

; i]XU`fUa a]b]gfUh]cbY
X]'Gi b'F UmGYfj Yf'GcZk UfY("&

February 2011

ORACLE®

Oracle Corporation and its affiliates. All rights reserved.

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Guida all'amministrazione di Sun Ray Server Software 4.2

A

Guida all'amministrazione di Sun Ray Server Software 4.2

Contents

- Overview of the Sun Ray System
 - Computing Model
 - Security Considerations
 - Parts of the Sun Ray System
 - Sun Ray DTU
 - Sun Ray Server Software
 - Network Components
 - Physical Connections
 - Feature Differences Between Solaris and Linux Platforms
 - Sun Ray System Deployment Examples
 - Small Deployments
 - Medium to Large Deployments
 - Failover Group Scenario
 - Regional Hotdesking
-

About SRSS (All Topics)

Overview of the Sun Ray System

Sun Ray(TM) computing, originally developed to run on the Solaris(TM) Operating System, is the first, perhaps the only, thin client implementation to offer both workstation-like user functionality and sufficient speed and reliability for mission-critical applications. Sun Ray Server Software supports Sun Ray thin clients, or desktop units (DTUs) on three flavors of Linux – Oracle Linux 5.4 and 5.5, Red Hat Enterprise Linux 5, and SuSE Linux Enterprise Server 10 – as well as Solaris 10, including Solaris Trusted Extensions.

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

The Sun Ray Connector for Windows Operating Systems manages connections from Sun Ray DTUs to user sessions running on Microsoft Windows Terminal Servers, including enhancements for improved video playback. It is described in the [Sun Ray Connector for Windows OS, Version 2.2 Information Center](#).

When used in conjunction with both the Sun Ray Connector for Windows and the Sun Virtual Desktop Connector, Sun Ray Server Software helps to enable access to multiple virtual desktops from Sun Ray DTUs. This capability is described in the [Sun Virtual Desktop Connector Installation and Administration Guide](#).

Computing Model

Other client-server models typically use combinations of remote and local operating systems, applications, memory, and storage, but the Sun Ray computing model moves all computing to a server. Instead of running applications, storing data, and doing computation on a desktop device like a PC, the Sun Ray model simply passes input and output data between Sun Ray DTUs and the Sun Ray server, where the operating system and applications are located.

Almost any Sun server with sufficient capacity can be configured as a Sun Ray server as long as it runs a supported version of the Solaris operating system or one of the supported flavors of Linux. See the [SRSS 4.2 Release Notes](#) for the current list of supported operating systems and versions.

Every Sun Ray DTU includes a smart card reader. The industry standard PC/SC-lite API is included for developers who want to encode custom applications or other information in their users' smart cards. Custom applications are frequently used to provide the following solutions:

- Strong smart card-based authenticated logins and PKCS#11
- S/MIME digital signature message signing and encryption

PC/SC-lite requires no additional administration.

Sun Ray DTUs have no local disks, applications, or operating systems and are therefore considered stateless. This setup is what makes them true thin clients. Stateless devices are inexpensive to maintain because they do not require administrators or technicians to install, upgrade, or configure software or to replace mechanical components on the desktop.



Note

The Sun Ray DTU contains a firmware module that performs a small set of tasks: it sends keyboard and mouse events and displays pixel data. If a desktop device contains an operating system that can execute code at the request of a user, it has state and it is not a true thin client. This type of device requires updating and maintenance at the desktop rather than server level and it is susceptible to viruses. Sun Ray DTUs update their firmware without user or administrator intervention.

Sun Ray DTUs are also extremely secure. For instance, managing USB mass storage devices, that is, controlling the ability to enable or disable their use, is done at the server or group level. This ability enables sites with particular security or intellectual property concerns to eliminate many of the risks imposed by PCs and other fat clients, which rely on local operating systems, local applications, and local data caches. Critical data can be compromised or lost when the physical device hosting the "fat" client is stolen or damaged.

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

Most large Sun Ray implementations include at least one [failover group](#) to ensure uninterrupted service whenever a server is off-line. When a failover group is configured, Sun Ray Server Software optimizes performance by spreading the computing load among the servers in the group. Failover groups and related concepts are discussed in [About Failover Groups](#).

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 intercepting communications between the server and the DTU is very difficult.

Sun Ray Server Software encryption features also help to protect sensitive data by providing options to encode keyboard input and display traffic. In addition, [Remote Hotdesk Authentication \(RHA\)](#), requires SRSS-based authentication before users can reconnect to existing sessions.

Parts of 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 can potentially exceed the full functionality of a workstation or a multimedia PC. The key features include:

- 24-bit, 2-D accelerated graphics up to 1920 x 1200 resolution at 70 Hz (640 x 480 at 60 Hz is the lowest resolution)
- Multichannel audio input and output capabilities
- Accelerated video output, handled by the Sun Ray Server Software for Sun Ray 1 series DTUs and by DTU hardware in newer Sun Ray 2 series DTUs
- Smart card reader

- USB ports that support hot-pluggable peripherals
- Serial port for the Sun Ray 170 and later models
- NAT gateway device support
- Integrated, routerless VPN capability on Sun Ray 2, 2FS, 270 and later models
- EnergyStar compliance
 - No fan, switch, or disk
 - Very low power consumption

The DTU acts as a [frame buffer](#) on the client side of the network. Applications run on the server and render their output to a [virtual frame buffer](#). The Sun Ray Server Software formats the rendered output and sends it to the appropriate DTU, where the output is interpreted and displayed.

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

An IP address is leased to each Sun Ray DTU when it is connected and can be reused when the DTU is disconnected. IP address leasing is managed by the [Dynamic Host Configuration Protocol \(DHCP\)](#). In cases where separate DHCP servers already exist on a network that supports Sun Ray DTUs, these servers can be used for tasks such as assigning IP addresses and network parameters to the DTUs. Separate DHCP servers are not required, however, because they require static IP addresses, Sun Ray servers cannot be DHCP clients. These considerations are discussed in [Sun Ray DTU Initialization Requirements Using DHCP](#).

Multihead Displays

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

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 a problem occurs with the DTU, the module displays an on-screen display (OSD) icon to make it easier to diagnose. OSD icons are described in [SRSS Troubleshooting Icons](#).

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

Sun Ray Server Software

The administrator can configure network connections, select an authentication protocol, administer authentication tokens, define desktop properties, monitor the system, and perform troubleshooting. Sun Ray Server Software includes:

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

Sun Ray Server Software enables direct access to all Solaris X11 applications. The Sun Ray Connector for Windows software enables Sun Ray users to access applications on remote Windows Terminal Servers. See the [Sun Ray Connector for Windows OS, Version Information Center](#). Third-party applications running on the Sun Ray server can also provide access to Microsoft Windows applications and a variety of legacy (mainframe) applications.

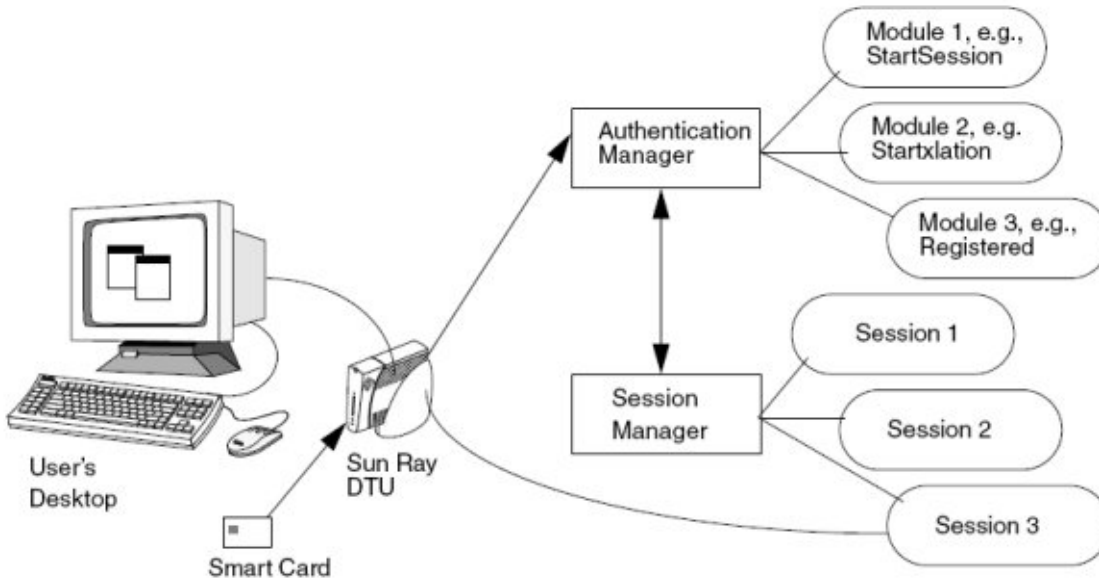
Authentication Manager

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

The interaction between the Authentication Manager and the DTU is depicted in the following figure and works as follows:

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

Authentication and Session Manager Interaction



The Sun Ray DTU contacts the `AuthSrvr` DHCP option's address. If that address 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 and only addresses on the list are checked. The addresses are tried in list 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 following table describes the commonly used modules.

Module	Description
StartSession	Any type of token is accepted. Users see the login window. This module is designed primarily for implementations in which Sun Ray DTUs replace workstations or PCs.
StartxlationSession	Any type of token is accepted. A temporary, transitional session is created for authentication purposes. This module is used for login and hotdesking with Non-Smart Card Mobility (NSCM) and for hotdesking when a Remote Hotdesk Authentication (RHA) policy is used.
Registered	<p>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 two conditions, it is rejected. If the token is accepted, users see the login window. This module is designed for sites that want to restrict access to only certain users or DTUs.</p> <p>Users can be registered in two ways, reflecting two possible policy decisions for the administrator:</p> <ul style="list-style-type: none"> • Central Registration - The administrator assigns smart cards 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. The user provides the same information as the information requested by a site administrator. If self-registration is enabled, users can still be registered centrally. If a token has been registered but disabled, the user cannot re-register the token. The user must contact the site administrator to re-enable the token.

Sessions and Services

A **session** consists of a group of services controlled by the Session Manager. The session is associated with a user through an authentication token.

A [service](#) is any application that can connect directly to the Sun Ray DTU. Such applications can include audio, video, Xservers, and device control of the DTU. For example, `dtmail` is not a service because it is accessed through an Xserver rather than directly.

Session Manager

The [Session Manager](#) interacts with the Authentication Manager and directs services to the user. The Session Manager is used at startup for services, for managing screen space, and as a rendezvous 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 following sequence describes how the process starts, ends, and restarts:

1. After a user's token is authenticated, the Authentication Manager determines whether a session exists for that token. If a session does not exist, the Authentication Manager asks the Session Manager to create a session and then starts the appropriate services for the session according to the authentication policy decisions taken by the administrator. Creating a session usually requires 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 must connect directly to the DTU.
4. The user can then interact with the session. The Session Manager mediates control of the screen space between competing services in a session and notifies the services of changes in screen space allocation.
5. When the user removes the smart card, or presses Shift+Pause in an NSCM session, or power cycles the DTU, or is inactive for longer than the screen lock idle timeout interval, the Authentication Manager determines that the session associated with that token must be disconnected from that DTU. The Authentication Manager notifies the Session Manager, which in turn notifies all the services in the session and any USB devices to disconnect.
6. When the user re-inserts the smart card, or logs in again to get access to an NSCM session, the Authentication Manager requests the Session Manager to create a new temporary session and then uses it to authenticate the user. This is known as Remote Hotdesk Authentication (RHA). After the user has been authenticated, the Sun Ray DTU is connected directly to the user's session.



Note

RHA does not apply to anonymous Kiosk Mode or to token readers. Sun Ray Server Software can be configured to [turn this security policy feature off](#).

The Session Manager is consulted only if the state of the session changes or if other services are added. When a user's token is no longer mapped to a DTU, for example, when a card is removed, the Session Manager disconnects the services from the DTU, but the services remain active on the server. For example, programs attached to the Xserver continue to run although their output is not visible. The Session Manager daemon must continue running. 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 authorized sessions and requires them to be reauthenticated. These services are disconnected but still active. If the Session Manager is disrupted, it restarts automatically. Each service contacts the Session Manager to request reattachment to a particular session.

Xserver

Sun Ray Server Software includes the Xserver process, [Xnewt](#), as the default Xserver. Xnewt, which supports all the latest [multimedia enhancements](#), is based on release 7.2 of the Xorg Community source.

Xnewt also includes the capability to use the X Rendering Extension (Render), which enables clients to use a new rendering model based on Porter-Duff compositing. See [How to Enable or Disable XRender](#) for more details.

For information about how to configure different Xservers, see the `utxconfig(1)` man page.

Sun Management Center (Solaris)

The Sun Management Center (SunMC) software monitors managed objects in the Sun Ray system. Objects that can be managed by default include the Sun Ray system itself, Sun Ray services, failover groups, interconnects, and desktops. Each managed object is monitored separately and has independent alarm settings.

Sun Management Center software also monitors Sun Ray Server Software daemons that authenticate users, start sessions, manage devices, and handle DHCP services. [About Sun Ray System Monitoring](#) describes how to use SunMC to monitor a Sun Ray system. For information about problems with SunMC, see [Troubleshooting Sun Management Center \(Solaris\)](#).

CLI and Admin GUI

Sun Ray Server Software has both a command-line interface (CLI) and an [Admin GUI](#) for administrative functions. The GUI presents a clear view of administrative functions, with a tab-based navigational model and context-sensitive help.

Data Store

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

Kiosk Mode

[Kiosk Mode](#) can provide anonymous users with limited access to specific applications on Sun Ray DTUs.

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. Possible configurations include the following:

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

For detailed descriptions of the types of network configuration and instructions on configuring each network type, see [About Sun Ray System Networks](#).

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 to shield users from the network interaction taking place at every display update, 100 Mbps switches are preferred. The two basic types of 100 Mbps switches are:

- 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, and also have one or more gigabit interfaces for attaching to the server.

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

Server-to-switch bandwidth must be scaled based on end-user multiplexing needs so that the server-to-switch link does not become saturated. Gigabit uplink ports on the switch provide high-bandwidth connections from the server, 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 can be dedicated and private, or a VLAN, or it can be part of the corporate LAN. For private interconnects, the Sun Ray server uses at least two network interfaces: one for the corporate LAN and the other interface 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.

Feature Differences Between Solaris and Linux Platforms

This page provides the list of SRSS feature that are not supported on a Sun Ray server running the Linux platform.

- PS/SC-lite for Sun Ray is not supported on Linux.
- [Non-Smart Card Mobile \(NSCM\)](#) feature is not supported on Linux.
- Mass storage is not recommended with [Kiosk Mode](#) on Linux. Linux does not write the files until the device is prepared to be ejected, which the user can't easily do from Windows.
- [Sun Management Center \(SunMC\)](#) is not supported on Linux.
- [Predefined kiosk sessions](#) that support a collection of applications in a restricted, desktop-like environment are not supported on Linux. Solaris has CDE based and Sun Java Desktop (JDS), Release 3 based support.

Sun Ray System 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 examples. In addition, detailed discussions of actual deployment scenarios and other Sun Ray-related information can be found on the following blogs:

- <http://blogs.sun.com/ThinkThin>
- <http://blogs.sun.com/ThinGuy>
- <http://blogs.sun.com/GoThinCity>
- <http://blogs.sun.com/bobd>

Small Deployments

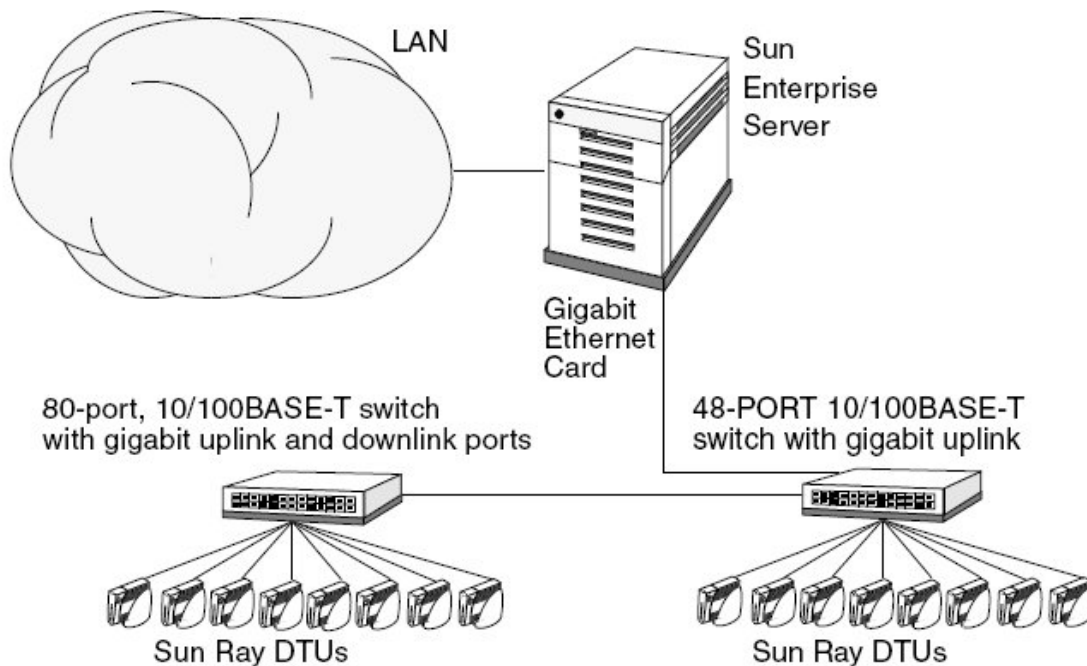
For smaller deployments, such as those with between 5 and 50 Sun Ray DTUs, the Sun Ray server uses a single 100BASE-T card to connect to a 100BASE-T switch. This switch, in turn, connects to the Sun Ray DTUs. With five or fewer DTUs, a wireless interconnect works acceptably at 10 Mbytes.

Medium to Large Deployments

For larger departments with groups consisting of hundreds or thousands of Sun Ray DTUs, the Sun Ray server uses a gigabit Ethernet card to connect to large 10/100BASE-T switches. Especially with recent low-bandwidth enhancements, more than one gigabit link from the server to the Sun Ray DTU's network is not necessary for enhanced performance.

A 100-user departmental system, for example, consisting of a Sun Enterprise(TM) 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 the following figure.

Typical Medium to Large Deployment Scenario



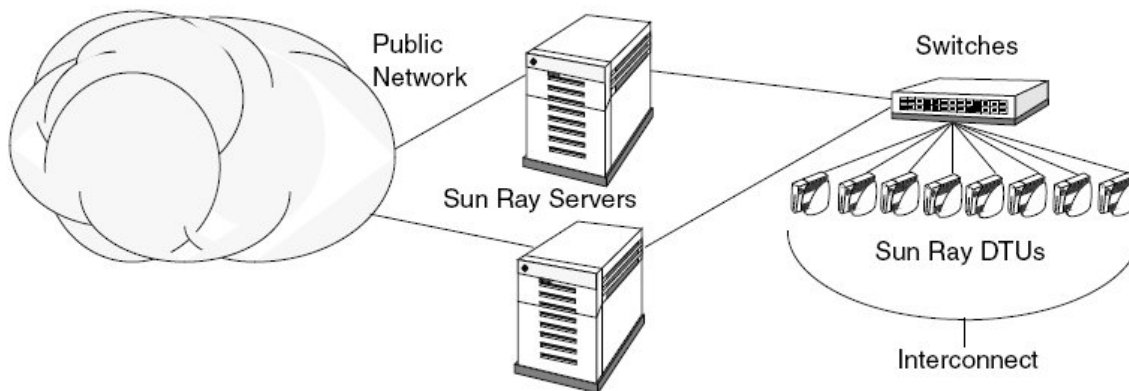
For example, a Sun Enterprise server with a Sun 10/100BASE-T card and a 24-port 10/100BASE-T switch can easily support 23 users performing standard desktop activities.

Failover Group Scenario

Sun Ray servers are often bound together to create failover groups. A failover group consisting of two or more servers that provide users with a high level of availability in case one server become unavailable. When a server in a failover group becomes unavailable, 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 one exists on that server. If the DTU can find no existing session for the current token, it 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 [About Failover Groups](#).

Simple Failover Group



Regional Hotdesking

Enterprises with multiple failover groups and users who move from one location to another, such as between corporate headquarters and various branch offices, might want to configure regional hotdesking. This feature provides users with access to their sessions across a wider domain and longer distance than a single failover group. It is described in [Managing Hotdesking With Smart Cards\(All Topics\)](#).

Contents

- [About Failover Groups](#)
 - [How Failover Works](#)
 - [Network Topologies](#)
 - [Using Different Sun Ray Server Software Versions](#)
 - [Authentication Requirements](#)
 - [Configuring Failover Groups](#)
- [Group Manager](#)
 - [Redirection](#)
 - [Group Manager Configuration](#)
- [Load Balancing](#)
 - [How to Turn Off the Load Balancing Feature](#)
- [Task Map - Managing Failover Groups](#)
 - [Initial Configuration](#)
 - [Related Tasks](#)
- [Setting Up IP Addressing](#)
 - [Setting Up Server and Client Addresses](#)
 - [Server Addresses](#)
 - [Configuring DHCP](#)
 - [Coexistence of the Sun Ray Server With Other DHCP Servers](#)
 - [Administering Other Clients](#)
- [How to Set Up IP Addressing on Multiple Servers, Each with One Sun Ray Interface](#)
- [How to Configure a Primary Server](#)
- [How to Add a Secondary Server](#)
 - [How to Add a Secondary Server](#)
- [How to Synchronize Primary and Secondary Sun Ray Servers](#)
- [How to Change the Group Manager Signature](#)
- [How to Take a Server Offline and Online](#)
 - [How to Take a Server Offline](#)
 - [How to Take a Server Online](#)
- [How to Show the Current SRDS Replication Configuration](#)
- [How to Remove the Replication Configuration](#)
- [How to View Network \(Failover Group\) Status](#)
- [Recovery Issues and Procedures](#)
 - [Primary Server Recovery](#)
 - [How to Rebuild the Primary Server's Administration Data Store](#)
 - [How to Replace the Primary Server with a Secondary Server](#)

- [Secondary Server Recovery](#)
-

Managing Failover Groups (All Topics)

About Failover Groups

A failover group (FOG) is a group of servers made up of one primary server and one or more secondary servers configured to provide continuity of service in the event of a network or system failure. Besides the high-availability feature, a failover group also provides a scalable Sun Ray service for a population of Sun Ray clients.

How Failover Works

For Sun Ray Server Software, the group manager manages the failover process. For every server in the failover group, the Group Manager does the following actions:

- Detects the presence of other Sun Ray servers belonging to the same group
- Monitors the availability (liveness) of the other servers
- Exchanges information about allocation of sessions and server load for load balancing purposes
- Facilitates the redirection of clients to other servers when needed

If you have Sun Ray dedicated interconnects, all services required by Sun Ray clients should be provided by multiple, redundant servers to ensure continuity of Sun Ray service in the case of a network or system failure. For example, you must configure DHCP (IP address assignment and configuration) or DNS (name resolution) on all servers.



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 will fail to operate properly.

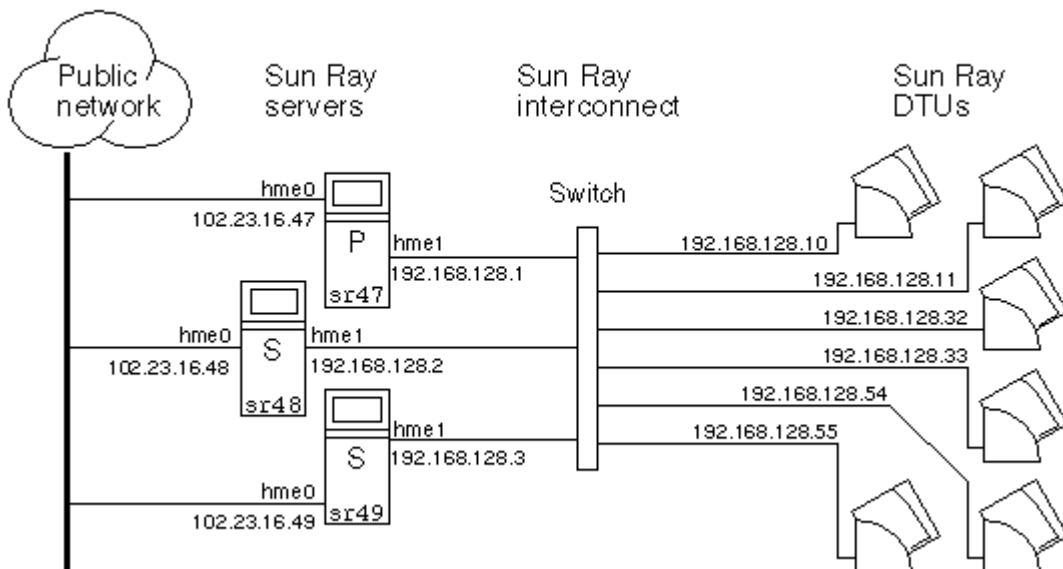
Network Topologies

A failover group can consist of servers in either a common, dedicated interconnect or servers within a LAN. 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. This key must be configured to be identical on each server.

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. Routers should not be attached to a dedicated interconnect. The failover environment supports the same interconnect topologies that are supported by a single-server Sun Ray environment; however, switches should be multicast-enabled.

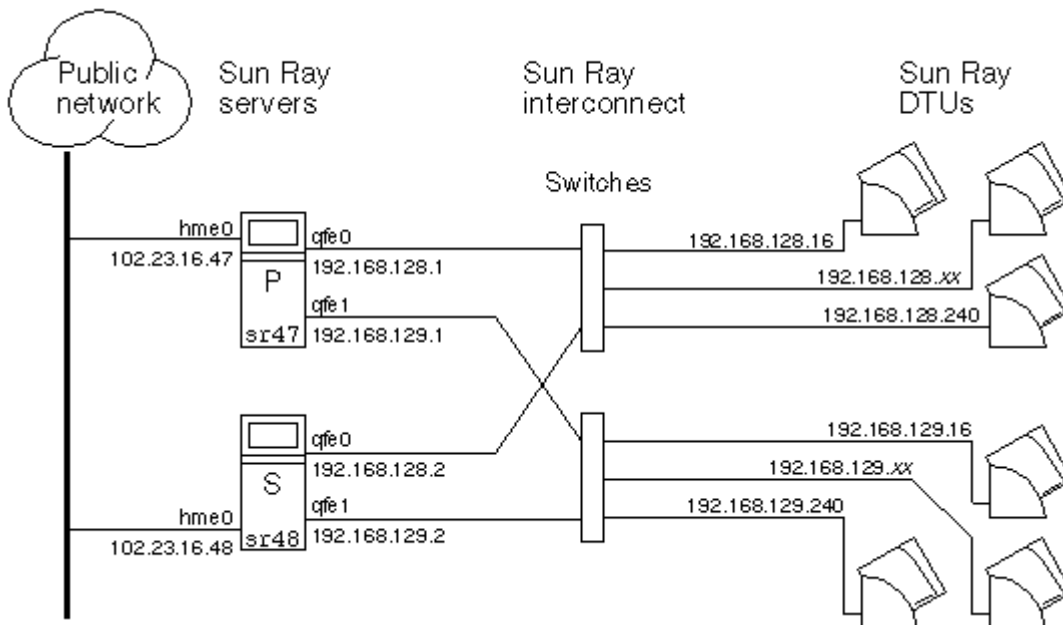
If multicast does not work in your network, you may use broadcast instead. To disable multicast, use the `enableMulticast` property in the `auth.props` file. In special cases, you may configure an explicit list of group servers using `utgmtarget`. For example, you would use `utgmtarget` to integrate servers on a different subnet into a failover group. Communication to these servers use unicast. Note that adding such a server to the group will require a restart of the entire server group.

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 session exists, 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.

Redundant Failover Group



The redundant failover group, shown in the illustration above, 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, and so on) are not shown.

Using Different Sun Ray Server Software Versions

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.



Note

When multiple versions of Sun Ray Server Software are used in a failover group, the primary server should run the oldest of the versions in use. Otherwise, the presence of a newer feature on the primary server might prevent proper replication of the Sun Ray Data Store to secondary servers that are running older versions.

Authentication Requirements

All of the servers in a failover group should use the same authentication mechanism and name service. For example, a failover group should not use one server with NIS authentication and other servers with NIS+ authentication.

If a failover group does have different authentication mechanisms, the servers might fail to obtain their existing non-smart card mobile (NSCM) sessions if a username contains the same characters but the case is different, for example, `ps121664`, `PS121664`, or `Ps121664`.

Configuring Failover Groups

When configuring failover groups, 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, by using `utadm -f` to take the server offline.

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.

For more information about how to set up multiple failover groups that use regional hotdesking, see [Managing Hotdesking](#).

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.



Caution

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 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 tracks 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 the server was booted
- IP information for every interface the server can reach
- Machine information, such as the number and speed of CPUs, configured RAM, and so on
- Load information, such as the CPU and memory utilization, number of sessions, and so on

The last two items are used to facilitate load distribution. For more information, see [Load Balancing](#).

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, because either the network connection or the server is probably down.

Redirection

In addition to automatic redirection at authentication, you can use the `utselect` or `utswitch` command for manual redirection.



Note

The `utselect` GUI is the preferred method to use for server selection. For more information, see the `utselect` man page.

Group Manager Configuration

The Authentication Manager configuration file, `/etc/opt/SUNWut/auth.props`, contains properties used by the Group Manager at runtime.

The properties are:

- gmport
- gmKeepAliveInterval
- enableGroupManager
- enableLoadBalancing
- enableMulticast
- multicastTTL
- gmSignatureFile
- gmDebug
- gmTarget



Note

These properties have default values that are rarely changed. Only very knowledgeable Sun support personnel should direct customers to change these values to help tune or debug their systems. Any properties that are changed must be changed for all servers in the failover group because the `auth.props` file must be the same on all servers in a failover group.

Property changes do not take effect until the Authentication Manager is restarted, which you can do by performing a [warm restart of the Sun Ray Services](#).

Load Balancing

When a server in a failover group fails, the Group Manager on each remaining server distributes the failed server's sessions among the remaining servers.

When the Group Manager receives a token from a Sun Ray DTU for which no server owns an existing session, it redirects the DTU. This redirection is determined according to the result of a load-sensitive session placement lottery conducted among the servers in the group, based on each server's capacity (number and speed of its CPUs), load, number of sessions, and other factors.



Note

Load balancing is handled automatically, as described. The administrator may choose to turn load balancing off but cannot assign values or otherwise modify the algorithm.

How to Turn Off the Load Balancing Feature

In the `auth.props` file, set `enableLoadBalancing` to `false`.

Task Map - Managing Failover Groups

For more information about failover groups, see [About Failover Groups](#).

Initial Configuration

Step	Description	Task
1	Set up server addresses and client addresses, and how to configure DHCP.	Set Up IP Addressing How to Set Up IP Addressing on Multiple Servers, Each with One Sun Ray Interface
2	Use the <code>utreplica</code> command to designate a primary server, advise the server of its administration primary status, and designate the host names of all the secondary servers.	How to Configure a Primary Server
3	Use the <code>utreplica</code> command to advise each secondary server of its secondary status and the host name of the primary server for the group.	How to Add a Secondary Server
4	Synchronize secondary servers with their primary server to make troubleshooting easier. Use <code>crontab</code> to schedule this command to execute periodically.	How to Synchronize Primary and Secondary Sun Ray Servers

5	Change the group manager signature.	How to Change the Group Manager Signature
---	-------------------------------------	---

Related Tasks

Task	Description
How to Take a Server Offline and Online	Explains how to take servers offline to make maintenance easier.
How to Show the Current SRDS Replication Configuration	Explains how to display the current SRDS configuration.
How to Remove the Replication Configuration	Explains how to remove the replication configuration.
How to View Network (Failover Group) Status	Explains how to view failover group status.
Recovery Issues and Procedures	Explains how to recover primary and secondary servers if they fail.

Setting Up IP Addressing

You can use the `utadm` command to set 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, see the `utadm` man page.

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 the number of Sun Ray DTUs. Consider the situation of 5 servers and 100 Sun Ray DTUs. If one of the servers fails, the remaining DHCP servers must have enough available addresses so that every "orphaned" Sun Ray DTU is assigned a new working address.

The following table lists configuration settings used to configure 5 servers for 100 Sun Ray DTUs, accommodating the failure of two servers (class C) or four servers (class B).

Configuring 5 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 setup requires 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

**Note**

If all available DHCP addresses are allocated, a Sun Ray DTU could request an address and still not find one available, perhaps because another unit has been allocated IP addresses by multiple servers. To prevent this condition, provide each DHCP server with enough addresses to serve all the Sun Ray 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 servers respond 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 a session for the token exists 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 information about explicit switching, see [Group Manager](#).

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 that 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, which is the default behavior for most routers.



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 issue "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.

How 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.

The table below lists the options available for the `utadm` command. For additional information, see the `utadm` man page.

Available Options

Option	Definition
<code>-c</code>	Create a framework for the Sun Ray interconnect.
<code>-r</code>	Remove all Sun Ray interconnects.
<code>-A <subnetwork></code>	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.
<code>-a <interface_name></code>	Add <code><interface_name></code> as Sun Ray interconnect.
<code>-D <subnetwork></code>	Delete the subnetwork specified from the list of configured Sun Ray subnetworks.
<code>-d <interface_name></code>	Delete <code><interface_name></code> as Sun Ray interconnect.
<code>-l</code>	Print the current configuration for all the Sun Ray subnetworks, including remote subnetworks.
<code>-p</code>	Print the current configuration.
<code>-f</code>	Take a server offline
<code>-n</code>	Bring a server online
<code>-x</code>	Print the current configuration in a machine-readable format

How to Configure a Primary Server

Layered administration of the group takes place on the primary server, where the master copy of SRDS resides. The `utreplica` command designates a primary server, advises the server of its administration primary status, and tells it the host names of all the secondary servers.

The term primary server reflects the replication relationship, not the failover order.

Adding or removing secondary servers requires services to be restarted on the primary server. In large failover groups, and significant loads may be pushed onto the primary server from various sources. In addition, runaway processes from user applications on the primary can degrade the health of the entire failover group. Failover groups of more than four servers should have a dedicated primary server devoted to solely serving the Sun Ray Data Store, i.e., not hosting any Sun Ray sessions.

Before You Begin

- Configure the primary server before you add the secondary servers.
- The purpose of a dedicated primary server is to serve the Sun Ray Data Store. Specifying a dedicated primary server enables secondary servers to be added or removed without disturbing user sessions. To specify a dedicated primary server, do not run `utadm` on the server.
- (Linux Only) If a common home directory is mounted on machines with different GNOME versions, conflicts between or among the versions cause unpredictable behavior. Do not try to use multiple GNOME versions with a common home directory.

Steps

1. Log in as superuser on the primary Sun Ray server.
2. Configure this server as the primary Sun Ray server and identify all secondary servers.

```
# /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.

The `utreplica` script:

- Stops and starts the Sun Ray services
- Reads the Authentication Manager policy

When the script ends, a log file is available at:

For Solaris:

```
/var/adm/log/utreplica.<year><month><date><hour>:<minute>:<second>.log
```

For Linux:

```
/var/log/SUNWut/utreplica.<year><month><date><hour>:<minute>:<second>.log
```

Next Steps

When you are finished, see [How to Add a Secondary Server](#).

How to Add a 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.

How to Add a Secondary Server

1. If the secondary server has not been configured on the primary server, become superuser on the primary server and rerun the `utreplica` command with the new secondary server.

```
# /opt/SUNWut/sbin/utreplica -p -a <secondary-server1> [<secondary-server2>...]
```

where `<secondary_server1> [<secondary_server2>...]` is a space-separated list of unique host names of the secondary servers.

2. Become superuser on the secondary server.
3. Add the secondary server.

```
# /opt/SUNWut/sbin/utreplica -s <primary-server>
```

where `<primary-server>` is the host name of the primary server.

How to Synchronize Primary and Secondary Sun Ray Servers

Log files for Sun Ray servers contain time-stamped error messages that can be difficult to interpret if the time is out of sync. To make troubleshooting easier, make sure that all secondary servers periodically synchronize with their primary server.

The Network Time Protocol (NTP) is the recommended protocol to synchronize primary and secondary servers. With NTP, you can synchronize to an absolute time source and it provides additional synchronization capabilities. In some deployments, the simpler TIME protocol configured through the `rdate` command may be sufficient.

For detailed information about configuring NTP on Solaris servers, see [Solaris 10 System Administration Guide: Network Services](#).



Note

Both the NTP and TIME protocols are disabled by default on Solaris servers.

How to Change the Group Manager Signature

The `utconfig` command asks for a group manager 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 meet the following criteria:

- Owned by root with only root permissions
- Contain at least eight characters, in which at least two characters are letters and at least one character is not



Note

For slightly better security, use long passwords.

Steps

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 the signature twice identically for acceptance.
3. For each Sun Ray server in the group, repeat the previous two steps.

**Note**

Be sure to use the `utgroupsig` command rather than any other method to provide the signature. `utgroupsig` also ensures proper internal replication.

How to Take a Server Offline and Online

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.

How to Take a Server Offline

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

How to Take a Server Online

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

How to Show the Current SRDS Replication Configuration

As superuser, open a shell window and type:

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

The result indicates whether the server is stand-alone, primary (with the secondary host names), or secondary (with the primary host name).

How to Remove the Replication Configuration

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

How to View Network (Failover Group) Status

A failover group is a set of Sun Ray servers all running the same release of Sun Ray Server Software and all having access to all the Sun Ray DTUs on the interconnect.



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

Command-Line Step

- To view the failover group status for the local Sun Ray server:

```
# utgstatus
```

Admin GUI Steps

1. Click the Servers tab.

2. Select a server name to display its Server Details screen.
3. Click View Network Status.

The Network Status screen appears, as shown below.

VERSION LOG OUT HELP

User: admin Server: srsdemo-01

Sun Ray Administration

Sun™ Microsystems, Inc.

Servers Sessions Desktop Units Tokens Advanced Log Files

All Servers > srsdemo-01 > Network Status

srsdemo-01 - Network Status Back to srsdemo-01

This page lists the network status of all trusted servers from the perspective of the selected server.


Network Status (2)			
10.6.133.0/24			
Server Name	Address	Status	Type
srsdemo-01	10.6.133.148	Up	LAN
Trusted Servers			
srsdemo-02	10.6.133.171	Up	LAN

Back to srsdemo-01

The Network Status screen provides information on group membership and network connectivity for trusted servers, which are those servers in the same failover group.

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.


 When the primary server fails, you cannot make administrative changes to the system. For replication to work, all changes succeed on the primary server.

Primary Server Recovery

You can use several strategies for recovering the primary server. The following procedure is performed on the server that was the primary server after it is fully operational again.

How to Rebuild the Primary Server's Administration Data Store

Use this procedure to rebuild the primary server's data store from a secondary server. This procedure uses the same host name for the replacement server.

 Be sure to set `umask` appropriately before running `utldbmcad`. Otherwise, unprivileged users can gain access to the `utadmin` password.

Steps

1. On one of the secondary servers, capture the current data store to a file called `/tmp/store`.

```
# /opt/SUNWut/srds/lib/utldbmcats
/var/opt/SUNWut/srds/dbm.ut/id2entry.dbb > /tmp/store
```

This command provides an LDIF format file of the current data store.

2. Use FTP to send this file to the `/tmp` directory on the primary server.
3. Follow the [SRSS installation instructions](#).
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/utldif2ldbmcats -c -j 10 -i /tmp/store
```

This command 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.

How to Replace the Primary Server with a Secondary Server



Note

This procedure is also known as promoting a secondary server to primary.

Steps

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 command 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

If a secondary server fails, administration of the group can continue. A log of updates is maintained and applied automatically to the secondary server once it has recovered. If the secondary server needs to be reinstalled, repeat the steps described in [Installing](#).

Contents

- [About Hotdesking](#)
 - [Regional Hotdesking](#)
 - [Regional Hotdesking Process](#)
 - [Site Requirements](#)
 - [Providing Site Integration Logic](#)
 - [Remote Hotdesk Authentication \(RHA\)](#)
 - [How to Configure a Site-specific Mapping Library](#)
 - [How to Configure the Token-based Mapping Implementation Provided as a Sample](#)
 - [How to Configure the User Name-based Mapping Implementation Provided as a Sample](#)
 - [How to Configure a Script-based Back-end Mapping](#)
 - [How to Perform a cold Restart of the SRSS Services](#)
 - [How to Use Token Readers with Regional Hotdesking](#)
 - [How to Configure the Sample Data Store](#)
 - [How to Disable and Re-enable Remote Hotdesk Authentication](#)
 - [How to Disable RHA](#)
 - [How to Re-enable RHA](#)
-

Managing Hotdesking (All Topics)

About Hotdesking

Hotdesking, or session mobility, is the ability for a user to remove a smart card, insert it into any other DTU within a failover 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. Every Sun Ray DTU is equipped with a smart card reader.

**Note**

On Solaris platforms, the Sun Ray system also provides Non-Smart Card Mobility (NSCM), or hotdesking without smart cards. For more information, see [Managing NSCM Hotdesking \(Solaris\)](#).

Regional Hotdesking

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.

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.

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.

Regional Hotdesking Process

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

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

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

Site Requirements

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

**Note**

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

Providing Site Integration Logic

To determine where given Sun Ray DTUs or users should be connected when creating or accessing sessions, the administrator must utilize enterprise data. Sun Ray Server Software includes the following software 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.

Remote Hotdesk Authentication (RHA)

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

If the Remote Hotdesk Authentication (RHA) feature is enabled and a reconnection is attempted, the Sun Ray Server Software creates a temporary new session for the DTU and uses that session to present an authentication dialogue to the user. (This RHA dialogue looks very similar to the NSCM authentication dialogue.) After the user has successfully authenticated to the dialogue, the temporary session is dismissed and the user's existing session is connected to the DTU.

RHA is designed to provide a more secure hotdesk experience than the previous hotdesk authentication model, which relied on authentication performed by a desktop screen lock in the user's existing session. (The "Remote" in RHA refers to the fact that the hotdesk authentication step takes place outside the user's existing session.) However, for environments where the in-session screen lock provides acceptable security or where no hotdesk authentication is desired, Sun Ray Server Software can be configured to turn the RHA security feature off.

Authentication does not apply to anonymous Kiosk Mode.

**Note**

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

How 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, or one of the sample implementations provided with the SRSS software.

**Note**

If you are using a Linux platform, library mapping for the 32-bit platform should be `/opt/SUNWutref/amgh/lib`, as shown below, and library mapping for the 64-bit platform should be `/opt/SUNWutref/amgh/lib64`.

How to Configure the Token-based Mapping Implementation Provided as a Sample

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

How to Configure the User Name-based Mapping Implementation Provided as a Sample

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

How to Configure a Script-based Back-end Mapping

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

How to Perform a cold Restart of the SRSS Services

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

How to Use Token Readers with Regional Hotdesking

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

Configured token readers should have the following value formats:

Key	Value
<code>insert_token</code>	<code>pseudo.MAC_address</code>
<code>token</code>	<code>TerminalId.MAC_address</code>

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

**Note**

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

How 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.

To create the back-end database file under `/opt/SUNWutref/amgh/back_end_db` on the Sun Ray server, do the following:

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

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

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

- 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 no token match is made (or if no `username` is included in the matches) the user is prompted for a `username`.
- A lookup is made for this `username`. 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
```

How to Disable and Re-enable Remote Hotdesk Authentication

The following procedures describe how to disable and re-enable RHA.

How to Disable RHA



Note

Disabling the RHA feature may present a security risk under some circumstances.

1. To disable RHA configuration for a group, type the following command:

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

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

2. Perform a cold restart of the SRSS services:

```
# utrestart -c
```

How to Re-enable RHA

1. Restate your policy using `utpolicy` without the `-D` option.

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

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

2. Perform a cold restart of the SRSS services:

```
# utrestart -c
```

Contents

- [About NSCM Hotdesking](#)
 - [NSCM Session](#)
 - [Sun Ray Mobile Session Login Dialog Box](#)
 - [NSCM and Failover Groups](#)
 - [How to Enable NSCM Sessions](#)
 - [Admin GUI Steps](#)
 - [Command Line Steps](#)
 - [How to Log In to an NSCM Session](#)
 - [Session Redirection](#)
 - [How to Disconnect a DTU Session](#)
-

Managing NSCM Hotdesking on Solaris (All Topics)

About NSCM Hotdesking

Configuring Sun Ray Server Software with non-smart card mobile (NSCM) sessions provides the benefits of hotdesking without the use of smart cards. This section explains NSCM sessions, how to configure them, and how to enable users to access their Sun Ray sessions across multiple failover groups.

For information about Regional Hotdesking or Remote Hotdesk Authentication, which NSCM can utilize, see [About Hotdesking](#).

NSCM Session

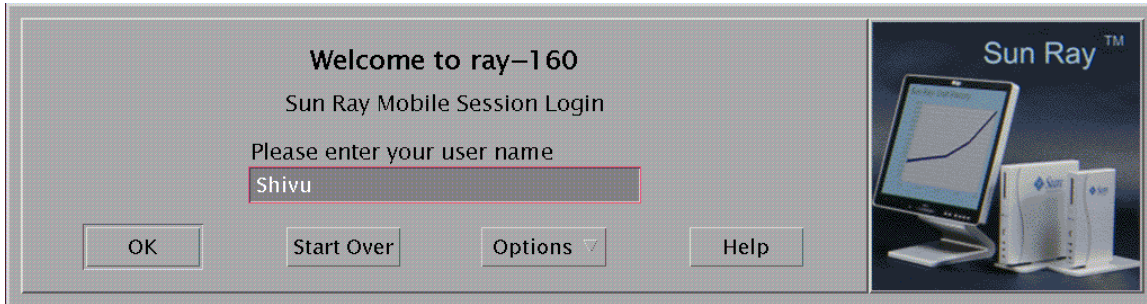
In an NSCM session, the user can:

- Type a user name and password instead of inserting a smart card.
- Type the `utdetach` command instead of removing a smart card.

If a user does not want to use the NSCM session, inserting a smart card causes the session to be disconnected and replaced by a smart card session.

Sun Ray Mobile Session Login Dialog Box

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



Right clicking the Options button displays a panel with the following options:

- QuickLogin - Applicable only to a new session only. Selecting Off enables the user to log in with the same options available through `dtlogin`. Selecting On enables the user to bypass the option selection phase. QuickLogin is on by default.
- Exit - Selecting Exit temporarily disables the NSCM session. An escape token session is started, and the dialog box is replaced by the `dtlogin` screen. A user without a valid account in this server group can exit to the `dtlogin` dialog and attempt a remote X (XDMCP) login to some other server where that user has a valid account.

NSCM and Failover Groups

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

The following situations might produce unfamiliar behavior:

- Load Balancing Between Servers - If server A is heavily loaded when a user logs into it with the NSCM GUI, the server redirects the user to server B.
- Switching Between Servers - A user with a session on server A who wants to switch to a session on server B invokes the `utselect` GUI to access the other session. In doing so, the user is required to log in with the NSCM GUI. Users familiar with the ease of the `utselect` GUI might be displeased that another login is necessary.
- Escape Token Sessions - The user bypasses the NSCM GUI by clicking the Exit button and logs into server A using `dtlogin`. The user now has a standard escape token session and invokes the `utselect` GUI to switch to server B, causing the NSCM GUI to be presented again. The user must click Exit again to get to the escape token session on server B. Users accustomed to switching rapidly might find this behavior annoying.

How to Enable NSCM Sessions

The Sun Ray administrator can toggle the NSCM session capability by choosing whether to include the `-M` argument with the `utpolicy` command. For more information, see the `utpolicy` man page.

Admin GUI Steps

1. Use the `utwall` command to inform your users that all active and detached sessions will be lost.

For example:

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

The following message is displayed in a pop-up window for all users:

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

2. Log in to the Admin GUI.
3. Go to the System Policy tab.
4. In the Non-Card Users panel, select the Enabled option next to Mobile Sessions.
5. Go to the Servers tab.

- Click Cold Restart to restart Sun Ray services and terminate all users' sessions.

Command Line Steps

- Use the `utwall` command to inform your users that all active and detached sessions will be lost.

For example:

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

The following message is displayed in a pop-up window for all users:

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

- As superuser, type the `utpolicy` command with the `-M` argument for your authentication policy.

For example:

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

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

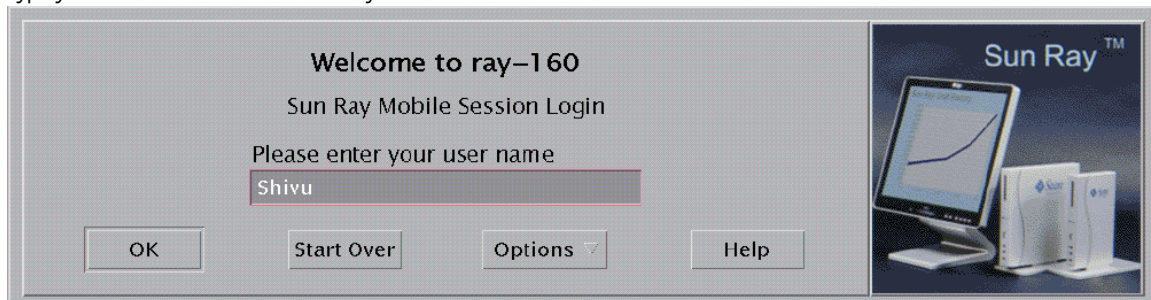
- Initialize Sun Ray services by restarting the Authentication Manager on the server, including each secondary Sun Ray server if in a failover group.

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

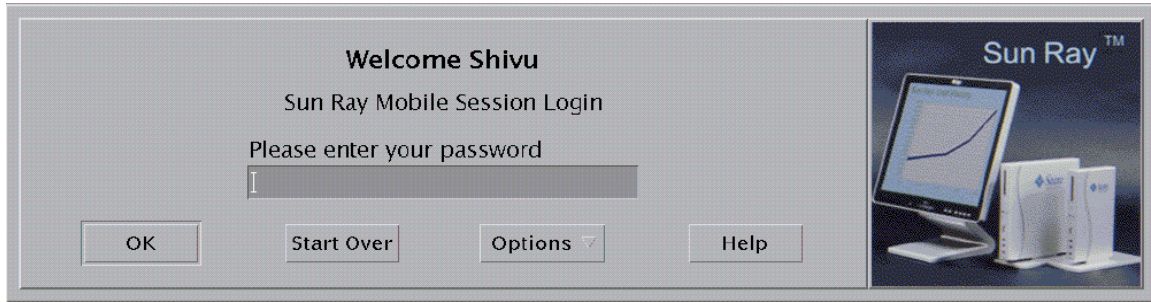
This command clears all active and detached sessions.

How to Log In to an NSCM Session

- Type your user name into the user entry field.



- Type your password into the password field.



If no NSCM session exists for this user, the Authentication Manager creates an NSCM session token with the format: `mobile.IEE802-MACID`.

Session Redirection

The user might be redirected to another server for the following reasons:

- If the Sun Ray server is part of a failover group, the load-balancing algorithm might redirect the user to another Sun Ray server.
- If the user has an NSCM session on a different Sun Ray server in a failover group, the user will be redirected to the server with the most current NSCM session.

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

How to Disconnect a DTU Session



Note

NSCM and RHA sessions are disconnected if the screen lock idle time interval is exceeded. See [Mass Storage Devices \(Linux\)](#) and [Mass Storage Devices \(Solaris\)](#).

You can disconnect a DTU session through any of the following methods:

- Lock the session through the current desktop manager. For example, in the Java Desktop System, choose Launch->Lock Screen.
- Type the following command:

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

- Press `Shift+Pause`.
To change the disconnect hot key combination, see [Sun Ray DTU Hot Keys](#).



Note

The hot key combination does not work with a full-screen Windows session.

- Connect to your session through another DTU, either by inserting your smart card and authenticating to RHA or by logging in through NSCM.

Contents

- [About Kiosk Mode](#)
 - [Kiosk Mode Security and Failover Considerations](#)
 - [Task Map - Managing Kiosk Mode](#)
 - [How to Configure Kiosk Mode](#)
 - [How to Configure a Kiosk Mode Session Type](#)
 - [How to Add an Application to a Kiosk Session Type](#)
 - [How to Enable and Disable Kiosk Mode](#)
 - [How to Override the Default Kiosk Mode Policy](#)
 - [How to Add Kiosk User Accounts](#)
-

Managing Kiosk Mode (All Topics)

About Kiosk Mode

Kiosk Mode enables controlled, simplified, and unauthenticated access to anonymous users without compromising the security of the Sun Ray server. Unauthenticated access is useful in settings such as public kiosks, where users cannot be expected to provide authentication credentials. When authentication is expected to be carried out by other means than the standard UNIX login, Kiosk Mode is all but indispensable. A good example of this situation is using the [Sun Ray Connector for Windows OS](#).



Note

Kiosk Mode is an optional component that might require additional installation steps. Ensure that Kiosk Mode has been configured with the `utconfig` command and that at least one session descriptor has been installed on the Sun Ray server. A session descriptor is a file that defines, at a minimum, an executable to be launched as the user session. All session descriptors are located in the `/etc/opt/SUNWkio/sessions` directory.

You can use the Admin GUI to configure Kiosk Mode. On the Kiosk Mode tab, accessed from the under Advanced tab, you can choose a predefined session type. You can also specify other general properties that control kiosk mode behavior, such as Timeout, Maximum CPU Usage, and Maximum VM Size.

Some session types allow additional Kiosk applications to be launched. Not all session types support this ability. For example, a Kiosk full-screen web browser session does not need to have this capability. The applications table on the Kiosk Mode page is displayed or hidden depending on what session type is selected.

You can add a new Kiosk application by clicking the New button in the applications table and specify it using either a predefined application descriptor file or by specifying the path to an executable or an application descriptor on the server. All predefined application descriptors are located in the `/etc/opt/SUNWkio/applications` directory.

For a detailed explanation of Kiosk Mode functionality, see the `kiosk` man page.

Kiosk Mode Security and Failover Considerations

Because 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, but applications that do not are 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 access is not desirable in a public environment and is not advised. However, using a custom application for a call center is perfectly acceptable.

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

Task Map - Managing Kiosk Mode

Task	Description
How to Configure Kiosk Mode	Explains how to initially configure the Kiosk Mode feature.
How to Configure a Kiosk Mode Session Type	Explains how to configure the Kiosk Mode session type.
How to Enable and Disable Kiosk Mode	Explains how to specify what types of session types are available to users, based on policy choices for different types of users and usage scenarios.
How to Override the Default Kiosk Mode Policy	Explains how to override the default Kiosk Mode policy or Kiosk Mode session type by using the <code>utkioskoverride</code> command.
How to Add an Application to a Kiosk Session Type	Explains how to add applications to a Kiosk Mode session type to extend the Kiosk Mode functionality.

How to Configure Kiosk Mode

As part of the [initial configuration of the Sun Ray server software](#), you are given the opportunity to initially configure Kiosk Mode. The initial Kiosk Mode configuration consists of configuring the Kiosk user accounts.

If you don't initially configure Kiosk Mode, you can always use the `utconfig -k` command to configure it later. You can also perform additional Kiosk Mode account management tasks by using the `kioskuseradm(1M)` command.

How to Configure a Kiosk Mode Session Type

Once you have selected a Kiosk session, that session is launched by default to provide basic Kiosk Mode functionality.

This procedure describes how to configure a Kiosk Mode session type, which determines what type of session is launched in Kiosk Mode. For information about Kiosk Mode security and failover considerations, see [About Kiosk Mode](#).

Admin GUI Steps



Note

Kiosk session and application configuration data created with the Admin GUI is stored as the default Kiosk session type under the name `session`. To store non-default Kiosk session types, use the `utkiosk` command on the command line.

1. Click the Advanced tab.
2. Click the Kiosk Mode tab from the Advanced tab, as shown in the following figure.

The screenshot shows the 'Edit Kiosk Mode' configuration window in the Sun Ray Administration GUI. The window title is 'Edit Kiosk Mode' and it includes the instruction: 'Specify the session type and general properties for Kiosk Mode. Click OK to store the changes.' The configuration fields are as follows:

- Session:** A dropdown menu with 'Sun Java Desktop System 3' selected.
- Timeout:** A dropdown menu with 'Common Desktop Environment (Obsolete)' selected.
- Maximum CPU Time:** An input field with 'seconds' as the unit.
- Maximum VM Size:** An input field with 'KB' as the unit.
- Maximum number of Files:** An input field.
- Maximum File Size:** An input field with '512B blocks' as the unit.
- Locale:** An input field.
- Arguments:** A text input field.

A yellow box highlights the 'Choose Session Type' button. At the bottom right, there are 'OK' and 'Cancel' buttons.

3. Click the Edit button.
4. Select your preferred Kiosk Session (Session Type) from the drop-down list, as shown in the figure.
5. Provide appropriate values for the remaining settings, which are described in the following table. For more information, see the `ulimit` man page.

**Caution**

Choosing unsuitable values for `ulimit` settings could cause Kiosk sessions to start incorrectly or to crash due to lack of resources.

Value	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.
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.
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.
Maximum File Size	Indicates the maximum file size per process for Kiosk sessions. By default, the system default is applied to all Kiosk sessions.
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 setting is specific to the Kiosk session. For more information about supported arguments, consult the session-specific documentation for your selected session.

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, you do not have to restart Sun Ray services for changes to take effect.

Command Line Steps

1. Create a session configuration file.

- a. To start with an existing configuration, export the settings to a file. For example:

```
utkiosk -e session -s > mysession.conf
```

- b. Edit the `mysession.conf` file.

See the `session.conf` man page for a description of available settings. The following example uses the [Sun Ray Windows Connector kiosk session](#):

```
KIOSK_SESSION=uttsc
KIOSK_SESSION_LIMIT_VMSIZE=20000
KIOSK_SESSION_ARGS=-h -- -r sound:low -E theming winserver.example.org
```

2. If applicable, create an application list file.

If you are using a kiosk session that can serve as a container for multiple applications, you should create an application list file.

- a. To start with existing settings, export the application list to a file:

```
utkiosk -e session -a > myapps.list
```

- b. Edit the `myapps.list` file.

See the `kiosk` man page for a description of application list files.

3. Import your settings into the Sun Ray Data Store.

- To import your session settings without an application list as the default session configuration:

```
utkiosk -i session -f mysession.conf
```

- To import your session settings and application list as the default session configuration:

```
utkiosk -i session -f mysession.conf -A myapps.list
```

- To import your session settings as non-default session configuration:

```
utkiosk -i MySpecialSession -f mysession.conf
```

How to Add an Application to a Kiosk Session Type

Some Kiosk session types, including the predefined JDS3 and CDE Kiosk session types, support the addition of applications to extend the basic functionality.



Note

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

Admin GUI Steps

1. Click the Advanced tab.
2. Click the Kiosk Mode tab from the Advanced tab.
If the currently selected Kiosk session supports the addition of applications, an Applications setting is displayed at the bottom of the page.
3. Click the New button.
 - To use one of the predefined Kiosk application descriptors:
 - a. Select Predefined Descriptor.
 - b. Choose the relevant descriptor from the drop-down menu.
 - To define a custom Kiosk application descriptor:
 - a. Select Custom Path to use your own custom Kiosk application descriptor or a system application.
 - b. Type 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.
4. Select your preferred Start Mode for the application.
 - USER allows users to start the application themselves, for instance from a menu or launcher item.
 - AUTO makes the application start automatically when the Kiosk session starts.
 - CRITICAL makes the application start automatically when the Kiosk session starts, allows users to start the application themselves, and forces the Kiosk session to restart if the application terminates.
5. Provide any application specific arguments.



Note

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

Command-Line Steps

Refer to steps 2 and 3 in the [How to Configure a Kiosk Mode Session Type](#) procedure.

If you use the command line, you must manually determine if a session type supports applications. This is done automatically by the Admin GUI.

1. List the session types configured in SRSS.

```
$ session_type=`/opt/SUNWut/sbin/utkiosk -e session -s | sed -n 's/^KIOSK_SESSION=//p'`
```

2. Check whether the session type supports applications.

```
$ /opt/SUNWkio/bin/kioskdesc print -s $session_type | grep '^KIOSK_SESSION_APPLAUNCHER='
```

How to Enable and Disable Kiosk Mode

Kiosk Mode enables the administrator to specify a session that is available to users without first authenticating to the Sun Ray server.

Kiosk Mode can be enabled as the default session type for smart card users, non-smart card users, or both. When Kiosk is enabled for a class of tokens, this choice can be overridden for individual tokens. For example when Kiosk Mode is enabled for card users, regular non-Kiosk session access can be configured for individual cards. Alternatively a kiosk session other than the default kiosk session can be configured for individual tokens. Enabling and disabling Kiosk Mode for individual tokens is described in [How to Override the Default Kiosk Mode Policy](#).

Before enabling Kiosk Mode, you must configure the Kiosk Mode. See [Task Map - Managing Kiosk Mode](#) for details.

Admin GUI Steps

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 options to enable Kiosk Mode for smart card users, non-smart card users, or both. See [Administration Tool \(Admin GUI\)](#) for more information.

Command-Line Steps

1. Become superuser on the Sun Ray server.
2. Enable a kiosk mode through the `utpolicy -k` command.

The following options determine whether access to the Sun Ray server is granted to certain tokens:

```
-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.

Examples

The examples below demonstrate how to enable Kiosk Mode from the command line.

How to Enable Kiosk Mode for All Users (Smart Card and Non-Smart Card)

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

All users are directed to Kiosk sessions.

How to Allow Only Smart Card Sessions in Kiosk Mode

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

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

How to Enable Kiosk Mode for Smart Card Users Only

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

Only smart card users are directed to Kiosk sessions.

How to Enable Kiosk Mode for Non-Smart Card Users Only

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

Only non-smart card users are directed to Kiosk sessions.

How to Enable Regular Sessions for Smart Card Users and Kiosk Sessions for Non-Smart Card Users

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

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

How to Enable Regular Sessions for Registered Smart Cards and Kiosk Sessions for Non-Smart Card Users

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

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

How to Enable Kiosk Sessions for Registered Smart Cards and Regular Sessions on Registered DTUs:

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

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

How 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 smart card users unless you specify overrides.

How to Override the Default Kiosk Mode Policy

Sometimes you might need to assign a different authentication policy setting for a particular smart card or Sun Ray DTU, or subset of smart cards or Sun Ray DTUs. Only tokens that have already been registered can be assigned policy overrides.

Admin GUI Steps



Note

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

1. Click the Tokens tab as shown in the following figure.

2. Select the token of interest from the list of tokens.
This token can be a card owner's smart card token or a pseudo-token associated with a DTU's MAC address. However, only tokens that have been registered in the Sun Ray Data Store can be overridden. For more information, see [How to Register a Token](#) and [How to Register a Pseudo-Token](#).
3. Click the Edit button.
4. Select the desired Session Type from the list of available session types.
The available session types are Default, Kiosk, and Regular.
 - Select Default to prevent the Kiosk Mode policy from being overridden for this token.
 - Select Kiosk to use a Kiosk session for this token regardless of the Kiosk Mode policy.
 - Select Regular to ensure that a Kiosk session is not used for this token regardless of the Kiosk Mode policy.
5. Click the OK button.

Command-Line Steps

1. Use the `utkioskoverride` command to override the policy.

```
/opt/SUNWut/sbin/utkioskoverride
```

The following examples demonstrate how to override the Kiosk Mode policy from the command line. For more detailed information about overriding Kiosk Mode policy, see the `utkioskoverride` man page.

How to Enable Kiosk Sessions Regardless of the Kiosk Mode Policy for a Registered Smart Card

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

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

How to Disable Kiosk Session Regardless of the Kiosk Mode Policy for a Registered Smart Card

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

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

How to Disable Kiosk Sessions Regardless of the Kiosk Mode Policy for a Logical Token

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

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

How to Assign and Enable a Non-Default Kiosk Session

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

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

How to Add Kiosk User Accounts

This procedure describes how to add more Kiosk user accounts to the user account pool. You can increase the number of Kiosk user accounts even while there are existing Kiosk sessions.



Note

This procedure may not work if any user accounts were added after the configuration of the initial pool of Kiosk user accounts. The `kioskuseradm extend` command relies on Kiosk user accounts with contiguous user IDs.

To work around this issue, you must delete all the Kiosk user accounts and recreate them by using the `kioskuseradm delete` and `kioskuseradm create` commands, respectively. This process requires you to stop the Sun Ray services on the Sun Ray server. If you have a failover group, performing these steps on each Sun Ray server separately will avoid user downtime.

1. Become superuser on the Sun Ray server.
2. Increase the number of Kiosk user accounts.

```
# /opt/SUNWkio/bin/kioskuseradm extend -c <number_of_new_users>
```

Contents

- About Multihead Configurations
 - Multihead Groups
 - Multihead Screen Display
 - Creating a Single Screen Across Several Monitors (XINERAMA)
 - Session Groups
 - Authentication Manager
- Task Map - Managing Multihead Configurations
 - Initial Configuration
 - Additional Tasks
- How to Create a New Multihead Group
- How to Enable Multihead Policy
- How to Override Automatic Sizing of Screen Dimensions
- How to Restore Automatic Sizing Behavior on the Next Login
- How to Manually Set the Multihead Display Geometry
 - How to Override the Automatic Geometry
 - How to Restore the Automatic Geometry on the Next Login
- How to Enable and Disable XINERAMA
 - How to Enable XINERAMA
 - How to Disable XINERAMA
 - How to Enable XINERAMA as Default for a Single System or Failover Group
- Troubleshooting Multihead Displays

- [Multihead Video](#)
 - [Problem: The display resolution is 640 x 480.](#)
 - [How To Reset the Screen Resolution](#)
-

Managing Multihead Configurations (All Topics)

About Multihead Configurations

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 2 and 16 DTUs controlled by one keyboard and mouse may be composed of virtually any mix of Sun Ray clients. Each Sun Ray client presents an X screen of the multihead X display.

For the multihead feature to function properly:

- You must be in administered mode.
- You must run `utconfig` before you run the `utmhconfig` or `utmhadm` commands.
- You must enable the multihead policy using either the `utpolicy` command or the Admin GUI.
- Always run the `utmhconfig` command from a Sun Ray DTU.

Note the following limitations:

- The Sun Ray 2FS and Sun Ray 3 Plus clients are designed to run a single display across two screens without additional configuration. It uses 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
- H264 and VC-1 streams are synchronized with the audio stream on the DTU. In a multihead group, the audio stream is directed only to the primary DTU, so audio/video synchronization can be performed only on the primary DTU. When video is displayed on secondary DTUs, the application must perform the A/V synchronization.
- Regional hotdesking is not enabled for multihead groups.

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.

Unless XINERAMA is enabled, sessions will have a separate CDE toolbar with separate workspaces per screen. See [How to Enable and Disable XINERAMA](#) for more details. A window cannot be moved between screens. However, as noted, the Sun Ray 2FS DTU treats two attached screens as a single display, based on a single frame buffer and controlled with a single keyboard and pointer device.

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 by using a smart card to identify the terminals with the `utmhconfig` GUI utility.

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 cursor can appear to get lost when it goes to the disconnected secondary DTU.

To recover from this situation, you can do one of the following actions:

- Reconnect the missing DTU.
- Delete the multihead group using the `utmhconfig` or `utmhadm` command, replace the missing DTU, and create a new multihead group that incorporates the replacement DTU.

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 following figure indicates that the user is on the second screen of a three-screen display.



Creating a Single Screen Across Several Monitors (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.

For CDE desktop sessions, a single CDE toolbar and set of workspaces manages the configured monitors. A window including the CDE toolbar itself can span monitors, because the monitor displays are still within the same screen.

XINERAMA can also be used with the SRWC `uttscc` command.

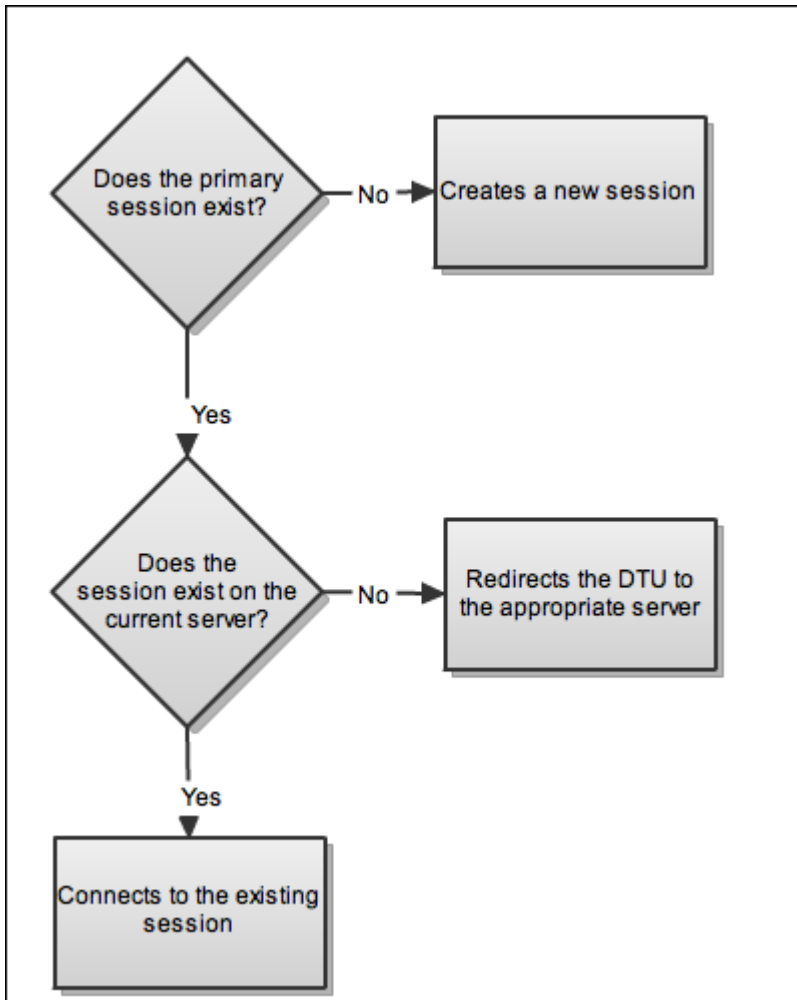
Session Groups

If you hotdesk from a multihead group to a Sun Ray 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 action 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 the DTU is not identified as part of a multihead group, it is treated normally.

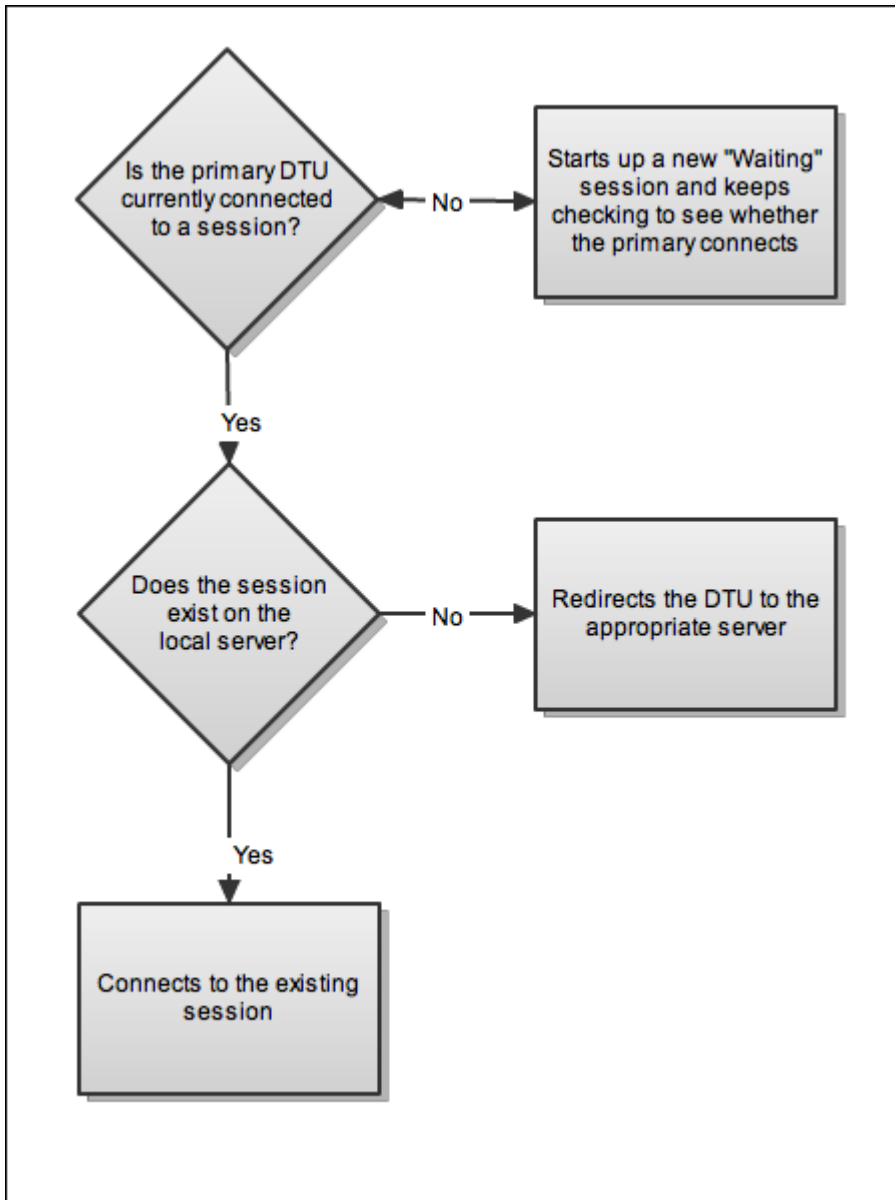
Authentication Manager Flowchart for the Primary DTU



If the DTU is recognized 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 a pre-existing session is found for the DTU or smart card on another server in the failover group, the primary DTU will be redirected to that server. If no session exists 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 recognized 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 the DTU is attached, the module redirects the secondary DTU to that server.

Authentication Manager Flowchart for the Secondary DTU



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

Task Map - Managing Multihead Configurations

Initial Configuration

Step	Task	Description
1	How to Create a New Multihead Group	Explains how to use the Multihead Administration Tool to create a new multihead group.
2	How to Enable Multihead Policy	Explains how to enable new multihead policy.

Additional Tasks

Task	Description
How to Manually Set Multihead Display Dimensions	Explains how to manually set screen dimensions for the multihead group.

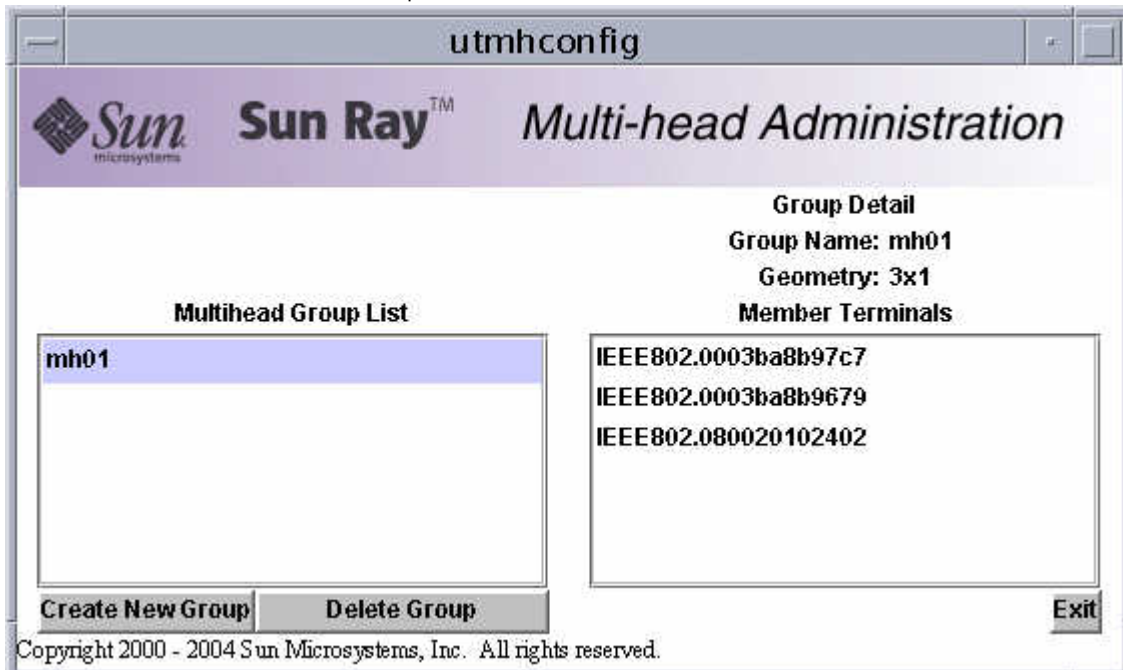
How to Manually Set the Multihead Display Geometry	Explains how to manually set how the screens are arranged in the multihead group.
How to Disable Multihead Displays for a Session	Explains how to disable multiple displays for a session.
How to Enable and Disable XINERAMA	Explains how to enable or disable XINERAMA, a feature that creates a single large screen displayed across several monitors.

How to Create a New Multihead Group

1. In the command-line interface, type:

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

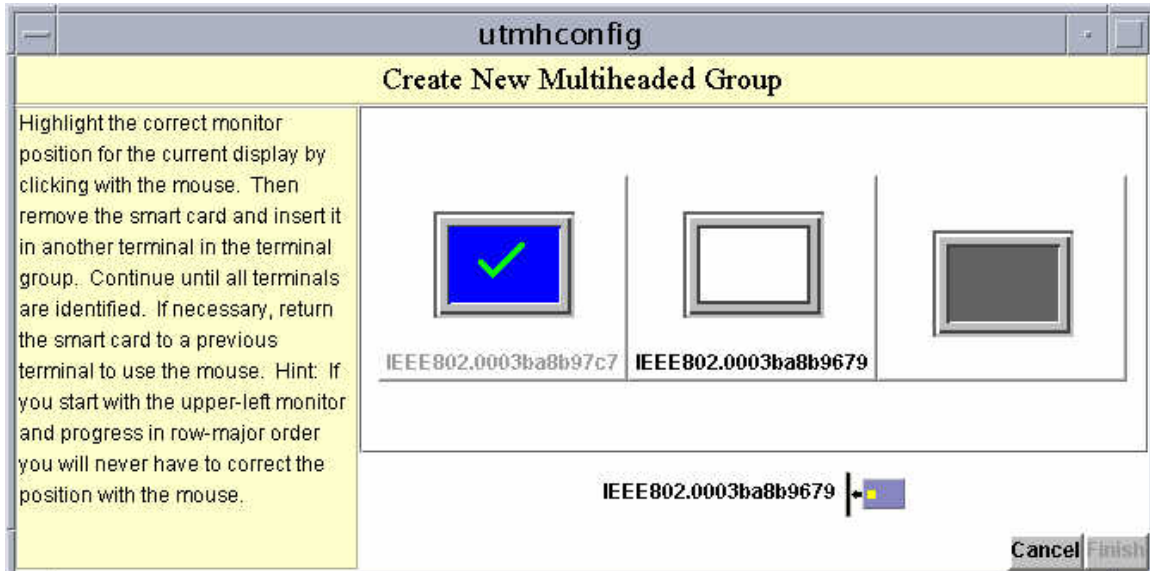
2. On the initial screen, click Create New Group.



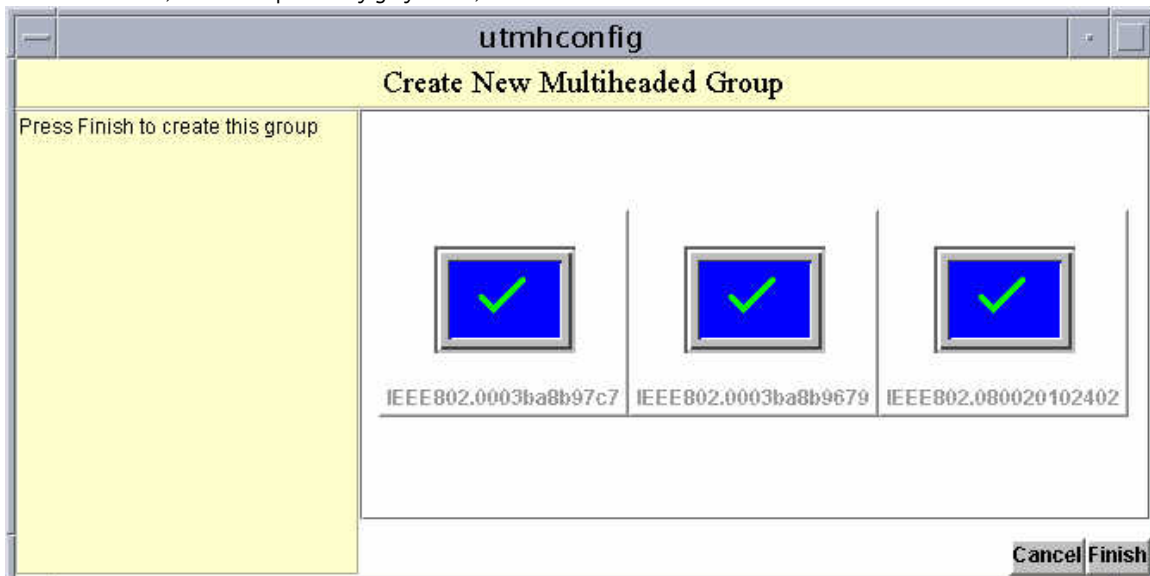
The Create New Multiheaded Group dialog box is displayed. The number of rows and the number of columns you provide are displayed as the group geometry when the group has been created.



3. Provide the information for the group.
Type a name for the group and the number of rows and columns.
4. Click the Next button.
A third screen is displayed.



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.



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

How to Enable Multihead Policy

Command-Line Steps

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

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



Note

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

Admin GUI Steps

1. Click the Advanced tab.
2. Click the System Policy tab, as in the following figure.

VERSION

User: admin Server: srstdemo-01

Sun Ray Administration

LOG OUT HELP

Servers Sessions Desktop Units Tokens Advanced Log Files

Security System Policy Kiosk Mode Card Probe Order Data Store Password

System Policy Save Reset

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

Card Users

Access: None All Users Users with Registered Tokens

Self-Registration Allowed User Account Authentication Required

Kiosk Mode: Enabled

Non-Card Users

Access: None All Users Users with Registered Tokens

Self-Registration Allowed User Account Authentication Required

Kiosk Mode: Enabled

Mobile Sessions: Enabled

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

Exit from Mobile Sessions Allowed

Multihead

Multihead Feature: Enabled

Save Reset

3. Select (or deselect) the Multihead Feature Enabled option.
4. Click the Save button.

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

How to Manually Set Multihead Display Dimensions

Screen dimensions for the multihead group are automatically set, by default, to the largest supported by the primary DTU. The primary DTU is the DTU 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 of `utxconfig`.



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.

How to Override Automatic Sizing of Screen Dimensions

```
% utxconfig -r <width>x<height>
```

For example:

```
% utxconfig -r 1280x1024
```

How to Restore Automatic Sizing Behavior on the Next Login

```
% utxconfig -r auto
```

How to Manually Set the Multihead Display Geometry

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.

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.

You can use the `-R` option to `utxconfig` to manipulate the automatic geometry.

How to Override the Automatic Geometry

```
% utxconfig -R <columns>x<rows>
```

How to Restore the Automatic Geometry on the Next Login

```
% utxconfig -R auto
```

How to Disable Multihead Displays for a Session

```
% utxconfig -m off
```

How to Enable and Disable XINERAMA

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



Note

XINERAMA tends to consume noticeable amounts of CPU, memory, and network bandwidth. For optimal performance, set the `shmsys:shminfo_shmmax` parameter in the `/etc/system` file to at least `LARGEST_NUMBER_OF_HEADS * width * height * 4`.

How to Enable XINERAMA

```
% utxconfig -x on
```

How to Disable XINERAMA

```
% utxconfig -x off
```

How to Enable XINERAMA as Default for a Single System or Failover Group

As superuser, type the following command:

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



Note

H264 and VC-1 support on the DTU is not available for XINERAMA sessions. In XINERAMA sessions, video windows may be dragged from one DTU to another or may span multiple DTUs, but audio/video synchronization of H264 and VC-1 support is limited to the primary DTU. The videos cannot be synchronized between DTUs. H264 and VC-1 videos may still be rendered by the application in the same manner they would be rendered on Sun Ray 1 DTUs.

Troubleshooting Multihead Displays

Multihead Video

The H264 and VC-1 streams are synchronized with the audio stream on the DTU. In a multihead group, the audio stream is directed only to the primary DTU, so audio/video synchronization can only be performed on the primary DTU. When video is displayed on secondary DTUs, the application must perform the A/V synchronization.

Problem: The display resolution is 640 x 480.

If the Sun Ray DTU is unable to read DDC data from the monitor, it defaults to 640 x 480 pixels. This condition occurs for the following reasons:

- The monitor was powered off when the Sun Ray DTU was started
- A bad cable
- An older monitor

How To Reset the Screen Resolution

1. Replace the cable.
2. Restart the Sun Ray DTU after powering the monitor on.
3. Replace the monitor.
4. Set a persistent display setting to override the default.

```
utresadm
```

Contents

- [About Security](#)
 - [Encryption and Authentication](#)

- Security Modes
 - Client Key Management
 - Key Fingerprint
 - Task Map - Managing Security for a Sun Ray System
 - DTU Keys
 - Security Status and Access
 - Client Authentication
 - How to Display Security Status for a DTU
 - How to Display Security Status for All Sessions
 - How to Confirm DTU Keys
 - How to Confirm a Specific DTU Key
 - How to Confirm All Unconfirmed DTU Keys
 - How to Display a DTU's Fingerprint Key from the DTU
 - How to Display DTU Keys
 - How to Display All DTU Keys
 - How to Display All Keys for a Specific DTU
 - How to Delete DTU Keys
 - How to Delete a Specific DTU Key
 - How to Delete All DTU Keys for a Specific DTU
 - How to Disable Client Authentication
 - How to Force Client Authentication From All DTUs
 - How to Deny Access to Clients With Unconfirmed Keys
 - Troubleshooting Authentication
 - Authentication Error Messages
 - Error Message Examples
-

Managing Security (All Topics)

About Security

Sun Ray Server Software (SRSS) provides interconnect security. The main aspects of this feature are:

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

See [Task Map - Managing Security for a Sun Ray System](#) for the list of tasks used to manage SRSS security.

Encryption and Authentication

By default, data packets between the Sun Ray server and client are sent "in the clear". This policy means that outsiders can easily "snoop" the traffic and recover vital and private user information, which malicious users might misuse. To avoid this type of attack, SRSS administrators can enable traffic encryption through the ARCFOUR encryption algorithm.

The ARCFOUR encryption algorithm, selected for its speed and relatively low CPU overhead, supports a higher level (128-bit) of security between Sun Ray services and Sun Ray desktop units.

However, encryption alone does not provide complete security. Spoofing a Sun Ray server or a Sun Ray client and posing as either is still possible, if not necessarily easy. Here are some examples:

- A man-in-the-middle attack, in which an impostor claims to be the Sun Ray server for the clients and pretends to be the client for the server. The impostor then intercepts all messages and has access to all secure data.
- Manipulating a client to pretend to be another client in order to gain access to sessions connected to the spoofed client.

Server and client authentication provided by SRSS can resolve these types of attacks. Server authentication uses pre-configured, public-private key pairs in the SRSS and firmware, and client authentication uses an automatically generated public-private key pair in every client.

SRSS uses the Digital Signature Algorithm (DSA) to verify that clients are communicating with a valid Sun Ray server and that the server is communicating with a legitimate client. This authentication scheme is not completely foolproof, but it mitigates trivial man-in-the-middle attacks and makes spoofing SRSS or Sun Ray clients harder for attackers.

Enabling encryption and authentication is optional. The system or network administrator can configure it based on site requirements. By default

only client authentication is enabled.

Security Modes

When you configure encryption and client authentication, you must decide between hard and soft security modes. Security mode can be configured separately for encryption requirements including server authentication and for client authentication requirements. Security mode settings are intended for compatibility with older firmware, which did not support the affected security feature.

- **Hard Security Mode** - Hard security mode ensures that every session is secure. If security requirements cannot be met, the session is refused.
- **Soft Security Mode** - Soft security mode ensures that connection requests are granted even for desktop units that don't support the configured security requirements. If security requirements cannot be met, the session is granted but not secure.

By default, the security modes for encryption and client authentication are both set to soft, which allows unauthenticated and unencrypted access to desktop units running older firmware.



Note

Security mode settings don't apply to software clients. Software clients will always be treated as if hard security mode for encryption or authentication is in effect.

The following table describes what happens when the different security modes are used.

Situation	Hard Security Mode	Soft Security Mode
Encryption - The Sun Ray DTU does not support encryption or server authentication because of old firmware	Sun Ray server denies the session.	Sun Ray server grants the DTU a non-secure session. The user must then decide whether to continue using a non-secure session.
Client Authentication - The Sun Ray DTU does not support client authentication because of old firmware	Sun Ray server denies the session.	Sun Ray server grants the DTU a non-secure session.
Client Authentication - The client supports authentication but authentication fails	Sun Ray server denies the session.	Sun Ray server denies the session.

Client Key Management

A Sun Ray client (DTU or software client) that supports client authentication has a public-private key pair for client authentication. The key pair for a DTU is generated when the DTU first boots with the appropriate firmware.



Note

Older versions of firmware or the firmware that is preinstalled on DTUs delivered from the factory do not generate keys and do not support client authentication. To help you identify preinstalled firmware, note that versions of preinstalled firmware start with `MEgPkg`. You must provision the DTUs with firmware that is delivered with SRSS in order to have keys generated.

When a client connects to a server and client authentication is enabled, the client sends its public key and a client identifier to the server. For a DTU, the client identifier is the MAC address. Initially the server can verify only that the client is the owner of the submitted key, but it cannot verify that the client legitimately uses the submitted client ID.

The Sun Ray server stores a list of known clients and their public keys in the Sun Ray data store. A stored key can be marked as confirmed to indicate that authenticity of the key for the given DTU has been confirmed through human intervention. As long as no key has been marked confirmed for a DTU, the client authentication feature can ensure only that a DTU identifier is not used by multiple different clients with different keys. Only when the key has been verified and marked confirmed can the client authentication actually authenticate the identity of the DTU.

**Note**

Keys for software clients are not stored in the data store and they are not displayed by the `utkeyadm` command or Admin GUI. Instead, a software client uses its key fingerprint as a client identifier so that the authenticity of the key for the given ID is established automatically. For more information, see the Key Fingerprint section.

By default, a DTU with an unconfirmed key is granted a session unless the identity of the DTU has been used with a different key. Multiple keys submitted for a client might indicate an attack on sessions for this client, so session access is denied for this client. A user needs to explicitly confirm one of the keys as being authentic to re-enable access for the client.

You can select a stricter policy that requires authenticated client identities and denies access to any DTU whose key is not verified and confirmed by using the `utpolicy` command or the Admin GUI. If you choose to use this policy, you must explicitly mark the key for every new client as 'confirmed' before the client can be used. To use this policy to full effect, you should also set the client authentication mode to 'hard' in the security configuration.

You can use the `utkeyadm` command to manage client identities and their associated keys. All keys that are used for a DTU are listed by the key management tools.

With the `utkeyadm` command, you can perform the following actions:

- List keys associated to known clients and their status
- Confirm a client key after verifying its authenticity. If multiple unconfirmed keys are stored for a DTU, all other keys are deleted when one is confirmed as authentic.
- Delete invalid or stale key entries
- Export key data for all or selected client identities for backup and for transfer to other Sun Ray server instances
- Import key data that has been exported on this or another Sun Ray server instance

You can also view, confirm, or delete associated keys for a DTU through the DTU's Desktop Properties page in the Admin GUI.

Key Fingerprint

A key fingerprint is a name for a key and is what the user can see. A key fingerprint is generated by an MD5 hash based on the public key data.

You can view the key fingerprint for a DTU in the key panel. To display the key panel, press `Stop+K` on a Sun keyboard or `Ctrl+Pause+K` on a non-Sun or PC keyboard. To verify the authenticity of a DTU key, you can compare key fingerprint displayed in the DTU's key panel with the one shown by the `utkeyadm` command for the same client.

Task Map - Managing Security for a Sun Ray System

For more information about the security available for a Sun Ray system, see [About Security](#).

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

- Enable encryption for upstream traffic only
- Enable encryption for downstream traffic only
- Enable bidirectional encryption
- Enable server authentication
- Disable client authentication

Additionally, you must decide whether to enable hard security mode for encryption and client authentication.

You can use the `utcrypto` command or the Admin GUI to configure the encryption option, authentication option, and security mode.

DTU Keys

Task	Description
How to Confirm DTU Keys	Describes how to confirm a specific DTU key or to confirm all unconfirmed DTU keys.
How to Display a DTU's Fingerprint Key from the DTU	Describes how to display a DTU's fingerprint key from the DTU.
How to Display DTU Keys	Describes how to display all the currently registered DTU keys.

How to Delete DTU Keys	Describes how to delete a specific DTU key or all the DTU keys for a specific DTU.
------------------------	--

Security Status and Access

Task	Description
How to Display Security Status for a DTU	Describes how to display a DTU's security status from the DTU.
How to Display Security Status for All Sessions	Describes how to display the security status for all sessions on a Sun Ray server.

Client Authentication

Task	Description
How to Disable Client Authentication	Describes how to disable client authentication for performance or upgrade reasons.
How to Force Client Authentication From All DTUs	Describes how to force all DTUs to authenticate by setting the hard security mode.
How to Deny Access to Clients With Unconfirmed Keys	Describes how to set policy to deny access to clients with unconfirmed keys.

How to Display Security Status for a DTU

Once a connection has been successfully established between a client and a server, you can display a DTU's security status by pressing the three volume keys simultaneously to display a security status icon and the DTU's MAC.

For a description of OSD icons and their respective codes, see [SRSS Troubleshooting Icons](#).

How to Display Security Status for All Sessions

To display the security status for all sessions on a Sun Ray server, type the following command:

```
# utsession -p
```

Output similar to the following example will be displayed.

```
Token ID                Registered Name      Unix ID  Disp   State
Payflex.000007450000202  ???                ???      2      IEA
Micropayflex.000003540004545  ???                ???      3      D
```

The State column displays the encrypted/authenticated state of the session:

State Column Value	Description
E	Encrypted session
A	Server is authenticated
C	Authenticated client with confirmed identity, including software clients with automatically confirmed keys
U	Authenticated clients with unconfirmed identity. Such connections might not have regular session access if the current policy requires a confirmed identity.
X	Clients that have successfully authenticated with an unconfirmed key, but that key is in conflict with other equally unconfirmed keys that have been used with the same client ID. Clients that have a conflicting key will not be granted session access and you need to confirm one of the known keys as authentic in order to admit the affected clients again.

For more information, see the `utsession` man page.

**Note**

A multihead group might have DTUs at different firmware levels. The `utsession` output shows the lowest security level across the set of all DTUs participating in the multihead group. For example, if at least one of the DTUs does not support encryption or authentication, the session will be marked as not encrypted or not authenticated.

How to Confirm DTU Keys

This procedure is required if a client receives a Keyerror (49) or Session Refused (50) icon due to conflicting or unconfirmed keys. Once the key is confirmed, you must disconnect the DTU by rebooting or inserting and removing a smart card to access a session after the change.

Before You Begin

- View the unconfirmed keys (key fingerprints) for all or specific DTUs.
- To determine whether an unconfirmed DTU key really belongs to that DTU, display the key fingerprint for the DTU by pressing `STOP+K`.

How to Confirm a Specific DTU Key

Command-Line Steps

```
# utkeyadm -a -c IEEE802.000000ee0d6b
1 key confirmed .
# utkeyadm -a -c IEEE802.00000f85f52f -k 1c:d4:b9:31:9d:f0:00:ba:db:ad:65:6c:8e:80:4d:b3
1 key confirmed .
```

Admin GUI Steps

1. Go to the Desktop Unit Properties page for a single DTU.
2. In the Client Keys table, select a single key and click Confirm.

How to Confirm All Unconfirmed DTU Keys

If you are certain that all DTUs requiring key confirmation have been connected to the server group (their genuine keys are stored on the server) and if you are certain that no unwanted DTUs have keys stored on the server, then you may also summarily confirm all known unconfirmed keys. If conflicting keys exist for a DTU, that DTU will be skipped.

1. Display all the DTU keys.

```
# utkeyadm -l -H
```

For example:

```
# utkeyadm -l -H
CID                TYPE KEY-FINGERPRINT                STATUS
IEEE802.00000adc1a7a DSA* 4f:98:25:60:3b:fe:00:ba:db:ad:56:32:c3:e2:8b:3e confirmed
IEEE802.00000f85f52f DSA* 1c:d4:b9:31:9d:f0:00:ba:db:ad:65:6c:8e:80:4d:b3 unconfirmed
IEEE802.00000f85f52f DSA* 4f:98:25:60:3b:fe:00:ba:db:ad:56:32:c3:e2:8b:3e unconfirmed
IEEE802.00000fe4d445 DSA* 13:d0:d4:47:aa:7f:00:ba:db:ad:26:3a:17:25:11:24 unconfirmed
IEEE802.000000ee0d6b DSA* d0:d7:d0:57:12:18:00:ba:db:ad:b7:0f:5a:c0:8b:13 unconfirmed
```

2. Confirm all unconfirmed DTU keys.

```
# utkeyadm -a -U
Skipping cid=IEEE802.00000f85f52f: Multiple (2) keys found.
2 keys confirmed.
```

Using the previous example, the unconfirmed DTU keys for `IEEE802.00000fe4d445` and `IEEE802.000000ee0d6b` are confirmed.

How to Display a DTU's Fingerprint Key from the DTU

To display the key fingerprint for a DTU, press the `Stop+K` key combination on a Sun keyboard or `Ctrl+Pause+K` on a non-Sun or PC keyboard.

If the key panel does not display, the DTU might have old firmware installed that doesn't support client authentication.

If the message `No key available` is displayed, the DTU still has preinstalled `MfgPkg` firmware or a bug exists.

How to Display DTU Keys

This procedure shows how to display DTU keys in the data store. For additional options to display DTU keys, see the `utkeyadm` man page.

How to Display All DTU Keys

Command Line Steps

- Use the `utkeyadm` command.

```
# utkeyadm -l -H
```

For example:

```
# utkeyadm -l -H
CID                TYPE KEY-FINGERPRINT                STATUS
IEEE802.00000adc1a7a DSA* 4f:98:25:60:3b:fe:00:ba:db:ad:56:32:c3:e2:8b:3e confirmed
IEEE802.00000f85f52f DSA* 1c:d4:b9:31:9d:f0:00:ba:db:ad:65:6c:8e:80:4d:b3 unconfirmed
IEEE802.00000f85f52f DSA* 4f:98:25:60:3b:fe:00:ba:db:ad:56:32:c3:e2:8b:3e unconfirmed
IEEE802.00000fe4d445 DSA* 13:d0:d4:47:aa:7f:00:ba:db:ad:26:3a:17:25:11:24 unconfirmed
IEEE802.00000ee0d6b DSA* d0:d7:d0:57:12:18:00:ba:db:ad:b7:0f:5a:c0:8b:13 unconfirmed
```

Admin GUI Steps

- For multiple DTUs, click the Desktop Units tab.

The Client Key Status column indicates whether the DTU has a key in a confirmed or unconfirmed status, whether the DTU has multiple unconfirmed keys creating a conflict, or whether a key exists for the DTU. The possible Client Key Status values are None, Unconfirmed, Confirmed, Conflict, Automatic, or Invalid.

How to Display All Keys for a Specific DTU

Command-Line Steps

- Use the `utkeyadm` command.

```
# utkeyadm [-l|-L] -c <cid> -H
```

where `<cid>` is the desktop ID of the DTU and `-L` displays additional auditing information.

Example

The following example displays all keys for the `IEEE802.0003ba0d93af` DTU with additional auditing information.

```
# utkeyadm -L -c IEEE802.0003ba0d93af -H
CID                               TYPE KEY-FINGERPRINT                STATUS      CREATED
CONFIRMED CONFIRMED BY
IEEE802.0003ba0d93af DSA* 4f:98:25:60:3b:fe:d6:f8:fb:38:56:32:c3:e2:8b:3e unconfirmed 2009-06-01
05:08:50 UTC -
```

Admin GUI Steps

- For a single DTU, go to the Desktop Unit Properties page.

The Client Keys table shows the known keys and their status for the DTU.

How to Delete DTU Keys

How to Delete a Specific DTU Key

- To delete a specific DTU key, use the following command:

```
# utkeyadm -d -c <cid> -k <key-id>
```

where <cid> is the desktop ID of the desktop to which the key belongs and <key-id> is the key fingerprint.

For example:

```
# utkeyadm -d -c IEEE802.00000f85f52f -k 1c:d4:b9:31:9d:f0:00:ba:db:ad:65:6c:8e:80:4d:b3
1 key deleted .
```

How to Delete All DTU Keys for a Specific DTU

- To delete all DTU keys for a specific DTU, type the following command:

```
# utkeyadm -d -c <cid>
```

where <cid> is the desktop id of the desktop to which the keys belong.

For example:

```
# utkeyadm -d -c IEEE802.00000f85f52f
2 keys deleted.
```

How to Disable Client Authentication

Some reasons to disable client authentication are:

- Reduce administrative overhead - At the cost of security, disabling client authentication saves time required to manage client keys on the servers.
- Eliminate log messages during upgrade - If you upgrade a Sun Ray server in a failover group with older servers, the upgraded server will repeatedly produce log messages indicated that it cannot store key data and the server will treat all keys as unconfirmed. Client authentication should be enabled once the entire group is upgraded.

**Caution**

Disabling client authentication creates a security risk. Make sure you understand the consequences before disabling client authentication. See [About Security](#) for details.

Before You Begin

- Disabling client authentication applies to all future connections without restarting the Sun Ray server.

Command-Line Steps

- Use the following command to disable client authentication:

```
# utcrypto -a auth_up_type=none
```

Use `-m` instead of `-a` if a non-default security policy already exists.

To enable client authentication, set the `auth_up_type` value to `default`.

Admin GUI Steps

On the Advanced->Security page, deselect Client Authentication and click Save.

How to Force Client Authentication From All DTUs

If you don't need to allow access to DTUs running older versions of firmware, you can improve security by requiring client authentication from all clients.

Command-Line Steps

- Use the following command to force client authentication.

```
# utcrypto -m auth_up_type=DSA auth_mode=hard
```

Use `-a` instead of `-m` if a non-default security policy already exists.

Admin GUI Steps

1. Navigate to the the Advanced->Security page.
2. Select the Client Authentication option and select Hard as the Security Mode.
3. Click Save.

How to Deny Access to Clients With Unconfirmed Keys

Sun Ray DTU keys are initially considered unconfirmed and need to be confirmed as authentic for the specific DTU by human intervention. Sun Desktop Access Client keys are always considered automatically confirmed (auto-confirmed), because the ID by which a Desktop Access Client is identified is uniquely derived from its key.

The following procedure sets the policy that a confirmed key is required before access to a client is granted. To enact a stronger policy, you should also set up the security policy to require client authentication from all DTUs, as described in [How to Force Client Authentication From All DTUs](#).

Command-Line Steps

1. View the current policies:


```
# utpolicy
Current Policy:
-a -g -z both -k pseudo -u pseudo
```

2. Set the client authentication policy with the `-c` option:

```
# utpolicy -a -g -z both -k pseudo -u pseudo -c
```

3. Restart the Sun Ray services:

```
# utrestart
```

Admin GUI Steps

1. On the Advanced-System Policy tab page, select the Client Key Confirmation Required option in the Client Authentication section.
2. Restart all servers in the server group.

Troubleshooting Authentication

Authentication Error Messages

Errors in authentication are reported in the following log files:

- Installation logs:
 - `/var/adm/log` (Solaris only)
 - `/var/log` (Linux only)
- Configuration logs:
 - `/var/adm/log` (Solaris only)
 - `/var/log/SUNWut` (Linux only)
- General log files:
 - `/var/opt/SUNWut/log`
 - `/var/opt/SUNWut/srds/log`
 - `/var/opt/SUNWut/srds/repllog`

Messages logged into `/var/opt/SUNWut/log/messages` are delivered through the `syslog` service described in the `syslogd` man page. The general format of these 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:
 - Worker# – Handles DTU authentication, access control, and session monitoring. 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, thread names are reused.
 - SessionManager# – Communicates with `utsessiondon` on behalf of a Worker# thread.
 - AdminJobQ – Used in the implementation to wrap a library that would not otherwise be thread-safe.
 - Callback# – Communicates with applications such as `utload`.

- WatchID – Used to poll data or terminals from connections
- Terminator – Cleans up terminal sessions
- Group Manager – Main group manager thread
- message_class:
 - 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 exits after this error is detected.
 - NOTICE – Indicates a normal event.
 - UNEXPECTED – Logs events or conditions that were not anticipated for normal operation but are not fatal.
 - DEBUG – Occurs only if explicitly enabled and is used by the development team. Debug messages can reveal session IDs, which must be kept secret to ensure proper security.

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 <code>utload</code> or <code>utidle</code> .
	.../ ... 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 error condition is also a way for <code>utauthd</code> to force the DTU to reset.

Contents

- [About Sun Desktop Access Clients](#)
 - [Product Requirements](#)
 - [User Information](#)
- [Client ID Differences Between Sun Desktop Access Clients and Sun Ray DTUs](#)
 - [Example Sun Ray DTU IDs](#)
 - [Example Sun Desktop Access Client IDs](#)
- [How to Enable Access for Sun Desktop Access Clients](#)
- [How to Install the Sun Desktop Access Client](#)
- [Troubleshooting the Sun Desktop Access Client](#)
 - [Enabling Access for the Sun Desktop Access Client](#)
 - [Using On-Screen Displays to Diagnose Connection Problems](#)
 - [Connection Problems When Using a Virtual Private Network](#)

- [Setting the Logging Level](#)
- [Sun Desktop Access Client Release Notes](#)
 - [Supported Platforms](#)
 - [Limitations of the Sun Desktop Access Client](#)
 - [Known Issues](#)

Managing Sun Desktop Access Clients (All Topics)



Release Update

For the Oracle Virtual Desktop Client 2.0 administration and user documentation, see the [Oracle Virtual Desktop Client Information Center](#).

About Sun Desktop Access Clients



Release Update

For the Oracle Virtual Desktop Client 2.0 administration and user documentation, see the [Oracle Virtual Desktop Client Information Center](#).

The Sun Desktop Access Client is a software application that runs on common client operating systems and provides the ability to connect to a desktop session running on a Sun Ray server. Users can switch between their Sun Ray DTU and any supported Desktop Access Client enabled PC without using smart cards.

In other words, a user can install and run the Sun Desktop Access Client instead of relying only on a Sun Ray Desktop Unit (DTU) for session access. For example, a user could connect to the same Sun Ray session from a PC laptop or desktop at home and a Sun Ray DTU at the office.



Note

Throughout the SRS documentation, the term "Sun Ray DTU" is used to refer to the hardware-based thin client. With the addition of the Sun Desktop Access Client, a majority of the Sun Ray DTU references also apply to the new Sun Desktop Access Clients. As the documentation evolves, the generic term "client" will refer to all clients supported by the Sun Ray system, where appropriate.

Product Requirements

The Sun Desktop Access Client requires the usage of at least Sun Ray Server Software 4.2.



Note

You must enable access to Sun Desktop Access Clients before you can use them. See [How to Enable Access for Sun Desktop Access Clients](#) for details.

User Information

For detailed information about using the Sun Desktop Access Client application, refer to the [Sun Desktop Access Client 1.0 User Guide](#).

Client ID Differences Between Sun Desktop Access Clients and Sun Ray DTUs



Release Update

For the Oracle Virtual Desktop Client 2.0 administration and user documentation, see the [Oracle Virtual Desktop Client Information Center](#).

If you have existing scripts using the SRSS commands or you plan to create scripts, you should be aware of the client ID differences between Sun Desktop Access Clients and Sun Ray DTUs.

All [Sun Ray clients](#) are represented in the SRSS administration tools by a client ID, also called "CID," "terminal CID," or "client identifier." A client ID has both a full ID and short ID version:

- Full client ID: namespace.id-part
- Short client ID: id-part

The namespace value is a tag that determines the format of the id-part value. Short client IDs are usually used and accepted because the current namespaces, one for DTUs and one for Desktop Access Clients, use different id-part formats. The full client ID is used to help distinguish between these different types of clients more easily.

The details of the client ID are as follows:

Client	namespace	id-part Origin/Meaning	id-part Format
Sun Ray DTU	IEEE802	MAC address of DTU	12 hex digits
Desktop Access Client	MD5	MD5 hash of client key	32 hex digits



The client key is part of a Sun Desktop Access Client profile, so every Desktop Access Client profile has its own Client ID.

Example Sun Ray DTU IDs

Short ID	Full CID
0003badc1b9d	IEEE802.0003badc1b9d
00144f85f52f	IEEE802.00144f85f52f
080020b5ca55	IEEE802.080020b5ca55

Example Sun Desktop Access Client IDs

Short ID	Full CID
1bd97b44ea9458fac256a7a778a282fe	MD5.1bd97b44ea9458fac256a7a778a282fe
d8b3a4eb29497e0c6fbb0f2a810267f5	MD5.d8b3a4eb29497e0c6fbb0f2a810267f5

How to Enable Access for Sun Desktop Access Clients



Release Update

For the Oracle Virtual Desktop Client 2.0 administration and user documentation, see the [Oracle Virtual Desktop Client Information Center](#).

Sun Desktop Access Clients can be used to access only non-card sessions. You can also enable NSCM on Sun Desktop Access Clients to provide hotdesking.



Note

The following procedure uses a warm restart of Sun Ray services. If you disable access for Sun Desktop Access Clients, use a cold restart.

Command-Line Steps

1. Use the `utpolicy` command to view the current policy.
For example:

```
# utpolicy
Current Policy:
-a -g -z both -M
```

2. Add the `-u pseudo` option to your policy options:

```
# utpolicy -a -g -z both -M -u pseudo
```



Note

(Solaris only) To use the Sun Desktop Access Clients with mobile sessions, use the `-M` option to enable non-smartcard mobile sessions.

3. Restart the Sun Ray services:

```
# utrestart
```

A restart of Sun Ray services in the server group is required after enabling or disabling access for Desktop Access Clients.

Admin GUI Steps

1. Click the Advanced tab.
2. Click the System Policy tab in the Advanced tab.
3. Select the Sun Desktop Access Client option in the Non-Card Users section.
4. Restart all servers in the server group using the Warm Restart button.

How to Install the Sun Desktop Access Client



Release Update

For the Oracle Virtual Desktop Client 2.0 administration and user documentation, see the [Oracle Virtual Desktop Client Information Center](#).



Note

To install the Sun Desktop Access Client, you must have administrator privileges on the client computer.

On a Microsoft Windows platform, do the following:

1. Copy the Sun Desktop Access Client Windows install program, `setup.exe`, to the client computer.
2. Double-click `setup.exe` and follow the instructions.
The Sun Desktop Access Client software is installed on the client computer and entries for the Sun Desktop Access Client are added to the Windows Start Menu.

For detailed information about using the Sun Desktop Access Client, refer to the [Sun Desktop Access Client 1.0 User Guide](#).

Troubleshooting the Sun Desktop Access Client



Release Update

For the Oracle Virtual Desktop Client 2.0 administration and user documentation, see the [Oracle Virtual Desktop Client Information Center](#).

This section includes some troubleshooting topics for the Sun Desktop Access Client.

Enabling Access for the Sun Desktop Access Client

The `utpolicy` setting for the Sun Ray Server Software (SRSS) must be configured to enable access using the Sun Desktop Access Client.

See [How to Enable Access for Sun Desktop Access Clients](#) for details of the required configuration.

You might also need to configure firewall settings as follows:

- Client computers – Ensure that firewall settings on the client computers allow the Sun Desktop Access Client to access the Internet.
- Sun Ray servers – See [Ports and Protocols](#) for information on the ports used by the Sun Desktop Access Client.

Using On-Screen Displays to Diagnose Connection Problems

SRSS uses on-screen displays (OSD) to display the status of a connection. The OSD can be used to diagnose connection problems with the Sun Desktop Access Client.

See [Sun Ray Icons](#) for more details about the available icons and messages used by SRSS.

Connection Problems When Using a Virtual Private Network

If you experience problems when using a Virtual Private Network (VPN), you might have to decrease the Maximum Transmission Unit (MTU) setting, to allow space for Internet Protocol Security (IPSec) headers.

The MTU is the maximum packet size for connections. By default, the MTU is set to 1500 bytes.

To set the MTU, either change the setting on the Network tab or run the following command:

```
sdac --mtu <bytes> <server-name>
```

where *bytes* is the maximum packet size, in bytes and *server-name* is the name of the Sun Ray server.

Setting the Logging Level

To help you to diagnose problems with the Sun Desktop Access Client, you can increase the logging level.

The available logging levels are shown in the following table.

Level	Description
0	No logging
1	Critical messages
2	Warnings
3	Informational messages

By default, the logging level is 0, which sets logging to off.

The logging level is cumulative. For example, the maximum logging level 3 includes informational messages, warnings, and critical messages.

To set the logging level, either change the setting on the Logging tab or run the following command:

```
sdac --logging-level <num> <server-name>
```

where *num* is the logging level and *server-name* is the name of the Sun Ray server.

Log messages are written to a `.log` text file on the client computer. The `.log` file is named after the profile used. For example, the log file for the default profile is called `default.log`.

The location of the log file depends on the installation platform, as follows:

- Microsoft Windows XP platforms – `C:\Documents and Settings\username\Application Data\Sun\SDAC\profilename.log`
- Microsoft Windows Vista and Microsoft Windows 7 platforms –

C:\Users\username\AppData\Roaming\Sun\SDAC\profilename.log

Sun Desktop Access Client Release Notes



Release Update

For the Oracle Virtual Desktop Client 2.0 administration and user documentation, see the [Oracle Virtual Desktop Client Information Center](#).

Supported Platforms

The following operating systems are supported:

- Microsoft Windows XP (32-bit and 64-bit)
- Microsoft Windows Vista (32-bit and 64-bit)
- Microsoft Windows 7 (32-bit and 64-bit)

Limitations of the Sun Desktop Access Client

In the current release, the following features are not supported by the Sun Desktop Access Client:

- Universal Serial Bus (USB) devices
- Serial and parallel port devices
- Smart cards
- Audio input and recording
- Integrated Virtual Private Network (VPN) support
- Copy and paste between the Sun Ray session and the local operating system running the Sun Desktop Access Client

Known Issues

Exit Key Combination Might Not Work on Some Client Computers (CR 6876016)

Problem

An exit key combination selected using the Hot Key tab does not work on the client computer.

Workaround

Choose an alternative exit key combination that works on the client computer.

Contents

- About Sun Ray DTU Firmware
 - How to Set DTU Configuration Parameters (Pop-up GUI)
 - Access Control
 - Features and Usage
 - How to Start the DTU Pop-Up GUI
 - Pop-up GUI Main Menu (Part I)
 - Pop-up GUI Main Menu (Part II)
 - Pop-up GUI Advanced Menu (Part I)
 - Pop-up GUI Advanced Menu (Part II)
 - How to Load DTU Configuration Data Remotely
 - How to Display Firmware Versions for All Currently Connected DTUs
 - How to Display a DTU's Firmware Version from the DTU
 - How to Update Firmware Versions on DTUs
 - How to Update All the DTUs on an Interface
 - How to Update a DTU Using the Ethernet (MAC) Address
 - How to Disable All Firmware Updates
-

Managing the Sun Ray DTU Firmware (All Topics)

About Sun Ray DTU Firmware

Every Sun Ray DTU contains a firmware module that handles the following items:

- Power-on self test (POST)
- DTU initialization
- Authentication
- Low-level input and output, such as keyboard, mouse, and display information.

In most cases, the firmware on Sun Ray DTUs are synchronized with the Sun Ray server as part of the post-installation or post-upgrade configuration steps. However, sometimes you might have to find out a DTU's firmware version or to specifically manage a DTU's firmware.

How to Set DTU Configuration Parameters (Pop-up GUI)

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

Access Control

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

- The default version of Sun Ray DTU firmware is installed at `/opt/SUNWut/lib/firmware`. This firmware does not enable the Pop-up GUI.
- The Pop-up GUI-enabled version of the firmware is installed at `/opt/SUNWut/lib/firmware_gui`. To make the Pop-up GUI available, the administrator must run `utfwadm -f` to install the firmware.

Features and Usage

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

- Non-DHCP network configuration for standalone operation, when configuring local DHCP operation is impossible
- Local configuration of Sun Ray specific parameters, such as server list, firmware server, MTU, and bandwidth limits
- DNS servers and domain name for DNS bootstrapping
- IPsec configuration
- Wireless network configuration, which is used in Tadpole laptops

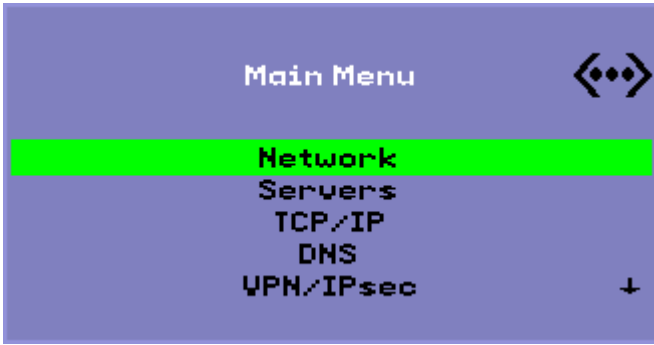
To protect the use of stored authentication information, the VPN configuration includes a PIN entry. This feature enables two-factor authentication for Sun Ray at Home VPN deployments.

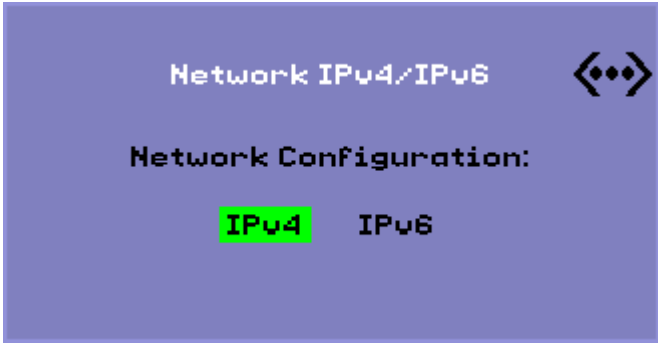

How to Start the DTU Pop-Up GUI

- If you are using a Sun keyboard, you can press one of the following key combinations:
 - `Stop+S`
 - `Stop+M`
- If you are using a non-Sun keyboard, you can press one of the following key combinations:
 - `Ctrl+Pause+S`
 - `Ctrl+Pause+M`

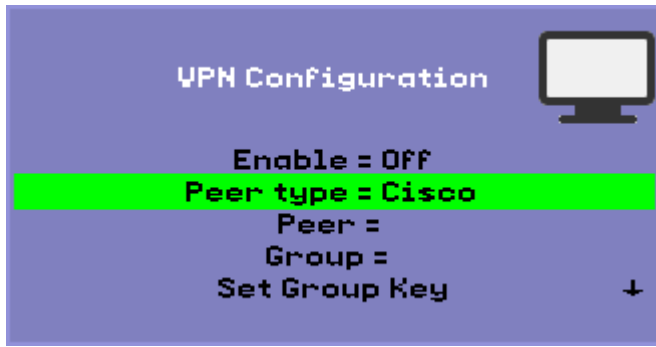
The arrow at the lower right corner indicates that the menu can be scrolled with the Up and Down arrow keys.

Pop-up GUI Main Menu (Part I)



Main Menu Item	Description
Network	
Servers	<ul style="list-style-type: none"> • Server list - A list of comma-separated server names or IP addresses • Firmware server - Name or IP address of firmware/config server • Log host - IP address of syslog host
TCP/IP	 <ul style="list-style-type: none"> • DHCP - MTU • Static - IP address, netmask, router, broadcast address, MTU
DNS	<ul style="list-style-type: none"> • Domain name - One only • DNS server list - List of IP addresses

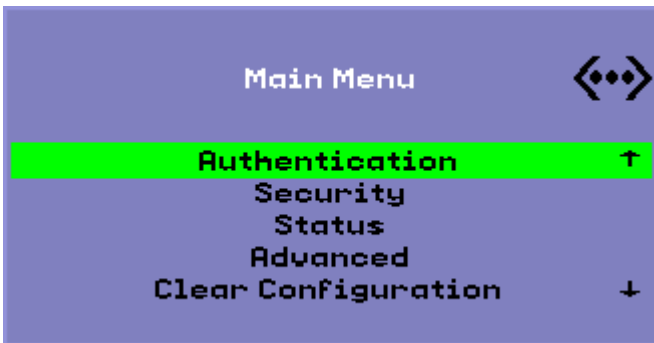
VPN/IPsec



Cisco EzVPN authentication model

- Enable - On/Off
- Peer type - Cisco or Netscreen (Juniper Networks)
- Peer - Gateway peer (name or IP address)
- Group - Group name
- Set Group Key
- Username - Xauth user name (if static)
- Set Password - 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.
- Advanced
 - DH Group - Diffie-Hellman group
 - PFS Group
 - IKE Lifetime - IKE Phase 1 lifetime
 - IPsec Lifetime
 - Dead Peer Detection
 - Session timeout - Idle timeout, after which VPN connection is dropped

Pop-up GUI Main Menu (Part II)



Main Menu Item	Description
Authentication	For HTTP authentication <ul style="list-style-type: none"> • Enable/Disable switch • Port number
Security	Set password (lock configuration under password control)
Status	Version (equivalent to STOP-V)

Advanced	<ul style="list-style-type: none"> • Download Configuration • Keyboard Country Code • Bandwidth Limit (in bits per second) • Session Disconnect (STOP-Q) • Force Compression • Lossless Compression • Disallow utload • Force Full Duplex • Enable Fast Download • Video (set blanking timeout) • Video Input Disable
Clear Configuration	Equivalent to STOP-C.

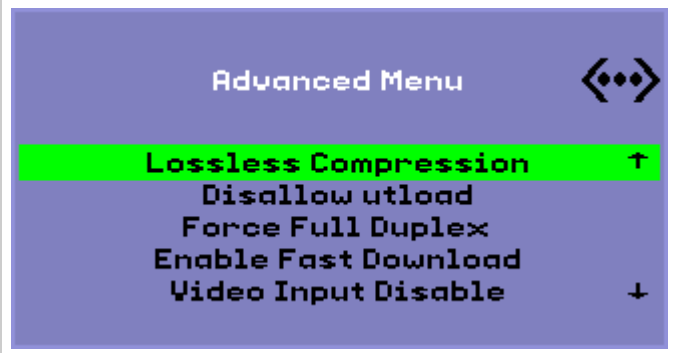

Pop-up GUI Advanced Menu (Part I)



Main Menu Item	Description
Download Configuration	<p>Prompts for a server name and file name of a file to be downloaded from the server, in the form <code>server:filename</code>. The default server is the TFTP server value if defined, and the default file name is <code>config.MAC</code>, where MAC is the unit's MAC address in upper-case hexadecimal. This field can be overwritten when selected. Pressing Return causes the corresponding file to be read and the configuration values parsed and set. For configuration values, see Pop-up GUI Menu Configuration Values.</p> <p>On success, the user is prompted to save the values. Otherwise, the previous menu is displayed. No other error indications are given.</p> <p>Some of the menus have an <code>Exit</code> 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 memory, the Escape key resets the DTU.</p>

Keyboard Country Code	<p>A keyboard country code (keyboard map) that is applied to a keyboard that returns a country code of 0, for use with non-U.S. USB keyboards that do not report a country code. Here are the valid keyboard country code values:</p> <ul style="list-style-type: none"> • 1 Arabic • 2 Belgian • 3 Canada_Bi • 4 French-Canadian • 5 Czech • 6 Denmark • 7 Finnish • 8 France • 9 Germany • 10 Greek • 12 Hungarian • 14 Italy • 15 Japan • 16 Korea • 17 Latin-American • 18 Netherland • 19 Norway • 21 Polish • 22 Portugal • 23 Russia • 24 Slovakian • 25 Spain • 26 Sweden • 27 Switzerland • 28 Switzerland_Ge • 30 Taiwan • 31 TurkeyQ • 32 UK-English • 33 US-English • 35 TurkeyF
Bandwidth Limit	The maximum amount of network bandwidth in bits per second that a given client will use.
Session Disconnect	Enables or disables the ability to terminate a session by pressing STOP-Q. This feature is useful when you want to terminate a VPN connection and leave the Sun Ray in an inactive state. Pressing the Escape key after the session has terminated reboots the Sun Ray DTU.
Force Compression	Sets a tag sent from the Sun Ray DTU to the Xserver telling it to enable compression regardless of available bandwidth.

Pop-up GUI Advanced Menu (Part II)

Sun Ray 270 (Video Input Disable)	Sun Ray 2, 2FS, 270, and later models
	

Main Menu Item	Description
----------------	-------------

Lossless Compression	Disables the use of lossy compression for image data.
Disallow utload	Disables the ability to explicitly force a firmware load into a DTU. In this way, firmware can be tightly controlled using <code>.parms</code> files or DHCP parameters.
Force Full Duplex	Allows the DTU to operate correctly when the network port that it is connected to does not auto-negotiate. In that case, the auto-negotiation results in the Sun Ray running at half duplex, which significantly impacts network performance. This setting allows the Sun Ray to operate with better performance in this situation.
Enable Fast Download	<p>If set, the DTU uses the maximum TFTP transfer size if the TFTP server supports it. Over a high latency connection, this setting typically doubles the speed of firmware downloads. There are no disadvantages to enabling fast downloads on low latency LANs.</p> <p>This parameter is disabled by default and the transfer size is set at 512-byte packets. It is disabled by default for backwards compatibility with TFTP servers that might not support the more advanced protocol. If this parameter were on by default and a firmware download were to fail, there would be no way to recover.</p>
Video	<ul style="list-style-type: none"> • Blanking Timeout - The time until the screen is put to sleep, in minutes. (specify zero to disable). • OSD Quiet Display - If set, disables most of the OSD icons except when error conditions are detected.
Video Input Disable	Sun Ray 270 only. If set, turns off the input selector on the front of a Sun Ray 270 and locks the monitor so that it displays only the Sun Ray output. This feature prevents users from connecting a PC to the VGA video input connector on a Sun Ray 270 and using it as a monitor.

How to Load DTU Configuration Data Remotely

To help avoid error-prone manual entry of configuration data for deployments where preconfiguration 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 [Pop-up GUI Advanced Menu \(Part I\)](#).

The following keywords correspond to configuration values that can be set from the Pop-up GUI menus. To group items that are logically related, some of the keywords take the form `family.field`.

Pop-up GUI Menu Configuration Values

VPN/IPsec Submenu	Comment
<code>vpn.enabled</code>	Enable toggle
<code>vpn.peer</code>	Remote gateway name/IP address
<code>vpn.group</code>	VPN group
<code>vpn.key</code>	VPN key
<code>vpn.user</code>	Xauth user
<code>vpn.passwd</code>	Xauth password
<code>vpn.pin</code>	PIN lock for use of user/passwd
<code>vpn.dhgroup</code>	Diffie-Hellman group to use
<code>vpn.lifetime</code>	Lifetime of IKE connection
<code>vpn.killtime</code>	Idle timeout value to drop VPN connection.
DNS Submenu	
<code>dns.domain</code>	Domain name
<code>dns.servers</code>	Server list (comma-separated IP addresses)
Servers Submenu	
<code>servers</code>	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")
Advanced Submenu	
kbcountry	Keyboard country code
bandwidth	Bandwidth limit in bits per second.
stopqon	Enable (1) or Disable (0) STOP-Q for disconnect
compress	Force compression on when 1
lossless	Force use of lossless compression when 1
utloadoff	Disallow use of utload to force firmware download when 1
fastload	Force maximum TFTP transfer rate when 1.
videoindisable	Disable input selector of Sun Ray 270 when 1.

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

Sample VPN Configuration File

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

How to Display Firmware Versions for All Currently Connected DTUs

1. Log in to the Sun Ray server.
2. Display the firmware versions.

```
$ utfwload -a
```

How to Display a DTU's Firmware Version from the DTU

Press `Stop+V` or `Ctrl+Pause+V`.

How to Update Firmware Versions on DTUs

Use the `utfwadm` command to keep the firmware version in the PROM on Sun Ray DTUs synchronized with that on the server. See also [Sun Ray DTU Initialization Requirements Using DHCP](#).

If the DHCP version variable is defined and a new DTU is plugged in, the DTU's firmware is automatically updated to the firmware version on the server. If you make manual changes to your DHCP configuration, you will have to update the firmware using this procedure.

If you need to update the firmware with the Pop-Up GUI, see [How to Install the Pop-up GUI Firmware on All DTUs](#).

Steps



Note

This procedure should be done on each Sun Ray server in a Failover Group (FOG).

1. Become superuser on the Sun Ray server.
2. Update the firmware based on one of the following network configurations.
3. Once you update the firmware, power-cycle the DTUs to load the new firmware.



Note

To update firmware versions for a specific DTU, you can use the `-e <MAC_address>` option.

On a Shared Network (LAN) with External DHCP Server Support

Use the following command if you configured the network using the `utadm -L on` command.

```
# utfwadm -AaV
```

On a Shared Network (LAN) with Sun Ray Server DHCP Support

Use the following command if you configured the network using the `utadm -A <subnet>` command.

```
# utfwadm -Aa -N all
```

On a Private Network

Use the following command if you configured the network using the `utadm -a <intf>` command.

```
# utfwadm -Aa -n all
```

How to Disable All Firmware Updates

```
# /opt/SUNWut/sbin/utfwadm -D -a -n all
```

Contents

- [About Sun Ray DTU Peripherals](#)
 - [List of Compatible Sun Ray Peripherals and 3rd Party Components](#)
 - [Supported Mass Storage Devices](#)

- Device Nodes and USB Peripherals
 - Device Node Paths
 - Device Links
 - Device Node Ownership
 - Hotdesking and Device Node Ownership
 - Enabling and Disabling Device Services
 - Mass Storage Devices (Solaris)
 - Device Nodes and Links
 - Mount Points
 - Device Ownership and Hotdesking
 - Mass Storage Devices and Idle Sessions
 - Commands for Common Disk Operation on SPARC and x86 Platforms
 - Mass Storage Devices (Linux)
 - Device Nodes and Links
 - Mount Points
 - Device Ownership and Hotdesking
 - Mass Storage Devices and Idle Sessions
 - Commands for Common Disk Operation on Linux Platforms
 - How to Determine the Current State of Device Services
 - How to Enable or Disable USB Services
 - How to Set Up an Attached PostScript Printer (Solaris)
 - How to Set Up an Attached PostScript Printer (Linux)
 - How to Set Up an Attached Non-PostScript Printer
 - How to Set Up Serial Attached Devices
 - How to Enable Applications to Access USB Devices
 - How to Unmount a Mass Storage Device From a DTU
 - Troubleshooting Printers
 - Problem: "Failed to open the printer port" message.
 - Troubleshooting USB Storage
 - Problem: Device nodes are not created.
 - Problem: The device is not automatically mounted.
 - Problem: The device is not automatically unmounted.
-

Managing Sun Ray DTU Peripherals (All Topics)

About Sun Ray DTU Peripherals

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.

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



Note

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

List of Compatible Sun Ray Peripherals and 3rd Party Components

For the latest list of compatible Sun Ray Peripherals and 3rd Party Components, see the [Sun Ray Peripherals List](#).

Supported Mass Storage Devices

Sun Ray Server Software supports the use of flash disks, memory card readers, zip drives, and hard drives on Sun Ray DTUs. Data CDs and DVDs can be read but not written. It does not support floppy drives. Most devices claiming USB 2.0 compliance are backwards compatible and should work with Sun Ray Mass Storage.

For troubleshooting tips, see [Troubleshooting USB Storage](#).

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 Node Paths

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. The nodes are named `manufacturer_name` and `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 example is a typical device node path:

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

Definitions of Naming Conventions

Term	Definition
physical topology	The physical topology is <code>hub@port/hub@port</code> 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 <code>devices</code> directory is <code>manufacturer, model@port</code> with a colon separating the numerical index when the string just described is not unique in the directory.
printer name 2, terminal name 2	The printer and terminal name in the Sun Ray <code>dev</code> directory is the manufacturer and serial number concatenated with an alphabetic index when the serial number is not unique.

Device Links

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

Typical device links are:

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

The variable `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 might be owned by root or by other users that had previously active sessions on the DTU. Device permissions, access controls and ownership rules are determined by the class of device. For serial devices, only the user whose session is active on the DTU or the superuser have permission to use the attached device. If no user has an active

session, superuser owns the serial and parallel device nodes. This rule might not be applicable 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 or 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 to or output from any affected device results in an error. For a serial device node, if the original session is restored within 15 seconds, the ownership is not relinquished, and input and output continue uninterrupted.

Devices currently opened by the superuser, including normal printing, remain unaffected by a session change.

Enabling and Disabling Device Services

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

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

When an 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 condition 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 situation does not 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.

For more information, see the following related tasks. The other device services can be enabled or disabled with the same syntax.

- [How to Determine the Current State of Device Services](#)
- [How to Enable or Disable USB Services](#)

Mass Storage Devices (Solaris)

Device Nodes and Links

Mass storage devices have two types of device nodes, block and raw, which are created in the DTU's device directory. A link to the block device is created in the DTU's `dev/disk` directory and a link to the raw device is created in the `dev/rdisk` directory.

Device links have a suffix denoting their slice number. Slice `s2` is known as the backup slice, signifying the complete disk. Other slices are numbered accordingly on the file system on the disk. For UFS disks, slice numbers are derived from the disk label. For FAT disks, slices (partitions in this case) are numbered starting from `s0`. Disk operations such as `format` or `eject` should be directed at slice `s2`. Partition operations such as `mount` or `fstyp` should be directed at the individual slice concerned. See the [Commands for Common Disk Operation on SPARC and x86 Platforms](#) Table for examples.

Mount Points

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

```
% utdiskadm -l
```

Device Ownership and Hotdesking

When the user's session disconnects from the DTU, the user loses access rights to the mass storage device. All pending I/O to the device halts. This situation can cause the data on the device to be corrupted. Users should use the `utdiskadm` command as follows to unmount all file systems safely before hotdesking or unplugging the disk from the DTU:

```
% utdiskadm -r <device_name>
```



Note

Before running this command, close all references to files and directories in the mount point to ensure that the device is not busy.

Mass Storage Devices and Idle Sessions

If you are using Remote Hotdesk Authentication (RHA), Non-Smart Card Mobility (NSCM), or smart card-based authentication, long I/O operations might fail when using mass storage devices on Sun Ray DTUs.

If these types of sessions become idle due to keyboard and mouse inactivity long enough to activate the screen lock, the session is detached. The user loses access to the storage device, causing any I/O in progress to halt, and data may become corrupted.

To avoid this situation, the following options are available:

- Maintain keyboard or mouse activity
- Increase the screen lock idle time sufficiently to allow I/O operations to complete
- Disable the screen lock program
- Disable the NSCM or RHA policies
- Find an alternative way to perform the I/O operation more securely, for example, plug the device directly into the Sun Ray server in a locked server room



Note

Some of these options have security and convenience implications that should be carefully weighed against the timeout issue to determine what is best for your site.

Commands for Common Disk Operation on SPARC and x86 Platforms

The following table is a summary of common disk operations and the commands used to perform them. Refer to the [Solaris System Administration Guide](#) and man pages for more information on the individual commands.

Operation	Command	Device Name Argument Examples (SPARC)	Device Name Argument Examples (x86)
Format	<code>rmformat</code>	Path of whole disk <code>\$UTDEVROOT/dev/rdisk/disk3s2</code>	Path of whole disk <code>\$UTDEVROOT/dev/rdisk/disk3p0</code>
Create file system	<code>mkfs</code>	Path of partition <code>\$UTDEVROOT/dev/rdisk/disk3s0</code>	Path of partition <code>\$UTDEVROOT/dev/rdisk/disk3p1</code>
Create UFS file system	<code>newfs</code>	Path of slice <code>\$UTDEVROOT/dev/rdisk/disk3s0</code>	Path of slice <code>\$UTDEVROOT/dev/rdisk/disk3s0</code>
Mount	<code>utdiskadm -m</code>	Partition name <code>disk3s0</code>	Partition name <code>disk3p1</code>

Unmount	<code>utdiskadm -u</code>	Mount point \$DTDEVROOT/mnt/label1	Mount point \$DTDEVROOT/mnt/label1
Prepare to unplug	<code>utdiskadm -r</code>	Device alias disk3	Device alias disk3
Eject media	<code>utdiskadm -e</code>	Device alias disk3	Device alias disk3
Check for media	<code>utdiskadm -c</code>	Device alias disk3	Device alias disk3
Create <code>fdisk</code> table	<code>fdisk</code>	Path of whole disk \$UTDEVROOT/dev/rdisk/disk3s2	Path of whole disk \$UTDEVROOT/dev/rdisk/disk3p0
Repair file system	<code>fsck</code>	Path of raw slice \$UTDEVROOT/dev/rdisk/disk3s0	Path of raw partition \$UTDEVROOT/dev/rdisk/disk3p1
Display file system capacity	<code>df -k</code>	Mount point \$DTDEVROOT/mnt/label1	Mount point \$DTDEVROOT/mnt/label1
Display slice capacity	<code>prtvtoc</code>	Path of backup slice \$UTDEVROOT/dev/rdisk/disk3s2	Path of backup slice \$UTDEVROOT/dev/rdisk/disk3s2
List devices	<code>utdiskadm -l</code>	None	None

Mass Storage Devices (Linux)

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 [Commands for Common Disk Operation on Linux Platforms](#) for examples.

Mount Points

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

```
% utdiskadm -l
```

Device Ownership and Hotdesking

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

**Caution**

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

```
% utdiskadm -r <device_name>
```

Mass Storage Devices and Idle Sessions

If you are using Remote Hotdesk Authentication (RHA), long I/O operations might fail when using mass storage devices on Sun Ray DTUs.

If these types of sessions become idle due to keyboard and mouse inactivity long enough to activate the screen lock, the session is detached. The user loses access to the storage device, causing any I/O in progress to halt, and data may become corrupted.

To avoid this situation, the following options are available:

- Maintain keyboard or mouse activity
- Increase the screen lock idle time sufficiently to allow I/O operations to complete
- Disable the screen lock program
- Disable the RHA policy
- Find an alternative way to perform the I/O operation more securely, for example, plug the device directly into the Sun Ray server in a locked server room

**Note**

Some of these options have security and convenience implications that should be carefully weighed against the timeout issue to determine what is best for your site.

Commands for Common Disk Operation on Linux Platforms

The following table is a summary of common disk operations and the commands used to perform them.

Operation	Command	Device Name Argument Examples
Create file system	<code>mkfs</code>	Path of partition <code>\$UTDEVROOT/dev/dsk/disk3p1</code>
Mount	<code>utdiskadm -m</code>	Partition name <code>disk3p1</code>
Unmount	<code>utdiskadm -u</code>	Mount point <code>\$DTDEVROOT/mnt/label1</code>
Prepare to unplug	<code>utdiskadm -r</code>	Device alias <code>disk3</code>
Eject media	<code>utdiskadm -e</code>	Device alias <code>disk3</code>
Check for media	<code>utdiskadm -c</code>	Device alias <code>disk3</code>
Create fdisk table	<code>fdisk</code>	Path of whole disk <code>\$UTDEVROOT/dev/dsk/disk3</code>
Repair file system	<code>fsck</code>	Path of partition <code>\$UTDEVROOT/dev/dsk/disk3p1</code>
Display file system capacity	<code>df -k</code>	Mount point <code>\$DTDEVROOT/mnt/label1</code>

List devices	utdiskadm -l	None
--------------	--------------	------

How to Determine the Current State of Device Services

The `utdevadm` command displays the enabled or disabled state of device services.

```
# utdevadm
```

How to Enable or Disable USB Services

To enable USB services, use the `utdevadm` command.

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

To disable USB services, use the `utdevadm` command.

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

How to Set Up an Attached PostScript Printer (Solaris)

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 [How to Set Up an Attached Non-PostScript Printer](#).



Note

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

For more information on Solaris Ready™ printers, go to <http://www.sun.com/solarisready/>.

Starting a print queue on a printer attached to a Sun Ray DTU, either directly or through an adapter, is the same process as starting a print queue in the Solaris OS.

Steps

1. On the Sun Ray DTU where the printer is attached, log in to a new session as superuser (root).
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 below 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. Add the new printer.
 - a. Start the Solaris Print Manager.

```
# /usr/sbin/printmgr &
```

- b. Click OK to choose files for repository.
 - c. Go to Printer -> New Attached Printer.
 - d. Type the following information:
 - Printer name: printername
 - Description (optional)
 - Printer port
 - Printer make
 - Printer model
 Choose Other to type the printer port path name. To locate the printer port, refer to Step 4.
7. Verify that the printer has been set up correctly.

```
# lpstat -d <printername>
```

How to Set Up an Attached PostScript Printer (Linux)

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 [How to Set Up an Attached Non-PostScript Printer](#).



Note

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

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

Steps

1. On the Sun Ray DTU where the printer is attached, log in to a new session as superuser (root).
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 below the connection icon is the MAC address.
3. Locate the Sun Ray DTU.

```
# 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.

```
# 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.
Choose Other so that you can provide the device node from Step 4.
7. Verify that the printer has been set up correctly.

```
# lpstat -d <printername>
```

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>`,
you would 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
```

How to Set Up an Attached Non-PostScript Printer

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 the following:

- 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.

How to Set Up Serial Attached Devices

To use serial attached devices with a DTU, you must attach them either to internal serial ports or by using USB-to-Serial adapters listed on the [Sun Ray Hardware Compatibility List](#).

All ports except port A on the Sun Ray 170 support full handshaking and standard UNIX semantics. Port A on the Sun Ray 170 has no hardware handshaking pins, so it can't be used when a hardware handshake is required.

Symbolic links to the serial port device nodes are located under `$UTDEVROOT/dev/term`. Built-in ports are named "a" or "b", and serial adapter ports have longer descriptive names.

Serial ports become unowned during hotdesking, so you should make sure any serial port activity is stopped before removing your smart card or resetting the DTU.

How to Enable Applications to Access USB Devices

`libusb` is an open-source userland USB API/library that enables an application to access USB devices. `libusb` has been implemented for a number of operating environments, including Linux, BSD, MacOS, and Windows, as well as for Solaris and Sun Ray environments.

`libusb` applications can run on any operating environment that supports `libusb`. For further information, see `/usr/sfw/share/doc/libusb/libusb.txt`.

The following table lists some open source applications that make use of `libusb` support and enable users to access scanners, digital cameras, and other devices.

Open-Source `libusb` Applications

Application	URL	Comments
Sane	http://www.sane-project.org	For scanner support
Gphoto	http://www.gphoto.org	For digital still cameras
ColdSync	http://www.coldsync.org	For Palm device support

For further information, please see:

- <http://sourceforge.net>
- [Sun Download Center](#)
- The `libusb` man page

How to Unmount a Mass Storage Device From a DTU



Caution

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 devices.

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

Troubleshooting Printers

Problem: "Failed to open the printer port" message.

Verify that the printer node used for configuring the printer has been created and is available under `/tmp/SUNWut/units/IEEE802.<macid>/dev/printers`.

If the printer node is not available, reboot the DTU.

Troubleshooting USB Storage

Problem: Device nodes are not created.

Check the log file `/var/opt/SUNWut/log/utstoraged.log` for a message about why device nodes were not created. Some mass storage device types are not supported.

Problem: The device is not automatically mounted.

Check the log file `/var/opt/SUNWut/log/utmountd.log` for an error message.

This condition occurs when the Sun Ray operating system does not recognize the storage devices's file system.

Problem: The device is not automatically unmounted.

This condition occurs when a user still has an open reference to the mount point at the time the storage device is unplugged or the user's session is disconnected. The mount point becomes a stale mount point and persists until the system is rebooted or until the administrator removes it.

How to Find and Remove Stale Mount Points

1. Search for stale mount points:

```
# utdiskadm -s
```

2. For each stale mount point, close all references to the mount point.
3. For each stale mount point, terminate all processes that refer to the mount point.
4. Remove the mount point.

```
# umount <stale_mount_path>
```

Contents

- [How to Power Cycle a Sun Ray DTU](#)
 - [How to Power Cycle a Sun Ray DTU \(Hard Reset\)](#)
 - [How to Power Cycle a Sun Ray DTU \(Soft Reset\)](#)
- [How to Terminate a DTU Session](#)
- [How to Disconnect a DTU Session](#)
- [How to Redirect a DTU Session](#)
 - [How to Redirect to a Different Server](#)
 - [How to Redirect a DTU Manually](#)
 - [How to List Available Hosts](#)
- [How to Disable Screen Blanking on a Sun Ray DTU](#)
- [How to Enable or Disable XRender](#)
 - [How to Disable XRender as the Default for All Clients](#)
- [How to Modify Screen Resolutions](#)
- [How to Display DTU Information](#)
- [How to Change Sun Ray DTU Settings](#)
 - [Sun Ray Settings GUI](#)
 - [utset Command](#)
- [Sun Ray DTU Hot Keys](#)
 - [Non-Configurable Hot Keys](#)
 - [Configurable Hot Keys](#)
- [How to Change Hot Key Settings for All Users](#)
- [How to Change the Hot Key Settings for a Single User](#)
- [About GNOME Display Manager \(GDM\) \(Linux\)](#)
 - [Installation of GDM](#)
 - [Uninstallation of GDM](#)
 - [Configuration of GDM](#)
 - [Bundled Greeter](#)
- [How to Limit Administrative Privileges for Non-root Users \(Linux\)](#)
- [Troubleshooting Audio Output](#)
 - [Tracking Audio Sessions](#)
 - [Audio Device Emulation](#)
 - [Problem: Audio is not working.](#)
 - [Problem: Audio is not working with Firefox.](#)
 - [Problem: An application ignores the \\$AUDIODEV environment variable.](#)
- [Keyboard Country Codes](#)

Managing Sun Ray DTU User Settings and Sessions (All Topics)

How to Power Cycle a Sun Ray DTU

How to Power Cycle a Sun Ray DTU (Hard Reset)

To power cycle a DTU with a hard reset:

- Disconnect and then reconnect the power cord.
- Press the power button if one is available.

How to Power Cycle a Sun Ray DTU (Soft Reset)

To power cycle a DTU with a soft reset, press 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. Therefore, the soft reset key sequence is often called `Ctrl+Moon`.

How to Terminate a DTU Session

To terminate the current session and the current X server process, perform one of the following actions:

- Choose Launch->Log Out from your JDS desktop.
- Press the key combination `Ctrl+Alt+Bksp+Bksp`.

A momentary delay might occur before the session terminates.



Caution

Use `Ctrl+Alt+Bksp+Bksp` only for emergencies when you are unable to log out from the desktop. When using this method, applications will not have the opportunity to exit properly and save data, and some application data corruption might result.

How to Disconnect a DTU Session



Note

NSCM and RHA sessions are disconnected if the screen lock idle time interval is exceeded. See [Mass Storage Devices \(Linux\)](#) and [Mass Storage Devices \(Solaris\)](#).

You can disconnect a DTU session through any of the following methods:

- Lock the session through the current desktop manager. For example, in the Java Desktop System, choose Launch->Lock Screen.
- Type the following command:

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

- Press `Shift+Pause`.
To change the disconnect hot key combination, see [Sun Ray DTU Hot Keys](#).



Note

The hot key combination does not work with a full-screen Windows session.

- Connect to your session through another DTU, either by inserting your smart card and authenticating to RHA or by logging in through NSCM.

How to Redirect a DTU Session

A DTU session is redirected to the appropriate server based on the following situations:

- Failover Group redirection occurs after token insertion.
- Regional Hotdesking redirection (if configured) occurs after token or user identification and before user authentication.

To redirect a session to a different server manually, use the `utselect` graphical user interface (GUI) or the `utswitch` command.

How to Redirect to a Different Server

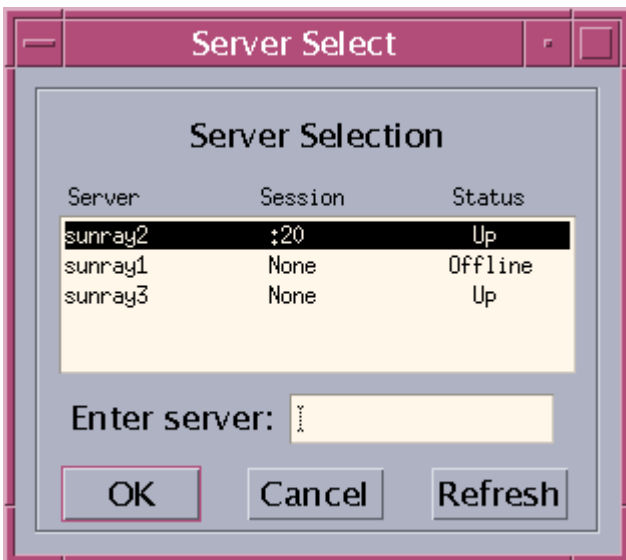
- From a shell window on the DTU, type:

```
% utselect
```

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

In the following figure, 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 selected by default. Select a server from the list or type 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.

Server Selection (`utselect`) GUI



This screen enables the user to select a server in a failover group.

How to Redirect a DTU Manually

- In a shell window on the DTU, type the following command:

```
% utswitch -h <host>
```

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

How to List Available Hosts

- In a shell window, type the following command:

```
% utswitch -l
```

Hosts within the current server group that are available to the Sun Ray DTU are listed.

How to Disable Screen Blanking on a Sun Ray DTU

There may be times when users do not want their DTUs in power saving mode, during which the screen goes blank after a specific period of nonuse.

Power management is a feature of the Sun Ray Server Software and it is enabled by default. There are a couple of ways to disable power saving mode.

To Disable Power Saving Mode...	Then...
At the desktop environment level,	<p>Refer to your desktop documentation about how to disable the power management feature or the screensaver feature.</p> <p>Here are some examples:</p> <ul style="list-style-type: none"> • Use the <code>xset</code> command. • For Solaris, make sure that <code>xscreensaver</code> (JDS) or <code>dtsession</code> (CDE) is disabled or configured to not blank or lock the screen. If active, <code>xscreensaver</code> overrides any settings you have made using the <code>xset</code> command. See the <code>xscreensaver(1)</code> man page for details. • For Linux, make sure that <code>gnome-screensaver</code> is disabled or configured to not blank or lock the screen. See the <code>gnome-screensaver-command(1)</code> man page for details.
From the Sun Ray DTU level,	Set the <code>Advanced->Video->Blanking</code> parameter to 0 in the Sun Ray DTU Pop-up GUI, if enabled. For more details, see How to Set DTU Configuration Parameters (Pop-up GUI) .

How to Enable or Disable XRender

The X Rendering Extension (XRender) allows applications on a client to use a rendering model based on Porter-Duff compositing. XRender is enabled by default because many new X applications require XRender to improve performance or to even function properly.

However, some applications use of XRender may conflict with optimizations in the Sun Ray protocol and create an increase in both CPU loading and network bandwidth consumption. In these instances, the applications may see a performance benefit by disabling the XRender extension.

If Sun Ray clients experience performance degradation with a particular application after upgrading to Sun Ray Software 5, use the following procedure to disable XRender.



Note

After enabling or disabling XRender, users must restart their current Sun Ray session (`Ctrl+Alt+Bksp+Bksp`) for the change to take affect. Or, they can log out from their current session and log back in.

To disable XRender on a client, type the following command:

```
% utxconfig -n off
```

To enable XRender on a client, type the following command:

```
% utxconfig -n on
```

How to Disable XRender as the Default for All Clients

1. Become root on the Sun Ray server.
2. Disable XRender as the default, overriding all user configured and system default settings.

```
# utxconfig -A -n off
```



Note

You can use the `-A` option to make the setting mandatory for all DTU users, regardless of their personal settings. See the `utxconfig` man page for details.

How to Modify Screen Resolutions

Sun Ray users can modify their screen resolution settings by invoking the `utsettings` command.

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 the `utsettings` command apply only to the DTU where the command is run.

When a user moves to another DTU, the resolution settings do not accompany the user to the new DTU, but the settings remain effective for the user's session on the original DTU if the user returns to the session through hotdesking.

If the session is associated with a personal mobile token, such as a smart card or an NSCM credential, a message displays offering 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 particular monitor timing to be used in the following situations:

- Whenever a specific token is presented on a specific DTU
- On a specific DTU regardless of the token that is presented at the DTU
- On all DTUs regardless of the token that is presented at the DTU

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

For further details, see the `utsettings` and `utresadm` man pages.

How to Display DTU Information

This procedure describes how to view information, including the currently installed firmware, about registered DTUs.

Command-Line Steps

1. Log in to the Sun Ray server.
2. Display information about a DTU.

```
utdesktop -p <desktopID>
```

where `<desktopID>` is the Sun Ray DTU identifier.

Admin GUI Steps



Note

To facilitate the searching process, you can use the Admin GUI to edit DTU properties. Click the DTU Identifier and then click edit. You can then provide a location or other information.

- Click the Desktop Units tab.
From the Desktop Units tab, you can do the following:
 - To display information about a specific DTU, click on the DTU Identifier (MAC address) or enter a search string in the text field.
 - To display information about a group of DTUs, select an option from the drop-down menu (All Connected Desktop Units,

Token Readers, or Multihead Groups) and/or enter a search string in the text field to narrow your search.

How to Change Sun Ray DTU Settings

Sun Ray Settings GUI

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

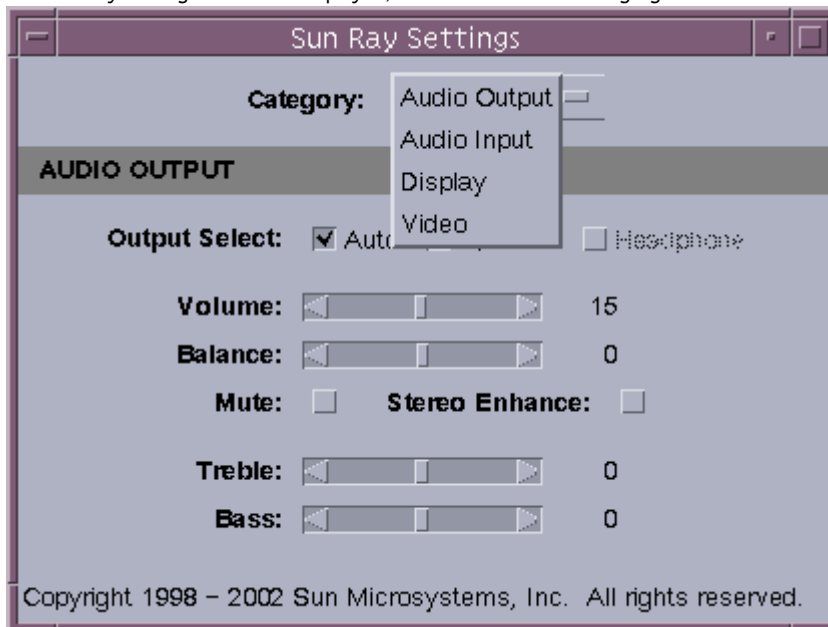
The Sun Ray Settings GUI contacts the Session Manager to determine which DTU is currently being used and connects to that unit to get the current values. The GUI maintains a connection to the Session Manager so that the Session Manager can notify the GUI if the user moves to another DTU by removing the smart card and inserting it into another DTU.

Steps

1. Press the Settings hot key or run the `utsettings` command.

The default Settings hot key combination is Shift+Props but this assignment can be reconfigured, as described in [Sun Ray DTU Hot Keys](#).

The Sun Ray Settings window is displayed, as shown in the following figure:



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

Changes to the monitor signal timing through the **Resolution/Refresh Rate** setting require confirmation before and after the change is applied to the DTU. All other changes take effect immediately.

4. Dismiss the Sun Ray Settings window.
 - If the window was launched by the Settings hot key, press the hot key again or apply the window manager's `close` action to that window.
 - If the window was launched by invoking `utsettings` directly, apply the window manager's `close` action to that window.

utset Command

The `utset` command provides a non-GUI mechanism for reporting and modifying Sun Ray DTU settings. For details, refer to the `utset` man page.

Sun Ray DTU Hot Keys

The Sun Ray Server Software provides a number of keyboard shortcuts, referred to as hot key sequences or hot keys, which can be used to trigger certain activities either on the DTU or within the Sun Ray session running on the Sun Ray server.

Some of these hot key sequences have fixed definitions that cannot be modified. Others have definitions that can be reconfigured by a user or by an administrator.

The activities controlled by these hot keys are specific to Sun Ray. Desktop software running in the Sun Ray session might provide a separate keyboard shortcut facility that provides additional hot keys for desktop activities, perhaps including the ability to launch certain programs.

Non-Configurable Hot Keys

The Sun Ray hot keys listed in the following table cannot be reconfigured. These hot key activities can be triggered by using either a Sun-specific key combination (using keys that might exist only on Sun keyboards) or by an alternative key combination that does not require Sun-specific keys.

Sun-specific Hot Key	Non-Sun Hot Key	Action
Mute	Ctrl+Pause+CursorDown	Audio mute and unmute.
Softer	Ctrl+Pause+CursorLeft	Decreases the audio volume.
Louder	Ctrl+Pause+CursorRight	Increases the audio volume.
Mute+Softer+Louder	Ctrl+Pause+N	Displays the DTU MAC and IP addresses and server IP address.
Ctrl+Power	Ctrl+Pause+A	Power cycles the DTU. On a Sun keyboard the <code>Power</code> key carries a crescent moon glyph and is positioned at the top right corner of the keyboard.
Stop+C	Ctrl+Pause+C	Clears any local configuration data on the DTU.
Stop+S or Stop+M	Ctrl+Pause+S or Ctrl+Pause+M	Activates the DTU's local Pop-up GUI to configure the DTU. This GUI is available only when the DTU has been loaded with GUI-capable firmware.
Stop+V	Ctrl+Pause+V	Shows the DTU's model, MAC address, and firmware version.
Ctrl+Alt+Bksp+Bksp	Ctrl+Alt+Bksp+Bksp	Terminates a session. This hot key cannot be reconfigured to another value, but it can be disabled. For details, see the <code>utxconfig</code> man page.
Ctrl+Alt+Del+Del	Ctrl+Alt+Del+Del	Terminates the process that has taken control of the X server.

Configurable Hot Keys

Hot keys can be configured to launch the `utsettings` or `utdetach` Sun Ray utilities. The scopes for these hot keys are as follows:

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

To support these levels of customization, at session startup Sun Ray examines a series of properties files in the order shown in the table below.

Sun Ray Settings Properties Files

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

If your policy is for all users to use the same standard hot key, modify the system-wide mandatory defaults file to specify this standard key. This setting 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 (currently either `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. Default values are shown in the following table.

Defaults for Configurable Hot Key Values

Configuration Property Name	Default Hot Key	Action
<code>utsettings.hotkey</code>	<code>Shift+Props</code>	Invokes the DTU Settings GUI.
<code>utdetach.hotkey</code>	<code>Shift+Pause</code>	Detaches the session from this DTU. (Often used to to detach a non-smartcard mobile session.)

How to Change Hot Key Settings for All Users

If you don't want your users to use the default hot keys, you can set up the system-wide defaults file to specify different hot keys. Users can still specify their preferences in the user defaults file.

You can change the following hot keys:

- `utsettings.hotkey`: Launches the DTU Settings GUI
- `utdetach.hotkey`: Detaches the session from the DTU

See [Sun Ray DTU Hot Keys](#) for details.

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



Note

If you want to make the change mandatory for all users even if they have user defaults set, change the value in the `/etc/opt/SUNWut/utslaunch_mandatory.properties` file.

2. Locate the original hot key entry for the utility you want to change and place a `#` in front of it to comment it out.

For example:

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

3. Type the new hot key property after the first statement.

For example,

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

4. Save the `utslaunch_defaults.properties` file.

The new hot key takes effect for each user when that user next logs in. Users who were logged in before you redefined the hot key continue to use the old value.

How to Change the Hot Key Settings for a Single User

You can change the following hot keys:

- `utsettings.hotkey`: Launches the DTU Settings GUI
- `utdetach.hotkey`: Detaches the session from the DTU

A user's hot key settings override any system-wide default settings, unless they are mandatory. See [Sun Ray DTU Hot Keys](#) for details.

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.

About GNOME Display Manager (GDM) (Linux)

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

Installation of GDM

During the SRSS installation process, you are asked whether the installation script should remove the existing GDM from your system if your GDM version is earlier than 2.12. Answer Yes to this question to continue with the SRSS installation, remove the old GDM from your system, and install the Sun Ray enhanced version. If you answer No, the SRSS install process quits.

Because older GDM versions are removed during SRSS installation, do not use a GDM-controlled display for the installation. Use either a telnet session into the server or a virtual terminal.

Uninstallation of GDM

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

Configuration of GDM

Sun Ray installation removes the current GDM from your system, including its configuration file. Therefore, if you have modified your GDM configuration, back up the file before installing SRSS. You may then wish to reapply your changes to the `/etc/X11/gdm/custom.conf` file that SRSS installs.



Caution

Do not simply replace the GDM configuration file that Sun Ray Server Software installs with your old GDM configuration file. The Sun Ray Server Software will not work correctly if you do.

Bundled Greeter

If you are using Kiosk mode, please see the `kiosk` man page for details about the bundled GDM greeter. See also [Managing Kiosk Mode](#).

How to Limit Administrative Privileges for Non-root Users (Linux)

Many Linux systems come configured with liberal administrative privileges for non-root users. These privileges should not be made available to users who log in using a Sun Ray DTU.

To limit administrative access, do the following:

- Review the man pages for `pam_console`, `console.perms`, and `console.apps`.

- 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.

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 the following example should be removed:

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

Troubleshooting Audio Output

Tracking Audio Sessions

Each time a user logs in to a Sun Ray DTU, a script automatically assigns the `$AUDIODEV` environment variable to that session. One `utaudio` process is assigned to each session. Refer to the `utaudio` and `audio` man pages for more information.

Audio Device Emulation

During hotdesking, an emulated audio device follows the user to the new session. The name of the emulated device is carried in the `$AUDIODEV` environment variable. It is the responsibility of the audio application to inspect `$AUDIODEV` and direct its output to that device.

The emulated audio devices are created as device nodes in the `/tmp/SUNWut/dev/utaudio` directory. This directory tree is recreated at boot time.



Caution

Do not remove the `/tmp/SUNWut/dev/utaudio` directory. If you delete this directory, users with `utaudio` sessions cannot use their audio pseudo device nodes.

Problem: Audio is not working.

- Use the Sun audio keys (top right of keyboard) and check the volume and mute buttons.
- Display the Sun Ray session's audio settings:

```
$ utsettings
```

and verify that the audio output is selected properly, for example, for headphones or speakers.

- Make sure the volume is not muted in your desktop session.
- Try a set of external speakers plugged into the Sun Ray's audio out or headphones port. If that works, the Sun Ray might have a broken speaker.
- To test whether the audio is working, type the following:

```
$ cat <audiofile> > $AUDIODEV
```

Solaris provides suitable sample PCM-encoded audio files in `/usr/share/audio/samples/au`, so for instance this command:

```
$ cat /usr/share/audio/samples/au/gong.au > $AUDIODEV
```

should produce the sound of a gong.

Linux generally does not provide PCM-encoded audio files. If you can not locate a suitable file then this command can be used to generate a continuous tone:

```
$ perl -e 'foreach(-8..8){push(@v,pack("n",4*$_))} while(1){print @v}' > $AUDIODEV
```

If the `cat` or `perl` command hangs, you might need to quit any other applications that are currently trying to play audio, for example, a browser.

Problem: Audio is not working with Firefox.

- Check the current release of the Flash plugin and make sure it is at version 9.0.r125 or later. To check the Flash plugin version, type `about:plugins` as the URL in the browser.
- Try quitting Firefox and explicitly restart it in a terminal window: `/usr/dist/exe/firefox`.
- If all else fails, quit Firefox, go to your `.mozilla` directory, and rename the "firefox" directory to something else, for example, `firefox.jan09`. Then, restart Firefox and see whether the audio works with a completely clean configuration.

If the audio works with the clean configuration, then something is wrong in your browser's previous configuration.

Problem: An application ignores the \$AUDIODEV environment variable.

Some applications fail to honor `$AUDIODEV` and unconditionally use a specific audio device node such as `/dev/audio` or `/dev/dsp`. To work around this shortcoming Sun Ray Server Software provides a preloadable shared library `libc_ut.so` that can be used to interpose on an application and redirect its activities to the device specified by `$AUDIODEV`. To put this redirection into effect:

1. Navigate to the shell or wrapper from which you started the audio player.
2. Set the environment variable `LD_PRELOAD` in the player application's environment to refer to the `libc_ut.so` interposer:

```
$ LD_PRELOAD=libc_ut.so
$ export LD_PRELOAD
```

3. Restart the application.

Keyboard Country Codes

A keyboard country code is a number representing a specific USB keyboard map that can be set in the Sun Ray client firmware to provide better Non-US keyboard support. This code is needed if the keyboard returns a country code of 0.

The code can be set through the [Pop-Up GUI](#) or the `.parms` file.

Keyboard Country Codes

- 1 Arabic
- 2 Belgian
- 3 Canada_Bi
- 4 French-Canadian
- 5 Czech
- 6 Denmark
- 7 Finnish
- 8 France
- 9 Germany
- 10 Greek
- 12 Hungarian
- 14 Italy

- 15 Japan
- 16 Korea
- 17 Latin-American
- 18 Netherland
- 19 Norway
- 21 Polish
- 22 Portugal
- 23 Russia
- 24 Slovakian
- 25 Spain
- 26 Sweden
- 27 Switzerland
- 28 Switzerland_Ge
- 30 Taiwan
- 31 TurkeyQ
- 32 UK-English
- 33 US-English
- 35 TurkeyF

Contents

- Sun Ray System Commands
- Man Pages
 - Solaris Man Pages
 - Linux Man Pages
 - How to View a Man Page (SUNWut Man Pages)
 - How to View a Man Page (SUNWkio Man Pages)
- Administrative Name and Password
- Admin GUI Functionality
- How to Log In to the Administration Tool (Admin GUI)
- How to Change the Admin GUI Locale
- How to Change the Admin GUI to English Locale
- How to Change the Admin GUI Timeout
- How to Start or Stop Sun Ray Services
 - How to Stop Sun Ray Services
 - How to Start Sun Ray Services (Warm Restart)
 - How to Start Sun Ray Services (Cold Restart)
- How to Display DTU Information
- User Fields in the Sun Ray Data Store
- How to Restart the Sun Ray Data Store (SRDS)
- How to Enable or Disable Multiple Administration Accounts (Solaris)
 - How to Configure UNIX Users to Have Admin GUI Privileges
 - How to Configure Only Admin to Have Admin GUI Privileges
- How to Enable or Disable Multiple Administration Accounts (Linux)
 - How to Configure UNIX Users to Have Admin GUI Privileges
 - How to Configure Only Admin to Have Admin GUI Privileges
- How to Audit Admin GUI Sessions

Sun Ray System Commands

The important commands used to administer the Sun Ray System are listed below. For further information, see the man page for the command in question.

See the [Man Pages](#) page to view the man pages for any of these commands.

Command	Definition
utaction	Provides a way to execute commands when a Sun Ray DTU session is connected, disconnected, or terminated.
utadm	Manages the private network, shared network, and DHCP (Dynamic Host Configuration Protocol) configuration for the Sun Ray interconnect.

<code>utadminuser</code>	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.
<code>utamghadm</code>	Used to configure or disable regional hotdesking, which enables users to access their sessions across multiple failover groups. Regional hotdesking was previously known as Automated Multigroup Hotdesking (AMGH).
<code>utcammigrate</code>	(Solaris only) Used to migrate existing CAM configuration to its Kiosk Mode equivalent with the intention of migrating from existing CAM sessions to Kiosk sessions. This migration includes the creation of Kiosk application descriptors, prototypes, session configuration and application lists. The migration does not include support for CAM wrapper scripts.
<code>utcapture</code>	Connects to the Authentication Manager and monitors packets sent and packets dropped between the Sun Ray server and the Sun Ray DTUs.
<code>utcard</code>	Enables the configuration of different types of smart cards in the Sun Ray Data Store
<code>utconfig</code>	Performs the initial configuration of the Sun Ray server and supporting administration framework software.
<code>utcrypto</code>	Used for security configuration.
<code>utdesktop</code>	Enables the user to manage Sun Ray DTUs connected to the Sun Ray server on which the command is run.
<code>utdetach</code>	Disconnects the current non-smart card mobile session or authenticated smart card session from its respective Sun Ray DTU. The session is not destroyed but put into a detached state. The session can be accessed again only after authentication. When Remote Hotdesk Authentication (RHA) is disabled (through <code>utpolicy</code> or the Admin GUI), <code>utdetach</code> affects only authenticated smart card sessions and non-smart card mobile sessions.
<code>utdevadm</code>	Used to enable/disable Sun Ray device services. The devices include USB devices connected through USB ports, embedded serial ports, and the internal smart card reader in the Sun Ray DTU.
<code>utdiskadm</code>	Used to administer Sun Ray mass storage.
<code>utdssync</code>	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.
<code>uteject</code>	Used to eject media from a removable storage media device.
<code>utfwadm</code>	Manages firmware versions on the Sun Ray DTUs.
<code>utfwload</code>	Used primarily to force the download of new firmware to a DTU running older firmware than its server.
<code>utfwsync</code>	Refreshes the firmware level on the Sun Ray DTUs to the level available on the Sun Ray servers in a failover group. It then forces all the Sun Ray DTUs within the group to restart.
<code>utgmtarget</code>	Manages a group-wide list of explicit destinations for Sun Ray group membership announcements.
<code>utgroupsig</code>	Sets the failover group signature for a group of Sun Ray servers. The <code>utgroupsig</code> command also sets the Sun Data Store <code>rootpw</code> used by Sun Ray to a value based on the group signature. Although <code>utgroupsig</code> sets the <code>rootpw</code> in the <code>utdsd.conf</code> file, it does not set the admin password, which is a separate entity, in the data store.
<code>utgstatus</code>	Enables the user to view the failover status information for the local server or for the named server. The information that the command displays is specific to that server at the time the command is run.
<code>utinstall</code>	Used to install, upgrade, and remove the Sun Ray Server Software.
<code>utkiosk</code>	Used to import/export kiosk configuration information into the data store. It also supports storage of multiple named kiosk session configurations in the data store.
<code>utkioskoverride</code>	Provides a way to set the session type associated with a token, to select a kiosk session configuration for a token associated with a kiosk session, or to query the session type and kiosk session currently associated with a token.
<code>utmhadm</code>	Provides a way to administer Sun Ray server multihead terminal groups. The information that <code>utmhadm</code> displays and that is editable is stored in the data store.
<code>utmhconfig</code>	Enables an administrator to list, add, or delete multiheaded groups easily.
<code>utmount</code>	Used to mount a file system on a Sun Ray mass storage device.
<code>utpolicy</code>	Sets and reports the policy configuration of the Sun Ray Authentication Manager, <code>utauthd</code> .
<code>utpreserve</code>	Saves existing Sun Ray Server Software configuration data to the <code>/var/tmp/SUNWut_upgrade</code> directory.

<code>utpw</code>	Changes the Sun Ray administrator password (also known as the UT admin password) used by the Web-based and command-line administration applications.
<code>utquery</code>	Collects DHCP information from the Sun Ray DTUs.
<code>utreader</code>	Used to add, remove, and configure token readers.
<code>utreplica</code>	Configures the Sun Ray Data Store server to enable replication of administered data from a designated primary server to each secondary server in a failover group. The data stores of the secondary servers remain synchronized automatically unless there is a power outage. The <code>-z</code> option is useful for updating the port number.
<code>utresadm</code>	Enables an administrator to control the resolution and refresh rate of the video monitor signal (persistent monitor settings) produced by the Sun Ray unit.
<code>utresdef</code>	Enables an administrator to create, delete, and view resolution definitions, that is, monitor signal timing definitions for monitors attached to Sun Ray DTUs.
<code>utrestart</code>	Used to start Sun Ray services.
<code>utselect</code>	Presents the output of <code>utswitch -l</code> as a list of servers in the current host group, to be used for reconnection of the current DTU. A user can either select a server from this list or specify a server not in the current host group by typing its full name in the <code>utselect</code> text box.
<code>utsession</code>	Lists and manages Sun Ray sessions on the local Sun Ray server.
<code>utset</code>	Enables a user to view and change Sun Ray DTU settings.
<code>utsettings</code>	Opens a Sun Ray Settings dialog box that enables the user to view or change audio and visual settings for the Sun Ray DTU.
<code>utsummc</code>	(Solaris only) Adds the Sun Ray Server Software module to the Sun Management Center (SunMC) and loads it to permit monitoring of Sun Ray Server Software. The <code>utsummc</code> command can also remove the Sun Ray Server Software module from SunMC.
<code>utsummcinstall</code>	(Solaris only) Used to install and uninstall the Sun Ray module for SunMC on a SunMC server where Sun Ray Server Software is not installed.
<code>utswitch</code>	Enables a Sun Ray DTU to be switched among various Sun Ray servers. <code>utswitch</code> can also list existing sessions for the current token.
<code>utumount</code>	Used to <code>unmount</code> a file system from a Sun Ray mass storage device.
<code>utuser</code>	Reports Sun Ray user token registrations and enables the administrator to manage those registrations. <code>utuser</code> is able to obtain smart card token values from DTUs that are configured as dedicated token reader devices.
<code>utwall</code>	Sends a message or an audio file to users having an Xnewt or Xsun (X server unique to Sun Ray) process. The messages can be sent in email and displayed in a pop-up window.
<code>utwho</code>	Assembles information about display number, token, logged-in user, and the like, in a compact format.
<code>utxconfig</code>	Manages X server configuration parameters for users of Sun Ray DTU sessions.

Man Pages



Note

To search for a specific command in the following pages, use your browser's find tool to search within the page.

Solaris Man Pages

The following links provide the entire output for each of the man page sections.

- [User Commands - man\(1\)](#)
- [System Administration Commands - man\(1m\)](#)
- [Interface Plugins - man\(3\)](#)
- [File Formats - man\(4\)](#)
- [Standards, Environments, and Macros - man\(5\)](#)

- [Device Drivers - man\(7d\)](#)

Linux Man Pages

- [User Commands - man\(1\)](#)
- [Interface Plugins - man\(3\)](#)
- [Device Drivers - man\(4\)](#)
- [File Formats - man\(5\)](#)
- [System Administration Commands - man\(8\)](#)

How to View a Man Page (SUNWut Man Pages)

```
% man -M /opt/SUNWut/man <command>
% setenv MANPATH=/opt/SUNWut/man
% man <command>
```

How to View a Man Page (SUNWkio Man Pages)

```
% man -M /opt/SUNWkio/man <command>
% setenv MANPATH=/opt/SUNWkio/man
% man <command>
```

Administration Tool (Admin GUI)

The Sun Ray Administration Tool (Admin GUI) is organized around primary Sun Ray objects such as servers, sessions, desktop units, and tokens. Each type of object has a dedicated tab that provides related functionality.

To access the Admin GUI, see [How to Log In to the Administration Tool \(Admin GUI\)](#).

Administrative Name and Password

The default user name for the administration account is `admin`.





The password is the one that was specified when the Sun Ray server was configured. For more information, see [How to Configure the Sun Ray Server Software](#). To change the administration password, use the [Advanced tab](#).





To allow another user account to perform administrative functions, see [How to Enable or Disable Multiple Administration Accounts \(Solaris\)](#) or [How to Enable or Disable Multiple Administration Accounts \(Linux\)](#).



Admin GUI Functionality

The Admin GUI provides the following functionality:

Tab	Functions	Screenshot
-----	-----------	------------

<p>Servers</p>	<p>From the Servers tab, you can do the following tasks:</p> <ul style="list-style-type: none"> • List all of the servers in the failover group. • Display the host group's network connectivity status. • Show the host group's installed Sun Ray packages. • Display details about each server. • Perform a warm restart of Sun Ray services on a local or failover group basis. A warm restart does not terminate sessions prior to the restart. • Perform a cold restart of Sun Ray services on a local or failover group basis. A cold restart terminates all sessions on the selected servers prior to the restart. 	
<p>Sessions</p>	<p>From the Sessions tab, you can do the following tasks:</p> <ul style="list-style-type: none"> • List all the sessions, sorted by user sessions and idle sessions. • Use the search function to find specific sessions such as those running on a single server or sessions where a specific user is logged in. • Select a session's server to display details about the server or DTU and to select and terminate sessions. 	
<p>Desktop Units</p>	<p>From the Desktop Units tab, you can do the following tasks:</p> <ul style="list-style-type: none"> • List all registered DTUs and Sun Desktop Access Clients. • List all connected DTUs and Sun Desktop Access Clients. • List all DTUs configured as token readers. • List all DTUs and Sun Desktop Access Clients participating in multihead groups. 	
<p>Tokens</p>	<p>From the Tokens tab, you can do the following tasks:</p> <ul style="list-style-type: none"> • Manage the tokens associated with users. • Manage the pseudo-tokens associated with DTUs. 	
<p>Advanced</p>	<p>The Advanced tab includes the following subtabs:</p>	

<p>Security Subtab From the Security subtab, you can disable and re-enable security settings, such as encryption of communication between DTU and server, server authentication, security mode, and device access.</p>		 <p>The screenshot shows the 'Security' subtab in the Sun Ray Administration interface. It features a navigation bar with 'Security', 'System Policy', 'Kiosk Mode', 'Card Probe Order', and 'Data Store Password'. The main content area is titled 'Security' and includes sections for 'Encryption and Server Authentication', 'Client Authentication', and 'Devices'. Each section contains several checkboxes for enabling or disabling various security features.</p>
<p>System Policy Subtab From the System Policy subtab, you can regulate authentication manager policy settings, such as:</p> <ul style="list-style-type: none"> • Access for card users and non-card users, which includes enabling Kiosk Mode, Sun Desktop Access Client (Software Client) access, or Mobile Sessions. • Enabling Client Authentication • Enabling the Multihead feature, • Session Access when Hotdesking 		 <p>The screenshot shows the 'System Policy' subtab. It has a navigation bar with 'System Policy', 'Kiosk Mode', 'Card Probe Order', and 'Data Store Password'. The main content area is titled 'System Policy' and includes sections for 'Card Users', 'Non-Card Users', 'Multihead Sessions', 'Client Authentication', and 'Resource Access when Hotdesking'. Each section contains checkboxes for enabling or disabling specific policy settings.</p>
<p>Kiosk Mode Subtab From the Kiosk Mode subtab, you can configure Kiosk Mode for your system.</p>		 <p>The screenshot shows the 'Kiosk Mode' subtab. It has a navigation bar with 'Kiosk Mode', 'Card Probe Order', and 'Data Store Password'. The main content area displays a message: 'No Kiosk Mode Settings Exist in Sun Ray Data Store. Click the Edit button to specify Kiosk Mode settings.' There is an 'Edit' button at the bottom right.</p>
<p>Card Probe Order Subtab From the Card Probe Order subtab, you can rearrange the order that smart cards are probed. You can move the cards that are used most frequently to the top of the list.</p>		 <p>The screenshot shows the 'Card Probe Order' subtab. It has a navigation bar with 'Card Probe Order' and 'Data Store Password'. The main content area is titled 'Card Probe Order' and includes a table with columns: Name, Multi, Device, Priority, Number, and Type. Below the table is a 'Get Probe Order' button.</p>

	<p>Data Store Password Subtab From the Data Store Password subtab, you can change the password for the administrator account.</p>	
<p>Log Files</p>	<p>From the Log Files tab, you can do the following tasks:</p> <ul style="list-style-type: none"> • View system messages. • View authentication events. • View administration events. • View mount messages. • View storage messages. 	

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

How to Log In to the Administration Tool (Admin GUI)

This procedure describes how to log in to the Sun Ray Administration tool.



Note

If a session is inactive for 30 minutes, you must log in again. To change the timeout value, see [How to Change the Admin GUI Timeout](#).

Steps

1. Log in to your Sun Ray server's console or to any DTU attached to it.
2. Open a browser window and type the following URL:

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



Note

If you specified a different port number when you configured the Sun Ray Server Software, use that port number in the URL. If you enabled secure communication, the browser might be redirected to a secure port. The default secure port is 1661.

3. In the User Name window, type the administrator user name and click the OK button.
4. In the password challenge screen, type the administration password and click the OK button.
The Sun Ray Administration tool appears.

If you get a message denying access, check the following items:

- 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.

How to Change the Admin GUI Locale

To display the locale correctly in the Admin GUI, change your browser's language preferences to the desired locale (`fr`, `ja`, or `zh_CN`).

For example, for Mozilla, go to Tools -> Options -> Advanced -> Edit Languages.

How to Change the Admin GUI to English Locale

This procedure describes how to change the Admin GUI to display English if it is displaying an undesired language.

1. Log in to the Sun Ray server as root.
2. Export the English locale.

```
export LC_ALL=C
```

3. Stop the web admin services.

```
/etc/init.d/utwadmin stop
```

4. Start the web admin services.

```
/etc/init.d/utwadmin start
```

For a more permanent solution, you can remove the non-English SRSS packages from the server. The following example removes the French packages and restarts the web admin services.

```
# /etc/init.d/utwadmin stop
# pkgrm SUNWfuta SUNWfuta SUNWfutwa SUNWfutwh SUNWfutwl
# /etc/init.d/utwadmin start
```

How to Change the Admin GUI Timeout

This procedure describes how to change the timeout for the SRSS Admin GUI. By default, the Admin GUI timeout value is 30 seconds.

1. Log in to the Sun Ray server as superuser.
2. Edit the `/etc/opt/SUNWut/webadmin/webadmin.conf` configuration file.
3. Change the following timeout value:

```
...
# The session timeout (specified in minutes)
session.timeout=30
...
```

4. Restart the webadmin program.

```
# /opt/SUNWut/lib/utwebadmin restart
```

This tool automatically updates the `web.xml` file used by the web server hosting the SRSS Admin GUI.

How to Start or Stop Sun Ray Services

How to Stop Sun Ray Services

1. Log in to the Sun Ray server.
2. Stop the Sun Ray services.

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

How to Start Sun Ray Services (Warm Restart)

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



Note

A disconnect will occur for a brief time on active Sun Ray DTUs before they reconnect again.

1. Log in to the Sun Ray server.
2. Start the Sun Ray services.

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

How to Start Sun Ray Services (Cold Restart)

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



Caution

Be sure to notify your users before performing a cold restart, which terminates all existing sessions on a server. To restart Sun Ray services without terminating sessions, perform a warm restart.

1. Log in to the Sun Ray server.
2. Start the Sun Ray services.

```
# utrestart -c
```

How to Display DTU Information

This procedure describes how to view information, including the currently installed firmware, about registered DTUs.

Command-Line Steps

1. Log in to the Sun Ray server.
2. Display information about a DTU.

```
utdesktop -p <desktopID>
```

where <desktopID> is the Sun Ray DTU identifier.

Admin GUI Steps



Note

To facilitate the searching process, you can use the Admin GUI to edit DTU properties. Click the DTU Identifier and then click edit. You can then provide a location or other information.

- Click the Desktop Units tab.

From the Desktop Units tab, you can do the following:

- To display information about a specific DTU, click on the DTU Identifier (MAC address) or enter a search string in the text field.
- To display information about a group of DTUs, select an option from the drop-down menu (All Connected Desktop Units, Token Readers, or Multihead Groups) and/or enter a search string in the text field to narrow your search.

User Fields in the Sun Ray Data Store

The following table describes the user fields in the Sun Ray Data Store.

Fields	Description
Token ID	User's unique token type and ID. For smart cards, this value is a manufacturer type and the card's serial ID. For DTUs, this value 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. This setting is optional.
Server Port	Sun Ray server's communication port. This field should generally be set to 7007. This setting is optional.
User Name	User's name.
Other Info	Any additional information you want to associate with the user, for example, an employee or department number. This setting is optional.

How to Restart 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. You might need to restart the SRDS daemon if you change one of its configuration parameters. The following procedure describes how to restart SRDS.

1. Stop the Sun Ray services.

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

2. Stop the Sun Ray Data Store daemon.

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

3. Restart the Sun Ray services.

```
# utrestart
```

How to Enable or Disable Multiple Administration Accounts (Solaris)

The Sun Ray server administrator can allow any valid UNIX user ID which has been added to the `utadmin` authorized user list to administer Sun Ray services using the Admin GUI. An audit trail of activity on these accounts is provided. The `utadminuser` command enables you to add existing UNIX users to the `utadmin` authorized user list.

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

How to Configure Admin GUI Privileges for UNIX Users

Use the following procedure to configure the Sun Ray Admin GUI to allow access by the UNIX users in the `utadmin` authorized user list instead of the default `admin` account. Once you enable Admin GUI privileges for authorized users, you can add or remove users to the `utadmin` authorized list to manage access to the Admin GUI.

1. For each UNIX user that needs authorization to the Admin GUI, add the user to the authorized user list.

```
# utadminuser -a <username>
```

You can run the `utadminuser` command without any options to list the current authorized users or with the `-d` option to delete a user.

2. Modify the `/etc/pam.conf` file to use the other authentication PAM stack auth entries to create the PAM stack for `utadmingui`.

```
# added to utadmingui by Sun Ray Server Software -- utadmingui
utadmingui auth requisite pam_authtok_get.so.1
utadmingui auth required pam_dhkeys.so.1
utadmingui auth required pam_unix_cred.so.1
utadmingui auth required pam_unix_auth.so.1
```



Note

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

How to Limit Admin GUI Privileges to the Admin User

A PAM module, `/opt/SUNWut/lib/pam_sunray_admingui.so.1`, is included in the Sun Ray product to support the old data store authentication.

To return to the old Sun Ray Admin GUI authentication scheme, modify the `/etc/pam.conf` file and replace the PAM stack for `utadmingui` with the `pam_sunray_admingui.so.1` module.

```
# added to utadmingui by Sun Ray Server Software -- utadmingui
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.

How to Enable or Disable Multiple Administration Accounts (Linux)

The Sun Ray server administrator can allow any valid UNIX user ID, which has been added to the `utadmin` authorized user list, to administer Sun Ray services using the Admin GUI. An audit trail of activity on these accounts is provided. The `utadminuser` command enables you to add existing UNIX users to the `utadmin` authorized user list.

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

How to Configure Admin GUI Privileges for UNIX Users

Use the following procedure to configure the Sun Ray Admin GUI to allow access by the UNIX users in the `utadmin` authorized user list instead of the default `admin` account. Once you enable Admin GUI privileges for authorized users, you can add or remove users to the `utadmin` authorized list to manage access to the Admin GUI.

1. For each UNIX user that needs authorization to the Admin GUI, add the user to the authorized user list.

```
# utadminuser -a <username>
```

You can run the `utadminuser` command without any options to list the current authorized users or with the `-d` option to delete a user.

2. Copy the auth entries from `/etc/pam.d/login` file into `/etc/pam.d/utadmingui`:

- On Oracle Linux or RHEL, the PAM entries are:

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

- On SLES 10, the PAM entries are:

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



Note

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

How to Limit Admin GUI Privileges to the Admin User

A PAM module, `/opt/SUNWut/lib/pam_sunray_admingui.so.1`, is included in the Sun Ray product to support the old data store authentication.

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.

How to Audit Admin GUI Sessions

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

The events are logged in the following log file:

```
/var/opt/SUNWut/log/messages
```

All audit events are prefixed with the keyword `utadt::` so you 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.1047750ble0e -k 2>&1}
message={terminated User "Cyberflex_Access_FullCrypto.1047750ble0e" 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
-

Contents

- About Sun Ray System Monitoring
 - Additional Sun Management Center Modules
 - Using Other Monitoring Programs
 - Task Map - Managing Sun Ray System Monitoring (Solaris)
 - Initial Configuration
 - Additional Tasks
 - How to Set Up the Monitoring Environment
 - How to Create an Object
 - How to Set an Alarm
 - How to Enable or Disable DTU Monitoring
 - How to Enable DTU Monitoring
 - How to Disable DTU Monitoring
 - How to Start Monitoring
 - How to Display Sun Ray System Information
 - Sun Ray System Properties
 - Sun Ray Services Properties
 - Failover Group Properties
 - Interconnect Properties
 - DTU Properties
 - Refreshing the Information
 - Troubleshooting Sun Management Center (Solaris)
 - Problem: Sun Management Center's Detail window does not show a Sun Ray object for the Sun Ray server node.
 - How To Load the Sun Ray Module
 - Problem: The list of modules on the Modules tab does not include an entry for Sun Ray.
 - How to Register and Start the Sun Ray Module
-

Managing Sun Ray System Monitoring on Solaris (All Topics)

About Sun Ray System Monitoring

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

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

Each managed object is monitored separately and has independent alarm settings. Alarms are used to notify you when errors occur or your performance needs to be tuned. Alarms are triggered (tripped) if:

- A server goes down
- An interconnect is no longer working
- A DTU is down

Alarms are set by default, but you can change them.

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

- Authenticate users
- Start sessions

- Manage peripheral devices
- Handle DHCP services

For more information, see [How to Set an Alarm](#).

For information on how to managing the Sun Management Center, see [Task Map - Managing Sun Ray System Monitoring \(Solaris\)](#).

Additional Sun Management Center Modules

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

Using Other Monitoring Programs

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

Task Map - Managing Sun Ray System Monitoring (Solaris)

Initial Configuration

To configure monitoring on a Sun Ray system using the Solaris OS, you need to perform the steps described in the following table.

Step	Description	Task
1	Install the Sun Management Center software.	How to Install SunMC
2	Set a home administrative domain. This domain is displayed whenever the console is started.	How to Set Up the Monitoring Environment
3	Create the hierarchy of the system you want to monitor, either manually by adding nodes to the administrative domain or by using the Discovery Manager.	How to Create an Object
4	Configure alarms to monitor your Sun Ray system.	How to Set an Alarm
5	Enable or disable DTUs for monitoring.	How to Enable or Disable DTU Monitoring
6	Start monitoring.	How to Start Monitoring

Additional Tasks

Task	Description
How to Display Sun Ray System Information	Explains how to display property and status information about your managed objects.

How to Set Up the Monitoring Environment

After installing the Sun Management Center software, you need to set up your monitoring environment. A default administrative domain is automatically created for you based on the Sun Management Center server component. You need to set a home administrative domain, which is displayed whenever the console is started.

Steps

1. Start the console on the server that has the console component installed.

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

The login screen is displayed.

2. Type your user name and password.
Specify the Sun Management Center server.
3. Click Login.
The Sun Management Center window is displayed. If this session is your first time using the SunMC console, the Set Home Domain window is also displayed.
4. In the Set Home Domain window, select the appropriate domain and click Go To.
The panels in the Sun Management Center window are populated.
5. Click Close to dismiss the Set Home Domain window.

How to Create an Object

This procedure describes how to create the hierarchy of the system you want to monitor. This can be done manually by adding nodes to the administrative domain or by using the Discovery Manager.

Steps

1. Start the Sun Management Center software.

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

2. Expand the Sun Management Center Domains list.
3. Select the domain you plan to add an object to.
The selected domain is displayed.
4. Choose Edit -> Create an Object.
The Create Topology Object window is displayed.
5. On the Node page, type a node label and description.
6. Type the Host name (server name), IP address, and port for the Sun Ray server.
The port provided here must be the same port you configured (entered) during the installation of the Sun Management Center.

How to Set an Alarm

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

This procedure describes how to set alarms to monitor the server and its load.

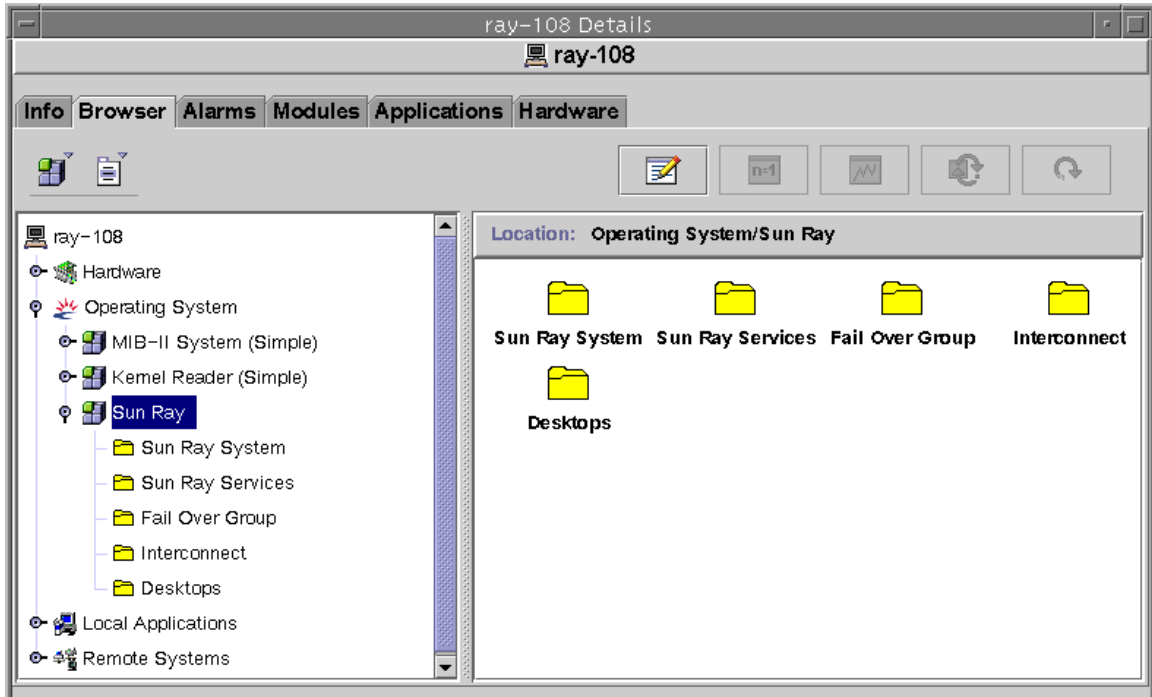
Base a tuning alarm on the number of active sessions on each server in a failover group to determine if one of the servers is overloaded. You set the thresholds that trigger this type of alarm.

Steps

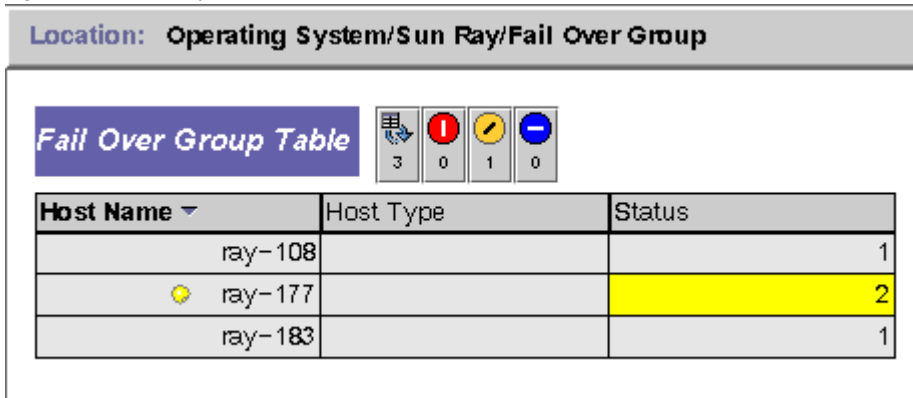
1. Start the Sun Management Center software.

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

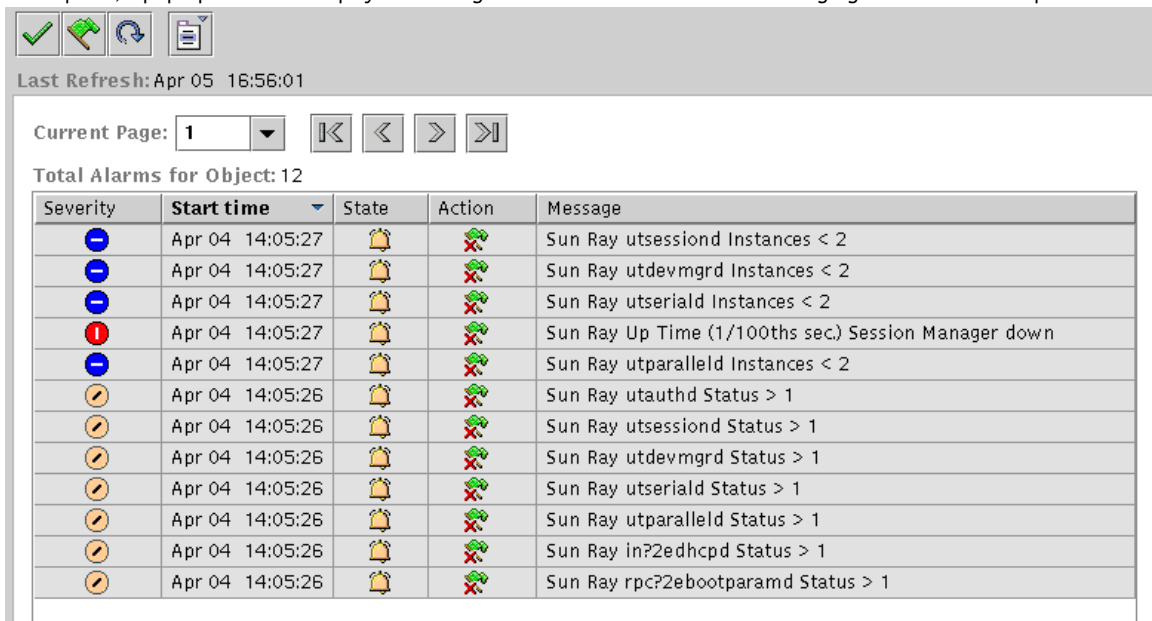
2. Display the Details window of the object.



3. Double-click the object folder in the left panel for which you would like to create an alarm.
4. Right-click the value portion of the table row.



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



The total number of alarms set for the current server object is displayed at the top of the alarm summary window. Critical alarms (red),

alert alarms (yellow), and caution alarms (blue) that are tripped are listed below. Details and comments are displayed in the Message column.

5. Select Attribute Editor.
The Attribute Editor window for that table entry is displayed.
6. Select the Alarms tab, shown in the following figure.

The screenshot shows the 'Attribute Editor' window for the object 'Active Users' located at 'Operating System/Sun Ray/Sun Ray System'. The 'Alarms' tab is selected. The window contains several input fields for setting thresholds:

- Critical Threshold (>)
- Alert Threshold (>)
- Caution Threshold (>)
- Critical Threshold (<)
- Alert Threshold (<)
- Caution Threshold (<)
- Alarm Window: (with an 'Advanced...' button)
- Parameter Description: (text area containing instructions on how to set thresholds)

At the bottom of the window are buttons for 'OK', 'Apply', 'Reset', 'Cancel', and 'Help'.

7. Supply an appropriate number for the type of alarm that you choose to monitor.
In this example, the Alert Threshold alarm is set at greater than 1 to notify you when that server in the failover group is down.
8. Click the Apply button to save the value of the alarm and continue setting other values in the Attribute Editor
9. Click the OK button, which saves the value of the alarm and closes the window.
As soon as you set an alarm it takes effect.
10. Select the Actions tab and type an action to perform.
You can specify an action such as sending email or running a script for each alarm.
11. Select the Refresh tab to set the number of seconds between pollings.
The default value is 300 seconds (5 minutes).

Note
Do not set the Refresh value to less than 60 seconds. The load will interfere with the Sun Ray server performance.

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

How to Enable or Disable DTU Monitoring

How to Enable DTU Monitoring

1. Start the Sun Management Center software.

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

2. Double-click the Sun Ray System icon in the left panel.
The Operating System/Sun Ray/Desktops panel is populated, as shown in the following figure.

Monitored Desktops											
Name	IP Address	Status	Packets	Lost Packets	Lost Percent	Location	Optional Data	Server	Model	Firmware Revision	
080020b5...	192.168.128.17	3	0	0	0.0			nomad-100	SunRay P1	1.3_04.a.REV=20...	
080020cf6...	192.168.128.16	1	0	0	0.0			nomad-100	SunRay P3	1.1_22.b.REV=20...	

Desktop Exceptions											
Name	IP Address	Status	Packets	Lost Packets	Lost Percent	Location	Optional Data	Server	Model	Firmware Revision	
080020b5...	192.168.128.17	2	0	0	0.0			nomad-100	SunRay P1	1.3_04.a.REV=20...	

3. Right-click the name.
A pop-up menu is displayed.
4. Click Add Row.
A pop-up window is displayed.
5. In the Add Row window, enter the MAC address of the DTU you want to monitor in the Name field.
6. Click OK.

How to Disable DTU Monitoring

1. Start the Sun Management Center software.

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

2. Double-click the Sun Ray System icon in the left panel.
The Operating System/Sun Ray/Desktops panel is populated.
3. Right-click the cell containing the MAC address.
A pop-up menu is displayed.
4. Click Delete Row.
A pop-up window is displayed.
5. Confirm the deletion by clicking Yes in the window.

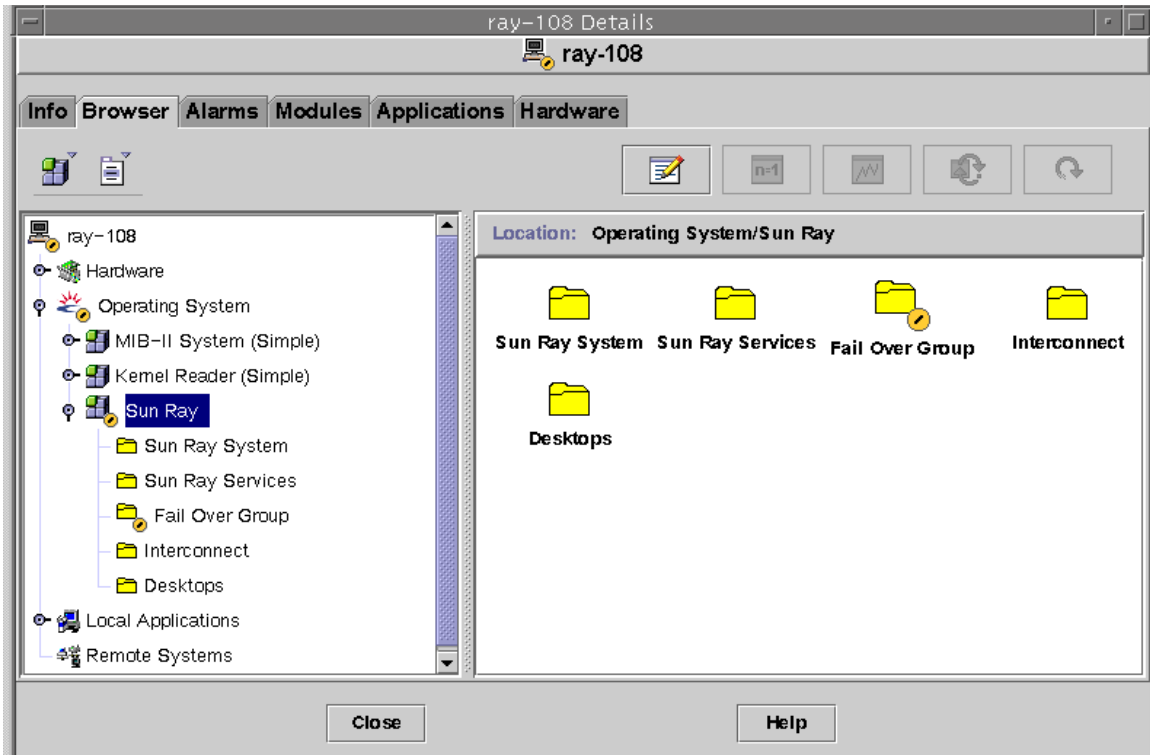
How to Start Monitoring

1. Start the Sun Management Center software.

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

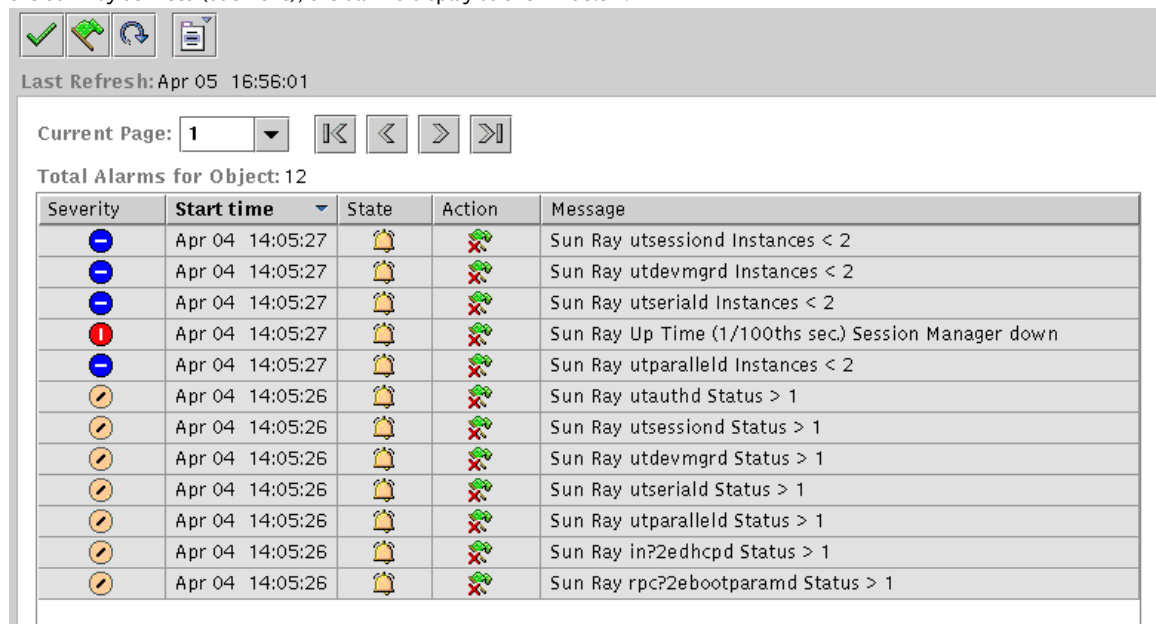
A window for the Default domain is displayed.

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



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

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



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

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

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

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

How to Display Sun Ray System Information

This procedure describes how to display status and property information about the Sun Ray system, Sun Ray services, failover group topography, interconnect, and DTUs.

Steps

1. Start the Sun Management Center software:

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

2. Double-click the appropriate folder (Sun Ray System, Sun Ray Services, Fail Over Group, Interconnect, and Desktops) in the left panel.

The right panel is populated with information about the selected object.

Details about the information displayed are described in the following sections.

Sun Ray System Properties

Sun Ray system properties are displayed in the Details window, as shown in the following figure.

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

The Sun Ray System properties displayed in the panel are explained in the following table.

Property	Value
Host Name	Name of server that was queried. This information is obtained when Sun Ray System is selected or on manual refresh.
Contact Name	This information is obtained when Sun Ray System is selected or on manual refresh.
Up Time (measured in hundredths of a second)	Number of hundredths of a second since the last of all the daemons critical to the Sun Ray server was started. A value of 0 means the server is down and an alarm is tripped. The default refresh rate is 300 seconds (five minutes)
Version	List of version, build, and date of build of Sun Ray Server Software. This information is obtained when Sun Ray System is selected or on manual refresh.
Install Date	Date Sun Ray Server Software was installed. This information is obtained when Sun Ray System is selected or on manual refresh.
Patch Information	List of Sun-Ray-specific patches. This information is obtained when Sun Ray System is selected or on manual refresh.
Active Sessions	Number of sessions based on logged-in sessions with a smart card plugged in, plus sessions for DTUs logged in without smart cards. Set an alarm here to watch for overloading of this server. The default refresh rate is 300 seconds (five minutes).

Total Sessions	Number of active and suspended sessions. The default refresh rate is 300 seconds (five minutes).
Active Desktops	Number of connected DTUs. The default refresh rate is 300 seconds.
Active Users	Number of currently active users. When pseudo-tokens are allowed, which is a policy setting for non-smart card users, this number includes DTUs at the login prompt. The default refresh rate is 300 seconds (five minutes).
Policy	The policy that has been set. This information is obtained when Sun Ray System is selected or on manual refresh.

Sun Ray Services Properties

The Sun Ray Services panel displays the status of the Sun Ray daemons, as shown in the following figure.

The screenshot shows the Sun Ray Services panel with a tree view on the left and a 'Services Table' on the right. The tree view includes 'Sun Ray' > 'Sun Ray Services'. The 'Services Table' has the following data:

Daemon	Status	Started Time	Last Changed	Instances	Description
utlogin	1	1183720130	1184183385	1	desktop login
in.dhcpd	1	1185443837	1185443837	1	DHCP daemon
utauthd	1	1185443850	1185443850	1	Auth Manager
utdevmgd	1	1185443850	1185443850	2	Device Manager
utdsd	1	1183956855	1183956855	1	Datastore daemon
utparallel	1	1185443850	1185443850	2	Parallel Device d...
utserial	1	1185443850	1185443850	2	Serial Device da...
utsessiond	1	1185443850	1185443850	2	Session Manager

If, for example, utauthd is not running, all user sessions are disconnected.

Some of the daemons have two instances corresponding to their two functions: one to listen and one to interact. You can reset these values.

The Status values are:

Status	Value
1	The daemon is running.
2	The daemon is down.

Failover Group Properties

The Failover Group panel displays the topography of the selected failover group, as shown in the following figure.

The screenshot shows the Failover Group panel with a 'Fail Over Group Table' containing the following data:

Host Name	Lost Type	Status
ray-178	secondary	1
ray-177	secondary	2
ray-183	primary	1



The panel lists the primary and secondary servers and their status.

The Status values are:

Status	Value
1	The server is running.
2	The server is down (displays a yellow alert).

Interconnect Properties

The Interconnect panel populates with information about usable interfaces, as shown in the following figure.

Location: Operating System/Sun Ray/Interconnect						
DHCP Table						
						
Network Name	Available Addresses					
SunRay-hme1	73					
Interface Table						
						
Entry Name	Status	Address	Netmask	Last Packet Seen (1/100ths sec.)	Lan Type	
hme0	1	192.9.116.108	255.255.255.0	1700	LAN	
hme1	1	192.168.128.1	255.255.255.0	1700		

The following information is displayed:

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

The Status values are:

Status	Value
1	The interface is up.
2	The interface is down.

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

DTU Properties

The Desktops panel displays the status of all DTUs, as shown in the following figure.

Unable to render embedded object: File (desktopspanel.pngalt="Screenshot showing the DTU Properties window.") not found.

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

The Status values are:

Status	Value
1	The DTU is running.
2	The DTU is down.
3	The DTU is displaying the hourglass cursor.

The following table describes the information in each column.

Property	Value
Name	Ethernet or MAC address of the DTU
IP Address	Assigned DHCP address of the DTU
Status	1 Running 2 Down 3 Displaying the green hourglass cursor
Packets	Number of packets received by the DTU
Lost Packets	Number of packets the DTU reported lost
Lost Percent	Percentage of packets lost
Location	Optional field; information supplied by system administrator

Optional Data	Optional field; information supplied by system administrator
Server	Server that owns the DTU
Model	The type of DTU: P1 (Sun Ray 1), P2 (Sun Ray 100), P3 (Sun Ray 150), P8 (Sun Ray 2, Sun Ray 2FS, Sun Ray 270)
Firmware Revision	List of version, build, and build date

Refreshing the Information

To refresh the panel, click the refresh button, which is the circular arrow in the upper right corner. The entire panel is refreshed.

The console is updated every five minutes unless an alarm occurs.

Troubleshooting Sun Management Center (Solaris)

When the Sun Ray server has the Sun Management Center agent installed, the normal operation is for the agent to start automatically. The Sun Ray server becomes a monitored Sun Management object.

Problem: Sun Management Center's Detail window does not show a Sun Ray object for the Sun Ray server node.

Load the Sun Ray module or enable the module manually.

How To Load the Sun Ray Module

1. Click the Sun Management Center's Modules tab.
2. In the Module Name column, look for the Sun Ray entry.
3. Check the status of the Sun Ray entry. Its Load status must be Yes and its Enabled status must be Yes.

The screenshot shows the Sun Management Center interface with the 'Modules' tab selected. The 'Modules with Load Status:' table is as follows:

Module Name	Loaded	Scheduled	Enabled
Agent Statistics	Yes	No	Yes
Config Reader (Ultra Work...	Yes	No	Yes
Kemel Reader (Simple)	Yes	No	Yes
MIB-II System (Simple)	Yes	No	Yes
Sun Ray	Yes	No	Yes

Below this table is the 'Available Modules:' section:

Module Name	Multi-instance
Data Logging Registry	No
MIB-II Proxy Monitoring	Yes

On the right side of the interface, there are several buttons: Unload, Load Now, Edit..., Enable, Disable, Rules..., and Load... (at the bottom).

4. If the Load status is not Yes, select the Sun Ray entry and then click the Load button. This action loads the module and moves it to the Modules with Load Status list.
5. If the Enabled status is not Yes, select the Sun Ray entry and then click the Enable button.
6. Return to the Detail window.

The Detail window now shows a Sun Ray object for the Sun Ray server node.

Problem: The list of modules on the Modules tab does not include an entry for Sun Ray.

Add the module manually and restart its agent.

How to Register and Start the Sun Ray Module

1. Issue the following command to add the module to the Sun Management Center and restart its agent:

```
# /opt/SUNWut/sbin/utsummc
```

2. If a message displays indicating that the agent failed to start, type the following command to verify that the agent is running:

```
# ps -ef |grep agent
```

If the Sun Management Center agent is running, wait a few minutes and then check the Detail window.

3. If the agent is not running, type the following command to start the Sun Management Center agent:

```
# /opt/SUNWsymon/sbin/es-start -a
```

Contents

- [About Tokens and Token Readers](#)
 - [What is a Token Reader?](#)
 - [How to Register a Token](#)
 - [How to Register a Pseudo-Token](#)
 - [How to Enable, Disable, or Delete a Token](#)
 - [How to Configure a Token Reader](#)
 - [How to Get a Token ID From a Token Reader](#)
 - [How to Locate a Token Reader](#)
-

Managing Tokens and Token Readers (All Topics)

About Tokens and Token Readers

As described in [Parts of the Sun Ray System](#), the Authentication Manager implements the chosen policies for identifying and authenticating users on Sun Ray DTUs. Tokens are the key piece for this process.

When a user accesses a DTU, the DTU sends the user's token information to the Authentication Manager and requests access. If the user inserts a smart card in the DTU, the card's type and ID are used as the token. If no smart card is inserted, the DTU's Ethernet address is used as a pseudo-token.

You can administer tokens through the `utuser` command or the Admin GUI.

What Is a Token Reader?

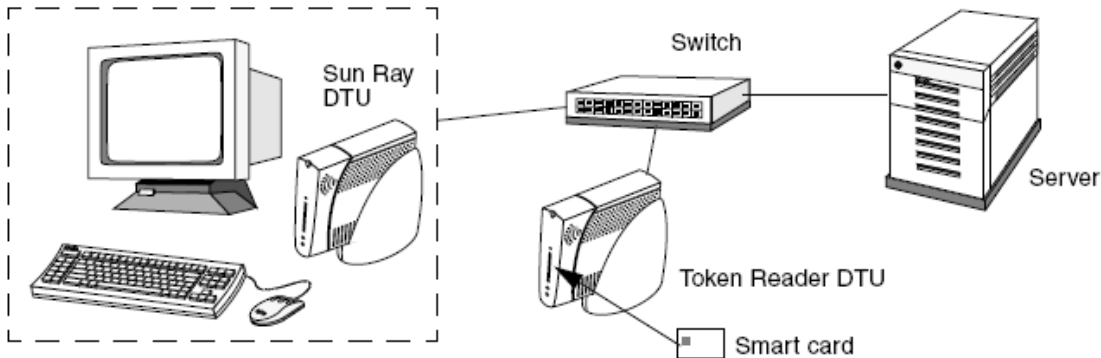
A token reader is a specific DTU that you can set up to administer user's tokens, such as registering smart cards. This token reader is not the same as hardware devices into which users insert their smart cards, which are typically called smart card readers.

Sun Ray Server Software provides a way to designate one or more specific DTUs as dedicated token readers. A dedicated token reader is not used for normal Sun Ray services, so it does not need a keyboard, mouse, or monitor. Inserting a smart card in a token reader does not enable hotdesking. It does allow the administrator to assign the card to a user.

When you enable an authentication policy with registered users or token owners, be sure to specify smart card IDs for them. To use token

readers with regional hotdesking based on Sun Ray pseudo-tokens, use the Site-specific Mapping Library. See [How to Configure a Site-specific Mapping Library](#) and [How to Use Token Readers with Regional Hotdesking](#).

In the following diagram, the second DTU is used as a token reader.



How to Register a Token

This procedure describes how to register a token using the Admin GUI.

Steps

1. Click the Tokens tab.
2. Select a token to display that token's properties.
3. Click the New button.
4. Type an identifier or select a token reader.

How to Register a Pseudo-Token

This procedure describes how to register a pseudo-token with the Admin GUI.

Steps

1. Click the Desktop Units tab.
2. Select any Desktop Unit Identifier to view properties for that DTU.
3. On the Desktop Unit Properties page, click View Token Details.
4. Click the Edit button to display the Edit Token Properties page.
5. Provide details such as ownership and to specify a session type: Default, Kiosk, or Regular.

How to Enable, Disable, or Delete a Token

This procedure describes how to enable, disable, or delete a token with the Admin GUI.

1. Select the token's identifier on the Token Properties page.
2. Click the Enable, Disable, or Delete button.

How to Configure a Token Reader

Command Line Steps

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

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

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

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

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

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

To unconfigure all token readers on this server:

```
# utreader -c
```

Admin GUI Steps

1. Click the Desktop Units tab.
2. Click the identifier of the DTU that you want to use as a token reader.
3. On the Desktop Units Properties window, click Edit.
4. On the Edit Desktop Unit Properties window, select the Token Reader option.
5. Click the OK button.

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

6. Restart Sun Ray services.

The DTU is now a token reader.

How to Get a Token ID From a Token Reader

You can access the token card reader by invoking `utuser -r` from any server in the relevant failover group.

Type the following command:

```
# utuser -r <token-reader>
```

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

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

How to Locate a Token Reader

This procedure describes how to locate a token reader using the Admin GUI.

Steps

1. Click the Desktop Units tab.
2. Select Token Readers from the drop-down list.
3. Click the Search button.

The default search finds all possible matches.

To change the search criteria, type text in the Search text box.

- SRSS Troubleshooting Icons
 - Types of Troubleshooting Icons
 - Troubleshooting Icon Quick Reference
 - DHCP State Codes
 - Power LED
 - (1) DTU Startup Icon
 - (2) Firmware Download in Progress Icon
 - (3) Saving PROM Software Icon
 - (4) Firmware Download Diagnostics Icon
 - (15) Session Refused Icon
 - (16) Bus Busy Icon
 - (21) Network Connection Verified Icon
 - (22) Waiting to Connect to Authentication Manager Icon
 - (23) No Ethernet Signal Icon
 - (25) Redirection Icon
 - (26) Wait for Session Icon
 - (27) DHCP Broadcast Failure Icon
 - (28) Establishing VPN Connection Icon
 - (29) VPN Connection Established Icon
 - (31-34) Ethernet Address Icon
 - (46) No Access to Server Icon
 - (47) No Access for Sun Desktop Access Clients Icon
 - (48) No Access: Registration Required Icon
 - (49) No Access: Key Rejected Icon
 - (50) No Access: Security Policy Violation Icon
 - (60) Insert Card Icon
 - (61) Waiting for Primary DTU Icon
 - (62) Token Reader Icon
 - (63) Card Error Icon
 - (64) Waiting For Access Icon
- Troubleshooting Audio Output
 - Tracking Audio Sessions
 - Audio Device Emulation
 - Problem: Audio features are malfunctioning.
 - Problem: An application has encoded the use of `/dev/audio` for output.
 - New Audio Troubleshooting from Patrick.
- Troubleshooting Authentication
 - Authentication Error Messages
 - Error Message Examples
- Troubleshooting General Problems
 - Problem: How do you get keyboard type information for a Sun Ray DTU?
- Troubleshooting Installation
 - Installation (utinstall) Error Messages
 - Modified System Files (Solaris)
 - Modified System Files (Linux)
- Log Files
- Troubleshooting Login Problems
 - Problem: The `dtlogin` daemon cannot start the Xsun server properly.
- Troubleshooting Multihead Displays
 - Multihead Video
 - Problem: The display resolution is 640 x 480.
- Troubleshooting Network Problems
 - The `utcapture` Utility
 - Problem: Sun Ray DTU traffic loss of more than 0.1%.
 - `utcapture` Examples
 - The `utquery` Command
 - OSD Icons
 - How To Identify a Hung Session
 - How To Kill a Hung Session
- Troubleshooting Printers
 - Problem: "Failed to open the printer port" message.
- Troubleshooting Sun Management Center (Solaris)
 - Problem: Sun Management Center's Detail window does not show a Sun Ray object for the Sun Ray server node.
 - Problem: The list of modules on the Modules tab does not include an entry for Sun Ray.

- Troubleshooting USB Storage
 - Problem: Device nodes are not created.
 - Problem: The device is not automatically mounted.
 - Problem: The device is not automatically unmounted.

Troubleshooting (All Topics)

SRSS Troubleshooting Icons

The Sun Ray Server Software displays various icons on the client screen to help identify problems quickly.

If you see the older version of the icons, the firmware has not been upgraded or is failing. To make sure that you are using the latest firmware, see [How to Update Firmware Versions on DTUs](#).

Types of Troubleshooting Icons

Icon Type	Example	Description
On-Screen Display (OSD)		<p>Indicates the current state of a client's connectivity. These icons are shown as white icons. They can display even if the client is not connected to a server, and they typically provide the following detailed information:</p> <ul style="list-style-type: none"> • A unique, white graphic • Ethernet address • IP address of the DTU • Status of link to Sun Ray server • IP address of Authentication Server • Numeric code for icon message • Alphabetic code for DHCP state • Encryption and authentication information, when appropriate • Some specialized icons have their own error codes: <ul style="list-style-type: none"> • Firmware Download Error Codes and Messages • Power LED
Server Policy		<p>Indicates a problem based on a specific server policy that needs attention. These icons are shown as blue icons. They are sent by the server in place of a regular session, they may be overlaid by a concurrent client state OSD icon, and they are not available if the client is behind a NAT router.</p>

Troubleshooting Icon Quick Reference













Note

Press the **Mute+Softer+Louder** keys or **Ctrl+Pause+N** keys simultaneously to display the current network status.

Icon Code (Click for More Information)	General Category	Meaning
	= Server Policy Icon	
1	Startup	Sun Ray DTU is starting up and is waiting for Ethernet link.

2	Firmware Download	Sun Ray DTU is downloading new firmware.
3	Firmware Download	Sun Ray DTU is storing new firmware in its flash memory.
4	Firmware Download	Either the download or storage of new firmware has failed.
5	Session Connection	There is no session to connect with the Sun Ray.
6	Session Connection	The server is denying access to the Sun Ray.
7	Smart Card	Local PIN entry to the smart card has failed.
8	Smart Card	In local smart card PIN entry mode.
9	USB	There is an "overcurrent" condition on the USB bus, that is, the total number of devices draws too much current. Consider using a powered hub.
11	Network Status	The server is authenticated and the graphic/keyboard network connections are encrypted.
12	Network Status	The server is not authenticated and the graphic/keyboard network connections are encrypted.
13	Network Status	The server is authenticated and the graphic/keyboard network connections are not encrypted.
14	Network Status	The server is not authenticated and the graphic/keyboard network connections are not encrypted.
15	Session Connection	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	USB	USB bus is busy servicing a high-speed device, and the keyboard or mouse might not be responsive to user input.
21	Startup	Sun Ray DTU is booting up and is waiting for DHCP IP address and parameter assignment.
22	Startup	Sun Ray DTU is booting up and is waiting for the initial connection to a Sun Ray server.
23	Network Status	The connection between the Sun Ray DTU and the network is down. Check the network drop cable. If the network drop cable is okay, check the network switch.
24	Session Connection	Sun Ray DTU has disconnected from the previous server.
25	Session Connection	Sun Ray DTU is being redirected to a new server.
26	Session Connection	Sun Ray DTU has connected to the server and is waiting for graphics traffic.
27	Startup	Sun Ray DTU is broadcasting to locate a Sun Ray server since either one was not provided or all of the specified servers are not responding.
28	Startup	VPN connection being attempted.
29	Startup	VPN connection established.
30	Startup	VPN connection error.
31	Network Status	The network link is up, the server is authenticated, and graphics/keyboard network connections are not encrypted.
32	Network Status	The network link is up, the server is not authenticated, and graphics/keyboard network connections are encrypted.

33	Network Status	The network link is up, the server is authenticated, and graphics/keyboard are encrypted.
34	Network Status	The network link is up, the server is not authenticated, and graphics/keyboard are not encrypted.
35	Startup	Sun Ray DTU has been disconnected from its server, either by a STOP-Q session disconnect event or by the VPN session timeout value having been set and exceeded.
41	Network Status	The server is authenticated, the client is authenticated, and the graphic/keyboard network connections are encrypted.
42	Network Status	The server is not authenticated, the client is authenticated, and the graphic/keyboard network connections are encrypted.
43	Network Status	The server is authenticated, the client is authenticated, and the graphic/keyboard network connections are not encrypted.
44	Network Status	The server is not authenticated, the client is authenticated, and the graphic/keyboard network connections are not encrypted.
46		No access to server.
47		No access for Oracle Virtual Desktop Clients.
48		No access: registration required.
49		No access: client key is rejected.
50		No access: security policy violation.
51	Network Status	The network link is up, the server is authenticated, the client is authenticated, and graphics/keyboard network connections are not encrypted.
52	Network Status	The network link is up, the server is not authenticated, the client is authenticated, and graphics/keyboard network connections are not encrypted.
53	Network Status	The network link is up, the server is authenticated, the client is authenticated, and graphics/keyboard are encrypted.
54	Network Status	The network link is up, the server is not authenticated, the client is authenticated, and graphics/keyboard are not encrypted.
60		Insert card. If the site's authentication policy allows access only by card, this icon is displayed to prompt the user to insert a card. Access without a card is disabled.
61		Waiting for primary DTU. The DTU is a secondary DTU in a multihead group, and the primary DTU is not currently connected.
62		Token reader. The DTU is a token reader. When a site policy disallows pseudo-sessions, a DTU configured as a token reader displays the Token Reader icon instead of the Login dialog box.
63		Smart card not recognized. The smart card is not recognized by the Sun Ray server or there is a reader error.
64		Waiting for session access. Access is temporarily denied, but the Sun Ray DTU automatically retries when this condition is resolved.

DHCP State Codes

Some icons also show a state code after the number to provide more information.

DHCP State Code	Meaning
A	DHCP only provided IP address with no additional parameters.

B	DHCP 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.

Power LED

DTU Hardware State	Action to Take
Off	Check to see whether the DTU is plugged in. Replace the DTU.
Green	Normal operation.
Amber	Hardware fault. Replace the DTU.
Blinking	PROM is corrupted. Check that firmware downloads are configured and enabled, then power cycle the DTU.
Card reader LED remains on even when card is removed	Card reader hardware problem. Replace the DTU.

(1) DTU Startup Icon



The DTU Startup icon indicates that the DTU has passed the power-on self test but has not yet detected an Ethernet signal. The icon is displayed for a few seconds as part of the normal startup process. When an Ethernet signal is detected, the [Network Connection Verified](#) OSD is displayed.

Problem: The DTU Startup OSD is displayed for more than 10 seconds.

- Check that the Ethernet cable is plugged into the DTU correctly and that the other end is plugged in to the correct hub, switch, or network outlet.
- If the DTU is connected through a hub or a switch, verify that the hub or switch is powered on and configured correctly. A link LED on the switch or hub indicates that the connection is alive.

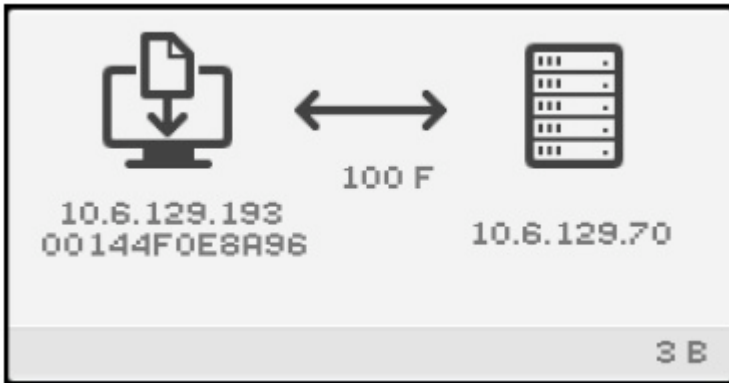
(2) Firmware Download in Progress Icon



The Firmware Download in Progress icon indicates that the DTU is downloading new firmware from a Sun Ray server.

If you see this OSD, wait until the download is complete. Downloading and saving the firmware takes less than a minute. If you interrupt the download, the DTU has to download new firmware the next time it reboots.

(3) Saving PROM Software Icon



The Saving PROM Software icon indicates that the DTU just downloaded new flash PROM software (firmware) from the Sun Ray server and is saving it to the DTU's PROM.

If you see this OSD, wait until the download is complete. Downloading and saving the new firmware takes less than a minute. If you interrupt the download, the DTU has to download new firmware the next time it reboots.

(4) Firmware Download Diagnostics Icon

The Firmware Download icon is displayed with a code or a message when an error occurs during a download of firmware. [Table 4](#) lists the error codes. These error messages appear in English even in localized versions of Sun Ray Server Software.



Firmware Download Error Codes and Messages

Firmware download error codes are valid only with OSD icon 4.

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

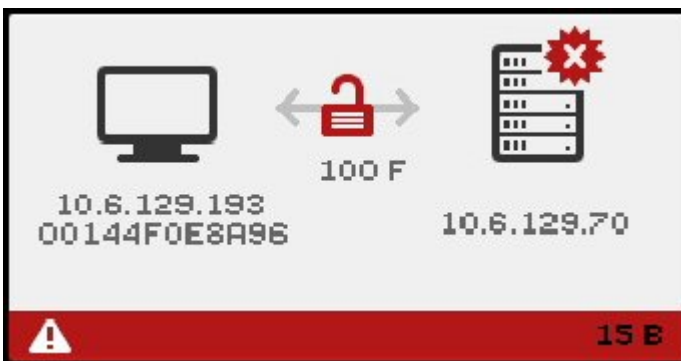
The Firmware Download with a 4 error code icon is displayed when the DTU fails to download new firmware. The message "FW Load: Prevented by barrier" indicates that the DTU already has a later version of the firmware.

In the `syslog`, the following message indicates that a barrier level has been set to prevent Sun Ray DTUs from downloading an earlier version of the firmware.

```
Firmware upgrade/downgrade not allowed! Barrier is 310 Firmware level is 0
```

- Check `/var/opt/SUNWut/log/messages` to confirm that your configuration is set up properly.

(15) Session Refused Icon



The Session Refused icons are displayed during a possible security breach because authentication has failed.

Problem: Icon shows the 15D message.

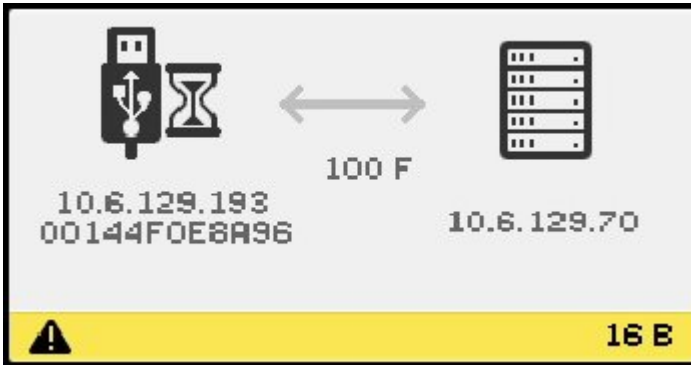
The DTU is refusing to connect to a server because the DTU is unable to verify the validity of the Sun Ray server. This error can occur only if an unknown Sun Ray server tries to emulate a valid Sun Ray server. This situation is a session security breach.

Problem: Icon shows the 50D message.

The Sun Ray server is refusing to grant a session to the DTU because the DTU is unable to fulfill the server's security requirements.

- Upgrade the DTU's firmware version. This error can occur with firmware versions earlier than 2.0 when the server is configured for hard security mode.
- As an alternative, determine whether your site requires hard security mode. If not, the session can be enabled with soft security mode.

(16) Bus Busy Icon



The Bus Busy OSD indicates that the Sun Ray USB bus is servicing a high-speed device and the keyboard or mouse might not be responsive to user input.

This icon is displayed during an unusually long print job and disappears when the job is done. No action is needed unless killing the print job is necessary.

(21) Network Connection Verified Icon



The Network Connection Verified icon indicates that the DTU has detected the Ethernet carrier but has not yet received its initial parameters or IP address from the DHCP server. The icon is displayed for a few seconds as part of the normal startup process.

After the DHCP server has allocated an IP address, the icon is updated with the DTU's assigned IP address. When the network connection is verified, the Sun Ray DTU connects to the Sun Ray server.

Problem: The icon is displayed for more than 10 seconds.

- Verify that the DHCP server is running and has not run out of IP addresses to assign to clients.
- Verify that the DHCP server is configured properly for network parameters.

Problem: The icon displays an IP address and an icon message, either 21A or 21B, depending on whether the Sun Ray server is on a LAN network or a dedicated interconnect.

This condition occurs when the DTU receives an IP address from the DHCP but no other parameters. The Sun Ray DTU issues a DHCP_INFORM request to obtain the Sun Ray-specific parameters.

- Code 21 A indicates that the DTU received an IP address and is waiting for a response to its DHCP `inform` request.
- Code 21 B indicates that the DTU received an IP address and IP router and is waiting for a response to its DHCP `inform` request.

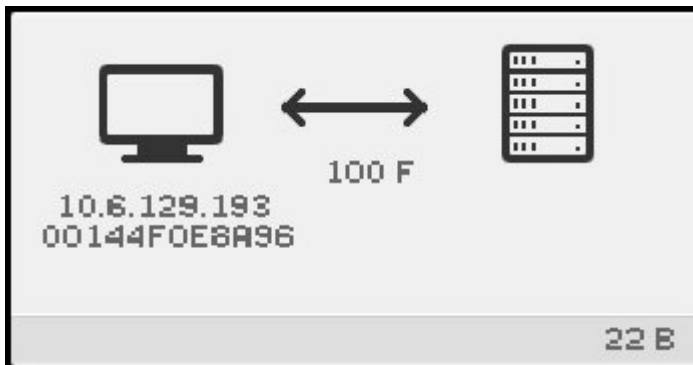
If no response is received, the Sun Ray DTU continues the startup process using only the IP address. In a private interconnect or simple LAN configuration, the DTU can function successfully. However, performance of the Sun Ray DTU might be affected. If the Sun Ray DTU is part of a complex LAN configuration, it can fail later in the start up process because it requires the additional parameters and Sun Ray-specific vendor options to handle network operations, such as when a DTU is located several hops away from the Sun Ray server's subnet.

Continue with the startup process, if possible, and at the next opportunity, do the following:

- 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.
- 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.
- For non-routed private interconnect configurations, the Sun Ray server performs the functions of a DHCP server. Verify that it is configured properly for DHCP services.

When the Sun Ray DTU concludes the interaction with the DHCP server, it connects to a Sun Ray server and then interacts with the server's Authentication Manager, indicated by the Waiting to Connect to Authentication Manager OSD. Occasionally, the Sun Ray DTU is first routed to another Sun Ray server. In this case, the [Redirection OSD](#) icon is displayed for a few seconds and then, as the Sun Ray DTU interacts with the new server's Authentication Manager, the Waiting to Connect to Authentication Manager OSD is displayed.

(22) Waiting to Connect to Authentication Manager Icon



The Waiting to Connect to Authentication Manager icon indicates that the DTU has received its parameters from the DHCP server and it has connected to the Sun Ray server but has not yet completed its authentication. The icon is displayed for a few seconds as part of the normal startup process.

Problem: The icon displays for more than 10 seconds or the DTU resets after the icon is displayed.

- Verify that Sun Ray services, including the Authentication Manager, are running on the Sun Ray server.

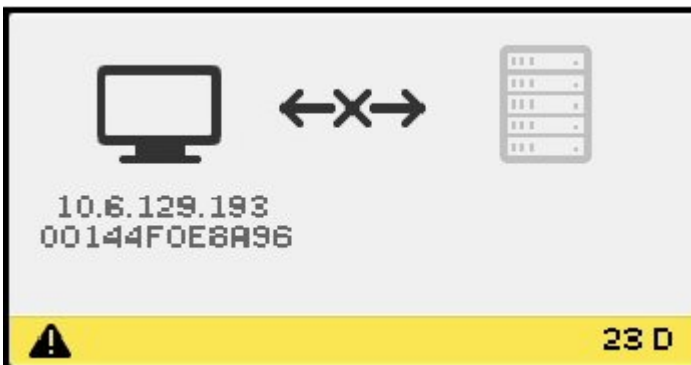
In a LAN configuration or other routed environment:

- Verify that the DTU's IP address can reach the Authentication Manager.
- Verify that the DTU's routing information, received from the Sun Ray server, is correct.
- 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.
- Run `utquery` for the DTU's IP address to see the parameters that the DTU received. If the parameters do not include an `AuthSrvr` parameter, the DHCP server might not have sent the Sun Ray parameters or the parameters might not be correct.
 - To confirm that the DHCP server can be reached, check the value of the `DHCPserver` parameter.
 - To confirm that the DHCP server sends the proper Sun Ray-specific parameter values, check the value of the `INFORMServer` parameter.

If a value is incorrect, 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.
- To restart DHCP on a Solaris server, type the following as superuser:

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

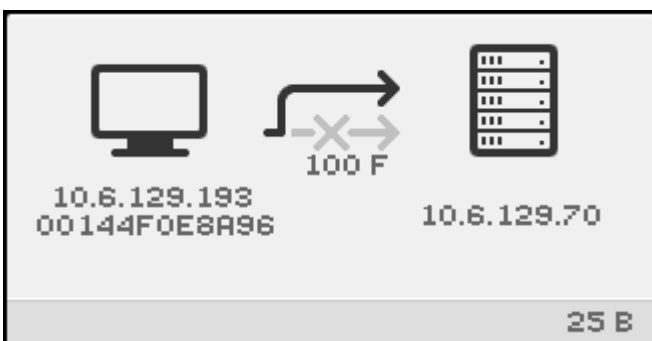
(23) No Ethernet Signal Icon



The No Ethernet Signal OSD indicates that the DTU had an Ethernet address and an IP address but later lost the Ethernet signal.

- Check that the Ethernet cable has not become unplugged from the DTU or from the switch or network outlet.
- If the DTU is connected through a hub or switch, make sure that the hub or switch is still powered on.

(25) Redirection Icon



The Redirection OSD indicates that the DTU is being redirected to a new Sun Ray server. This redirection can occur for any of several reasons, including load balancing. The icon is displayed for a few seconds while the DTU connects to the new Sun Ray server and then the Waiting to Connect to Authentication Manager OSD is displayed.

(26) Wait for Session Icon



The Wait for Session OSD indicates that the DTU is waiting for its X Window session. The icon is displayed for a few seconds as part of the normal startup process.

If this icon is displayed for a long time, display traffic from the server is not arriving to the client. Some possible reasons for this problem are:

- The network (routers, switches, firewalls) is not correctly transmitting UDP traffic from the server to the client.
- The server is attempting to display one of the Server Policy icons, but the client is behind a NAT router or gateway.
- The X server (Xnewt or Xsun) that is the source of the display traffic on the Sun Ray server side is not working properly. It might be crashed or hung.
- The display manager (`dtlogin` on Solaris 10 or `gdm` on Linux) has failed to start an X server for the session. It might be crashed, hung, or not configured properly. If you suspect that `dtlogin` configuration files have been corrupted, see [How to Check and Fix Corrupted Configuration Files \(Solaris\)](#).

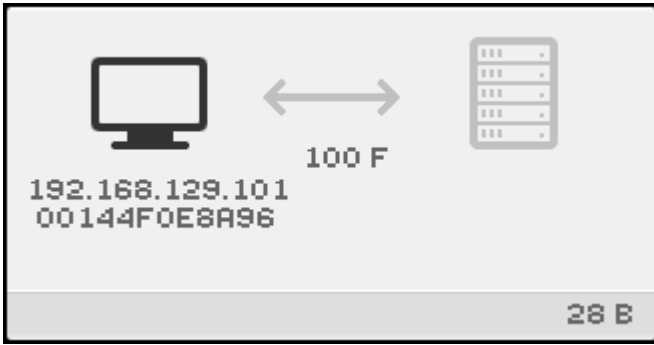
(27) Sun Ray Server Broadcast Discovery In Progress Icon



A Sun Ray DTU uses broadcast discovery for one of the following reasons:

- No individual server addresses were provided by the DTU's configuration (Pop-Up GUI), DHCP, or a `.parms` file.
- Individual server addresses were provided, but no server responded at the supplied addresses and the current configuration allows the DTU to attempt a broadcast discovery after failing to contact the supplied addresses.

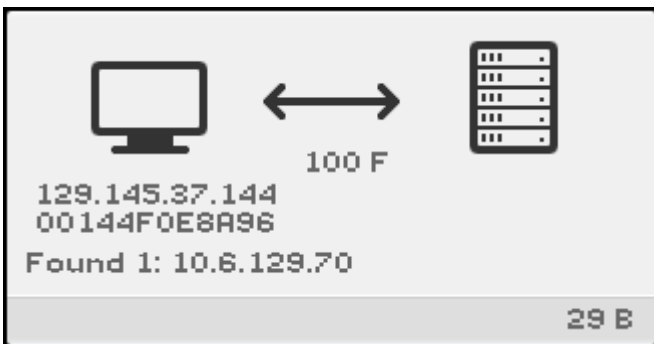
(28) Establishing VPN Connection Icon



The Establishing VPN Connection icon is displayed while a DTU is trying to connect to the Sun Ray server through a VPN connection. This icon can also include one of the following state codes for more information:

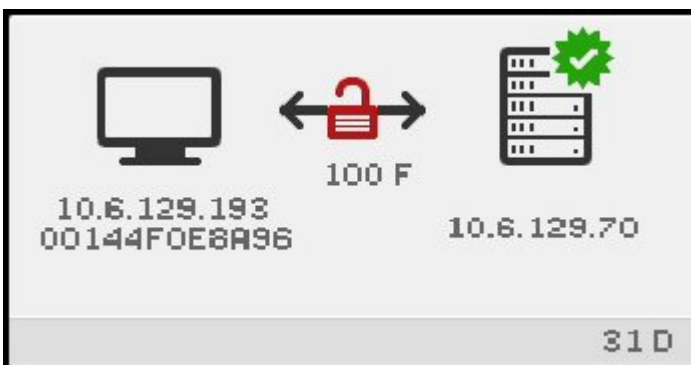
State Code	Meaning
E	VPN Phase 1 IKE initiated.
F	VPN Phase 1 IKE complete.
G	VPN connection expired.
H	VPN Phase 2 initiated.
I	VPN Phase 2 complete.

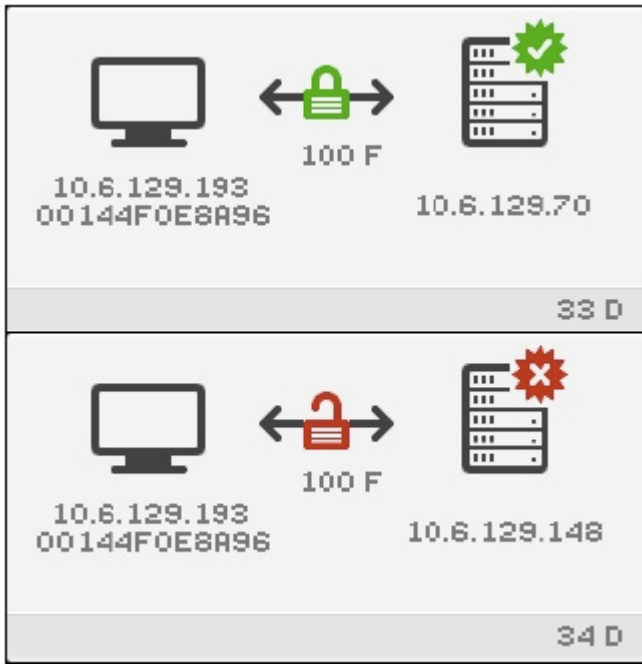
(29) VPN Connection Established Icon



When the VPN connection is established, the VPN Connection Established icon is displayed.

(31-34) Ethernet Address Icon





The Ethernet Address OSD shows the Ethernet address, the assigned IP address, the connected server, encryption status, DHCP state, link speed and link mode.

To display current information about the Ethernet link, do one of the following at any time.

- On a Sun keyboard, press the three audio volume keys simultaneously. To get the same effect on a non-Sun keyboard, type `Ctrl-Pause-N`.
- Disconnect and reconnect the Ethernet cable.

A value of 10 indicates a link speed of 10 Mbps; 100 indicates 100 Mbps. A value of F indicates that the link mode is full duplex. A value of H indicates half-duplex mode.

(46) No Access to Server Icon



This icon usually displays if the policy disallows card access and a card is inserted.

(47) No Access for Oracle Virtual Desktop Clients Icon



This icon indicates that access for Oracle Virtual Desktop Clients is disabled by default. To enable access for Oracle Virtual Desktop Clients, go to [Enabling Access for OVDC](#).

(48) No Access: Registration Required Icon



The card or DTU is not registered. If ATI is configured for a site, the ATI script is run when this icon is first displayed. If the script registers the card, this state might not last long.

(49) No Access: Key Rejected Icon



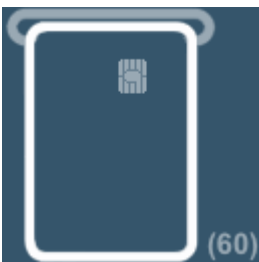
This icon is displayed if only confirmed keys are allowed access by policy. It might be displayed if there is a key conflict, but other icons might display instead.

(50) No Access: Security Policy Violation Icon



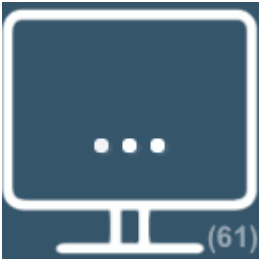
This icon is displayed if the client is running old firmware that does not support encryption or client authentication and the server has "hard" security mode set. This icon might also display in other security-related cases, such as key conflict or failed key validation, but other icons might display instead.

(60) Insert Card Icon



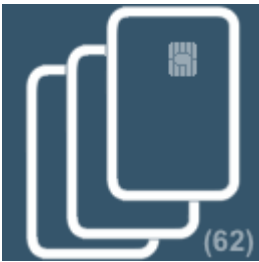
If the site's authentication policy allows access only by card, this icon is displayed to prompt the user to insert a card. Access without card is disabled.

(61) Waiting for Primary DTU Icon



The DTU is a secondary DTU in a multihead group, and the primary DTU is not currently connected.

(62) Token Reader Icon



The DTU is a token reader. When a site policy disallows pseudo-sessions, a DTU configured as a token reader displays the Token Reader icon instead of the Login dialog box.

(63) Smart Card Not Recognized Icon



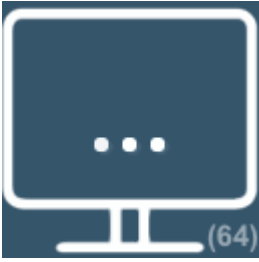
The smart card is not recognized by the Sun Ray server or there is a reader error. The following reasons may include:

- The Sun Ray client is running an older firmware.
- The smart card's contacts are dirty, the contacts on the smart card reader are dirty, or the card is not properly inserted.
- The smart card is malfunctioning.
- The Sun Ray server is not configured to read this type of smart card or an error exists in the configuration file.

To fix this problem, try one of the following actions:

- Upgrade the firmware on the Sun Ray client.
- Clean the smart card.
- Replace the smart card.
- Verify that the Sun Ray server has the appropriate smart card configuration files installed and configured.

(64) Waiting For Access Icon



This icon indicates that the server is not allowing access at the current time. This problem occurs when a Sun Ray DTU loses power or the network connection to the server is interrupted and the smart card from the Sun Ray DTU is inserted into a different Sun Ray DTU before the server has timed out the lost connection. Because the old connection is still active, new connections using the same smart card are unable to gain access.

When this conditions occurs, the server checks the status of the old connection. After the time reserved for this check has elapsed (an initial default of 10 seconds), the Sun Ray DTU connection is restarted and the condition should be automatically resolved. Either the session access is granted or the Sun Ray DTU remains in this Waiting for Access state (64).

If a Sun Ray DTU continues to remain in this state, the same `token` is being used with another connection. Specifically, two physical tokens (smart card, DTU, Oracle Virtual Desktop Client profile) are trying to connect to the same session.

Possible reasons for this issue include the following:

- A security incident where a copied or fake smart card is used to gain access to the session.
- A security incident where a copy of an Oracle Virtual Desktop Client profile is used to gain access to the session. This situation might also indicate a user error. Oracle Virtual Desktop Client profile files should not be copied to a different computer or user account.
- A registered token policy is in effect, alias tokens have been configured, and an alias token is still connected to the session the user is trying to access. If access is denied because of a currently connected alias token, the connected alias token needs to be disconnected to regain access. For example, the aliased smart card must be removed from its Sun Ray DTU.

Troubleshooting Audio Output

Tracking Audio Sessions

Each time a user logs in to a Sun Ray DTU, a script automatically assigns the `$AUDIODEV` environment variable to that session. One `utaudio` process is assigned to each session. Refer to the `utaudio` and `audio` man pages for more information.

Audio Device Emulation

During hotdesking, an emulated audio device follows the user to the new session. The name of the emulated device is carried in the `$AUDIODEV` environment variable. It is the responsibility of the audio application to inspect `$AUDIODEV` and direct its output to that device.

The emulated audio devices are created as device nodes in the `/tmp/SUNWut/dev/utaudio` directory. This directory tree is recreated at boot time.



Caution

Do not remove the `/tmp/SUNWut/dev/utaudio` directory. If you delete this directory, users with `utaudio` sessions cannot use their audio pseudo device nodes.

Problem: Audio is not working.

- Use the Sun audio keys (top right of keyboard) and check the volume and mute buttons.
- Display the Sun Ray session's audio settings:

```
$ utsettings
```

and verify that the audio output is selected properly, for example, for headphones or speakers.

- Make sure the volume is not muted in your desktop session.

- Try a set of external speakers plugged into the Sun Ray's audio out or headphones port. If that works, the Sun Ray might have a broken speaker.
- To test whether the audio is working, type the following:

```
$ cat <audiofile> > $AUDIODEV
```

Solaris provides suitable sample PCM-encoded audio files in `/usr/share/audio/samples/au`, so for instance this command:

```
$ cat /usr/share/audio/samples/au/gong.au > $AUDIODEV
```

should produce the sound of a gong.

Linux generally does not provide PCM-encoded audio files. If you can not locate a suitable file then this command can be used to generate a continuous tone:

```
$ perl -e 'foreach(-8..8){push(@v,pack("n",4*$_))} while(1){print @v}' > $AUDIODEV
```

If the `cat` or `perl` command hangs, you might need to quit any other applications that are currently trying to play audio, for example, a browser.

Problem: Audio is not working with Firefox.

- Check the current release of the Flash plugin and make sure it is at version 9.0.r125 or later. To check the Flash plugin version, type `about:plugins` as the URL in the browser.
- Try quitting Firefox and explicitly restart it in a terminal window: `/usr/dist/exe/firefox`.
- If all else fails, quit Firefox, go to your `.mozilla` directory, and rename the "firefox" directory to something else, for example, `firefox.jan09`. Then, restart Firefox and see whether the audio works with a completely clean configuration.

If the audio works with the clean configuration, then something is wrong in your browser's previous configuration.

Problem: An application ignores the `$AUDIODEV` environment variable.

Some applications fail to honor `$AUDIODEV` and unconditionally use a specific audio device node such as `/dev/audio` or `/dev/dsp`. To work around this shortcoming Sun Ray Server Software provides a preloadable shared library `libc_ut.so` that can be used to interpose on an application and redirect its activities to the device specified by `$AUDIODEV`. To put this redirection into effect:

1. Navigate to the shell or wrapper from which you started the audio player.
2. Set the environment variable `LD_PRELOAD` in the player application's environment to refer to the `libc_ut.so` interposer:

```
$ LD_PRELOAD=libc_ut.so
$ export LD_PRELOAD
```

3. Restart the application.

Troubleshooting Authentication

Authentication Error Messages

Errors in authentication are reported in the following log files:

- Installation logs:
 - `/var/adm/log` (Solaris only)
 - `/var/log` (Linux only)
- Configuration logs:
 - `/var/adm/log` (Solaris only)

- /var/log/SUNWut (Linux only)
- General log files:
 - /var/opt/SUNWut/log
 - /var/opt/SUNWut/srds/log
 - /var/opt/SUNWut/srds/repllog

Messages logged into /var/opt/SUNWut/log/messages are delivered through the `syslog` service described in the `syslogd` man page. The general format of these 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:
 - Worker# – Handles DTU authentication, access control, and session monitoring. 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, thread names are reused.
 - SessionManager# – Communicates with `utsessiondon` on behalf of a Worker# thread.
 - AdminJobQ – Used in the implementation to wrap a library that would not otherwise be thread-safe.
 - CallBack# – Communicates with applications such as `utload`.
 - WatchID – Used to poll data or terminals from connections
 - Terminator – Cleans up terminal sessions
 - Group Manager – Main group manager thread
- message_class:
 - 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 exits after this error is detected.
 - NOTICE – Indicates a normal event.
 - UNEXPECTED – Logs events or conditions that were not anticipated for normal operation but are not fatal.
 - DEBUG – Occurs only if explicitly enabled and is used by the development team. Debug messages can reveal session IDs, which must be kept secret to ensure proper security.

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.
CONFIG_ERROR	invalid key:	DTU does not properly implement the authentication protocol.
	attempt to instantiate CallBack 2nd time.	Program error.
	AuthModule.load	Problem encountered while loading configuration module.
NOTICE	Cannot find module	Program or installation error.
	"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 <code>utload</code> or <code>utidle</code> .
	.../ ... 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 error condition is also a way for <code>utauthd</code> to force the DTU to reset.

Troubleshooting General Problems

Problem: How do you get keyboard type information for a Sun Ray DTU?

No method currently exists to get the keyboard type information for a Sun Ray DTU.

Problem: Gnome Display Manager (GDM) consuming CPU cycles on headless Sun Ray server.

If you plan to use a headless Sun Ray server running Linux and Sun Ray clients using Gnome Display Manager (GDM), then this configuration will generate errors on the Sun Ray client and consume CPU processes. The errors occur because GDM assumes that the console display is present and GDM will continually attempt to (and fail to) service a non-existent console device.

The workaround is to add the `--no-console` option to the `preadm` command in the Sun Ray server's `/etc/inittab` file:

```
x:5:respawn:/etc/X11/xfstpm --nodaemon --no-console
```

Oracle servers have the Integrated Lights Out Manager (ILOM) Service Processor to provide a virtual console, so this configuration is not an issue and the workaround is not needed.

Troubleshooting Installation

Installation (utinstall) Error Messages

If during an installation, upgrade, or uninstall the `utinstall` script returns an error, refer to the following table for assistance.

All Installations

Message	Meaning	Resolution
<code>utinstall: fatal, media-dir is not a valid directory.</code>	You called the <code>-d</code> option, but <code>media-dir</code> is incomplete.	The <code>media-dir</code> directory requires relevant patches and packages for installation. The <code>media-dir</code> directory includes the Sun Ray directory.
<code>xxxxxx not successfully installed</code>	Might occur for the installation of any application or patch if relevant packages have not been properly installed.	Verify that the component <code>xxxxxx</code> is present in the installation media directory path and has the correct permissions, then run the <code>utinstall</code> script again.
<code>{{A different version x.x of product has been detected. The other-product Software is only compatible with product y.y. You must either upgrade or remove the current product installation before proceeding. Exiting ...}}</code>	Some of the applications provided with Sun Ray Server Software are compatible only with certain versions of other applications.	Compatible and necessary applications are included with Sun Ray Server Software. Remove older versions, then run the <code>utinstall</code> script again.

error, no Sun Ray software packages installed.	None of the Sun Ray components are installed on this system.	No action is required as the product is not installed.
The following files were not successfully replaced during this upgrade. The saved copies can be found in <directory>	Some files were not properly replaced as part of the upgrade.	Manually copy the listed files from the directory, overwriting the newer files if applicable.
<pre> Partition Name Space Required Space Available ----- ----- partition xxx YYY </pre>	Not enough disk space was allocated for partition. Repartition the disk and run <code>utinstall</code> again.	

Linux Installations

Message	Meaning	Resolution
The following packages were not successfully removed xxxxxx ...	The packages listed have not been properly removed.	Use the <code>rpm -e</code> command to remove each listed rpm manually, then run <code>utinstall -u</code> again.
Removal of product was not successfully completed. See log file for more details.	Removal of Sun Ray Server Software was incomplete.	Check the log file for the package that started the problem and manually remove it with the <code>rpm -e</code> command, then run <code>utinstall -u</code> again.

Solaris Installations

Message	Meaning	Resolution
Cannot open for read admin-file	The <code>admin_default</code> file is unreadable, or you called the <code>-a</code> option and the <code>admin-file</code> is unreadable.	Verify that the installation administration file exists (<code>admin_default</code> or other) and the permissions are correct.
For SPARC platforms: SunOS release is x.x, valid releases are: 10	You are attempting to install Sun Ray Server Software onto a Solaris software version that does not support SRSS 4.2.	Upgrade to the supported version 10 of the Solaris OS before installing Sun Ray Server Software.
For x86 platforms: SunOS release is x.x, valid releases are: 10	You are not running a valid OS release for this platform.	Upgrade to the supported version 10 of the Solaris OS before installing Sun Ray Server Software.
Please clean up the directory <code>/var/tmp/SUNWut.upgrade</code> before rerunning <code>utinstall</code> .	Other unrelated files were found in the preserve directory.	Remove unrelated files from the directory.
Please remove the existing preserved file <code><preserved_tarfilename></code> before rerunning <code>utinstall</code> .	You decided not to restore from the indicated tar file.	Remove the tar file before running <code>utinstall</code> again.
<code>utpreserve: unable to preserve data. Error while creating archive file</code>	The <code>utinstall</code> script failed to preserve existing configuration files.	Either exit and manually preserve these files or just continue.
The following packages were not successfully removed xxxxxx ...	The packages listed have not been properly removed.	Use the <code>pkgrm</code> command to remove each listed package manually, then run <code>utinstall -u</code> again.
Removal of product was not successfully completed. See log file for more details.	Removal of Sun Ray Server Software was incomplete.	Check the log file for the package that started the problem and manually remove it with the <code>pkgrm</code> command, then run <code>utinstall -u</code> again.

Modified System Files (Solaris)

The following files are modified during `utadm`:

- `/etc/inet/hosts`
- `/etc/inet/networks`
- `/etc/inet/netmasks`
- `/etc/inet/dhcpsvc.conf` # including all DHCP-related files
- `/etc/nsswitch.conf`
- `/etc/hostname.intf`

The following files are modified during Sun Ray service startup:

- `/etc/inet/services`
- `/etc/inet/inetd.conf`

The following files are modified during `utconfig`:

- `/etc/passwd`
- `/etc/shadow`
- `/etc/group`

After installation, the following files are updated upon reboot:

- `/etc/syslog.conf`
- `/etc/pam.conf`

Modified System Files (Linux)

The following files are modified during `utadm`:

- `/etc/dhcpd.conf`
- `/etc/nsswitch.conf`
- `/etc/opt/SUNWut/net/dhcp/SunRay-options`
- `/etc/opt/SUNWut/net/dhcp/SunRay-interface-eth1`
- `/etc/opt/SUNWut/net/hostname.eth1`
- `/etc/opt/SUNWut/net/networks`
- `/etc/opt/SUNWut/net/netmasks`
- `/etc/hosts`

The following files are modified during `utconfig`:

- `/etc/passwd`
- `/etc/shadow`
- `/etc/group`

SRSS also updates the GDM configuration file, `custom.conf`, to make sure it has the following entries, which are removed when SRSS is removed:

```
VTAllocation=false
DynamicXServers=true
```

In addition, display files are created for each Sun Ray DTU in the following directories:

- `PreSession`
- `PostSession`
- `Init`
- `PostLogin`

Log Files

Significant activity occurring on the Sun Ray server is logged and saved. The server stores this information in text files. The following table describes the log files that are maintained.

Log File	Path	Description
Administration	<code>/var/opt/SUNWut/log/admin_log</code>	Lists operations performed during server administration. This log is updated daily. Archived files are stored on the system for up to one week and are annotated using numeric extensions, for example, from file name <code>admin_log.0</code> to <code>admin_log.5</code> .
Authentication	<code>/var/opt/SUNWut/log/auth_log</code>	Lists events logged from the Authentication Manager. The <code>auth_log</code> file is updated up to a limit of 10 every time the server's authentication policy is changed or started. The archived authentication files are annotated using numeric extensions, for example, from <code>auth_log.0</code> to <code>auth_log.9</code> .
Automatic Mounting	<code>/var/opt/SUNWut/log/utmouted.log</code>	Lists mount messages for mass storage devices. The archived <code>mountd</code> files are annotated using numeric extensions, for example, from <code>utmouted.log.0</code> to <code>utmouted.log.9</code> .
Mass Storage Devices	<code>/var/opt/SUNWut/log/utstoraged.log</code>	Lists mass storage device events. The archived storage files are annotated using numeric extensions, for example, from <code>utstoraged.log.0</code> to <code>utstoraged.log.9</code> .
Messages	<code>/var/opt/SUNWut/log/messages</code>	Lists events from the server's DTUs, including details of registering, inserting, or removing smart cards. This file is updated daily. Archived files are stored up to seven days or 3.5 MB, annotated with numeric extensions, for example, from <code>messages.0</code> to <code>messages.5</code> .
Web Administration	<code>/var/opt/SUNWut/log/utwebadmin.log</code>	Lists web administration-related messages. The archived log files are annotated with numeric extensions.

The structure and content of the various messages written to these files and other SRSS log files is arbitrary and might change at any time. The messages do not provide a stable interface for programmatic consumption.

Troubleshooting Login Problems

The Sun Ray administration model has seven types of user sessions:

- Default – Normal user login
- Register – User self-registration
- Kiosk – Anonymous user operation
- Insert card – User smart card required
- Card error – Unrecognized user smart card type
- No entry – User's smart card token is blocked
- Session Refused – The server refuses to grant a session to a DTU that does not meet the server's security requirements

The Default, Register, and Kiosk session types have normal login processes. When a problem occurs, investigate the following:

- Sun Ray server configuration files. However, the Sun Ray Server Software itself modifies some configuration files. In most cases, these changes are identified with SRSS-specific comments. Do not change these modifications.
- Any X server startup files that have been modified
- `dtlogin` status

Although the last four session types display icons on the Sun Ray DTU, they do not have login processes. If the user removes and reinserts the smart card immediately, the icon disappears but the Wait for Session OSD icon remains. These session types and their OSDs do not cause concern. The user can perform one of the following actions:

- 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

Problem: The `dtlogin` daemon cannot start the Xsun server properly.

See [How to Check and Fix Corrupted Configuration Files \(Solaris\)](#).

Troubleshooting Multihead Displays

Multihead Video

The H264 and VC-1 streams are synchronized with the audio stream on the DTU. In a multihead group, the audio stream is directed only to the primary DTU, so audio/video synchronization can only be performed on the primary DTU. When video is displayed on secondary DTUs, the application must perform the A/V synchronization.

Problem: The display resolution is 640 x 480.

If the Sun Ray DTU is unable to read DDC data from the monitor, it defaults to 640 x 480 pixels. This condition occurs for the following reasons:

- The monitor was powered off when the Sun Ray DTU was started
- A bad cable
- An older monitor

How To Reset the Screen Resolution

1. Replace the cable.
2. Restart the Sun Ray DTU after powering the monitor on.
3. Replace the monitor.
4. Set a persistent display setting to override the default.

```
utresadm
```

Troubleshooting Network Problems

The `utcapture` Utility

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.

The `utcapture` command outputs the following information:

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

Problem: Sun Ray DTU traffic loss of more than 0.1%.

Sun Ray DTU traffic loss of more than 0.1%, may indicate a network problem. You may want to allocate higher priority to the VLAN that carries Sun Ray DTU traffic. For more information on how to change the priority, see the manufacturer's documentation for your switch.

`utcapture` Examples

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

```
% utcapture -h |
```

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

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

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

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

The following 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.

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

The `utquery` Command

The `utquery` command interrogates a DTU and displays the DTU's initialization parameters with the IP addresses of the DHCP services that supplied those parameters. This command 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 [SRSS Troubleshooting Icons](#).

How To Identify a Hung Session

1. Become superuser
2. Type the following command:

```
# /opt/SUNWut/sbin/utdesktop -l -w
```

How To Kill a Hung Session

1. Become superuser
2. Type the following command:

```
# /opt/SUNWut/sbin/utsession -k -t token
```

Troubleshooting Printers

Problem: "Failed to open the printer port" message.

Verify that the printer node used for configuring the printer has been created and is available under `/tmp/SUNWut/units/IEEE802.<macid>/dev/printers`.

If the printer node is not available, reboot the DTU.

Troubleshooting Sun Management Center (Solaris)

When the Sun Ray server has the Sun Management Center agent installed, the normal operation is for the agent to start automatically. The Sun Ray server becomes a monitored Sun Management object.

Problem: Sun Management Center's Detail window does not show a Sun Ray object for the Sun Ray server node.

Load the Sun Ray module or enable the module manually.

How To Load the Sun Ray Module

1. Click the Sun Management Center's Modules tab.
2. In the Module Name column, look for the Sun Ray entry.
3. Check the status of the Sun Ray entry. Its Load status must be Yes and its Enabled status must be Yes.

The screenshot shows the Sun Management Center interface with the 'Modules' tab selected. The 'Modules with Load Status' table is as follows:

Module Name	Loaded	Scheduled	Enabled
Agent Statistics	Yes	No	Yes
Config Reader (Ultra Work...	Yes	No	Yes
Kernel Reader (Simple)	Yes	No	Yes
MIB-II System (Simple)	Yes	No	Yes
Sun Ray	Yes	No	Yes

Below this table is the 'Available Modules' section:

Module Name	Multi-instance
Data Logging Registry	No
MIB-II Proxy Monitoring	Yes

On the right side of the interface, there are buttons for 'Unload', 'Load Now', 'Edit...', 'Enable', 'Disable', 'Rules...', and 'Load...'.

4. If the Load status is not Yes, select the Sun Ray entry and then click the Load button. This action loads the module and moves it to the Modules with Load Status list.
5. If the Enabled status is not Yes, select the Sun Ray entry and then click the Enable button.
6. Return to the Detail window.

The Detail window now shows a Sun Ray object for the Sun Ray server node.

Problem: The list of modules on the Modules tab does not include an entry for Sun Ray.

Add the module manually and restart its agent.

How to Register and Start the Sun Ray Module

1. Issue the following command to add the module to the Sun Management Center and restart its agent:

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

2. If a message displays indicating that the agent failed to start, type the following command to verify that the agent is running:

```
# ps -ef |grep agent
```

If the Sun Management Center agent is running, wait a few minutes and then check the Detail window.

3. If the agent is not running, type the following command to start the Sun Management Center agent:

```
# /opt/SUNWsymon/sbin/es-start -a
```

Troubleshooting USB Storage

Problem: Device nodes are not created.

Check the log file `/var/opt/SUNWut/log/utstoraged.log` for a message about why device nodes were not created. Some mass storage device types are not supported.

Problem: The device is not automatically mounted.

Check the log file `/var/opt/SUNWut/log/utmouted.log` for an error message.

This condition occurs when the Sun Ray operating system does not recognize the storage devices's file system.

Problem: The device is not automatically unmounted.

This condition occurs when a user still has an open reference to the mount point at the time the storage device is unplugged or the user's session is disconnected. The mount point becomes a stale mount point and persists until the system is rebooted or until the administrator removes it.

How to Find and Remove Stale Mount Points

1. Search for stale mount points:

```
# utdiskadm -s
```

2. For each stale mount point, close all references to the mount point.
3. For each stale mount point, terminate all processes that refer to the mount point.
4. Remove the mount point.

```
# umount <stale_mount_path>
```

Indice

- Ottimizzazione delle applicazioni
 - Ottimizzazione di Java Desktop System
 - Ottimizzazione della rete
 - Switch di rete
 - Carico di rete
 - Ottimizzazione del server Sun Ray
 - Swap su disco eccessivo
 - Consumo di risorse del salvaschermo
-

Ottimizzazione (tutti gli argomenti)

Ottimizzazione delle applicazioni

Alcune applicazioni quali le simulazioni visive a utilizzo intensivo di effetti 3D possono risultare molto lente in un client Sun Ray.

Le applicazioni che utilizzano il doppio buffering, quali i visualizzatori PSVS (pseudo-stereo) e le applicazioni che utilizzano inversioni dinamiche della tabella colori ad alta frequenza in schermi a 8 bit potrebbero non mostrare i risultati appropriati. Disattivare l'antialiasing per risparmiare risorse dello schermo.

Installare le applicazioni interattive quali browser Web e StarOffice(TM) e gli strumenti di interoperabilità per PC quali Citrix e Sun Secure Global Desktop (SGD) nel server Sun Ray. Le applicazioni beneficiano di un trasporto più rapido dei comandi al server X Sun Ray e il traffico di rete risulta ridotto.

Se un'applicazione può essere configurata per l'utilizzo della memoria condivisa anziché di DGA o OpenGL(R), l'utilizzo della memoria condivisa garantirà prestazioni migliori.

Ottimizzazione di Java Desktop System

Per ottimizzare le prestazioni a livello desktop, utilizzare sfondi schermo uniformi e spostamenti delle finestre in modalità wireframe.

Per istruzioni e consigli aggiuntivi, vedere le seguenti informazioni:

- [Documentazione di Java Desktop System](#)
- [GNOME Performance Enhancement Tips for the Solaris Platform](#) (Suggerimenti per il miglioramento delle prestazioni di GNOME per la piattaforma Solaris)
- [GNOME Performance Script for Solaris](#) (Script per il miglioramento delle prestazioni di GNOME in Solaris)

Ottimizzazione della rete

Switch di rete

Alcuni switch di rete non funzionano correttamente con le DTU Sun Ray quando la connessione sul server è configurata per l'esecuzione a 1 Gbps. Poiché le DTU Sun Ray eseguono a 100 Mbps e i dati vengono inviati dal server X Window mediante impulsi periodici, tali switch devono prevedere il buffering di una determinata quantità di dati. La situazione può verificarsi anche quando la velocità media dei dati provenienti dal server X è ampiamente inferiore a 100 Mbps.

Il server X è programmato in modo che una determinata quantità di dati consentita viene inviata a intervalli tick. L'implementazione originale prevedeva 50 tick per secondo. Il server X è in grado di inviare dati a una determinata velocità, supportata dalla DTU Sun Ray.

Se ad esempio la velocità supportata dalla DTU Sun Ray è di 40 Mbps, può inviare 5 MB al secondo in impulsi inviati ogni cinquantesimo di secondo. Ciò significa che a ogni tick il server può inviare 100 KB di dati a una velocità di 1 Gbps. Questa velocità determinerà la creazione di una coda di circa 100 KB nello switch, che verrà smaltita a 100 Mbps nel successivo cinquantesimo di secondo.

La prima operazione per ovviare a questo tipo di problema consiste nell'incrementare il numero di tick al secondo da 50 a 100. In tal modo, nell'esempio precedente, il server X invierebbe 50 KB ogni 10 ms anziché 100 KB ogni 20 ms. Tale impostazione migliorerà notevolmente la situazione, ma il problema persisterà. La velocità di 100 tick al secondo è stata scelta perché corrispondeva alla risoluzione normale del timer nel software Solaris e Linux.

Incremento del timer del sistema operativo (Solaris)

Per incrementare il numero di tick per secondo oltre il valore 100 è necessario incrementare anche il timer del sistema. Nella piattaforma Solaris utilizzare la seguente procedura.

1. Aprire il file `/etc/system`.
2. Aggiungere il seguente comando:

```
set hires_tick = 1
```

3. Salvare e chiudere il file.
4. Riavviare il sistema.

L'impostazione `hires_tick = 1` incrementa la risoluzione del timer di sistema a 1000 tick al secondo.

Poiché il codice del server X utilizza l'impostazione di sistema, gli impulsi di dati del server X ora utilizzano lo stesso valore, 1000 tick = 1 secondo, ovvero 1 tick = 1 ms. Nell'esempio, l'utilizzo della nuova frequenza di tick determina l'invio di 5 KB di dati per millisecondo da parte del server X.

La modifica della durata dei tick consente di ridurre la quantità di buffering necessaria nello switch di rete e di ottenere pertanto migliori prestazioni delle DTU Sun Ray.

Carico di rete

In situazioni in cui il carico di rete o la perdita di pacchetti risultano troppo elevati, è possibile che in rari casi gli switch o i cavi di rete siano difettosi.

1. Verificare che l'impostazione per le connessioni di rete sia 100F.
2. Utilizzare `utcapture` per valutare la latenza di rete e la perdita di pacchetti.

Se la latenza e la perdita di pacchetti aumentano, le prestazioni risultano ridotte.

Ottimizzazione del server Sun Ray

Swap su disco eccessivo

Se il server Sun Ray non dispone di sufficiente memoria virtuale, l'istanza del server X Window non si avvia e l'utente nota un rallentamento dell'esecuzione. Quando la memoria virtuale è insufficiente, il server Sun Ray effettua una quantità eccessiva di swap su disco.

Per determinare se la quantità di swap su disco del server Sun Ray è eccessiva, utilizzare il comando `vmstat`:

```
# vmstat 5
```

Se la quantità di swap è eccessiva, è possibile che il sistema sia sottodimensionato o utilizzato oltre i suoi limiti.

La soluzione consiste nell'aggiunta di memoria o nell'incremento delle dimensioni della partizione di swap.

Consumo di risorse del salvaschermo

I programmi salvaschermo che includono una grande quantità di elementi grafici possono consumare grandi quantità di memoria e ampiezza di banda della CPU e della rete. Per evitare un consumo di risorse eccessivo nei server Sun Ray, è consigliabile disattivarli.

Disattivazione dei salvaschermo (Solaris)

Rimuovere i pacchetti dei salvaschermo.

```
# pkgrm SUNWxscreensaver-hacks
# pkgrm SUNWxscreensaver-hacks-g1
```

Se la rimozione del pacchetto `SUNWxscreensaver-hacks-g1` non riesce, rimuovere il pacchetto `g1` e quindi il pacchetto `SUNWxscreensaver-hacks-g1`.