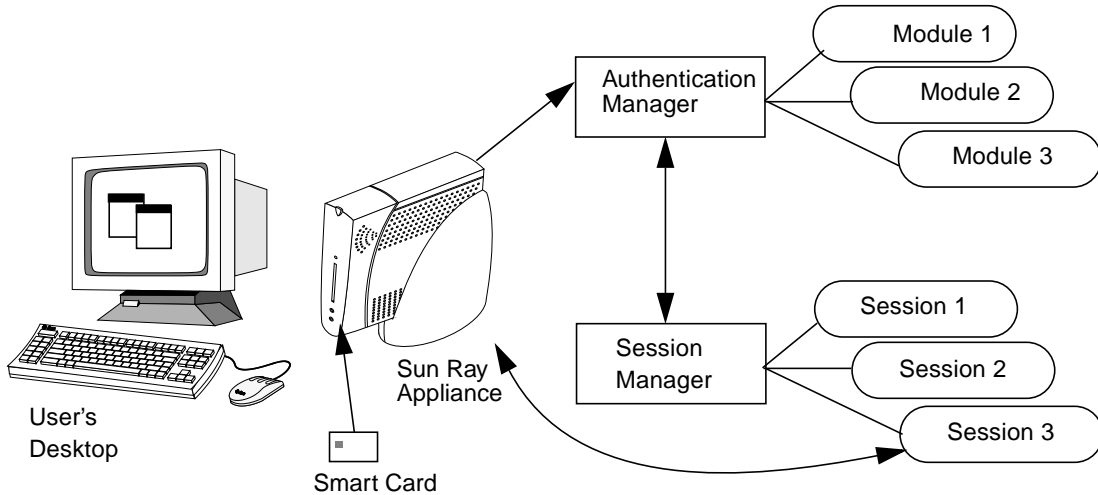
A *session* consists of a group of services controlled by the Session Manager.

The session is associated with a user through an authentication token. A *service* is any application that can 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 takes authentication only from authorized Authentication Managers listed in the `/etc/opt/SUNWut/auth.permit` file.



**FIGURE 1-1** Authentication and Session Manager Interaction

The steps below describe how the process starts and ends:

1. After a user's token is authenticated, the Authentication Manager determines whether 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 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 an intruder to use `xprop` to capture a user’s session ID. This action can expose the user’s screen images and keyboard input to anyone interested.

---

---

**Tip** – Use `xhost username@system` to enable only those people you specify to access the display and the user’s appliance.

---

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.

---

**Note** – The Session Manager daemon must continue running all the time. To verify that it is running, use the `ps` command and look for `utssessiond`.

---

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

## User and Device Administration

The Sun™ Management Center (SunMC) software monitors managed objects in the Sun Ray system. Objects that can be managed by default include the Sun Ray system itself, Sun Ray services, failover groups, interconnects, and desktops.

Each managed object is monitored separately and has independent alarm settings.

Sun Management Center software also monitors Sun Ray Server Software daemons that authenticate users, start sessions, manage devices, and handle DHCP services. Chapter 8 describes how to use the SunMC to monitor a Sun Ray system. For problems with the SunMC, see “Troubleshooting the Sun Management Center” on page 199.

## CLI and Admin GUI

Sun Ray Server Software has both a command-line interface (CLI) and a graphical user interface (GUI) for administrative functions. The Command-Line Interface (CLI) is the recommended interface for enabling assistive technologies; the GUI is provided for convenience.

## Data Store

In place of the old Sun Directory Service (Sun DS), Sun Ray Server Software 2.0 provides a private data store service, the Sun Ray Data Store (SRDS). No port conversion is required unless there is a need to continue to run SunDS on a recently upgraded 2.0 server.

## Controlled Access (Kiosk) Mode

Sun Ray appliances are becoming more common in public locations, such as airports, where anonymous users have limited access to specific applications. See Chapter 10 for details.

## Controlled Browser

For publicly accessed Sun Ray appliances, Sun Ray Server Software provides a browser environment with minimal risk of server security compromise. The browser is set up to provide a controlled and secure environment. In this context, Netscape Navigator functions normally with the exception of disabled downloads and a new GUI print interface to the command-line print interface. The controlled browser is described in some detail in Appendix B.

## Network Components

The Sun Ray system offers simplified administration by relying on the most advanced developments in client-server computing. Centralized computing and administration, inexpensive hardware components, and innovative use of smart card technology make Sun Ray the platform of choice in an increasing range of network configurations.

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

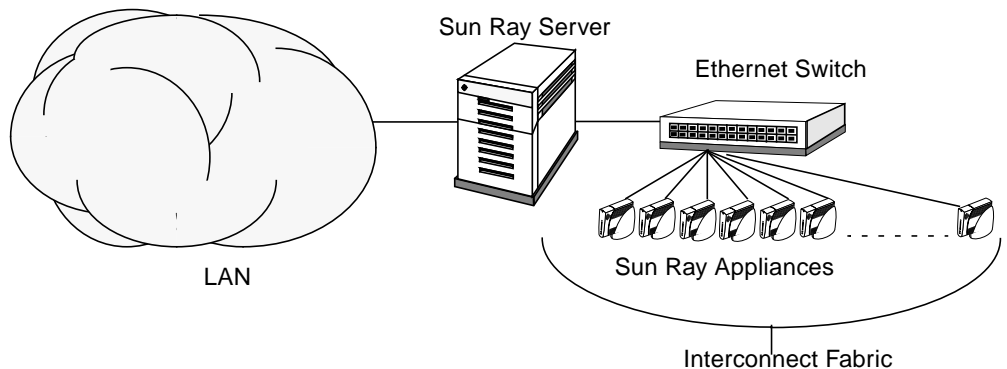


- Dedicated interconnect
- VLAN (Virtual Local Area Network)
- LAN (Local Area Network), with or without network routers

Various types of network configuration are discussed in Chapter 7.

## Sun Ray Interconnect Fabric

Historically, most Sun Ray interconnects have been implemented with physically dedicated Ethernet networks or logically dedicated networks. Beginning with the 2.0 release, Sun Rays can be deployed on existing Local Area Network (LAN) infrastructure, eliminating the requirement for a dedicated interconnect.



**FIGURE 1-2** Sun Ray System with a Dedicated Interconnect Fabric

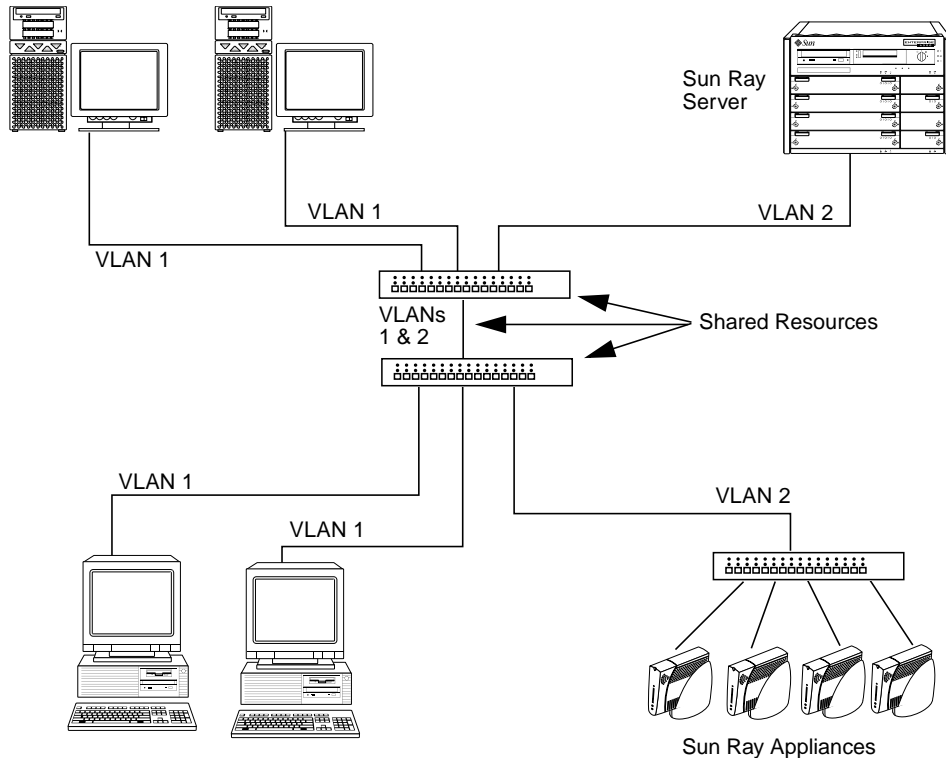
The Sun Ray interconnect fabric is based on 10/100BASE-T Ethernet technology, using layer-2 or layer-3 switches and Category 5 wiring. Each Sun Ray appliance is attached to the interconnect fabric through its built-in 10/100BASE-T interface.

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

## VLAN Implementation

VLANs logically partition a single physical interconnect into two or more broadcast domains. VLANs are commonly configured to implement virtual subnets in a shared physical interconnect. However, because VLANs must share backplane and link bandwidth, they are not true dedicated interconnects.

Implementing a Sun Ray interconnect through VLANs creates a logically dedicated connection, but can also mean sharing physical resources with uncontrolled traffic that is not Sun Ray appliance traffic. These resources could be the limited backplane bandwidth within a switch or on a link that carries multiple VLANs between switches (see FIGURE 1-3). If these resources are consumed by other devices, significant amounts of Sun Ray appliance traffic might be dropped and the results seen as horizontal bands or blocks on the user's display.



**FIGURE 1-3** Example of Shared Physical Resources in Multiple VLANs Configuration

Since switch manufacturers configure their products differently, please refer to the documentation provided with your switch and refer all questions relating to setting up or configuring VLANs to your switch manufacturer.

## LAN Implementation

Sun Ray Server Software 2.0 is the first release to support LAN implementations. With Sun Rays deployed on a LAN, users can exercise session mobility across a much larger “domain”—a huge convenience. Although it is beyond the scope of this

manual to provide step-by-step instructions for configuring different types of local area networks, the most common configurations are discussed and illustrated in Chapter 7 and in the *Sun Ray Server Software 2.0 Installation and Configuration Guide*.

## DHCP

For certain large-scale implementations, and especially where they already exist on a network that will support Sun Ray appliances, it may be desirable to use separate dynamic host configuration protocol (DHCP) servers for tasks such as assigning IP addresses and network parameters to the appliances. The use of separate DHCP servers is not required, but where they already exist, they can be used to reduce the load on dedicated Sun Ray servers and provide better overall performance. These questions are discussed in Chapter 7 and Appendix C.

## Physical Connections

The physical connection between the Sun Ray server and Sun Ray clients relies on standard switched Ethernet technology.

Implementing the interconnect with a physically dedicated and isolated set of Ethernet switches is recommended because it is easy and reliable. For instance:

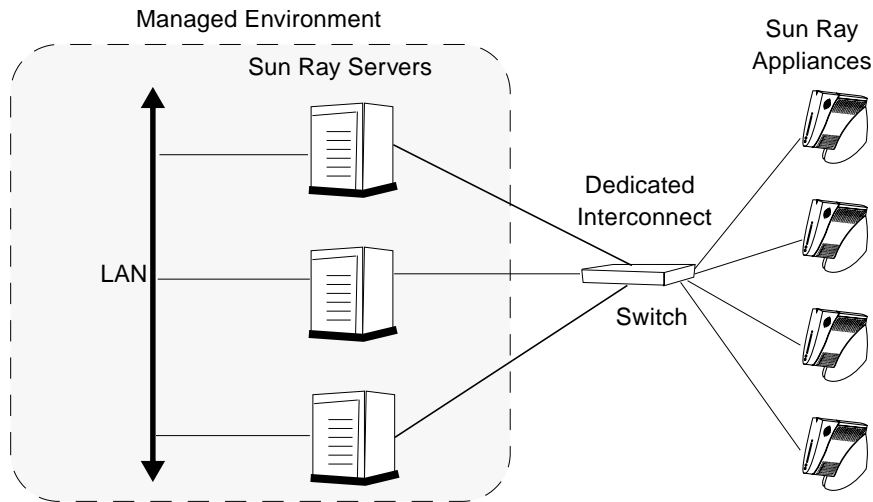
- Only layer 2 switches are required.
- The only switch configuration required is to enable fast boot times.
- No ongoing switch configuration and management is required.
- Issues of bandwidth and poor topology are greatly reduced.

To boost the power of the interconnect and shield Sun Ray appliance users from the network interaction taking place at every display update, 100 Mbps switches are preferred.

There are two basic types of 100 Mbps switches:

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

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



**FIGURE 1-4** The Sun Ray System in a Dedicated Interconnect Configuration

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

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

While 10 Mbps services are supported, the preferred configuration is a 100BASE-T, full-duplex network to maximize interconnect quality of service and the number of Sun Ray appliances supported.

## Deployment Examples

There is no physical or logical limit to the ways that a Sun Ray system can be configured. The following sections offer some typical examples.

### Workgroup Scenario

For small workgroups with between five 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. With five or fewer appliances, a wireless interconnect works acceptably at 10 Mbytes.

For example, in FIGURE 1-2 a Sun Enterprise™ 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 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 (see FIGURE 1-5).

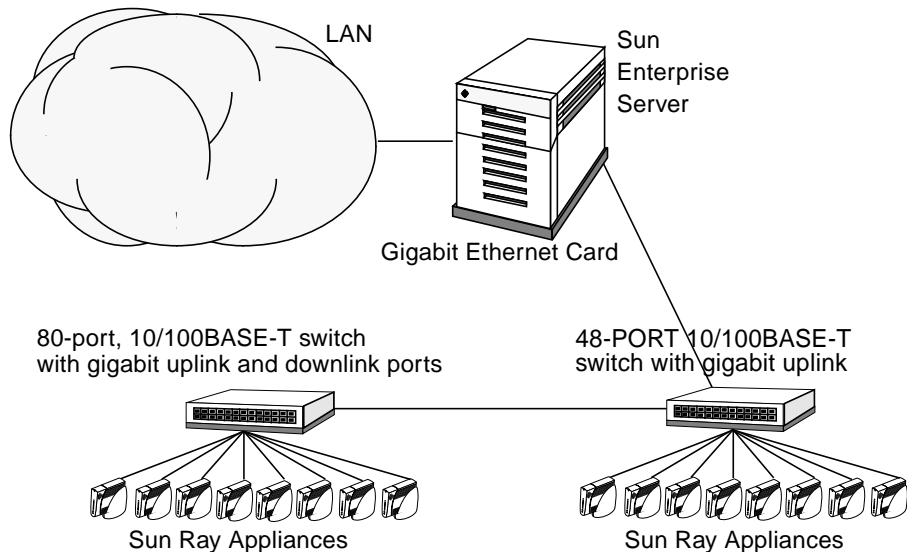


FIGURE 1-5 Department Scenario

## Failover Group Scenario

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

When a server in a failover group goes down, whether for maintenance, a power outage, or any other reason, each Sun Ray appliance connected to it reconnects to another server in the failover group. The appliance connects to a previously existing

session for the current 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, who must log in again to create a new session. The session on the failed server is lost. Failover groups are discussed in Chapter 11 as well as in the *Sun Ray Server Software 2.0 Installation and Configuration Guide*.

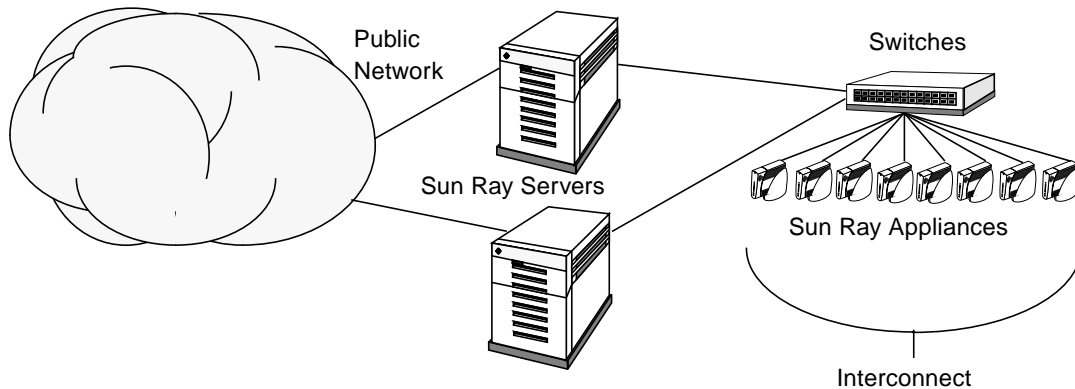


FIGURE 1-6 Simple Failover Group

---

## 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 send packets only to the proper output port, a snooper plugged into another port receives no unauthorized data. If the server and wiring closet are secure, the last step is switched, and the appliance is plugged directly into the wall jack, then it is virtually impossible to intercept communications between the server and the appliance.

Before release 2.0, the Sun Ray system did not encrypt its communications; thus, anyone who gained access to the data had access to what was typed and displayed at each Sun Ray appliance. This potential security flaw has been corrected for the 2.0 release. For more information, see Chapter 6.

# Command-Line Interface

---

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

This chapter contains the following information:

- “Supported Commands” on page 15
- “Session Redirection” on page 19
- “Changing Policies” on page 21
- “Configuring Interfaces on the Sun Ray Interconnect Fabric” on page 22
- “Managing Firmware Versions” on page 25
- “Restarting the Sun Ray Data Store” on page 26
- “Solaris Lock Screen for Detached Sessions” on page 26
- “Configuring Hot Key Preferences” on page 28
- “Setting Hot Key Values” on page 30
- “Smart Card Configuration Files” on page 32
- “Using the `utcapture` Tool” on page 34

---

## Supported Commands

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

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

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

or type:

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

**TABLE 2-1** Supported Commands

Command	Definition
utaction	The <code>utaction</code> program provides a way to execute commands when a Sun Ray appliance session is connected or disconnected.
utadm	The <code>utadm</code> command manages the private network and DHCP (Dynamic Host Configuration Protocol) configuration for the Sun Ray interconnect.
utcapture	The <code>utcapture</code> command connects to the Authentication Manager and monitors packets sent and packets dropped between the Sun Ray server and the Sun Ray appliances.
utcard	The <code>utcard</code> command allows configuration of different types of smart cards in the Sun Ray administration database.
utconfig	The <code>utconfig</code> command performs the initial configuration of the Sun Ray server and supporting administration framework software.
utcrypto	The <code>utcrypto</code> command is a utility for security configuration.
utdesktop	The <code>utdesktop</code> command allows the user to manage Sun Ray appliance desktop units connected to the Sun Ray server that the command is run on.
utdetach	The <code>utdetach</code> command disconnects the current non-smart card mobile session or authenticated smart card session from its respective Sun Ray 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.
utdssync	The <code>utdssync</code> command converts the port number for the Sun Ray Data Store service to the new default port on servers in a failover group, then forces all servers in the group to restart Sun Ray services.
utfwadm	The <code>utfwadm</code> command manages firmware versions on the Sun Ray appliances.
utfwsync	The <code>utfwsync</code> command refreshes the firmware level on the Sun Ray appliances to what is available on the Sun Ray servers in a failover group. It then forces all the Sun Ray appliances within the group to restart.



**TABLE 2-1** Supported Commands (*Continued*)

Command	Definition
<code>utglpolicy</code>	The <code>utglpolicy</code> command, which gets or sets group <code>utpolicy</code> options, is deprecated as of the 2.0 release. Please use <code>utpolicy</code> , which sets group policy automatically, then follow it with a reset or restart of services.
<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 Data Store <code>rootpw</code> used by Sun Ray to a value based on the group signature. Although <code>utgroupsig</code> sets the <code>rootpw</code> in the <code>utdsd.conf</code> file., it does <i>not</i> set the admin password in the Admin database.
<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.
<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 import/export kiosk configuration information into the LDAP database.
<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 sets and reports the policy configuration of the Sun Ray Authentication Manager, <code>utauthd(1M)</code> . In the 2.0 and subsequent releases, this command's <code>-i</code> and <code>-t</code> options are deprecated. Please continue to use the <code>utpolicy</code> command for policy changes, but use the <code>utrestart</code> command instead of <code>utpolicy -i</code> , and use <code>utreader</code> instead of <code>utpolicy -t</code> .
<code>utpreserve</code>	The <code>utpreserve</code> command saves existing Sun Ray Server Software configuration data to the <code>/var/tmp/SUNWut.upgrade</code> directory.
<code>utpw</code>	The <code>utpw</code> command changes the Sun Ray administrator password (also known as the UT admin password) used by the Web-based and command-line administration applications.
<code>utquery</code>	The <code>utquery</code> command collects DHCP information from the Sun Ray appliances.
<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.utrcmd</code> daemon on the remote <code>hostname</code> and executes the specified <i>command</i> with the specified arguments, <i>args</i> (if any).
<code>utreader</code>	The <code>utreader</code> command is used to add, remove, and configure token readers.
<code>utreplica</code>	The <code>utreplica</code> command configures the Sun Ray Data Store server to enable replication of administered data from a designated primary server to each secondary server in a failover group. The new <code>-z</code> option is useful for updating the port number.

**TABLE 2-1** Supported Commands (*Continued*)

Command	Definition
<code>utresadm</code>	The <code>utresadm</code> command allows an administrator to control the resolution and refresh rate of the video monitor signal (persistent monitor settings) produced by the Sun Ray unit.
<code>utresdef</code>	The <code>utresdef</code> command lists the monitor resolutions and refresh rates that can be applied to Sun Ray units through the <code>utresadm</code> command.
<code>utrestart</code>	This command is highly recommended as a substitute for the old <code>utglpolicy</code> and <code>utpolicy -i</code> commands. Use <code>utrestart</code> instead of <code>utpolicy -i</code> .
<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.
<code>utsession</code>	The <code>utsession</code> command lists and manages Sun Ray sessions on the local Sun Ray server.
<code>utset</code>	Use <code>utset</code> to view and change Sun Ray appliance settings.
<code>utsettings</code>	The <code>utsettings</code> command opens a Sun Ray Settings dialog box that allows the user to view or change audio, visual, and tactile settings for the Sun Ray appliance.
<code>utsunmc</code>	The <code>utsunmc</code> command adds the Sun Ray Server Software 2.0 module to the Sun Management Center (SunMC) and loads it to permit monitoring of Sun Ray Server Software. The <code>utsunmc</code> command can also remove the Sun Ray Server Software 2.0 module from SunMC.
<code>utsunmcinstall</code>	Use <code>utsunmcinstall</code> to install and uninstall the Sun Ray module for SunMC on a SunMC server where Sun Ray Server Software is not installed.
<code>utswitch</code>	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.
<code>utsvc</code>	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. Use <code>utrestart</code> instead of <code>utsvc</code> .
<code>utuser</code>	The <code>utuser</code> command allows the administrator to manage Sun Ray users registered on the Sun Ray server that this command is run on. It also provides information on the currently inserted token (smart card) for a specified DTU that is configured as a token reader.
<code>utwall</code>	The <code>utwall</code> utility sends a message or an audio file to users having an Xsun (X server unique to Sun Ray) process. The messages can be sent in email and displayed in a pop-up window.
<code>utxconfig</code>	The <code>utxconfig</code> program provides X server configuration parameters for users of Sun Ray appliance sessions.
<code>utxset</code>	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:**

```
# /opt/SUNWut/sbin/utrestart
```

This procedure starts Sun Ray services without clearing existing sessions.

Or

- **Type:**

```
# /opt/SUNWut/sbin/utrestart -c
```

This procedure starts Sun Ray services and clears existing sessions.

---

# Session Redirection

In addition to automatic redirection after you authenticate yourself, you can use the `utselect` graphical user interface (GUI) or the `utswitch` command to redirect your session to a different server.

## ▼ To Redirect to a Different Server

- **From a shell window on the client, type:**

```
% /opt/SUNWut/bin/utselect
```

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

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

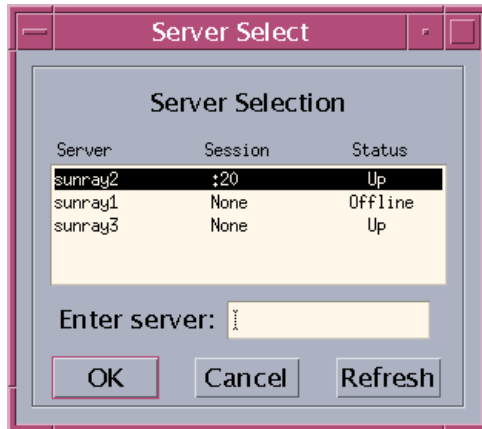


FIGURE 2-1 The Server Selection (utselect) GUI

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

---

**Note** – If only one server in the failover group is up, it is displayed in the `utselect` GUI. However, if you set `selectAtLogin` to `true` in the `/etc/opt/SUNWut/auth.props` file, the GUI is not displayed, because there appears to be only one server in the failover group.

---

## ▼ To Redirect an Appliance Manually

- From a shell window on the client, type:

```
% /opt/SUNWut/bin/utswitch -h host [ -k token ] [ -s sid ]
```

where *host* is the host name or IP address of the Sun Ray server to which the selected appliance is redirected.

## ▼ To List Available Hosts

- From a shell window, type:

```
% /opt/SUNWut/bin/utswitch -l
```

Hosts available from the Sun Ray appliance are listed.

## ▼ To Select a Different Server

- In a shell window, type:

```
% /opt/SUNWut/bin/utswitch -t
```

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

---

# Changing Policies

The `utglpolicy` command and the `utpolicy` options `-i` and `-t` are deprecated in release 2.0. Consequently, please:

- Use the `utrestart` command instead of the `-i` option to `utpolicy`.
- Use the `utreader` command instead of the `-t` option to `utpolicy`.
- Use the `utpolicy` command to make policy changes.

When you set a policy with `utpolicy`, the group policy is set automatically, so all you need to do at that point is to reset or restart services. This eliminates the need for `utglpolicy`.

---

**Tip** – Use the `utrestart -c` command instead of rebooting the server.

---

**TABLE 2-2** `utrestart` Commands

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

## ▼ To Configure CAM Using the CLI

- As superuser, type the `utpolicy` command for your authentication policy with the addition of the `-k` argument. For example:

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

---

# Configuring Interfaces on the Sun Ray Interconnect Fabric

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

---

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

---

---

**Tip** – If you issue a <CTRL>C signal while performing `utadm` configuration, `utadm` may not function correctly the next time you invoke it. To correct this condition, type: `dhtadm -R`.

---

## ▼ To Add an Interface

- **Type:**

```
# /opt/SUNWut/sbin/utadm -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. If you choose to specify your own subnet, make sure it is not already in use.

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

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

```
hme[0-9], qfe[0-3]
```

## ▼ To Delete an Interface

- **Type:**

```
# /opt/SUNWut/sbin/utadm -d interface_name
```

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

## ▼ To Print the Sun Ray Private Interconnect Configuration

- Type:

```
# /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.

## ▼ To Add a LAN Subnet

- Type:

```
# /opt/SUNWut/sbin/utadm -A subnet_number
```

## ▼ To Delete a LAN Subnet

- Type:

```
# /opt/SUNWut/sbin/utadm -D subnet_number
```

## ▼ To Print Public LAN Subnets

- Type:

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

## ▼ To Remove All Interfaces and Subnets

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 structures relating to all of the Sun Ray interfaces and subnets.

---

## Managing Firmware Versions

Use the `utfwadm` command to keep the firmware version in the PROM on Sun Ray appliances synchronized with that on the server.

---

**Note** – If you define the DHCP *version* variable, then when you plug in a new appliance, the appliance's firmware is changed to the firmware version on the server.

---

### ▼ To Update All the Appliances on an Interface

- **Type:**

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

---

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

---

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

- **Type:**

```
# /opt/SUNWut/sbin/utfwadm -A -e MAC_address -n interface
```

---

# Restarting the Sun Ray Data Store

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

## ▼ To Restart Sun Ray Data Store

### 1. Stop the Sun Ray services:

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

### 2. Stop the Sun Ray Data Store daemon:

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

### 3. Restart the Sun Ray services:

```
# /opt/SUNWut/sbin/utrestart
```

---

# 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
```

---

# Managing Monitor Settings

Sun Ray users can modify their screen resolution settings by invoking `utsettings`. Any resolution selections they make within a session remain effective whenever the session is displayed on that particular DTU. The selection is not lost if the unit goes into power-save mode or is power-cycled.

Settings selected through `utsettings` apply *only* to the DTU where `utsettings` is run; *hot desking* to another DTU does not bring the new timing along as part of the session. However, the selected timing is retained and used again if a user hot desks back to the original DTU.

If the session is associated with a personal mobile token (a smartcard or an NSCM credential), then `utsettings` offers to make the selected timing permanent. If a user accepts that offer, then the timing is retained and reused on that user's subsequent personal mobile token sessions on the same DTU.

In addition, the administrator may use the `utresadm` command to:

- Arrange for a particular monitor timing to be used whenever a specific token is presented on a specific DTU.
- Arrange for a particular monitor timing to be used on a specific DTU, regardless of the token that is presented at the DTU.
- Arrange for a particular monitor timing to be used on all DTU's regardless of the token that is presented at the DTU.

Any conflict among settings is resolved in favor of the most tightly-specified configuration rule. That is, a configuration record for a specific token at a specific DTU takes precedence over a record for *any token* at that specific DTU, and a configuration record for *any token* at a specific DTU takes precedence over a record for *any token* at *any DTU*.

---

# Configuring Hot Key Preferences

You can configure hot keys for various Sun Ray utilities. The scope for these hot keys can be:

- System-wide default setting
- User default setting
- System-wide mandatory setting

To support these levels of customization, the utilities look for the properties files in TABLE 2-3, in the following order, at startup:

**TABLE 2-3 Sun Ray Settings Properties Files**

File	Defaults	Description
/etc/opt/SUNWut/utslaunch_defaults.properties	System-wide	This file contains helpful default properties. Any properties specified here override any defaults built into the application itself.
\$HOME/.utslaunch.properties	User	This file contains the user's preferred values, which override any application or site-wide defaults.
/etc/opt/SUNWut/utslaunch_mandatory.properties	System-wide mandatory	This file contains site-wide mandatory settings that cannot be overridden by the user. These properties override any application, site-wide, or user defaults.

If your policy is for all appliances to use a standard hot key, use the system-wide mandatory defaults file to specify this standard key. This prevents users from specifying their own hot key preferences.

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

`<utility_name>.hotkey=value`

where `<utility_name>` is the name of the utility, such as `utsettings` or `utdetach`, and `value` is a valid X keysym name preceded by one or more of the supported modifiers (Ctrl, Shift, Alt, Meta) in any order.

Values are shown in the following table.

**TABLE 2-4 Sun Ray Server Software 2.0 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 detaches a non-smart card mobility session.
Mute+Softer+Louder	This displays the appliance's MAC address.
Ctrl+Power Key	This cycles power.

Users can configure both Shift+Props and Shift+Pause.

---

## Setting Hot Key Values

### ▼ To Change the Hot Key for the Settings GUI

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. Users can still specify their preferences in the user defaults file.

Use this procedure to modify the settings GUI for all users on a server.

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

---

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

---

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

The # comments out the first hot key property.

```
# utdetach.hotkey=Shift Pause
```

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

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

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

The new hot key takes effect when the next user logs in. The next user to log in uses the new hot key to display the Sun Ray Settings screen. Users who were logged in before you changed the hot key continue to use the old value.

## ▼ To Change the Hot Key Used to Detach NSCM Sessions

---

**Note** – This resembles the procedure for changing the hot key for the settings GUI except for Step 3.

---

1. **As superuser, open the** `/etc/opt/SUNWut/utslaunch_defaults.properties` **file in a text editor.**
2. **Locate the original hot key entry for the utsettings utility and place a # in front of it to comment it out.**

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

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

```
utdetach.hotkey=Alt F9
```

## ▼ 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.**

---

**Note** – You can modify other hot keys in a similar fashion.

---

---

# Smart Card Configuration Files

---

**Tip** – Use the Administration Tool or the `utcard` command to add additional smart card vendor configuration files.

---

Smart card configuration files are available from a variety of sources, including Sun.

## ▼ To Load a Configuration File Into the Directory

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

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

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

---

# Configuring and Using Token Readers

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

In the example configuration in FIGURE 2-2, the second appliance 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.

---



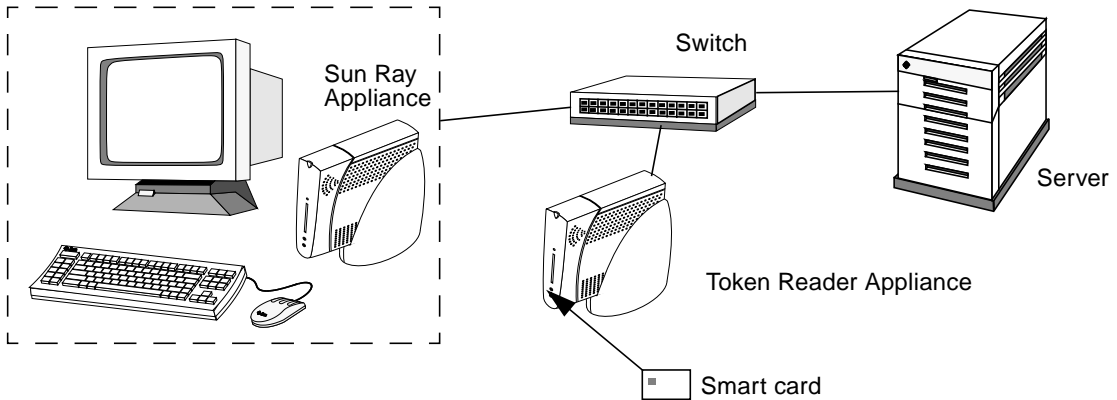


FIGURE 2-2 Using a Token Reader to Register Smart Cards

## ▼ To Configure a Token Reader

The `utreader` command specifies an appliance for registering smart cards. When a DTU is configured as a token reader, inserting or removing a smart card does not cause session mobility to occur; instead, any session connected to the DTU remains connected to that DTU over a card movement event.

Token reader mode is useful when you want to determine the raw token ID of a smart card. For example, to configure the DTU with MAC address `0800204c121c` as a token reader, issue the following `utreader` command:

```
# /opt/SUNWut/sbin/utreader -a 0800204c121c
```

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

```
# /opt/SUNWut/sbin/utreader -d 0800204c121c
```

To unconfigure all token readers on this server:

```
# /opt/SUNWut/sbin/utreader -c
```

## ▼ To Get a Token ID From a Token Reader

- Type the following command:

```
# /opt/SUNWut/sbin/utuser -r Token Reader
```

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

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

---

## Using the `utcapture` Tool

The `utcapture` tool connects to the Authentication Manager and collects data about the packets sent and packets dropped between the Sun Ray server and the appliance. This data in TABLE 2-5 is then displayed on the screen in the following format:

TABLE 2-5 Data Elements Displayed

Data Element	Description
TERMINALID	The MAC address of the appliance
TIMESTAMPM	The time the loss occurred in year-month-day-hour-minute-second format. Example: 20021229112512
TOTAL PACKET	Total number of packets sent from server to appliance
TOTAL LOSS	Total number of packets reported as lost by appliance
BYTES SENT	Total number of bytes sent from server to appliance
PERCENT LOSS	Percentage of packets lost between the current and previous polling interval
LATENCY	Time in milliseconds for a round trip from appliance to server.

---

**Tip** – If Sun Ray appliance traffic loss is more than .1%, allocate higher priority to the VLAN that carries Sun Ray appliance traffic. For more information on how to change the priority, please refer to the manufacturer’s documentation for your switch.

---

The following `utcapture` options are supported:

**TABLE 2-6** `utcapture` Options

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

## ▼ To Start `utcapture`

From a command line, enter one of the following commands

```
% /opt/SUNWut/sbin/utcapture -h
```

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

```
% /opt/SUNWut/sbin/utcapture
```

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

```
% /opt/SUNWut/sbin/utcapture -r > raw.out
```

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

```
% /opt/SUNWut/sbin/utcapture -s sunray_server5118.eng \  
080020a893cb 080020b34231
```

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

```
% /opt/SUNWut/sbin/utcapture -i raw-out.txt
```

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

# Administration Tool

---

You can use the Administration Tool to administer Sun Ray users and appliances, but the Command-Line Interface (CLI), documented in Chapter 2, is the recommended interface for enabling assistive technologies.

This chapter is divided into the following sections:

- “Administration Data” on page 38
- “Logging In” on page 38
- “Changing Policies” on page 41
- “Resetting and Restarting Sun Ray Services” on page 43
- “Token Readers” on page 44
- “Managing Desktops” on page 48
- “Sun Ray Appliance Settings” on page 51
- “Managing Multihead Groups” on page 52
- “Examining Log Files” on page 55
- “Managing Smart Cards” on page 56
- “Sun Ray System Status” on page 60
- “Administering Users” on page 62
- “Controlled Access Mode” on page 71
- “Managing Sessions” on page 75

---

**Note** – This chapter describes a standalone server. Servers in failover groups are discussed in Chapter 11.

---

---

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

---

**Tip** – To avoid operational errors, do not modify data except with the Administration Tool.

---

---

## Logging In

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

### ▼ 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`

---

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

---

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).

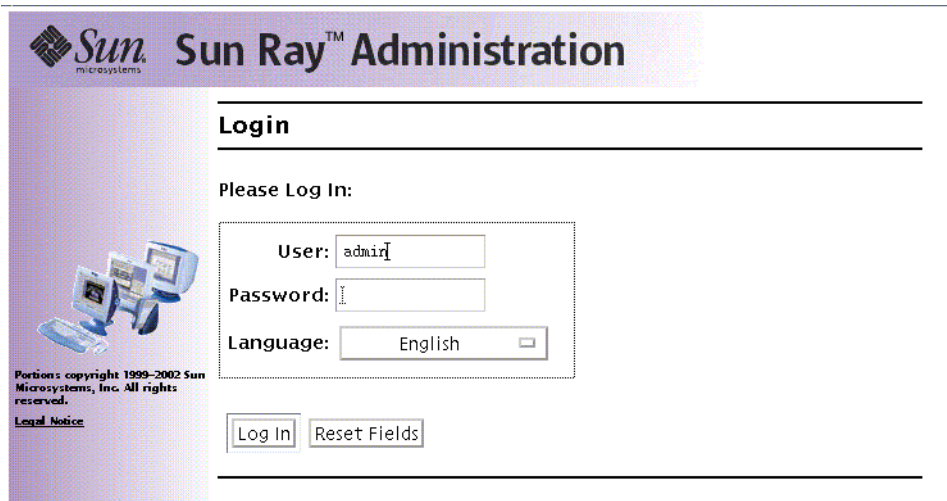


FIGURE 3-1 Login Window

4. Enter the administrator user name `admin` and the administration password you specified when you configured the Sun Ray Server Software.

---

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

---

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

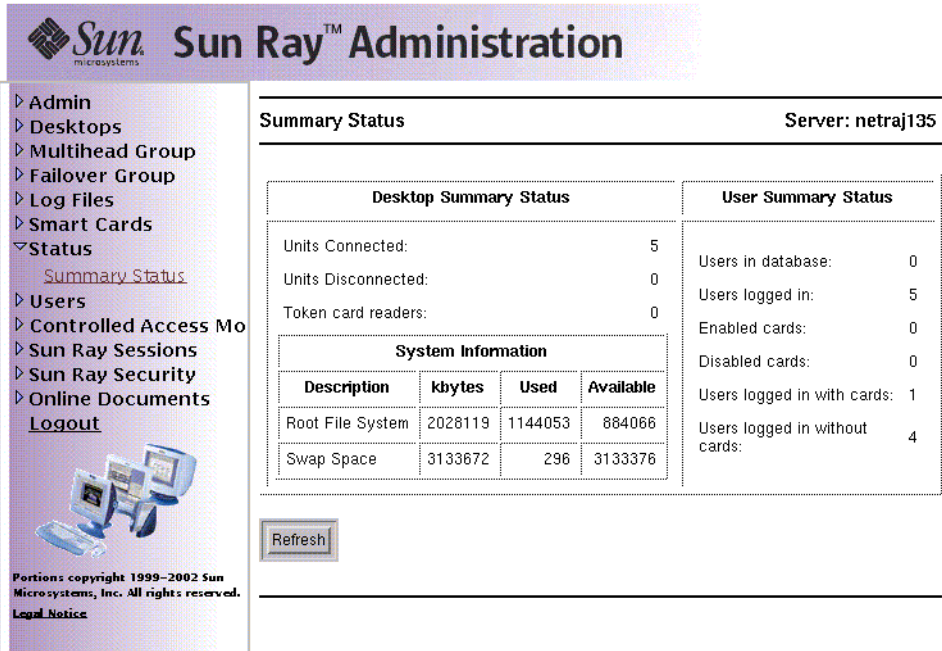
The Summary Status window is displayed.

Use the navigation bar on the left to navigate through the Administration Tool.

---

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

---



The image shows the Sun Ray Administration Summary Status window. On the left is a navigation menu with options like Admin, Desktops, Multihead Group, Failover Group, Log Files, Smart Cards, Status (selected), Users, Controlled Access Mo, Sun Ray Sessions, Sun Ray Security, and Online Documents. Below the menu is a small graphic of a computer workstation and copyright information for Sun Microsystems, Inc. (1999-2002). The main content area is titled 'Summary Status' and shows 'Server: netraj135'. It contains two summary tables: 'Desktop Summary Status' and 'User Summary Status'. Below these is a 'System Information' table with columns for Description, kbytes, Used, and Available. A 'Refresh' button is located at the bottom of the main content area.

Desktop Summary Status		User Summary Status																	
Units Connected:	5	Users in database:	0																
Units Disconnected:	0	Users logged in:	5																
Token card readers:	0	Enabled cards:	0																
<table border="1"> <thead> <tr> <th colspan="4">System Information</th> </tr> <tr> <th>Description</th> <th>kbytes</th> <th>Used</th> <th>Available</th> </tr> </thead> <tbody> <tr> <td>Root File System</td> <td>2028119</td> <td>1144053</td> <td>884066</td> </tr> <tr> <td>Swap Space</td> <td>3133672</td> <td>296</td> <td>3133376</td> </tr> </tbody> </table>		System Information				Description	kbytes	Used	Available	Root File System	2028119	1144053	884066	Swap Space	3133672	296	3133376	Disabled cards:	0
System Information																			
Description	kbytes	Used	Available																
Root File System	2028119	1144053	884066																
Swap Space	3133672	296	3133376																
		Users logged in with cards:	1																
		Users logged in without cards:	4																

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.

---

**Note** – In failover groups, all servers must use the same password for the admin account.

---



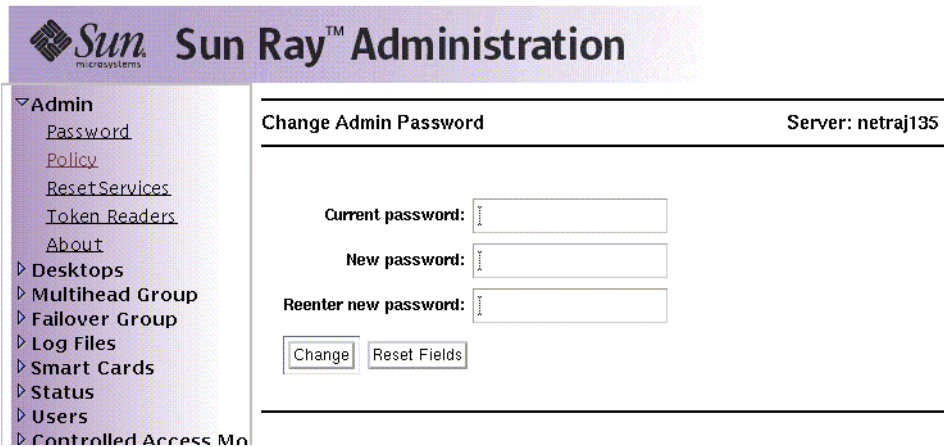


FIGURE 3-3 Change Admin Password Window

3. Enter your current password.
4. Enter a new password.
5. Re-enter the new password.

---

**Tip** – 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 effect and the internal database hierarchy is updated.

---

## Changing Policies

Set the same policies on all the Sun Ray servers in a given failover group. If all 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.

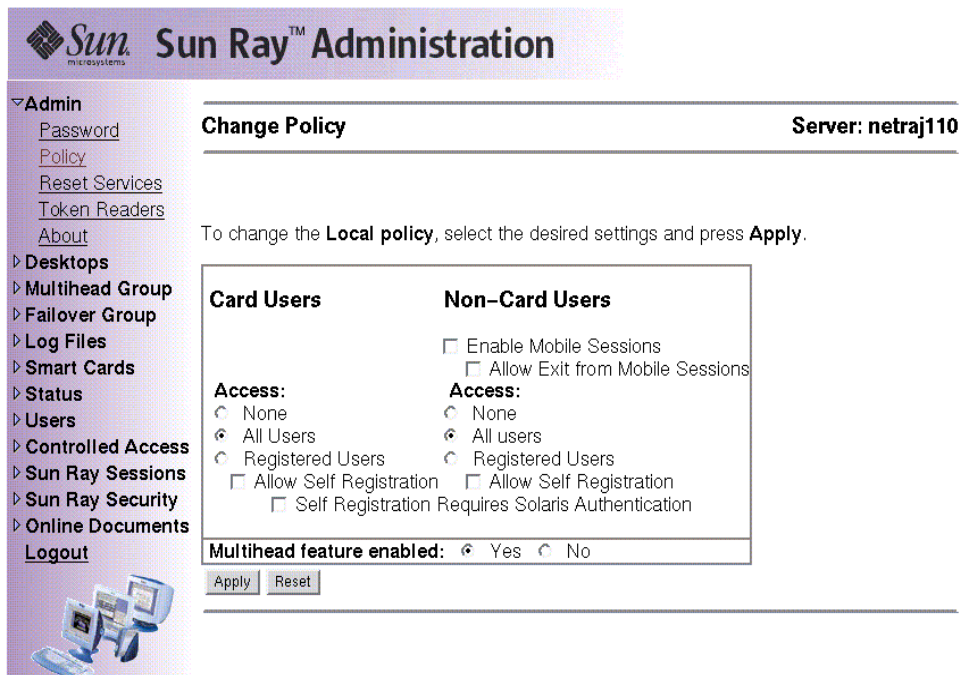


FIGURE 3-4 Change Policy Window

3. Under **Card Users**, select either **None**, **All Users**, or **Registered Users**.
4. Under **Non-Card Users**, select either **None**, **All Users**, or **Registered Users**.  
Registered users are those you have registered. Allow Self Registration enables users to self-register when they insert their cards. 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**.
7. Notify users to log off to avoid losing their sessions.
8. Restart services.

When changing the Multihead feature, you have the option of resetting Sun Ray services. All other changes require you to restart Sun Ray services.

---

# Resetting and Restarting Sun Ray Services

## ▼ To Reset Sun Ray Services

1. From the expanded navigation menu under Admin, click the **Reset Services** link. The Sun Ray Services window is displayed.



FIGURE 3-5 Sun Ray Services Window

2. Click **Reset**.

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 Sun Ray services are restarted.

---

**Note** – In a failover group, you must initiate a group reset or restart from the primary server in the group.

---

# Token Readers

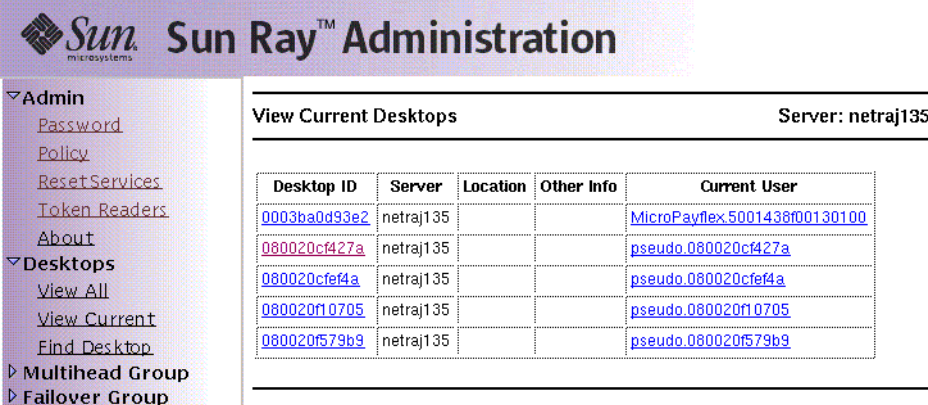
You can use the Administration Tool to create token readers and locate Sun Ray appliances designated as token readers. Sun Ray appliances configured as token readers do not support hot desking.

## Creating a Token Reader

A token reader is a Sun Ray appliance that reads a smart card and returns card's ID. A valid ID allows 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.



The screenshot shows the Sun Ray Administration web interface. The top header includes the Sun Microsystems logo and the text "Sun Ray™ Administration". On the left is a navigation menu with the following items: Admin (expanded), Password, Policy, Reset Services, Token Readers, About, Desktops (expanded), View All, View Current, Find Desktop, Multihead Group, and Failover Group. The main content area is titled "View Current Desktops" and shows "Server: netraj135". Below this is a table with the following data:

Desktop ID	Server	Location	Other Info	Current User
<a href="#">0003ba0d93e2</a>	netraj135			<a href="#">MicroPayflex.5001438f00130100</a>
<a href="#">080020cf427a</a>	netraj135			<a href="#">pseudo_080020cf427a</a>
<a href="#">080020cfe4a</a>	netraj135			<a href="#">pseudo_080020cfe4a</a>
<a href="#">080020f10705</a>	netraj135			<a href="#">pseudo_080020f10705</a>
<a href="#">080020f579b9</a>	netraj135			<a href="#">pseudo_080020f579b9</a>

FIGURE 3-6 View Current Desktops Window

3. Select the desktop of the appliance you want to use as a token reader. The Current Properties window is displayed.

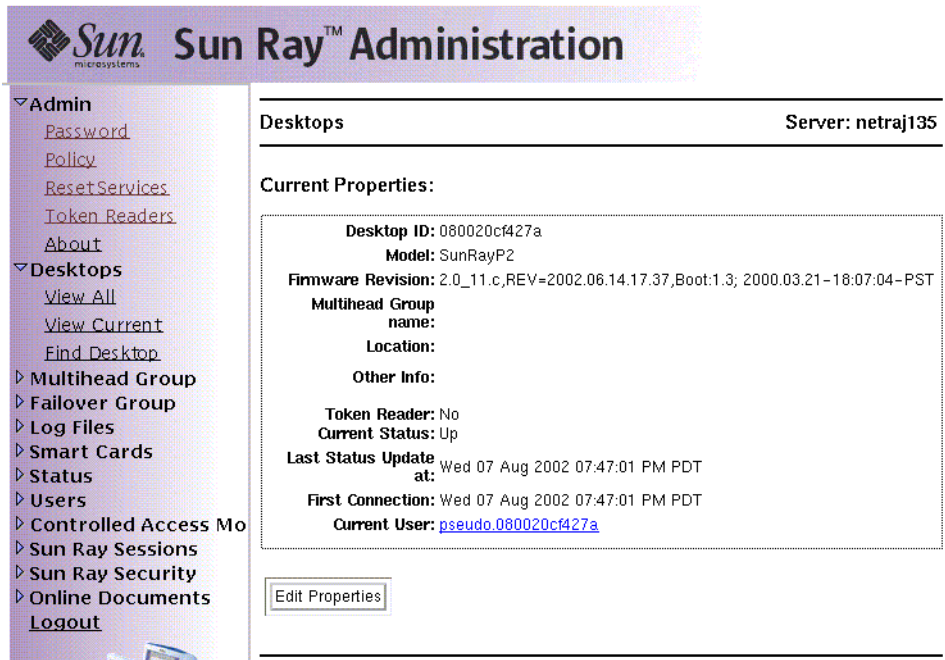


FIGURE 3-7 Current Properties Window

**4. Click the Edit Properties button.**

The Edit Desktop Properties window is displayed.

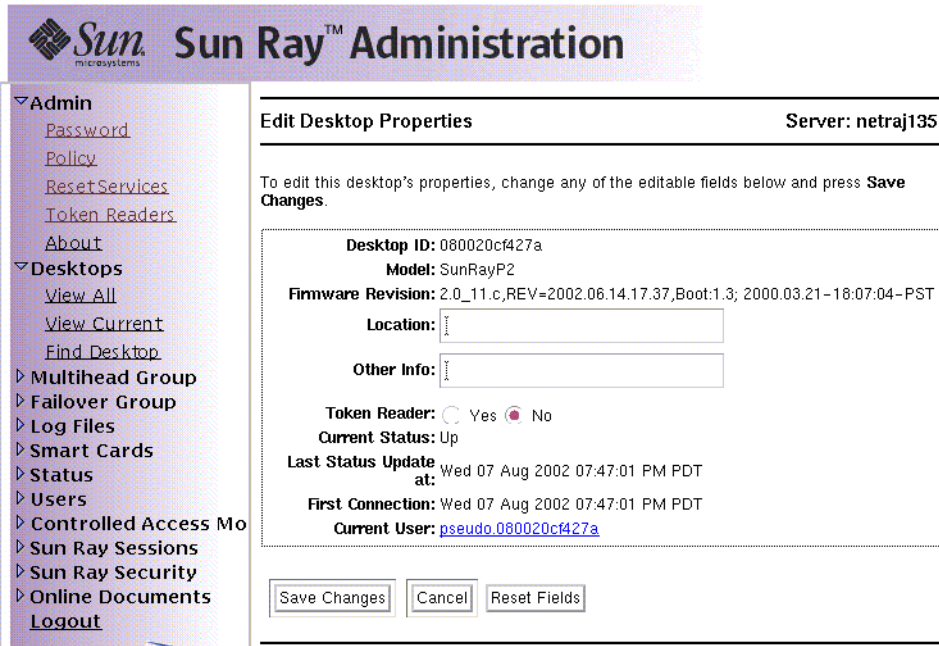


FIGURE 3-8 Edit Desktop Properties Window

5. Next to **Token Reader**, select the **Yes** radio button.

6. Click the **Save Changes** button.

The appliance you have selected is now set up to read smart cards.

7. Restart **Sun Ray** services.

The appliance is now a token reader.

## ▼ To Locate Token Readers

- From the expanded navigation menu under **Admin**, click the **Token Readers** link.

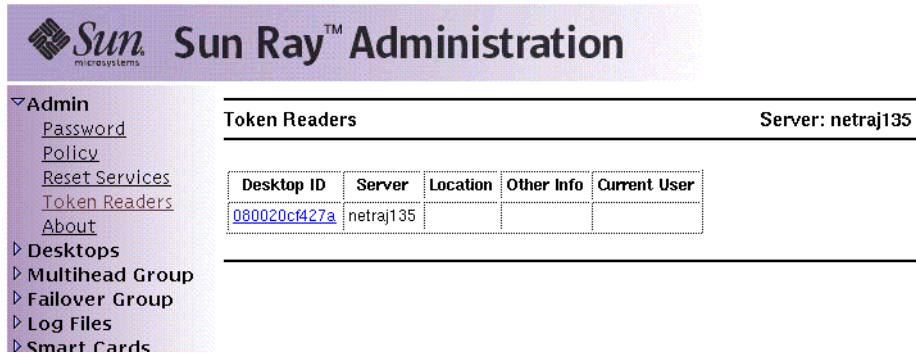


FIGURE 3-9 Token Readers Window

## ▼ To Get Information on a Token Reader

- Click the Desktop ID link in the Token Readers window.

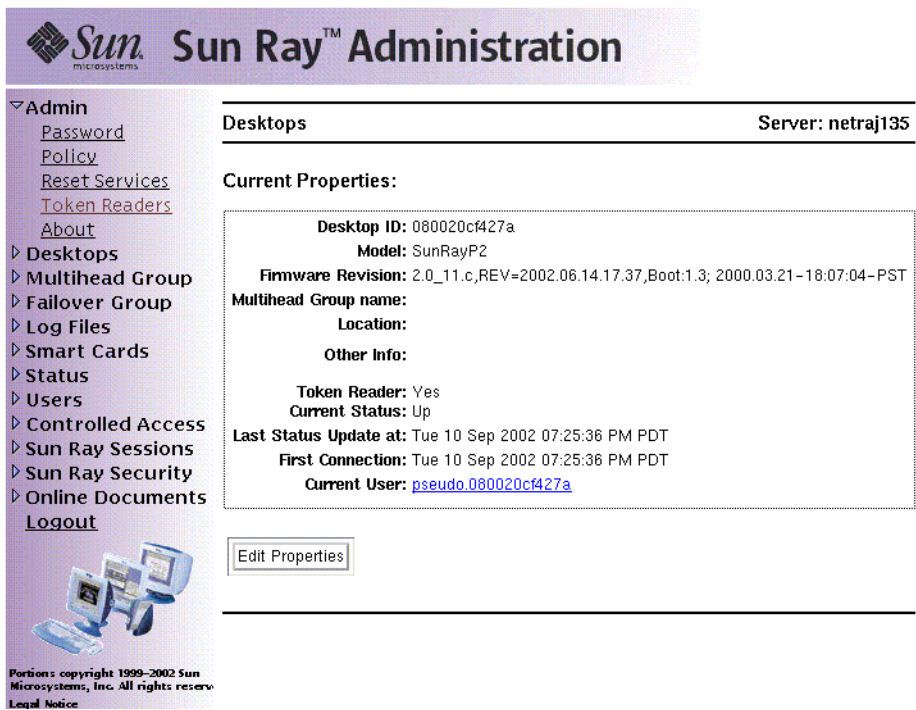


FIGURE 3-10 Current Properties of a Token Reader

# Managing Desktops

## ▼ 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.

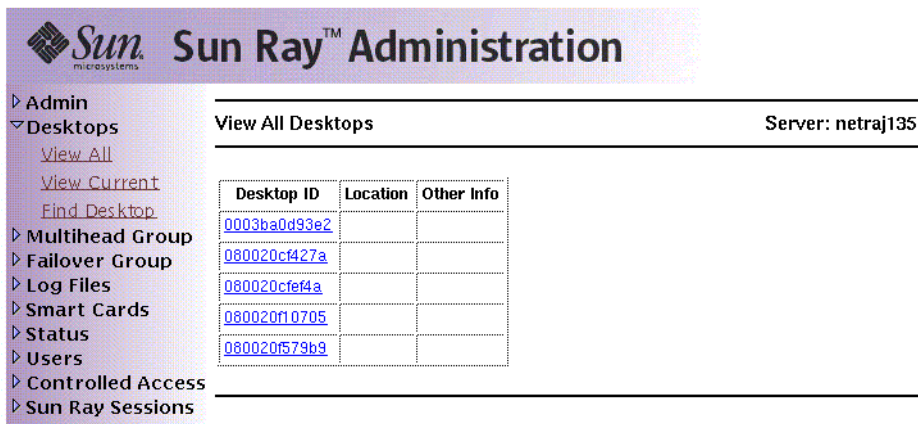


FIGURE 3-11 View All Desktops Window

## ▼ To Display a Desktop's Current Properties

- Click a Desktop ID link.

The Desktops Current Properties window is displayed (see FIGURE 3-7).

## ▼ 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 (see FIGURE 3-6). This window lists the desktops that are currently connected to this Sun Ray server and communicating with the Authentication Manager or with any other Sun Ray server in the same failover group.

## ▼ 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 (see FIGURE 3-7).

## ▼ 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 left-hand navigation menu is expanded to show the 'Desktops' section, which includes links for 'View All', 'View Current', and 'Find Desktop'. The 'Find Desktop' window is active, displaying the server name 'netraj135'. The search criteria section is titled 'Search for All Desktops that Contain:' and includes three input fields: 'Desktop ID' (with the value '0800'), '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.

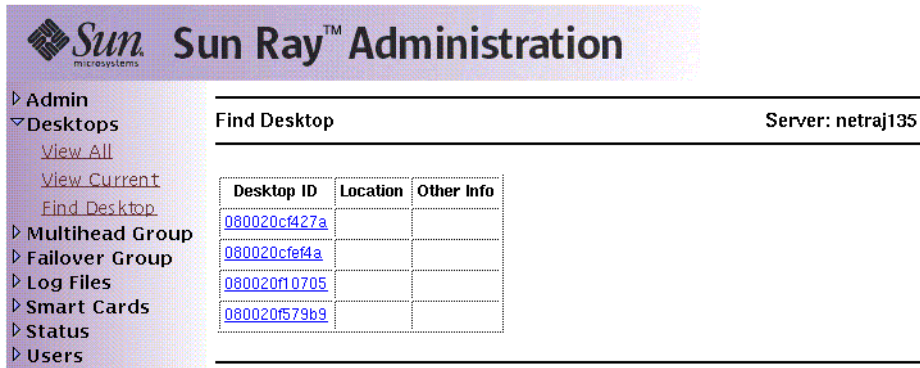


FIGURE 3-13 Find Desktop Search Results Window

## ▼ 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 (see FIGURE 3-7).

- 2. Click the Edit Properties button.**

The Edit Desktop Properties window is displayed (see FIGURE 3-8).

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

---

# 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.

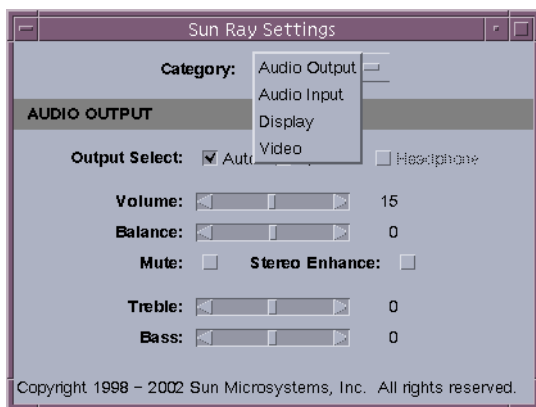


FIGURE 3-14 Settings Screen

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

The 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 per session of Sun RaySun Ray Settings runs in hot key mode.

---

---

## Managing Multihead Groups

The multihead feature allows users to control separate applications on multiple Sun Ray screens. Only a single keyboard and pointer device, attached to the primary appliance, are needed. The multihead feature also allows users to display and control a single application, such as a spreadsheet, on multiple screens.

System administrators create multihead groups so that users can access them. A multihead group, consisting of two or more appliances controlled by one keyboard and mouse, can consist of Sun Ray 1, Sun Ray 100, Sun Ray 150, and Sun Ray 160 appliances.

For further information on multihead implementations, see Chapter 9.

### ▼ 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.

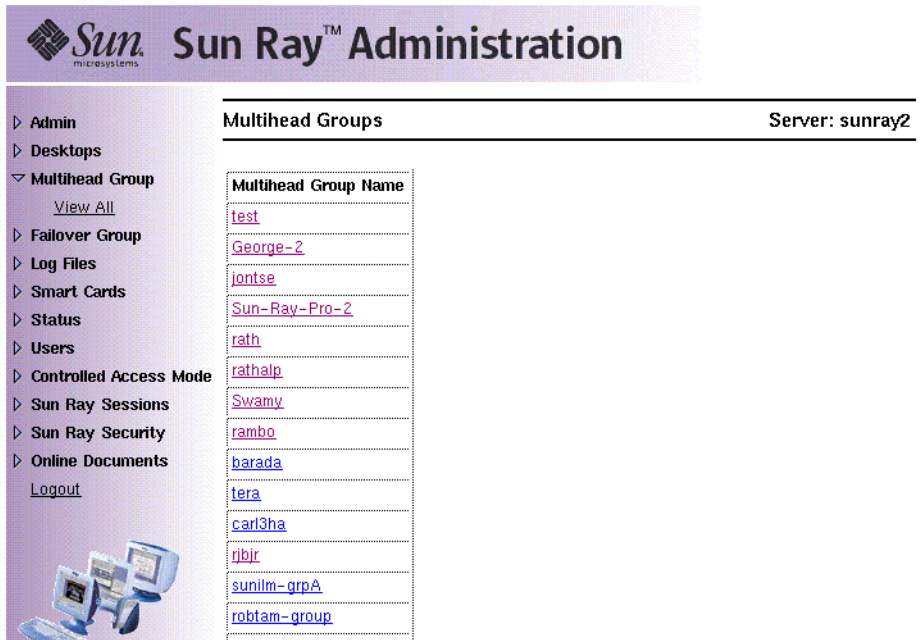


FIGURE 3-15 The Multihead Groups Window (truncated)

3. To view the properties for this group, click the Multihead Group Name link. The Multihead Group Properties window is displayed.

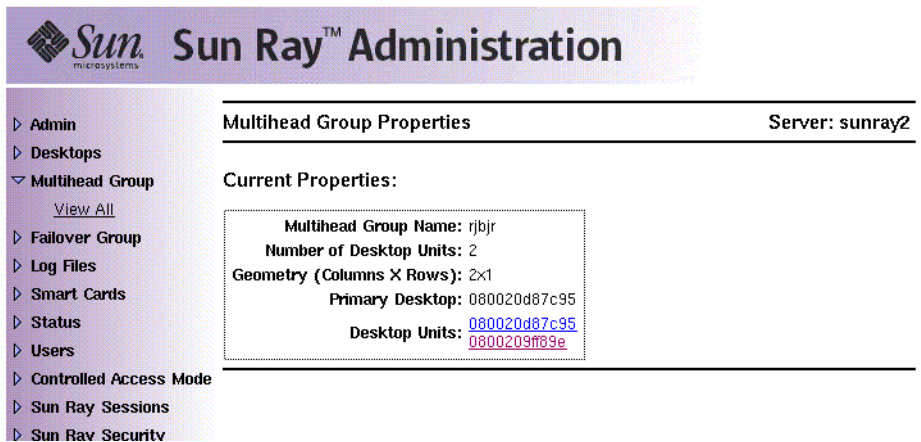


FIGURE 3-16 The Multihead Group Properties Window

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.



The screenshot displays the Sun Ray Administration web interface. The top header features the Sun Microsystems logo and the text "Sun Ray™ Administration". On the left is a navigation menu with items: Admin, Desktops, Multihead Group (with a "View All" link), Failover Group, Log Files, Smart Cards, Status, Users, Controlled Access Mode, Sun Ray Sessions, Sun Ray Security, and Online Documents (with a "Logout" link). Below the menu is an illustration of three computer monitors. The main content area is titled "Desktops" and shows "Server: sunray2". Underneath, the "Current Properties:" section is enclosed in a dotted border and lists the following information: Desktop ID: 0800209ff89e, Model: SunRayP1, Firmware Revision: 2.0\_19.a,REV=2002.08.07.06.04,Boot:1.2; 1999.04.11-11:13:51-PDT, Multihead Group name: rjbjr, Location: (blank), Other Info: Token Reader: No, Current Status: Up, Last Status Update at: Wed Sep 11 11:50:30 2002, First Connection: Mon Apr 29 09:02:05 2002, and Current User: None. An "Edit Properties" button is located below the dotted box.

FIGURE 3-17 Desktops Current Properties Window

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

---

# Examining Log Files

Significant activity concerning files retrieved from the Sun Ray server is logged and saved. The server stores this information in text files. TABLE 3-1 describes the log files that are maintained.

**TABLE 3-1** 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. Archived files are stored on the server for one week annotated with numeric extensions (for example, from <code>messages.0</code> to <code>messages.5</code> ).
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 during server administration. This log is updated daily. Archived files are stored on the system for up to one week and are annotated using numeric extensions (for example, from 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. Choose the Log link you want to inspect: Messages, Auth Log, Admin Log, or Archived Logs.

The appropriate Log File window is displayed. Use the scroll bar to access data to the right and bottom of the window.

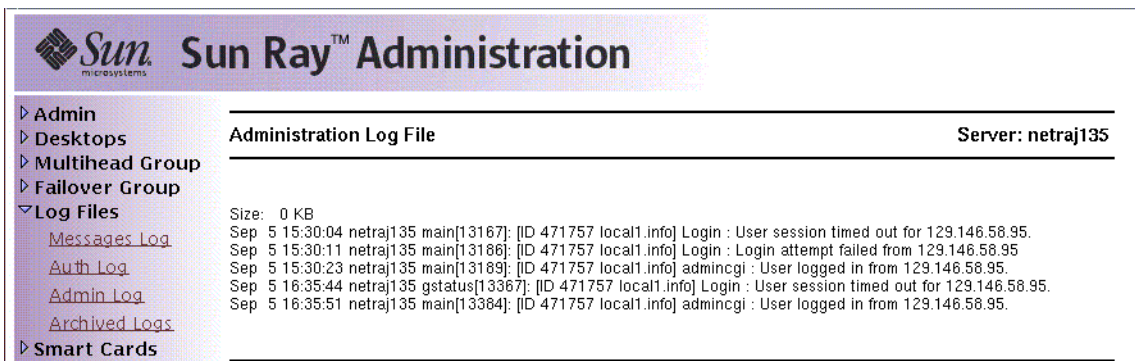


FIGURE 3-18 Administration Log File Window

## Managing Smart Cards

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 may 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.

---

**Note** – Smart Card Frameworks, which enable custom applications to be written for smart cards, are supported in Solaris 8 Update 7 and Solaris 9 Update 1, but not in the initial release of Solaris 9.

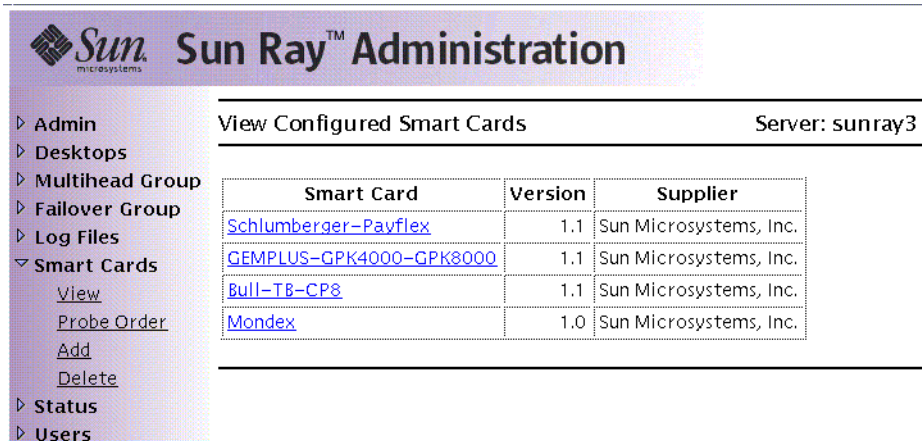
---



## ▼ 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. Smart cards are listed in probe order, i.e., the order in which they are inspected.



Screenshot of the Sun Ray Administration interface showing the View Configured Smart Cards window. The window displays a table of smart cards with columns for Smart Card, Version, and Supplier. The table lists four smart cards: Schlumberger-Payflex, GEMPLUS-GPK4000-GPK8000, Bull-TB-CP8, and Mondex, all supplied by Sun Microsystems, Inc. The interface also shows a navigation menu on the left with options like Admin, Desktops, Multihead Group, Failover Group, Log Files, Smart Cards (with sub-options View, Probe Order, Add, Delete), Status, and Users.

Smart Card	Version	Supplier
<a href="#">Schlumberger-Payflex</a>	1.1	Sun Microsystems, Inc.
<a href="#">GEMPLUS-GPK4000-GPK8000</a>	1.1	Sun Microsystems, Inc.
<a href="#">Bull-TB-CP8</a>	1.1	Sun Microsystems, Inc.
<a href="#">Mondex</a>	1.0	Sun Microsystems, Inc.

FIGURE 3-19 The View Configured Smart Cards Window

From this window an administrator can see the current list of smart cards as well as the supplier and version number for each card.

3. From 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 3-20.

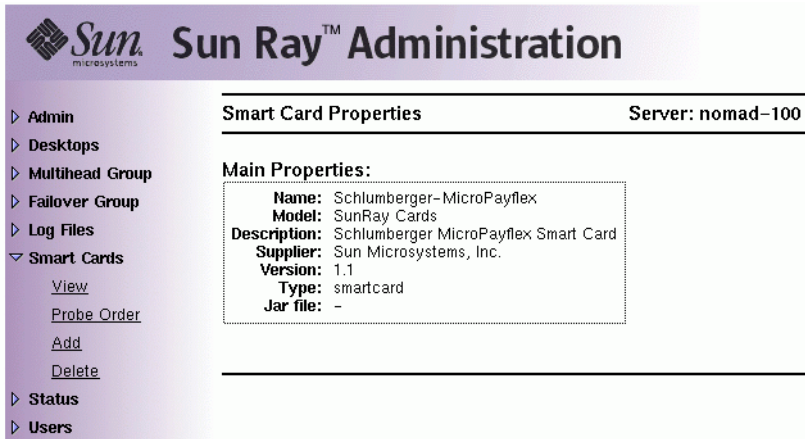


FIGURE 3-20 Smart Card Properties Window

## ▼ 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.

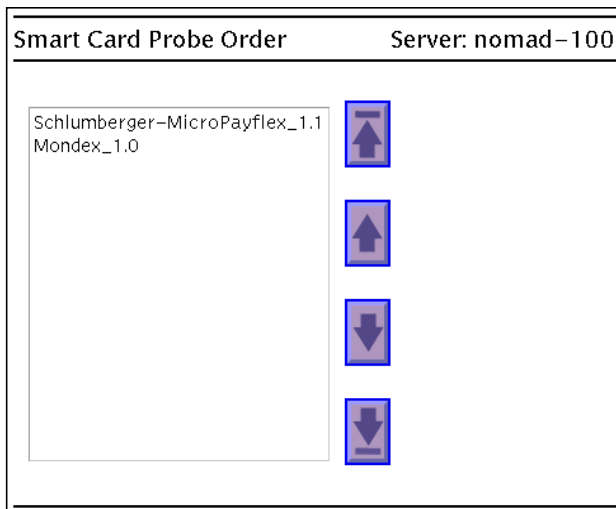


FIGURE 3-21 Smart Card Probe Order Window

Smart cards are probed in the order in which they appear in this list.

---

**Tip** – 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 buttons (from top to bottom) 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

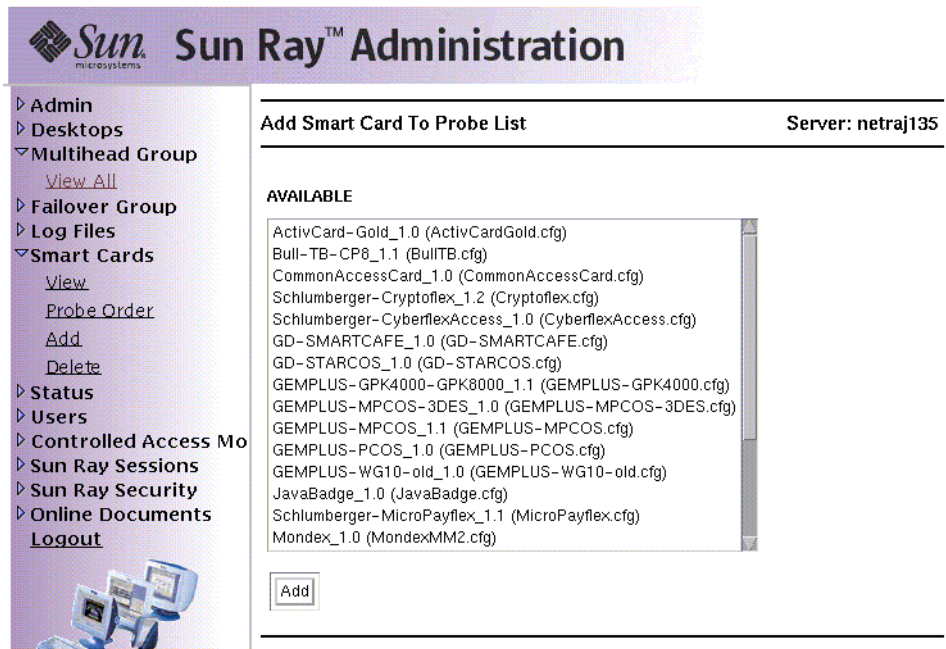


FIGURE 3-22 Add Smart Card to Probe List Window

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.
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. The Summary Status window is displayed.
2. Click the Summary Status link.

**Sun Ray Administration** Server: netraj135

**Summary Status**

Desktop Summary Status		User Summary Status	
Units Connected:	5	Users in database:	0
Units Disconnected:	0	Users logged in:	5
Token card readers:	0	Enabled cards:	0
		Disabled cards:	0
		Users logged in with cards:	1
		Users logged in without cards:	4

System Information			
Description	kbytes	Used	Available
Root File System	2028119	1144053	884066
Swap Space	3133672	296	3133376

Refresh

Portions: copyright 1999-2002 Sun Microsystems, Inc. All rights reserved.

FIGURE 3-23 Summary Status Window

**TABLE 3-2** Summary Status Field Descriptions

<b>Options</b>	<b>Description</b>
<b>Desktop Summary Status</b>	
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.
<b>User Summary Status</b>	
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.
<b>System Information</b>	
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 3-3 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.

## ▼ 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. 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.

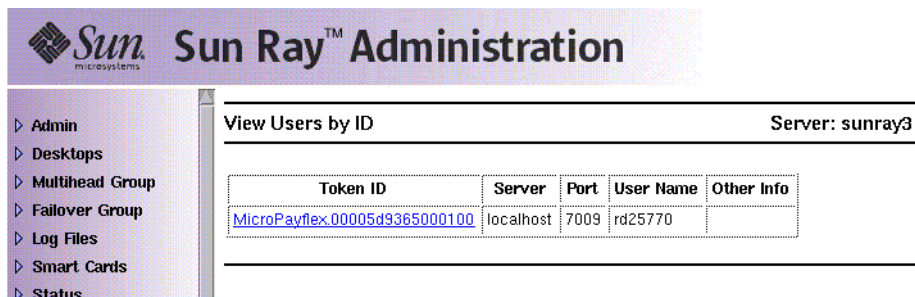


FIGURE 3-24 View Users by ID Window

## ▼ To View Users by Name

- From 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.

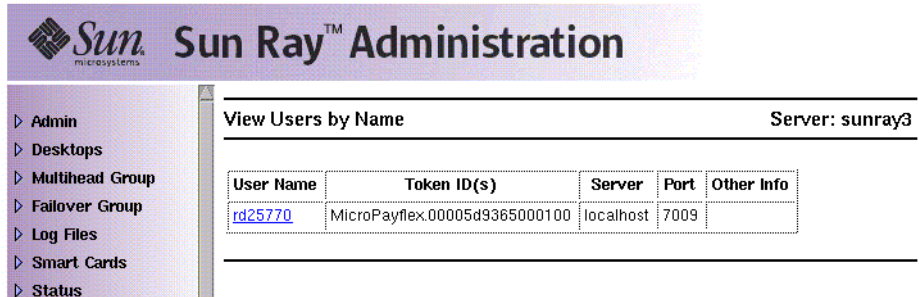


FIGURE 3-25 View Users by Name Window

## ▼ To Delete a User

---

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

---

1. From the View by Name window, click the User Name of the user you want to delete.

The Current Properties window displays information about the user, host, token, and allows the administrator to edit the user's properties, delete the user, and view the user's session.

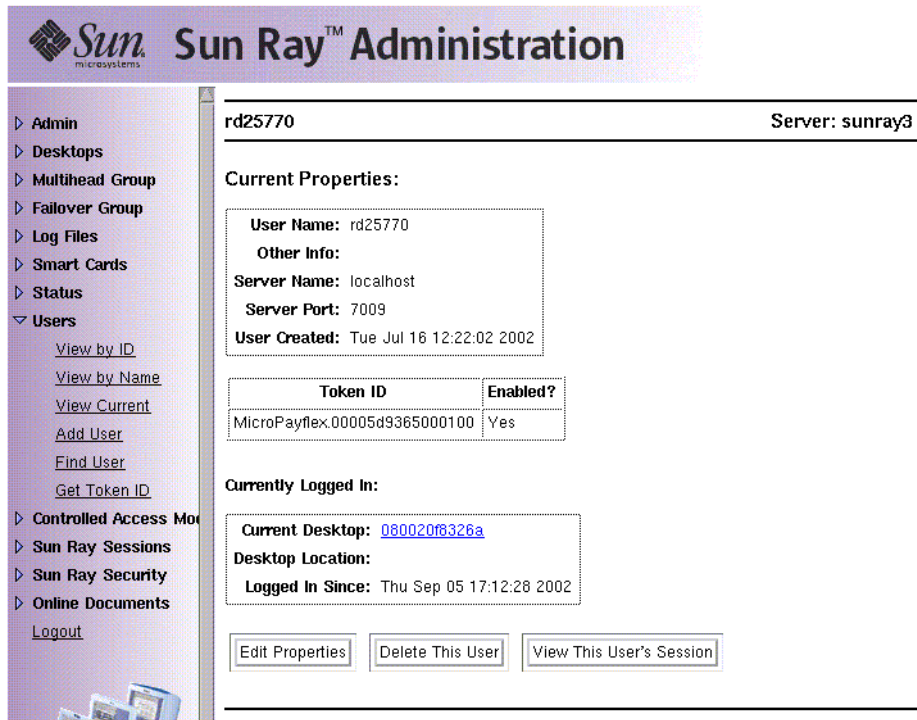


FIGURE 3-26 The Current Properties Window Shows Administrative Options for a User

**2. Press the Delete This User button.**

The Delete User page is displayed.

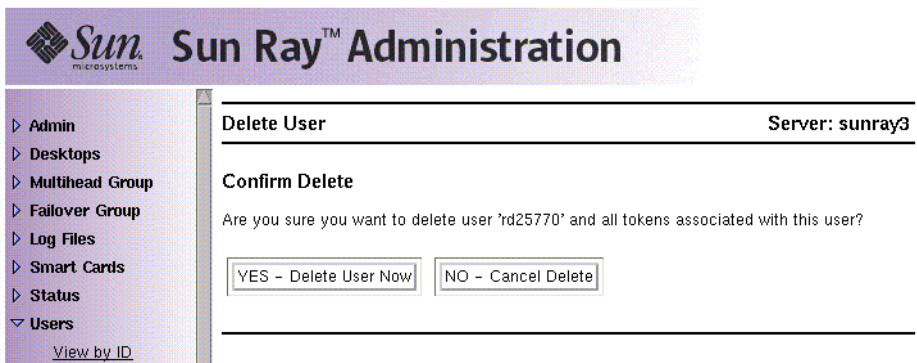


FIGURE 3-27 Delete User Window



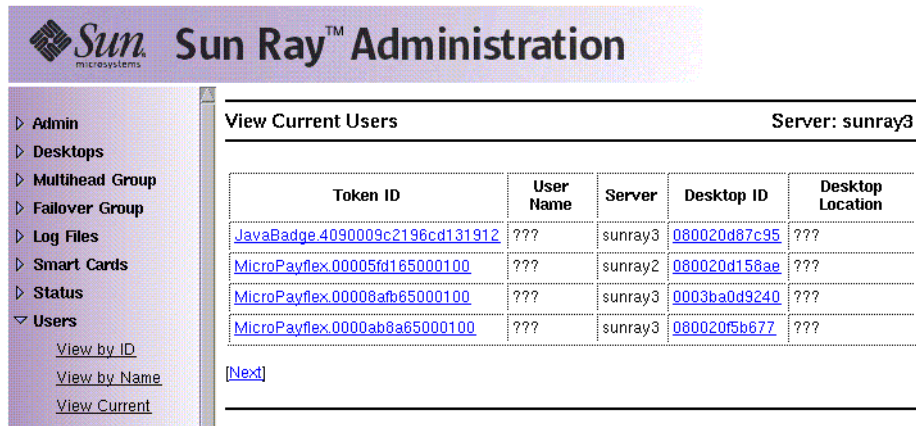
### 3. To delete the user, press the YES — Delete User Now button.

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 those registered users who are currently logged into an appliance connected to this Sun Ray server.



The screenshot shows the Sun Ray Administration interface. The title bar reads "Sun Ray™ Administration". On the left is a navigation menu with options: Admin, Desktops, Multihead Group, Failover Group, Log Files, Smart Carts, Status, and Users. Under Users, there are links for "View by ID", "View by Name", and "View Current". The main content area is titled "View Current Users" and shows "Server: sunray3". Below this is a table with the following data:

Token ID	User Name	Server	Desktop ID	Desktop Location
<a href="#">JavaBadge.4090009c2196cd131912</a>	???	sunray3	<a href="#">060020d87c95</a>	???
<a href="#">MicroPayflex.00005fd165000100</a>	???	sunray2	<a href="#">060020d158ae</a>	???
<a href="#">MicroPayflex.00008afb65000100</a>	???	sunray3	<a href="#">0003ba0d9240</a>	???
<a href="#">MicroPayflex.0000ab8a65000100</a>	???	sunray3	<a href="#">060020f5b677</a>	???

Below the table is a "[Next]" link.

FIGURE 3-28 View Current Users Window

## ▼ To Display a User's Current Properties

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

The Current Properties page for the user is displayed (see FIGURE 3-26). It displays the information about the user contained in the administration database, including the user's current login status.

The possible states are:

- Never Logged In
- Currently Logged In
- Logged Off

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

TABLE 3-4 Login Status Fields

Option	Description
Current Desktop/Last Desktop	Current/last appliance (desktop) where the user is or was logged in.
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 Add a User

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

The Add User window is displayed.

**Sun** Sun Ray™ Administration  
microsystems

▶ Admin  
▶ Desktops  
▼ Multihead Group  
    [View All](#)  
▶ Failover Group  
▶ Log Files  
▶ Smart Cards  
▶ Status  
▼ Users  
    [View by ID](#)  
    [View by Name](#)  
    [View Current](#)  
    [Add User](#)  
    [Find User](#)  
    [Get Token ID](#)  
▶ Controlled Access Mo  
▶ Sun Ray Sessions  
▶ Sun Ray Security  
▶ Online Documents  
    [Logout](#)

**Add User** Server: netraj135

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: (None Available)

Token ID:

Server Name:

Server Port:

User Name:

Other Info:

FIGURE 3-29 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 View the User's Sessions

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

## ▼ 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.

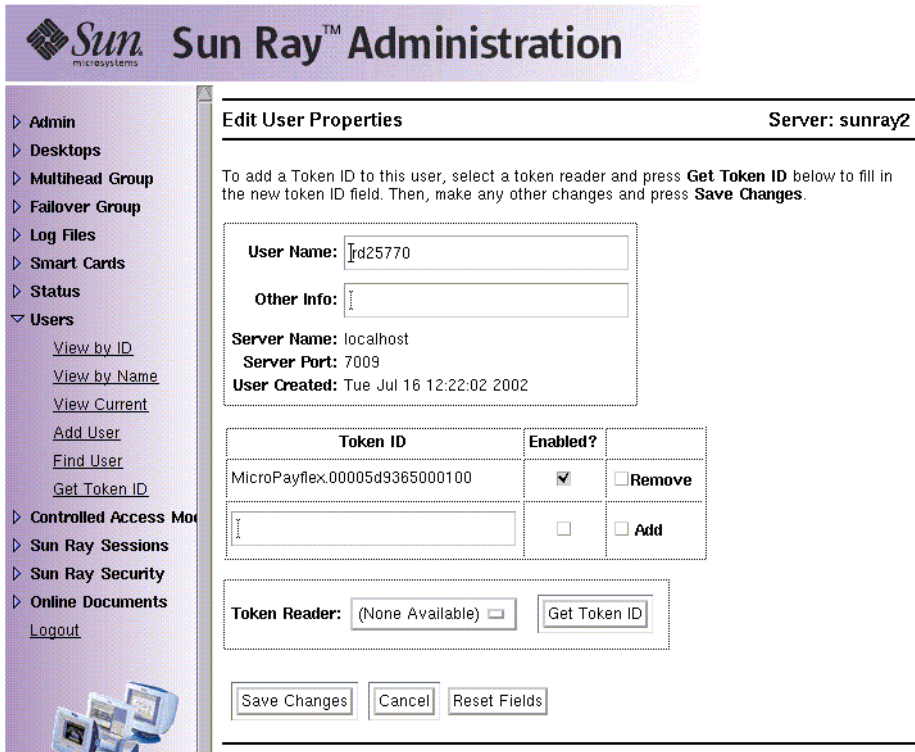


FIGURE 3-30 Edit User Properties Page

**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 Find a User

**1. From the expanded menu under Users, click the Find link.**

The Find User window is displayed.

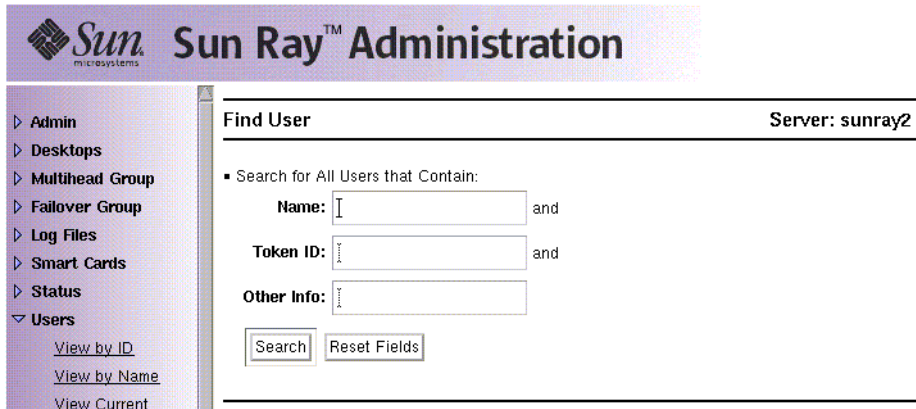


FIGURE 3-31 Find User Window

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.

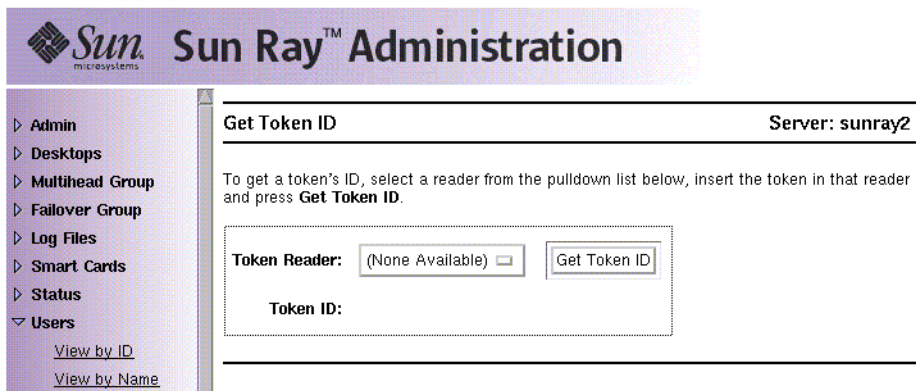


FIGURE 3-32 Get Token ID Window

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

### ▼ To Configure Controlled Access Mode

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

---

**Note** – The Controlled Browser menu item is displayed only if the Controlled Browser package is installed. See Appendix B for details.

---

2. Click the Settings link.

The Controlled Access Mode Configuration Window is displayed.

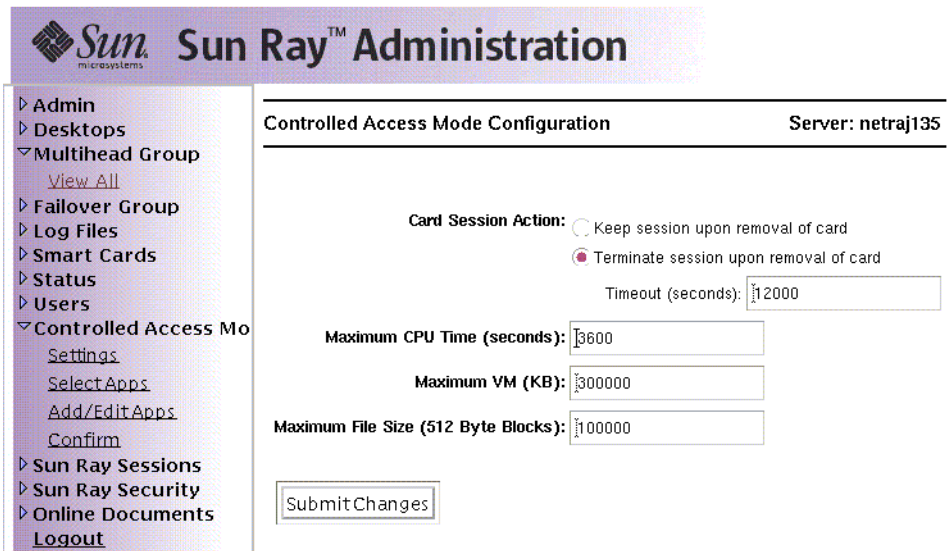


FIGURE 3-33 Controlled Access Mode Configuration Window

If the administrator selects the Terminate session upon removal of card option, the length of session time-out, in seconds, is displayed.

**3. Click the Submit Changes button.**

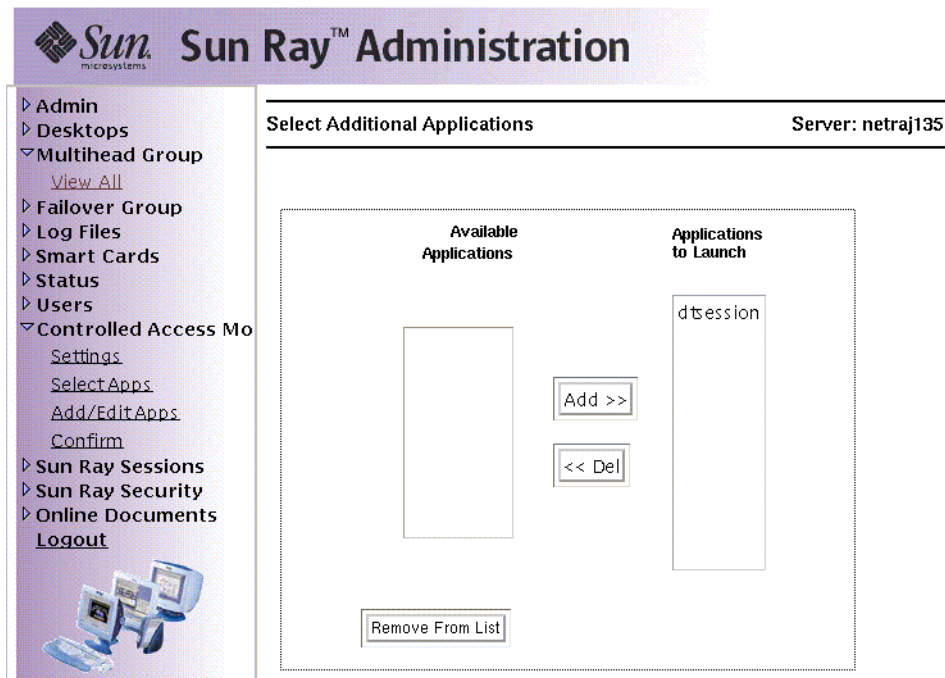
Use the link in the navigation bar to confirm before activating any changes.

## ▼ 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.



**FIGURE 3-34** Select Additional Applications Window

From this window the administrator can configure browser behavior, home page, and proxy to work in 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. To be executable, an application must be in the Applications to Launch box.

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. To 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. Expand the Controlled Access Mode menu and click the Add/Edit Applications link.

The Add/Edit Apps Window is displayed.

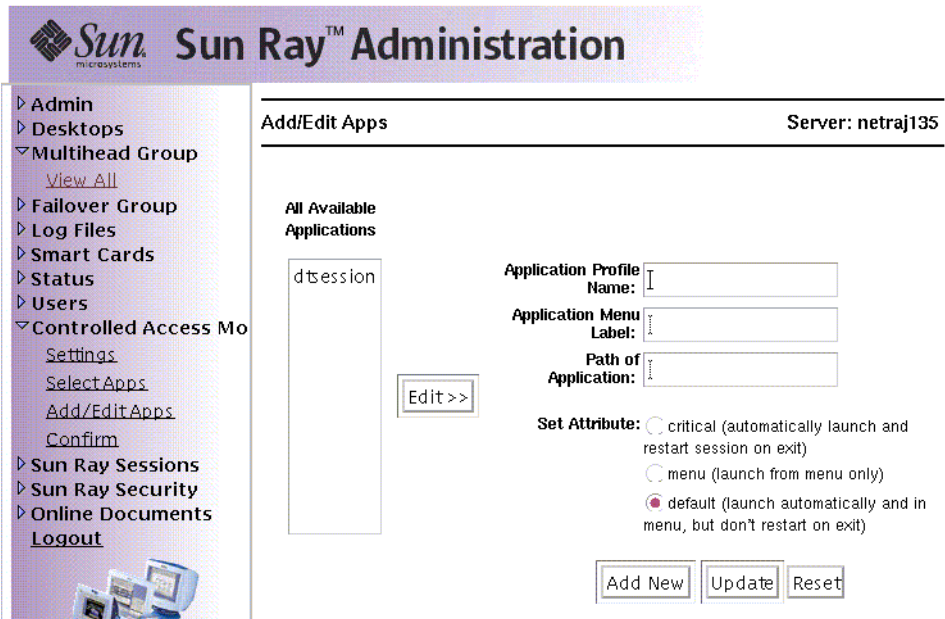


FIGURE 3-35 Add/Edit Apps Window

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.

---

2. To edit an application, highlight the application in the All Available Applications scroll box.
3. Click the Edit button.  
The information for the application is displayed in the text fields.
4. When you have edited the text fields and selected the radio button for your preferred launch attribute, click the Update button.
5. To add an application, fill in the text fields and click the Add New button.
6. Click Confirm in the expanded navigation menu under Controlled Access Mode.

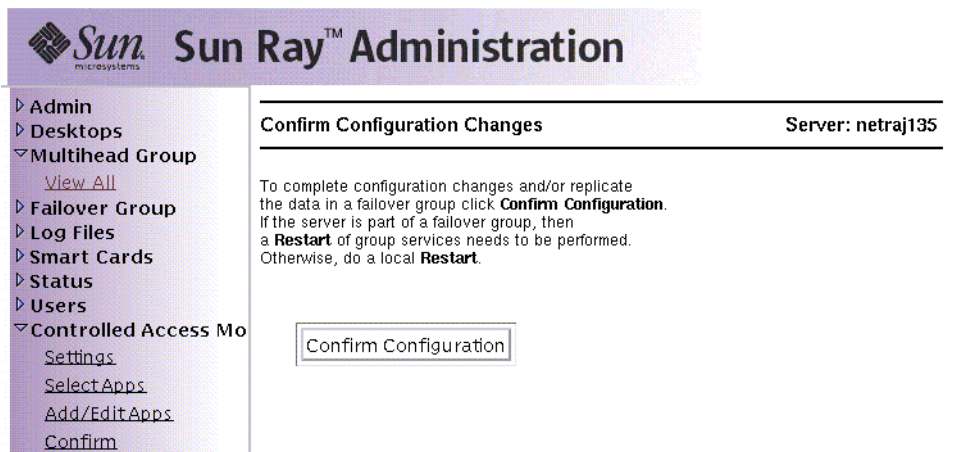


FIGURE 3-36 Confirmation Window

7. Click the Confirm Configuration button.

# Managing Sessions

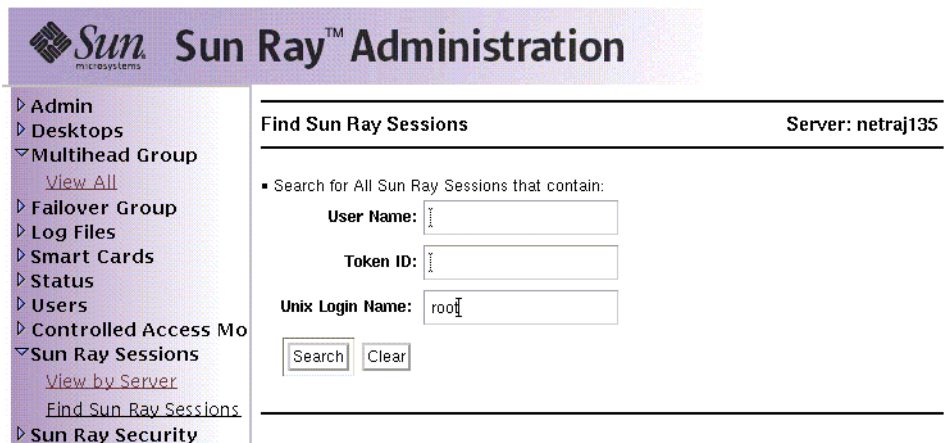
A Sun Ray session is created when the user logs in to a Sun Ray appliance. A Sun Ray session has three possible states, as shown in TABLE 3-5.

TABLE 3-5 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 Find Sun Ray Sessions

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



The screenshot shows the Sun Ray Administration web interface. On the left is a navigation menu with the following items: Admin, Desktops, Multihead Group (with a 'View All' link), Failover Group, Log Files, Smart Cards, Status, Users, Controlled Access Mo, Sun Ray Sessions (expanded), Sun Ray Sessions (with 'View by Server' and 'Find Sun Ray Sessions' links), and Sun Ray Security. The 'Find Sun Ray Sessions' window is open, displaying the title 'Find Sun Ray Sessions' and the server name 'Server: netraj135'. Below the title is a search instruction: 'Search for All Sun Ray Sessions that contain:'. There are three text input fields: 'User Name:', 'Token ID:', and 'Unix Login Name:' (which contains the text 'root'). At the bottom of the search area are two buttons: 'Search' and 'Clear'.

FIGURE 3-37 The Find Sun Ray Sessions Window

3. In the text fields, enter the User Name, Token ID, or Unix Login Name.

#### 4. 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.

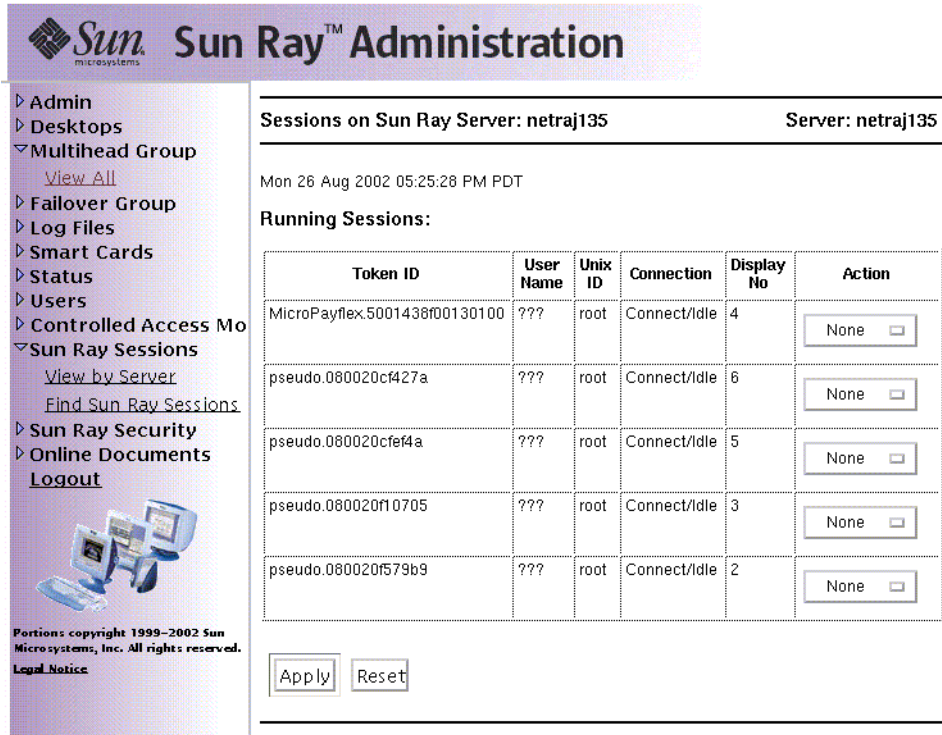
The screenshot shows the Sun Ray Administration web interface. The top header includes the Sun Microsystems logo and the text "Sun Ray™ Administration". On the left is a navigation menu with items like Admin, Desktops, Multihead Group, Failover Group, Log Files, Smart Cards, Status, Users, Controlled Access Mo, Sun Ray Sessions (selected), Sun Ray Security, and Online Documents. The main content area is titled "Sun Ray Sessions" and shows "Server: netraj135". It displays the current time as "Mon 26 Aug 2002 05:43:50 PM PDT" and a section for "Running Sessions:" containing a table with columns for Sun Ray Token ID, User Name, Unix ID, Server, Connection, Display No, and Action. The table lists five sessions, each with a "None" button in the Action column. Below the table are "Apply" and "Reset" buttons.

Sun Ray Token ID	User Name	Unix ID	Server	Connection	Display No	Action
MicroPayflex.5001438f00130100	???	root	netraj135	Connect/Idle	4	None <input type="checkbox"/>
pseudo.080020cf427a	???	root	netraj135	Connect/Idle	6	None <input type="checkbox"/>
pseudo.080020cfe4a	???	root	netraj135	Connect/Idle	5	None <input type="checkbox"/>
pseudo.080020f10705	???	root	netraj135	Connect/Idle	3	None <input type="checkbox"/>
pseudo.080020f579b9	???	root	netraj135	Connect/Idle	2	None <input type="checkbox"/>

FIGURE 3-38 Sun Ray Sessions Window Showing Search Results

## ▼ 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.  
Running sessions on the current server are displayed.



The screenshot displays the Sun Ray Administration web interface. The top header shows the Sun Microsystems logo and the title "Sun Ray™ Administration". A navigation menu on the left includes options like Admin, Desktops, Multihead Group, Failover Group, Log Files, Smart Cards, Status, Users, Controlled Access Mo, Sun Ray Sessions (expanded), Sun Ray Security, and Online Documents. Under "Sun Ray Sessions", the "View by Server" link is selected. The main content area shows "Sessions on Sun Ray Server: netraj135" for "Server: netraj135" on "Mon 26 Aug 2002 05:25:28 PM PDT". A table titled "Running Sessions:" lists five sessions with columns for Token ID, User Name, Unix ID, Connection, Display No, and Action. Each session has a "None" button in the Action column. At the bottom, there are "Apply" and "Reset" buttons.

Token ID	User Name	Unix ID	Connection	Display No	Action
MicroPayflex.5001438f00130100	???	root	Connect/Idle	4	None <input type="button" value=""/>
pseudo.080020c427a	???	root	Connect/Idle	6	None <input type="button" value=""/>
pseudo.080020cfef4a	???	root	Connect/Idle	5	None <input type="button" value=""/>
pseudo.080020f10705	???	root	Connect/Idle	3	None <input type="button" value=""/>
pseudo.080020f579b9	???	root	Connect/Idle	2	None <input type="button" value=""/>

FIGURE 3-39 Sessions on Current Sun Ray Server Window

3. 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.
4. To apply your changes, click the Apply button.



## 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 79
- “Attached Printers” on page 82
- “PDA Synchronization” on page 84
- “Adapters” on page 86

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.

Third-party adapters are useful for supporting legacy serial and parallel devices.

Sun Ray Server Software 2.0 recognizes a parallel printer with an adapter as a USB printer.

---

**Note** – The printer naming conventions in Sun Ray Server Software differ from those in a Solaris operating environment.

---

---

## Device Nodes and USB Peripherals

Sun Ray Server Software creates a device directory called `IEEE802.MACID` in the `/tmp/SUNWut/units` directory. This directory contains the MAC address for each 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 some of the devices connected to the appliance.

---

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

---

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

## Device Nodes

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

*manufacturer\_name, model\_name@upstream\_hub\_port*

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

The following is a typical device node path:

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

**TABLE 4-1** Definitions of Naming Conventions

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



## Device Links

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

Typical device links are:

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

```
manufacturer_name-serial_numberindex
```

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

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

## Device Node Ownership

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

## Hot Desking and Device Node Ownership

---

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

---

Changing the active session on 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 or removes a smart card from an appliance

- Logs into a session
- Detaches from a session using non-smart card mobility

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

---

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

---

---

## Attached Printers

Sun Ray Server Software 2.0 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 84.

---

**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 string 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 once. 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

To synchronize PDAs that use the Palm OS to a Sun Ray appliance, use a USB-to-serial adapter.

# 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.

Certain components of the Java Communications API 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. **Get the latest Java Communications API (javax.comm api version 2.0.2 and above) from**

<http://java.sun.com/products/javacomm/>

3. **Uncompress the downloadcd file.**

```
# uncompress javax_comm-2_0_2-solsparc.tar.Z
# tar -xvf javax_comm-2_0_2-solsparc.tar
```

4. **To change directories to the commapi directory, type:**

```
# cd commapi
```

5. **Copy the comm.jar file by typing:**

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

6. **Copy the libSolarisSerialParallel.so file by typing:**

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

7. **Run the PDASync application by typing:**

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

or select Application Manager -> Desktop\_Apps->PDASync.

---

# Adapters

For a list of verified serial and parallel adapters, see:

[http://www.sun.com/io\\_technologies/sunray/usb/sunray-usb.html](http://www.sun.com/io_technologies/sunray/usb/sunray-usb.html)

---

## Mobile Sessions (Hot Desking)

---

The Sun Ray system was designed, in part, to enable hot desking with Smart Cards, and every Sun Ray appliance is equipped with a Smart Card reader. Sun Ray Server Software 2.0 also includes Smart Card frameworks for developers who wish to encode custom applications or other information in their users' Smart Cards. This enhancement requires no additional administration. For further information on Smart Card Frameworks, see the latest version of the *Solaris Smart Card Administration Guide*.

Configuring Sun Ray Server Software 2.0 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 87
- “NSCM and Failover Groups” on page 92
- “Configuring the Authentication Manager for NSCM Sessions” on page 93

---

### 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.

---

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

---

# Sun Ray Mobile Session Login Dialog Box

When Sun Ray Server Software 2.0 is configured for NSCM sessions, the Sun Ray Mobile Session Login dialog box is displayed on the Sun Ray appliance.

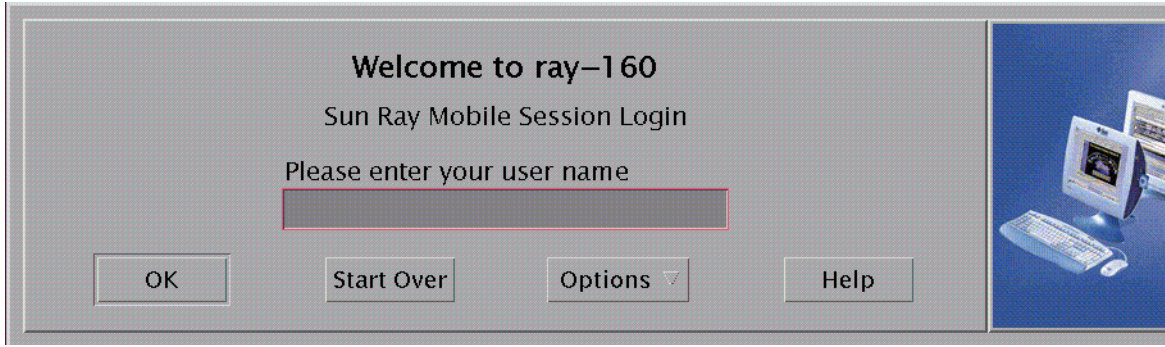


FIGURE 5-1 Sun Ray Mobile Session Login Dialog Box

A right click on the Options button opens a panel where the user can select:

- QuickLogin—To a new session only. 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. An escape 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.

## ▼ To Log In to an NSCM Session

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

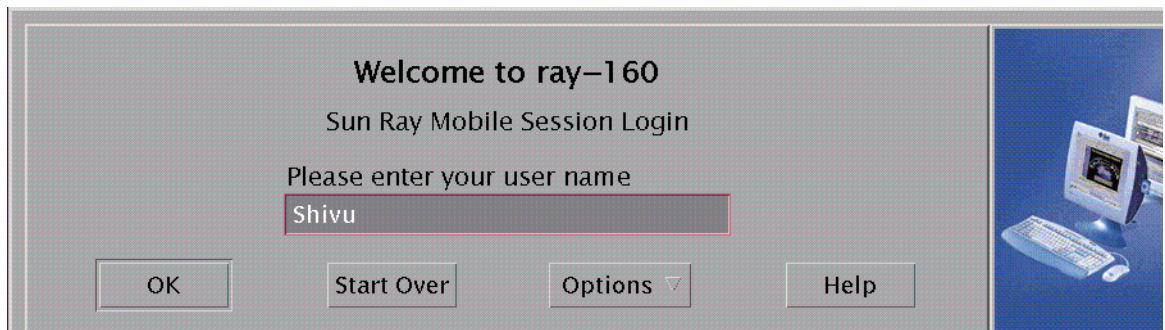


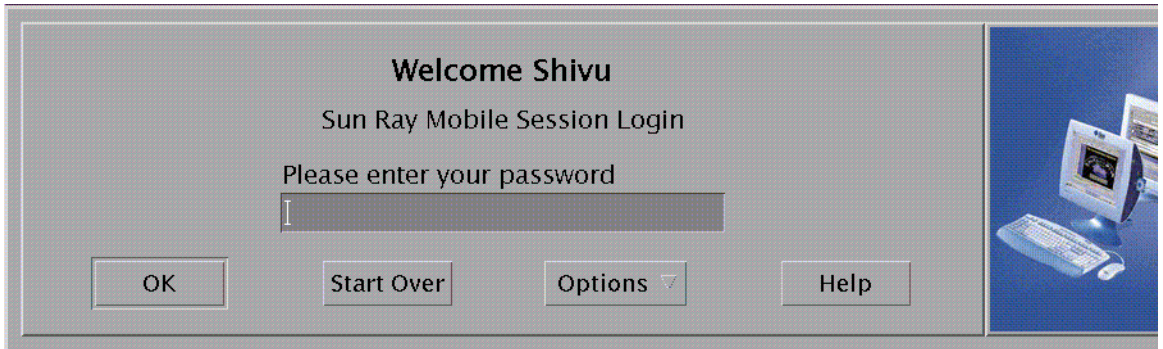
FIGURE 5-2 User Name Entry



If an NSCM session for this user does not exist, the Authentication Manager creates an NSCM session token for the user. The token has the format: `mobile.username`, where `username` is the user's identification.

If the Sun Ray server is part of a failover group, the load-balancing algorithm may redirect the user to another Sun Ray server, where the user types a username and password again before an NSCM session is created.

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.



**FIGURE 5-3** User Password Entry

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 may be 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.

---

---

**Tip** – 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.

---

If an NSCM session exists on the current Sun Ray server, the session is displayed to the user. If a user wants to move to another location, there are two methods of disconnecting an NSCM session:

**2. Type the `utdetach` command in a shell window:**

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

### 3. 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.

### 4. Repeat Step 1 at the second Sun Ray appliance.

The session becomes active.

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** – 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 NSCM session:

- Hot Key combination
- `utdetach`

### Hot Key

To disconnect a NSCM session, the user presses the key combination Shift-Pause.

### ▼ To Disconnect the Current Session

- Press the key combination Shift-Pause.

or

- Type:

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

### ▼ To Terminate the Current Session

- Click the Exit button on the CDE panel.

or

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

## ▼ To Reconfigure the Disconnect Hot Key Combination

You can change the disconnect key combination (hot key) in the `/etc/opt/SUNWut/utslaunch_defaults.properties` file, where the site-wide default configuration of the hotkey key combination is specified. Individual users can override the default key combination by configuring the `~/.utslaunch.properties` file located in their home directory.

- **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, to configure the key combination of Alt + Esc, type:

```
% utdetach.hotkey=Alt Escape
```

## ▼ To Create a `utdetach` Alias

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

- **As superuser, type the following command line to create an alias for all users:**

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

## ▼ To Customize the Short Cut for Disconnecting an NSCM Session

You can disconnect the current session using the key combination (hot key) in the `utslaunch.properties` files.

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 Escape
```

configures the key combination of Alt+Esc.

---

## NSCM and Failover Groups

The user login experience for NSCM sessions may be different than expected when systems are configured as part of a failover group.

The Sun Ray Authentication Manager uses a properties file, `/etc/opt/SUNWut/auth.props`. When the system is first configured, the `acceptRedirectToken` property in this file is set to `false` to support a model of high security by default. Because the property is set to `false`, the following situations may produce unfamiliar behavior:

### Load Balancing Between Servers

If server A is heavily loaded when a user logs into it with the NSCM GUI, it redirects the user to server B, which requires another login with the NSCM GUI. If server B is running an earlier Solaris version than Server A, the user must log in a third time. Thus, the user gets a session, but only after three logins. Users accustomed to smart card ease of use might find this repetitious behavior confusing or annoying.

### Connecting to Existing Sessions

If a user with an existing session on server B logs in to server A, the user is redirected and must log in a second time using the NSCM GUI. Instead of simply inserting a smart card, the user must log in twice to use NSCM sessions.

### Switching Between Servers

A user with a session on server A who wants to switch to a session on server B invokes the `utselect` GUI to access the other session. In doing so, the user is required to log in with the NSCM GUI. Users familiar with the ease of the `utselect` GUI might be discouraged that another log in is necessary.

## Escape Token Sessions

The user bypasses the NSCM GUI by clicking the Exit button and logs into server A using `dtlogin`. The user now has a standard escape token session and 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 escape 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 Sun Ray administrator can enable the NSCM session features with:

- Sun Ray Administration Tool
- Command-line interface

---

**Note** – 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. In particular, configuring the Sun Ray server’s interconnect IP address as a duplicate of any other server’s interconnect IP address may cause the Sun Ray Authentication Manager to throw “ Out of Memory” errors.

---

## ▼ 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.**

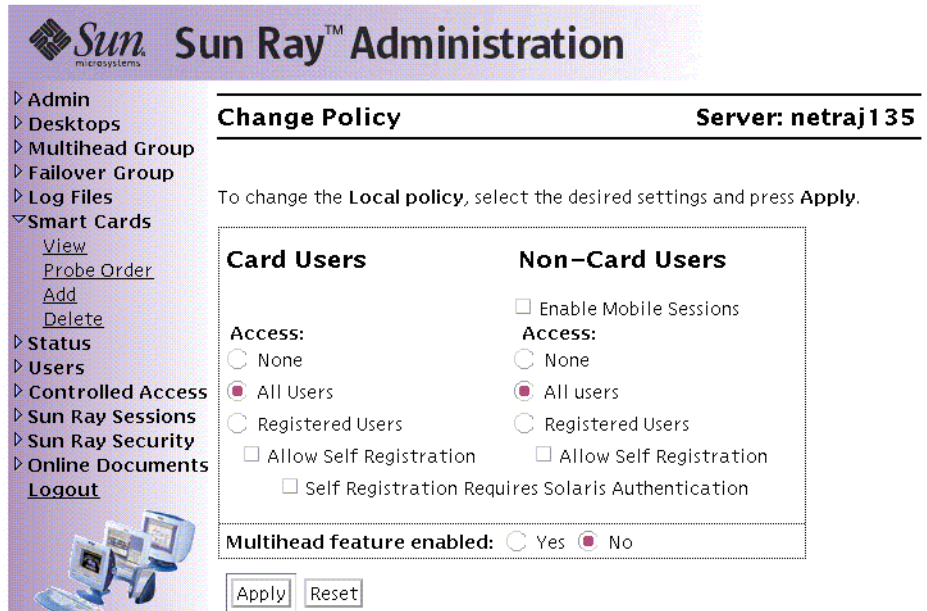


FIGURE 5-4 Change Policy Window

**5. Click the Apply button.**

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

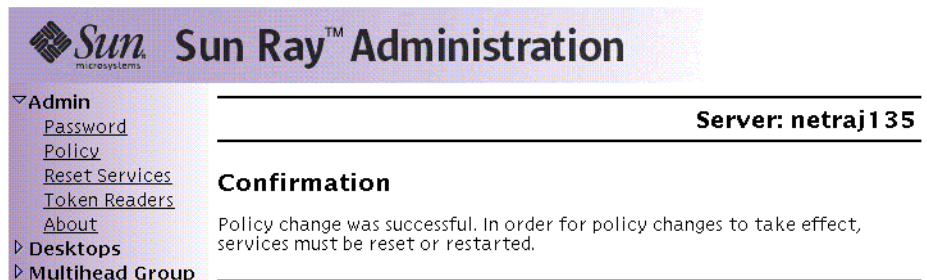


FIGURE 5-5 Change Policy Confirmation Window

**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 NSCM 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` command. For more information, see the `utpolicy` man page.

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` 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 NSCM sessions are enabled.

3. **Initialize Sun Ray services.**

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

```
# /opt/SUNWut/sbin/utrestart -c
```

This command clears all active and detached sessions

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



# Encryption and Authentication

---

The SunRay Server Software 2.0 release provides interconnect security. Two main aspects of this feature are:

- Traffic encryption between the SunRay client and server
  - SunRay server-to-client authentication
- 

## Introduction

In earlier versions of Sun Ray Server Software, data packets on the SunRay interconnect were sent in the clear. This made it easy to “snoop” the traffic and recover vital and private user information, which malicious users might misuse. To avoid this type of attack, SunRay 2.0 allows administrators to enable traffic encryption. This feature is optional; the system or network administrator can configure it based on site requirements.

The ARCFOUR encryption algorithm, selected for its speed and relatively low CPU overhead, supports a higher level of security between Sun Ray services and SunRay desktop units. In the 2.0 release, only the X server traffic is encrypted.

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

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

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

---

## Security Configuration

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

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

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

## Security Mode

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

For example, in hard security mode, if any SunRay appliance that does not support security features (for instance, because of old firmware) connects to a Sun Ray 2.0 server, the server denies the session.

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

For more information, please see the man page for `utcrypto` or “Administration Tool” on page 37.

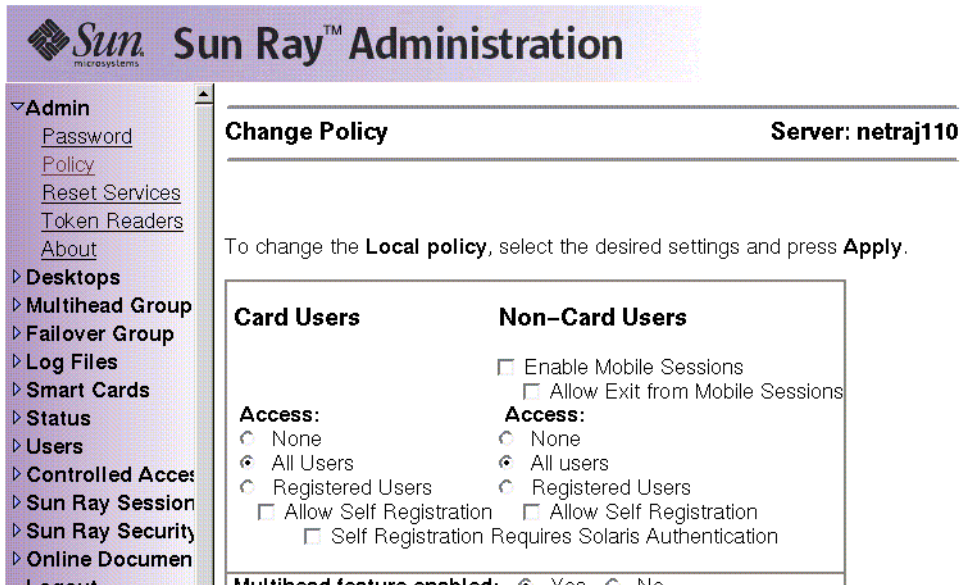


FIGURE 6-1 Sun Ray Security Configuration Window

## Session Security

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

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

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

# Security Status

Once a connection has been successfully established between a client and a server, the user can determine whether the connection is secure at any time by pressing the three volume keys together (currently used to determine MAC address of the terminal).

One of the following icons is also displayed when a Sun Ray appliance connects to a session. Each icon displays information about connection security status.

There are several variations on the security icon:

## Locked Authenticated



The server is authenticated to the client and the data link is encrypted.

## Locked Not Authenticated



The server is not authenticated to the client and the data link is encrypted.

## Unlocked Not Authenticated



The server is not authenticated to the client and the data link is not encrypted.



### Unlocked Authenticated

The server is authenticated to the client but the data link is not encrypted.

## Session Connection Failures

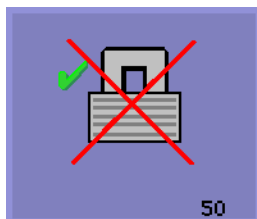
The following icons are displayed when there might be a security breach.



### Session Refused

Definition: The client is refusing to connect to a server because it is unable to verify the validity of the Sun Ray server.

This error can occur only if an unknown Sun Ray server intercepts the messages and tries to emulate a valid Sun Ray server. This is a session security breach.



### Session Refused

Definition: The server is refusing to grant a session to the client because the client is unable to fulfill the server's security requirements.

Actions to take:

- Check the client's firmware version. This error may occur with firmware versions earlier than 2.0 if the server is configured for hard security mode.
- Upgrade the firmware to version 2.0 or later. As an alternative, confirm whether your site requires hard security mode. If not, the session can be enabled with soft security mode.



# Network Configuration

---

This chapter describes the network infrastructure required to deliver Sun Ray services to the Sun Ray clients.

Topics include:

- “Introduction” on page 103
- “Network Infrastructure Requirements” on page 104
- “Network Topology” on page 105

---

## Introduction

The Sun Ray system employs a highly network-dependent computing model in which all actual computing is performed at a server, and display data, as well as mouse, keyboard and other device traffic, are sent over the network.

A well-designed network between server and appliances is essential for providing high quality of service to users; poor network design can make the Sun Ray unusable.

Sun Ray Server Software 2.0 enables shared as well as dedicated network support. The network segment between Sun Ray server and the Sun Ray clients may be any kind of network as long as it meets the Sun Ray network infrastructure requirements.

---

# Network Infrastructure Requirements

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

## Packet Loss

Packet loss between any Sun Ray client and its server must not exceed 0.1% for any extended period of time, such as a minute or more.

The `utcapture` utility reports the packet loss statistics for each of the Sun Ray clients connected.

## Latency

Latency between any Sun Ray client and its server must not exceed 25ms for any extended period of time, such as a minute or more. The `utcapture` utility reports round-trip latency statistics for each connected Sun Ray client.

## Out-of-Order Packets

Sun Ray clients can handle occasional out-of-order packets, but if the network segment generates a large number of out-of-order packets, the quality of service delivered to the Sun Ray client suffers. Out-of-order packets are counted as dropped packets and are reported to `utcapture`.

## DHCP Services

Sun Ray desktop appliances are stateless, and they rely entirely on network services.

When a Sun Ray DTU is powered on and plugged into a network, it sends a Dynamic Host Configuration Protocol (DHCP) request for a network address. At the most basic level of operation, on a dedicated network, the Sun Ray server responds with an IP address and some additional tags, or vendor options. If the server has a later version than the one installed on the DTU, the Sun Ray DTU can use this information to upgrade its firmware. It then either reconnects to an existing session or starts a new session on a Sun Ray server.



On a shared network, the Sun Ray DTU may receive only a network address in response to its DHCP request. It then sends a second DHCP request for network parameters. If the DTU resides on a different subnet than the Sun Ray server, then it needs the help of `bootp` forwarding to reach the Sun Ray server; the Sun Ray server can then reply with the information the DTU needs in order to start a session.

All Sun Ray appliances must have access to at least one DHCP service for network parameters and should also have access to Sun Ray parameters. Depending on your physical network topology, you may need to configure a `bootp` forwarding agent for each subnetwork to which Sun Ray clients are connected. If it receives no parameters, then the DTU broadcasts a server location request.

---

## Network Topology

Beginning with the 2.0 release, Sun Ray servers and appliances can be deployed in shared as well as dedicated networks. The following table lists the various configuration options based on the ease of set-up and quality of service that can be expected. (The easiest option is listed first.)

**TABLE 7-1** Most Desirable Network Topologies

Rank	Order	Private/Public IP Addresses	Dedicated/Shared	Configuration
1		either	dedicated	interconnect
2		either	dedicated	VLAN interconnect
3		either	dedicated	routed interconnect
4		either	shared	interconnect with or without VLAN
5		either	shared	routed interconnect with or without VLAN

Generally speaking, less complexity provides more reliability; however, with careful planning, it is possible to gain the advantages of increased functionality and still maintain a high degree of reliability.

# DHCP Configuration

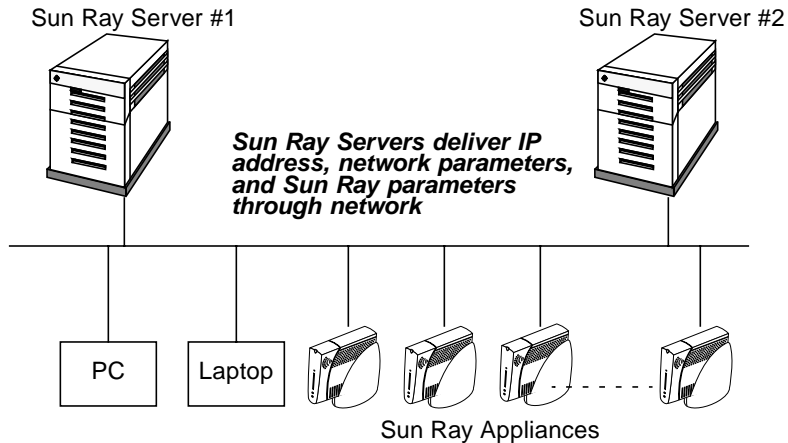
In shared deployments, a DHCP server may be available on the network. With Sun Ray Server Software 2.0, you need not disturb the existing DHCP infrastructure. The following table shows the four possible options, in order of increasing complexity.

**TABLE 7-2** DHCP Configuration Options

Routed? (Y/N)	Existing DHCP Server? (Y/N)	Figure #
N	N	Figure 7-1 on page 106
Y	N	Figure 7-2 on page 107
N	Y	Figure 7-3 on page 108
Y	Y	Figure 7-4 on page 109

## No DHCP Service on the Network

If there is no existing DHCP server on your network, configure the Sun Ray server to deliver both network and Sun Ray parameters. A non-routed solution that uses the Sun Ray server for DHCP service is depicted in FIGURE 7-1.



**FIGURE 7-1** Non-routed Configuration with No Separate DHCP Server

---

**Note** – If you choose not to use a Sun Ray server for DHCP services, you must provide Sun Ray parameters through a separate DHCP server. Since all the tools provided as part of Sun Ray Server Software are written to work only with Sun Ray servers, making this choice means you must configure and maintain the DHCP server manually. See Appendix C for further details.

---

FIGURE 7-2 shows a routed configuration with no separate DHCP server:

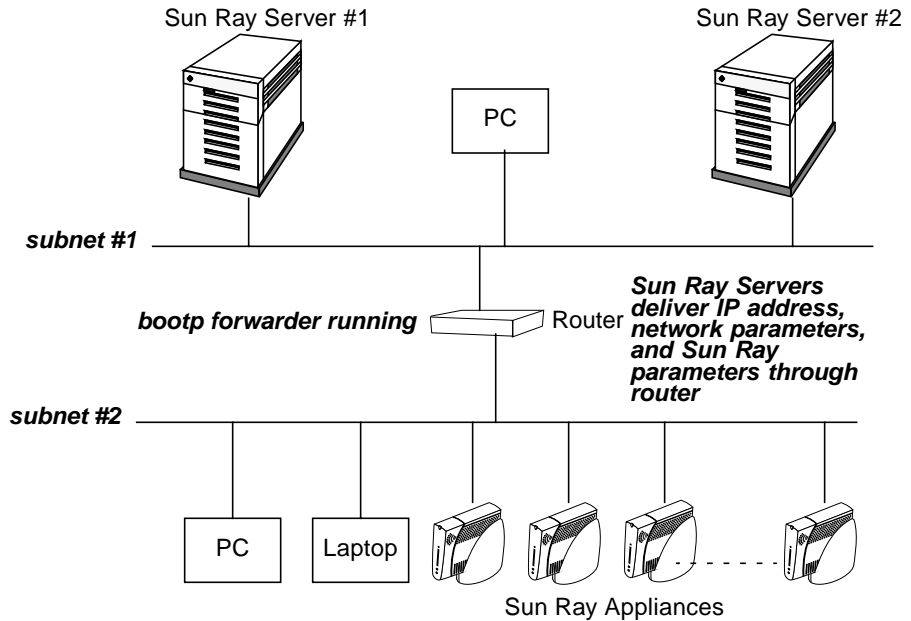


FIGURE 7-2 Routed Configuration with No Separate DHCP Server

## Existing DHCP Service for Network Parameters

To use an existing DHCP server on your network, use the `utadm` command to:

- Configure the Sun Ray server to deliver Sun Ray parameters only
- Run a `bootp` proxy for each of the subnets where Sun Ray clients are located.

The forwarder points to one of the Sun Ray servers. For better fault tolerance, you may run multiple forwarders.

FIGURE 7-3 shows a non-routed configuration with a separate DHCP server:

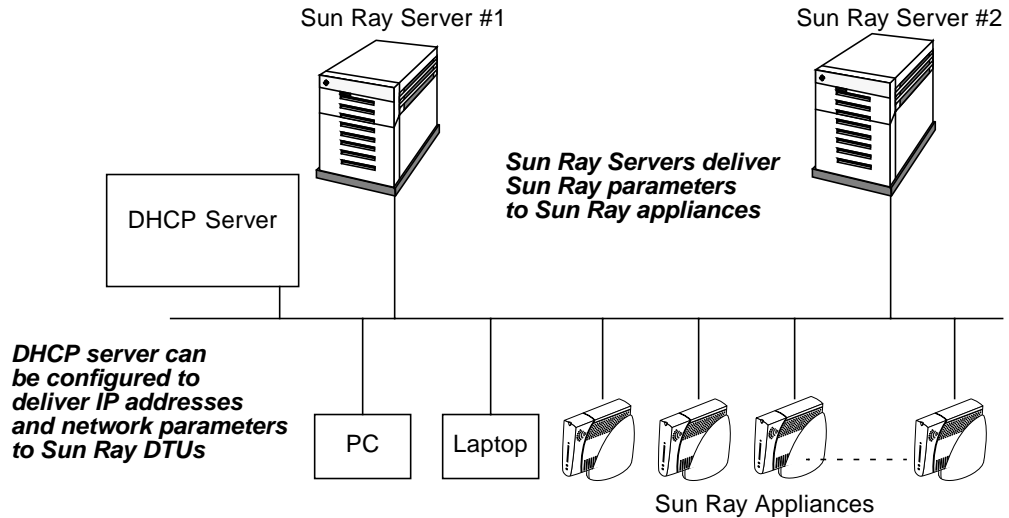


FIGURE 7-3 Non-routed Configuration with Separate DHCP Server

## Using Separate DHCP Servers

If you choose to use a separate DHCP server, it must deliver both network parameters and Sun Ray parameters.

If you want to use separate DHCP servers to supply network parameters only, and Sun Ray servers to supply Sun Ray parameters, then the Sun Ray servers must run Sun Ray Server Software 2.0, and the Sun Ray clients must run at least version 2.0 firmware.

Sun Ray clients running firmware versions lower than 2.0 in this configuration cannot locate a Sun Ray server. Thus, they cannot:

- Obtain the required Sun Ray parameters
- Download firmware updates on their own

FIGURE 7-4 illustrates a routed configuration with an existing DHCP server:

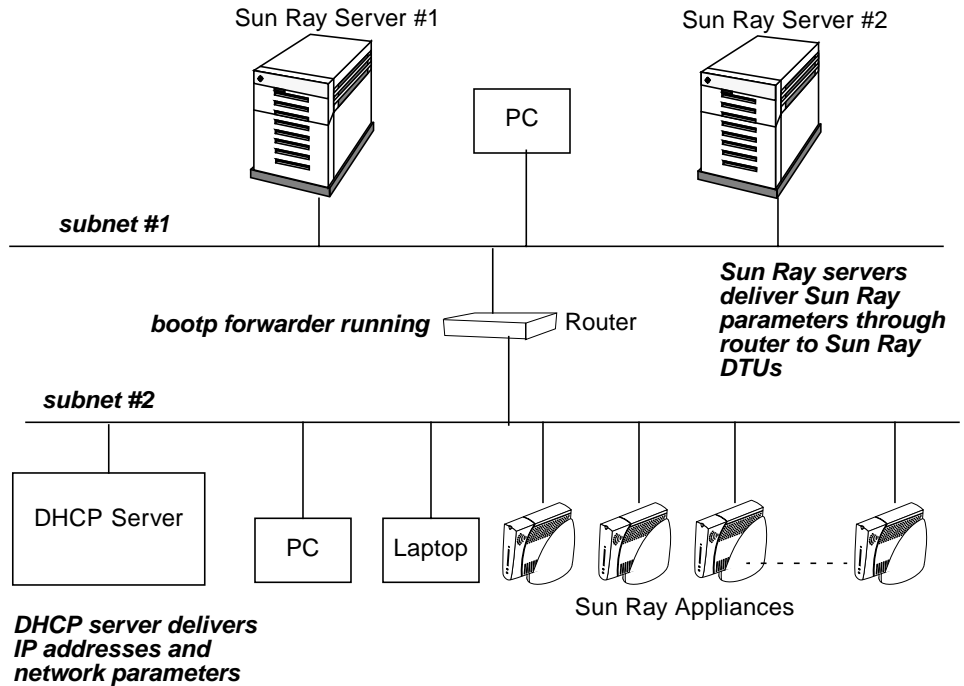


FIGURE 7-4 Routed Configuration with Separate DHCP Server

Consequently, to correct this situation—to upgrade older clients to 2.0 firmware, or to restore 2.0 firmware to clients that have been downgraded—establish a *filling station*, where clients can retrieve the latest firmware. For this purpose, you can use:

- Any private network configured for Sun Ray services
- Any shared network in which the Sun Ray DHCP server is the only DHCP server

---

**Note** – Make sure that each Sun Ray client deployed in this configuration runs the 2.0 or later version of the firmware before you install it on the shared network.

---

## Firmware Barrier

The *firmware barrier* is a new feature in Sun Ray Server Software 2.0 that helps administrators maintain extra control over Sun Ray appliance firmware versions.

Client firmware is now associated with a barrier level. When a client tries to download firmware, the barrier levels of the current firmware and the firmware to be downloaded are compared.

If the firmware to be downloaded has a lower barrier level than the current firmware, the client is prevented from downloading the older firmware. Thus, the default barrier level prevents units upgraded to 2.0 firmware from reverting to a lower, less capable version, and the administrator seldom has to send clients to a filling station.

The barrier level symbol `BarrierLevel` is defined by default in the DHCP table of Sun Ray servers running version 2.0 or later. If the `BarrierLevel` parameter is present in the DHCP response, it is used for the comparison. If the `BarrierLevel` symbol is not present, however, the client uses its internal value for the comparison. The administrator can specify the firmware barrier level by assigning a value to `BarrierLevel`.

The barrier level for firmware shipped with Sun Ray Server Software 2.0 is set to a value of 200. Firmware shipped with previous versions of Sun Ray Server Software had no Barrier Level, which equates to a `BarrierLevel` of 0. Therefore, clients running 2.0 firmware do not download firmware versions shipped with previous releases of Sun Ray Server Software unless the DHCP `BarrierLevel` is set to 0.

## ▼ To Override the Firmware Barrier Level

If you are running 1.3 or earlier versions of Sun Ray Server Software:

1. **Inspect the DHCP table to see whether the barrier mechanism is defined.**

```
# dhtadm -P
```

The `-P` option displays the symbols and macros defined in the DHCP table (see Appendix C). If the `BarrierLevel` symbol is not defined, go to step 2.

2. **Add the definition of the `BarrierLevel` symbol to the DHCP table.**

```
# dhtadm -A -s BarrierLevel -d Vendor=SUNW.NewT.SUNW,36,NUMBER,4,1
```

3. **To force the Sun Ray clients in your network to downgrade from 2.0 firmware, set the `BarrierLevel` value in the DHCP table for the network to 0.**

```
# dhtadm -M -m <network macro> -e BarrierLevel=0
```

As an alternative, you can simply remove the `BarrierLevel` symbol from the network macro.

```
# dhtadm -M -m <network macro> -e BarrierLevel=
```

## Other Configuration Issues

- To get the best speed and mode, connect Sun Ray clients to switches that are capable of auto-negotiation.
- Servers in a failover group need to be able to locate one another. If they are on the same subnet in at least one of their interfaces, they can use subnet broadcast to discover each other; otherwise, they can use IP multicast.
- Every server in a Sun Ray failover group should be reachable from the Sun Ray clients.
- Enabling the Spanning Tree protocol in the switches causes the Sun Ray client to take more time to connect to the server when power cycled. To avoid this problem, disable the Spanning Tree protocol in the switches for ports that are connected directly to Sun Ray DTUs or Sun Ray servers.
- To reduce performance hits caused by various network issues in VLAN implementations, assign the Sun Ray segment a higher priority.
- IP addresses sometimes get marked as unusable during system boot if they are perceived to be in use. If this occurs, use the `dhcpmgr` tool to diagnose the problem, and release the IP addresses back into the pool.





# Monitoring the Sun Ray System

---

This chapter describes how to use the Sun Management Center software to monitor the Sun Ray System.

Topics include:

- “Sun Management Center (SunMC) Software Features” on page 113
- “SunMC Software Requirements” on page 115
- “Installing the SunMC Software” on page 116
- “Setting Up the Monitoring Environment” on page 119
- “Setting Monitoring Guidelines” on page 126
- “Using Other Monitoring Programs” on page 132
- “Removing the Sun Ray Module from SunMC” on page 134

---

## Sun Management Center (SunMC) Software Features

The Sun™ Management Center software monitors managed objects in the Sun Ray system. A *managed object* is any object that can be monitored. Sun Ray nodes contain many managed objects. The Create Topology Object dialog box enables you to create a Sun Ray node. If the Sun Ray packages are installed when you create a Sun Ray node, the following managed objects are created by default:

- Sun Ray system
- Sun Ray services
- Failover group
- Interconnect
- Desktops

Each managed object is monitored separately and has independent alarm settings.

For example, in a failover configuration, the entire group as well as any part of the group can be monitored—each server and its load, each interconnect, and each appliance. Sun Management Center software also monitors Sun Ray Server Software daemons that:

- Authenticate users
- Start sessions
- Manage peripheral devices
- Handle DHCP services

After you set an alarm, the Sun Management Center software notifies you when your specified parameter value has been reached. For example, you might want to track the number of appliances on a server so that you can monitor possible overload scenarios. Other alarms can be set to notify you when a server, interconnect, or appliance goes down or when a daemon is not running.

The three Sun Management Center components (TABLE 8-1) can be installed on three separate machines.

**TABLE 8-1** Three Components of Sun Management Center Software

Component	Function
Console	Enables you to set and view alarms and to request system information. Requests can be automated or on demand.
Server	Processes requests and passes them on to the appropriate agent. The agent returns the requested information to the server, which then forwards it to the console.
Agents	Monitor the system. Agents return the requested information to the server. These agents, based on SNMP (Simple Network Management Protocol), monitor the status of the <i>managed object</i> (server, interface, or appliance).

Sun Ray system monitoring consists of ten packages, which are installed as part of Sun Ray Server Software 2.0. If you run the Sun Management Center on a non-Sun Ray server, you must add some packages that contain localized messages and icons to the Sun Management Center monitoring server.

This feature interfaces with the Sun Management Center software using SNMP. For information on additional monitoring programs that interact with Sun Management Center software, see “Using Other Monitoring Programs” on page 132.

---

# SunMC Software Requirements

The Sun Ray system monitoring feature has the following software requirements:

- Sun Management Center 2.1.1 or 3.0 software
- Sun Ray Server Software 2.0

The Sun Ray module adds the following requirements when added to either the Sun Management Center server or agent component:

**TABLE 8-2** Additional Requirements for the Server

Component	Size
RAM	8 KB
/opt/SUNWut	153 KB
/opt/SUNWsymon	12 KB

**TABLE 8-3** Additional Requirements for the Agent

Component	Size
RAM	1 MB
Swap	1 MB
/opt/SUNWut	602 KB
/opt/SUNWsymon	12 KB
/var/opt/SUNWsymon	0.5 KB

The Sun Ray module adds the following requirements to the Sun Management Center server and agent components:

**TABLE 8-4** Additional Requirements to the Server and Agent Components

Component	Size
RAM	1008 KB
Swap	1 MB
/opt/SUNWut	602 KB
/opt/SUNWsymon	12 KB
/var/opt/SUNWsymon	.5 KB

---

**Caution** – The Sun Management Center server component has very high resource requirements. Do not install the complete Sun Management Center software on a Sun Ray server, especially if the Sun Ray server is configured for failover.

---

---

## Installing the SunMC Software

Sun Ray Server Software includes a module for interfacing with Sun Management Center software. If Sun Ray Server Software and Sun Management Center software are to run on the same server, different procedures are used, depending on the order in which the software is installed. If Sun Ray Server Software and Sun Management Center server component are configured on separate servers, then the module must be installed on both servers.

If you are doing a clean installation of Sun Management Center software and Sun Ray Server Software on the same server, it is easier to install Sun Management Center software first.

When you install Sun Management Center software, you are given the option of installing any of the three components on the selected server. If you want to add only the agent to a Sun Ray server, just choose to add the agent component.

After the appropriate hardware configuration product is installed on the server, you can choose to run the setup now or later. When you run the setup, you are prompted for a host name of Sun Management Center server, a seed to generate security keys, a base URL for the console, and if there is a conflict, a different port for the agent.

---

**Tip** – To monitor all the servers in a failover group, make sure every server runs Sun Ray Server Software 1.3 or 2.0. In addition, all servers must run the Sun Management Center agent component.

---

### ▼ To Install Sun Ray Server Software After Installing the Sun Management Center Software

#### 1. Start the Sun Management Center software:

```
# /opt/SUNWsymon/sbin/es-start -c &
```

Check to see if the Sun Management Center works. If not, reinstall the Sun Management Center software. Use the *Sun Management Center 3.0 Software Installation Guide* and the *Sun Management Center 3.0 Software User's Guide* to install the Sun Management Center software.

**2. Use the standard Sun Ray installation script to add the Sun Ray module:**

```
# utinstall
```

If the Sun Management Center agent software is running, the standard Sun Ray install script automatically stops it, adds the Sun Ray module, and restarts the Sun Management Center agent software.

If the Sun Management Center agent software is not running, the Sun Ray install script adds the Sun Ray module but does not start the Sun Management Center agent software.

▼ **To Install Sun Management Center Software After Installing Sun Ray Server Software**

**1. Use the standard Sun Ray installation script:**

```
# utinstall
```

The Sun Ray module for SunMC is installed automatically on the server when `utinstall` installs Sun Ray Server Software.

**2. Follow the installation instructions found in the *Sun Management Center 3.0 Software Installation Guide* to install the Sun Management Center software.**

**3. Type the following to enable Sun Ray monitoring:**

```
# /opt/SUNWut/sbin/utsunmc
```

**4. Start the Sun Management Center software:**

```
# /opt/SUNWsymon/sbin/es-start -c &
```

Check to see if Sun Management Center works. If not, reinstall the Sun Management Center software.

## ▼ To Install the SunMC Agent on Separate Servers

1. Verify that the Sun Management Center agent, `SUNWesagt`, is installed on the Sun Ray server:

```
# pkginfo -l SUNWesagt
```

2. Perform a standard installation of Sun Ray Server Software:

```
# utinstall
```

If the Sun Management Center agent is running, the installation process stops and restarts the SunMC software.

---

**Note** – You can install Sun Management Center agents after Sun Ray Server Software installation; however, you must then enable the Sun Ray module by typing `/opt/SUNWut/sbin/utsunmc` to register the Sun Ray module with the SunMC.

---

3. Install the Sun Ray interface package on the Sun Management Center server:

If you have already mounted the Sun Ray Server Software 2.0 CD-ROM on the SunMC server or from a remote server, or if you have extracted the ESD files to an image directory, begin at Step c.

- a. As superuser, open a shell window on the SunMC server.

- b. Insert the Sun Ray Server Software 2.0 CD-ROM

If a File Manager window opens, close it. The File Manger CD-ROM window is not necessary for installation.

- c. Change to the image directory. For example:

```
# cd /cdrom/cdrom0
```

- d. Install the Sun Ray module:

```
# ./utsunmcinstall
```

The installation process begins. The `utsunmcinstall` script:

- Verifies that the SunMC software is installed.
- Verifies that Sun Ray Server Software is *not* installed.

- Installs the parts of the Sun Ray module needed on the SunMC server.

---

## Additional Sun Management Center Modules

There are other useful Sun Management Center modules available to monitor processes and help tune your Sun Ray system. For example, the Health Monitor module monitors resources on the Sun Ray server so you know when to add memory, swap space, or additional CPUs. The Sun Management Center Process Monitoring module helps identify runaway processes and limit multimedia applications.

---

## Setting Up the Monitoring Environment

After installing the Sun Management Center software, you need to set up your monitoring environment. A default administrative domain is automatically created for you based on the Sun Management Center server component. You need to set a home administrative domain. This domain is displayed whenever the console is started. Next, create the hierarchy of the system you want to monitor. This can be done manually by adding nodes to the administrative domain or by using the Discovery Manager.

### ▼ To Set Up the Monitoring Environment

1. **After installing the Sun Management Center software, start the console on the server that has the console component installed:**

```
# /opt/SUNWsymon/sbin/es-start -c &
```

The login screen is displayed.

2. **Enter your user name and password.**

Specify the Sun Management Center server.

3. **Click Login.**

The Sun Management Center window is displayed. If this is your first time using the SunMC console, the Set Home Domain window is also displayed.

4. **In the Set Home Domain window, highlight the appropriate domain and click Go To.**

The panels in the Sun Management Center window are populated.

5. **Click Close to dismiss the Set Home Domain window.**

## ▼ To Create an Object

1. **Expand the Sun Management Center Domains list.**

2. **Select the domain you plan to add an object to.**

The selected domain is displayed.

3. **Select Edit -> Create an Object.**

The Create Topology Object pop-up window is displayed.

4. **On the Node page, enter a Node Label and Description. Then enter the Hostname (server name), IP Address, and Port for the Sun Ray server.**

The port entered here must be the same port you configured (entered) during the installation of the Sun Management Center.

## Setting Alarms

Alarms are used to notify you when errors occur or your performance needs to be tuned. Alarms are triggered (tripped) if:

- A server goes down.
- An interconnect is no longer working.
- An appliance is down.

These alarms are set by default, but you can change them. Base a tuning alarm on the number of active sessions on each server in a failover group to determine if one of the servers is overloaded. You set the thresholds that trigger this type of alarm.

## ▼ To Set an Alarm

1. **After creating an object, bring up the Details window of the object.**



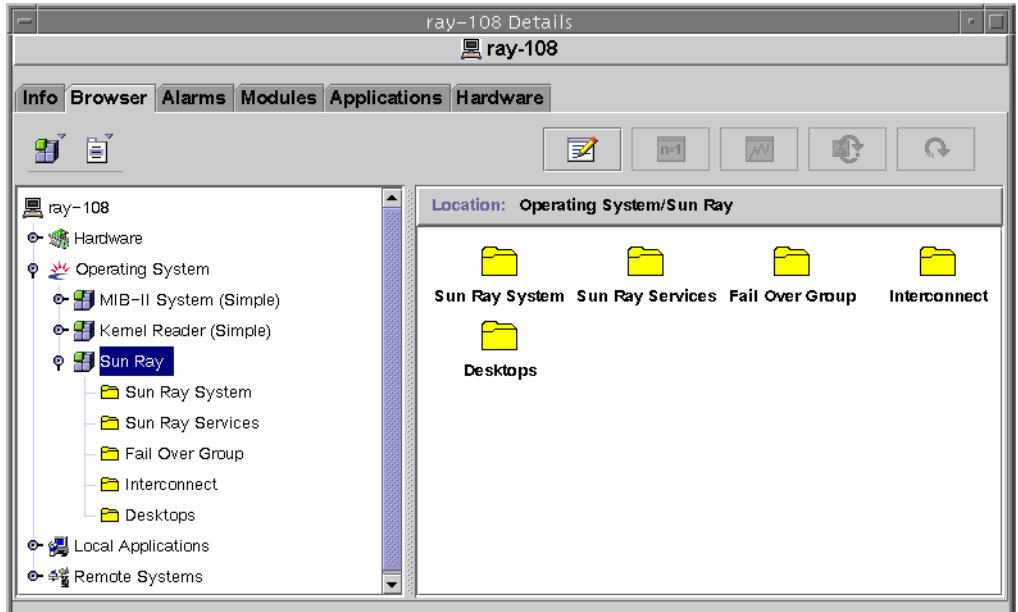


FIGURE 8-1 Sun Management Center Details Window

2. Double-click, for example, Failover Group in the left panel.
3. Right-click the value portion (Status) of the table row.

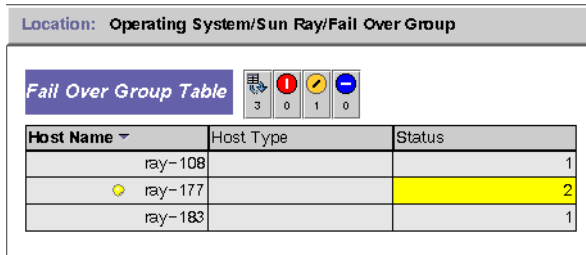


FIGURE 8-2 Example Using the Failover Group Panel

A pop-up menu is displayed.

4. Select Attribute Editor.

The Attribute Editor window for that table entry is displayed.

5. Select the Alarms tab (See FIGURE 8-3.)

The possible alarm values are:

- Critical Threshold (>)

- Alert Threshold (>)
- Caution Threshold (>)
- Critical Threshold (<)
- Alert Threshold (<)
- Caution Threshold (<)

**6. Supply an appropriate number for the type of alarm that you choose to monitor.**

In this example, the Alert Threshold alarm is set at greater than 1 to notify you when that server in the failover group is down.

**7. Click the Apply button to save the value of the alarm and continue setting other values in the Attribute Editor**

**8. Click the OK button, which saves the value of the alarm and closes the window.**

As soon as you set an alarm it takes effect.

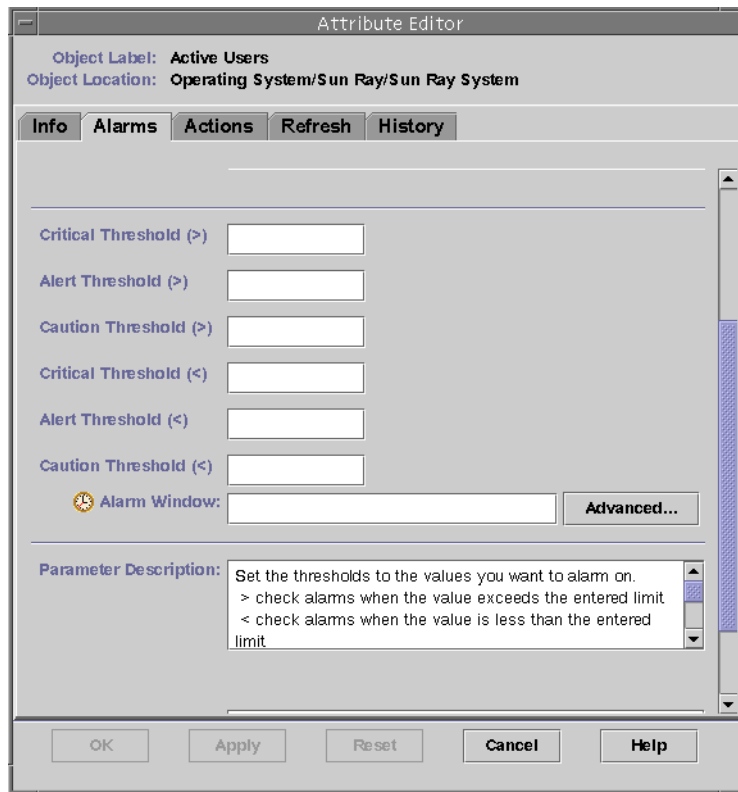
**9. Select the Actions tab and enter an action to perform.**

Here you can also specify an action such as sending email or running a script for each alarm.

**10. Select the Refresh tab to set the number of seconds between pollings.**

The default value is 300 seconds (5 minutes).

**11. Select the History tab to view information about the log file that records monitored values.**



**FIGURE 8-3** Alarm Window

If an alarm is tripped, a critical alarm displays as red, an alert alarm displays as yellow, and a caution displays as blue (see FIGURE 8-4).

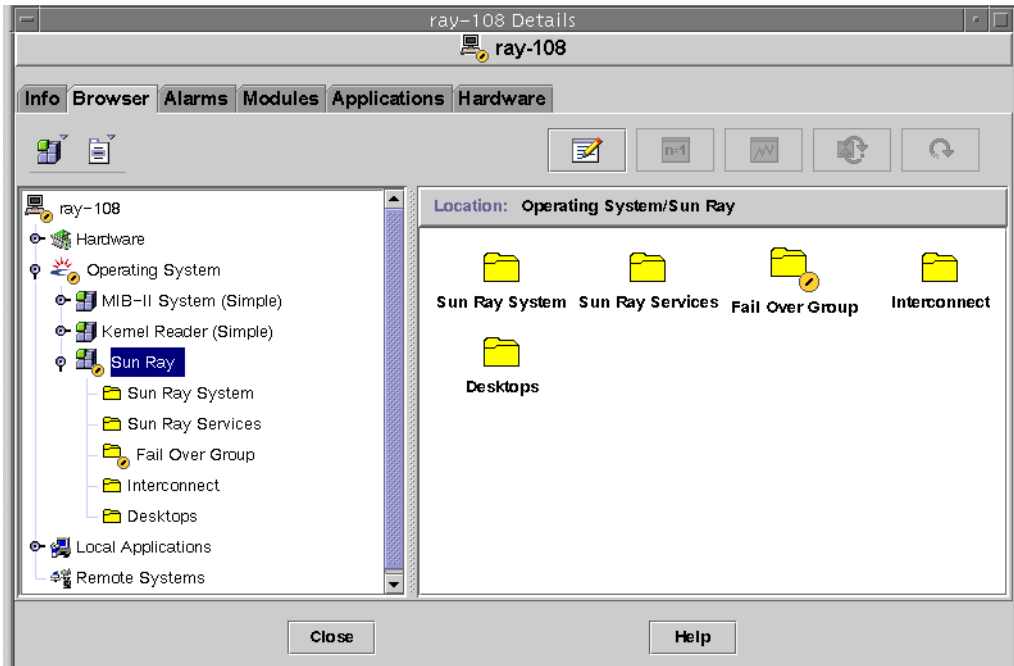
## ▼ To Start Monitoring

1. **Start the Sun Management Center software:**

```
# /opt/SUNWsymon/sbin/es-start -c &
```

A window for the Default domain is displayed.

2. **Log in to the Sun management Center server.**
3. **Double-click the server in either panel.**  
The server Details window is displayed.
4. **Expand the hierarchy in the left or right panel until it displays the level you want.**



**FIGURE 8-4** Details Window With Alarms

This console Details window shows the hierarchical details of your system. You can immediately see if any alarms have been tripped. An alarm's area and type appear in the left panel as a colored circle with a bar. The Alert alarm also shows up on the title bar by the server node name and at the Operating System, Sun Ray, and Failover Group levels. Double-clicking the area where an alarm icon is present updates the right panel with the detailed information. If you position the mouse pointer over one of the colored circles in either panel, a pop-up window is displayed detailing the alarm information.

If you click the Alarms tab in the Details window, a window is displayed that lists a summary of all the current alarms. When you stop the Sun Ray services (daemons), the alarms display as shown in FIGURE 8-5.

✓ 🚧 ↻ 📄

Last Refresh: Apr 05 16:56:01

Current Page: 1

Total Alarms for Object: 12

Severity	Start time	State	Action	Message
🔵	Apr 04 14:05:27	🔔	🚧	Sun Ray utsessiond Instances < 2
🔵	Apr 04 14:05:27	🔔	🚧	Sun Ray utdevmgrd Instances < 2
🔵	Apr 04 14:05:27	🔔	🚧	Sun Ray utseriald Instances < 2
🔴	Apr 04 14:05:27	🔔	🚧	Sun Ray Up Time (1/100ths sec.) Session Manager down
🔵	Apr 04 14:05:27	🔔	🚧	Sun Ray utparallel Instances < 2
🟡	Apr 04 14:05:26	🔔	🚧	Sun Ray utauthd Status > 1
🟡	Apr 04 14:05:26	🔔	🚧	Sun Ray utsessiond Status > 1
🟡	Apr 04 14:05:26	🔔	🚧	Sun Ray utdevmgrd Status > 1
🟡	Apr 04 14:05:26	🔔	🚧	Sun Ray utseriald Status > 1
🟡	Apr 04 14:05:26	🔔	🚧	Sun Ray utparallel Status > 1
🟡	Apr 04 14:05:26	🔔	🚧	Sun Ray in?2edhcpd Status > 1
🟡	Apr 04 14:05:26	🔔	🚧	Sun Ray rpc?2ebootparamd Status > 1

**FIGURE 8-5** Alarm Summary Window

The total number of alarms set for the current server object is displayed at the top of the alarm summary window. Critical alarms (red), alert alarms (yellow), and caution alarms (blue) that are tripped are listed below. Details and comments are displayed in the Message column.

Some cells in the table respond to a mouse-over event by displaying a pop-up window called a *Tool Tip window*. This window shows the current status and when it last changed, plus the type of alarm, its value, and when it occurred or when the last alarm was cleared. The Tool Tip time can also be the last time the agent was restarted. For example, on the Sun Ray System panel, a Tool Tip for Up Time (1/100ths sec.) would be:

Clear. Up Time (1/100th sec.) OK Status changed Mar. 6, 15:23:55.

indicating that the server was restarted and the alarm cleared on March 6 at 15:23:55. Similar information is provided for Active Sessions, Desktops, Users, and Total Sessions.

# Setting Monitoring Guidelines

There are five managed objects that you can monitor:

- Sun Ray System—Describes the Sun Ray server and load information
- Sun Ray Services—Describes the Sun Ray daemons on a Sun Ray server
- Failover Group—Lists all the servers in the group
- Interconnect—Lists all the interfaces on a Sun Ray server
- Desktops—Lists all monitored appliances (desktops) and appliances that have exceptions that are connected to a Sun Ray server

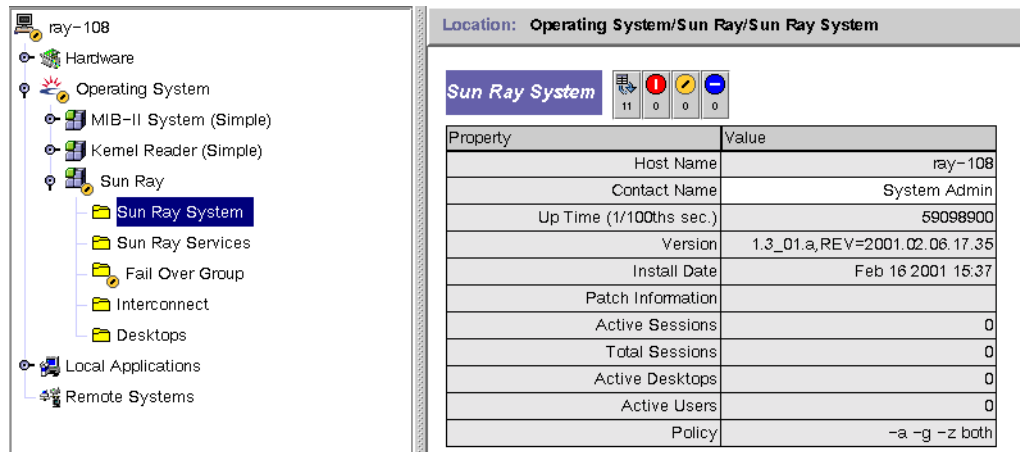
## Sun Ray System Panel

The Sun Ray System panel displays an overview of your Sun Ray system. From this window you can set specific alarms to monitor the server and its load.

### ▼ To Display the Sun Ray System Panel

- **Double-click the Sun Ray System icon in the left panel.**

The Operating System/Sun Ray/Sun Ray System panel is populated.



The screenshot shows the Sun Ray System panel. On the left is a tree view with the following structure:

- ray-108
  - Hardware
  - Operating System
    - MIB-II System (Simple)
    - Kernel Reader (Simple)
    - Sun Ray
      - Sun Ray System** (highlighted)
      - Sun Ray Services
      - Fail Over Group
      - Interconnect
      - Desktops
    - Local Applications
    - Remote Systems

On the right is the Sun Ray System panel with the following table:

Property	Value
Host Name	ray-108
Contact Name	System Admin
Up Time (1/100ths sec.)	59098900
Version	1.3_01.a,REV=2001.02.06.17.35
Install Date	Feb 16 2001 15:37
Patch Information	
Active Sessions	0
Total Sessions	0
Active Desktops	0
Active Users	0
Policy	-a -g -z both

FIGURE 8-6 Sun Ray System Panel

## ▼ To Refresh the Sun Ray System Panel

- **Click the refresh button (circular arrow in the upper right corner).**

The entire system panel is refreshed.

The Up Time, session, appliance (desktop), and user information is refreshed periodically based on the number of seconds you set in the Attribute Editor. However, the console is updated only every five minutes unless an alarm occurs. The number of seconds set in the Attribute Editor only changes how soon an alarm is triggered.

---

**Tip** – Do not set the seconds to less than 60. The load interferes with the Sun Ray server performance.

---

In this panel, you set alarms to monitor the status of the server; how many sessions, users, or appliances are active; and how many total sessions exist.

## ▼ To Set Alarms

1. **Click the Value cell of the Property you want to set an alarm for with the right mouse button.**
2. **Select Attribute Editor.**
3. **Click the Alarms tab.**
4. **Enter a value for each threshold you want to monitor.**
5. **Click OK.**

**TABLE 8-5** Properties on the Sun Ray System Panel

Property	Value
Host Name	Name of server that was queried. This information is obtained when Sun Ray System is selected or on manual refresh.
Contact Name	This information is obtained when Sun Ray System is selected or on manual refresh.
Up Time (1/100ths sec.)	Number of 1/100th seconds since the last of all the daemons critical to the Sun Ray server was started. A value of 0 means the server is down and an alarm is tripped. The default refresh rate is 300 seconds.
Version	List of version, build, and date of build of Sun Ray Server Software. This information is obtained when Sun Ray System is selected or on manual refresh.

**TABLE 8-5** Properties on the Sun Ray System Panel *(Continued)*

Property	Value
Install Date	Date Sun Ray Server Software was installed. This information is obtained when Sun Ray System is selected or on manual refresh.
Patch Information	List of Sun-Ray-specific patches. This information is obtained when Sun Ray System is selected or on manual refresh.
Active Sessions	Number of sessions based on logged-in sessions with a smart card plugged in, plus sessions for appliances logged in without smart cards. Set an alarm here to watch for overloading of this server. The default refresh rate is 300 seconds.
Total Sessions	Number of active and suspended sessions. The default refresh rate is 300 seconds.
Active Desktops	Number of connected appliances. The default refresh rate is 300 seconds.
Active Users	Number of currently active users. When pseudo tokens are allowed (this is a policy setting), this number includes appliances at the login prompt. The default refresh rate is 300 seconds.
Policy	The policy that has been set. This information is obtained when Sun Ray System is selected or on manual refresh.

## Sun Ray Services Panel

The Sun Ray Services panel displays the status of the Sun Ray daemons. If, for example, `utauthd` is not running, all user sessions are disconnected.

On the Sun Ray Services panel, default alarm values are set for the status of each daemon and the number of instances. You can reset them if you want to.



Daemon	Status	Started Time	Last Changed	Instances	Description
in.dhcpd	1	1030644821	1030644821	1	DHCP daemon
rpc.bootparamd	1	1030480972	1030480972	1	Net boot parameter daemon
utauthd	1	1030481109	1030481109	1	Auth Manager
utdevmgrd	1	1030481108	1030481108	2	Device Manager
utdsd	1	1030480934	1030480934	1	Datastore daemon
utparalleld	1	1030481108	1030481108	2	Parallel Device daemon
utscreventd	2	0	0	0	Smartcard Manager
utseriald	1	1030481109	1030481109	2	Serial Device daemon
utsessiond	1	1030481108	1030481108	2	Session Manager
utwsd	1	1030480942	1030480942	1	Web Admin daemon

FIGURE 8-7 Sun Ray Services (daemons) Panel

The Status values are:

1. The daemon is running;
2. The daemon is down.

Some of the daemons have two instances, corresponding to their two functions: one to listen and one to interact.

---

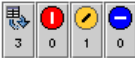
**Note** – The `utscreventd` daemon does not run unless third-party Smart Card software is installed, so no alarm is triggered when the `utscreventd` status is 2.

---

## Failover Group Panel

The Failover Group panel displays the topography of your failover group. The panel lists the primary and secondary servers and their status.

Location: Operating System/Sun Ray/Fail Over Group

**Fail Over Group Table** 


Host Name	Host Type	Status
ray-108	secondary	1
 ray-177	secondary	2
ray-183	primary	1

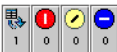
FIGURE 8-8 Failover Group Panel

If the Status is 1, the server is running. If the Status is 2, the server is down and there is one Alert (yellow) alarm.


## Interconnect Panel

The Interconnect panel lists all the network interfaces usable by the Sun Ray server.

Location: Operating System/Sun Ray/Interconnect

**DHCP Table** 

Network Name	Available Addresses
SunRay-hme1	73

**Interface Table** 

Entry Name	Status	Address	Netmask	Last Packet Seen (1/100ths sec)	Lan Type
hme0	1	192.9.116.108	255.255.255.0	1700	LAN
hme1	1	192.168.128.1	255.255.255.0	1700	

FIGURE 8-9 Interconnect Panel

The DHCP Table lists the interfaces that are used for the Sun Ray interconnect. Available Addresses lists the number of addresses available for new end users. The alarms that are set here let the system administrator know when the Sun Ray server is running out of addresses to give to users.

The Interface Table lists all the interfaces on the Sun Ray server. The Address is the IP address for the interface. You entered this address as the Net Mask when you first configured your system.

If the Status is 1, the interface is up. If the Status is 2, the interface is down.

## ▼ To Set an Alarm for Running Out of Addresses

1. **Click the Available Addresses cell in the DHCP Table using the right mouse button.**
2. **Select Attribute Editor.**
3. **Click the Alarms tab.**
4. **Enter the number of addresses left when an alarm should be tripped.**
5. **Click OK.**

## Desktops Panel

The Desktops panel is where you can select individual appliances to monitor. The possible values for the status of the appliances are: 1, running; 2, down; and 3, displaying the green hourglass cursor. The default polling time is 300 seconds (5 minutes).

Appliances can be added and deleted from the Monitored Desktops list.

In a failover group, you can monitor any desktop from any server.

## ▼ To Add an Appliance to Be Monitored

1. **Click Name using the right mouse button.**  
A pop-up menu is displayed.
2. **Click Add Row.**  
A pop-up window is displayed.
3. **In the Add Row window, enter the MAC address of the appliance you want to monitor in the Name field.**
4. **Click OK.**

## ▼ To Delete an Appliance to Exclude Monitoring

1. **Using the right mouse button, click the cell containing the MAC address.**  
A pop-up menu is displayed.
2. **Click Delete Row.**  
A pop-up window is displayed.

### 3. Confirm the deletion by clicking Yes on the pop-up window.

Sample results of polling the Desktops are provided below.

The screenshot shows two tables: 'Monitored Desktops' and 'Desktop Exceptions'. Both tables have columns for Name, IP Address, Status, Packets, Lost Packets, Lost Percent, Location, Optional Data, Server, Model, and Firmware Revision. The Status column uses icons: a green circle with '2' for running, a red circle with '1' for down, and a yellow circle with '3' for displaying the green hourglass cursor. In the 'Monitored Desktops' table, the first row has a yellow '3' icon and the second row has a green '2' icon. The 'Desktop Exceptions' table has one row with a yellow '3' icon.

FIGURE 8-10 Desktops Panel

TABLE 8-6 describes the information in each column:

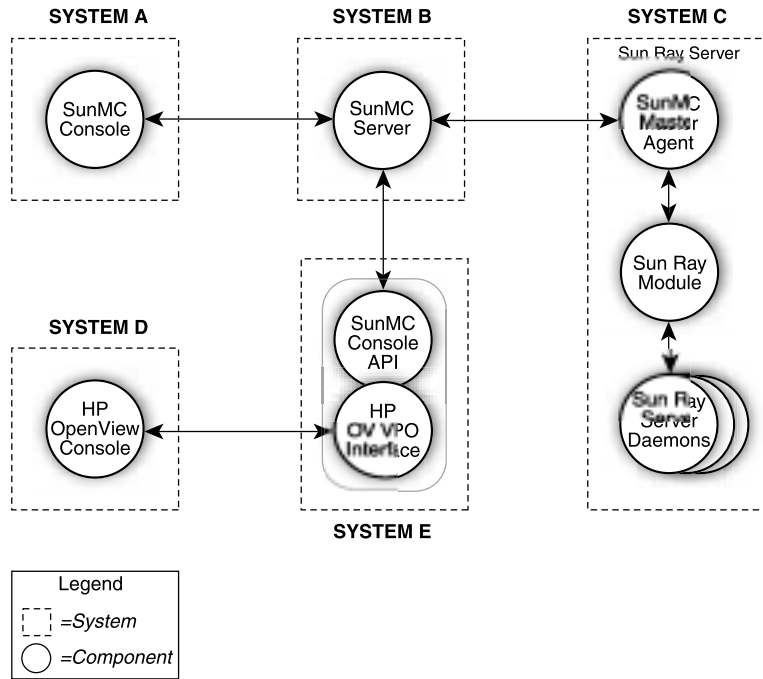
TABLE 8-6 Desktop Information

Property	Value
Name	Ethernet or MAC address of the appliance
IP Address	Assigned DHCP address of the appliance
Status	1 running, 2 down, and 3 displaying the green hourglass cursor
Packets	Number of packets received by the appliance
Lost Packets	Number of packets the appliance reported lost
Lost Percent	Percentage of packets lost
Location	Optional field; information supplied by system administrator
Optional Data	Optional field; information supplied by system administrator
Server	Server that owns the appliance
Model	The type of appliance: SunrayP1 (Sun Ray 1), SunrayP2 (Sun Ray 100), or SunrayP3 (Sun Ray 150)
Firmware Revision	List of version, build, and build date

## Using Other Monitoring Programs

System administrators using HP OpenView™ VPO, Tivoli TMS, or CA Unicenter can also monitor Sun Ray servers. An interoperability interface exists between each of these packages and the Sun Management Center software. These interfaces translate Sun Management Center alarms appropriately so that you are notified when problems arise. These interfaces also enable you to view the server status. Hewlett-

Packard provides the interface needed between HP OpenView™VPO and Sun Management Center. Sun provides the interface needed between Sun Management Center and Tivoli TMS or CA Unicenter.



**FIGURE 8-11** Example of Interoperability (System B, System C, and System E must be SPARC Solaris systems)

---

# Removing the Sun Ray Module from SunMC

The Sun Ray module is uninstalled automatically when the `utinstall` script uninstalls Sun Ray Server Software. If you are uninstalling the Sun management Center software manually, please remove the Sun Ray module first.

## ▼ To Remove the Sun Ray module

- To unregister the module on the Sun Ray server, type:

```
# /opt/SUNWut/sbin/utsummc -u
```

If the SunMC agent is running, `utsummc` stops and restarts the Sun Management Center agent software.

- To remove the Sun Ray module on the SunMC server, type:

```
# /opt/SUNWut/lib/utsummcinstall -u
```

## Multihead Administration

---

The multihead feature on Sun Ray™ appliances enables users to control separate applications on multiple screens, or *heads*, 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 between two and 16 appliances controlled by one keyboard and mouse, may be composed of Sun Ray 1, Sun Ray 100, and Sun Ray 150 appliances. Each appliance presents an X screen of the multihead X display.

---

**Note** – For the multihead feature to function properly:

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

By default, when the user logs into a multihead group, the user gets a multihead session using the number of screens available in that group. The resolution for the group is automatically set to the largest supported resolution of the primary appliance, which is the appliance that controls the other appliances in the group and to which all peripherals are attached. Auto-size can be turned off and the Xserver size can be changed using the `utxconfig` command. Because auto-size affects X display dimensions as well as the initial multihead session group geometry, the user might experience panning or black-band effects.

The user can explicitly choose not to use multiple screens for a session by executing the `utxconfig -m off` command. The user can also choose a particular number of screens in a particular geometry by executing (in the following order):

- the `utxconfig -s off` command to disable autosize
- the `utxconfig -R geometry` command to have it take effect

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

---

## Multihead Groups

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

Unless XINERAMA is enabled (see “XINERAMA” on page 141 for more details), sessions will have a separate CDE toolbar (with separate workspaces) per screen. A window cannot be moved between screens.

The primary appliance hosts the input devices, such as a keyboard and a pointer device, and the USB devices associated with the session. The remaining appliances, called the secondaries, provide the additional displays. All peripherals are attached to the primary appliance, and the group is controlled from the primary appliance.

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

---

**Tip** – For best results, run `utmhconfig` only from a client desktop.

---

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

## Multihead Screen Display

When the multihead feature is used, a small window indicating the current session on each screen is displayed with the current screen highlighted for easy identification. This window is automatically displayed for users during session creation. For example, the display in “XINERAMA” on page 141 indicates that the user is on the second screen of a three-screen display.





FIGURE 9-1 The Multihead Screen Display

## Display Resolution

To avoid panning, all the monitors in a workgroup must support the same resolution.

The auto-size feature sets the user's X server display dimensions automatically to match the preferred resolution supported by the primary appliance when the session is created. This resolution will be the optimum resolution for the multihead group. This feature can be turned off and on using the `utxconfig` command. The default geometry, which is the number of rows and columns in the multihead group, and the screen order are also automatically set when a session is created. This feature can be turned off and on using the `utxconfig` command.

If auto-size is on when you create a session on a 2x1 multihead group, the result is a 2x1 session. If auto-size is turned off, the size of the session is whatever you designate. For instance, if auto-size is off and the geometry is set to 3x1, then even if you log in to a 2x1 multihead group (or even a non-multihead, 1x1 terminal), you will get a 3x1 session with screen flipping. This might be useful if you know you are going to Hot Desk to a 3x1 multihead group in the future and want to take full advantage of it when you get there.

---

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

---

## Multihead Administration Tool

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

## ▼ To Turn On Multihead Policy From the Command Line

- On the command-line interface, type:

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

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

---

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

---

## ▼ To Turn On Multihead Policy Using the Administration Tool

1. **Bring up the Administration Tool by typing the following URL into your browser's location field:**

```
http://hostname:1660
```

2. **Select Admin from the navigation menu on the left side of the tool.**
3. **Select Policy.**
4. **Next to Multihead feature enabled, click the Yes radio button.**
5. **Click the Apply button.**
6. **Under Admin in the lefthand menu, select Reset Services.**
7. **Click the Restart button.**

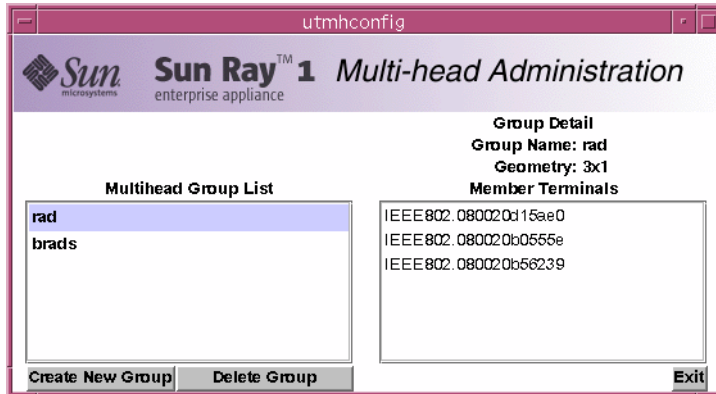
This sets the multihead policy for all servers and restarts Sun Ray Server Software on all servers.

## ▼ To Create a New Multihead Group

1. **On the command-line interface, type:**

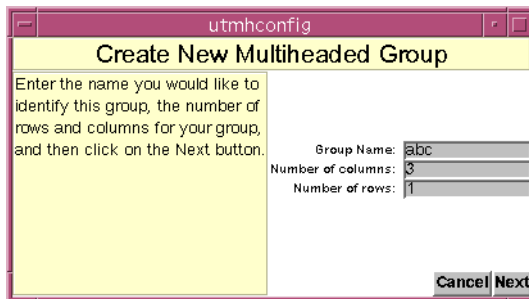
```
# /opt/SUNWut/sbin/utmhconfig
```

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



**FIGURE 9-2** Multihead Group List With Group Detail

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



**FIGURE 9-3** Create New Multiheaded Group Pop-up Dialog Box

**3. Enter the information for the group.**

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

**4. Click the Next button.**

A third screen is displayed.

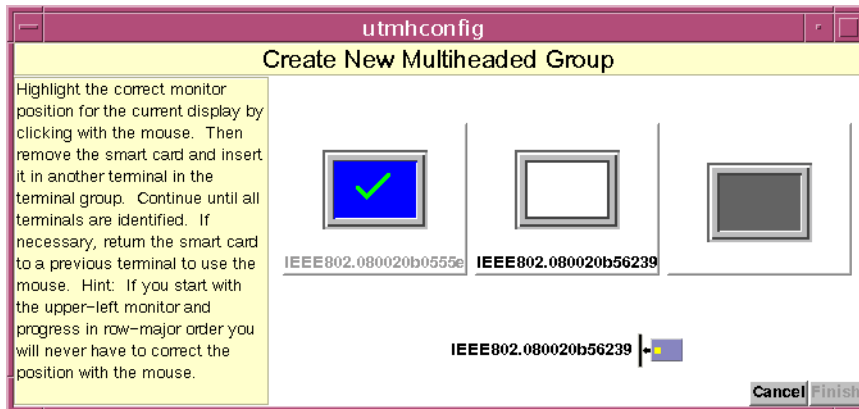


FIGURE 9-4 Setup Display for the New Multihead Group

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

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

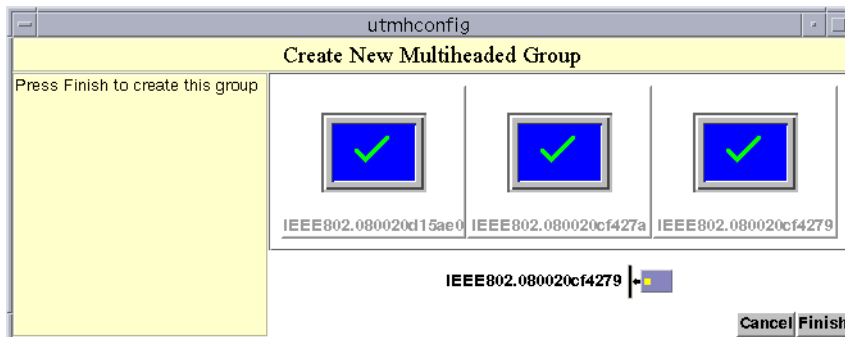


FIGURE 9-5 Completed Multihead Group List With Active Finish Button

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

---

# XINERAMA

The XINERAMA extension to X11 creates one single large screen displayed across several monitors. With XINERAMA only one toolbar is displayed, and a window can be moved smoothly from one part of the screen to the next. XINERAMA is supported in both the Solaris 8 and Solaris 9 operating environments.

A single CDE toolbar (and set of workspaces) manages the configured monitors. A window can span monitors, since they are still within the same screen. This includes the CDE toolbar itself.

---

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

---

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

The XINERAMA feature is enabled using the following command:

```
% /opt/SUNWut/bin/utxconfig -x on
```

The XINERAMA feature is disabled using the following command:

```
% /opt/SUNWut/bin/utxconfig -x off
```

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

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

---

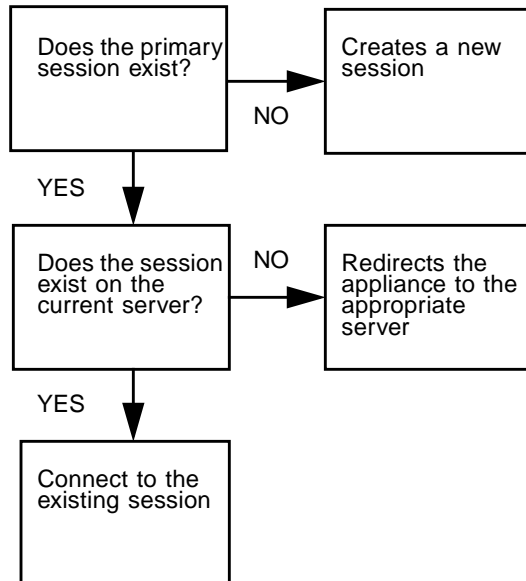
# Session Groups

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

---

# Authentication Manager

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

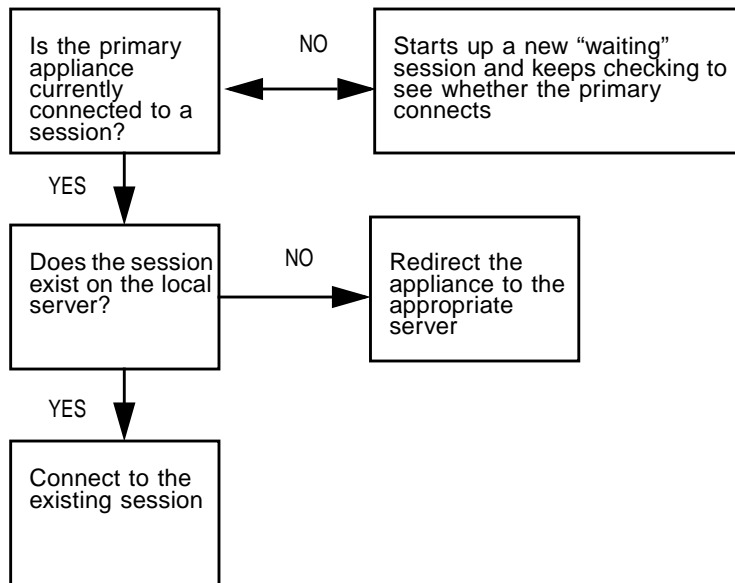


*This flow chart asks the following questions:*

**FIGURE 9-6** Authentication Manager Flowchart for the Primary Appliance

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

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



**FIGURE 9-7** Authentication Manager Flowchart for the Secondary Appliance

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





## Controlled Access Mode

---

This chapter describes Controlled Access Mode (CAM) as well as how to deploy, install, and configure your system to allow controlled, simplified access to anonymous users without compromising the Sun Ray server's security.

Topics include:

- “Controlled Access Mode Functionality” on page 145
- “Advanced Application Setup” on page 153
- “Security and the Controlled Access Mode Environment” on page 154

---

## Controlled Access Mode Functionality

The Sun Ray system is well-suited to host a CAM application, such as public terminals in an airport. In CAM, a user accesses only specified applications. The user does not need to pass security to log in or to use a smart card.

## Enabling Controlled Access Mode

The CAM feature is administered through the Sun Ray Administration Tool or through the Command-line Interface (CLI).

CAM is a policy decision that affects system-level operations. Turn controlled access mode on and off in the Change Policy section of the Admin function of the Administration Tool. You can enable the CAM Policy option for smart card users, non-smart card users, or both.

When controlled access mode is turned on, `kiosk.start` uses scripts to choose temporary users and home directories, then uses the `kiosk.conf` file to configure and populate the user's environment and to launch enabled applications. When a session terminates, `kiosk.start` cleans up all the files and entries related to the session, then recreates the environment for a new user.

---

**Tip** – To enable CAM, use `utconfig`.

---

## ▼ To Enable Controlled Access Mode with the Admin GUI

1. Start the Administration Tool.
2. Select the arrow to the left of Admin to expand the navigation menu.
3. Click the Policy link.

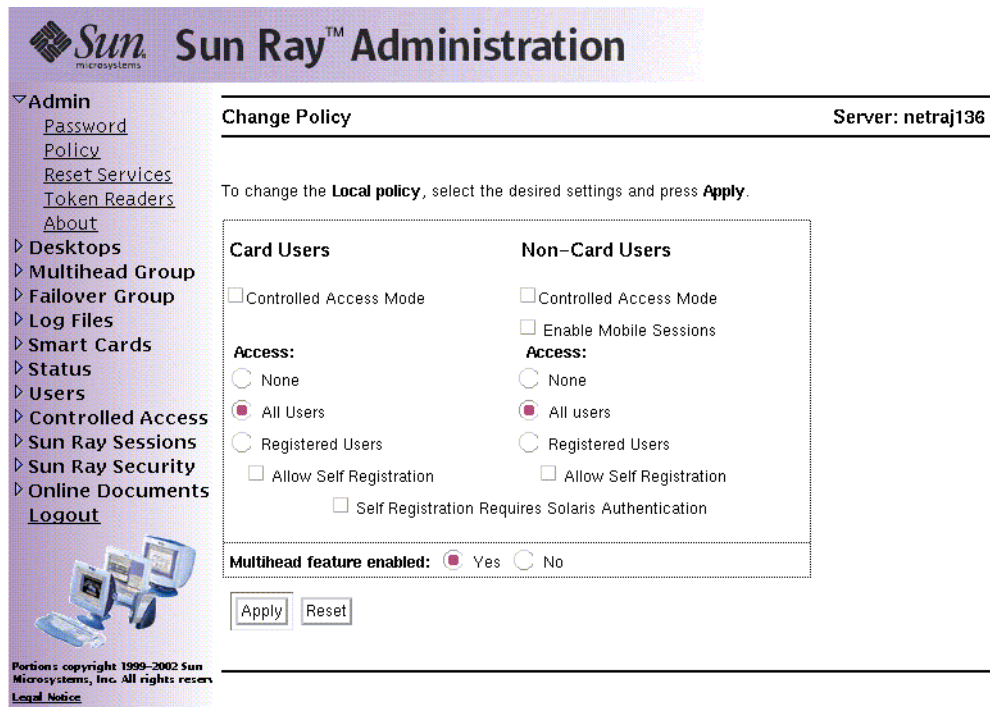


FIGURE 10-1 Change Policy Window

4. For smart card users, select the **Controlled Access Mode** check box in the **Card Users** column.

All smart card users get a Controlled Access Mode session.

5. For non-smart card users, select the **Controlled Access Mode** check box in the **Non-Card Users** column.
6. Click the **Apply** button.
7. Select the **Reset Services** menu.
8. Under **Scope**, click the **Local** or **Group** radio button, depending on the failover scenario.
9. Click the **Reset** or **Restart** button.

## ▼ To Configure CAM Settings

1. Click the arrow to the left of **Controlled Access Mode** in the navigation menu.
2. Click the **Settings** link.

This panel is where the action parameters are set for the Controlled Access Mode. The values define how a session is managed.

3. Click the **Submit Changes** button to store the action parameters in the `/var/opt/SUNWut/kiosk/kiosk.conf` file, which is the controlled access mode configuration file.

The Controlled Access Mode Configuration panel is displayed.

The screenshot shows the Sun Ray Administration web interface. The title bar displays the Sun logo and 'Sun Ray Administration'. The navigation menu on the left includes: Admin, Desktops, Multihead Group, Failover Group, Log Files, Smart Cards, Status, Users, and Controlled Access (expanded). Under 'Controlled Access', the 'Settings' link is selected. The main configuration area is titled 'Controlled Access Mode Configuration' and shows 'Server: netraj135'. The configuration includes:
 

- Card Session Action:  Keep session upon removal of card,  Terminate session upon removal of card
- Timeout (seconds):
- Maximum CPU Time (seconds):
- Maximum VM (KB):
- Maximum File Size (512 Byte Blocks):

 A 'Submit Changes' button is located at the bottom of the configuration area.

FIGURE 10-2 Controlled Access Mode Configuration Panel

The default settings for each controlled access mode session can be edited from this panel. The Card Session Action option determines if card sessions remain resident after a card is removed. If you choose the option to kill the session (the default), the Time-out text box value determines how long to wait before killing the session.

The default values in the maximum CPU, VM, and File Size text boxes are set with the `ulimit` command. These limits contain the CAM user processes.

4. Click the **Confirm** link in the navigation menu to save the changes.
5. Click the **Confirm Configuration** button.
6. Click the arrow to the left of **Admin** to expand the navigation menu.
7. Click the **Reset Services** link.
8. Select the **Local** or **Group** radio button, depending on the failover scenario.

### ▼ To Configure CAM Using the CLI

- As superuser, type the `utpolicy` command for your authentication policy with the addition of the `-k` argument. For example:

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

## Building the Controlled Access Mode Environment

When CAM is enabled, `dtsession` is launched by default to provide basic Controlled Access Mode functionality. Additional applications need to be added to the user's session to extend this basic functionality. Possible applications include:

- Browser (You can use the demonstration version of the Controlled Browser on the Sun Ray 2.0 CD-ROM. See Appendix B.)
- Clock
- Calculator
- Custom application

---

**Tip** – Complete your additions and edits in the Add/Edit Apps section and your selections in the Select Applications section before clicking the **Confirm** link.

---

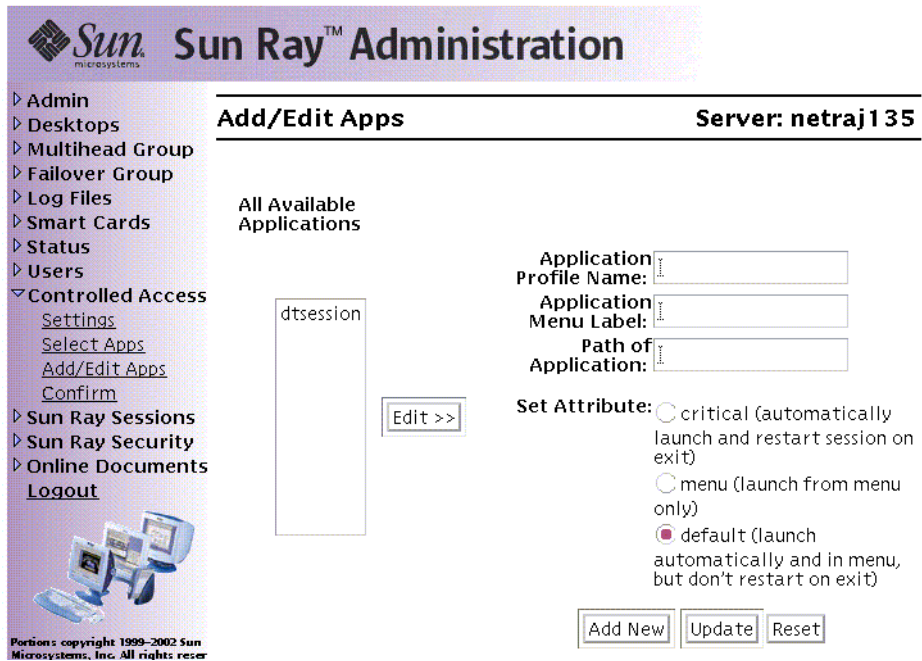


FIGURE 10-3 Add/Edit Apps Panel

## ▼ To Add a New Application

1. **Click the Add/Edit Applications link from the Controlled Access Mode menu.**  
The Add/Edit Apps window is displayed.
2. **Enter a profile name, a menu label, and a path to the application.**  
In the Path of Application text field:
  - List the full path with command-line options or
  - Point to a script that you want to run at session start up (see “Advanced Application Setup” on page 153)
3. **Set the application behavior by clicking one of the radio buttons.**
4. **Click the Add New button.**  
The new application is added to the Available Applications list.
5. **Click the Confirm link.**  
The confirm panel is displayed.
6. **Click the Confirm Configuration button.**

The Confirm link sends `kiosk.conf` information to the internal Sun Ray database which is then replicated to the failover group. After defining a user's session by writing the `kiosk.conf` file, failover services must be restarted to propagate the configuration to all the servers in a failover group.

7. **To enable the newly added application, go to the Select Applications panel and add the application to the Applications to Launch list.**

All applications must be accessible to all servers in the failover group. Add new applications to all servers in a failover group.

## ▼ To Edit an Available Application

1. **Click the Add/Edit Applications link from the Controlled Access Mode menu.**

The Add/Edit Apps window is displayed.

2. **Highlight the application in the All Available Applications list that you want to change and click the Edit button.**

The fields on the right are populated. If, for example, you want to change a default application to be a critical application, you must edit the application and change the attribute to critical.

3. **Make the changes and click the Update button.**

The application information is updated.

---

**Note** – You cannot change the Application Profile Name.

---

4. **Click the Confirm link.**

The confirm panel is displayed.

5. **Click the Confirm Configuration button.**

---

**Note** – You cannot edit `dtsession`.

---

6. **If the application is enabled, click the Reset Services link in the Admin menu.**

7. **Click the Restart button.**

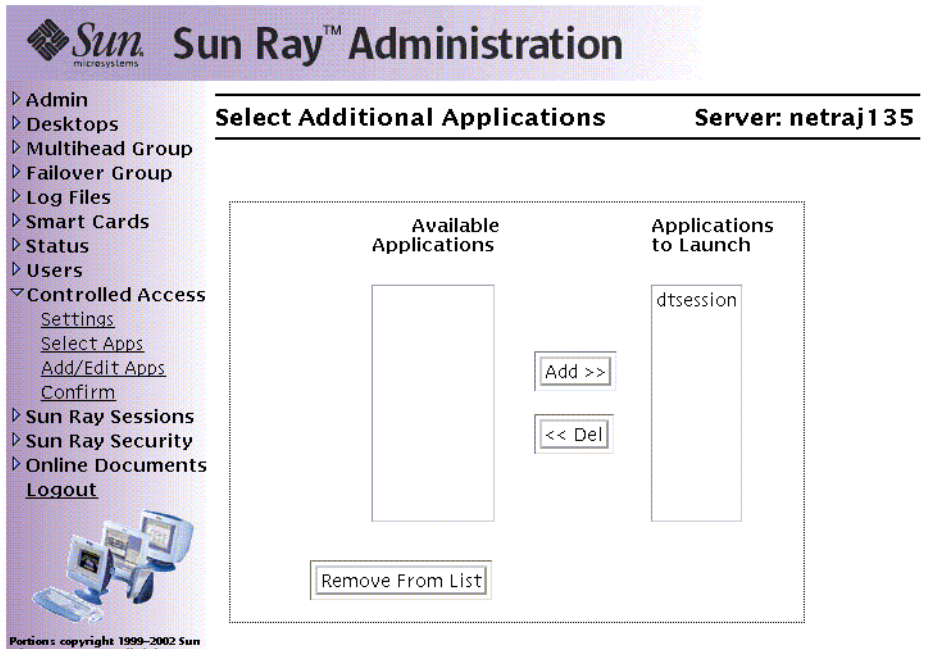


FIGURE 10-4 Additional Applications Configuration Panel

## ▼ To Make an Application Available to Users

### 1. Choose **Select Applications** from the **Controlled Access Mode** menu.

This panel lists the other applications that are available for the user's sessions. In FIGURE 10-4, there are default applications and two possible additional applications you can make available to the user.

### 2. In the **Available Applications** column, highlight the application that you plan to add.

### 3. Click the **Add** button to add it to the **Applications to Launch** column.

### 4. Click the **Confirm** link.

The confirm panel is displayed.

### 5. Click the **Confirm Configuration** button.

### 6. Under the **Admin** menu, click the **Reset Services** link.

### 7. Click the **Restart** button.

## ▼ To Make an Application Not Available to Users

1. **From the Controlled Access Mode menu, click the Select Applications link.**
2. **In the Applications to Launch list, highlight the application that you want to make unavailable.**
3. **Click the Del button.**  
This moves the application back to the Available Applications list.
4. **Click the Confirm link.**  
The confirm panel is displayed.
5. **Click the Confirm Configuration button.**
6. **Under the Admin menu, click the Reset Services link.**
7. **Click the Restart button.**

## ▼ To Remove an Application

1. **From the Controlled Access Mode menu, click the Select Applications link.**
2. **In the Available Applications list, highlight the application that you want to remove.**
3. **Click the Remove From List button.**  
This completely removes the application.
4. **Click the Confirm link.**  
The confirm panel is displayed.
5. **Click the Confirm Configuration button.**



---

# Advanced Application Setup

To customize the CAM user's environment further, you can use prototypes or wrapper scripts to enhance application behavior. Prototypes enhance application behavior by providing files in the user's home directory specific to that application.

---

**Note** – Prototypes must be duplicated on each server in a failover group.

---

## Enabling Prototypes

---

**Note** – When you add new applications, the name of the prototype directory must match the name in the Application Profile Name field of the Administration Tool.

---

### ▼ To Enable Prototypes

1. Create a directory with the same name as the application profile name provided in the Add/Edit Applications section of the Administration Tool:

```
/var/opt/SUNWut/kiosk/prototypes/application_profile_name
```

2. Populate the new prototype directory with files specific to that application:

```
files/directories to be copied into the user's home directory
```

If the application is enabled, everything below the prototype directory is copied recursively to each user's home directory at runtime by the Controlled Access Mode startup scripts. For example, at runtime, there is a `dtsession` prototype directory that matches the application profile name, `dtsession`.

- The application name is `dtsession`.
- The prototype directory is  
`/var/opt/SUNWut/kiosk/prototypes/dtsession`.
- The prototype directories and files are  
`/var/opt/SUNWut/kiosk/prototypes/dtsession/.dt`
- The files and directories at the `.dt` level are copied to the user's home directory (`/HOME/user1/.dt`) at runtime.

# Using Wrapper Scripts to Customize Controlled Access Mode Applications

If an application requires specific environment variables to be set or if you need to launch the application instead of simply providing the path to the application with options, you can use a wrapper script.

## ▼ To Launch an Application Using a Wrapper Script

- **When you add the application using the Administration Tool, provide the path to the wrapper script instead of a path to the executable:**

```
/opt/SUNWut/kiosk/bin/dtsession
```

This example wrapper script customizes the right-click menu button to reflect application labels for menu or default-attributed applications. The script then launches `dtsession`.

- **Alternatively, put the wrapper script in the directory where the Controlled Access Mode program checks for wrapper scripts:**

```
/opt/SUNWut/kiosk/wrappers
```

In this case, the wrapper scripts must have the same name as the path of the application entered in the Add/Edit Applications tab. For an example of a wrapper script, refer to `ControlledBrowser`, which is installed when `cbinstall` is executed. The `cbinstall` script is found in the Supplemental directory on the CD-ROM, in the `/opt/SUNWut/kiosk/wrappers` directory.

---

## Security and the Controlled Access Mode Environment

Since Controlled Access Mode bypasses a login mechanism, you must consider the security of the applications added to the user environment. Many custom applications provide built-in security while other applications do not and, therefore, are not suitable for Controlled Access Mode.

For example, adding an application, such as `xterm`, provides users with access to a command-line interface from a Controlled Access Mode session. This would not be desirable in a public environment and is not advised. However, using a custom application for a call center would be an ideal situation. See Appendix A for an example of an application modified for Controlled Access Mode.

## Failover

In a failover environment, the administrative settings in the `kiosk.conf` file are copied to the failover servers. Be sure that all application paths added to the Controlled Access Mode sessions are copied across the servers in the failover group. For example, if the Netscape application is added to the sessions with the executable path, `/usr/local/exe/netscape`, make sure that the path to the binary is available to all servers in the failover group.

---

**Note** – Applications must be installed in the same location and set up the same way on each server in the failover group. Prototypes and wrapper scripts must also exist on each server in the failover group.

---

## Localization

Controlled Access Mode sessions use their server's default locale.

### ▼ To Change the Locale for Controlled Access Mode Sessions Without Changing the System Locale

- Add the following line to the end of the `/etc/default/init` file:

```
LANG=new-locale
```

The new locale is used by the Controlled Access Mode sessions.

---

**Note** – Adding this line changes the locale for all users on this server.

---



# Failover Groups

---

Sun Ray servers configured in a failover group provide users with a high level of availability when one of those servers becomes unavailable because of a network or system failure. This chapter describes how to configure a failover group.

This chapter covers these topics:

- “Failover Group Overview” on page 158
- “Setting Up IP Addressing” on page 160
- “Group Manager” on page 166
- “Load Balancing” on page 168
- “Setting Up a Failover Group” on page 169
- “Viewing the Administration Status” on page 171
- “Viewing Failover Group Status” on page 171
- “Recovery Issues and Procedures” on page 173
- “Setting Up a Group Signature” on page 176
- “Taking Servers Offline” on page 177

---

# Failover Group Overview

A failover group consists of two or more Sun Ray servers grouped together to provide highly-available and scalable Sun Ray service for a population of Sun Ray appliances. Releases earlier than 2.0 supported appliances available to the servers only on a common, dedicated interconnect. Beginning with the 2.0 release, this capability has been expanded to allow access across the LAN to either local or remote Sun Ray devices. However, there is still a requirement for the servers in a failover group to be able to reach one another, using multicast or broadcast, over at least one shared subnet. Servers in a group authenticate (or “trust”) one another using a common group signature. The group signature is a key used to sign messages sent between servers in the group; it must be configured to be identical on each server.

Failover groups that use more than one version of Sun Ray Server Software will be unable to use all the features provided in the 2.0 release. On the other hand, the failover group can be a heterogeneous group of Sun servers (for example, a mixture of E250s and E450s) running various releases of the Solaris operating environment, such as Solaris 8 and Solaris 9.

When a dedicated interconnect is used, all servers in the failover group should have access to, and be accessible by, all the Sun Ray appliances on a given sub-net. The failover environment supports the same interconnect topologies that are supported by a single-server Sun Ray environment. However, switches should be multicast-enabled.

FIGURE 11-1 illustrates a typical Sun Ray failover group. For an example of a redundant failover group, see FIGURE 11-2.

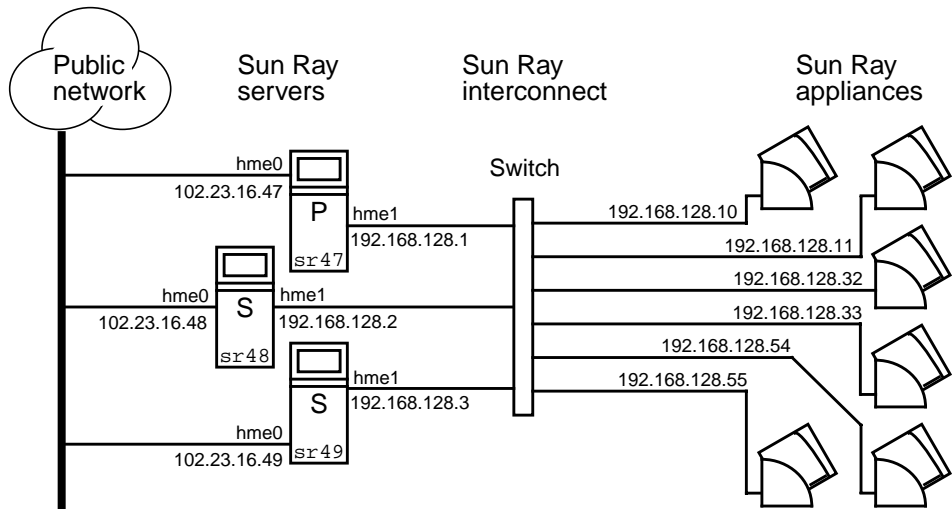


FIGURE 11-1 Simple Failover Group

When a server in a failover group fails for any reason, each Sun Ray appliance connected to that server reconnects to another server in the same failover group. The failover occurs at the user authentication level; the appliance connects to a previously existing session for the user's token. If there is no existing session, the appliance connects to a server selected by the load-balancing algorithm. This server then presents a login screen to the user and the user must relogin to create a new session. The state of the session on the failed server is lost.

The principal components needed to implement failover are:

- Group Manager—A module that monitors the availability (liveness) of the Sun Ray servers and facilitates redirection when needed.
- Multiple, coexisting Dynamic Host Configuration Protocol (DHCP) servers—All DHCP servers configured to assign IP addresses to Sun Ray appliances have a non-overlapping subset of the available address pool.

---

**Note** – The failover feature cannot work properly if the IP addresses and DHCP configuration data are not set up properly when the interfaces are configured. In particular, if the Sun Ray server's interconnect IP address is a duplicate of any other server's interconnect IP address, the Sun Ray Authentication Manager throws "Out of Memory" errors.

---

The redundant failover group illustrated in FIGURE 11-2 can provide maximum resources to a few Sun Ray appliances. The server `sr47` is the primary Sun Ray server and `sr48` is the secondary Sun Ray server; other secondary servers (`sr49`, `sr50` . . . are not shown.

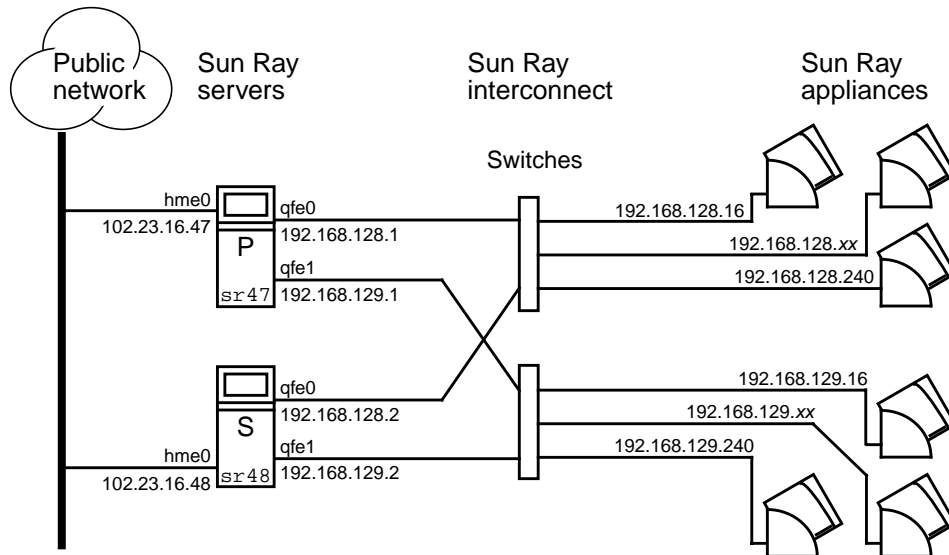


FIGURE 11-2 Redundant Failover Group

## Setting Up IP Addressing

The `utadm` command assists you in setting up a DHCP server. The default DHCP setup configures each interface for 225 hosts and uses private network addresses for the Sun Ray interconnect. For more information on using the `utadm` command, see the man page for `utadm`.

Before setting up IP addressing, you must decide upon an addressing scheme. The following examples discuss setting up class C and class B addresses.

## Setting Up Server and Client Addresses

The loss of a server usually implies the loss of its DHCP service and its allocation of IP addresses. Therefore, more DHCP addresses must be available from the address pool than there are Sun Ray appliances. Consider the situation of 5 servers and 100 appliances. If one of the servers fails, the remaining DHCP servers must have enough available addresses so that all “orphaned” appliances get a new working address.

TABLE 11-1 describes how to configure five servers for 100 appliances, accommodating the failure of two servers (class C) or four servers (class B).



**TABLE 11-1** Configuring Five Servers for 100 Appliances

Servers	Class C (2 Servers Fail)		Class B (4 Servers Fail)	
	Interface Address	Appliance Address Range	Interface Address	Appliance Address Range
serverA	192.168.128.1	192.168.128.16 to 192.168.128.49	192.168.128.1	192.168.128.16 to 192.168.128.116
serverB	192.168.128.2	192.168.128.50 to 192.168.128.83	192.168.129.1	192.168.129.16 to 192.168.129.116
serverC	192.168.128.3	192.168.128.84 to 192.168.128.117	192.168.130.1	192.168.130.16 to 192.168.130.116
serverD	192.168.128.4	192.168.128.118 to 192.168.128.151	192.168.131.1	192.168.131.16 to 192.168.131.116
serverE	192.168.128.5	192.168.128.152 to 192.168.128.185	192.168.132.1	192.168.132.16 to 192.168.132.116

The formula for address allocation is: address range (AR) = number of appliances / (total servers - failed servers). For example, in the case of the loss of two servers, each DHCP server must be given a range of  $100 / (5 - 2) = 34$  addresses.

Ideally, each server would have an address for each appliance. This would require a class B network. Consider these conditions:

- If AR multiplied by the total number of servers is *less than or equal to 225*, configure for a class C network
- If AR multiplied by the total number of servers is *greater than 225*, configure for a class B network

**Tip** – If all available DHCP addresses are allocated, it is possible for a Sun Ray appliance to request an address yet not find one available, perhaps because another unit has been allocated IP addresses by multiple servers. To prevent this condition, give each DHCP server enough addresses to serve the all the appliances in a failover group.

## Server Addresses

Server IP addresses assigned for the Sun Ray interconnect should all be unique. Use the `utadm` tool to assign them.

When the Sun Ray appliance boots, it sends a DHCP broadcast request to all possible servers on the network interface. One (or more) server responds with an IP address allocated from its range of addresses. The appliance accepts the first IP address that it receives and configures itself to send and receive at that address.

The accepted DHCP response also contains information about the IP address and port numbers of the Authentication Managers on the server that sent the response.

The appliance then attempts to establish a TCP connection to an Authentication Manager on that server. If it is unable to connect, it uses a protocol similar to DHCP in which it uses a broadcast message to ask the Authentication Managers to identify themselves. The appliance then attempts to connect to the Authentication Managers that responded in the order in which the responses were received.

---

**Note** – For the broadcast feature enabled, the broadcast address (255.255.255.255) must be the last one in the list. Any addresses after the broadcast address are ignored. If the local server is not in the list, Sun Ray appliances cannot attempt to contact it.

---

Once a TCP connection to an Authentication Manager has been established, the appliance presents its token. The token is either a pseudo-token representing the individual appliance (its unique Ethernet address) or a smart card. The Session Manager then starts an X window/X server session and binds the token to that session.

The Authentication Manager then sends a query to all of the other Authentication Managers on the same subnet and asks for information about existing sessions for the token. The other Authentication Managers respond, indicating whether there is a session for the token and the last time the token was connected to the session.

The requesting Authentication Manager selects the server with the latest connection time and redirects the appliance to that server. If no session is found for the token, the requesting Authentication Manager selects the server with the lightest load and redirects the token to that server. A new session is created for the token.

The Authentication Manager enables both implicit (smart card) and explicit switching. For explicit switching, see “Group Manager” on page 166.

## Configuring DHCP

In a large IP network, a DHCP server distributes the IP addresses and other configuration information for interfaces on that network.

## Coexistence of the Sun Ray Server With Other DHCP Servers

The Sun Ray interconnect is not intended to be shared with any other network traffic.

The Sun Ray DHCP server can coexist with DHCP servers on other subnets, provided you isolate the Sun Ray DHCP server from other DHCP traffic. Verify that all routers on the network are configured not to relay DHCP requests. This is the default behavior for most routers.

---

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

---

## Administering Other Clients

The Sun Ray interconnect is intended to be private. No devices other than switches and Sun Ray appliances should reside on the interconnect. If the Sun Ray server has multiple interfaces (one of which is the Sun Ray interconnect), the Sun Ray DHCP server should be able to manage both the Sun Ray interconnect and the other interfaces without cross-interference.

### ▼ To Set Up IP Addressing on Multiple Servers Each With One Sun Ray Interface

1. Log in to the Sun Ray server as superuser and, open a shell window. Type:

```
# /opt/SUNWut/sbin/utadm -a <interface_name>
```

where *<interface\_name>* is the name of the Sun Ray network interface to be configured; for example, *hme[0-9]*, *qfe[0-9]*, or *ge[0-9]*. You must be logged on as superuser to run this command. The *utadm* script configures the interface (for example, *hme1*) at the subnet (in this example, 128).

The script displays default values, such as the following:

```
Selected values for interface "hme1"
  host address:      192.168.128.1
  net mask:         255.255.255.0
  net address:      192.168.128.0
  host name:        serverB-hme1
  net name:         SunRay-hme1
  first unit address: 192.168.128.16
  last unit address: 192.168.128.240
  firmware server:  192.168.128.1
  router:           192.168.128.1
  alternate servers:
```

The default values are the same for each server in a failover group. Certain values must be changed to be unique to each server.

**2. When you are asked to accept the default values, type n:**

```
Accept as is? ([Y]/N): n
```

**3. Change the second server's IP address to a unique value, in this case 192.168.128.2:**

```
new host address: [192.168.128.1] 192.168.128.2
```

**4. Accept the default values for netmask, host name, and net name:**

```
new netmask: [255.255.255.0]
new host name: [serverB-hme1]
```

**5. Change the appliance address ranges for the interconnect to unique values. For example:**

```
Do you want to offer IP addresses for this interface? [Y/N]:
new first Sun Ray address: [192.168.128.16] 192.168.128.50
number of Sun Ray addresses to allocate: [205] 34
```

**6. Accept the default firmware server and router values:**

```
new firmware server: [192.168.128.2]
new router: [192.168.128.2]
```

The utadm script asks if you want to specify an alternate server list:

```
Specify alternate server list? (Y/[N]): n
```

These servers are specified by a file containing a space-delimited list of server IP addresses or by manually entering the server IP addresses.

---

**Note** – Under most conditions, an alternate server list is not required.

---

The newly selected values for interface hme1 are displayed:

```
Selected values for interface "hme1"
  host address:      192.168.128.2
  net mask:         255.255.255.0
  net address:      192.168.128.0
  host name:        serverB-hme1
  net name:         SunRay-hme1
  first unit address: 192.168.128.50
  last unit address: 192.168.128.83
  firmware server:  192.168.128.2
  router:           192.168.128.2
  alternate servers:
```

**7. If these are correct, accept the new values:**

```
Accept as is? ([Y]/N): y
```

**8. Stop and restart the server and power cycle the appliances to download the firmware.**

TABLE 11-2 lists the options available for the `utadm` command. For additional information, see the `utadm` man page.

TABLE 11-2 Available Options

Option	Definition
-c	Create a framework for the Sun Ray interconnect
-r	Remove all Sun Ray interconnects
-a <interface_name>	Add <interface_name> as Sun Ray interconnect
-d <interface_name>	Delete <interface_name> as Sun Ray interconnect
-p	Print current configuration
-f	Take a server offline
-n	Bring a server online

---

## Group Manager

Every server has a group manager module that monitors availability and facilitates redirection. It is coupled with the Authentication Manager.

In setting policies, the Authentication Manager uses the selected authentication modules and decides what tokens are valid and which users have access.

---

**Warning** – The same policy must exist on every server in the failover group or undesirable results might occur.

---

Each Group Manager creates maps of the failover group topology by exchanging `keepalive` messages among themselves. These `keepalive` messages are sent to a well-known UDP port (typically 7009) to all of the configured network interfaces. The `keepalive` message contains enough information for each Sun Ray server to construct a list of servers and the common subnets that each server can access. In addition, the group manager remembers the last time that a `keepalive` message was received from each server on each interface.

The `keepalive` message contains the following information about the server:

- Server's host name
- Server's primary IP address
- Elapsed time since it was booted

- IP information for every interface it can reach
- Machine information (number and speed of CPUs, configured RAM, and so on)
- Load information (CPU and memory utilization, number of sessions, and so on)

---

**Note** – The last two items are used to facilitate load distribution. See “Load Balancing” on page 168.

---

The information maintained by the Group Manager is used primarily for server selection when a token is presented. The server and subnet information is used to determine the servers to which a given appliance can connect. These servers are queried about sessions belonging to the token. Servers whose last `keepalive` message is older than the timeout are deleted from the list, since either the network connection or the server is probably down.

## Redirection

In addition to automatic redirection at authentication, you can use the `utselect` graphical user interface (GUI) or `utswitch` command for manual redirection.

---

**Note** – The `utselect` GUI is the preferred method to use for server selection. For more information, see the `utselect` man page.

---

## Group Manager Configuration

The Authentication Manager configuration file, `/etc/opt/SUNWut/auth.props`, contains properties used by the Group Manager at runtime. The properties are:

- `gmport`
- `gmKeepAliveInterval`
- `enableGroupManager`
- `enableLoadBalancing`
- `enableMulticast`
- `multicastTTL`
- `gmSignatureFile`
- `gmDebug`

These properties have default values that are rarely changed. Only very knowledgeable Sun support personnel should direct customers to change these values to help tune or debug their systems. If any properties are changed, they must be changed for all servers in the failover group, since the `auth.props` file must be the same on all servers in a failover group.

## ▼ To Restart the Authentication Manager

Property changes do not take effect until the Authentication Manager is restarted.

- **As superuser, open a shell window and type:**

```
# /opt/SUNWut/sbin/utrestart
```

The Authentication Manager is restarted.

---

# Load Balancing

At the time of a server failure, the Group Manager on each remaining server attempts to distribute the failed server's sessions evenly among the remaining servers. The load balancing algorithm takes into account each server's capacity (number and speed of its CPUs) and load so that larger or less heavily loaded servers host more sessions.

When the Group Manager receives a token from a Sun Ray appliance and finds that no server owns an existing session for that token, it redirects the Sun Ray appliance to the server in the group with the lightest load. It is possible that a Sun Ray appliance appears to connect twice; once on the server that answered its DHCP request and a second time on a server that was less loaded than the first.

## ▼ To Turn Off the Load Balancing Feature

- **In the `auth.props` file set:**

```
enableLoadBalancing = false
```



---

# Setting Up a Failover Group

A failover group is one in which two or more Sun Ray servers use a common policy and share services. It is composed of a primary server and one or more secondary servers. For such a group, you must configure Sun Ray Data Store to enable replication of the Sun Ray administration data across the group.

The `utconfig` command sets up the internal database for a single system initially, and enables the Sun Ray servers for failover. The `utreplica` command then configures the Sun Ray servers as a failover group.

If the Sun Ray server is currently monitored by Sun Management Center, `utreplica` restarts the agent automatically. Log files for Sun Ray servers contain time-stamped error messages which are difficult to interpret if the time is out of sync. To make troubleshooting easier, all secondary servers should periodically synchronize with their primary server.

---

**Tip** – Use `rdate <primary-host>`, preferably with `crontab`, to synchronize secondary servers with their primary server.

---

## Primary Server

Layered administration of the group takes place on the primary server. The `utreplica` command designates a primary server, advises the server of its Administration Primary status, and tells it the host names of all the secondary servers.

---

**Tip** – Configure the primary server before you configure the secondary servers.

---

### ▼ To Specify a Primary Server

- As a superuser, open a shell window on the primary server and type:

```
# /opt/SUNWut/sbin/utreplica -p secondary-server1 [secondary-server2 ...]
```

where `secondary_server1 [secondary_server2...]` is a space-separated list of unique host names of the secondary servers.

## Secondary Server

The secondary servers in the group store a replicated version of the primary server's administration data. Use the `utreplica` command to advise each secondary server of its secondary status and also the host name of the primary server for the group.

### ▼ To Specify Each Secondary Server

- As superuser, open a shell window on the secondary server and type:

```
# /opt/SUNWut/sbin/utreplica -s primary-server
```

where *primary-server* is the hostname of the primary server.

### ▼ To Add Additional Secondary Servers

To include an additional secondary server in an already configured failover group:

1. On the primary server, rerun `utreplica -p -a` with a list of secondary servers.

```
# /opt/SUNWut/sbin/utreplica -p -a secondary-server1, secondary-server2,...
```

2. Run `utreplica -s primary-server` on the new secondary server.

```
# /opt/SUNWut/sbin/utreplica -s primary-server
```

## Removing Replication Configuration

### ▼ To Remove the Replication Configuration

- As superuser, open a shell window and type:

```
# /opt/SUNWut/sbin/utreplica -u
```

This removes the replication configuration.

---

# Viewing the Administration Status

## ▼ To Show Current Administration Configuration

- As superuser, open a shell window and type:

```
# /opt/SUNWut/sbin/utreplica -l
```

The result indicates whether the server is standalone, primary (with the secondary host names), or secondary (with the Primary host name).

---

# Viewing Failover Group Status

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

## ▼ To View Failover Group Status

1. From the navigation menu in the Admin GUI, 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.

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 11-3 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.







Failover Group Status		Server:nomad-100	
	Network / IP		
	172.16.126.0/24	192.168.128.0/24	
<a href="#">nomad-100</a> 	 172.16.126.100	 192.168.128.1	
<a href="#">nomad-101</a> 	 172.16.126.101	 192.168.128.2	

FIGURE 11-3 Failover Group Status Table

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

## Sun Ray Failover Group Status Icons

These icons depict current failover group status:

TABLE 11-3 Failover Group Status Icons







Icons	Description
	Information is displayed 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.

TABLE 11-3 Failover Group Status Icons (Continued)

Icons	Description
	<p>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.</p>
	<p>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.</p>
	<p>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.</p>

---

## Recovery Issues and Procedures

If one of the servers of a failover group fails, the remaining group members operate from the administration data that existed prior to the failure.

The recovery procedure depends on the severity of the failure and whether a primary or secondary server has failed.

---

**Note** – When the primary server fails, you cannot make administrative changes to the system. For replication to work, all changes must be successful on the primary server.

---

### Primary Server Recovery

There are several strategies for recovering the primary server. The following procedure is performed on the same server which was the primary after making it fully operational.

## ▼ To Rebuild the Primary Server Administration Data Store

1. On one of the secondary servers, capture the current data store to a file called `/tmp/store`:

```
# /opt/SUNWut/srds/lib/utldbmcats \
/var/opt/SUNWut/srds/dbm.ut/id2entry.dbb > /tmp/store
```

This provides an LDIF format file of the current database.

2. FTP this file to the `/tmp` directory on the primary server.
3. Follow the directions in the *Sun Ray Server Software 2.0 Installation and Configuration Guide* to install Sun Ray Server Software.
4. After running `utinstall`, type the following:

```
# /opt/SUNWut/srds/lib/utldif2ldbmcats -c -n 2 -j 10 -i /tmp/store
```

This populates the primary server and synchronizes its data with the secondary server.

5. Follow the configuration procedures in the *Sun Ray Server Software 2.0 Installation and Configuration Guide*.
6. Reboot the Sun Ray server:

```
# sync;sync;init 6
```

7. Confirm that the data store is repopulated:

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

8. Perform any additional configuration procedures.

## ▼ To Replace the Primary Server with a Secondary Server

1. On one of the secondary servers, capture the current data store to a file called `/tmp/store`:

```
# /opt/SUNWut/srds/lib/utldbmcats \
/var/opt/SUNWut/srds/dbm.ut/id2entry.dbb > /tmp/store
```

This provides an LDIF format file of the current database.

2. FTP this file to the `/tmp` directory on the secondary server.
3. Type:

```
# /opt/SUNWut/srds/lib/utldif2ldbmcats -c -n 2 -j 10 -i /tmp/store
```

4. On all servers, type `unconfigure replication`:

```
# /opt/SUNWut/sbin/utreplica -u
```

5. Configure the primary and secondary servers.

Refer to “To Configure the Sun Ray Server Hierarchy” on page 45 of the *Sun Ray Server Software 2.0 Installation and Configuration Guide* or the `utreplica` man page for further information.

## ▼ To Replace a Primary Server

1. On one of the secondary servers, capture the current data store to a file called `/tmp/store`:

```
# /opt/SUNWut/srds/lib/utldbmcats \
/var/opt/SUNWut/srds/dbm.ut/id2entry.dbb > /tmp/store
```

This provides an LDIF format file of the current database.

2. Install and configure a Sun Ray server according to the procedures in the *Sun Ray Server Software 2.0 Installation and Configuration Guide*.
3. Reboot the Sun Ray server:

```
# sync;sync;init 6
```

4. FTP the `/tmp/store` file to the new Sun Ray server.

5. Type:

```
# /opt/SUNWut/srds/lib/utldif2ldb -c -n 2 -j 10 -i /tmp/store
```

6. On the secondary servers, unconfigure replication:

```
# utreplica -u
```

7. Configure the primary and secondary servers.

Refer to “To Configure the Sun Ray Server Hierarchy” on page 45 of the *Sun Ray Server Software 2.0 Installation and Configuration Guide* or the `utreplica` man page for further information.

## Secondary Server Recovery

Where a secondary server has failed, administration of the group can continue. A log of updates is maintained and applied automatically to the secondary server when it has recovered. If the secondary server needs to be reinstalled, repeat the steps described in the *Sun Ray Server Software 2.0 Installation and Configuration Guide*.

---

## Setting Up a Group Signature

The `utconfig` command asks for a group signature if you chose to configure for failover. The signature, which is stored in the `/etc/opt/SUNWut/gmSignature` file, must be the same on all servers in the group.

The location can be changed in the `gmSignatureFile` property of the `auth.props` file.

To form a fully functional failover group, the signature file must:

- be owned by root with only root permissions
- contain at least eight characters, in which at least two are letters and at least one is not

---

**Tip** – For slightly better security, use long passwords.

---



## ▼ To Change the Group Manager Signature File

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

```
# /opt/SUNWut/sbin/utgroupsig
```

You are prompted for the signature.

2. Enter it twice identically for acceptance.
3. For each Sun Ray server in the group, repeat the steps, starting at step 1.

---

**Note** – It is important to use the `utgroupsig` command, rather than any other method, to enter the signature. `utgroupsig` also ensures that internal database replication occurs properly.

---

---

## Taking Servers Offline

Being able to take servers offline makes maintenance easier. In an offline state, no new sessions are created. However, old sessions continue to exist and can be reactivated unless Sun Ray Server Software is affected.

### ▼ To Take a Server Offline

- At the command-line interface, type:

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

### ▼ To Bring a Server Online

- At the command-line interface, type:

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



# Troubleshooting

---

This appendix contains the following sections:

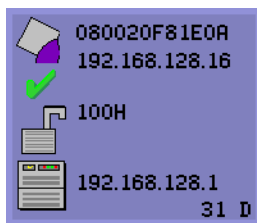
- “Understanding OSD” on page 179
- “Authentication Manager Errors” on page 191
- “Audio” on page 194
- “Performance Tuning” on page 196
- “Troubleshooting the Sun Management Center” on page 199

---

## Understanding OSD

Sun Ray Server Software 2.0 uses a different, larger set of on-screen displays (OSD) than earlier releases, to help administrators and others identify problems visually. The most important information about the Sun Ray appliance and its current state is displayed on the screen.

### OSD Icon Topography



The OSD icons display:

- Ethernet address
- Currently assigned IP address of the appliance
- Link status of the currently connected Sun Ray server
- Authentication Server IP address
- Icon code and DHCP state

To help you locate problems, the OSD icons display a numeric icon code followed by an alphabetic DHCP state code. You can look up the meaning of the numeric OSD message codes in TABLE A-1 and the alphabetic DHCP state codes in TABLE A-2. Encryption and authentication information is also displayed when appropriate.

---

**Note** – Sun Ray appliances can function in a private interconnect or in a simple LAN environment with only an IP address, but additional basic parameters and Sun Ray-specific vendor options are needed for more complex LAN operations, such as when an appliance is located several hops away from the Sun Ray Server’s subnet.

---

OSD icon messages and codes are summarized in the following tables:

**TABLE A-1** Icon Messages

Icon Code	Meaning
1	Sun Ray unit is starting up and is waiting for ethernet link
2	Sun Ray unit is downloading new firmware
3	Sun Ray unit is storing new firmware in its flash memory
4	Either the download or storage of new firmware has failed
5	There is no session to connect with the Sun Ray
6	The server is denying access to the Sun Ray
7	Local pin entry to the smart card has failed
8	In local smartcard pin entry mode
9	There is an over current condition on the USB bus, i.e., the total number of devices draws too much current. Consider using a powered hub.
11	Server is authenticated by the Sun Ray and the graphic/keyboard network connection is encrypted
12	The Sun Ray cannot authenticate the server but the graphic/keyboard network connection is still being encrypted
13	Server authenticated to the Sun Ray; network connection between Sun Ray and server not encrypted
14	Server not authenticated to the Sun Ray; graphic/keyboard network connection is not encrypted
15	The Sun Ray is refusing to talk to the server due to the server’s refusal or inability to authenticate or encrypt the network connection
16	The Sun Ray USB bus is temporarily busy servicing a high-speed device, and the keyboard or mouse may not be responsive to user input.
21	The Sun Ray unit is booting up and is waiting on DHCP IP address and parameter assignment.
22	The Sun Ray unit is booting up and is now waiting for the initial connection to a Sun Ray server.
23	The connection between the Sun Ray and the network is down. Check the network drop cable and (if the network drop cable is okay) the network switch.

**TABLE A-1** Icon Messages

Icon Code	Meaning
24	The Sun Ray has disconnected from the previous server.
25	The Sun Ray is being redirected to a new server.
26	The Sun Ray has connected to the server and is waiting for graphics traffic (this is the GNC state).
27	The Sun Ray is broadcasting to locate a Sun Ray server since either it was not provided with Sun Ray specific DHCP parameters or all of the specified servers are not responding.  <b>Icon numbers 31 through 34 are the network status display brought up by the user pressing all three audio keys.</b>
31	The network link is up and not encrypted.
32	The network link is up and graphics/keyboard are encrypted.
33	The network link is up, the server is authenticated and graphics/keyboard are encrypted.
34	The network link is up, the server is not authenticated and graphics/keyboard are not encrypted.
50	The server is refusing to talk to the Sun Ray due to the Sun Ray's refusal or inability to authenticate or encrypt the network connection

**TABLE A-2** DHCP State Codes

DCHP State Code	State Meaning
A	DCHP only provided IP address with no additional parameters
B	DCHP provided IP address, subnet mask, and router, but Sun Ray vendor-specific parameters are missing.
C	DHCP provided IP address and Sun Ray vendor-specific parameters, but subnet mask and router are missing.
D	DHCP provided all expected parameters.

**TABLE A-3** Power LED

DTU Hardware State	Action to Take
Off	Check to see if the appliance is plugged in. Replace the appliance.
Amber	Hardware fault. Replace the appliance.
Blinking	PROM is corrupted. Check that firmware downloads are properly configured and enabled. Then power cycle the appliance.
Card reader LED remains on even when smart card is removed	Card reader hardware problem. Replace the appliance.

# Sun Ray Desktop Unit Startup

The first display a user should see is OSD 1: 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.**

A link light on the switch or hub indicates that the connection is alive.

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.**

After the Sun Ray desktop unit has verified its network connection, the user should see the DHCP Pending display.

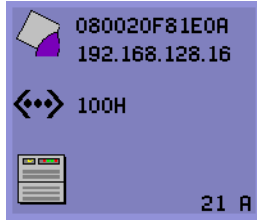


Definition: The appliance has detected the Ethernet carrier but has not yet received its initial parameters or IP address from DHCP. This icon is displayed as part of the normal startup phase and is usually displayed for only a few seconds.

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

1. **Make sure that the DHCP server is configured correctly, is up and running, and has not run out of IP addresses to assign to clients.**
2. **Verify that your DHCP server is configured properly for network parameters.**

At this point, depending on whether you have configured your Sun Ray servers to run on a LAN or a dedicated interconnect, one of the following icons may display:



### Startup Wait for DHCP Information

After the DHCP server has allocated an IP address, the icon is updated with the unit's IP address; if the response is inadequate, the Sun Ray issues a `DHCP inform` request to attempt to obtain the Sun Ray vendor-specific parameters. The Sun Ray continues all the way through booting with just a DHCP supplied IP address but usually functions better with some additional parameters.



Code 21 A indicates that the appliance got an IP address and is waiting for a `DHCP inform` response to other parameters.

Code 21 B indicates that the appliance got an IP address and IP router and is waiting for Sun Ray vendor-specific options from `DHCP inform`.

---

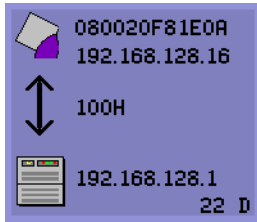
**Note** – If you see a 21 A or 21 B with a DTU IP address in a LAN deployment, the Sun Ray appliance is trying to use `DHCP_INFORM` to get Sun Ray-specific parameters.

---

### ▼ Actions to take:

1. For LAN configurations with other (non-Sun Ray) DHCP services but no `bootp` proxy agent, verify the DHCP server and the Sun Ray vendor tags.
2. For routed configurations, verify that the `bootp` proxy agent is configured correctly in the Sun Ray appliance's subnet and that it points to one of the Sun Ray servers in the failover group.
3. For non-routed private interconnect configurations, the Sun Ray server also performs the functions of a DHCP server. Verify that it is configured properly for DHCP services.

When DHCP has finished, the Sun Ray appliance tries to connect to a Sun Ray server and the authentication manager that is running on that server.



### Waiting to Connect to Authentication Manager

Definition: The appliance has received its initial parameters from DHCP but has not yet connected to the Sun Ray Authentication Manager. This icon is displayed as part of the normal startup phase and is usually displayed for only a few seconds.

## ▼ Actions to take if the icon displays for more than a few seconds or if the appliance continues to reset after the icon is displayed:

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

In a LAN configuration or other routed environment:

2. **Make sure that the authentication manager can be reached from the IP address assigned to the appliance.**
3. **Verify that the routing information the appliance receives is correct.**
4. **Run `utquery` for the appliance's IP address.**

The `utquery` command displays the parameters a Sun Ray appliance has received. If `utquery` fails to display an `AuthSrvr` parameter, the DHCP server for Sun Ray parameters may not be reachable or may not be configured properly. Confirm that the `DHCP`Server and `INFORM`Server values are appropriate. If not, look at your `bootp` relay configurations and DHCP server configurations for network and Sun Ray parameters. For details of these parameters, see the `utquery` man page.

---

**Note** – To Restart DHCP on a Solaris server, type the following as superuser:

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

---

## ▼ To Identify a Hung Session

- **As superuser, type:**

```
# /opt/SUNWut/sbin/utdesktop -l -w
```

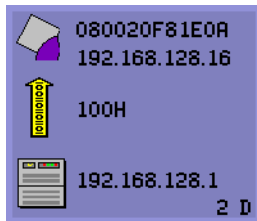


## ▼ To Kill a Hung Session

- As superuser, type:

```
# /opt/SUNWut/sbin/utsession -k -t token
```

## Firmware Download



### Downloading PROM Software

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

## ▼ Actions to take:

1. **Wait until the download is complete.**

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

If the firmware download fails, the following syslog message indicates that the barrier level has been set to prevent Sun Ray appliances with 2.0 firmware from automatically downloading an earlier version of the firmware:

```
Firmware upgrade/downgrade not allowed! Barrier is 200 Firmware level is 0
```

2. **Check** `/var/opt/SUNWut/log/messages` **to confirm that your configuration is set up properly.**

---

**Note** – For LAN configurations, the minimum barrier level is 200. For more information on barrier levels, see “Firmware Barrier” on page 109.

---



### 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.



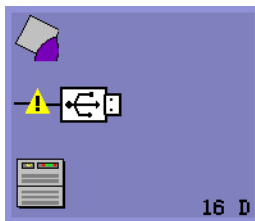
### Firmware Download Failed

Definition: The appliance has failed to download new firmware.

## ▼ Actions to take:

1. **Check the messages file** `/var/opt/SUNWut/log` **to verify the version number.**
2. **Correct, if necessary, with** `utadm -l`.

## Bus Busy

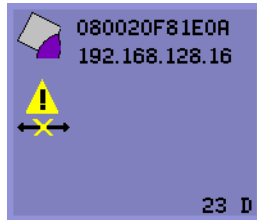


### Sun Ray USB Bus Busy

Definition: The Sun Ray USB bus is temporarily busy servicing a high-speed device, and the keyboard or mouse may not be responsive to user input.

This icon typically appears only during an unusually long print job and disappears when the job is done. This is an informational OSD; there is no particular action to take unless it is necessary to kill the print job.

# No Ethernet



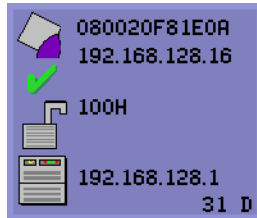
## No Ethernet Connection

Definition: The appliance has an Ethernet address and an IP address but has lost the Ethernet signal. This icon is displayed only after the appliance successfully boots and receives an IP address, but then loses its Ethernet signal.

### ▼ Actions to take:

1. Check that the Ethernet cable is correctly plugged in to the back of the 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.

# Ethernet Address



Definition: This OSD, shows the Ethernet address, the currently assigned IP address, the currently connected server, the encryption status, and the DHCP state. To display it, press the three audio volume keys simultaneously.

**Tip** – To get the same effect on non-Sun keyboard, disconnect and reconnect the Ethernet wire.

Link speed is also indicated (for example, 10F, 10H, 100F, 100H). F stands for full duplex, and H stands for half duplex. 10 stands for 10 Mbps, and 100 for 100 Mbps.

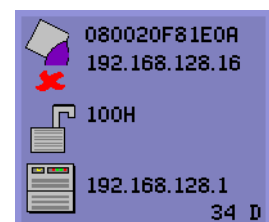
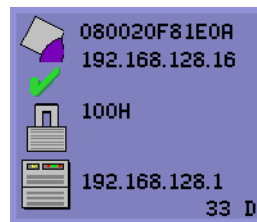
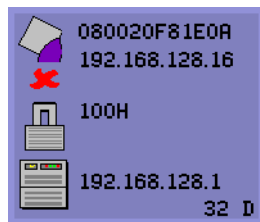


FIGURE A-1 Ethernet Address OSD with Different Encryption and Authentication States

# Session Connection Failures

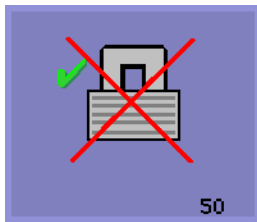
The following icons are displayed when there might be a security breach.



## Session Refused

Definition: The client is refusing to connect to a server because it is unable to verify the validity of the Sun Ray server.

This error can occur only if an unknown Sun Ray server intercepts the messages and tries to emulate a valid Sun Ray server. This is a session security breach.



## Session Refused

Definition: The server is refusing to grant a session to the client because the client is unable to fulfill the server's security requirements.

## ▼ Actions to take:

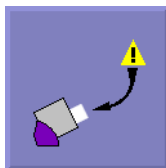
### 1. Check the client's firmware version.

This error may occur with firmware versions earlier than 2.0 if the server is configured for hard security mode.

### 2. Upgrade the firmware to version 2.0 or later.

As an alternative, confirm whether your site requires hard security mode. If not, the session can be enabled with soft security mode.

# Card Read Error OSD



## Card Read Error

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:

1. Upgrade the firmware.
2. Replace the card.

## Prompt for Card Insertion OSD



Prompt for Card Insertion

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



Access Denied

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.

The Sun Ray administration model has seven user session types:

- Default—Normal user login
- Register—User self-registration
- Kiosk—Anonymous user operation
- Insert card—User smart card required
- Card error—Unrecognized user smart card type
- No entry—User's smart card token is blocked
- Session Refused—The server refuses to grant a session to a client that does not meet the server's security requirements

The first three session types have normal login processes. When there is a problem, the administrator should examine:

- Sun Ray Server configuration files

---

**Caution** – Sun Ray Server Software modifies certain system configuration files. In most cases, these changes are identified with SRSS-specific comments. Please do not change these modifications.

---

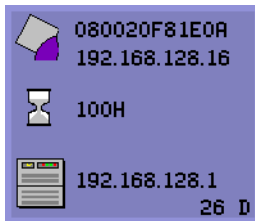
- Any locally modified X server startup files
- `dtlogin` status

Although the last four session types display icons on the Sun Ray appliance, they do not have login processes at all. The icons indicate that the user must take steps before a successful login is possible. If the user immediately removes and reinserts the smart card, the icon disappears, but the Wait for Session OSD remains.

These last four session types and their OSDs should not cause alarm. The user can:

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

## Wait for Session OSD



### Wait for Session

This OSD represents the transition state for the Sun Ray appliance. If it is displayed for an extended period, there is probably no X Window server running.

---

**Note** – The current wait icon is a white “X” cursor. In earlier releases, the wait icon was displayed as a green newt cursor.

---

---

**Tip** – If you suspect that the configuration files have been corrupted, please see “To Determine the Integrity of the Configuration Files” on page 49 in the *Sun Ray Server Software 2.0 Installation and Configuration Guide*.

---

## Wait Icon 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.

The dtlogin daemon has been part of the Solaris operating environment since long before Sun Ray Server Software existed. The Sun Ray administration model uses the dtlogin daemon in new ways, and certain bugs in the dtlogin daemon have become apparent. Patches to fix these bugs in the dtlogin daemon are available.

## Patches

For the latest information regarding Sun Ray Server Software patches, check:

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

Solaris operating environment patches and other software patches are available at:

<http://access1.sun.com>

---

# Authentication Manager Errors

Authentication Manager errors can be found in the following error logs:

- Installation logs:
  - /var/adm/log
  - /var/opt/SUNWut/log
- General log files:
  - /var/opt/SUNWut/srds/log
  - /var/opt/SUNWut/srds.repllog

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 “worker” plus number. The Worker# thread names are reused when a connection terminates. Other threads are:

- SessionManager#—Communicate with `utsessiond` on behalf of a Worker# thread.
  - AdminJobQ—Used in the implementation to wrap a library that would not otherwise be thread-safe.
  - CallBack#—Communicate with applications such as `utload`.
  - WatchID—Used to poll data/terminals from connections
  - Terminator—Cleans up terminal sessions
  - Group Manager—Main group manager thread
- message\_class

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

- CLIENT\_ERROR—Indicates unexpected behavior from 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-4** Error Message Examples

<b>Error class</b>	<b>Message</b>	<b>Description</b>
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.

---

# Audio

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.

## Audio Device Emulation

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.

## Audio Malfunction

If audio features are malfunctioning:

1. **To confirm whether audio is working, run the following command on the appliance:**

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

2. **Bring up `utsettings`:**

```
% utsettings
```

3. **Verify that audio output is selected properly, e.g., for headphones or speakers.**
4. **Check the volume level.**

5. **Verify that Mute is not selected.**

Some applications are hard-coded to use `/dev/audio` for output. Sun Ray System Software provides a redirection library that you can use to correct this behavior.

▼ **To Activate the Redirection Library**

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

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

2. **Restart the application.**

---

## PDA Synchronization Issues

If your users have problems running `PDASync` on a Sun Ray, use the following procedure:

1. **Get the latest Java Communications API (`javax.comm` api version 2.0.2 and above) from**

<http://java.sun.com/products/javacomm/>

2. **Make sure that you are using a supported USB-serial adapter.**

A list of supported USB devices is available at:

[http://www.sun.com/io\\_technologies/sunray/usb/](http://www.sun.com/io_technologies/sunray/usb/)

3. **Click the change Synchronization Settings icon.**

Select the port to which the Palm cradle is connected.

4. **Click OK.**

---

**Tip** – If the ports are not shown correctly in the Serial Port drop-down menu, close the application and hot plug the device, then start the application again.

---

---

# Performance Tuning

Some applications, such as intensive 3-D visual simulations, may run very slowly on Sun Ray. Other applications, such as pseudo-stereo viewers using double-buffering, or high-frequency dynamic color table flips on 8-bit visuals, do not produce the expected visual result.

## General Configuration

You can usually improve performance by configuring `/etc/system` shared memory segment parameters. The exact settings depend on application demands and the number of Sun Ray users, but a convenient starting point is:

```
set shmsys:shminfo_shmmax = 0x2000000
set shmsys:shminfo_shmmni = 0x1000
set shmsys:shminfo_shmseg = 0x100
```

Due to the nature of the Xinerama (single virtual X display) mode of multihead, the system shared memory requirements may be even higher. To get reasonable performance, the `shmsys:shminfo_shmmax` parameter must be at least:

```
LARGEST_NUMBER_OF_HEADS * width * height * 4
```

## Applications

Placing the user's interactive applications, such as Netscape or StarOffice, or PC interoperability tools, such as Citrix or Tarantella, on the Sun Ray server usually helps performance by reducing network load. The applications benefit from faster transport of commands to the Sun Ray's X server.

Applications that can be configured to use shared memory instead of DGA or OpenGL usually perform better on Sun Ray when they used shared memory.

# Sluggish Performance

Sluggish Sun Ray server performance or excessive disk swapping is an indication that the Sun Ray server is under-provisioned. Under these circumstances, there is not enough virtual memory available to start an X Window server instance for a user's session.

The solution in this situation is to add more memory or increase the size of the swap partition. In other situations, network load or packet loss may be too high. In very rare cases, network cables or switch equipment may be defective.

1. **To determine whether there is excessive swapping, use `vmstat 5`.**

```
# vmstat 5
```

If there is excessive swapping, the system may be undersized or overutilized.

2. **Verify that network connections are 100E.**
3. **Use `utcapture` to assess network latency and packet loss.**  
As latency and packet loss increase, performance suffers.

# Monitor Display Resolution Defaults to 640 x 480

First, eliminate the most obvious possible causes:

- An older monitor
- A bad cable
- Monitor was off when the Sun Ray appliance was started

If the Sun Ray appliance is unable to read DDC data from the monitor, then it defaults to 640 x 480 pixels.

To correct this condition:

1. **Replace the cable**
2. **Restart the Sun Ray appliance after powering the monitor on**
3. **Replace the monitor**
4. **Use the `utresadm` to set persistent display setting to override the default.**

## Old Icons (Hourglass with Dashes Underneath) Appear on Display

If the old, pre-2.0 icons appear on the display, either the DTU's firmware has not been upgraded or it is failing.

1. **Upgrade the firmware from 1.x to 2.0 or higher.**
2. **Follow the procedure to upgrade the firmware. See the *Sun Ray Software 2.0 Installation and Configuration Guide*.**

You may need to use a dedicated private network.

## Port Currently Owned by Another Application

If this message displays, use the following procedure to correct it:

1. **Download the latest Java Communications API (javax.comm API version 2.0.2 and above)**
2. **Make sure that the supported USB-Serial Adapter is used.**  
  
The supported USB devices list is available at  
[http://www.sun.com/io\\_technologies/sunray/usb/](http://www.sun.com/io_technologies/sunray/usb/)
3. **Click the Change Synchronization Settings icon and select the appropriate port (to which the Palm cradle should be connected), then click OK.**
4. **If the ports are not correctly shown in the Serial Port drop down menu, close the application and hot plug the device.**
5. **Start the application again.**

## Design Tips

- Avoid drawing into off-screen memory and then copying large areas to the screen. This technique produces slow Sun Ray performance.
- GXcopy mode is usually the fastest drawing mode.
- To display large images, use shared memory pixmaps, if possible.
- Opaque stipple patterns are faster than transparent stipples.
- Opaque (image) text is faster than other text.

---

# Troubleshooting the Sun Management Center

Usually, if all the software is installed, the agent for Sun Ray monitoring starts automatically.

## No Sun Ray Object

If the Sun Ray server has the Sun Management Center agent component installed, but the Detail window shows no Sun Ray object for the Sun Ray server node, load the Sun Ray module:

### ▼ To Load the Sun Ray Module

#### 1. Click the Modules tab.

Note where the Sun Ray module is listed (if it is not listed, see “No Sun Ray Module” on page 200). For the module to be loaded, it should be listed in Modules with Load Status. In addition, it should be loaded and enabled.

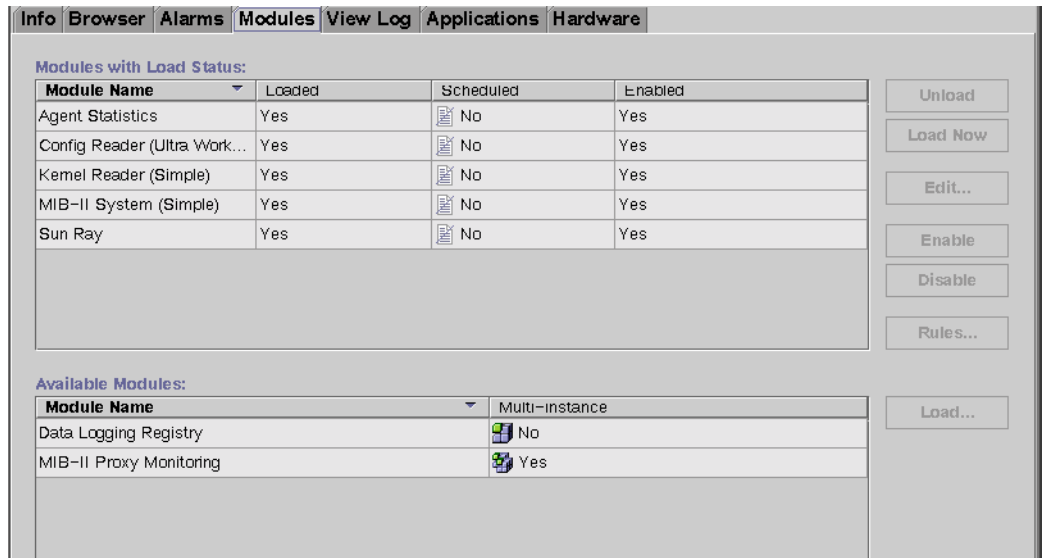


FIGURE A-2 Module Panel

2. **If the Sun Ray module is listed, highlight it and then click the Load button.**

This loads the module and moves it to the Modules with Load Status list.

3. **If the Sun Ray module is disabled, highlight it and then click the Enable button.**

This enables the module.

4. **Return to the Detail window.**

The Detail window shows a Sun Ray object for the Sun Ray server node.

## No Sun Ray Module

If, after clicking the Modules tab on the Details window of the Sun Ray server node, the Sun Ray module is not listed, activate the Sun Ray module:

### ▼ To Activate the Sun Ray Module

1. **Register the module by typing:**

```
# /opt/SUNWut/sbin/utsumc
```

This command adds the module to the Sun Management Center and restarts the agent if it is active.

2. **If you receive the following message, perform steps 3 and 4.**

```
Starting the SunMC agent...
NOTICE:          SunMC agent failed to start.
                 To start it manually run the command
```

3. **Check to see if the agent is running:**

```
# ps -ef |grep agent
```

If the Sun Management Center agent is running, wait then rcheck the Detail window.

4. **If the agent is not running, type the following to start it:**

```
# /opt/SUNWsymon/sbin/es-start -a
```



## Controlled Browser

---

The Controlled Browser is an unsupported product. For your convenience, we have provided a sample implementation of the Netscape Navigator 4.76 browser. This browser is provided in English only and has not been localized.

The objective of this implementation is to provide a browser environment for a publicly accessed Sun Ray appliance with minimal risk of server security compromise. The browser is specially set up to provide for a more controlled and secure browser environment. Netscape Navigator functions normally with the exception of disabled downloads and a new GUI print interface to the command-line print interface.

This appendix contains the following sections:

- “Controlled Browser Installation” on page 201
- “Controlled Browser Functionality” on page 203
- “Browser Printing” on page 206
- “Adding Plug-ins to the Controlled Browser” on page 208

---

## Controlled Browser Installation

**Note** – Do not install a controlled browser until your system is configured with Controlled Access Mode. Please run the `utconfig` script or refer to “Controlled Access Mode” on page 71.

---

## ▼ To Install the Controlled Browser

1. If you have already mounted the Sun Ray Server Software 2.0 CD-ROM locally or from a remote server or if you extracted the ESD files to an image directory, begin at Step 4.

2. As superuser, open a shell window on the Sun Ray server.

3. Insert the Sun Ray Server Software 2.0 CD-ROM.

If a file manager window opens, close it. The file manager CD-ROM window is not necessary for this procedure.

4. Change to the image directory by typing:

```
# cd /cdrom/cdrom0
```

5. Change to the controlled browser directory by typing:

```
# cd Supplemental/Controlled_Browser/Solaris_8+/Packages
```

6. Install the browser by typing:

```
# ./cbinstall
```

The controlled browser is installed and set as a critical application for CAM sessions.

To further configure the browser, refer to the Controlled Browser Functionality in this section.

## ▼ To Remove the Controlled Browser

The `cbinstall` script also removes the controlled browser.

---

**Note** – When you remove Sun Ray Server Software, you must first remove the controlled browser if it has been installed.

---

1. If you have already mounted the Sun Ray Server Software 2.0 CD-ROM locally or from a remote server or if you extracted the ESD files to an image directory, begin at Step 4.

2. As superuser, open a shell window on the Sun Ray server.

### 3. Insert the Sun Ray Server Software 2.0 CD-ROM.

If a file manager window opens, close it. The file manager CD-ROM window is not necessary for this procedure.

### 4. Change to the image directory by typing:

```
# cd /cdrom/cdrom0
```

### 5. Change to the controlled browser directory by typing:

```
# cd Supplemental/Controlled_Browser/Solaris_8+/Packages
```

### 6. Remove the browser by typing:

```
# ./cbinstall -u
```

The controlled browser is removed.

---

## Controlled Browser Functionality

The browser environment is controlled by taking advantage of the Solaris `chroot` command. This command allows for the execution of the browser to run relative to an alternative root directory. Sun Ray users run the browser within the confined environment setup in `/var/opt/SUNWbb/root`, thus avoiding potential access to damaging commands and system files.

To maintain security, since these users are not authenticated, they have access only to specified applications confined to the directory tree below the `chroot` directory. The `chroot` environment is analogous to a Web server's document root in that users of the environment are confined to the directory tree below the `chroot` directory. The `chroot` environment creates a subdirectory that appears as the `root` directory for a given process or set of processes. The browser and all subprocesses that it may spawn are run in this restricted environment.

---

**Note** – This controlled browser does not address general network security, Java applet security, or plug-in security.

---

## ▼ To Setup the Controlled Browser in Control Access Mode Administration

1. Start the Administration Tool.
2. Click the arrow to the left of **Controlled Access Mode** to expand the navigation menu.
3. Click the **Controlled Browser** link.

The Controlled Browser Configuration window is displayed.

**Sun Ray™ Administration** Server: nomad-100

Controlled Browser Configuration

Set Behavior:  critical (automatically launch and restart session on exit)  
 menu (launch from menu only)  
 default (launch automatically and in menu, but don't restart on exit)

Home Page:

Browser Window Location (pixels x,y):

Browser Window Size (pixels width,height):

Proxy Setting:  Manual Proxy Configuration  Direct Connection  
**Will retain default values if "Direct Connection" is selected**

HTTP cache:  port:

SSL cache:  port:

FTP cache:  port:

WAIS cache:  port:

Gopher cache:  port:

Copyright 2000-2001 Sun Microsystems, Inc. All rights reserved.

FIGURE B-1 Controlled Browser Configuration Window

---

**Note** – This menu selection appears only after a Controlled Browser is installed.

---

4. Set the browser behavior by clicking one of the radio buttons.
  - If you select critical, the session starts with this application. If the session dies, the whole session is regenerated automatically.
  - If you select menu, this application is only presented on the menu, which is accessed when the user clicks the right mouse button.

- If you select default, the session starts with this application but does not restart if it dies. This application is also available on the menu. A user can restart the application by using the menu.
5. In the Home Page text box, type the URL to be accessed when the browser first starts.
  6. In the Browser Window Location text field, displays the screen location in pixels.
  7. The Browser Window Size text field displays the size in pixels.
  8. If a proxy server is being used, click the Manual Proxy Configuration button and set the proxy values for the controlled browser by typing the values in the text boxes.

**Proxy Setting:**  
 Will retain default values if "Direct Connection" is selected  
 Manual Proxy Configuration  Direct Connection

HTTP cache:  port:

SSL cache:  port:

FTP cache:  port:

WAIS cache:  port:

Gopher cache:  port:

FIGURE B-2 Controlled Browser Configuration—Proxy Setting Section

9. Click the Submit Changes button to save your selections in the `kiosk.conf` file.
10. Click the Confirm link in Controlled Access Mode menu.  
The confirm panel is displayed.
11. Click the Confirm Configuration button.  
The `kiosk.conf` file is updated. If the internal Sun Ray database is up, the configuration file is imported to it.

---

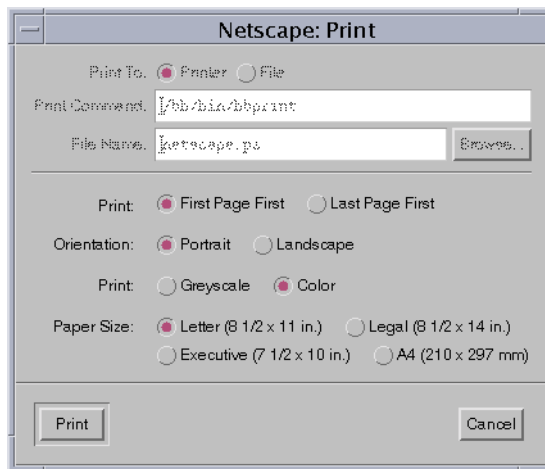
# Browser Printing

This browser implementation has replaced the command-line print interface with a graphical interface.

## ▼ To Print from the Browser

1. Select the **Print** icon on the Netscape menu bar or select **File->Print** from the pull-down menu.

The Netscape: Print dialog box is displayed.



**FIGURE B-3** Netscape Print Dialog Box

2. Press the **Print** button.

A new Print dialog box is displayed.

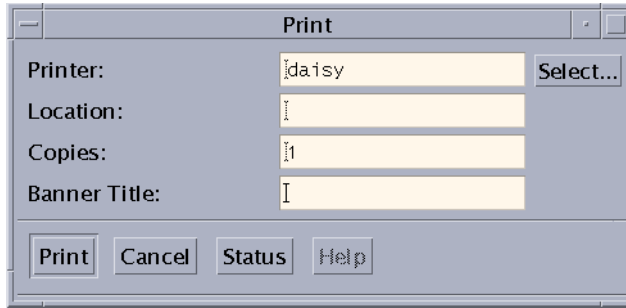


FIGURE B-4 Graphical Printing Interface

3. If there is no printer name in the Printer text box or if you wish to send your print job to a printer other than the one listed in the Printer text box, press the Select button.

The Select Printer dialog box, which contains a list of configured printers for your server, is displayed.



FIGURE B-5 Select Printer Dialog Box

4. Highlight the desired printer and press the OK button.
5. Once a printer has been selected, press the Status button on the Print dialog box to view the status of the printer.

The Printer Status dialog shows the printer name, the number of jobs queued for this printer, and details of each of the print jobs including print job number, size of file to print, and date stamp for this job. This information helps the user determine if whether to print to a different printer in cases where print queues are too long or individual print jobs on the print queue are too big.

6. Enter the number of print copies required in the Copies text box.
7. If the printer selected is configured to print banners before each print job, enter a banner name in the Banner Title text box.

The Location field cannot be edited and may contain information regarding the location of the selected printer.

8. To print the page, press the Print button or the Cancel button to cancel print operations

## ▼ To Configure the Printer Location

```
# lpadmin -p printerName -D "Location description"
```

---

# Adding Plug-ins to the Controlled Browser

Plug-ins can be added to the Controlled Browser. Since the browser is executed through the `chroot` restricted runtime environment and Controlled Access Mode, extra steps need to be taken to make sure that the plug-ins work properly.

Some plug-ins, such as Macromedia Flash Player plug-in, need only to be installed into the browser's plug-in directory. Others require more work to install files into the Control Access Mode user's home directory, add lines to the browser's `mimetypes` file, and setup environment variables needed before the browser is executed.

Some scripts installed for plug-ins may try to use Solaris commands under such directories as `/usr/bin` and `/bin`. In `chroot`, however, these directories are not available. To solve this problem, copy the needed commands to the `/var/opt/SUNWbb/root/bin` directory.

`chroot` also has an automated setup mechanism to support the creation of dynamic user environments. A UNIX user ID is selected dynamically for every new CAM session. The home directory is created and populated with a configured set of files at the start of the session and destroyed upon reset or exit of a session or critical application. The sections below discuss to set the files up to populate the home directory with respect to plug-ins and their associated helper applications.



# Set Up Considerations

For plug-ins and helper applications to work properly, the following might be set up:

1. Mime types
2. Environment variables
3. Per user configuration (for example, `$HOME/.xyz` files)

## Mime Types

The restricted runtime environment provides an interface to register mime types with the restricted browser. A plug-in usually registers its mime type through the plug-in API, but helper applications use the `.mimetype` and `.mailcap` files.

To register its mime types, a helper application installs a file *helper.mimedef* into the `/opt/SUNWbb/mime.d/` directory.

The file syntax is:

*helper;flags;extensions;mime-type;description*

---

**Note** – A line may take the form of the line above, or be either empty or a comment, in which case it begins with `#`. Each mime type definition must be contained in a single line. A mime type definition cannot contain a new line.

---

TABLE B-1 Mime Type Definition Syntax

Variable	Definition
<i>helper</i>	<code>bbhelper helperpath args exts</code>
<i>helperpath</i>	helper app to execute for this mime type
<i>args</i>	usually <code>%s</code> or <code>%u</code>
<i>exts</i>	Space-separated list of extensions to match on the URL. If no match, then the first extension is concatenated to the file name. This allows the helper application to guess what content type it deals with. This is because the browser does not provide any hint to the helper on the mime type being handled.
<i>flags</i>	Browser-specific flags such as: <code>x-mozilla-flags=plugin;</code> Usually empty field for helper applications

**TABLE B-1** Mime Type Definition Syntax (*Continued*)

Variable	Definition
<i>extensions</i>	exts="ext0 ext1" list of possible extensions for files of this mime type
<i>mime-type</i>	type=mimetype/subtype
<i>description</i>	desc="....."

## Environment Variables

To provide environment variables to helper applications or plug-ins, the restricted runtime environment uses files located in `/opt/SUNWbb/appschr.d/`.

These files define variables exported by the controlled browser. A line in these files can either be empty, a comment (start with #), or can have exactly one assignment of the following form:

```
VARIABLE=value
```

The assignments should be valid bourne shell assignments.

## Per User Configuration

Some helper applications need per user configuration data. To allow helper applications to set up a user's home directory, the restricted runtime environment uses files located in `/opt/SUNWbb/apps.d/`.

These files can be bourne or korn shell scripts that are sourced and run with the permissions of the selected user. The following environment variables are available:

**TABLE B-2** Environment Variables

Variable	Definition
<i>BBUSER</i>	The user for whom the set up is done.
<i>BBHOME</i>	The user's home directory.

## General Requirements and Other Considerations

For a plug-in or helper application to run in the restricted runtime environment, it must install into a selectable directory location. The recommended location is:

```
/var/opt/SUNWbb/root/bb/apps/helper-plugin-dir
```

This is the path seen when the browser executes the helper application or plug-in.

Sometimes the install procedure puts the install path into the installed helper application or plug-in configuration files or scripts. Then, at run-time, it tries to find components in `/var/opt/SUNWbb/root/bb/apps/helper-plugin-dir`, which does not exist in the restricted runtime environment.

To solve this problem, create the following symbolic link:

```
# cd /var/opt/SUNWbb/root/var/opt/SUNWbb/root
# ln -s /bb bb
```

---

**Tip** – For setup and testing purposes, it might be a good idea to temporarily configure `xterm` as an application on the CAM desktop. This aids in the testing and configuration of the plug-ins and their helper applications, many of which use the home directory for configuration files and directories. To avoid potential security problems, remove `xterm` from the CAM desktop before the Sun Ray appliances are ready for use.

---

## Sample Plug-In Setup

Below are steps for setting up some of the more popular browser plug-ins and helper applications for the Solaris operating environment.

---

**Note** – The download file names, version numbers, and installation conventions of the plug-ins referenced may change over time.

---

### ▼ To Add Macromedia Flash Player Plug-in

1. Create the directory for the plug-in download by typing:

```
# mkdir /var/opt/SUNWbb/root/bb/apps/Flash
```

2. Download the Macromedia Flash Player plug-in for the Solaris operating environment from the Macromedia Web site and save it in the following directory:

```
/var/opt/SUNWbb/root/bb/apps/Flash
```

**3. Change directory, uncompress the file, and untar the file by typing:**

```
# cd /var/opt/SUNWbb/root/bb/apps/Flash
# /usr/bin/gunzip flash_solaris.tar.gz
# tar xvf flash_solaris.tar
```

**4. Copy the resulting files into the Netscape plug-ins directory by typing:**

```
# cp libflashplayer.so /var/opt/SUNWbb/root/bb/apps/netscape/plugins
# cp ShockwaveFlash.class /var/opt/SUNWbb/root/bb/apps/netscape/plugins
```

▼ **To Add Adobe Acrobat Reader Plug-in and Application**

**1. Create a temporary directory for the plug-in download by typing:**

```
# mkdir /var/opt/SUNWbb/root/bb/apps/temp
```

**2. Download the Adobe Acrobat Reader for Solaris from the Adobe Web site and save in the following directory:**

`/var/opt/SUNWbb/root/bb/apps/temp`

**3. Change directory, uncompress the file, untar the file, and install by typing:**

```
# cd /var/opt/SUNWbb/root/bb/apps/temp
# /usr/bin/gunzip sunsparc-rs-405.tar.gz
# tar xvf sunsparc-rs-405.tar
# cd SSOLRS.install
# ./INSTALL
```

**4. Follow the installation instructions. When prompted for the installation directory, enter:**

`/var/opt/SUNWbb/root/bb/apps/Acrobat4`

---

**Note** – After installation is complete, you can delete the `temp` directory.

---

5. Copy the Acrobat Reader plug-in library into the Netscape plug-in directory by typing:

```
# cd /var/opt/SUNWbb/root/bb/apps/Acrobat4/Browsers/sparcsolaris
# cp nppdf.so /var/opt/SUNWbb/root/bb/apps/netscape/plugins
```

6. Create the file `/opt/SUNWbb/mime.d/acrobat.mimedef` containing the following lines:

```
/bb/apps/Acrobat4/bin/acroread %s;exts="pdf";type=application/pdf;desc="Portable Document Format"
/bb/apps/Acrobat4/bin/acroread -iconic %s;exts="fdf";type=application/vnd.fdf;desc="application/vnd.fdf"
```

7. Execute the following script to update the browser's mime information:

```
# /opt/SUNWbb/init.d/bbnsinit
```

8. Copy the following executable commands into the `/bin` directory of the `chroot` directory by typing:

```
# cp -p /usr/bin/basename /var/opt/SUNWbb/root/bin
# cp -p /usr/bin/cat /var/opt/SUNWbb/root/bin
# cp -p /usr/bin/dirname /var/opt/SUNWbb/root/bin
# cp -p /usr/bin/expr /var/opt/SUNWbb/root/bin
# cp -p /usr/bin/uname /var/opt/SUNWbb/root/bin
# cp -p /usr/bin/ksh /var/opt/SUNWbb/root/bin
```

The executable for the helper application `acroread` is a script. In the script, executable commands are used to launch the application. Since this script is launched from the browser running under the `chroot` environment, these executable commands have to be explicitly copied into the `/bin` directory of the `chroot` directory.

9. Determine what default files need to be copied into the CAM user's home directory by running the browser and plug-in once to see what files are copied into the users directory.

In the case of Acrobat Reader, the files `.acrorc` and `.acrosrch` are created. The default files can be created by having the CAM user access a PDF file through the Controlled Browser. Once the Acrobat Reader brings up the PDF file, exit Acrobat Reader. This writes out the `.acrorc` and `.acrosrch` file into the home directory of the CAM user (`/var/opt/SUNWbb/root/home/CAM_user_name`).

**10. Copy the resulting files into a permanent directory by typing:**

```
# cp .acrorc /opt/SUNWbb/config/acrobat4.acrorc
# cp .acrosrch /opt/SUNWbb/config/acrobat4.acrosrch
# chmod 644 /opt/SUNWbb/config/acrobat4.*
```

**11. Create the file /opt/SUNWbb/app.d/acrobat.rc containing the following lines:**

```
cp /opt/SUNWbb/config/acrobat4.acrorc $BBHOME/.acrorc
chmod 644 $BBHOME/.acrorc
cp /opt/SUNWbb/config/acrobat4.acrosrch $BBHOME/.acrosrch
chmod 644 $BBHOME/.acrosrch
```

**12. Make /opt/SUNWbb/app.d/acrobat.rc executable:**

```
# chmod 755 /opt/SUNWbb/app.d/acrobat.rc
```

## ▼ To Add RealPlayer Plug-in and Application

**1. To create a temporary directory for the plug-in download, type:**

```
# mkdir /var/opt/SUNWbb/root/bb/apps/temp
```

**2. Download the RealPlayer for the Solaris operating environment from the Real Web site and save it in the following directory:**

```
/var/opt/SUNWbb/root/bb/apps/temp
```

**3. Change directory, make the binary file executable, and execute by typing:**

```
# cd /var/opt/SUNWbb/root/bb/apps/temp
# chmod 755 rp8_solaris27_sparc_cs2.bin
# ./rp8_solaris27_sparc_cs2.bin
```

**4. Follow the installation instructions. When you are prompted for the installation directory, enter:**

```
# /var/opt/SUNWbb/root/bb/apps/RealPlayer
```

---

**Tip** – After installation is complete, you can delete the `temp` directory.

---

5. Copy the RealPlayer plug-in libraries into the Netscape plug-in directory by typing:

```
# cd /var/opt/SUNWbb/root/bb/apps/RealPlayer
# cp raclass.zip /var/opt/SUNWbb/root/bb/apps/netscape/plugins
# cp rpnp.so /var/opt/SUNWbb/root/bb/apps/netscape/plugins
```

6. Create the file `/opt/SUNWbb/mime.d/realplayer.mimedef` containing the following lines:

```
/bb/apps/RealPlayer/realplay %u;exts="ra,rm,ram";type=audio/x-pn-realaudio;desc="Realaudio"
/bb/apps/RealPlayer/realplay %u;exts="ra,rm,ram";type=audio/vnd.rn-realaudio;desc="Realaudio"
/bb/apps/RealPlayer/realplay %u;exts="smi";type=application/smil;desc="Realaudio"
bbhelper /bb/apps/RealPlayer/realplay %s m3u;exts="m3u";type=audio/x-mpegurl;desc="streaming Mpeg audio"
bbhelper /bb/apps/RealPlayer/realplay %s m3u;exts="m3u";type=audio/mpegurl;desc="streaming Mpeg audio"
```

7. To execute the following script to update the browser's mime information, type:

```
# /opt/SUNWbb/init.d/bbnsinit
```

8. Create the following file `/opt/SUNWbb/appschr.d/realplayerenv.rc` containing the following lines:

```
REALPLAYER_HOME=/bb/apps/RealPlayer
```

9. Determine what default files need to be copied into the CAM user's home directory by running the browser and plug-in once to see what files are copied into the user's directory.

In the case of RealPlayer, the files `.RealNetworks_RealMediaSDK_60`, `.RealNetworks_RealPlayer_60`, and `.RealNetworks_RealShared_00` are created.

The ideal user session should be set up at this point. Default settings, such as transport protocol used, proxy settings, and so on, should be set.

**10. Copy the resulting files to a permanent directory by typing:**

```
# cp .RealNetworks_RealMediaSDK_60
/opt/SUNWbb/config/realplayer.RealNetworks_RealMediaSDK_60
# cp .RealNetworks_RealPlayer_60
/opt/SUNWbb/config/realplayer.RealNetworks_RealPlayer_60
# cp .RealNetworks_RealShared_00
/opt/SUNWbb/config/realplayer.RealNetworks_RealShared_00
# chmod 644 realplayer.*
```

**11. Create the file /opt/SUNWbb/app.d/realplayer.rc containing the following lines:**

```
cp /opt/SUNWbb/config/realplayer.RealNetworks_RealMediaSDK_60 $BBHOME/.RealNetworks_RealMediaSDK_60
chmod 644 $BBHOME/.RealNetworks_RealMediaSDK_60
cp /opt/SUNWbb/config/realplayer.RealNetworks_RealPlayer_60 $BBHOME/.RealNetworks_RealPlayer_60
chmod 644 $BBHOME/.RealNetworks_RealPlayer_60
cp /opt/SUNWbb/config/realplayer.RealNetworks_RealShared_00 $BBHOME/.RealNetworks_RealShared_00
chmod 644 $BBHOME/.RealNetworks_RealShared_00
```

**12. Make /opt/SUNWbb/app.d/realplayer.rc executable by typing:**

```
# chmod 755 /opt/SUNWbb/app.d/realplayer.rc
```



## Sun Ray and Network Parameter Delivery (DHCP)

---

Sun Ray relies on DHCP to obtain network parameters and Sun Ray parameters. Network parameters include IP address, subnet mask, and router.

Sun Ray parameters enable Sun Ray devices to function normally in a Sun Ray environment. For Sun Ray appliances to be able to discover the Sun Ray server on the network, they need to have at least the `AuthSRVR` parameter delivered through DHCP.

For a more comprehensive treatment of DHCP, see the *Dynamic Host Configuration Protocol RFC* at <http://www.ietf.org/rfc/rfc2131.txt?number=2131>.

For details on *DHCP Options and BOOTP Vendor Extensions*, see <http://www.ietf.org/rfc/rfc2132.txt?number=2132>

TABLE C-1 lists the Sun Ray parameter symbol values defined in the DHCP table. The remainder of this appendix describes the encapsulated options.

**TABLE C-1** Sun Ray Parameter Symbol Values (as defined in the DHCP table)

Parameter Name	Vendor ID	Code	Type	Mandatory/ Optional	Comments	
NewTFlags	Vendor=SUNW.NewT.SUNW,	34,	NUMBER,	4,1	Optional	
Intf	Vendor=SUNW.NewT.SUNW,	33,	ASCII,	1,0	Optional	Interface used for Sun Ray service
NewTDispIndx	Vendor=SUNW.NewT.SUNW,	32,	NUMBER,	4,1	Optional	
FWSrvr	Vendor=SUNW.NewT.SUNW,	31,	IP,	1,1	Optional	Firmware server IP address (needed for firmware upgrade)
LogAppl	Vendor=SUNW.NewT.SUNW,	29,	NUMBER,	1,1	Optional	Log level for application
LogVid	Vendor=SUNW.NewT.SUNW,	28,	NUMBER,	1,1	Optional	Log level for video
LogUSB	Vendor=SUNW.NewT.SUNW,	27,	NUMBER,	1,1	Optional	Log level for USB
LogNet	Vendor=SUNW.NewT.SUNW,	26,	NUMBER,	1,1	Optional	Log level for network
LogKern	Vendor=SUNW.NewT.SUNW,	25,	NUMBER,	1,1	Optional	Log level for kernel
LogHost	Vendor=SUNW.NewT.SUNW,	24,	IP,	1,1	Optional	Log level for host
NewTBW	Vendor=SUNW.NewT.SUNW,	30,	NUMBER,	4,1	Optional	Limits bandwidth available for the Sun Ray
NewTVer	Vendor=SUNW.NewT.SUNW,	23,	ASCII,	1,0	Optional	Specifies which firmware version to upgrade to.
AuthPort	Vendor=SUNW.NewT.SUNW,	22,	NUMBER,	2,1	Optional	Sun Ray server port to connect to
AltAuth	Vendor=SUNW.NewT.SUNW,	35,	IP,	1,0	Optional	Alternate set of Sun Ray server IP addresses
AuthSrvr	Vendor=SUNW.NewT.SUNW,	21,	IP,	1,1	Mandatory	Sun Ray server IP address to connect to
BarrierLevel	Vendor=SUNW.NewT.SUNW,	36,	NUMBER,	4,1	Optional	Barrier level for firmware download

Sun Ray parameters are encapsulated vendor-specific options; that is, the value for the standard DHCP vendor-specific information is an encapsulated set of options that only the vendor equipment—the Sun Ray server, in this case—knows how to interpret.



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

# Glossary

---

---

## B

- backplane bandwidth** Sometimes also referred to as switch fabric. A switch's backplane is the pipe through which data flows from an input port to an output port. Backplane bandwidth usually refers to the aggregate bandwidth available amongst all ports within a switch.
- barrier mechanism** To prevent clients from downloading firmware that is older than the firmware they already have, the administrator can set a barrier mechanism. The barrier mechanism symbol `BarrierLevel` is defined by default in the DHCP table of Sun Ray servers running version 2.0 or later of Sun Ray Server Software.
- bpp** Bits per pixel.

---

## C

- CAM** Controlled access mode, also known as *kiosk 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.
- client-server** A common way to describe network services and the user processes (programs) of those services.
- cut-through switches** The switch begins forwarding the incoming frame onto the outbound port as soon as it reads the MAC address, while it continues receiving the remainder of the frame.

---

## D

- DHCP** Dynamic Host Configuration Protocol, which is a means of distributing IP addresses and initial parameters to the appliances.
- domain** A set of one or more system boards that acts as a separate system capable of booting the OS and running independently of any other board.

---

## 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.
- filling station** When a client's firmware is downgraded to an earlier version because it connects to a server running the earlier version, it needs to be connected to a filling station so that it can download newer firmware. For this purpose, a filling station can be any private network configured for Sun Ray services or any shared network in which the Sun Ray DHCP server is the only DHCP server.
- firmware barrier** See *barrier mechanism*.
- FTP** File Transfer Protocol. The name of the Internet protocol and the program used to transfer files between hosts.

---

## G

**GEM** Gigabit Ethernet.

---

## H

**head** Colloquial term for a screen, or display, or monitor, especially in a context where more than one is used in conjunction with the same keyboard and mouse, as in “multihead” feature.

**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.

---

## K

**kiosk mode** Same as *CAM*.

---

## 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.
- managed object** An object monitored by the Sun Management Center software.
- 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.
- multicasting** The process of enabling communication between Sun Ray servers over their Sun Ray network interfaces in a failover environment.
- multihead** See *head*.
- multiplexing** The process of transmitting multiple channels across one communications circuit.

---

## N

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

- network latency** The time delay associated with moving information through a network. Interactive applications such as voice, video displays and multimedia applications are sensitive to these delays.
- network mask** A number used by software to separate the local subnet address from the rest of a given Internet protocol address. An example of a network mask for a class C network is 255.255.255.0.
- network protocol stack** A network suite of protocols, organized in a hierarchy of layers called a stack. TCP/IP is an example of a Sun Ray protocol stack.
- NIC** Network interface card.
- 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

- screen flipping** The ability to pan to individual screens on an appliance with a single head that were originally created by a multihead group.
- server** A computer system that supplies computing services or resources to one or more clients.
- service** For the purposes of the Sun Ray Server Software, any application that can directly connect to the Sun Ray 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.
- session mobility** The ability for a session to “follow” a user’s login ID or a token embedded on a smart card.
- smart card** A plastic card containing a microprocessor capable of making calculations.
- spanning tree** The spanning tree protocol is an intelligent algorithm that allows bridges to map a redundant topology and eliminates packet looping in Local Area Networks (LAN).
- store-and-forward switches** The switch reads and stores the entire incoming frame in a buffer, checks it for errors, reads and looks up the MAC addresses, and then forwards the complete good frame out onto the outbound port.
- subnet** A working scheme that divides a single logical network into smaller physical networks to simplify routing.

---

## T

- TCP/IP** Transmission Control Protocol/Internet Protocol (TCP/IP) is a networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and operating systems.
- thin client** Thin clients remotely access some resources of a computer server, such as compute power and large memory capacity. The Sun Ray 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.

**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.

---

## 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

---

## NUMERICS

100BASE-T, 12

## A

acceptRedirectToken, 89, 92

Acrobat, 213

acrorc, 213

acrosrch, 213

adapters, 86

Adding

    script, 149

Adding applications

    calendar, 151

    clock, 151

    other, 151

admin password, 17, 40

Administration Group

    viewing failover group status, 171

Administration Tool, 38, 94

    changing the admin password, 40

    controlled access mode, 71

        adding or editing applications, 73

        selecting additional applications, 72

    desktops

        displaying current properties, 48

        editing a single desktop's properties, 50

        searching for, 49

        viewing, 48

        viewing properties of current user, 49

    examining log files, 55

    finding Sun Ray sessions, 75

    locating token readers, 44

    log files

        viewing messages logs, 56

    logging in, 38

    managing Sun Ray sessions, 75

    resetting Sun Ray Services, 43

    restarting Sun Ray Services, 43

    smart card

        adding, 59

        changing the probe order, 59

        deleting, 60

        viewing or listing configured, 57

        viewing the probe order, 58

    users

        adding a token ID, 68

        adding a user with token ID, 66

        deleting, 63

        deleting a token ID, 69

        displaying current properties, 65

        editing properties, 67

        enabling or disabling a token ID, 69

        finding a user, 69

        getting a token ID from token reader, 70

        viewing by ID, 62

        viewing by name, 63

        viewing current, 65

    viewing all multihead groups, 52

    viewing Sun Ray sessions, 77

agent, 114, 115, 116

    additional requirements with Sun Ray  
    module, 115

alarms, 114

    Details window, 124

- monitoring, 123
  - setting, 120
  - Tool Tip window, 125
  - values, 121
- AltAuth, 218
- Applet
  - security, 203
- appliance, 34
  - adding to be monitored, 131
  - deleting to be excluded, 131
  - Hot Desking to a multihead group, 142
  - multihead feature, 135
  - multihead group, 136
- Application
  - adding, 149
  - critical, 204
  - default, 204
  - menu, 204
- ARCFOUR, 97
- attacks
  - man-in-the-middle, 98
- Attribute Editor, 127
- AUDIODEV environment variable, 194
- authentication, 97
  - server, 98
- Authentication Manager, 4, 34, 38, 142, 162, 166
  - configuration file, 167
  - flowchart for primary appliance, 142, 143
  - interacting with Session Manager, 5
  - restarting, 168
- AuthPort, 218
- AuthSrvr, 184, 217, 218
- Automatic restart, 204
- auto-size feature, 137

## B

- bandwidth
  - limited backplane, 10
- barrier
  - firmware, 109, 185
- BarrierLevel, 218
- bidirectional encryption, 98
- bootp, 105, 108
- Browser
  - proxy settings, 205

## C

- C, 23
- Cabling
  - fiber-optic, 12
- CAM, 22, 148
- CDE
  - locking the screen, 27
- CDE toolbar, 136, 141
- central registration, 5
- chroot, 208
- Citrix, 196
- client
  - authentication, 97
- code
  - DHCP option, 219
- command
  - utadm, 160, 166
  - utcapture
    - data elements, 34
  - utconfig, 135, 169, 176
  - utmhconfig, 136
  - utreplica, 169
  - utswitch, 21
  - utxconfig, 135
- commands
  - utadm, 22
  - utadm -r, 24
  - utaudio, 194
  - utdetach, 89, 91
  - utfwadm, 25
  - utpolicy, 96
  - utpolicy -i clear, 22
  - utrestart -c, 22
  - utwall, 94, 96
- configuration
  - security, 98, 99
- configuration data
  - DHCP, 22, 93, 159, 163
- console, 114
- controlled access mode
  - adding or editing applications, 73
  - configuring, 71
  - selecting additional applications, 72
- Critical application, 204
- crontab, 169
- cursor



- green newt, 190
- X, 190

## D

- daemons
  - Sun Ray Service panel, 129
- Data Store, 169
- DCHP
  - state codes, 181
- Default application, 205
- departments, 13
- desktopID, 35
- desktops
  - displaying current properties, 48
  - editing a single desktop's properties, 50
  - searching for, 49
  - viewing, 48
  - viewing properties of current user, 49
- Desktops panel, 131
- device
  - directory, 79
  - links, 81
  - node ownership, 81
  - nodes, 80
  - USB, 80
- DHCP, 160, 184
  - configuring for failover, 162
  - parameters, 217
- DHCP configuration data, 22, 93, 159, 163
- DHCP server, 163
- DHCP servers, 159
- DHCPACK, 219
- dhcpmgr, 111
- DHCPServer, 184
- dhtadm, 110
- dhtadm -R, 23
- display resolution
  - auto-size feature, 137
  - on workgroup monitors, 137
- DSA, 97
- dtlogin, 191
- dtlogin screen, 4, 88
- dtprofile file, 27
- duplicate IP addresses, 22, 93, 159, 163
- Dynamic Host Configuration Protocol (DHCP), 3

## E

- encapsulated options, 219
- encryption
  - algorithm, 97
  - bidirectional, 98
  - downstream only, 98
  - upstream only, 98
- errors
  - out of memory, 22, 93, 159, 163
- escape tokens, 93
- Ethernet switch, 11

## F

- Failover
  - controlled access mode, 155
- failover
  - address allocation formula, 160
  - configuring DHCP, 162
  - group, 113, 157
    - primary server, 169
    - removing replication configuration, 170
    - secondary server, 170
  - Group Manager module, 159
  - principle components needed, 159
  - server IP addresses, 161
  - setting up group, 169
  - taking servers offline, 177
- failover group, 13, 111
  - administration status, 171
  - monitoring servers, 116
  - recovery procedures, 173
  - viewing status, 171
- failover groups, 159
- filling station, 109
- firmware barrier, 109
- firmware module, 3
  - PROM version management, 25
- FWSrvr, 218, 220

## G

- gmSignature, 173, 176
- green newt cursor, 190
- green newt icon, 190
- Group Manager
  - keepalive message, 166

- load balancing, 2, 168
- redirection, 19, 167
- using Authentication Manager properties, 167

Group manager, 166

group manager

- keepalive message, 166

group manager module, 166

group signature, 17, 172

- setting up, 176

GXcopy, 198

## H

hacking

- man-in-the-middle attacks, 98

hard security mode, 98

Hot Desk, 137, 142

Hot Desking, 81, 87, 194

hot key, 28

- changing setting, 31
- changing setting site-wide, 30
- detaching a mobile session, 90
- entry, 29
- values, 29

hotkey key combination, 91

## I

icon messages

- OSD, 180

IEEE802.MACID directory, 79

INFORMServer, 184

Interconnect, 11

interconnect, 11, 163

- boost power of, 11
- implementing a Sun Ray, 10

interconnect fabric, 9

- adding an interface, 23
- deleting an interface, 23
- departments, 13
- failover group, 13
- managing, 22
- printing configuration, 24
- removing an interface, 25
- workgroups, 12

interconnect IP address, 22, 93, 159, 163

Interconnect panel, 130

Internal database, 169

Intf, 218

IP address

- duplicate, 22, 93, 159, 163

## K

keepalive message, 166

key combination, 91

kiosk.conf, 146, 147, 155

kiosk.start, 146

## L

layer 2 switch, 11

LDIF, 174, 175

load balancing, 2, 168

- turning off, 168

log files

- examining, 55
- viewing messages logs, 56

LogAppl, 218

LogHost, 218

LogKern, 218

LogNet, 218

LogUSB, 218

LogVid, 218

## M

managed object, 113

- desktops, 131
- Interconnect panel, 130
- monitoring, 126
- Sun Ray system, 126

man-in-the-middle attack, 98

Menu application, 204

message\_class, 192

modules, 4

- Registered, 5
- StartSession, 5

monitoring programs

- CA Unicenter, 132
- HP OpenView VPO, 132
- Tivoli TMS, 132

monitors

- display resolution, 137

multicast

- IP, 111
- multihead, 196
  - administration tool, 137
  - creating a new group, 138
  - group, 136, 143
  - Hot Desking to an appliance, 142
  - screen display, 136, 137
    - auto-size feature, 137
  - turning on policy from command line, 138
  - turning on policy with administration tool, 138
- multihead feature, 135
- multihead groups
  - viewing all, 52

## N

- Netscape, 196
- network
  - adding an interface, 23
  - deleting an interface, 23
  - removing an interface, 25
- Network security, 203
- NewTBW, 218
- NewTDispIndx, 218
- NewTFlags, 218
- NewTVer, 218
- non-secure session, 98
- NSC mobile session, 87, 96
- NSC mobile session login, 88
- NSCM session, 88
  - disconnecting, 90
  - enabling from Administration Tool, 94
  - enabling from command line, 96
  - logging in to, 89

## O

- OpenGL, 196
- option code, 219
- options
  - encapsulated, 219
  - vendor-specific, 218
- OSD
  - icon messages, 180
  - understanding, 179
- out of memory error, 22, 93, 159, 163
- out-of-order packets, 104

## P

- packet loss
  - utcapture, 34
- packets
  - out-of-order, 104
- panel
  - Desktops, 131
  - Interconnect, 130
  - Sun Ray System, 127
- panning, 137
- parallel peripherals, 79
- PDA synchronization, 84
- PDASync, 195
- peripherals
  - parallel, 79
  - serial, 79
- persistent settings (monitor), 18
- policies, 4
  - removing old, 22
- power cycle, 3
- power-on self test (POST)
  - firmware module, 3
- Primary server, 169
- printer
  - printing to attached, 82
- printers
  - non-PostScript, 84
  - setting up, 82
- printing, 82
- PROM, 25
- protocol
  - Spanning Tree, 111
- ps, 7
- pseudo-token, 93

## Q

- QuickLogin, 88

## R

- rdate, 169
- redirection
  - Group Manager, 19, 167
- redundant failover group, 160
- Registered module, 5

- Remove replication, 170
- restart, 138
- restricted runtime environment
  - chroot, 208
- runtime environment
  - chroot, 208
- S**
- screen flipping, 142
- Secondary server, 169
- secure session, 98
- security
  - configuration, 98, 99
  - interconnect, 97
  - session, 99
- security mode
  - hard, 98
  - soft, 98
- security status, 100
- selectAtLogin, 20
- self-registration, 5, 96
- serial peripherals, 79
- server
  - authentication, 97, 98
- Server addresses, 161
- Server-to-switch bandwidth, 12
- service, 5
- session, 5
  - changes, 7
  - connection failures, 101
  - finding, 75
  - managing, 75
  - secure vs non-secure, 98
  - viewing, 77
- session change, 82
- Session Manager, 1, 5
- settings
  - monitor
    - persistent, 18
- shared memory, 196
- Short Cut, 91
- simple failover group, 159
- Simple Network Management Protocol, 114
- smart card, 26
  - adding, 59
  - changing the probe order, 59
  - deleting, 60
  - viewing or listing configured, 57
  - viewing the probe order, 58
- Smart Card Frameworks, 56
- SNMP, 114
- soft security mode, 98
- Spanning Tree protocol, 111
- spoofing, 98
- StarOffice, 196
- StartSession module, 5
- state codes
  - DHCP, 181
- status
  - security, 100
- subnet broadcast, 111
- Sun Directory Services (SunDS) daemon, 26
- Sun Management Center (Sun MC), 113
- Sun MC
  - additional modules, 119
  - additional requirements with Sun Ray
    - module, 115
  - components, 114
  - creating an object, 120
  - installing, 116
  - notifying when parameter reached, 114
  - setting up monitoring environment, 119
- Sun Ray
  - Data Store, 169
- Sun Ray administration data, 38
  - changing, 40
- Sun Ray administration database
  - users
    - adding a token ID, 68
    - adding a user with token ID, 66
    - deleting, 63
    - deleting a token ID, 69
    - displaying current properties, 65
    - editing properties, 67
    - enabling or disabling a token ID, 69
    - finding, 69
    - getting a token ID from a token reader, 70
    - viewing by ID, 62
    - viewing by name, 63
    - viewing current, 65
- Sun Ray appliance, 1, 2, 34

- finding sessions, 75
  - firmware module, 3
  - locking the screen, 26
  - managing sessions, 75
  - multihead feature, 135
  - multihead group, 136
  - shield users, 11
  - starting a print queue, 82
  - updating and upgrading, 25
  - viewing sessions, 77
  - Sun Ray daemons, 128
  - Sun Ray interconnect, 163
    - server IP addresses, 161
  - Sun Ray module
    - activating for troubleshooting, 200
    - loading, 199
    - requirements, 115
    - troubleshooting, 199
  - Sun Ray node
    - creating, 113
  - Sun Ray server, 1, 34
    - device directory, 79
    - installing software, 116
    - installing the software, 116
    - monitoring with CA Unicenter, 132
    - monitoring with HP OpenView VPO, 132
    - monitoring with Tivoli TMS, 132
    - network interfaces, 12
    - performing standard software installation, 118
    - software, 3
    - software daemons, 114
    - viewing all multihead groups, 52
  - Sun Ray Services
    - resetting, 43
    - restarting, 43
  - Sun Ray services, 113
  - Sun Ray Services panel
    - daemons, 129
  - Sun Ray Settings
    - changing, 51
  - Sun Ray system, 113
    - computing model, 1
    - monitoring feature, 114
    - security, 14
    - software requirements, 115
  - Sun Ray System panel
    - displaying, 126
    - refreshing, 127
    - setting alarms, 127
  - SunMC, 113
    - Health Monitor module, 119
    - Process Monitoring, 119
  - SUNWesagt package
    - to verify installation on Sun Ray, 118
  - SUNWsynom, 119
  - SUNWutesa package
    - removing, 134
  - Switch
    - high-capacity, 11
    - low-capacity, 11
  - switch
    - basic types of 100 Mbps, 11
    - layer 2, 11
  - syslog, 185
- ## T
- Tarantella, 196
  - TCP, 162
  - TerminalGroup policy, 142
  - TFTP, 220
  - thread\_name, 192
  - token reader
    - creating, 44
    - getting a token ID from, 70
    - locating, 44
  - troubleshooting
    - activating the Sun Ray module, 200
    - loading the Sun Ray module, 199
- ## U
- ulimit, 148
  - Uplink ports, 12
  - utaction, 16
  - utadm, 16, 23, 108
  - utadm command, 22, 160
    - available options, 166
  - utadm -r command, 24
  - utaudio command, 194
  - utauthd, 193
  - utcapture, 16, 104
  - utcapture command
    - data elements, 34

- utcard, 16, 32
- utconfig, 16
- utconfig command, 135, 169, 176
- utcrypto, 16, 98
- utdesktop, 16
- utdetach, 16, 29
- utdetach command, 89, 91
- utdsd daemon, 26
- utdssync, 16
- utfwadm, 16
- utfwadm command, 25
- utfwsync, 16
- utglpolicy, 21
- utglpolicy (decremented in 2.0), 17
- utgroupsig, 17, 177
- utgstatus, 17
- utidle, 193
- utinstall, 17
- utkiosk, 17
- utload, 193
- utmhadm, 17, 135
- utmhconfig, 17, 135
- utmhconfig command, 136
- utmhscreen, 17
- utpolicy, 17, 21, 22, 148
- utpolicy command, 96
- utpolicy -i clear command, 22
- utpreserve, 17
- utpw, 17
- utquery, 17, 184
- utrcmd, 17
- utreader, 17, 21
- utreplica, 17, 169
- utreplica command, 169
- utresadm, 18, 28
- utresdef, 18
- utrestart, 18, 21, 138
- utrestart -c, 22
- utselect, 18, 19, 82, 167
- utsession, 18
- utsessiond, 7, 192
- utset, 18
- utsettings, 18, 28, 29, 31

- utslaunch.properties files, 91
- utsunmc, 18, 134
  - install, 117
- utsunmcinstall, 18, 134
- utsvc, 18
- utswitch, 18, 19, 82
- utswitch command, 21
- utuser, 18
- utwall, 18
- utwall command, 94, 96
- utxconfig, 18, 137
- utxconfig command, 135
- utxset, 18

## V

- vendor-specific options, 218
- virtual frame buffer, 2
- VLAN, 12
  - implementing a Sun Ray interconnect, 10
  - multiple configuration, 10

## W

- workgroups, 12

## X

- X cursor, 190
- Xconfig, 191
- XINERAMA, 136, 141
- Xinerama, 196
- xinitrc file, 27
- Xservers, 191
- Xsun, 191
- xterm, 211