Sun Ray™ Server Software 4.0 Administrator’s Guide

for the Linux Operating System

Sun Microsystems, Inc.
www.sun.com

Part No 820-0412-06
June 2007 Beta Release

Submit comments about this document at: `http://www.sun.com/hwdocs/feedback`

Contents

Figures

Tables

Preface

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

Before You Read This Book

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

How This Book Is Organized

Chapter 1 gives an overview of the Sun Ray system.

Chapter 2 describes the command-line interface.

Chapter 3 describes the Administration Tool.

Chapter 4 describes peripherals for Sun Ray DTUs.

Chapter 5 describes mobile sessions, also known as Hotdesking.

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

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

Chapter 8 outlines issues pertinent to the Gnome Display Manager.

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

Chapter 10 prsents Kiosk Mode, for controlled access to applications.

Chapter 11 discusses failover groups.

Appendix A addresses user settings and concerns.

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

This manual also contains a glossary and an index.

Using UNIX Commands

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

Typographic Conventions

Typeface	Meaning	Examples
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail.`

`AaBbCc123`	What you type, when contrasted with on-screen computer output	`%` **`su`**
		`Password:`

AaBbCc123	Book titles, new words or terms, words to be emphasized	Read Chapter 6 in the *User's Guide*. These are called *class* options. You *must* be superuser to do this.
	Command-line variable; replace with a real name or value	To delete a file, type `rm` *filename*.

Shell Prompts

Shell	Prompt
C shell	*machine_name*`%`
C shell superuser	*machine_name*`#`
Bourne shell and Korn shell	`$`
Bourne shell and Korn shell superuser	`#`

Related Documentation

Application	Title	Part Number
Installation	*Sun Ray Server Software 4.0 Installation and Configuration Guide for the Linux Operating System*	820-0414
Release Notes	*Sun Ray Server Software 4.0 Re;ease Notes for the Linux Operating System*	820-0418

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`

Please include the part number (820-0412) of your document in the subject line of your email.

CHAPTER 1

Sun Ray System Overview

Although thin client computing has been discussed and attempted 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. Originally developed on Sun's Solaris™ Operating System, Sun Ray Server Software is now also supported on Red Hat Enterprise Linux Advanced Server 4 and SuSE Linux Enterprise Server 9. It also supports many USB peripheral devices, and LAN and low-bandwidth WAN deployment.

Computing Model

The Sun Ray system employs a network-dependent 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 Desktop Units (DTUs). Nearly any Sun server with sufficient capacity can be configured as a Sun Ray server so long as it runs a supported version of the Solaris operating system or one of the supported flavors of Linux.

Various models of Sun Ray DTU are available, differing primarily with respect to size and type of screen; however, all Sun Ray DTUs also include a smart card reader, a keyboard, and a mouse. Sun Ray DTUs have no local disks, operating systems, or applications; they are therefore considered *stateless*. This is what makes them true, or "ultra" thin clients, and it is what makes them inexpensive to maintain as well as extremely secure, both from an intellectual property perspective and for government work. The ability to use USB mass storage devices is administered centrally so that sites with security requirements can easily remove the sort of risk imposed by PCs and other fat clients, which allow the theft of data in case a physical device is stolen.

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. If a server is taken out of service, the Group Manager on each remaining server tries to distribute that 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 4.0 Installation and Configuration Guide*.

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 DTU. Because Sun Ray DTUs are stateless, a session can be redirected to any Sun Ray DTU on the appropriate network or subnetwork when a user logs in or inserts a smart card.

While the session continues to reside on a server, it appears to follow the user to the new DTU. This functionality, called *session mobility*, is the key architectural feature that enables *hotdesking*—the ability of users to access their sessions from any DTU on their network. In addition, *regional hotdesking* now lets users access their sessions from increasingly remote locations.

The Sun Ray System

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

Sun Ray DTU

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

- 24-bit, 2-D accelerated graphics up to 1920 x 1200 resolution at 72 Hz (640 x 480 at 60 Hz is the lowest resolution)
- Multichannel audio input and output capabilities
- Smart card reader
- USB ports that support hot-pluggable peripherals

- Serial port (for the Sun Ray 170 and later models)
- EnergyStar™ compliance
  - No fan, switch, or disk
  - Very low power consumption

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

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

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

Multihead Displays

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. To use multiple screens, the administrator sets up multihead groups, consisting of two or more DTUs, for those users who need them. Administration of multihead groups is explained in Chapter 9.

Firmware Module

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

Sun Ray Server Software

Sun Ray server software allows the administrator to configure network connections, select an authentication protocol, administer authentication tokens, define desktop properties, 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 DTUs
- System administration tools
- Session management
- Device management, including application-level USB access
- Virtual device drivers for audio and serial, parallel, and mass storage USB devices

Sun Ray server software enables direct access to all Linux X11 applications. Third-party applications running on the Sun Ray server can provide access to Microsoft Windows NT applications and a variety of legacy (mainframe) applications. The Sun Ray Connector for Windows enables Sun Ray users to access applications running on remote Windows Terminal Servers (see the *Sun Ray™ Connector for Windows OS, Version 2.0 Installation and Administration Guide*).

Authentication Manager

The Authentication Manager implements the chosen policies for identifying and authenticating users on Sun Ray DTUs. 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 defined by the administrator. It also supplies an audit trail of the actions of users who have been granted administrative privileges over Sun Ray services. The Authentication Manager is not visible to the user.

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

1. A user accesses a DTU.

2. The DTU sends the user's *token* information to the Authentication Manager and requests access. If a smart card is inserted in the DTU, the smart card's type and ID are used as the token. If not, the DTU's Ethernet address is used as a *pseudo-token*.

3. If the Authentication Manager runs through the entire list of modules and no module takes responsibility for the request, the user is denied access.

4. If the user is accepted, the Authentication Manager starts an X Windows session which takes the user to the login screen. Solaris implementations use the `dtlogin` screen; Linux implementations use GDM.

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

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

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

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 DTUs replace workstations or PCs.

- Registered

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

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

  - Central Registration

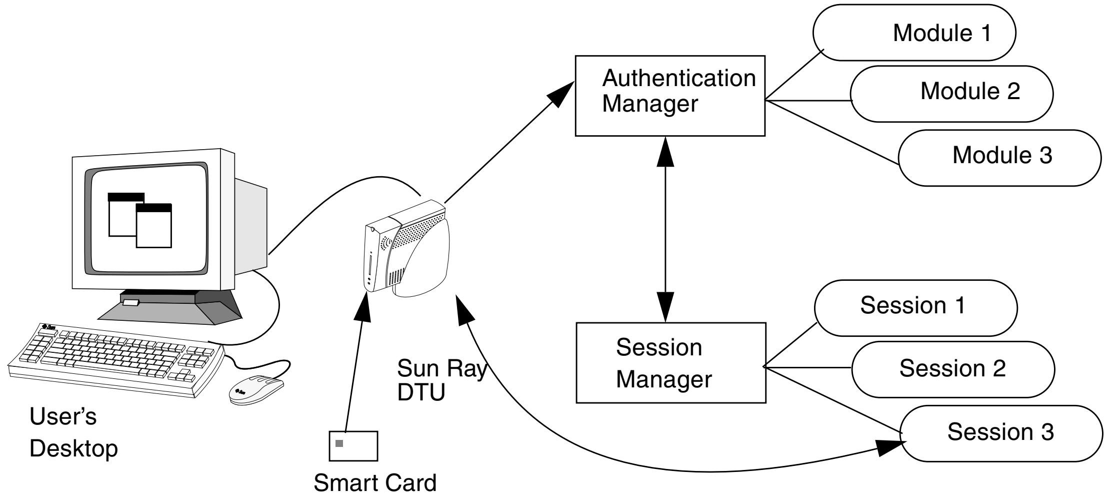
    The administrator assigns smart cards and/or DTUs to authorized users and registers users' tokens in the Sun Ray data store.

  - Self-Registration

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

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

FIGURE 1-1 Authentication and Session Manager Interaction



Sessions and Services

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

The session is associated with a user through an authentication token. A *service* is any application that can connect directly to the Sun Ray DTU. This can include audio, video, X servers, and device control of the DTU. 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 DTU. The Session Manager takes authentication only from authorized Authentication Managers listed in the `/etc/opt/SUNWut/auth.permit` file.

The steps below describe how the process starts and ends:

1. After a user's token is authenticated, the Authentication Manager determines whether a session exists for that token. If a session does not exist, the Authentication Manager asks the Session Manager to create a session and then

starts the appropriate service(s) for the session according to the authentication policy decisions taken by the administrator. Creating a session usually involves starting an Xserver process for the session.

2. When services are started, they join the session explicitly by contacting the Session Manager.

3. The Authentication Manager informs the Session Manager that the session associated with the token is to be connected to a specific Sun Ray DTU. The Session Manager then informs each service in the session that it should connect directly to the DTU.

4. The Authentication Manager determines that the session associated with a token should be disconnected from a DTU. 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 changes in screen real estate allocation.

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 DTU. The `xprop(1)` command can reveal a user's secret session ID. 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 user name@system` to enable only those people you specify to access the display and the user's DTU.

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

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

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

CLI and Admin GUI

Sun Ray Server Software has both a command-line interface (CLI) and a graphical user interface for administrative functions. The Sun Ray Administration Tool (Admin GUI) has been completely rewritten for the 4.0 release to present a clearer view of administrative functions, with tab-based navigational model and context-sensitive help.

Data Store

Sun Ray Server Software 4.0 provides a private data store service, the Sun Ray Data Store (SRDS), for access to SRSS administration data across failover groups.

Kiosk (Controlled Access) Mode

Sun Ray DTUs are becoming more common in public locations, such as airports, where anonymous users have limited access to specific applications. Sun Ray Kiosk mode software has been revised for the 4.0 release. It is described in Chapter 10, along with instructions for migrating configuration data from the previous Controlled Access Mode (CAM).

Network Components

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

- Dedicated interconnect
- VLAN (Virtual Local Area Network)
- LAN (Local Area Network), with or without network routers
- Low-bandwidth[1] WAN (Wide Area Network)
- VPN (Virtual Private Network)

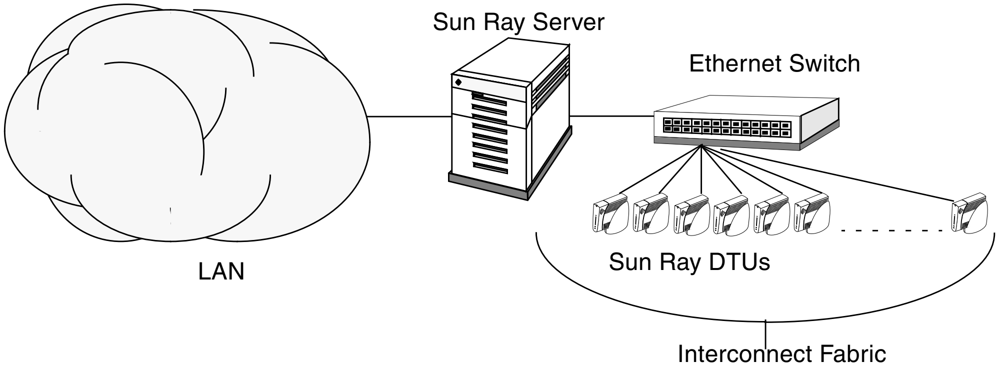
[1] Bandwidth less than 2 Mbps.

Various types of network configuration are discussed in depth in Chapter 7.

Sun Ray Interconnect Fabric

The first Sun Ray implementations relied on dedicated interconnects, using physically dedicated Ethernet networks or logically dedicated networks. Sun Rays can also 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 DTU is attached to the interconnect fabric through its built-in 10/100BASE-T interface.

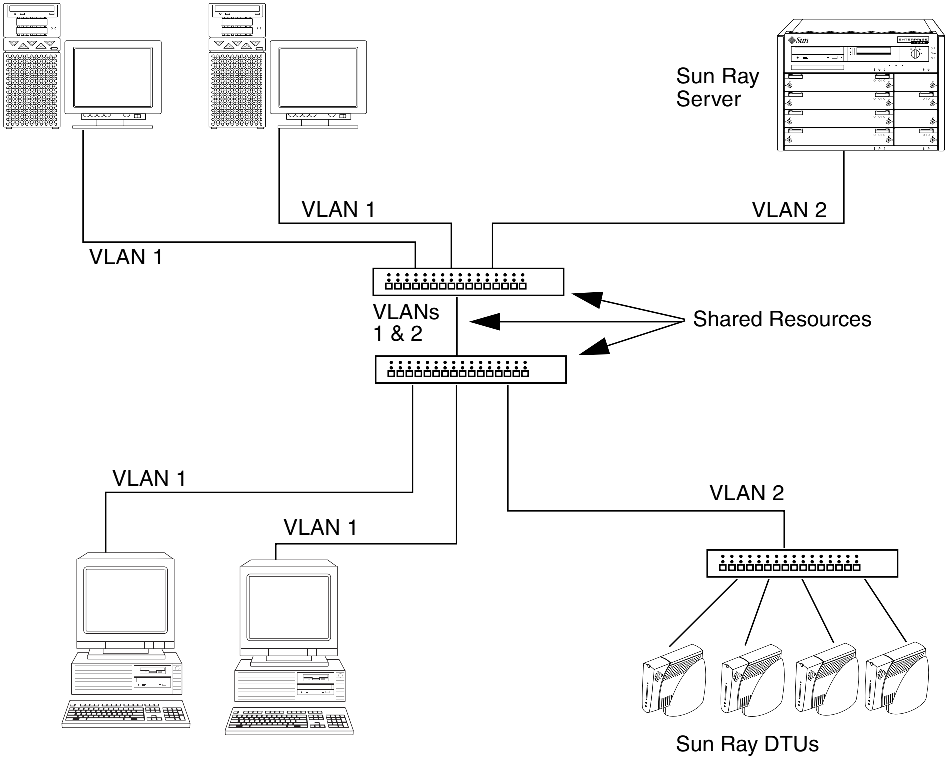
The following sections illustrate some conservative methods of providing good desktop performance to Sun Ray users at a low cost. Many other network scenarios are possible.

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, non-Sun Ray 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 DTU 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.

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.

LAN Implementation

With Sun Ray DTUs deployed on a LAN, users can exercise session mobility across a much larger “domain”—a huge convenience. For basic instructions on configuring different types of networks for Sun Ray implementation, see “Basic Network Topology” on page 36 of the *Sun Ray Server Software 4.0 Installation and Configuration Guide*. For a more detailed discussion of network taxonomy and configuration, see “Deployment on Shared Networks” on page 75.

Physical Connections

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

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

There are two basic types of 100 Mbps switches:

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

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

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

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

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

Deployment Examples

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

Small Deployments

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

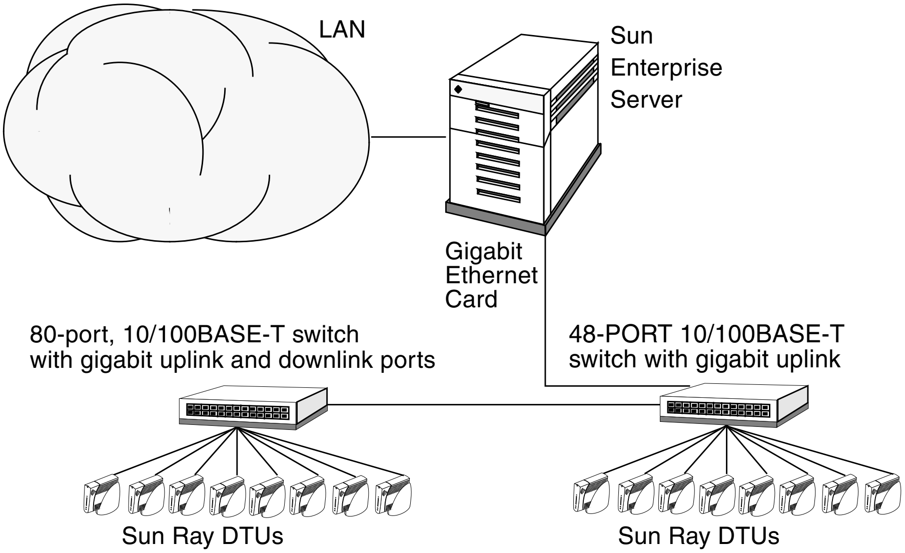
For example, in FIGURE 1-2 a Sun Enterprise™ server with a Sun 10/100BASE-T card and a 24-port 10/100BASE-T switch can easily support 23 users performing standard desktop activities.

Medium to Large Deployments

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

A 100-user departmental system, for example, consisting of a Sun Enterprise server, one gigabit Ethernet card, and two large (48-port and 80-port) 10/100BASE-T switches delivers services to the 100 Sun Ray DTUs (see FIGURE 1-4).

FIGURE 1-4 Small Deployment Scenario


LAN
Sun Enterprise Server
Gigabit Ethernet Card
80-port, 10/100BASE-T switch with gigabit uplink and downlink ports
48-PORT 10/100BASE-T switch with gigabit uplink
Sun Ray DTUs
Sun Ray DTUs

Failover Group Scenario

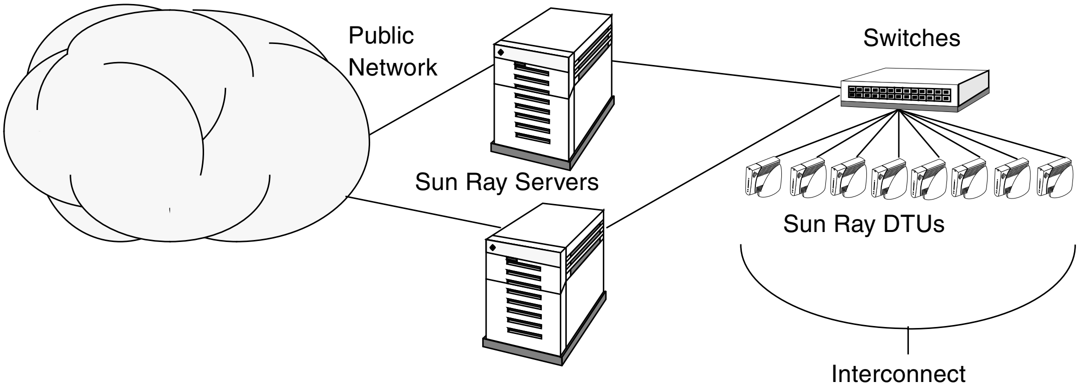
Sun Ray servers can be bound together to create failover groups. A failover group, comprising two or more servers, provides users with a higher level of availability in case one servers become unavailable due to a network or system failure.

When a server in a failover group goes down, whether for maintenance, a power outage, or any other reason, each Sun Ray DTU connected to it reconnects to another server in the failover group. and to a previously existing session for the current token, if there is one, on that server. If it can find no existing session for the current token, the DTU connects to a server selected by the load balancing algorithm. This server presents a login screen to the user, who then logs in to create a new session. The session on the failed server is lost. Failover groups are discussed in Chapter 11 as well as in the *Sun Ray Server Software 4.0 Installation and Configuration Guide*.

Regional Hotdesking

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

FIGURE 1-5 Simple Failover Group



Security Considerations

Using switched network gear for the last link to the DTUs makes it difficult for a malicious PC user or network snooper at one of the network ports to obtain unauthorized information. Because switches send packets only to the proper output port, a snooper plugged into another port receives no unauthorized data. If the server and wiring closet are secure, the last step is switched, and the DTU is plugged directly into the wall jack, then it is very difficult to intercept communications between the server and the DTU. SRSS encryption features also help to protect sensitive data by providing the options to encode keyboard input and display traffic.

CHAPTER 2

Command-Line Interface

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

This chapter contains the following information:

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

TABLE 2-1 Supported Commands *(Continued)*

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

TABLE 2-1 Supported Commands *(Continued)*

Command	Definition
`utpolicy`	The `utpolicy` command sets and reports the policy configuration of the Sun Ray Authentication Manager, `utauthd`(1M). This command's `-i` and `-t` options were deprecated as of the 2.0 release. Continue to use the `utpolicy` command for policy changes, but use the `utrestart` command instead of `utpolicy -i`, and use `utreader` instead of `utpolicy -t`.
`utpreserve`	The `utpreserve` command saves existing Sun Ray Server Software configuration data to the `/var/tmp/SUNWut.upgrade` directory.
`utpw`	The `utpw` command changes the Sun Ray administrator password (also known as the UT admin password) used by the Web-based and command-line administration applications.
`utquery`	The `utquery` command collects DHCP information from the Sun Ray DTUs.
`utreader`	The `utreader` command is used to add, remove, and configure token readers.
`utreplica`	The `utreplica` command configures the Sun Ray Data Store server to enable replication of administered data from a designated primary server to each secondary server in a failover group. The data stores of the secondary servers remain synchronized automatically unless there is a power outage. The `-z` option is useful for updating the port number.
`utresadm`	The `utresadm` 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.
`utresdef`	The `utresdef` command lists the monitor resolutions and refresh rates that can be applied to Sun Ray units through the `utresadm` command.
`utrestart`	The `utrestart` command is used to start Sun Ray services.
`utselect`	The `utselect` command presents the output of `utswitch -l` as a list of servers in the current host group, to be used for reconnection of the current DTU. A user can either select a server from this list or specify a server not in the current host group by typing its full name in the utselect text box.
`utsession`	The `utsession` command lists and manages Sun Ray sessions on the local Sun Ray server.
`utset`	Use `utset` to view and change Sun Ray DTU settings.
`utsettings`	The `utsettings` command opens a Sun Ray Settings dialog box that allows the user to view or change audio, visual, and tactile settings for the Sun Ray DTU.
`utswitch`	The `utswitch` command allows a Sun Ray DTU to be switched among various Sun Ray servers. `utswitch` can also list existing sessions for the current token.
`utumount`	The `utumount` command is used to unmount a file system from a Sun Ray mass storage device.

TABLE 2-1 Supported Commands *(Continued)*

Command	Definition
`utuser`	The `utuser` 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.
`utwall`	The `utwall` utility sends a message or an audio file to users having anXnewt (X server unique to Sun Ray) process. The messages can be sent in email and displayed in a pop-up window.
`utwho`	The `utwho` script assembles information about display number, token, logged-in user, etc., in a compact format.
`utxconfig`	The `utxconfig` program provides X server configuration parameters for users of Sun Ray DTU sessions.

▼ To Stop Sun Ray Services

- **Type:**

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

▼ To Start Sun Ray Services

- **Type:**

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

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

Or

- **Type:**

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

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

Session Redirection

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

▼ To Redirect to a Different Server

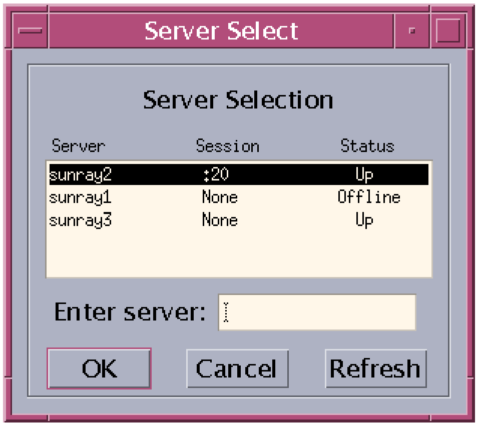
- **From a shell window on the DTU, type:**

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

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

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

FIGURE 2-1 The Server Selection (utselect) GUI



Server	Session	Status
sunray2	:20	Up
sunray1	None	Offline
sunray3	None	Up

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

Note – If only one server in the failover group is up, it is displayed in the utselect GUI. However, if selectAtLogin is set 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 a DTU Manually

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

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

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

▼ To List Available Hosts

- **From a shell window, type:**

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

Hosts available from the Sun Ray DTU are listed.

▼ To Select a Server with the Latest Session

- **In a shell window, type:**

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

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

Managing User Data in the Sun Ray Data Store

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

TABLE 2-2 Key User Fields

Field	**Description**

Token ID	User's unique token type and ID. For smart cards, this is a manufacturer type and the card's serial ID. For DTUs, this is the type "`pseudo`" and the DTU's Ethernet address. Examples:
	`mondex.9998007668077709`
	`pseudo.080020861234`

Server Name	Name of the Sun Ray server that the user is using.

TABLE 2-2 Key User Fields

Field	Description
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.

Note – Sun Ray Server Software now supports multiple administration accounts. This feature is described in "Enabling Multiple Administration Accounts" on page 24.

Changing Authentication Policies

When you set an authentication policy with `utpolicy`, the failover group policy is set automatically, so all that is needed at that point is to reset or restart services. The Admin GUI's System Policy tab refers to authentication policy.

TABLE 2-3 `utrestart` Commands

Command/Option	Result
`/opt/SUNWut/sbin/utrestart`	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. This is a warm restart.
`/opt/SUNWut/sbin/utrestart -c`	Use this option if a significant policy change has been made, such as enabling or disabling access to mass storage devices. All existing sessions are terminated. This is a cold restart.

Enabling Multiple Administration Accounts

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

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

PAM Entries

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

`utconfig(1M)` adds the following PAM entry for Sun Ray Admin GUI configuration:

- On Linux (`/etc/pam.d/utadmingui`):

```
auth sufficient /opt/SUNWut/lib/pam_sunray_admingui.so.1
```

▼ To Configure UNIX Users

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

- **Copy the `auth` entries from `/etc/pam.d/login` file into `/etc/pam.d/utadmingui`:**
  - On RHEL AS 4, the PAM entries are:

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

- On SLES 9, the PAM entries are:

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

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

▼ To Revert to the Old admin User

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

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

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

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

Administration GUI Audit Trail

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

SRSS 4.0 uses the syslog implementation. Events are logged into /var/opt/SUNWut/log/messages file, where audit events are prefixed with the keyword utadt:: so that administrator can filter events from the messages file.

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

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

where

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

Enabling and Disabling Device Services

Sun Ray device services can be enabled/disabled with the `utdevadm` command line tool or with the Admin GUI. Sun Ray device services include USB devices connected through USB ports, internal serial ports, and internal smart card readers on the Sun Ray DTU. Device services can also be administered from the Security tab on the Admin GUI’s Advanced tab.

When internal serial service is disabled, users cannot access embedded serial ports on the Sun Ray DTU. The Sun Ray 170 has two embedded serial ports.

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

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

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

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

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

▼ To Determine the Current State of Device Services

- **Use the utdevadm command:**

```
# /opt/SUNWut/sbin/utdevadm
```

This displays enabled or disabled state of the devices.

▼ To Enable USB Service

- **Use the utdevadm command as below:**

```
# /opt/SUNWut/sbin/utdevadm -e -s usb
```

▼ To Disable USB Service

- **Use the utdevadm command as below:**

```
# /opt/SUNWut/sbin/utdevadm -d -s usb
```

▼ To Perform a Cold Restart

- **Use the utrestart command as below:**

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

Configuring Interfaces on the Sun Ray Interconnect Fabric

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

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

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

▼ To Add an Interface

- **Type:**

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

This command configures the network interface *interface_name* as a Sun Ray interconnect. Specify a subnet address or use the default address, which is selected from reserved private subnet numbers between 192.168.128.0 and 192.168.254.0.

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

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

Any valid network interface can be used. For example:

```
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 DTUs by DHCP.

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

▼ 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 DTUs synchronized with that on the server. See also “Firmware Download” on page 103.

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

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

▼ To Update All the DTUs on an Interface

- **Type:**

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

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

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

- **Type:**

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

Restarting the Sun Ray Data Store (SRDS)

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

▼ To Restart Sun Ray Data Store

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

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

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

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

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

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

Smart Card Configuration Files

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 and various of smart card manufacturers.

▼ To Load a Configuration File Into the Directory

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

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

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

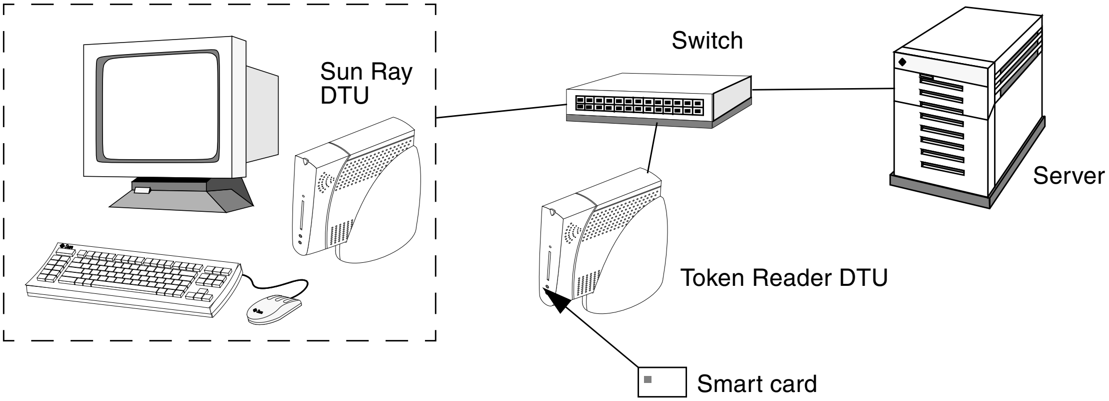
Configuring and Using Token Readers

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 DTUs as dedicated token readers. Site administrators can use a dedicated token reader to administer Sun Ray users through their tokens. A token reader is not used for normal Sun Ray services, so it does not need a keyboard, mouse, or monitor.

Note – When you enable an authentication policy with registered users, or token owners, be sure to specify smart card IDs for the appropriate token owners.

In the example configuration in FIGURE 2-2, the second DTU acts as a token reader.

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



▼ To Configure a Token Reader

The `utreader` command specifies a DTU 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

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

- **Type the following command:**

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

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

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

Using the `utcapture` Tool

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

TABLE 2-4 Data Elements Displayed

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

Tip – If Sun Ray DTU traffic loss is more than .1%, allocate higher priority to the VLAN that carries Sun Ray DTU 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 2-5 `utcapture` Options

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

▼ To Start `utcapture`

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

```
% /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 a DTU.

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

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

```
% /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 DTU 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 the data only for those DTUs that had packet loss.

Examining Log Files

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

TABLE 2-6 Log Files

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

CHAPTER 3

Administration Tool

The Sun Ray Administration Tool (Admin GUI) is organized, as of the 4.0 release, around primary Sun Ray objects, such as servers, sessions, desktop units, and tokens. The tab navigation model is easier to use than the previous navigation tree, and context-sensitive help makes it easier to manage a Sun Ray installation with little need for official documentation. Search functionality has been integrated into the main GUI tabs, and all tables can be sorted by clicking on the column headers.

The navigation hierarchy is organized as follows:

- Servers Tab
  - Server Details
    - View Installed Sun Ray Packages
    - View Network Status
    - View Connected Desktop Units
    - View Session Details
- Sessions Tab
- Desktop Units Tab
  - Desktop Unit Properties
    - Edit Desktop Unit Properties
- Tokens Tab
  - Registered Tokens
  - Currently Used Tokens
  - Add New Token
  - Token Properties
    - Edit Token Properties
- Advanced Tab
  - Security
  - System Policy
  - Kiosk Mode
    - Display Kiosk Mode details

        - Edit Kiosk Mode (specify session type and properties)
    - Card Probe Order
        - Edit Card Probe Order
    - Data Store Password
- Log Files Tab

Login Page

The default user name for the Admin GUI administration account is `admin`. The initial password is set at configuration time (see "Configure Sun Ray Server Software" on page 43 of the *Sun Ray Server Software 4.0 Installation and Configuration Guide for Linux)*.

To allow another user account or accounts to perform administrative functions, see "Enabling Multiple Administration Accounts" on page 24 of this manual.

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

```
http://localhost:1660
```

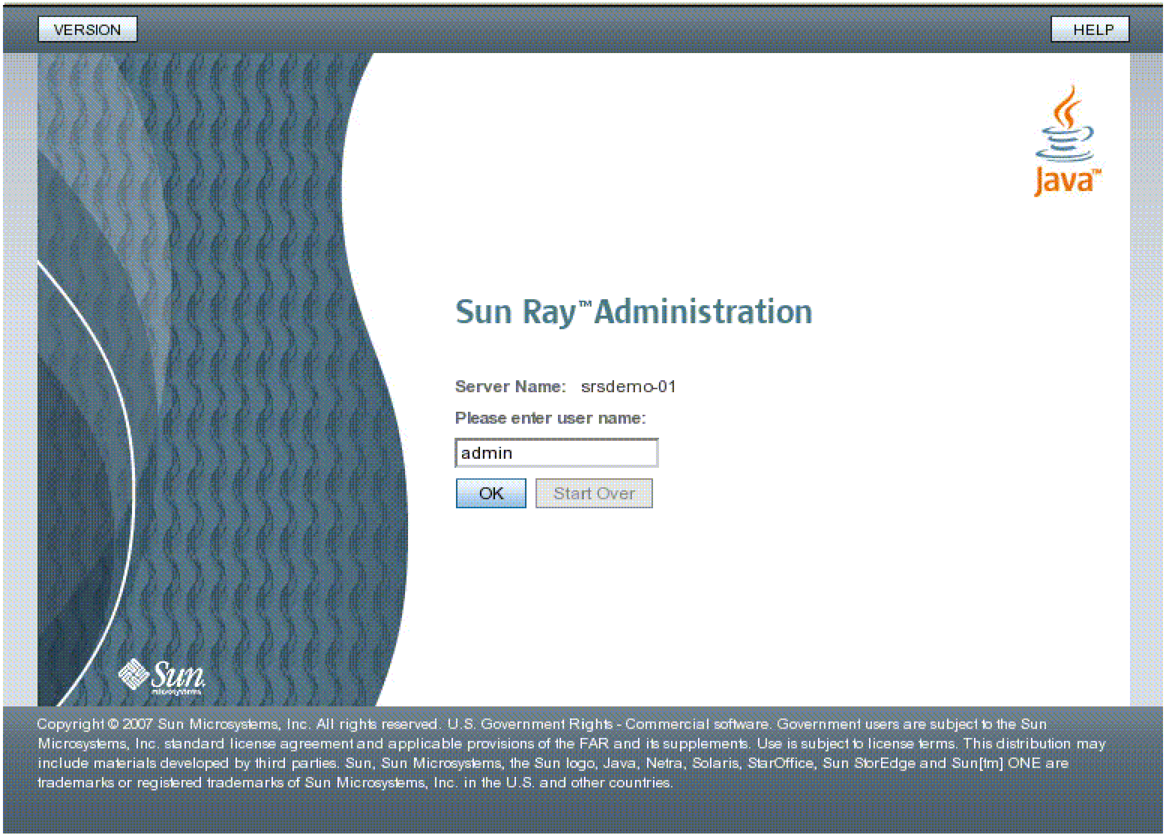
Note – If you chose a different port number when you configured the Sun Ray Server Software, substitute that number for 1660 in the URL above. If secure communication was enabled during SRSS configuration, the browser may be redirected to a secure port (default 1661).

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

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

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

FIGURE 3-1 User Name Challenge Screen



Sun Ray™ Administration

Server Name: srsdemo-01

Please enter user name:

admin

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

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

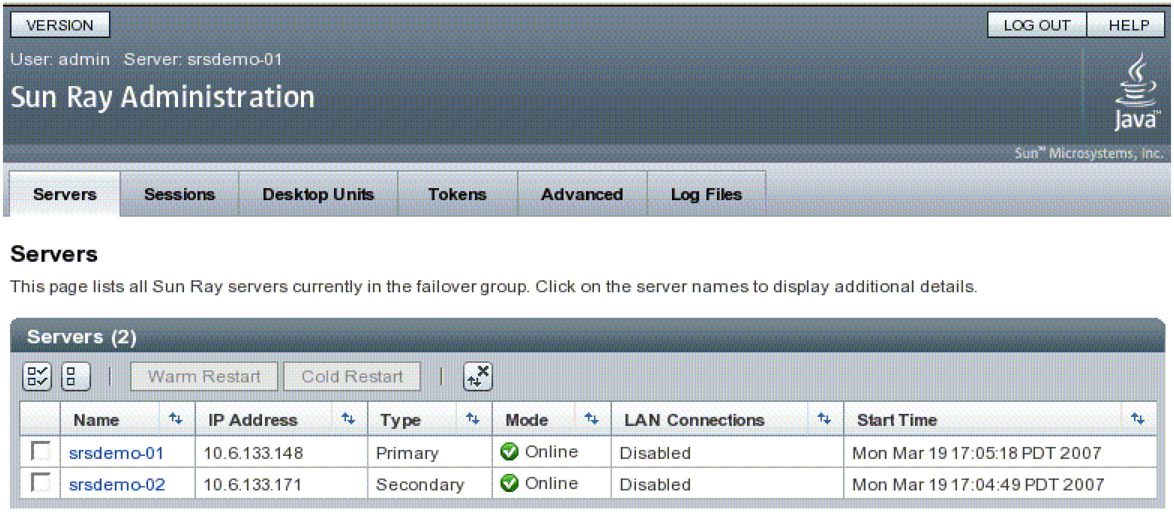
Note – To change the administration password, use the Advanced tab. See "Data Store Password" on page 52.

Servers Tab

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

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

FIGURE 3-2 Top-level Servers Tab



Servers

This page lists all Sun Ray servers currently in the failover group. Click on the server names to display additional details.

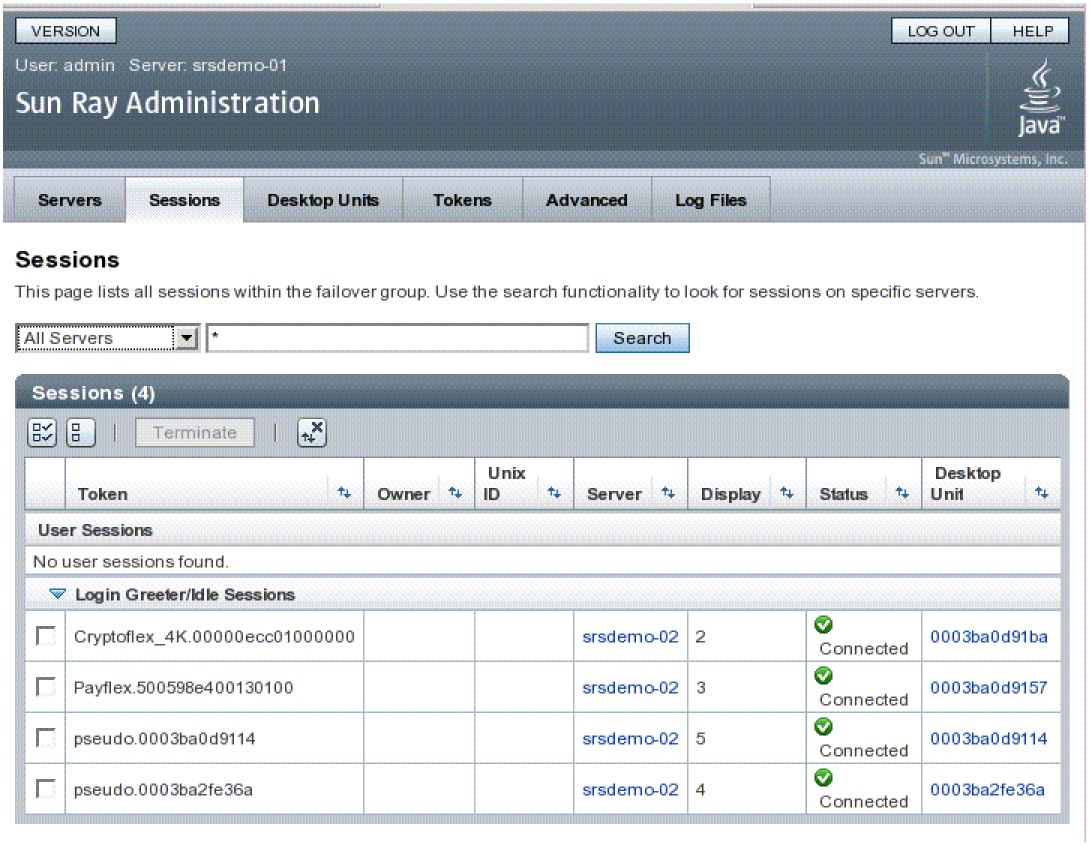
Servers (2)

	Name	IP Address	Type	Mode	LAN Connections	Start Time
□	srsdemo-01	10.6.133.148	Primary	✓ Online	Disabled	Mon Mar 19 17:05:18 PDT 2007
□	srsdemo-02	10.6.133.171	Secondary	✓ Online	Disabled	Mon Mar 19 17:04:49 PDT 2007

Sessions Tab

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

FIGURE 3-3 Sessions Tab Displays Active and Idle Sessions



Sessions

This page lists all sessions within the failover group. Use the search functionality to look for sessions on specific servers.

Sessions (4)

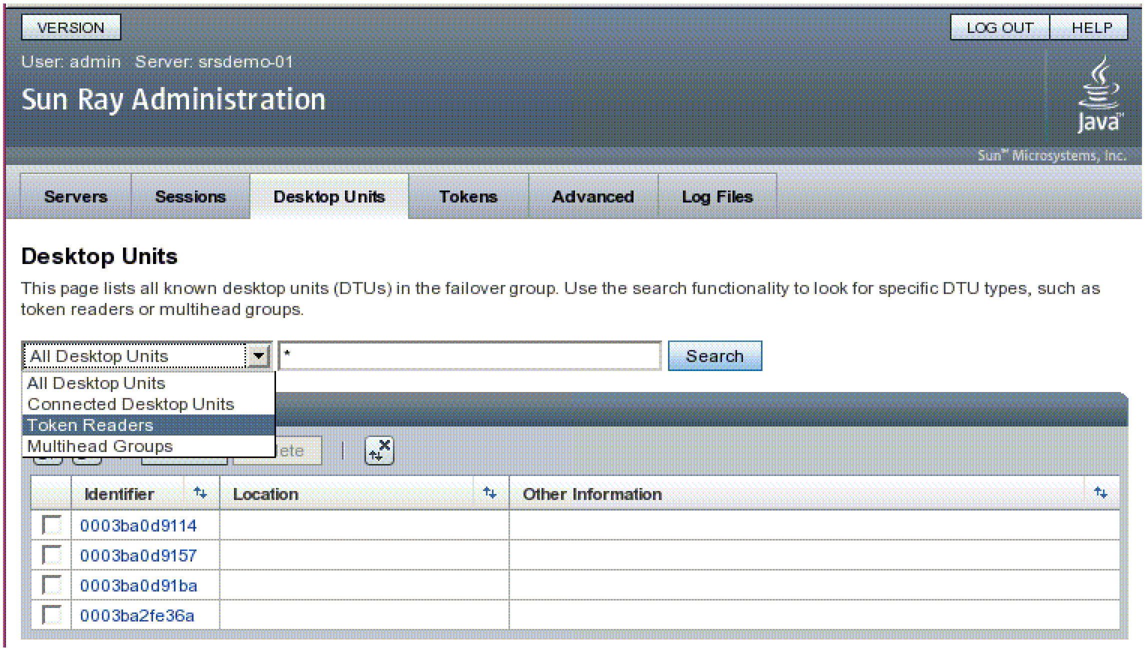
	Token	Owner	Unix ID	Server	Display	Status	Desktop Unit
User Sessions							
No user sessions found.							
Login Greeter/Idle Sessions							
☐	Cryptoflex_4K.00000ecc01000000			srsdemo-02	2	✓ Connected	0003ba0d91ba
☐	Payflex.500598e400130100			srsdemo-02	3	✓ Connected	0003ba0d9157
☐	pseudo.0003ba0d9114			srsdemo-02	5	✓ Connected	0003ba0d9114
☐	pseudo.0003ba2fe36a			srsdemo-02	4	✓ Connected	0003ba2fe36a

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

Desktop Units Tab

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

FIGURE 3-4 Desktop Units Tab



This page lists all known desktop units (DTUs) in the failover group. Use the search functionality to look for specific DTU types, such as token readers or multihead groups.

	Identifier	Location	Other Information
☐	0003ba0d9114		
☐	0003ba0d9157		
☐	0003ba0d91ba		
☐	0003ba2fe36a		

The search drop-down menu provides access to the choices of listing all registered DTUs, listing all connected DTUs, displaying DTUs configured as token readers, or DTUs participating in multihead groups (see “Multihead Groups” on page 120). As on other tabs in the new Admin GUI, clicking on the identifier (MAC address) displays additional details for each DTU. All fields can be sorted by clicking their column headers.

▼ To Display Properties for a DTU

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

▼ To Edit a DTU’s Properties

1. **Click any Desktop Identifier link on the Desktop Units tab, then click the Edit button.**

2. **Enter or modify data in the text boxes, and click the OK button to save the changes to the data store.**

Multihead Groups

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

Token Readers

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

▼ To Set Up a Token Reader

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

   The DTU you have selected is now set up to read smart card tokens.
5. **Restart Sun Ray services.**

   The DTU is now a token reader.

▼ To Locate a Token Reader

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

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

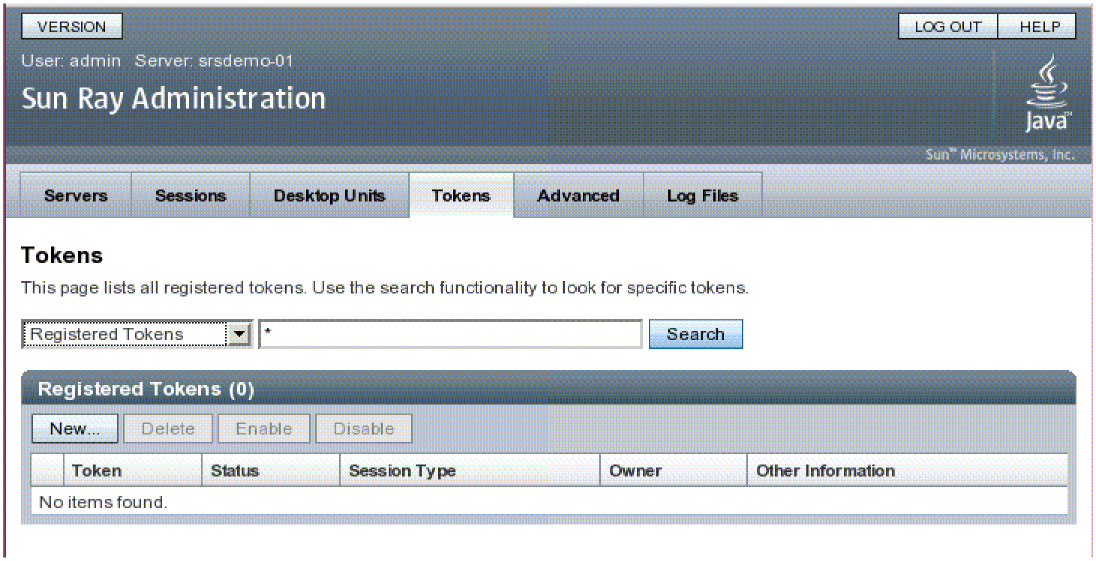
▼ To Get Information on a Token Reader

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

Tokens Tab

The Admin GUI manages *tokens* associated with users.

FIGURE 3-5 Tokens Tab



User: admin Server: srsdemo-01

Sun Ray Administration

Tokens

This page lists all registered tokens. Use the search functionality to look for specific tokens.

Registered Tokens ▾ *

Registered Tokens (0)

	Token	Status	Session Type	Owner	Other Information
No items found.					

For example, smart cards can be registered to specific users, considered as *token owners*.

The Tokens tab also provides check boxes to enable session types, such as Kiosk or regular desktop sessions, to control what type of desktop is displayed for each user token or class of user token.

Note – The Tokens tab is not used to administer token readers. See "Token Readers" on page 45.

▼ To Register a Token

1. **Click on any token on the Tokens tab to display that token's Token Properties page.**
2. **To register a token, press the New button to display.**

   The New Alias Token screen allows you to enter an identifier or select a token reader.

▼ To Enable, Disable, or Delete a Token

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

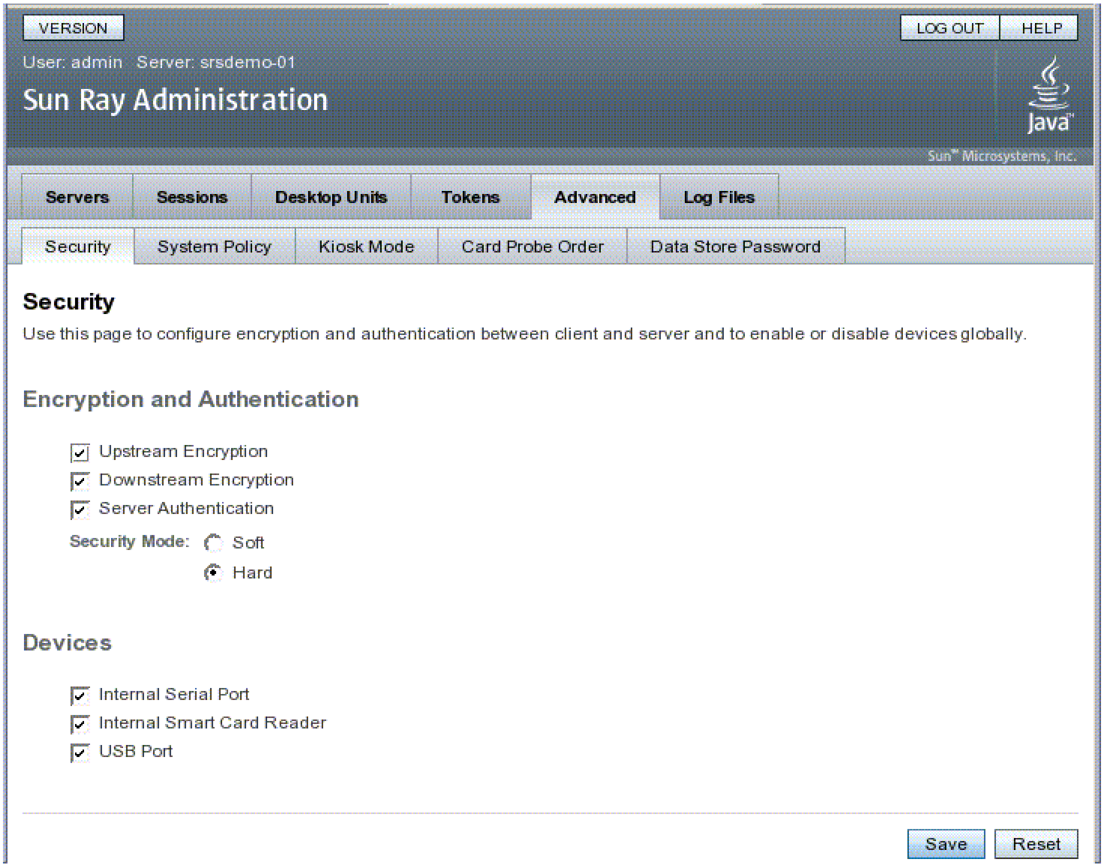
Advanced Tab

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

Security Settings

Security settings include encryption of communication between DTU and server, server authentication, security mode, and device access, as shown in FIGURE 3-6.

FIGURE 3-6 The Security Tab



Security

Use this page to configure encryption and authentication between client and server and to enable or disable devices globally.

Encryption and Authentication

☑ Upstream Encryption
☑ Downstream Encryption
☑ Server Authentication

Security Mode: ○ Soft
● Hard

Devices

☑ Internal Serial Port
☑ Internal Smart Card Reader
☑ USB Port

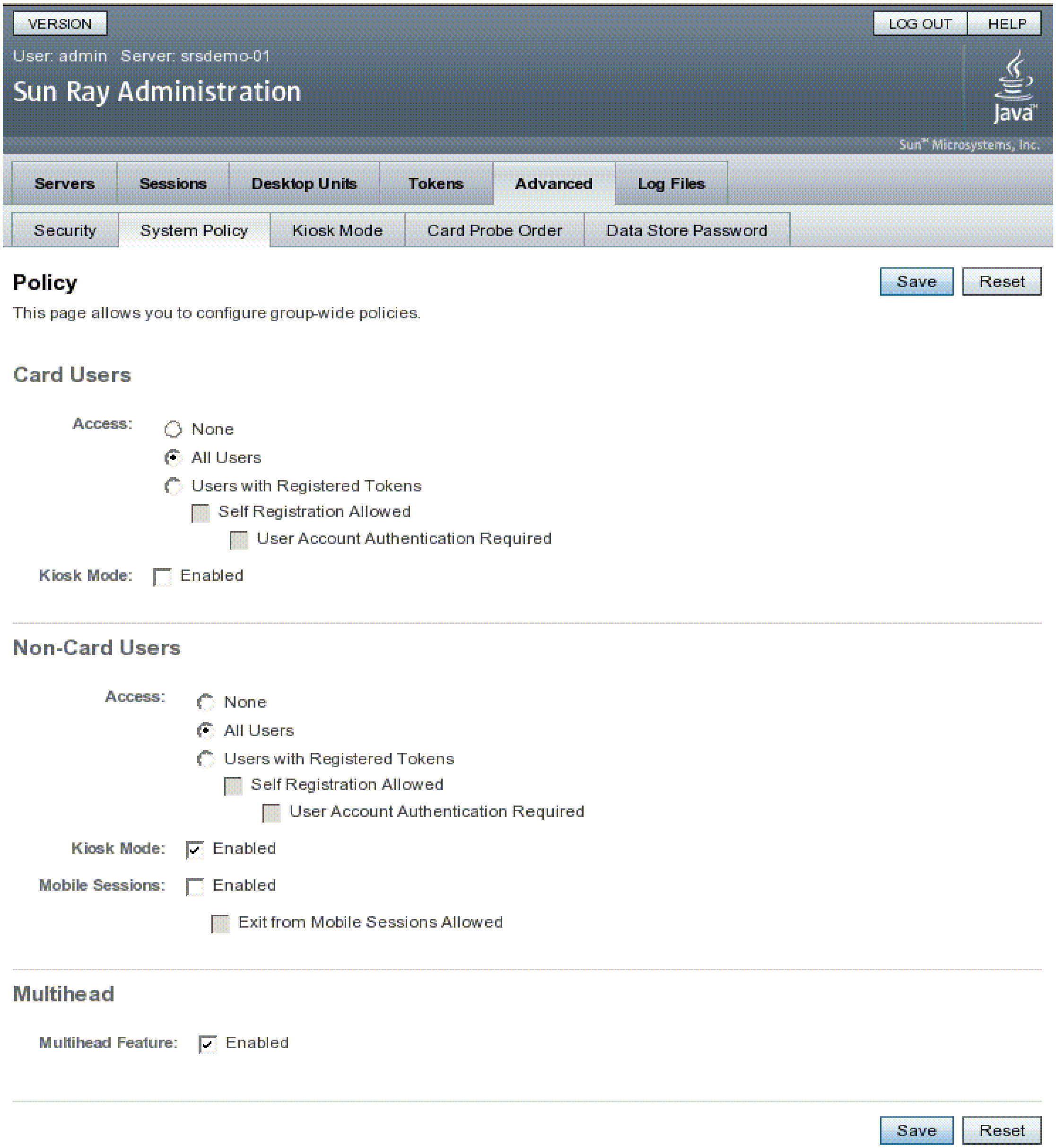
All Sun Ray device services are enabled by default. Sun Ray device services include USB devices connected through USB ports, internal serial ports, and internal smart card readers on the Sun Ray DTU.To enable or disable these services, use the `utdevadm` command line tool (see "Enabling and Disabling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

For a description of encryption and authentication options, see "Encryption and Authentication" on page 71. For devices, see "Peripherals for Sun Ray DTUs" on page 55.

System Policy

Use this tab to regulate authentication manager policy settings, such as access for card users and non-card users, and enabling Kiosk mode and the multihead feature, for each Sun Ray server, or system.

FIGURE 3-7 System Policy Tab



User: admin Server: srsdemo-01

Sun Ray Administration

Policy

This page allows you to configure group-wide policies.

Card Users

Access:
○ None
● All Users
○ Users with Registered Tokens
□ Self Registration Allowed
□ User Account Authentication Required

Kiosk Mode: □ Enabled

Non-Card Users

Access:
○ None
● All Users
○ Users with Registered Tokens
□ Self Registration Allowed
□ User Account Authentication Required

Kiosk Mode: ☑ Enabled

Mobile Sessions: □ Enabled

□ Exit from Mobile Sessions Allowed

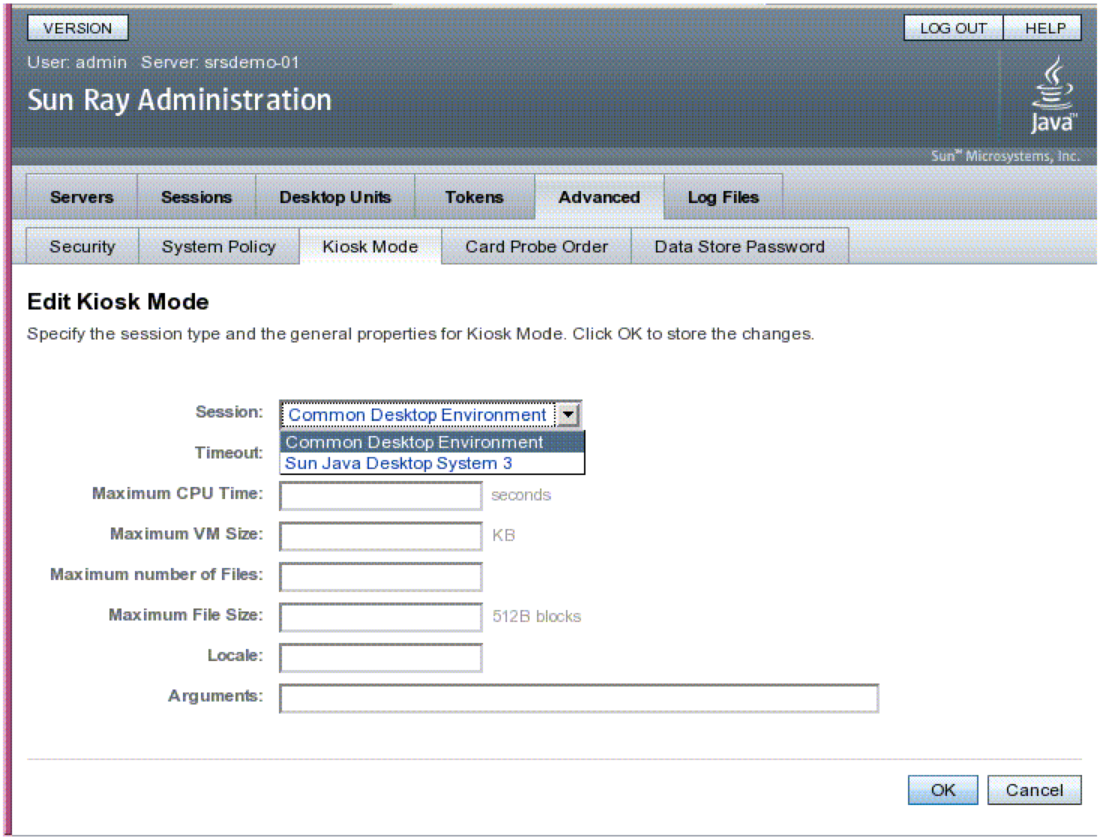
Multihead

Multihead Feature: ☑ Enabled

Kiosk Mode Configuration

To use Kiosk Mode, enable it on the System Policy tab (see FIGURE 3-7) and use the Kiosk Mode tab for setup. For a more detailed description, see "Kiosk Mode" on page 129 of this manual and the *Sun Ray Server Software 4.0 Installation and Configuration Guide for Linux*

FIGURE 3-8 Edit Kiosk Mode Tab



Edit Kiosk Mode

Specify the session type and the general properties for Kiosk Mode. Click OK to store the changes.

Session: Common Desktop Environment
- Common Desktop Environment
- Sun Java Desktop System 3

Timeout:

Maximum CPU Time: seconds

Maximum VM Size: KB

Maximum number of Files:

Maximum File Size: 512B blocks

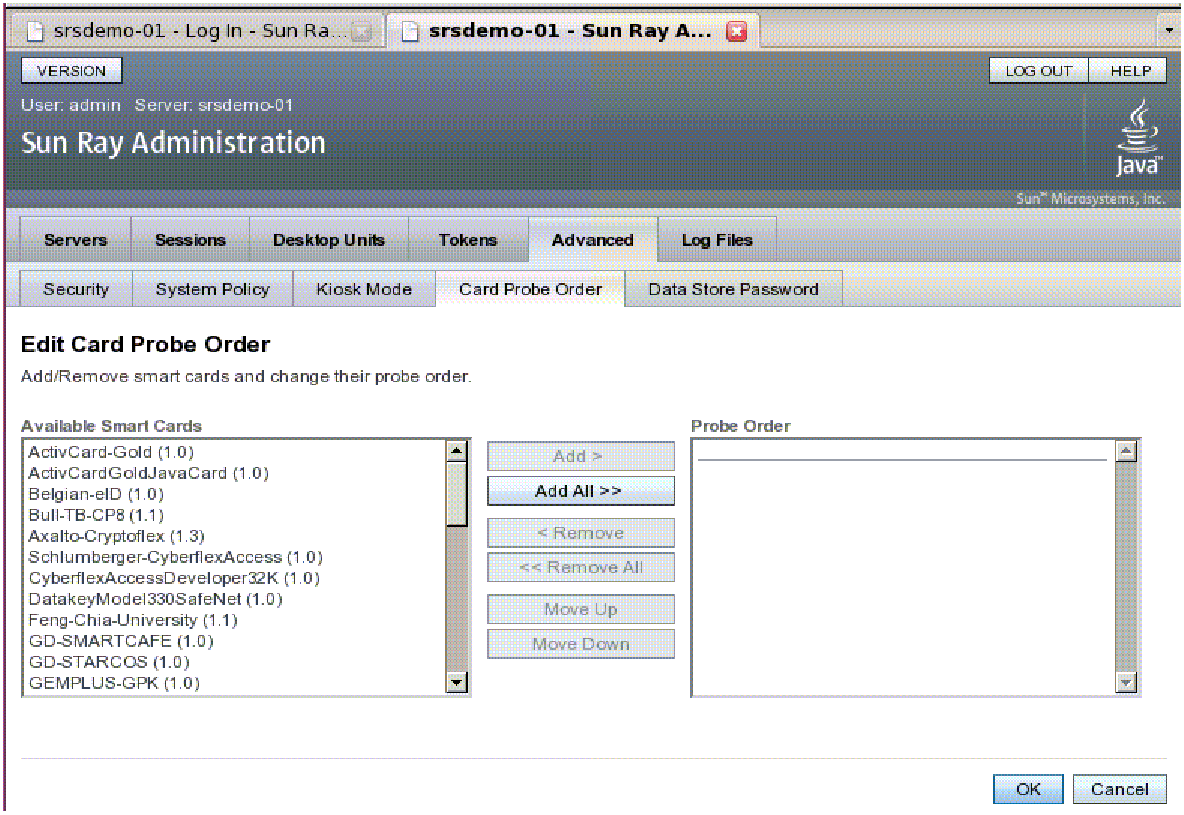
Locale:

Arguments:

Smart Card Probe Order

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

FIGURE 3-9 Edit Smart Card Probe Order



User: admin Server: srsdemo-01

Sun Ray Administration

Edit Card Probe Order

Add/Remove smart cards and change their probe order.

Available Smart Cards

ActivCard-Gold (1.0)
ActivCardGoldJavaCard (1.0)
Belgian-eID (1.0)
Bull-TB-CP8 (1.1)
Axalto-Cryptoflex (1.3)
Schlumberger-CyberflexAccess (1.0)
CyberflexAccessDeveloper32K (1.0)
DatakeyModel330SafeNet (1.0)
Feng-Chia-University (1.1)
GD-SMARTCAFE (1.0)
GD-STARCOS (1.0)
GEMPLUS-GPK (1.0)

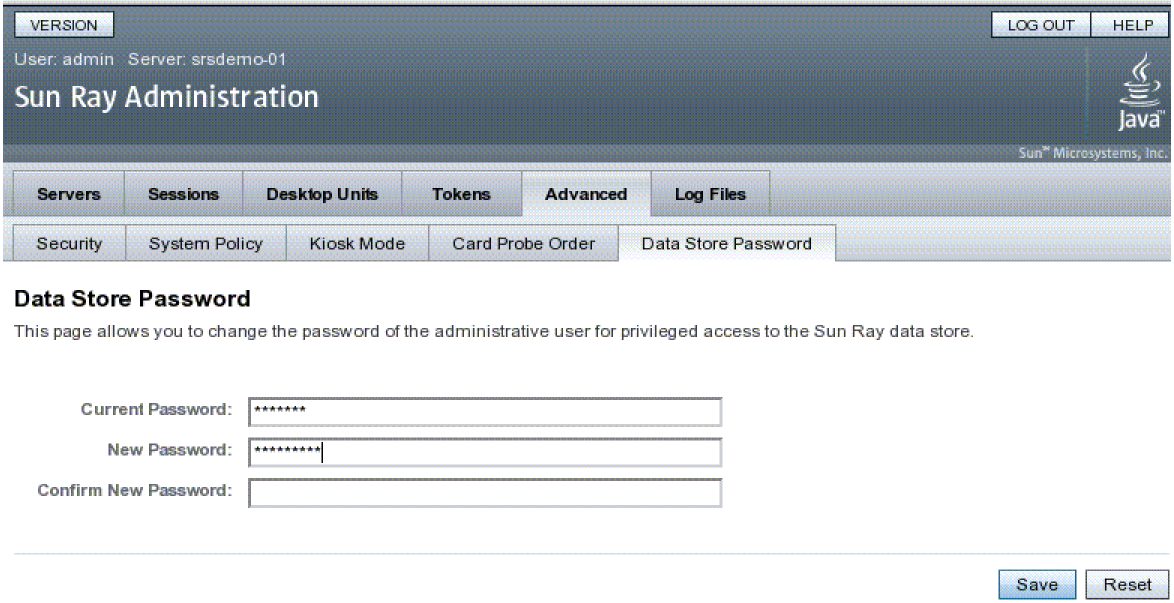
Probe Order

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

Data Store Password

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

FIGURE 3-10 Use the Data Store Password Tab to Change the Admin Password



Data Store Password

This page allows you to change the password of the administrative user for privileged access to the Sun Ray data store.

Current Password: *******

New Password: *********

Confirm New Password:

The Data Store Password tab allows you to change the password for the admin account. The password was set at configuration time (see "Configure Sun Ray Server Software" on page 43 of the *Sun Ray Server Software 4.0 Installation and Configuration Guide for Linux)*.

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

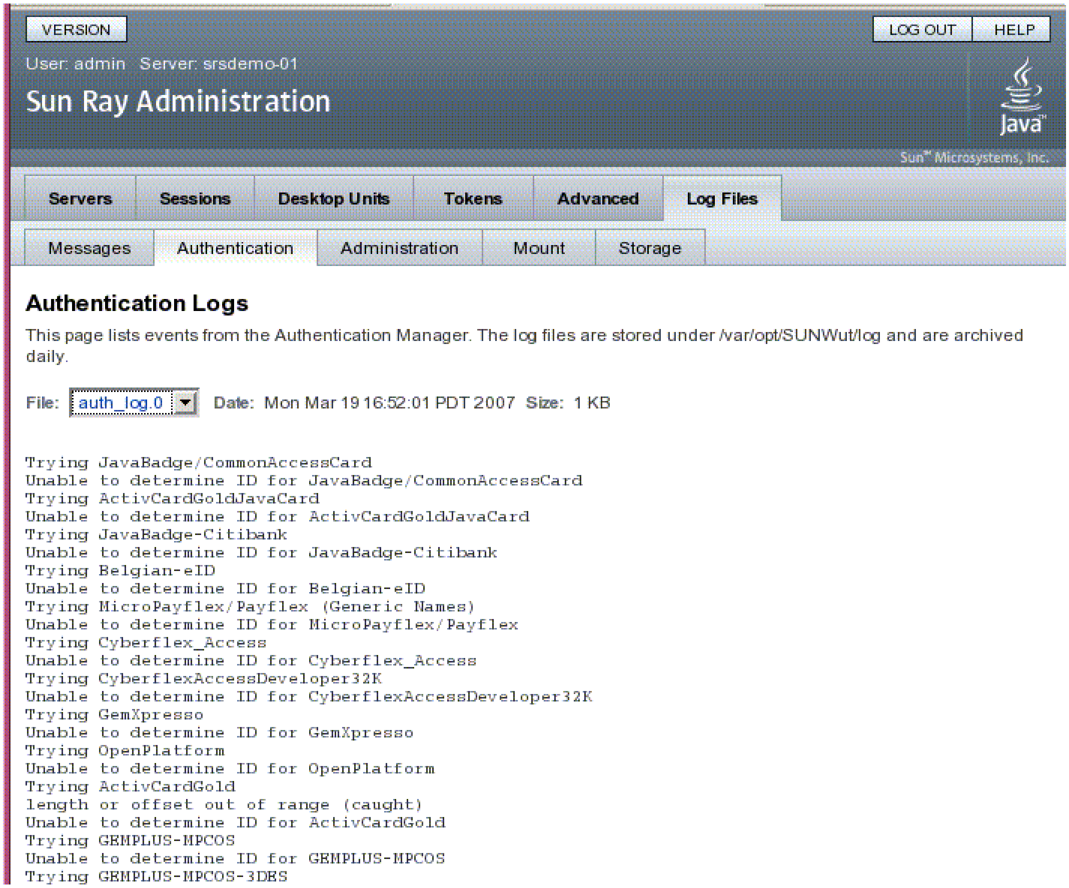
Note – Every server in a failover group must use the same password for the admin account.

The layout of the data store is described in "Managing User Data in the Sun Ray Data Store" on page 22. To allow other UNIX accounts to perform administrative functions, see "Enabling Multiple Administration Accounts" on page 24.

Log Files Tab

This tab provides sub-tabs for displaying the various log files recording events such as system messages, authentication logs, server administration events, mount logs, and storage related actions. To locate Sun Ray log files from the command line, see "Examining Log Files" on page 37.

FIGURE 3-11 Sample Excerpt From an Authentication Log



Authentication Logs

This page lists events from the Authentication Manager. The log files are stored under /var/opt/SUNWut/log and are archived daily.

File: auth_log.0   Date: Mon Mar 19 16:52:01 PDT 2007   Size: 1 KB

```
Trying JavaBadge/CommonAccessCard
Unable to determine ID for JavaBadge/CommonAccessCard
Trying ActivCardGoldJavaCard
Unable to determine ID for ActivCardGoldJavaCard
Trying JavaBadge-Citibank
Unable to determine ID for JavaBadge-Citibank
Trying Belgian-eID
Unable to determine ID for Belgian-eID
Trying MicroPayflex/Payflex (Generic Names)
Unable to determine ID for MicroPayflex/Payflex
Trying Cyberflex_Access
Unable to determine ID for Cyberflex_Access
Trying CyberflexAccessDeveloper32K
Unable to determine ID for CyberflexAccessDeveloper32K
Trying GemXpresso
Unable to determine ID for GemXpresso
Trying OpenPlatform
Unable to determine ID for OpenPlatform
Trying ActivCardGold
length or offset out of range (caught)
Unable to determine ID for ActivCardGold
Trying GEMPLUS-MPCOS
Unable to determine ID for GEMPLUS-MPCOS
Trying GEMPLUS-MPCOS-3DES
```

CHAPTER 4

Peripherals for Sun Ray DTUs

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

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

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

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

Device Nodes and USB Peripherals

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

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

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

Device Nodes

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

```
manufacturer_name, model_name@upstream_hub_port
```

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

The following is a typical device node path:

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

TABLE 4-1 Definitions of Naming Conventions

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

Device Links

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

Typical device links are:

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

```
manufacturer_name-serial_numberindex
```

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

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

Device Node Ownership

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

Hotdesking and Device Node Ownership

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

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

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

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

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

Mass Storage Devices

Device Nodes and Links

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

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

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

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

Mount Points

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

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

Device Ownership and Hotdesking

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

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

```
 % /opt/SUNWut/bin/utdiskadm -r device_name
```

Common Disk Operations

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

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

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

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

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

Attached Printers

Sun Ray Server Software supports PostScript™ printers connected directly to a USB port on the Sun Ray DTU or connected through a USB-to-parallel port adapter. For non-PostScript printer support, refer to "Non-PostScript Printers" on page 63.

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

Printer Setup

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

▼ To Set Up a Printer

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

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

3. **To locate the Sun Ray DTU, type:**

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

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

4. **Locate the port for the printer by typing:**

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

5. **In the directory, locate the printer node.**

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

   Make sure to choose `Other` so that you can enter the device node from Step 4 above.

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

```
# lpstat -d printername
```

Note – For SLES 9, perform the following additional steps:

---

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

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

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

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

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

10. **Restart the `cups` daemon.**

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

Non-PostScript Printers

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

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

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

Adapters

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

libusb

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

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

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

The libusbut man page provided with SRSS 4.0 for Linux discusses options available for using the Sun Ray `libusb` plugin alongside the Linux server-side libusb support.

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

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

CHAPTER 5

Hotdesking (Mobile Sessions)

Note – The Sun Ray system is designed to enable session mobility, or hotdesking, with smart cards. Every Sun Ray DTU is equipped with a smart card reader. Non-Smart Card Mobility is implemented only on Solaris platforms.

Regional Hotdesking

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

- Availability

  It is sometimes advantageous to have multiple, geographically-separate locations, each with a failover group, so that if an outage occurs at one location, another location can continue to function.

- Organizational Policies

  Some sites have different administrative policies at different locations. It can be advantageous to keep separate failover groups at these locations.

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

Note – Regional hotdesking is not enabled for multihead groups.

Functional Overview

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

1. When a smart card is inserted or removed from the system or a user logs in via the greeter GUI, parameters such as the user name (if known at the time), smart card token, and terminal identifier are passed to a piece of site-integration logic.

2. The site-integration software uses these parameters to determine to which Sun Ray servers it should direct the Sun Ray DTU.

3. If the smart card token is associated with a local session, then that session gets preference, and regional hotdesking is not invoked.

4. Otherwise, the regional hotdesking software redirects the Sun Ray DTU to connect to the appropriate Sun Ray server.

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

Site Requirements

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

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

Providing Site Integration Logic

To determine where given Sun Ray DTUs or users should be connected when creating or accessing sessions, the administrator must utilize enterprise data. Sun Ray Server Software 4.0 includes for this purpose:

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

▼ To Configure a Site-specific Mapping Library

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

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

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

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

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

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

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

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

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

Token Readers

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

Configured token readers should have the following value formats:

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

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

To Configure the Sample Data Store

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

- **Create the back-end database file under** `/opt/SUNWutref/amgh/back_end_db` **on the Sun Ray server:**

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

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

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

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

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

- Comments (lines beginning with #) are ignored,
- Key/value pairs other than those mentioned above are ignored.
- The order of key/value pairs is not significant.

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

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

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

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

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

▼ To Disable Regional Hotdesking

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

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

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

CHAPTER 6

Encryption and Authentication

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

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

Introduction

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

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

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

Client and server authentication can resolve this type of attack. This release offers server-side authentication only, through the pre-configured public-private key pairs in Sun Ray Server Software and firmware. The Digital Signature Algorithm (DSA) is used to verify that clients are communicating with a valid Sun Ray server. This authentication scheme is not completely foolproof, but it mitigates trivial man-in-the-middle attacks and makes it harder for attackers to spoof Sun Ray Server Software.

Security Configuration

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

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

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

Security Mode

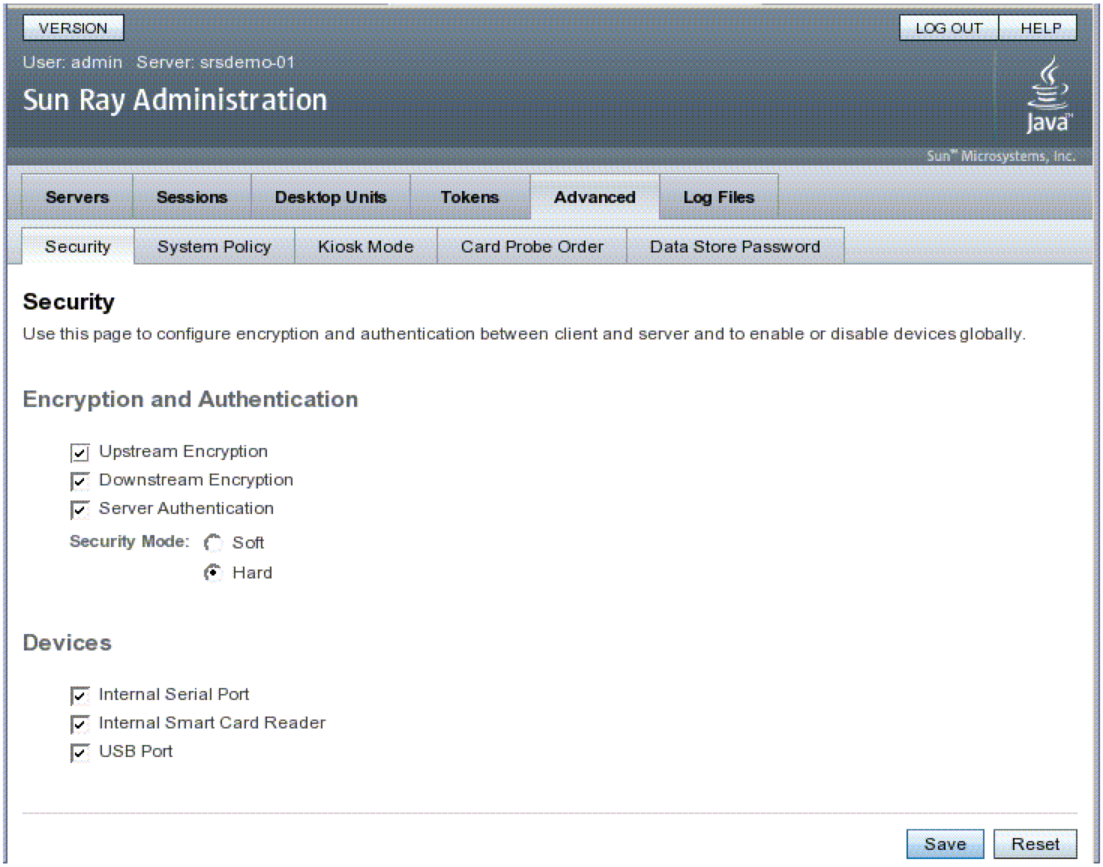
Hard security mode ensures that every session is secure. If security requirements cannot be met, the session is refused. Soft security mode ensures that every client that requests a session gets one; if security requirements cannot be met, the session is granted but not secure.

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

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

For more information, please see the man page for `utcrypto`.

FIGURE 6-1 Sun Ray Security Configuration Tab



Security

Use this page to configure encryption and authentication between client and server and to enable or disable devices globally.

Encryption and Authentication

☑ Upstream Encryption
☑ Downstream Encryption
☑ Server Authentication

Security Mode: ○ Soft
● Hard

Devices

☑ Internal Serial Port
☑ Internal Smart Card Reader
☑ USB Port

Session Security

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

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

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

Security Status

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

CHAPTER 7

Deployment on Shared Networks

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

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

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

Sun Ray DTU Initialization Requirements

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

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

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

DHCP Basics

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

The DHCP protocol defines a number of *standard options* that can be used to inform the client of a variety of common network capabilities. DHCP also allows for a number of *vendor-specific options* (see TABLE 7-3), which carry information that is meaningful only to individual products.

The Sun Ray DTU depends on a small number of standard options to establish its basic network parameters. It depends on several standard and vendor-specific options to provide the additional information that constitutes a complete DTU

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

configuration. If these additional configuration parameters are not supplied, the DTU cannot perform certain activities, the most important of which is the downloading of new DTU firmware. TABLE 7-3 lists the vendor-specific options.

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

The location of the Sun Ray server is usually conveyed to the DTU through one of a pair of DHCP vendor-specific options, *AuthSrvr* and *AltAuth* (see TABLE 7-3).

If the DTU does not receive this information, it uses a broadcast-based discovery mechanism to find a Sun Ray server on its subnet. The DTU firmware now goes one step further. If the broadcast-based discovery mechanism fails, the DTU interprets the DHCP standard option (option 49) of the *X Window Display Manager* as a list of Sun Ray server addresses where it attempts to contact Sun Ray services (see "Configure the external DHCP service." on page 95). This can simplify the DHCP configuration of LAN-deployed Sun Rays by removing the need for a DHCP vendor option to carry this information (see TABLE 7-1).

TABLE 7-1 DHCP Service Parameters Available

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

DHCP Parameter Discovery

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

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

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

DHCP Relay Agent

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

In certain cases, an existing enterprise DHCP service provides the DTU with its IP address while a Sun Ray server provides it with firmware version details and Sun Ray server location. If a deployment plan calls for DHCP parameters to be provided to the DTU by multiple servers, and none of those servers is connected to the subnet where the DTU resides, the DHCP Relay Agent should be configured so that the DTUs subnet can deliver broadcasts to all the DHCP servers. For example, in routers controlled by a Cisco IOS Executive (see “Deployment on a Remote Subnet” on page 90), the ip helper-address command activates a DHCP Relay Agent. Specifying multiple arguments to the ip helper-address command enables relaying to multiple DHCP servers.

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

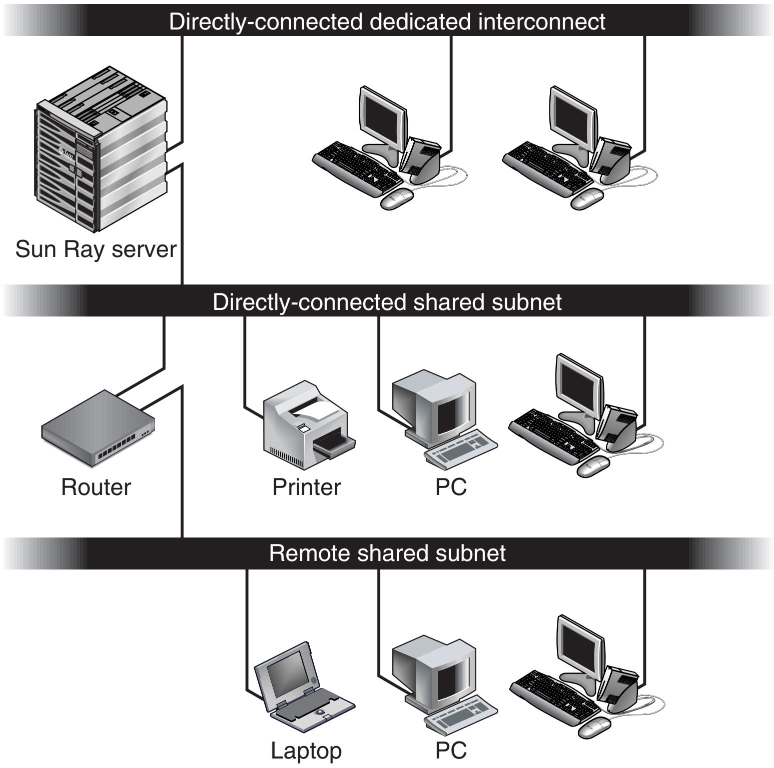
Network Topology Options

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

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

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

FIGURE 7-1 Network Topologies for Sun Ray DTU Deployment


Directly-connected dedicated interconnect
Sun Ray server
Directly-connected shared subnet
Router
Printer
PC
Remote shared subnet
Laptop
PC

Note – Sun Ray traffic on shared networks is potentially more exposed to an eavesdropper than traffic on a dedicated Sun Ray interconnect. Modern switched network infrastructures are far less susceptible to snooping activity than earlier shared technologies, but to obtain additional security the administrator may choose to activate Sun Ray's encryption and authentication features. These capabilities are discussed in "Encryption and Authentication" on page 71.

Directly-Connected Dedicated Interconnect

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

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

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

Directly-Connected Shared Subnet

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

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

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

Remote Shared Subnet

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

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

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

Network Configuration Tasks

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

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

- Deployment on a Directly-Connected Dedicated Interconnect
- Deployment on a Directly-Connected Shared Subnet
- Deployment on a Remote Subnet

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

Preparing for Deployment

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

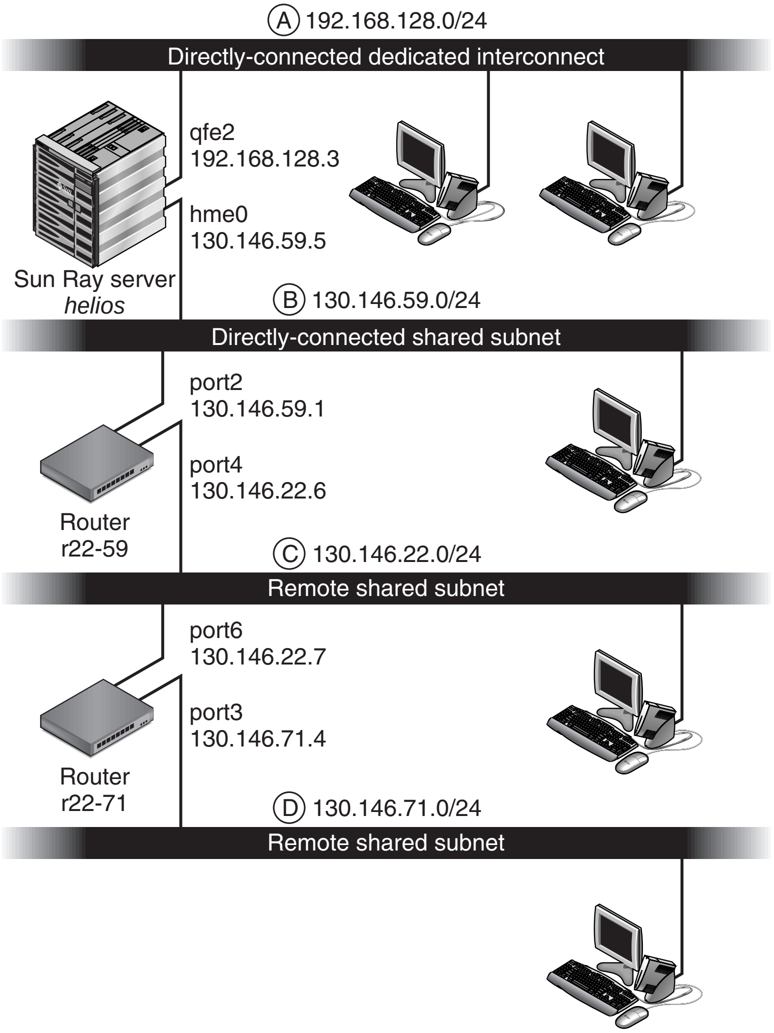
1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?
2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?
3. How will DTUs on this subnet locate their Sun Ray server?

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

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

FIGURE 7-2 Sun Ray Network Topology

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



Deployment on a Directly-Connected Dedicated Interconnect

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

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

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

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

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

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

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

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

Directly-Connected Dedicated Interconnect: Example

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

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

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

CODE EXAMPLE 1

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

CODE EXAMPLE 1

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

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

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

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

```
# /opt/SUNWut/sbin/utrestart
Resetting servers... messages will be logged to
/var/opt/SUNWut/log/messages.
```

Deployment on a Directly-Connected Shared Subnet

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

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

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

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

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

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

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

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

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

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

Directly-Connected Shared Subnet: Example 1

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

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

   From the Sun Ray server.

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

   From the Sun Ray server.

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

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

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

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

TABLE 3

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

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

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

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

```
# /opt/SUNWut/sbin/utrestart
Resetting servers... messages will be logged to
/var/opt/SUNWut/log/messages.
```

Directly-Connected Shared Subnet: Example 2

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

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

   From an external DHCP service.

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

   The DTUs will not be supplied with additional parameters.

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

   By using the local subnet broadcast discovery mechanism.

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

1. **Configure the external DHCP service.**

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

- If the external DHCP service does not have its own direct connection to this subnet, the administrator must configure a DHCP Relay Agent to deliver DHCP traffic on this subnet to the external DHCP service. The most likely location for such a Relay Agent would be on a router in this subnet, in this case the router named `r22-59` in FIGURE 7-2. For a brief introduction to this topic refer to "DHCP Relay Agent" on page 78.
- An existing external DHCP service may need to have its IP address allocation for this subnet increased in order to support the new DTUs. (This applies whenever additional DHCP clients are placed on a subnet.) It might also be desirable to reduce the lease time of addresses on this subnet so that addresses become eligible for reuse quickly.

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

   Run `utadm -L on`:

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

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

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

```
# /opt/SUNWut/sbin/utrestart
Resetting servers... messages will be logged to
/var/opt/SUNWut/log/messages.
```

Deployment on a Remote Subnet

Subnets C and D in FIGURE 7-2 are remote shared subnets.

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

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

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

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

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

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

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

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

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

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

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

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

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

Note – For examples of shared subnet deployments in which both basic networking parameters and additional parameters are delivered by the Sun Ray server and basic networking parameters are supplied by an external DHCP service (with no additional DTU parameters provided), see "Directly-Connected Shared Subnet" on page 81.

Remote Shared Subnet: Example 1

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

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

   From an external DHCP service.

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

   From the Sun Ray server.

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

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

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

1. **Configure the external DHCP service.**

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

- If the external DHCP service does not have its own direct connection to this subnet, the administrator must configure a DHCP Relay Agent to deliver DHCP traffic on this subnet to the external DHCP service. The most likely location for such a Relay Agent would be on a router in this subnet, in this case the router named `r22-59` in FIGURE 7-2. For a brief introduction to this topic refer to "DHCP Relay Agent" on page 78.

- An existing external DHCP service may need to have its IP address allocation increased for this subnet to support the new DTUs. (This applies whenever additional DHCP clients are placed on a subnet.) It might also be desirable to reduce the lease time of addresses on this subnet so that addresses become eligible for re-use quickly.

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

   Because the Sun Ray server does not have its own direct connection to this subnet, the administrator must configure a DHCP Relay Agent to deliver the subnet's DHCP traffic to the Sun Ray server. The most likely location for such a Relay Agent would be on a router in this subnet, in this case the router named `r22-59` in FIGURE 7-2. For a brief introduction to this topic refer to "DHCP Relay Agent" on page 78.

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

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

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

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

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

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

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

---

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

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

CODE EXAMPLE 2

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

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

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

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

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

```
# /opt/SUNWut/sbin/utrestart
Resetting servers... messages will be logged to
/var/opt/SUNWut/log/messages.
```

Remote Shared Subnet: Example 2

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

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

   From an external DHCP service.

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

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

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

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

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

1. Configure the external DHCP service.

Determining how to configure the external DHCP infrastructure to provide basic networking parameters to the DTUs on this subnet is beyond the scope of this document. However, for this example, assume that DHCP service is provided by

Cisco IOS-based router r22-71 in FIGURE 7-2, attached to the 130.146.71.0 subnet through its 10/100 Ethernet port 3. This router can be configured to provide basic networking parameters and the location of a Sun Ray server as follows:

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

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

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

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

---

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

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

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

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

```
# /opt/SUNWut/sbin/utrestart
Resetting servers... messages will be logged to
/var/opt/SUNWut/log/messages.
```

TABLE 7-3 lists the vendor-specific DHCP options that Sun Ray defines and uses.

TABLE 7-3 Vendor-specific DHCP Options

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

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

- `AltAuth` and `AuthSrvr` indicate the IP addresses of Sun Ray servers. Addresses in the `AltAuth` list are tried in order until a connection is established. Current firmware ignores `AuthSrvr` if `AltAuth` is provided, but it is good practice always to specify `AuthSrvr` for the benefit of old (pre Sun Ray Server Software 1.3) firmware, which does not understand the `AltAuth` option. If neither of these options is supplied, the DTU tries to locate a Sun Ray server by sending broadcasts on the local subnet. If the DTU contains firmware at Sun Ray Server

Software 2.0 patch level 114880-01 or later, it resorts to trying to contact a Sun Ray server at the address supplied in the option of the *X Window Display Manager* if that option has been provided.

- `NewTVer` and `FWSrvr` must both be provided in order for the DTU to attempt a firmware download. `NewTVer` contains the name of the firmware version that the DTU should use. If this name does not match the name of the firmware version that the DTU is actually running, the DTU tries to download the desired firmware from a TFTP server at the address given by `FWSrvr`.
- `LogHost` must be specified in order for the DTU to report messages through the syslog protocol. Reporting thresholds for major DTU subsystems are controlled by the `LogKern`, `LogNet`, `LogUSB`, `LogVid`, and `LogAppl` options.

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

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

Network Performance Requirements

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

Packet Loss

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

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

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

Latency

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

Out-of-Order Packets

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

Encapsulated Options

For each parameter name, there is a vendor ID, an option code, an option type, and an indication as to whether the parameter is mandatory.

Vendor-specific options are delivered through encapsulated options in DHCP. Encapsulated options are somewhat more complicated, as illustrated in the following DHCPINFORM response, or DHCPACK, which shows the taxonomy of the bytes in the vendor-specific information portion.

```
                                  2b 4a 17 1d 32 2e 30   .......: .+J..2.0
0140  5f 31 39 2e 63 2c 52 45  56 3d 32 30 30 32 2e 30   _19.c,RE V=2002.0
0150  39 2e 30 36 2e 31 35 2e  35 34 21 04 68 6d 65 30   9.06.15. 54!.hme0
0160  1f 04 81 92 3a 88 15 04  81 92 3a 88 1d 01 06 1c   ....:... ..:.....
0170  01 06 1b 01 06 1a 01 06  19 01 06 18 04 81 92 3a   ........ .......:
0180  88 16 02 1b 61
```

Note – In this description, hexadecimal values are preceded by 0x and followed by their decimal value, after an = sign, as in 0x2b=43.

- The first byte is the option code.
- The next byte represents the encapsulated option length, that is, the number of bytes that make up the option value.
- The next one or more bytes make up the multi-byte option value.
  The option value is followed by another encapsulated option code, and so on.

The example begins with 0x2b=43, the DHCP option for vendor-specific information. It has a length of 0x4a=74 bytes, which is the total number of bytes that follow. These bytes contain the encapsulated vendor options.

The remainder of the example represents the value of the vendor-specific information options. The first byte contains the first encapsulated option, whose value is 0x17=23, and the NewTVer option, whose value type is ASCII. The next byte is 0x1d=29, which is the length of the NewTVer string. These options are followed by 29 bytes that represent the string itself.

The ASCII interpretation at the right of the DHCPACK, is 2.0_19.c,REV=2002.09.06.15.54. This is the end of the first encapsulated option. The next byte is the beginning of the next option, Intf, represented by 0x21=33. The next byte, the length, is 0x04=4, and the next four bytes are the ASCII value hme0. That's the end of the second encapsulated option.

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

Troubleshooting Tools

utcapture

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

utquery

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

OSD Icons

Sun Ray DTU on-screen display (OSD) icons contain information that can help the administrator understand and debug network configuration problems. The amount of information encoded into the icons has been significantly expanded in the firmware delivered with Sun Ray Server Software. The icon structure and progression are described in detail in Appendix B. Recent updates to Sun Ray DTU firmware include OSD icons that are larger and easier to read than previous versions. The icon message codes and DHCP states they display, however, remain the same and are listed in Table B-1 on page 177 and Table B-2 on page 178 respectively.

Remote Configuration

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

For a more complete treatment of network configuration, including DHCP and vendor-specific options, see TABLE 7-1and TABLE 7-3.

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

```
ip dhcp excluded-address 129.149.244.161
ip dhcp pool CLIENT
    import all network 129.149.244.160 255.255.255.248
    default-router 129.149.244.161
    option 26 hex 0556
    option 49 ip 10.6.129.67 129.146.58.136
    lease 0 2
```

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

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

The router's WAN port either plugs directly into the DSL/Cable modem[4] or into the home firewall/gateway. The Sun Ray DTU then plugs into one of the four LAN ports on the router. If the router has been configured to supply DHCP parameters to the Sun Ray DTU, it will tell the DTU to try to connect to the appropriate Sun Ray server.

The router should bring up a VPN tunnel when it is plugged in; it should always be on. Each router should be connected to the VPN gateway and programmed with a user name based on an employee's ID and a random password. The VPN gateway should be configured to allow only Sun Ray traffic to pass, and only to a limited

[4] IA VPN router plugged directly into the DSL or Cable modem can be connected only to a Sun Ray DTU.

number of hosts, so that users cannot connect anything else to the LAN side of the router and then connect into the corporate network. However, users may connect more than one Sun Ray DTU.

Firmware Download

Improvements in the firmware make it easier to bring up a set of Sun Ray DTUs with nothing more than generic DHCP parameters.

- The burden of defining the server list can be shifted to the Domain Name Service (DNS).
- Firmware management can be shifted completely to TFTP.
- If `sunray-config-servers` and `sunray-servers` are defined appropriately by the DNS serving a set of remote Sun Rays DTUs, no extra DHCP parameters are required other than basic network information.

The enhancements include:

1. Incorporation of a DNS client in the firmware, which allows many values to be names rather than IP addresses.

2. Support for DHCP option 66 (TFTP server name) as an alternative to the `FWSrvr` vendor option. This can resolve to a list of IP addresses, one of which is chosen randomly.

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

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

5. Inclusion of `servers=<`*server name list*`>` and `select=<inorder|random>` in the `*.parms` files to allow:

   - specification of a list of server names
   - specification of whether the names should be used in order, or at random

   If a name resolves to multiple addresses, then an IP address is chosen according to the select keyword.

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

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

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

Routerless VPN Capability

Sun Ray Server Software and the most recent firmware provide a VPN solution for remote users that does not require a separate VPN router. The IPsec capability in the Sun Ray firmware allows the Sun Ray DTU to act as a standalone VPN device. The most commonly used encryption, authentication, and key exchange mechanisms are supported, along with Cisco extensions that allow a Sun Ray DTU to interoperate with the Cisco 3000 family of VPN gateways.

Although digital certificates are not supported, the security model is identical to that of the Cisco software VPN client. Using a common group name and key for the initial (IKE phase one) authentication exchange, the DTU authenticates the user individually with the Cisco `Xauth` protocol, either by presenting a fixed user name and password stored in flash or by requiring the entry of a user name and one-time password generated by a token card. See “Download Configuration” on page 108.

Pop-up GUI

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

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

- Non-DHCP network configuration for standalone operation, when it is impossible to configure local DHCP operation

- Local configuration of Sun Ray specific parameters, such as server list, firmware server, MTU, and bandwidth limits
- DNS servers and domain name for DNS bootstrapping
- PPPoE configuration
- IPsec configuration
- Wireless network configuration (used in Tadpole laptops)

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

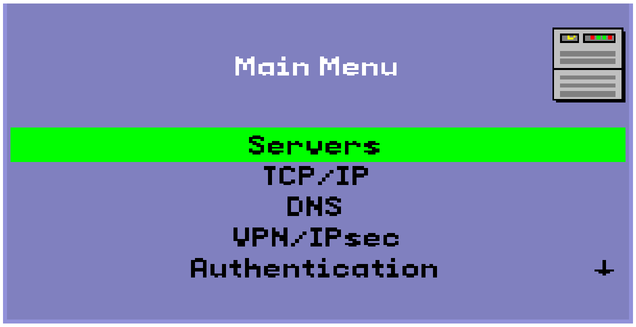
The key combinations used to enter this prompt model are unlikely to be used for other purposes. On a regular Sun keyboard, the key combinations are of the form `Stop-`<*x*>, where <*x*> is one of the keys listed in TABLE 7-4. On non-Sun (PC) keyboards, use the key combination `Ctrl-Pause-`<*x*>.

TABLE 7-4 Prompt Mode Key Codes

Code	Meaning
A	Soft reset (Ctrl-Moon)
C	Clear configuration
N	Show status (3 audio keys)
S or M	Enter main configuration menu
V	Show model, MAC address, and firmware version
W	Enter wireless configuration menu (currently disabled)
Right arrow	Volume up (right arrow)
Left arrow	Volume down (left arrow)
Down arrow	Mute/Unmute

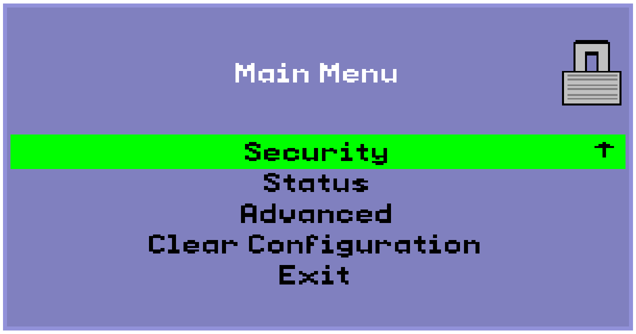
`Stop-M` invokes the main configuration menu.

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



The arrow at the lower right corner indicates that the menu can be scrolled with the Up and Down arrow keys. To clear the contents of an existing entry, use `Ctrl-u`.

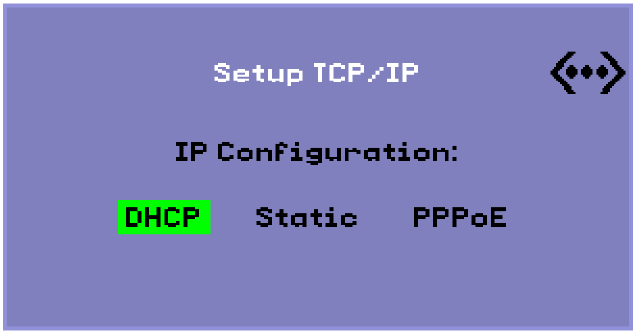
FIGURE 7-5 Pop-up GUI Main Menu (Part II)



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

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

FIGURE 7-6 DHCP Configuration Selection on the Setup TCP/IP OSD



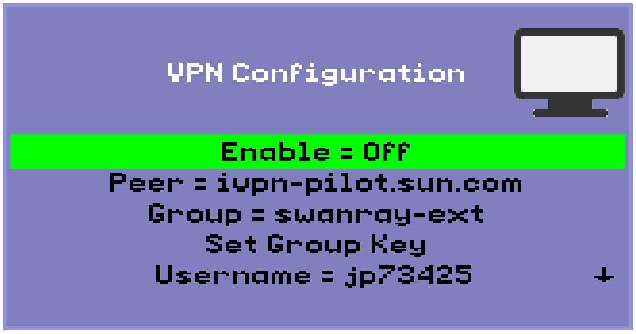
Setup TCP/IP

IP Configuration:

DHCP Static PPPoE

  - Type
    DHCP, Static, or PPPoE
  - DHCP
    MTU only
  - Static
    IP address, netmask, router, broadcast address, MTU
  - PPPoE
    PAP user name and password, MTU
- DNS
  - Domain name
    One only
  - DNS Server list
    List of IP addresses
- VPN/IPsec (Cisco 3000 semantics)

FIGURE 7-7 Enable VPN Configuration Policy Toggle



VPN Configuration

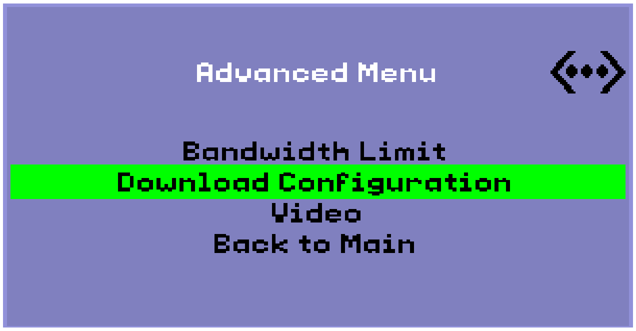
Enable = Off
Peer = ivpn-pilot.sun.com
Group = swanray-ext
Set Group Key
Username = jp73425

  - Enable/Disable switch (toggles with Return key (CR))
  - Gateway peer (Name or IP address)

  - Group name
  - Group key
  - Xauth user name (if static)
  - Xauth password (if static)
  - Set PIN

    If the PIN has been set, the user is prompted for it before a locally stored Xauth user name and password are used.
  - Diffie-Hellman group
  - IPsec lifetime
- Authentication (for HTTP authentication)
  - Enable/Disable switch
  - Port number
- Security
  - Set password
    Lock configuration under password control
- Status
  - Version
    Equivalent to STOP-V
- Advanced
  - Bandwidth limit
    In bits per second
  - Download Configuration

FIGURE 7-8 Download Configuration Selection



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

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

  - Set blanking timeout
- Clear Configuration
(also available with STOP-C)

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

Remote Loading of Configuration Data

To help avoid error-prone manual entry of configuration data for deployments where pre-configuration is required, you can use the Pop-up GUI to download a configuration to a Sun Ray DTU from a file on a server via TFTP, as indicated in FIGURE 7-8.

The following keywords correspond to configuration values that can be set from Pop-up GUI menus (see "Pop-up GUI" on page 104). To group items that are logically related, some of the keywords take the form <*family*>.<*field*>.

TABLE 7-5 Pop-up GUI Menu Configuration Values

VPN/IPsec Submenu	
vpn.enabled	enable toggle
vpn.peer	remote gateway name/IP address
vpn.group	VPN group
vpn.key	VPN key
vpn.user	Xauth user
vpn.passwd	Xauth password
vpn.pin	PIN lock for use of user/passwd
vpn.dhgroup	Diffie-Hellman group to use
vpn.lifetime	Lifetime of IKE connection

TABLE 7-5 *(Continued)*Pop-up GUI Menu Configuration Values

DNS Submenu	
dns.domain	Domain name
dns.servers	Server list (Comma-separated IP addresses)
Servers Submenu	
servers	Sun Ray server
tftpserver	TFTP server
loghost	Syslog host
Security Submenu	
password	Set administrator password
TCP/IP Submenu	
ip.ip	Static IP
ip.mask	Static netmask
ip.bcast	Static broadcast address
ip.router	Static router
ip.mtu	MTU
ip.type	Type of network (“DHCP” | “Static” | “PPPoE”)
ip.papname	PPPoE user name
ip.pappasswd	PPPoE password

The format of the file is a set of <*key*>=<*value*> lines, each terminated by a newline character, which are parsed and the corresponding configuration items set (see the sample file below). No whitespace is permitted. Key values are case-sensitive, always lower case, as listed above. To assign a null value, leave the value assigned to a key empty.

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

FIGURE 7-9 Sample VPN Configuration File

Ports and Protocols

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

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

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

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

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

TABLE 7-6 *(Continued)*Sun Ray DTU-to-Server Ports and Protocols

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

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

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

TABLE 7-7 *(Continued)*Sun Ray Server-to-Server Protocols

Sun Ray Server Port	Protocol	Port	Peer	Notes
1660 (HTTP)	<<-HTTP/TCP->	Transient	Localhost	Web GUI, if configured
7007 (UTSESSIOND)	<<-UTSESSION/TCP->	Privileged	Localhost	Session management
7013 (UTSCREVENTD)	<<-UTSCREVENT/TCP->	Transient	Localhost	Smart card events

CHAPTER 8

Gnome Display Manager

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

Unfortunately the version of GDM that is supplied with your system is not able to work in a Sun Ray environment. Therefore, the Sun Ray server software includes a GDM that has been enhanced with the ability to manage Sun Ray devices. This enhanced GDM is otherwise identical to the GDM it replaces, and can still be used to manage the console and/or other displays.

Installation

During the SRSS installation process, you will be asked whether the installation script should remove the existing GDM from your system. You must answer “yes” to this question in order to continue with the SRSS installation. SRSS will then remove the old GDM from your system and install the Sun Ray-enhanced version. If you answer “no”, the SRSS install process will be aborted.

Since the existing GDM will be removed during SRSS install, it is recommended that you *not* use a GDM-controlled display to do the install. Use a telnet session into the server, or a virtual terminal.

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

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

Uninstallation

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

Configuration

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

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

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

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

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

Gnome Display Manager Privileges

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

For example, a line that reads:

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

should instead read:

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

And a line such as:

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

should be removed altogether.

CHAPTER 9

Multihead Administration

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

Note – Regional hotdesking is not enabled for multihead groups.

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

Multihead Groups

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

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

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

Tip – For best results, run `utmhconfig` only from a DTU.

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

Multihead Screen Configuration

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

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

```
% utxconfig -R geometry
```

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

```
% utxconfig -R auto
```

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

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

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

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

```
% utxconfig -r dimensions
```

- **To restore automatic sizing behavior on the next login:**

```
% utxconfig -r auto
```

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

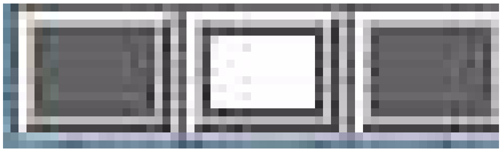
```
% utxconfig -m off
```

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

Multihead Screen Display

When the multihead feature is used, a small window indicating the current session on each screen is displayed with the current screen highlighted for easy identification. This window is automatically displayed for users during session creation. For example, the display in "XINERAMA" on page 125 indicates that the user is on the second screen of a three-screen display.

FIGURE 9-1 The Multihead Screen Display



Multihead Administration Tool

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

▼ To 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.

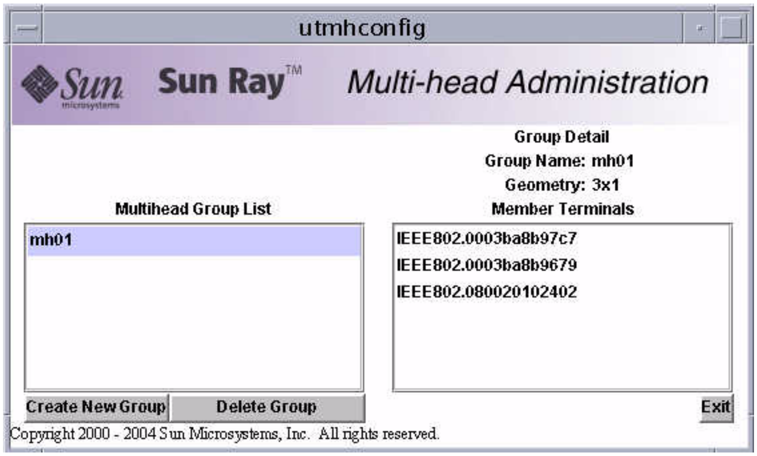
▼ To Create a New Multihead Group

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

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

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

FIGURE 9-2 `utmhconfig` GUI Lists Multihead Groups and Details



utmhconfig

Sun Ray™ Multi-head Administration

Group Detail
Group Name: mh01
Geometry: 3x1

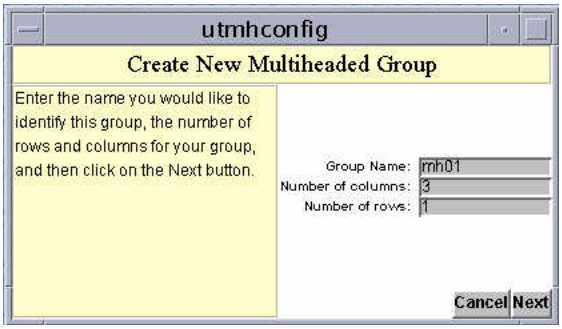
Multihead Group List

Multihead Group List	Member Terminals
mh01	IEEE802.0003ba8b97c7 IEEE802.0003ba8b9679 IEEE802.080020102402

Copyright 2000 - 2004 Sun Microsystems, Inc. All rights reserved.

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



Enter the name you would like to identify this group, the number of rows and columns for your group, and then click on the Next button.

Group Name: mh01
Number of columns: 3
Number of rows: 1

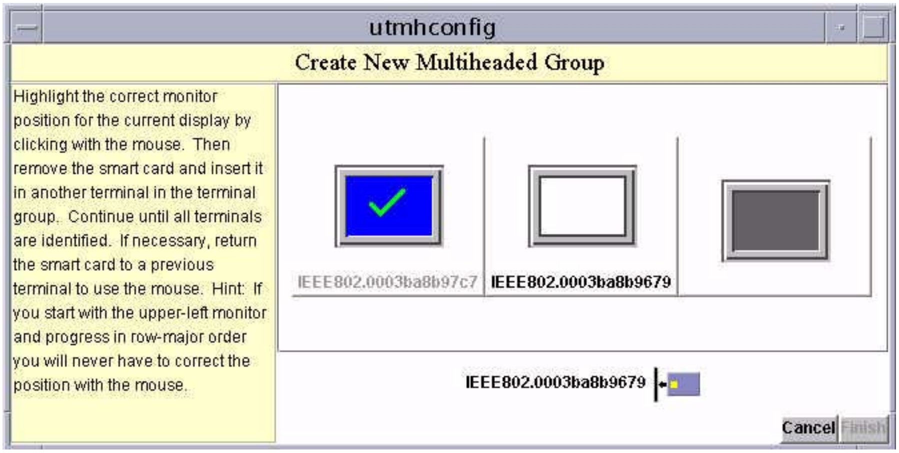
3. **Enter the information for the group.**

   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

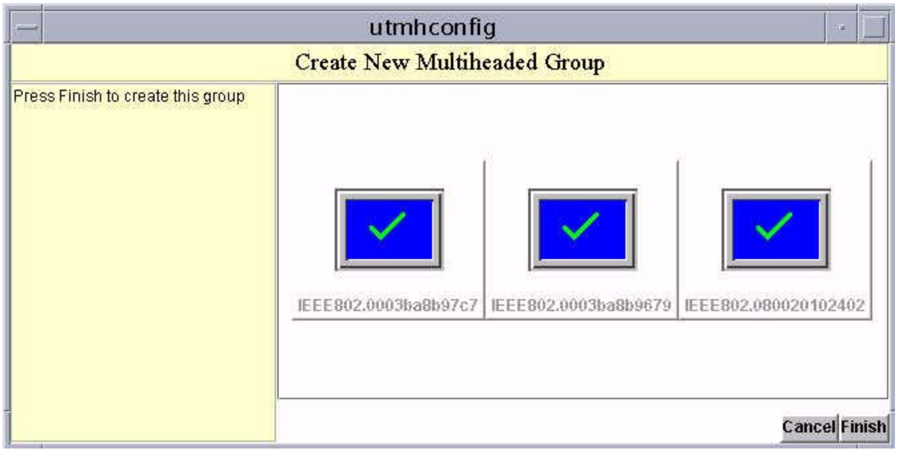


Highlight the correct monitor position for the current display by clicking with the mouse. Then remove the smart card and insert it in another terminal in the terminal group. Continue until all terminals are identified. If necessary, return the smart card to a previous terminal to use the mouse. Hint: If you start with the upper-left monitor and progress in row-major order you will never have to correct the position with the mouse.

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

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

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



Press Finish to create this group

IEEE802.0003ba8b97c7 IEEE802.0003ba8b9679 IEEE802.080020102402

6. **Click the Finish button.**

7. **Exit the session or disconnect by removing your card.**

XINERAMA

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

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

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

The XINERAMA feature is enabled using the following command:

```
% /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
```

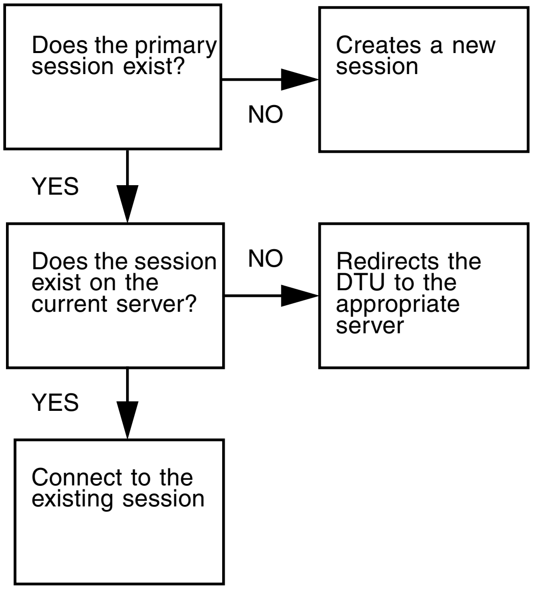
Session Groups

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

Authentication Manager

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

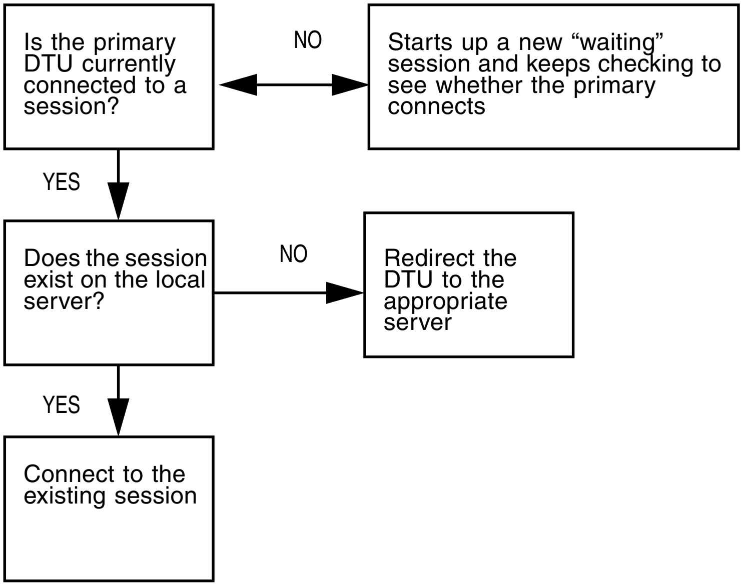
FIGURE 9-6 Authentication Manager Flowchart for the Primary DTU


Does the primary session exist?
NO
Creates a new session
YES
Does the session exist on the current server?
NO
Redirects the DTU to the appropriate server
YES
Connect to the existing session

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

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

FIGURE 9-7 Authentication Manager Flowchart for the Secondary DTU


Is the primary DTU currently connected to a session?
NO
Starts up a new “waiting” session and keeps checking to see whether the primary connects
YES
Does the session exist on the local server?
NO
Redirect the DTU to the appropriate server
YES
Connect to the existing session

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

CHAPTER 10

Kiosk Mode

This chapter describes Kiosk Mode, including instructions for deployment, installation, and configuration of your system to allow controlled, simplified access to anonymous users without compromising the security of the Sun Ray server. Kiosk Mode was formerly known as Controlled Access Mode (CAM).

Topics include:

Kiosk Mode Functionality

The Sun Ray thin client infrastructure is well suited to host Kiosk Mode applications, such as public terminals in airports, in which users access only specified applications and do not need to pass security to log in or to use smart cards. For a detailed explanation of Kiosk Mode, see `kiosk(5)`.

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

Enabling Kiosk Mode

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

Kiosk Mode functionality can be enabled and disabled from the System Policy section of the Advanced tab, and administered from the Kiosk Mode section, which provides check boxes to enable Kiosk Mode for smart card users, non-smart card users, or both.

Note – Before enabling Kiosk Mode you must configure it using `utconfig`.

Enabling Kiosk Mode Using the CLI

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

Note – The following options determine access to the Sun Ray server:
`-z both/pseudo/card`
or
`-r both/pseudo/card [-s both/pseudo/card]`
The `-k both/pseudo/card` option determines whether some or all of the granted sessions are Kiosk sessions.

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

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

All users are directed to Kiosk sessions.

To Enable Kiosk Mode for Card Users Only

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

Only card users are directed to Kiosk sessions.

To Enable Kiosk Mode for Non-card Users Only

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

Only non-card users are directed to Kiosk sessions.

To Enable Both Card and Non-Card Sessions

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

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

To Allow Only Card Sessions in Kiosk Mode

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

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

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

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

Non-card sessions are Kiosk sessions. Allow non-Kiosk card sessions only for registered tokens.

To Enable Kiosk Sessions for Registered Cards and Regular Sessions on Registered DTUS

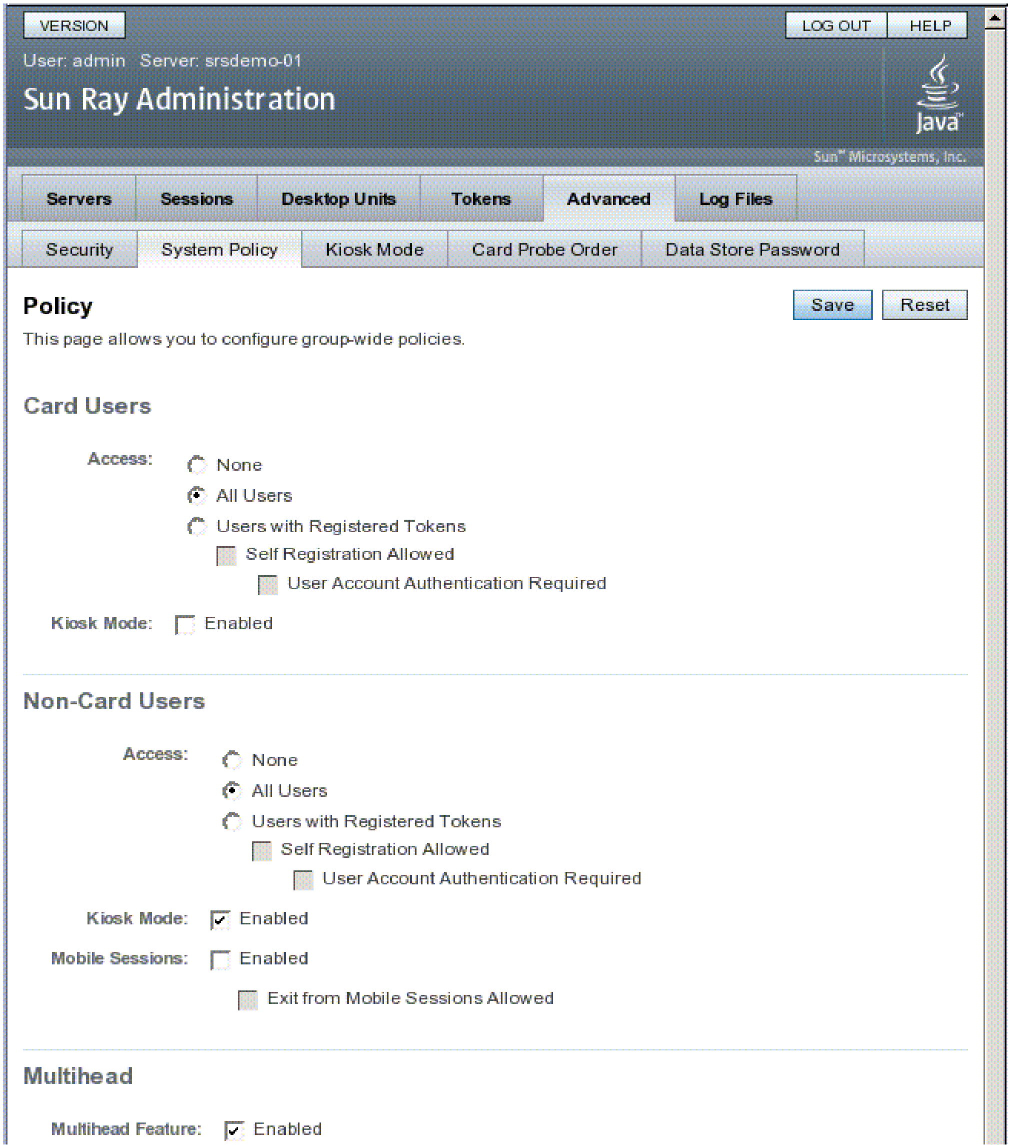
```
# /opt/SUNWut/sbin/utpolicy -r both -s both -k card
```

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

Enabling Kiosk Mode with the Admin GUI

1. **Start the Administration Tool.**
2. **Select the Advanced tab.**
3. **Select the System Policy tab (see FIGURE 10-1).**

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



User: admin Server: srsdemo-01

Sun Ray Administration

Policy

This page allows you to configure group-wide policies.

Card Users

Access:
○ None
● All Users
○ Users with Registered Tokens
□ Self Registration Allowed
□ User Account Authentication Required

Kiosk Mode: □ Enabled

Non-Card Users

Access:
○ None
● All Users
○ Users with Registered Tokens
□ Self Registration Allowed
□ User Account Authentication Required

Kiosk Mode: ☑ Enabled

Mobile Sessions: □ Enabled

□ Exit from Mobile Sessions Allowed

Multihead

Multihead Feature: ☑ Enabled

4. **Select the Kiosk Mode checkbox in the Card Users section, the Non-Card Users section, or both, depending on whether you wish to enable Kiosk Mode for card users, non-card users, or both.**

5. **Click the Save button.**

6. **Select the Servers tab**

7. **Select the relevant server(s) from the list of servers.**

8. **Click the Cold Restart button.**

Overriding Kiosk Mode Policy

To override Kiosk Mode policy for a given token, use the `utkioskoverride` command.

Note – If your policy specifies access for All Users, as in FIGURE 10-1, there is no need to override Kiosk Mode policy.

For example, to enable Kiosk sessions regardless of Kiosk Mode policy for the registered smart card MicroPayFlex.12345678:

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

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

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

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

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

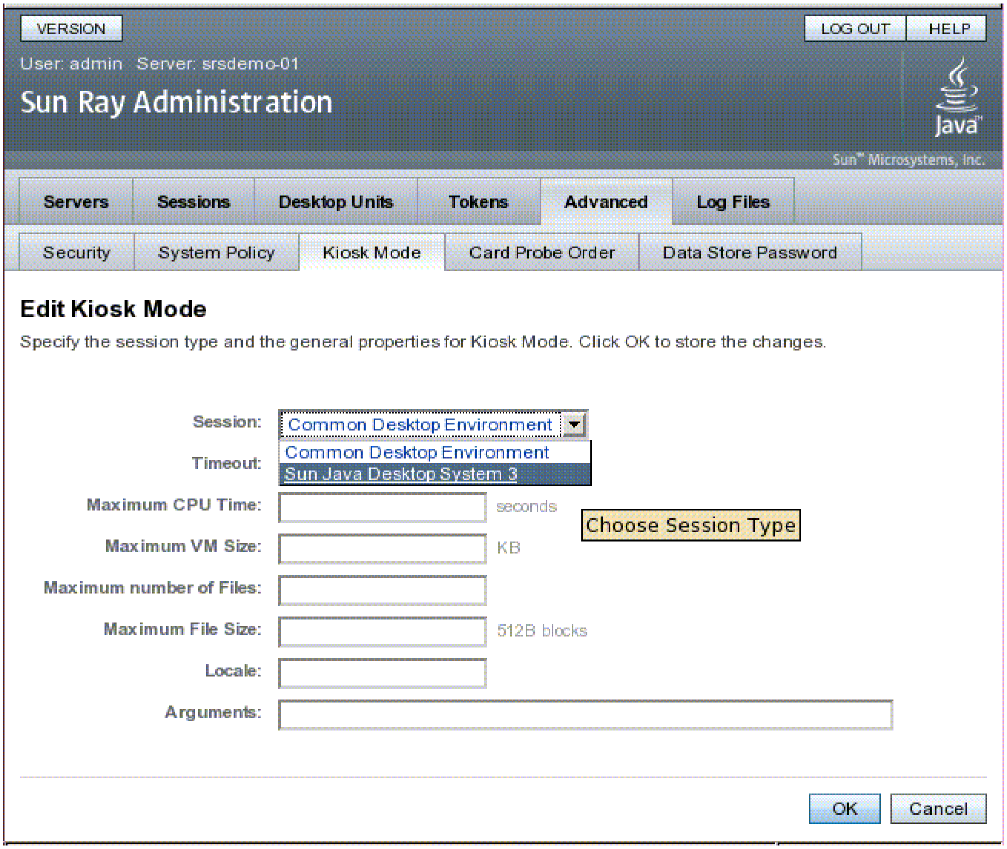
▼ To Override Kiosk Mode Policy from the GUI

1. **Select the Tokens tab.**

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

3. **Click the Edit button.**

FIGURE 10-2 Edit Kiosk Mode Tab



Edit Kiosk Mode

Specify the session type and the general properties for Kiosk Mode. Click OK to store the changes.

Session: Common Desktop Environment

Timeout:

Maximum CPU Time: seconds

Maximum VM Size: KB

Maximum number of Files:

Maximum File Size: 512B blocks

Locale:

Arguments:

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

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

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

      or

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

      or

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

5. **Click the OK button.**

Building the Kiosk Mode Environment

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

▼ To Configure Kiosk Mode Settings

1. **Select the Advanced tab.**
2. **Select the Kiosk Mode tab.**
3. **Click the Edit button.**
4. **Select your preferred Kiosk Session from the Session drop-down list.**
5. **Provide appropriate values for the remaining settings. See** TABLE 10-1 **for descriptions of individual settings.**
6. **Click the OK button.**

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

TABLE 10-1 Kiosk Mode Settings

Setting	Description
Timeout	Indicates the number of seconds after which a disconnected session will be terminated. If you provide no value for this setting, termination of disconnected sessions will be disabled.
Maximum CPU Time	Indicates the maximum number of CPU seconds per process for Kiosk sessions. By default, the system default is applied to all Kiosk sessions. For more information see `ulimit(1)`.
Maximum VM Size	Indicates the maximum Virtual Memory size per process for Kiosk sessions. By default, the system default is applied to all Kiosk sessions. For more information see `ulimit(1)`.
Maximum Number of Files	Indicates the maximum number of open files per process for Kiosk sessions. By default, the system default is applied to all Kiosk sessions. For more information see `ulimit(1)`.

TABLE 10-1 Kiosk Mode Settings *(Continued)*

Setting	Description
Maximum File Size	Indicates the maximum file size per process for Kiosk sessions. By default, the system default is applied to all Kiosk sessions. For more information see `ulimit(1)`.
Locale	Indicates the locale to be used by the Kiosk session. By default, the system default is applied to all Kiosk sessions.
Arguments	Indicates a list of arguments that should be passed to Kiosk sessions as they start. This is a Kiosk session-specific setting. For more information on supported arguments, consult the session-specific documentation for your selected session.

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

▼ To Add an Application

1. **Select the Advanced tab.**
2. **Select the Kiosk Mode tab.**

   If the currently selected Kiosk session supports the addition of applications, there is an Applications setting at the bottom of the page.
3. **Click the New button.**
   a. **To use one of the predefined Kiosk application descriptors:**
      i. **Select Predefined Descriptor.**
      ii. **Choose the relevant descriptor from the drop-down menu.**

   b. **To define a custom Kiosk application descriptor:**
      i. **Select Custom Path to use your own custom Kiosk application descriptor or a system application.**
      ii. **Enter the path to your custom Kiosk application descriptor or executable.**

      If you choose Custom Path, indicate whether the path refers to a custom Kiosk application descriptor or an executable by choosing either Descriptor or Executable.
4. **Select your preferred Start Mode for the application.**
   a. **Choose USER to allow users to start the application themselves, for instance from a menu or launcher item.**

b. **Choose AUTO to make the application start automatically when the Kiosk session starts.**

c. **Choose CRITICAL to make the application start automatically when the Kiosk session starts, to allow users to start the application themselves, and to force the Kiosk session to restart if the application terminates.**

5. **Enter any application specific arguments.**

Note – Individual Kiosk sessions may handle the various application start modes and arguments differently. For precise details on these, consult the session-specific documentation of your selected Kiosk session.

Kiosk Mode and Security

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

For example, adding an application such as `xterm` provides users with access to a command-line interface from a Kiosk Mode session. This would not be desirable in a public environment and is not advised. However, using a custom application for a call center would be perfectly acceptable.

Failover

In a failover environment, the Kiosk Mode administrative settings are copied to the failover servers. Be sure that all application descriptor and executable paths added to the Kiosk Mode sessions are copied across the servers in the failover group (FOG). For example, if the Mozilla application is added to the sessions with the executable path `/usr/sfw/bin/mozilla`, make sure that the path to the binary is available to all servers in the failover group. One way of ensuring that sessions and applications are available on all servers in a FOG is to put them into a shared network directory, which is available on all hosts in the FOG.

Kiosk Mode Session Using Sun Ray Connector for Windows OS

This product provides support for Sun Ray Connector sessions in Kiosk Mode. The core components of this product are a Kiosk Session Service session descriptor (`/etc/opt/SUNWkio/sessions/uttsc.conf`) and a Kiosk Session Service session script (`/etc/opt/SUNWkio/sessions/uttsc/uttsc`). This session does not support added applications.

Session Descriptor

The session descriptor defines a number of attributes useful for the administration and launching of the session. These include

TABLE 10-2 Kiosk Session Descriptors

Descriptor	Description
`KIOSK_SESSION_EXEC`	Identifies the location of the session script.
`KIOSK_SESSION_LABEL` `KIOSK_SESSION_DESCRIPTION`	Identify a label and description respectively to be used by the Sun Ray Admin GUI.
`KIOSK_SESSION_ARGS`	Identifies default session script arguments.

For more details, see "Session Script Arguments" on page 140.

Session Script

The session script is responsible for launching the Sun Ray Connector. The script provides a simple wrapper on the Sun Ray Connector executable, `/opt/SUNWuttsc/bin/uttsc`.

A two-minute timeout is imposed on Windows sessions that remain at the Windows login screen. When this timeout elapses, the associated Windows session is terminated, and the Sun Ray Connector terminates subsequently. This can result in a user experience where, assuming no Windows login takes place, a desktop unit appears to reset every two minutes. To avoid this, the session script supports its own timeout, which affects its behavior when it detects that the Sun Ray Connector has terminated. If the timeout interval has not elapsed, the session script relaunches the

Sun Ray Connector. If the timeout has elapsed, the session script terminates, and the Kiosk session also terminate as a result. The timeout may be specified as a session script argument. It has a default value of 30 minutes.

Session Script Arguments

A number of arguments are supported by the session script. These may be specified using the Sun Ray Admin GUI. The list of supported arguments may be split into Sun Ray Connector and non-Sun Ray Connector arguments. Sun Ray Connector arguments are not processed in any way by the session script and are simply passed directly to the Sun Ray Connector. Non-Sun Ray Connector arguments are processed by the session script itself.

The complete argument list should be formatted according to the following example:

```
[<Non Sun Ray Connector arguments>] [ "--" <Sun Ray Connector arguments>]
```

Non-Sun Ray Connector Arguments

Currently, only a single non-Sun Ray argument, `-t`, is supported. It is defined as follows:

`-t` *<timeout>* sets the value of a timeout interval (in seconds) after which the session script will terminate in the event of a Sun Ray Connector termination. If Sun Ray Connector terminates before the timeout has elapsed it will be restarted by the session script. The default value for *<timeout>* is 1800 (30 minutes). Values less than or equal to 0 indicate that the session script should never restart the Sun Ray Connector.

Sun Ray Connector Arguments

You may specify any valid `uttsc(1)` arguments here. The `-m` and `-b` `uttsc(1)` arguments are used by default. These arguments enable full-screen mode and disable the pull-down header respectively.

Note – The Sun Ray Connector requires at least a *server* argument. As previously mentioned, you may use the Sun Ray Admin GUI to include this server argument in the session script argument list.

Supplemental Information

Two features linked to Sun Ray Connector are commonly implemented at customer sites: Follow-Me-Printing and Windows Session Locking. Implementations of these features rely on technology not available by default and non-public Sun Ray interfaces as well as the use of certain public Sun Ray interfaces for purposes other their intended use. For these reasons, these features are not provided as supported elements of this session; however, descriptions of how these features are commonly implemented are provided in the following sections.

Follow-Me-Printing

This feature is used to allow the default printer for a given Windows session to appear to move with a user from one Sun Ray DTU to another. Use the following steps to provide this feature.

1. **For each Sun Ray of interest, specify an associated printer in the Sun Ray Data Store.**

   This may be done by navigating to the relevant Desktop Unit in the Sun Ray Admin GUI and setting its Other Information field to the name of the relevant printer.

2. **Provide a shell script which queries the printer name stored in the Sun Ray Data Store for the current Sun Ray DTU and writes that name to the user's** `$HOME/.printers` **file.**

   For example:

```
#!/bin/sh
if [ `uname` = Linux ] ; then
 theFlag="-P"
fi
theMACAddress=`cd $theFlag $UTDEVROOT ; pwd | sed
's/.*<............>/\1/'`
thePrinter=`/opt/SUNWut/sbin/utdesktop -o |
            grep $theMACAddress           |
            /usr/bin/awk -F, '{print $3}'`
echo "_default $thePrinter" > $HOME/.printers
```

3. **Use utaction(1) to invoke the script above on an initial connection and subsequently whenever a user moves from one Sun Ray DTU to another.**

This can be done by providing an `Xsession.d script` if you are using `dtlogin` as your login manager or an `xinitrc.d script` if you are using Gnome Display Manager (GDM) as your login manager. For example, you might create the script `/usr/dt/config/Xsession.d/1100.SUNWut` for `dtlogin` or `/etc/X11/xinit/xinitrc.d/1100.SUNWut` for GDM as follows:

```
#!/bin/sh
/opt/SUNWut/bin/utaction -i -c <path-to-script> &
```

where *<path-to-script>* is the path to the script you created to retrieve the printer name.

Note – The name `1100.SUNWut` is chosen purposely in this case to ensure that the script is run or sourced after the existing script `0100.SUNWut`. This is required as `0100.SUNWut` is responsible for setting `$UTDEVROOT` which is needed by the first sample script above.

---

4. **Modify your Kiosk session script arguments to redirect the printer to Windows.**

You may modify these arguments using the Sun Ray Admin GUI. In this example you need to add the argument `-r printer:_default` to the existing arguments, resulting in an argument list similar to the following:

```
  -t 1800 -- -m -b -r printer:_default myHost
```

where *myHost* corresponds to the server argument passed to `uttsc(1).`

Windows Session Locking

It may be preferable that a Windows session be locked when a user's session moves away from a given Sun Ray DTU. A commonly used approach to implement this is to send the lockscreen keystrokes to the Windows Session using `xvkbd` (invoked by utaction).

As with the previous example, you may invoke `utaction` from an `Xsession.d` or `xinitrc.d` script as follows:

```
#!/bin/sh
XVKBD=/usr/openwin/bin/xvkdb
/opt/SUNWut/bin/utaction  -d "$XVKBD -text '\Ml'" &
```

Note – xvkbd is not available by default, so you should modify the XVKBD setting above so that it correctly identifies the installation location of xvkbd in your case.

Note – The keystroke sequence \Ml activates the Windows lock for Windows 2003/XP sessions. You may need to modify it for other Windows versions.

CHAPTER 11

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 failover groups.

For a discussion on how to utilize multiple failover groups to utilize *regional hotdesking*, see "Hotdesking (Mobile Sessions)" on page 65.

This chapter covers these topics:

Failover Group Overview

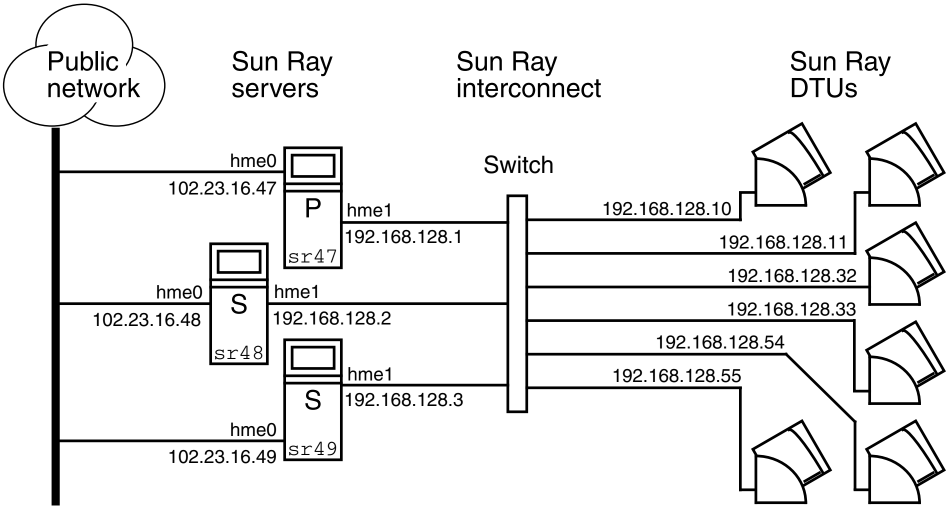
A failover group consists of two or more Sun Ray servers grouped together to provide highly-available and scalable Sun Ray service for a population of Sun Ray DTUs. Releases earlier than 2.0 supported DTUs available to the servers only on a common, dedicated interconnect. Beginning with the 2.0 release,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

Failover groups that use more than one version of Sun Ray Server Software will be unable to use all the features provided in the latest releases. On the other hand, the failover group can be a heterogeneous group of Sun servers.

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

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

FIGURE 11-1 Simple Failover Group



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

The principal components needed to implement failover are:

- Group Manager

  A module that monitors the availability (liveness) of the Sun Ray servers and facilitates redirection when needed.

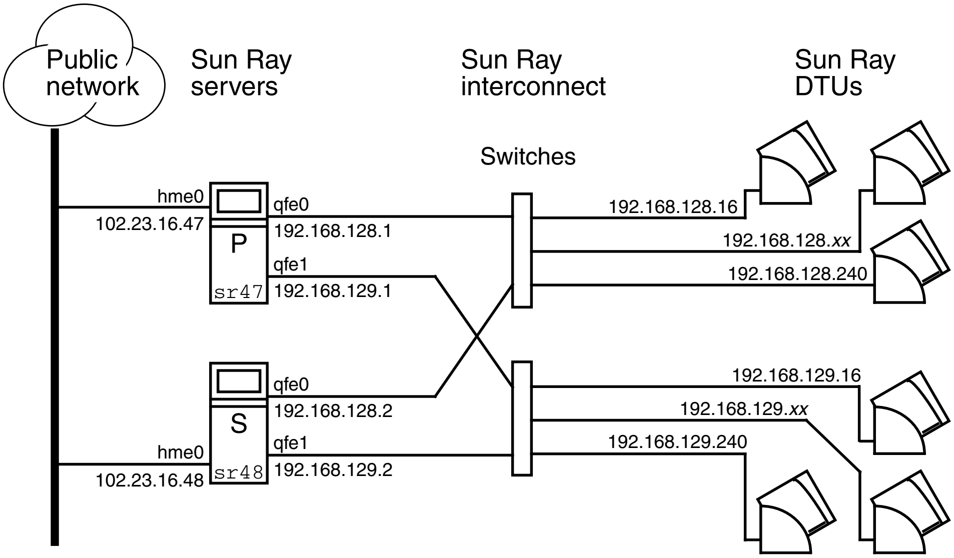
- Multiple, coexisting Dynamic Host Configuration Protocol (DHCP) servers

  All DHCP servers configured to assign IP addresses to Sun Ray DTUs have a non-overlapping subset of the available address pool.

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

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

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 DTUs. Consider the situation of five servers and 100 DTUs. If one of the servers fails, the remaining DHCP servers must have enough available addresses so that every “orphaned” DTUs gets a new working address.

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

TABLE 11-1 Configuring Five Servers for 100 DTUs

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

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

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

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

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

Server Addresses

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

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

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

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

Note – For the broadcast feature to be enabled, the broadcast address (255.255.255.255) must be the last one in the list. Any addresses after the broadcast address are ignored. If the local server is not on the list, Sun Ray DTUs cannot attempt to contact it.

Once a TCP connection to an Authentication Manager has been established, the DTU presents its token. The token is either a pseudo-token representing the individual DTU (its unique Ethernet address) or a smart card. The Session Manager then starts an X window/X server session and binds the token to that session.

The Authentication Manager then sends a query to all the other Authentication Managers on the same subnet and asks for information about existing sessions for the token. The other Authentication Managers respond, indicating whether there is a session for the token and the last time the token was connected to the session.

The requesting Authentication Manager selects the server with the latest connection time and redirects the DTU to that server. If no session is found for the token, the requesting Authentication Manager selects the server with the lightest load and redirects the token to that server. A new session is created for the token.

The Authentication Manager enables both implicit (smart card) and explicit switching. For explicit switching, see “Group Manager” on page 154.

Configuring DHCP

In a large IP network, a DHCP server distributes the IP addresses and other configuration information for interfaces on that network.

Coexistence of the Sun Ray Server With Other DHCP Servers

The Sun Ray DHCP server can coexist with DHCP servers on other subnets, provided you isolate the Sun Ray DHCP server from other DHCP traffic. Verify that all routers on the network are configured not to relay DHCP requests. This is the default behavior for most routers.

Caution – If the IP addresses and DHCP configuration data are not set up correctly when the interfaces are configured, the failover feature cannot work properly. In particular, configuring the Sun Ray server's interconnect IP address as a duplicate of any other server's interconnect IP address may cause the Sun Ray Authentication Manager to throw "Out of Memory" errors.

Administering Other Clients

If the Sun Ray server has multiple interfaces, one of which is the Sun Ray interconnect, the Sun Ray DHCP server should be able to manage both the Sun Ray interconnect and the other interfaces without cross-interference.

▼ To Set Up IP Addressing on Multiple Servers Each With One Sun Ray Interface

1. **Log in to the Sun Ray server as superuser and, open a shell window. Type:**

```
# /opt/SUNWut/sbin/utadm -a <interface_name>
```

   where <*interface_name*> is the name of the Sun Ray network interface to be configured; for example, `hme[0-9]`, `qfe[0-9]`, or `ge[0-9]`. You must be logged on as superuser to run this command. The `utadm` script configures the interface (for example, `hme1`) at the subnet (in this example, 128).

The script displays default values, such as the following:

```
Selected values for interface "hme1"
    host address:       192.168.128.1
    net mask:           255.255.255.0
    net address:        192.168.128.0
    host name:          serverB-hme1
    net name:           SunRay-hme1
    first unit address: 192.168.128.16
    last unit address:  192.168.128.240
    auth server list:   192.168.128.1
    firmware server:    192.168.128.1
    router:             192.168.128.1
```

The default values are the same for each server in a failover group. Certain values must be changed to be unique to each server.

2. **When you are asked to accept the default values, type** `n`**:**

```
Accept as is? ([Y]/N): n
```

3. **Change the second server's IP address to a unique value, in this case 192.168.128.2:**

```
new host address: [192.168.128.1] 192.168.128.2
```

4. **Accept the default values for netmask, host name, and net name:**

```
new netmask: [255.255.255.0]
new host name: [serverB-hme1]
```

5. **Change the DTU address ranges for the interconnect to unique values. For example:**

```
Do you want to offer IP addresses for this interface? [Y/N]:
new first Sun Ray address: [192.168.128.16] 192.168.128.50
number of Sun Ray addresses to allocate: [205] 34
```

6. **Accept the default firmware server and router values:**

```
new firmware server: [192.168.128.2]
new router: [192.168.128.2]
```

The utadm script asks if you want to specify an authentication server list:

```
auth server list:     192.168.128.1
To read auth server list from file, enter file name:
Auth server IP address (enter <CR> to end list):
If no server in the auth server list responds, should an auth
server be located by broadcasting on the network? ([Y]/N):
```

These servers are specified by a file containing a space-delimited list of server IP addresses or by manually entering the server IP addresses.

The newly selected values for interface hme1 are displayed:

```
Selected values for interface "hme1"
    host address:       192.168.128.2
    net mask:           255.255.255.0
    net address:        192.168.128.0
    host name:          serverB-hme1
    net name:           SunRay-hme1
    first unit address: 192.168.128.50
    last unit address:  192.168.128.83
    auth server list:   192.168.128.1
    firmware server:    192.168.128.2
    router:             192.168.128.2
```

7. **If these are correct, accept the new values:**

```
Accept as is? ([Y]/N): y
```

8. **Stop and restart the server and power cycle the DTUs to download the firmware.**

TABLE 11-2 lists the options available for the `utadm` command. For additional information, see the `utadm` man page.

TABLE 11-2 Available Options

Option	Definition
-c	Create a framework for the Sun Ray interconnect.
-r	Remove all Sun Ray interconnects.
-A <*subnetwork*>	Configure the subnetwork specified as a Sun Ray sub-network. This option only configures the DHCP service to allocate IP address and/or to provide Sun Ray parameters to Sun Ray clients. It also will automatically turn on support for LAN connections from a shared subnetwork.
-a <*interface_name*>	Add <*interface_name*> as Sun Ray interconnect.
-D <*subnetwork*>	Delete the subnetwork specified form the list of configured Sun Ray subnetworks.
-d <*interface_name*>	Delete <*interface_name*> as Sun Ray interconnect.
-l	Print the current configuration for all the Sun Ray subnetworks, including remote subnetworks.
-p	Print the current configuration.
-f	Take a server offline
-n	Bring a server online
-x	Print the current configuration in a machine-readable format

Group Manager

Every server has a group manager module that monitors availability and facilitates redirection. It is coupled with the Authentication Manager.

In setting policies, the Authentication Manager uses the selected authentication modules and decides what tokens are valid and which users have access.

Warning – The same policy must exist on every server in the failover group or undesirable results might occur.

The Group Managers create maps of the failover group topology by exchanging `keepalive` messages among themselves. These `keepalive` messages are sent to a well-known UDP port (typically 7009) on all of the configured network interfaces.

The keepalive message contains enough information for each Sun Ray server to construct a list of servers and the common subnets that each server can access. In addition, the Group Manager remembers the last time that a keepalive message was received from each server on each interface.

The keepalive message contains the following information about the server:

- Server's host name
- Server's primary IP address
- Elapsed time since it was booted
- IP information for every interface it can reach
- Machine information (number and speed of CPUs, configured RAM, and so on)
- Load information (CPU and memory utilization, number of sessions, and so on)

Note – The last two items are used to facilitate load distribution. See "Load Balancing" on page 156.

The information maintained by the Group Manager is used primarily for server selection when a token is presented. The server and subnet information is used to determine the servers to which a given DTU can connect. These servers are queried about sessions belonging to the token. Servers whose last keepalive message is older than the timeout are deleted from the list, since either the network connection or the server is probably down.

Redirection

In addition to automatic redirection at authentication, you can use the utselect or utswitch command for manual redirection.

Note – The utselect GUI is the preferred method to use for server selection. For more information, see the utselect man page.

Group Manager Configuration

The Authentication Manager configuration file, /etc/opt/SUNWut/auth.props, contains properties used by the Group Manager at runtime. The properties are:

- gmport
- gmKeepAliveInterval
- enableGroupManager

- enableLoadBalancing
- enableMulticast
- multicastTTL
- gmSignatureFile
- gmDebug

Note – These properties have default values that are rarely changed. Only very knowledgeable Sun support personnel should direct customers to change these values to help tune or debug their systems. If any properties are changed, they must be changed for all servers in the failover group, since the `auth.props` file must be the same on all servers in a failover group.

▼ To Restart the Authentication Manager

Property changes do not take effect until the Authentication Manager is restarted.

- **As superuser, open a shell window and type:**

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

The Authentication Manager is restarted.

Load Balancing

At the time of a server failure, the Group Manager on each remaining server attempts to distribute the failed server's sessions evenly among the remaining servers. The load balancing algorithm takes into account each server's capacity (number and speed of its CPUs) and load so that larger or less heavily loaded servers host more sessions.

When the Group Manager receives a token from a Sun Ray DTU and finds that no server owns an existing session for that token, it redirects the Sun Ray DTU to whichever server in the group has the lightest load. A Sun Ray DTU may appear to connect twice, once on the server that answered its DHCP request and a second time on a server that was less loaded than the first.

▼ To Turn Off the Load Balancing Feature

- **In the `auth.props` file set:**

```
enableLoadBalancing = false
```

Setting Up a Failover Group

A failover group is one in which two or more Sun Ray servers use a common policy and share services. It is composed of a primary server and one or more secondary servers. For such a group, you must configure a Sun Ray Data Store to enable replication of the Sun Ray administration data across the group. Configure the secondary servers so that they serve users directly in addition to serving the Data Store. For best results in groups of four or more servers, configure the primary server so that it serves only the Sun Ray Data Store.

The `utconfig` command sets up the data store for a single system initially, and enables the Sun Ray servers for failover. The `utreplica` command then configures the Sun Ray servers as a failover group.

Log files for Sun Ray servers contain time-stamped error messages which are difficult to interpret if the time is out of sync. To make troubleshooting easier, all secondary servers should periodically synchronize with their primary server.

Tip – Use `rdate` <*primary-host*>, preferably with `crontab`, to synchronize secondary servers with their primary server.

Primary Server

Layered administration of the group takes place on the primary server. 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.

Adding or removing secondary servers requires services to be restarted on the primary server. In large failover groups, and significant loads may be pushed onto the primary server from various sources. In addition, runaway processes from user applications on the primary can degrade the health of the entire failover group.

Failover groups of more than four servers should have a dedicated primary server devoted to solely serving the Sun Ray Data Store, i.e., not hosting any Sun Ray sessions.

Tip – Configure the primary server before you configure the secondary servers.

▼ To Specify a Primary Server

- **As a superuser, open a shell window on the primary server and type:**

```
# /opt/SUNWut/sbin/utreplica -p secondary-server1 [secondary-server2 ...]
```

where *secondary_server1 [secondary_server2...]* is a space-separated list of unique host names of the secondary servers.

▼ To Specify a Dedicated Primary Server

The purpose of a dedicated primary server is to serve the Sun Ray Data Store.

- **Follow the procedure to specify a primary server, as above; however, do not run** `utadm` **on this server.**

Secondary Server

The secondary servers in the group store a replicated version of the primary server's administration data. Use the `utreplica` command to advise each secondary server of its secondary status and also the host name of the primary server for the group.

▼ To Specify Each Secondary Server

- **As superuser, open a shell window on the secondary server and type:**

```
# /opt/SUNWut/sbin/utreplica -s primary-server
```

where *primary-server* is the hostname of the primary server.

▼ To Add Additional Secondary Servers

To include an additional secondary server in an already configured failover group:

1. **On the primary server, rerun** `utreplica -p -a` **with a list of 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).

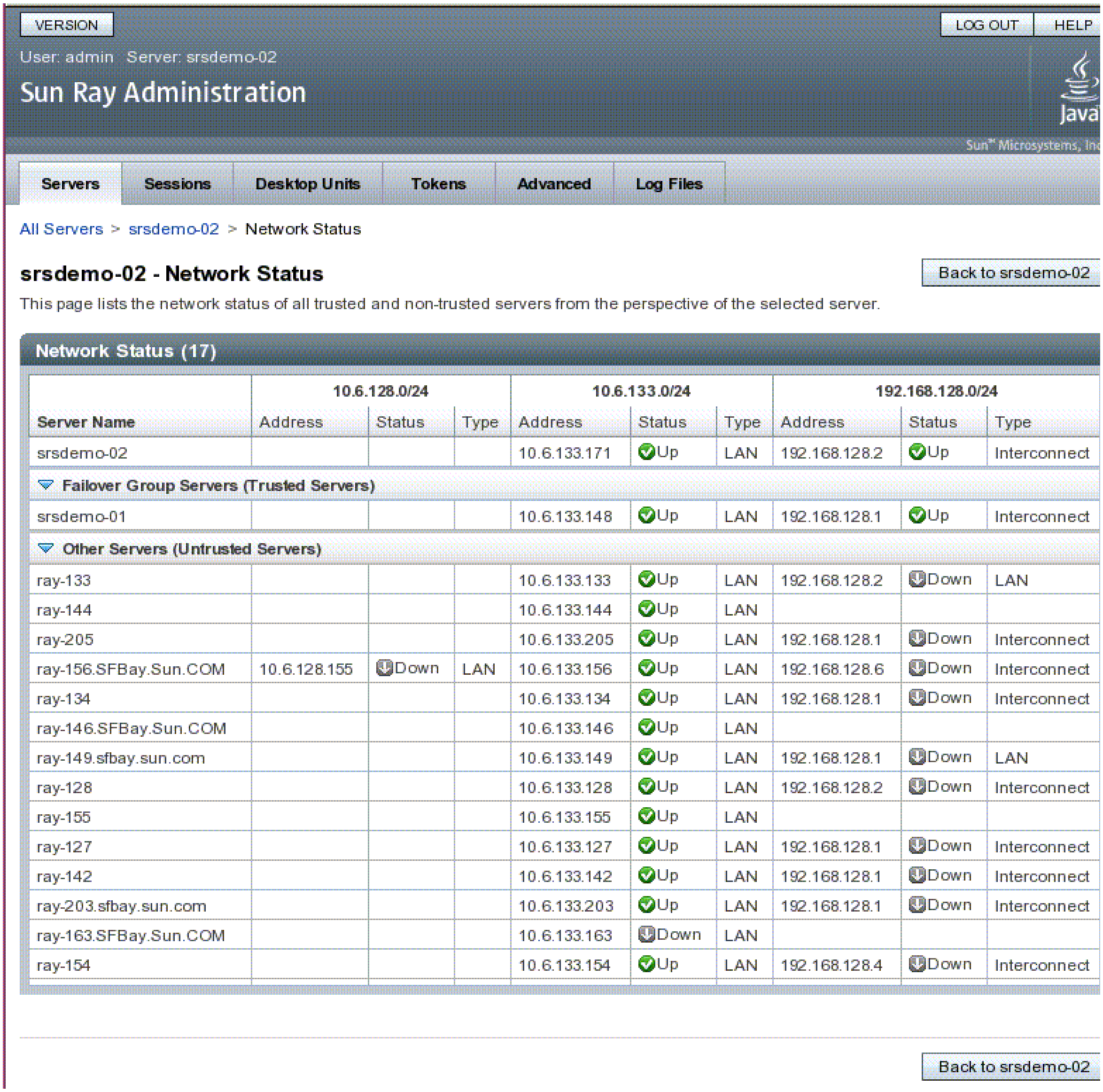
Viewing Network (Failover Group) Status

A failover group is a set of Sun Ray servers all running the same release of Sun Ray Server Software and all having access to all the Sun Ray DTUs on the interconnect.

▼ To View Failover Group Status

1. **From the Servers tab in the Admin GUI, click on a server name to display its Server Details screen.**
2. **Click View Network Status.**

FIGURE 11-3 Network Status Screen



User: admin Server: srsdemo-02

Sun Ray Administration

All Servers > srsdemo-02 > Network Status

srsdemo-02 - Network Status

This page lists the network status of all trusted and non-trusted servers from the perspective of the selected server.

Network Status (17)

	10.6.128.0/24			10.6.133.0/24			192.168.128.0/24		
Server Name	Address	Status	Type	Address	Status	Type	Address	Status	Type
srsdemo-02				10.6.133.171	✓Up	LAN	192.168.128.2	✓Up	Interconnect
Failover Group Servers (Trusted Servers)									
srsdemo-01				10.6.133.148	✓Up	LAN	192.168.128.1	✓Up	Interconnect
Other Servers (Untrusted Servers)									
ray-133				10.6.133.133	✓Up	LAN	192.168.128.2	Down	LAN
ray-144				10.6.133.144	✓Up	LAN			
ray-205				10.6.133.205	✓Up	LAN	192.168.128.1	Down	Interconnect
ray-156.SFBay.Sun.COM	10.6.128.155	Down	LAN	10.6.133.156	✓Up	LAN	192.168.128.6	Down	Interconnect
ray-134				10.6.133.134	✓Up	LAN	192.168.128.1	Down	Interconnect
ray-146.SFBay.Sun.COM				10.6.133.146	✓Up	LAN			
ray-149.sfbay.sun.com				10.6.133.149	✓Up	LAN	192.168.128.1	Down	LAN
ray-128				10.6.133.128	✓Up	LAN	192.168.128.2	Down	Interconnect
ray-155				10.6.133.155	✓Up	LAN			
ray-127				10.6.133.127	✓Up	LAN	192.168.128.1	Down	Interconnect
ray-142				10.6.133.142	✓Up	LAN	192.168.128.1	Down	Interconnect
ray-203.sfbay.sun.com				10.6.133.203	✓Up	LAN	192.168.128.1	Down	Interconnect
ray-163.SFBay.Sun.COM				10.6.133.163	Down	LAN			
ray-154				10.6.133.154	✓Up	LAN	192.168.128.4	Down	Interconnect

The Network Status screen provides information on group membership and network connectivity for servers in the same failover group and for any other Sun Ray servers that have responded to a Sun Ray broadcast. The servers are listed by name in the first column. Failover Group Status only displays public networks and Sun Ray interconnect fabrics.

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

Recovery Issues and Procedures

If one of the servers of a failover group fails, the remaining group members operate from the administration data that existed prior to the failure.

The recovery procedure depends on the severity of the failure and whether a primary or secondary server has failed.

Note – When the primary server fails, you cannot make administrative changes to the system. For replication to work, all changes 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

Use this procedure to rebuild the primary server data store from a secondary server. This procedure uses the same hostname for the replacement server.

1. **On one of the secondary servers, capture the current data store to a file called** `/tmp/store`**:**

```
# /opt/SUNWut/srds/lib/utldbmcat \
/var/opt/SUNWut/srds/dbm.ut/id2entry.dbb > /tmp/store
```

   This provides an LDIF format file of the current data store.

2. **FTP this file to the** `/tmp` **directory on the primary server.**

3. **Follow the directions in the *Sun Ray Server Software 4.0 Installation and Configuration Guide* to install Sun Ray Server Software.**

4. **After running** `utinstall`**, configure the server as a primary server for the group. Make sure that you use the same admin password and group signature.**

```
# utconfig
  :
# utreplica -p <secondary-server1> <secondary-server2> ...
```

5. **Shut down the Sun Ray services, including the data store:**

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

6. **Restore the data:**

```
# /opt/SUNWut/srds/lib/utldif2ldbm -c -j 10 -i /tmp/store
```

   This populates the primary server and synchronizes its data with the secondary server. The replacement server is now ready for operation as the primary server.

7. **Restart Sun Ray services:**

```
# utrestart -c
```

8. **(Optional) Confirm that the data store is repopulated:**

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

9. **(Optional) Perform any additional configuration procedures.**

▼ To Replace the Primary Server with a Secondary Server

Note – This procedure is also known as promoting a secondary server to primary.

---

1. **Choose a server in the existing failover group to be promoted and configure it as the primary server:**

```
# utreplica -u
# utreplica -p <secondary-server1> <secondary-server2> ...
```

2. **Reconfigure each of the remaining secondary servers in the failover group to use the new primary server.:**

```
# utreplica -u
# utreplica -s <new-primary-server>
```

This resynchronizes the secondary server with the new primary server.

Note – This process may take some time to complete, depending on the size of the data store. Since Sun Ray services will be offline during this procedure, you may want to schedule your secondary servers' downtime accordingly. Be sure to perform this procedure on each secondary server in the failover group.

Secondary Server Recovery

Where a secondary server has failed, administration of the group can continue. A log of updates is maintained and applied automatically to the secondary server when it has recovered. If the secondary server needs to be reinstalled, repeat the steps described in the *Sun Ray Server Software 4.0 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 proper internal replication.

Taking Servers Offline

Being able to take servers offline makes maintenance easier. In an offline state, no new sessions are created. However, old sessions continue to exist and can be reactivated unless Sun Ray Server Software is affected.

▼ To Take a Server Offline

- **At the command-line interface, type:**

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

▼ To Bring a Server Online

- **At the command-line interface, type:**

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

APPENDIX **A**

User Settings

This appendix covers topics that users as well as administrators may find useful. There are sections for:

- "Supported Devices and Libraries" on page 167
- "Sun Ray DTU Settings" on page 168
- "Monitor Settings" on page 169
- "Hot Key Preferences" on page 170
- "Hot Key Values" on page 171
- "Power Cycling a Sun Ray DTU" on page 172

Supported Devices and Libraries

Sun Ray Server Software supports a wide variety of end-user devices, including mass storage and end-user peripherals that can be connected to a Sun Ray DTU's serial, parallel, or USB ports; however, because of the growing number of USB devices available, it has not been possible to test all of them on Sun Ray DTUs.

Supported Mass Storage Devices

Sun Ray Server Software 4.0 supports the use of flash disks, memory card readers, Zip drives, and hard drives on Sun Ray DTUs. It allows data CDs and DVDs to be read but not written. It does *not* support floppy drives.

For troubleshooting tips, please see "Troubleshooting USB Mass Storage Devices" on page 197.

Note – Most devices claiming USB 2.0 compliance are backwards compatible and should work with Sun Ray Mass Storage.

Sun Ray DTU Settings

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

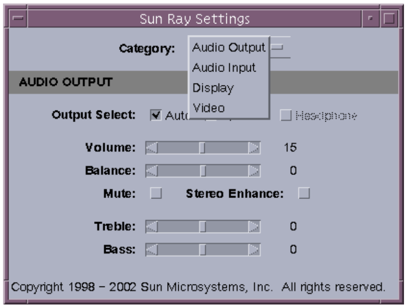
The Sun Ray Settings GUI contacts the Session Manager to determine which DTU is currently being used and connects to that unit to get the current values. The GUI maintains a connection to the Session Manager so that the Session Manager can notify the GUI if the user moves to another DTU by removing the smart card and inserting it into another DTU.

▼ To Change the Sun Ray Settings

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

   The Sun Ray Settings window is displayed.

FIGURE A-1 Settings Screen



Sun Ray Settings

Category: Audio Output

AUDIO OUTPUT

Output Select: ☑ Auto □ Headphone

Volume: 15

Balance: 0

Mute: □ Stereo Enhance: □

Treble: 0

Bass: 0

Copyright 1998 – 2002 Sun Microsystems, Inc. All rights reserved.

2. **Use the Category pull-down menu to access Audio Output, Audio Input, Display, and Video settings.**

3. **To change a setting, move the appropriate scroll bar, checkbox, or pull-down menu.**

   The DTU is updated immediately.

   The only exception is the "Resolution/Refresh Rate" setting, which prompts the user with confirmation dialog boxes before and after the change is made on the DTU.

4. **Press the hot key to close the window.**

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

Monitor Settings

Sun Ray users can modify their screen resolution settings by invoking `utsettings`.

Any resolution selection made within a session remains effective whenever the session is displayed on that particular DTU. The selection is not lost if the unit goes into power-save mode or is power-cycled; however, the resolution settings selected through `utsettings` apply *only* to the DTU where `utsettings` is run.

When a user moves to another DTU, the resolution settings do not accompany the user to the new DTU, but the settings remain effective for the user's session on the original DTU if the returns to it via hotdesking.

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

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

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

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

For further details, see the utsettings and utresadm man pages.

Hot Key Preferences

Hot keys can be configured for various Sun Ray utilities. The scope for these hot keys can be:

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

To support these levels of customization, the utilities look for the properties files in TABLE A-1, in the following order, at startup:

TABLE A-1 Sun Ray Settings Properties Files

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

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

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

```
<utility_name>.hotkey=value
```

where <*utility_name*> is the name of the utility, such as `utsettings` or `utdetach`, and *value* is a valid X keysym name preceded by one or more of the supported modifiers (`Ctrl`, `Shift`, `Alt`, `Meta`) in any order. Values are shown in TABLE A-2.

TABLE A-2 Specific Hot Key Values

Example Value	Notes
`Shift+Props`	Invoke the Settings GUI.
`Stop+S`	Invoke the Pop-up GUI
`Ctrl+Alt+Backspace`	Press this key sequence twice to kill a session.
`Ctrl+Alt+Del`	Press this key sequence twice to kill the process that has taken control of the X server.
`Mute+Softer+Louder`	Display the DTU’s MAC address.
`Ctrl+Power`	Power cycle the DTU.

Hot Key Values

▼ To Change the Hot Key for the Settings GUI

If you do not want to use `Shift  Props` as your default hot key, use the system-wide defaults file to specify a function key. Users can still specify their preferences in the user defaults file.

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

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

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

---

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

   The `#` comments out the first hot key property.

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

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

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

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

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

▼ To Change the Hot Key Setting for a Single User

1. **In the user's home directory, create the** `.utslaunch.properties` **file.**

Note – Make sure that the user owns and can read this file.

2. **Add a line to the** `.utslaunch.properties` **file with the value for the hot key. For example:**

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

3. **Save the** `.utslaunch.properties` **file.**

4. **Log out and log back in to enable the new hot key.**

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

Power Cycling a Sun Ray DTU

▼ To Power Cycle a Sun Ray DTU

- **Disconnect then reconnect the power cord.**

▼ To Perform a Soft Reset

- **Use the key sequence** `Ctrl-Power`**. The Power key at the right side of the top row of a Sun Type 6 or Type 7 keyboard has a crescent moon icon; the soft reset key sequence is often called** `Ctrl-Moon`**.**

▼ To Kill a User's Session

- **Use the key sequence** `Ctrl-Alt-Backspace` **twice.**

  This kills the Xserver process, alerting the current session's parent process to start another session.

APPENDIX **B**

Troubleshooting and Tuning Tips

This appendix contains the following sections:

Note – For the latest information regarding Sun Ray Server Software patches, check: `http://www.sun.com/software/sunray/patches.xml`

Understanding OSD

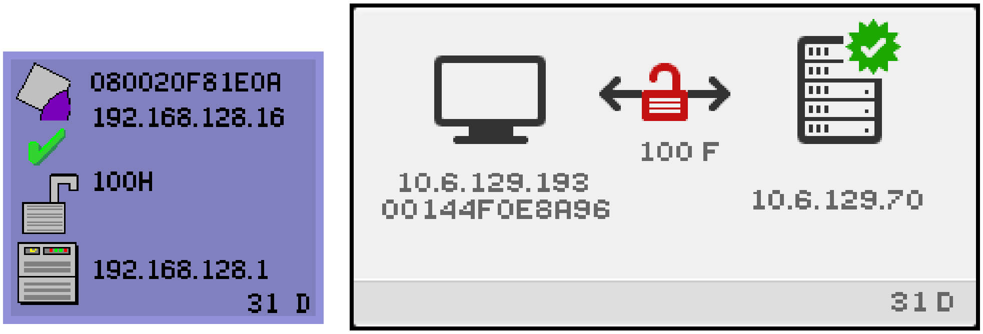
Sun Ray Server Software on-screen displays (OSD) to help administrators and others identify problems visually. The most important information about the Sun Ray DTU and its current state is displayed on the screen.

OSD Icon Topography

The original OSD supplied with earlier versions of Sun Ray Server Software and DTU firmware have now been replaced with larger icons that provide the same information in an easier to read format. It is always a good idea to make sure that you are using the latest firmware. See "Managing Firmware Versions" on page 30.

Both sets of OSD icons are composited live, based on the current state of connectivity at a given moment. Examples of the original OSD are shown at left in the figures below, with equivalent or similar examples of the newer OSD at the right.

FIGURE B-1 Layout of Old (left) and New (right) OSD Icons



The OSD icons display:

- Ethernet address
- Currently assigned IP address of the DTU
- Link status of the currently connected Sun Ray server
- Authentication Server IP address
- Icon code and DHCP state

To help you locate problems, the OSD icons display a numeric icon code followed by an alphabetic DHCP state code. You can look up the meaning of the numeric OSD message codes in TABLE B-1 and the alphabetic DHCP state codes in TABLE B-2, and firmware download error codes in TABLE B-4. Encryption and authentication information is also displayed when appropriate.

Sun Ray DTUs can function in a private interconnect or in a simple LAN environment with only an IP address, but additional basic parameters and Sun Ray-specific vendor options are needed for more complex LAN operations, such as when a DTU is located several hops away from the Sun Ray Server's subnet.

OSD icon messages and codes are summarized in the following tables:

TABLE B-1 Icon Messages

Icon Code	Meaning
1	Sun Ray DTU is starting up and is waiting for ethernet link
2	Sun Ray DTU is downloading new firmware
3	Sun Ray DTU is storing new firmware in its flash memory

TABLE B-1 Icon Messages

Icon Code	Meaning
4	Either the download or storage of new firmware has failed
5	There is no session to connect with the Sun Ray
6	The server is denying access to the Sun Ray
7	Local pin entry to the smart card has failed
8	In local smart card pin entry mode
9	There is an over current condition on the USB bus, i.e., the total number of devices draws too much current. Consider using a powered hub.
11	Server is authenticated by the Sun Ray DTU and the graphic/keyboard network connection is encrypted
12	The Sun Ray DTU cannot authenticate the server but the graphic/keyboard network connection is still being encrypted
13	Server authenticated to the Sun Ray; network connection between Sun Ray and server not encrypted
14	Server not authenticated to the Sun Ray; graphic/keyboard network connection is not encrypted
15	the Sun Ray DTU is refusing to talk to the server due to the server's refusal or inability to authenticate or encrypt the network connection
16	The Sun Ray USB bus is temporarily busy servicing a high-speed device, and the keyboard or mouse may not be responsive to user input.
21	The Sun Ray DTU is booting up and is waiting on DHCP IP address and parameter assignment.
22	The Sun Ray DTU is booting up and is now waiting for the initial connection to a Sun Ray server.
23	The connection between the Sun Ray DTU and the network is down. Check the network drop cable and (if the network drop cable is okay) the network switch.
24	The Sun Ray DTU has disconnected from the previous server.
25	The Sun Ray DTU is being redirected to a new server.
26	The Sun Ray DTU has connected to the server and is waiting for graphics traffic.
27	The Sun Ray DTU is broadcasting to locate a Sun Ray server since either it was not provided with Sun Ray specific DHCP parameters or all of the specified servers are not responding.
28	VPN connection being attempted
29	VPN connection established
30	VPN connection error
	Icons 31 through 34 display network status when the three audio keys are pressed simultaneously.
31	The network link is up, the server is authenticated, and graphics/keyboard network connections are not encrypted.
32	The network link is up, the server is not authenticated, and graphics/keyboard network connections are encrypted.

TABLE B-1 Icon Messages

Icon Code	Meaning
33	The network link is up, the server is authenticated and graphics/keyboard are encrypted.
34	The network link is up, the server is not authenticated and graphics/keyboard are not encrypted.
50	The server is refusing to talk to the Sun Ray DTU due to the Sun Ray's refusal or inability to authenticate or encrypt the network connection

TABLE B-2 DCHP State Codes

DCHP State Code	Meaning
A	DCHP only provided IP address with no additional parameters.
B	DCHP provided IP address, subnet mask, and router, but Sun Ray vendor-specific parameters are missing.
C	DHCP provided IP address and Sun Ray vendor-specific parameters, but subnet mask and router are missing.
D	DHCP provided all expected parameters.
	Codes E, F, H, and I are valid only with OSD icon 28
E	VPN Phase 1 IKE initiated.
F	VPN Phase 1 IKE complete.
H	VPN Phase 2 initiated.
I	VPN Phase 2 complete.

TABLE B-3 Power LED

DTU Hardware State	Action to Take
Off	Check to see if the DTU is plugged in. Replace the DTU.
Amber	Hardware fault. Replace the DTU.
Blinking	PROM is corrupted. Check that firmware downloads are properly configured and enabled, then power cycle the DTU.
Card reader LED remains on even when smart card is removed	Card reader hardware problem. Replace the DTU.

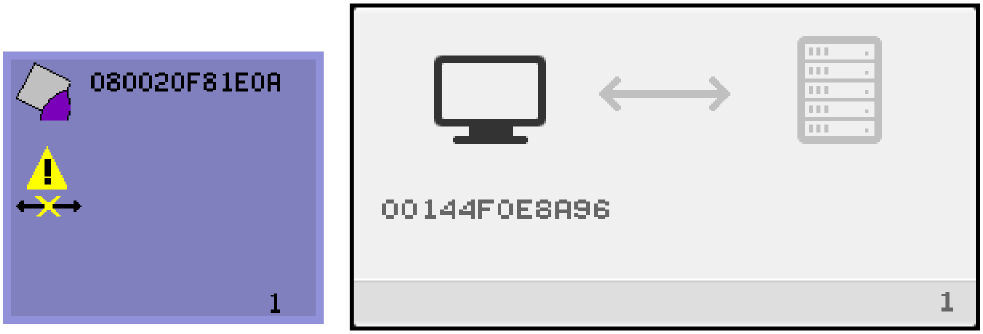
TABLE B-4 Firmware Download Error Codes and Messages

Error Code	Error Message
E	FW Load: No server
F	FW Load: Name too long
G	FW Load: Bad read
H	FW Load: Bad signature
I	FW Load: Failed decompression
J	FW Load: Invalid module type
K	FW Load: Version mismatch
L	FW Load: Not enough memory
M	FW Load: Prevented by barrier
N	FW Load: Invalid HW version
O	FW Load: Flash write error

Sun Ray Desktop Unit Startup

The first display a user should see is depicted below:

FIGURE B-2 DTU Startup OSD



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

▼ If this icon stays on for more than 10 seconds

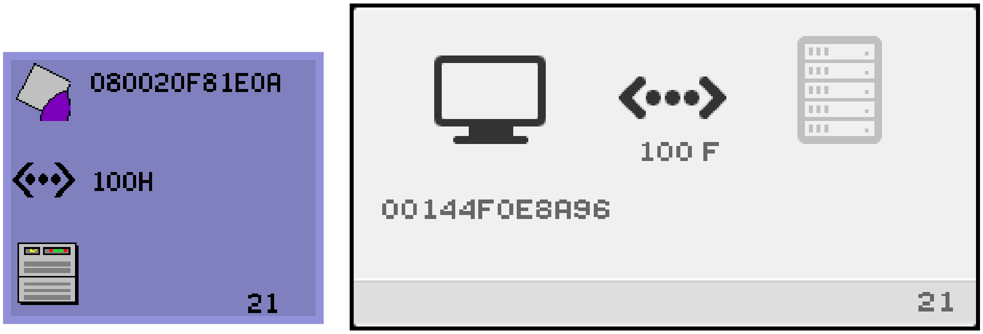
1. **Check that the Ethernet cable is correctly plugged into the DTU and the other end is plugged in to the correct hub, switch, or network outlet.**

A link light on the switch or hub indicates that the connection is alive.

2. **If the DTU is connected through a hub or a switch, make sure that the hub or switch is powered on and configured correctly.**

After the Sun Ray DTU has verified its network connection, the user should see this OSD:

FIGURE B-3 Network Connection Verified



This icon indicates that the DTU has detected the Ethernet carrier but has not yet received its initial parameters or IP address from DHCP. This icon is displayed as part of the normal startup phase and is usually displayed for only a few seconds.

▼ If this icon stays on for more than 10 seconds

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

2. **Verify that your DHCP server is configured properly for network parameters.**

After the DHCP server has allocated an IP address, the icon is updated with the unit's IP address; if the response is inadequate, the Sun Ray DTU issues a `DHCP inform` request to attempt to obtain the Sun Ray vendor-specific parameters. The Sun Ray DTU continues all the way through booting with just a DHCP supplied IP address but usually functions better with some additional parameters.

At this point, depending on whether you have configured your Sun Ray servers to run on a LAN or a dedicated interconnect, OSD 21A or 21B may display.

Code 21 A indicates that the DTU got an IP address and is waiting for a `DHCP inform` response to other parameters.

Code 21 B indicates that the DTU got an IP address and IP router and is waiting for Sun Ray vendor-specific options from `DHCP inform`.

Note – If you see a 21 A or 21 B with a DTU IP address in a LAN deployment, the Sun Ray DTU is trying to use `DHCP_INFORM` to get Sun Ray-specific parameters.

▼ Actions to Take

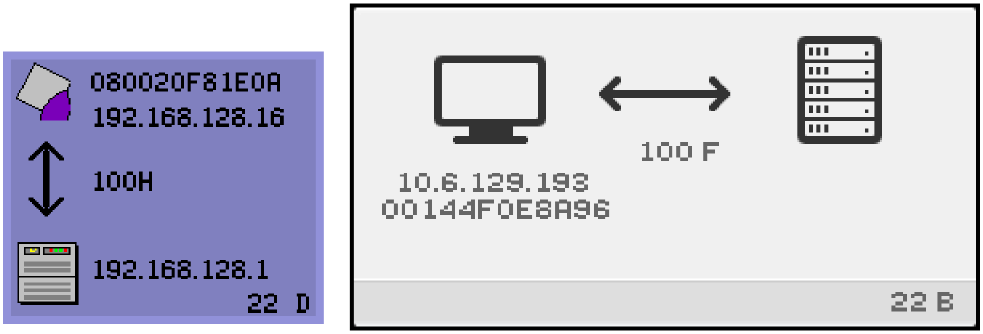
1. **For LAN configurations with other (non-Sun Ray) DHCP services but no `bootp` proxy agent, verify the DHCP server and the Sun Ray vendor tags.**

2. **For routed configurations, verify that the `bootp` proxy agent is configured correctly in the Sun Ray DTU's subnet and that it points to one of the Sun Ray servers in the failover group.**

3. **For non-routed private interconnect configurations, the Sun Ray server also performs the functions of a DHCP server. Verify that it is configured properly for DHCP services.**

When DHCP finishes, the Sun Ray DTU tries to connect to a Sun Ray server and the Authentication Manager running on it.

FIGURE B-4 Waiting to Connect to Authentication Manager



This icon indicates that the DTU has received its initial parameters from DHCP but has not yet connected to the Sun Ray Authentication Manager. This icon is displayed as part of the normal startup phase and is usually displayed for only a few seconds.

▼ If the icon displays for more than a few seconds or if the DTU continues to reset after the icon is displayed

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

In a LAN configuration or other routed environment:

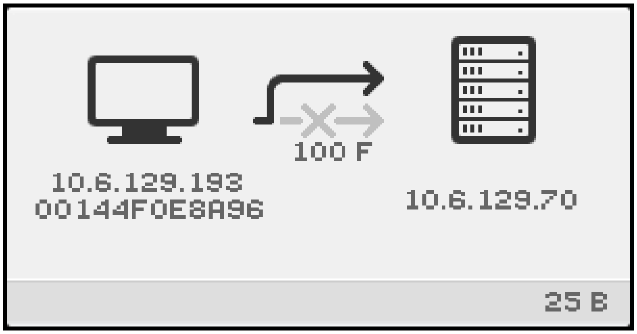
2. **Make sure that the Authentication Manager can be reached from the IP address assigned to the DTU.**

3. **Verify that the routing information the DTU receives is correct.**

4. **Run `utquery` for the DTU's IP address.**

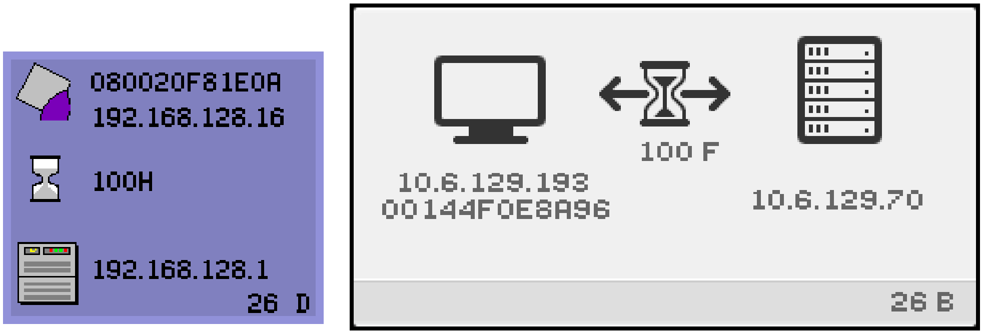
The `utquery` command displays the parameters a Sun Ray DTU has received. If `utquery` fails to display an *AuthSrvr* parameter, the DHCP server for Sun Ray parameters may not be reachable or may not be configured properly. Confirm that the *DHCPServer* and *INFORMServer* values are appropriate. If not, look at your `bootp` relay configurations and DHCP server configurations for network and Sun Ray parameters. For details of these parameters, see the `utquery` man page.

FIGURE B-5 Redirection OSD



This OSD indicated that the DTU is being redirected to a new server. This can occur for any of several reasons, including load balancing.

FIGURE B-6 Wait for Session OSD



This OSD represents the transition state for the Sun Ray DTU. If it is displayed for an extended period, there is probably no X Window server running.

Note – The current wait icon is a white "X" cursor. In earlier releases, the wait icon was displayed as a green newt cursor.

To Identify a Hung Session

- **As superuser, type:**

```
# /opt/SUNWut/sbin/utdesktop -l -w
```

To Kill a Hung Session

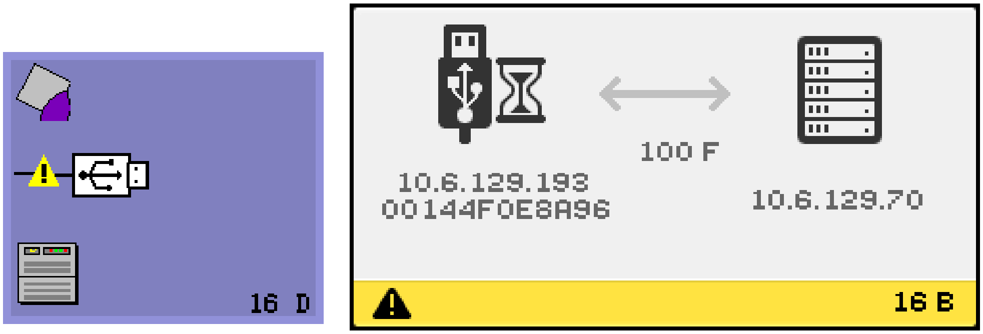
- **As superuser, type:**

```
# /opt/SUNWut/sbin/utsession -k -t token
```

Actions to Take

1. **Check the messages file** `/var/opt/SUNWut/log/messages` **to verify the version number.**
2. **Correct, if necessary, with** `utadm -l`**.**

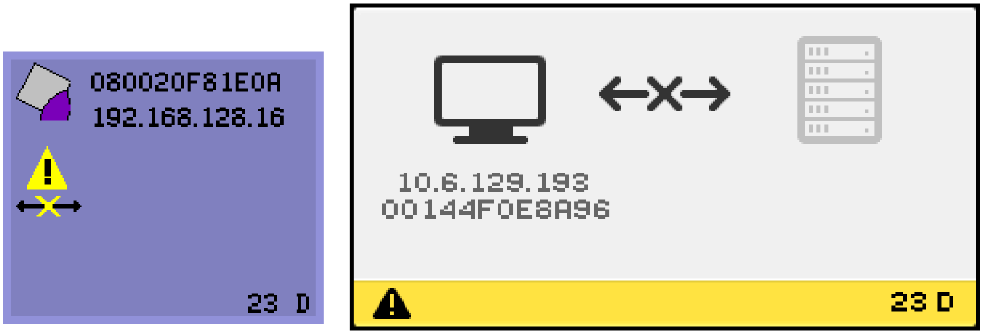
FIGURE B-7 Bus Busy



This icon indicates that the Sun Ray USB bus is temporarily busy servicing a high-speed device, and the keyboard or mouse may not be responsive to user input.

This icon typically appears only during an unusually long print job and disappears when the job is done. This is an informational OSD; there is no particular action to take unless it is necessary to kill the print job.

FIGURE B-8 No Ethernet Signal



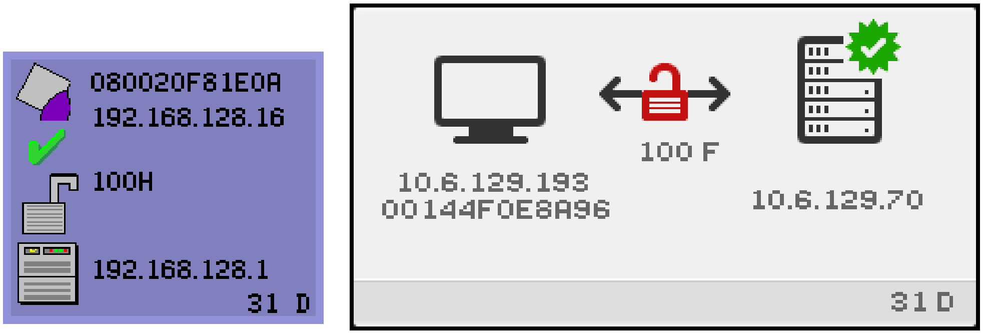
This icon indicates that the DTU has an Ethernet address and an IP address but has lost the Ethernet signal. This icon is displayed only after the DTU successfully boots and receives an IP address, but then loses its Ethernet signal.

▼ Actions to Take

1. **Check that the Ethernet cable is correctly plugged in to the back of the DTU and the other end is plugged into the correct switch or network outlet.**

2. **If the DTU is connected through a hub or switch, make sure that the hub or switch is on and configured correctly.**

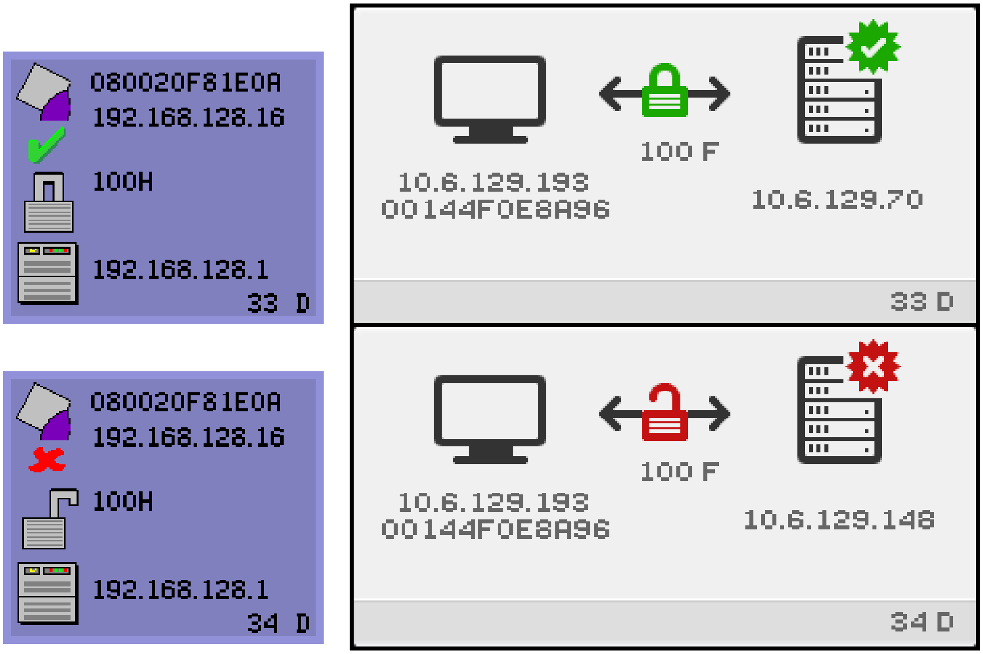
FIGURE B-9 Ethernet Address



This OSD shows the Ethernet address, currently assigned IP address, currently connected server, encryption status, DHCP state, and link speed and mode. 10 stands for 10 Mbps, and 100 for 100 Mbps. F stands for full duplex, H stands for half-duplex mode.To display this OSD with current information, press the three audio volume keys simultaneously.

Tip – To get the same effect on non-Sun keyboard, disconnect and reconnect the Ethernet cable.

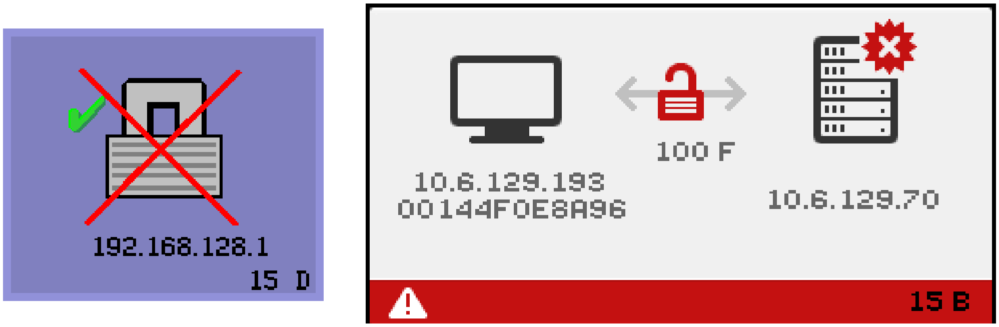
FIGURE B-10 Ethernet Address OSD with Different Encryption and Authentication States



Session Connection Failures

The following icons are displayed in the event of a possible security breach.

FIGURE B-11 Session Refused by Client



This icon indicates that 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.

A graphically similar icon displaying the number 50 indicates that 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.**

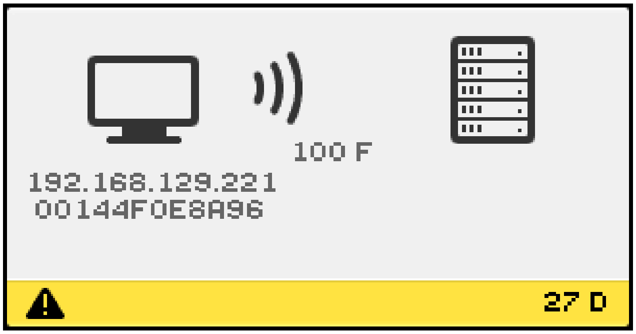
   This error may occur with firmware versions earlier than 2.0 if the server is configured for hard security mode.

2. **Upgrade the firmware.**

   As an alternative, confirm whether your site requires hard security mode. If not, the session can be enabled with soft security mode.

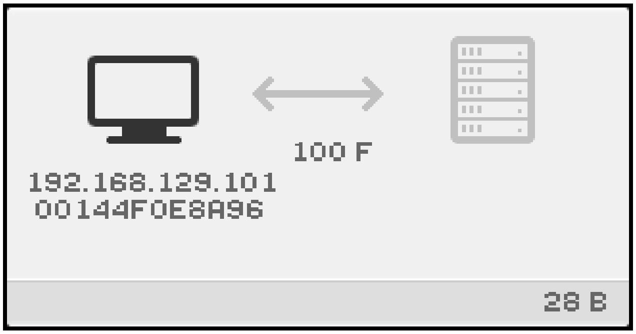
The following icon is displayed if the DTU is broadcasting to locate a server and either no servers respond or Sun Ray specific DHCP parameters have not been supplied correctly.

FIGURE B-12 DHCP Broadcast Failure



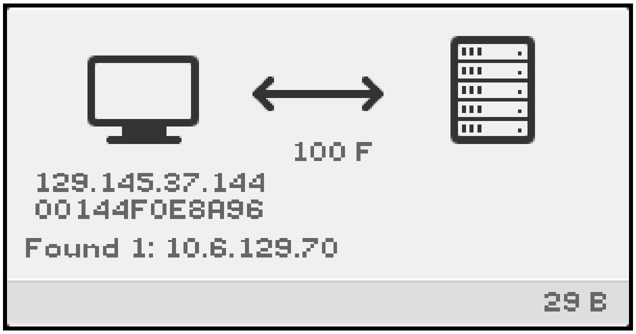
The following icon is displayed while a DTU is trying to establish a VPN connection.

FIGURE B-13 Establishing a VPN Connection



When the VPN connection is established, the following icon is displayed.

FIGURE B-14 VPN Connection Established



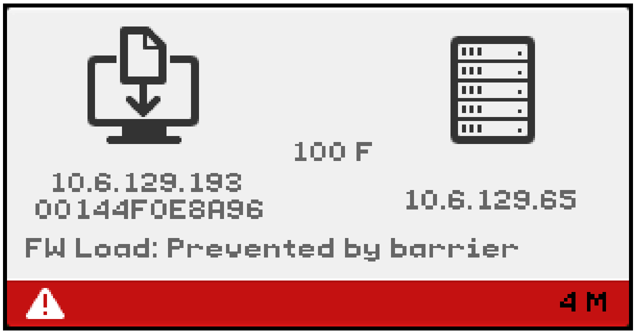
```
100 F
129.145.37.144
00144F0E8A96
Found 1: 10.6.129.70
29 B
```

Firmware Download Diagnostics

When firmware download error occurs, OSD icon 4 (see FIGURE B-15) displays the appropriate error code and a descriptive text string. These error codes are listed in TABLE B-4.

Note – These error messages appear in English even in localized versions of Sun Ray Server Software.

FIGURE B-15 OSD Icon 4 Displays Firmware Download Error Messages

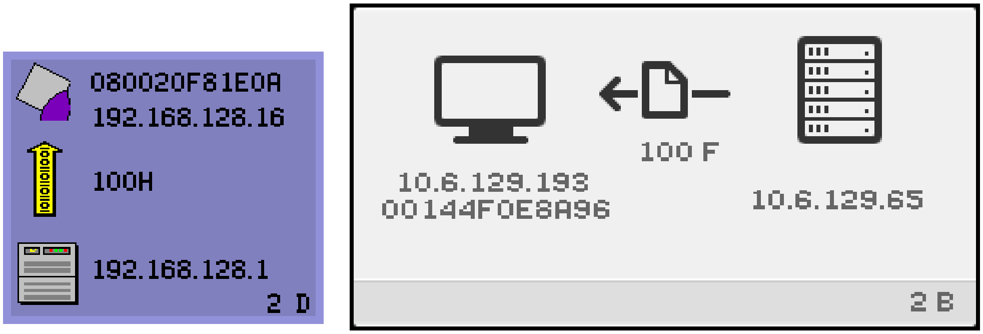


```
100 F
10.6.129.193
00144F0E8A96
10.6.129.65
FW Load: Prevented by barrier
4 M
```

Firmware Download OSD

The following OSD are typical of those that may display when new firmware is downloaded to a DTU from a Sun Ray server.

FIGURE B-16 Firmware Download in Progress



This icon indicates that the DTU is currently downloading new flash PROM software from the Sun Ray server.

▼ Actions to Take

1. **Wait until the download is complete.**

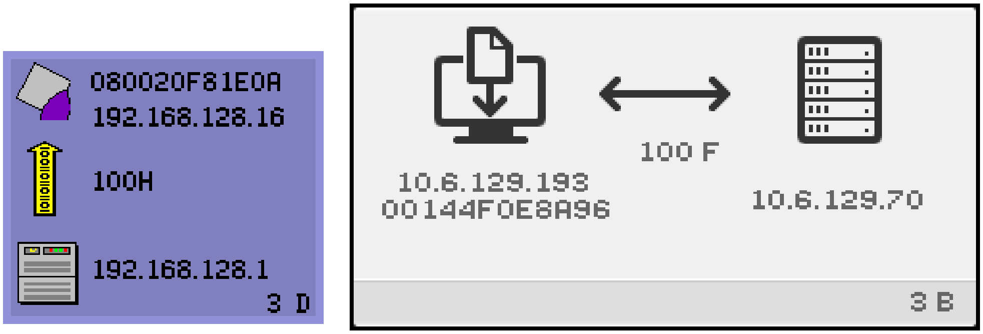
   Downloading and saving the new PROM software usually takes less than a minute. If you interrupt the download, the DTU has to download new PROM software the next time it reboots.

If the firmware download fails, the following syslog message indicates that the barrier level has been set to prevent Sun Ray DTUs with SRSS 4.0 firmware from automatically downloading an earlier version of the firmware:

```
Firmware upgrade/downgrade not allowed! Barrier is 310 Firmware level is
0
```

2. **Check** `/var/opt/SUNWut/log/messages` **to confirm that your configuration is set up properly.**

FIGURE B-17 Saving PROM Software



080020F81E0A
192.168.128.16
100H
192.168.128.1
3 D

10.6.129.193
00144F0E8A96
100 F
10.6.129.70
3 B

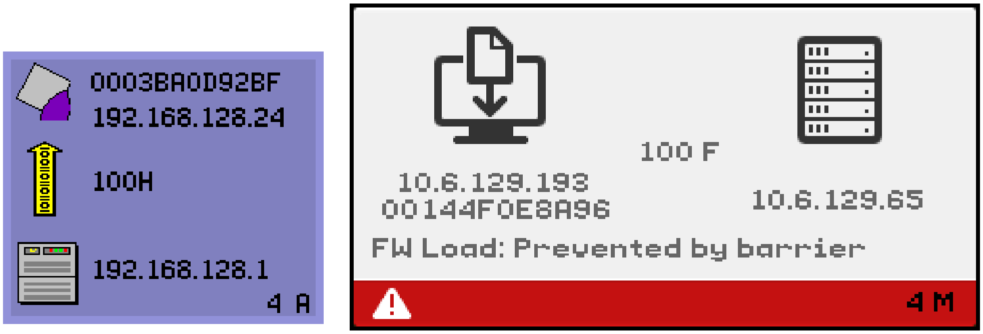
This icon indicates that the DTU has just downloaded new PROM software from the Sun Ray server and is saving it to the DTU's PROM.

▼ Actions to Take

- **Wait until the download is done.**

  Downloading and saving the new PROM software usually takes less than a minute. If you interrupt the download, the DTU has to download new PROM software the next time it reboots.

FIGURE B-18 Firmware Download Failed



0003BA0D92BF
192.168.128.24
100H
192.168.128.1
4 A

10.6.129.193
00144F0E8A96
100 F
10.6.129.65
FW Load: Prevented by barrier
4 M

This icon indicates that the DTU has failed to download new firmware. OSD 4 now includes error code text, as shown above.

Token Reader Icons

When a site policy disallows pseudo-sessions, DTUs configured as token readers display the Card Reader icon instead of the Login Dialog box card.

Note – The token reader was called the card reader in earlier releases. The smart card token itself is an integrated circuit embedded in or printed on the card, and it is data on the token that is read when a user inserts a card. In practice, the terms card reader and token reader are used interchangeably.

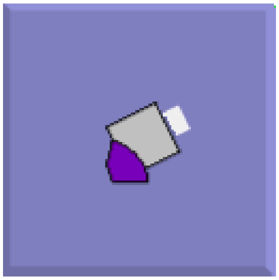
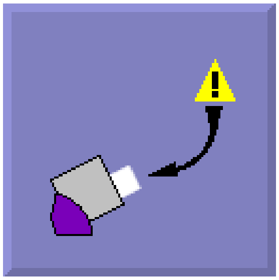


FIGURE B-19 Card Reader OSD

FIGURE B-20 Card Read Error OSD



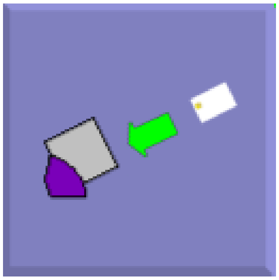
This icon indicates that the Card Read Error OSD icon appears whenever the firmware is unable to read the card due to one of the following causes:

- The DTU is running old firmware.
- The card contacts are dirty, the contacts on the card reader are dirty, or the card is not properly inserted.
- The card is malfunctioning.
- The card is of a type that the firmware is not configured to read.
- There is an error in the configuration for reading this type of card.

▼ Actions to Take

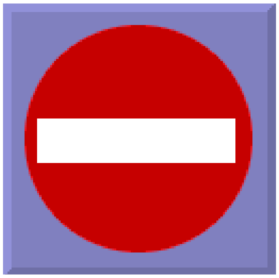
1. **Upgrade the firmware.**
2. **Replace the card.**

FIGURE B-21 Prompt for Card Insertion OSD



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

FIGURE B-22 Access Denied OSD



This icon indicates that the Access Denied OSD icon appears when the current authentication policy denies access to the presented token. Specifically, this icon is displayed if a disabled card has been inserted into a DTU.

The Sun Ray administration model has seven user session types:

- Default—Normal user login
- Register—User self-registration
- Kiosk—Anonymous user operation
- Insert card—User smart card required
- Card error—Unrecognized user smart card type
- No entry—User's smart card token is blocked

- Session Refused—The server refuses to grant a session to a 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

Although the last four session types display icons on the Sun Ray DTU, they do not have login processes at all. The icons indicate that the user must take steps before a successful login is possible. If the user immediately removes and reinserts the smart card, the icon disappears, but the Wait for Session OSD remains.

These last four session types and their OSDs should not cause alarm. The user can:

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

Authentication Manager Errors

Authentication Manager errors can be found in the following error logs:

- Installation logs:
  - `/var/adm/log`
  - /var/opt/SUNWut/log
- General log files:
  - `/var/opt/SUNWut/srds/log`
  - `/var/opt/SUNWut/srds/replog`

The general format of the log messages is:

```
timestamp   thread_name    message_class     message
```

For example:

```
May  7 15:01:57 e47c utauthd: [ID 293833 user.info] Worker3
NOTICE: SESSION_OK pseudo.080020f8a5ee
```

Message components are defined as follows:

- `timestamp` format:

  year.month.day hours:minutes:seconds

- `thread_name`

  There are several different types of threads. The most common thread handles DTU authentication, access control, and session monitoring. These threads are named “worker” plus number. The Worker# thread names are reused when a connection terminates. Other threads are:

  - SessionManager#—Communicate with `utsessiond` on behalf of a Worker# thread.
  - AdminJobQ—Used in the implementation to wrap a library that would not otherwise be thread-safe.
  - CallBack#—Communicate with applications such as `utload`.
  - WatchID—Used to poll data/terminals from connections
  - Terminator—Cleans up terminal sessions
  - Group Manager—Main group manager thread

- `message_class`

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

  - `CLIENT_ERROR`—Indicates unexpected behavior from a DTU. These messages can be generated during normal operation if a DTU is rebooted.
  - `CONFIG_ERROR`—Indicates a system configuration error. The Authentication Manager generally exits after one of these errors is detected.
  - `NOTICE`—Logs normal events.
  - `UNEXPECTED`—Logs events or conditions that were not anticipated for normal operation but are generally not fatal. Some of these errors should be brought to the attention of the Sun Ray product development team.
  - `DEBUG`—Only occurs if explicitly enabled. Beneficial to developers. Debug messages can reveal session IDs, which must be kept secret to ensure proper security.

TABLE B-5 Error Message Examples

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

Troubleshooting USB Mass Storage Devices

The most common problems encountered with USB mass storage devices on Sun Ray DTUs are described in the following sections.

Device Nodes Are Not Created

Some mass storage device types are not supported on Sun Ray. Inspect the log file `/var/opt/SUNWut/log/utstoraged.log` for an indication as to why device nodes were not created.

Device Is Not Automatically Mounted

If the storage medium does not have a OS-recognizable file system, it will not get automatically mounted. An error message will be logged to:
`/var/opt/SUNWut/log/utmountd.log`

Device Is Not Automatically Unmounted

If the device is unplugged, or if the user's session is disconnected from the DTU, all mount points for that DTU are automatically unmounted unless the user has open references to the mount point. In that case, the mount point becomes stale. A stale mount point persists until the administrator unmounts it manually or until the system is rebooted.

Run the following command to find stale mount points.

```
# /opt/SUNWut/bin/utdiskadm -s
```

Note – Close all references to the mount point or terminate all processes that refer to the mount before running the `umount` command.

Audio

Each time a user logs in to a Sun Ray DTU, a script automatically assigns the $AUDIODEV environment variable to that session. One utaudio(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 hotdesking. The device name appears in the $AUDIODEV environment variable but is transparently interpreted by audio programs for Sun systems. Device nodes are created in the /tmp/SUNWut/dev/utaudio directory. The directory tree is completely recreated at boot time.

Caution – Do not remove the /tmp/SUNWut/dev/utaudio directory. Deleting this directory prevents existing users with utaudio sessions from using their audio pseudo device nodes.

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

Audio Malfunction

If audio features are malfunctioning:

1. **To confirm whether audio is working, run the following command on the DTU:**

```
% cat <audio file> >/$AUDIODEV
```

2. **Bring up** utsettings**:**

```
% utsettings
```

3. **Verify that audio output is selected properly, for example, for headphones or speakers.**
4. **Check the volume level.**
5. **Verify that Mute is not selected.**

Some applications are hard-coded to use /dev/audio for output. Sun Ray System Software provides a redirection library that you can use to correct this behavior.

▼ To Activate the Redirection Library

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

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

2. **Restart the application.**

Performance Tuning

Some applications, such as intensive 3-D visual simulations, may run very slowly on Sun Ray. Other applications, such as pseudo-stereo viewers using double-buffering, or high-frequency dynamic color table flips on 8-bit visuals, do not produce the expected visual result.

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 100F.**

3. **Use utcapture to assess network latency and packet loss.**

   As latency and packet loss increase, performance suffers.

Screensaver Resource Consumption

Many graphics-intensive screensaver programs consume large amounts of CPU, memory, and network bandwidth. To avoid excessive resource consumption, they should be disabled on Sun Ray servers.

▼ To Disable Screensaver Hacks on Solaris Systems

- **Remove the packages that contain the screensaver hacks:**

```
pkgrm SUNWxscreensaver-hacks
```

- **On machines that have the** `SUNWxscreensaver-hacks-gl` **package installed, modify the** `pkgrm` **command as follows:**

```
pkgrm SUNWxscreensaver-hacks-gl
```

Note – It may be necessary to remove the gl (graphics library) package first.

▼ To Disable Screensaver Hacks on Linux Systems

It is slightly more complicated to perform the equivalent procedure on Linux systems because the screensaver hacks all reside in one RPM with the `xscreensaver` executables. Thus, instead of removing all the hacks with a single command, it may be necessary to rename the directory or directories that contain the screensavers or restrict their permissions.

Multihead Displays

For information on multihead displays, please see "Multihead Administration" on page 119.

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

Monitor Display Resolution Defaults to 640 x 480

First, eliminate the most obvious possible causes:

- An older monitor
- A bad cable

- Monitor was off when the Sun Ray DTU was started

If the Sun Ray DTU is unable to read DDC data from the monitor, then it defaults to 640 x 480 pixels.

▼ To Correct or Reset the Screen Resolution

1. **Replace the cable**
2. **Restart the Sun Ray DTU after powering the monitor on**
3. **Replace the monitor**
4. **Use the** `utresadm` **to set persistent display setting to override the default.**

Old Icons (Hourglass with Dashes Underneath) Appear on Display

If the old icons appear on the display, either the DTU's firmware has not been upgraded or it is failing.

1. **Upgrade the firmware to SRSS 4.0.**
2. **Follow the procedure to upgrade the firmware. See the** *Sun Ray Software 4.0 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/`

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 then other text.

CHAPTER

Glossary

A

AMGH Automatic Multigroup Hotdesking. See *regional hotdesking*.

AH Authentication headers, used as part of an IPSec implementation.

authentication policy The Authentication Manager, using the selected authentication modules, decides what tokens are valid and which users, as token owners, have access to the system and sessions.

authentication token Although all tokens are used by the Authentication Manager to grant or deny access to Sun Ray sessions, this term usually refers to a user's smart card token.

B

backplane bandwidth Sometimes also referred to as switch fabric. A switch's backplane is the pipe through which data flows from an input port to an output port. Backplane bandwidth usually refers to the aggregate bandwidth available amongst all ports within a switch.

barrier mechanism To prevent clients from downloading firmware that is older than the firmware they already have, the administrator can set a barrier mechanism. The barrier mechanism symbol `BarrierLevel` is defined by default in the DHCP table of Sun Ray servers running version 2.0 or later of Sun Ray Server Software.

bpp Bits per pixel.

C

CAM Controlled Access Mode, also known as *kiosk mode*. As of SRSS 4.0, the CAM module has been replaced by a rewritten Kiosk module.

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.

cold restart Pressing the Cold Restart button terminates all sessions on a given server before restarting Sun Ray services. See *restart*.

cut-through switches The switch begins forwarding the incoming frame onto the outbound port as soon as it reads the MAC address, while it continues receiving the remainder of the frame.

D

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

domain A set of one or more system boards that acts as a separate system capable of booting the OS and running independently of any other board.

DTU Sun Ray desktop units were originally known as Desktop Terminal Units.

E

ESP Encapsulating Security Payloads, used as part of *IPSec*.

Ethernet Physical and link-level communications mechanism defined by the IEEE 802.3 family of standards.

Ethernet address The unique hardware address assigned to a computer system or interface board when it is manufactured. See *MAC address*.

Ethernet switch A unit that redirects packets from input ports to output ports. It can be a component of the Sun Ray interconnect fabric.

F

failover The process of transferring processes from a failed server to a functional server

failover group Two or more Sun Ray servers configured to provide continuity of service in the event of a network or system failure.

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.

group-wide Across a failover group.

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.

hotdesking The ability for a user to remove a smart card, insert it into any other DTU within a server group, and have the user's session "follow" the user, thus allowing the user to have instantaneous access to the user's windowing environment and current applications from multiple DTUs.

hot key A pre-defined key that causes something to appear on your screen. A hot key is used to bring up the Settings screen on the Sun Ray DTU.

hot-pluggable A property of a hardware component that can be inserted into or removed from a system that is powered on. USB devices connected to Sun Ray DTUs are hot-pluggable.

I

idle session A session that is running on a Sun Ray server but to which no user (identified by a smart card token or a pseudo-token) is logged in.

IKE Internet Key Exchange, a component of *IPSec*.

interconnect fabric All the cabling and switches that connect a Sun Ray server's network interface cards to the Sun Ray DTUs.

internet A collection of networks interconnected by a set of routers that enable them to function as a single, large virtual network.

Internet The largest internet in the world, consisting of large national backbone nets (such as MILNET, NSFNET, and CREN) and myriad regional and local campus networks all over the world. It is a global collection of networks connecting a wide range of computers using a common protocol to communicate and share services.

intranet Any network that provides similar services within an organization to those provided by the Internet but which is not necessarily connected to the Internet.

IP address A unique number that identifies each host or other hardware system on a network. An IP address is composed of four integers separated by periods. Each decimal integer must be in the range 0-255 (for example, 129.144.0.0).

IP address lease The assignment of an IP address to a computer system for a specified length of time, rather than permanently. IP address leasing is managed by the Dynamic Host Configuration Protocol (DHCP). Sun Ray DTU IP addresses are leased.

IPSec Internet Protocol (Security) set of protocols seeks to secure IP communications by encoding data packets through authentication headers (*AH*) and encapsulating security payloads (*ESP*) and by providing a key exchange mechanism (*IKE*).

K

kiosk mode Used interchangeably with *CAM* in earlier versions of SRSS. As of version 4.0, this module, now called Kiosk, has been completely rewritten.

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.

mobile token If mobile sessions are enabled, a user can log into an existing session from different locations without a smart card, in which case the user name is associated with the session. This type of *pseudo-token* is called a mobile token.

mobility For the purposes of the Sun Ray Server Software, the property of a session that allows it to follow a user from one DTU to another within a server group. On the Sun Ray system, mobility requires the use of a smart card or other identifying mechanism.

modules Authentication modules are used to implement various site-selectable authentication policies.

MTU Maximum Transmission Unit, used to specify the number of bytes in the largest packet a network can transmit.

multicasting The process of enabling communication between Sun Ray servers over their Sun Ray network interfaces in a failover environment.

multihead See *head*.

multiplexing The process of transmitting multiple channels across one communications circuit.

N

namespace A set of names in which a specified ID must be unique.

network Technically, the hardware connecting various computer systems enabling them to communicate. Informally, the systems so connected.

network address The IP address used to specify a network.

network address translation NAT. Network address translation typically involves the mapping of port numbers to allow multiple machines (Sun Ray DTUs in this case) to share a single IP address.

network interface An access point to a computer system on a network. Each interface is associated with a physical device. However, a physical device can have multiple network interfaces.

network interface card NIC. The hardware that links a workstation or server to a network device.

network latency The time delay associated with moving information through a network. Interactive applications such as voice, video displays and multimedia applications are sensitive to these delays.

network mask A number used by software to separate the local subnet address from the rest of a given Internet protocol address. An example of a network mask for a class C network is 255.255.255.0.

network protocol stack A network suite of protocols, organized in a hierarchy of layers called a stack. TCP/IP is an example of a Sun Ray protocol stack.

NIC Network interface card.

non-smart card mobility A mobile session on a Sun Ray DTU that does not rely on a smart card. NSCM requires a policy that allows *pseudo-token*s.

NSCM See *non-smart card mobility*.

O

OSD On-screen display. The Sun Ray DTU uses OSD icons to alert the user of potential start-up or connectivity problems.

P

PAM Pluggable Authentication Module. A set of dynamically loadable objects that gives system administrators the flexibility of choosing among available user authentication services.

PAM session A single PAM handle and run time state associated with all PAM items, data, etc.

patch A collection of files and directories that replace or update existing files and directories that prevent proper execution of the software on a computer system. The patch software is derived from a specified package format and can only be installed if the package it fixes is already present.

policy See *authentication policy*.

Pop-up GUI A mechanism that allows the entry of configuration parameters for a Sun Ray DTU from the attached keyboard.

port (1) A location for passing data in and out of a computer system. (2) The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host.

power cycling Using the power cord to restart a DTU.

pseudo-session A Sun Ray session associated with a *pseudo-token* rather than a smart card token.

pseudo-token A user accessing a Sun Ray session without a smart card is identified by the DTU's built-in type and MAC address, known as a pseudo-token. See *token*.

R

regional hotdesking Originally known as Automatic Multigroup Hotdesking (AMGH), this SRSS feature allows users to access their sessions across wider domains and greater physical distances than was possible in earlier versions of SRSS. Administrators enable this feature by defining how user sessions are mapped to an expanded list of servers in multiple failover groups.

restart Sun Ray services can be restarted either from the utrestart command or with the Warm Restart or Cold Restart buttons on the GUI. A a cold restart terminates all Sun Ray sessions; a warm restart does not.

S

screen flipping The ability to pan to individual screens on a DTU with a single head that were originally created by a multihead group.

server A computer system that supplies computing services or resources to one or more clients.

service For the purposes of the Sun Ray Server Software, any application that can directly connect to the Sun Ray DTU. It can include audio, video, X servers, access to other machines, and device control of the DTU.

session A group of services associated with an authentication token. A session may be associated with a token embedded on a smart card

session mobility The ability for a session to "follow" a user's login ID or a token embedded on a smart card.

smart card Generically, a plastic card containing a microprocessor capable of making calculations. Smart cards that can be used to initiate or connect to Sun Ray sessions contain identifiers, such as the card type and ID. Smart card tokens may also be registered in the Sun Ray Data Store, either by the Sun Ray administrator or, if the administrator chooses, by the user.

smart card token An authentication token contained on a smart card. See *token*.

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 DTUs rely on the server for all computing power and storage.

timeout value The maximum allowed time interval between communications from a DTU to the Authentication Manager.

token The Sun Ray system requires each user to present a token, which the Authentication Manager uses to allow or deny access to the system and to sessions. A token consists of a type and an ID. If the user uses a smart card, the smart card's type and ID are used as the token. If the user is not using a smart card, the DTU's built-in type and ID (the unit's Ethernet, or MAC, address) are used instead as a *pseudo-token*. If mobile sessions are enabled, a user can log into an existing session from different locations without a smart card, in which case the user name is associated with the session. A pseudo-token used for mobile sessions is called a *mobile token*.

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 (such as HTTP or FTP), `host` specifies the Internet name of the host on which to find it, and `localinfo` is a string (often a file name) passed to the protocol handler on the remote host.

USB Universal Serial Bus.

user name The name a computer system uses to identify a particular user. Under UNIX, this is a text string of up to eight characters composed of letters (a-z and A-Z), digits (0-9), hyphens (-), and underscores (_), for example, *jpmorgan*, *jp_morg*, *jpm-888*. The first character must be a letter.

user session A session that is running on a Sun Ray server and to which a user (identified by a smart card token or a pseudotoken) is logged in.

V

virtual frame buffer A region of memory on the Sun Ray server that contains the current state of a user's display.

VPN Virtual Private Network.

VLAN Virtual Local Area Network.

W

warm restart See *restart*.

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

X

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

Index