Sun Ray Software: Security Guide for Release 5.4

Abstract

This guide explains how to securely install, configure, and manage the Sun Ray Software 5.4 release.
# Table of Contents

Preface .................................................................................................................. v
1. Overview .......................................................................................................... 1
2. Desktop Client Security ...................................................................................... 3
   2.1. Sun Ray Clients .......................................................................................... 3
       2.1.1. Fiber Ethernet Connections ................................................................. 3
       2.1.2. 802.1x Authentication .......................................................................... 3
       2.1.3. Built-in Virtual Private Network (VPN) ............................................... 3
       2.1.4. IPsec .................................................................................................... 3
       2.1.5. Firmware Update Authentication ....................................................... 4
   2.2. Oracle Virtual Desktop Clients .................................................................... 4
   2.3. Operating System ....................................................................................... 6
3. Sun Ray Server Security ..................................................................................... 5
   3.1. Operating System ....................................................................................... 5
   3.2. Installation ................................................................................................ 6
   3.3. Administration ........................................................................................... 6
       3.3.1. Administration Privilege Requirements ............................................ 6
       3.3.2. Admin GUI ......................................................................................... 6
4. Client-to-Server Security .................................................................................. 7
   4.1. Network Topology ................................................................................... 7
   4.2. Network Traffic ......................................................................................... 7
   4.3. Appliance Link Protocol (ALP) ................................................................ 7
   4.4. Client Access Policy ................................................................................ 8
       4.4.1. Oracle Virtual Desktop Clients Access ........................................... 8
       4.4.2. Client Authentication ....................................................................... 8
   4.5. Session Access Policy .............................................................................. 8
       4.5.1. Access Without Smart Cards ............................................................. 8
       4.5.2. Access Using Smart Cards ................................................................. 8
       4.5.3. Authenticated Sessions ...................................................................... 8
       4.5.4. Unauthenticated Sessions With Kiosk Mode .................................... 10
       4.5.5. External Peripherals ......................................................................... 11
5. Server-to-Server Security .............................................................................. 13
   5.1. Sun Ray Data Store .................................................................................. 13
   5.2. Group Manager ......................................................................................... 13
   5.3. Failover Group Network Service ............................................................... 13
6. Desktop Connector Security ............................................................................ 15
   6.2. VMware View Manager Authentication ................................................. 15
Preface

This document provides information for the Sun Ray Software 5.4 product.

Audience

This document is intended for users with system administration experience. It is assumed that readers are familiar with Web technologies and have a general understanding of Windows and UNIX platforms.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Related Documents

The entire set of documentation for this product is available at:

http://www.oracle.com/technetwork/server-storage/sunrayproducts/docs

The documentation set includes the following manuals:

• Sun Ray Software 5.4 Administration Guide
• Sun Ray Software 5.4 Release Notes
• Sun Ray Software 5.4 Security Guide
• Oracle Enterprise Manager System Monitoring Plug-in Installation Guide for Sun Ray Software

Conventions

The following text conventions are used in this document:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>boldface</td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td>italic</td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td>monospace</td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
Chapter 1. Overview

The Sun Ray computing model has always had a fundamental security advantage at a server/client level, which starts with the Sun Ray Clients themselves. With no local operating system or local applications on the client, sensitive data remains on the server instead of on individual hard drives, desktops, or laptops. This model makes the user's data significantly less vulnerable to theft, loss, and viruses. Security is built into the system by design and is not dependent on keeping clients, which contains sensitive data, patched and updated to ensure data integrity.

Beyond the inherent security benefits of the hardware and the server/client model, security in a Sun Ray environment is provided at the various management layers:

- Sun Ray Server - Runs the Sun Ray Software and is the foundation of the Sun Ray environment. It provides all the necessary administrative support for the desktop clients, including Sun Ray Clients and Oracle Virtual Desktop Clients.

- Network - The physical network and the protocols used for communication between the Sun Ray Server and the desktop clients.

- Desktop Clients - The desktop clients used by the users, which includes both the Sun Ray Client and the Oracle Virtual Desktop Client.

It is recommended that you read the *Sun Ray Software Administration Guide* to become familiar with the basic features and concepts of the Sun Ray Software product. This *Security Guide* is intended to provide all the Sun Ray Software security-related information in one place, but you will be referred to the *Administration Guide* for most of the details.
Chapter 2. Desktop Client Security

This chapter describes the security benefits provided by the Sun Ray Clients and Oracle Virtual Desktop Clients. Specifically, these are the client-side security benefits that are independent from the communication with the Sun Ray server.

2.1. Sun Ray Clients

This section describes the security benefits provided by the Sun Ray Clients.

2.1.1. Fiber Ethernet Connections

Both the Sun Ray 2FS Client and the Sun Ray 3 Plus Client provide fiber ethernet capabilities, which provide an additional security benefit over copper-based ethernet. Fiber cable does not generate radiated emissions along the length of the wire, so fiber cable is more difficult to tap than copper-based cable.

The Sun Ray 2FS Client has a built-in 100-FX port and the Sun Ray 3 Plus Client has an SFP (Small Form-factor Pluggable) network module slot. The SFP slot on the Sun Ray 3 Plus Client can accept a third-party module supporting a variety of commercial 1 Gb or 100 Mb optical fiber SFP network modules. See the Sun Ray 3 Series Clients Product Guide for details.

2.1.2. 802.1x Authentication

With the 802.1x authentication feature, you can configure Sun Ray Clients to provide proper credentials to successfully authenticate and gain access to the local area network under 802.1x access control. Sun Ray Clients support the Extensible Authentication Protocol Modes: MD5, TLS, MSCHAPV2, PEAP, TTLS, GTC, and OTP.

See 802.1x Authentication in the Administration Guide for details.

2.1.3. Built-in Virtual Private Network (VPN)

Sun Ray Clients can be located anywhere. If they are located outside the corporate network, their built-in VPN capabilities make it more difficult for network traffic to be intercepted.

The IPsec capability in the Sun Ray Client firmware enables the Sun Ray Client to act as a VPN endpoint device. The most commonly used encryption, authentication, and key exchange mechanisms are supported, along with Cisco extensions that enable a Sun Ray Client to interoperate with Cisco gateways that support the Cisco EzVPN protocol. Sun Ray Clients currently support IPsec VPN concentrators from Cisco and Netscreen (Juniper). See VPN Support in the Administration Guide for details.

2.1.4. IPsec

Beyond the IPsec capability to make Sun Ray Client as a VPN endpoint device, Sun Ray Software also supports IPsec to provide high quality, cryptographically-based security between Sun Ray Clients and Sun Ray servers. After configuring and enabling IPsec on the Sun Ray server and the Sun Ray Client, the Sun Ray Client will negotiate a secure end-to-end IPsec tunnel with the Sun Ray server before interacting with Sun Ray services on the server.

The Sun Ray Software implementation of IPsec is incorporated into the Sun Ray Client firmware. The Sun Ray Client will always be the initiator of a connection, so it does not have to respond to inbound connection requests. This type of negotiation is similar to the current IPsec VPN behavior, where IPsec is established with a VPN gateway before Sun Ray services are invoked. However, both IPsec implementations require different configurations.
2.1.5. Firmware Update Authentication

The Sun Ray Operating Software (firmware) images for the Sun Ray Clients are digitally signed. Because
the Sun Ray Client verifies the firmware signature as part of the firmware update process, the client will not
accept an image that has been tampered with. This minimizes the chance of installing firmware that can
compromise the Sun Ray Client.

To gain the latest features and security enhancements, you should always update your site’s Sun Ray
Clients with the latest Sun Ray Operating Software.

2.2. Oracle Virtual Desktop Clients

Similar to Sun Ray Clients, Oracle Virtual Desktop Clients provide a stateless connection to the desktop
session running in the server infrastructure, which users can access with or without smart cards. However,
Oracle Virtual Desktop Clients do not provide many of the built-in security capabilities that the Sun Ray
Clients provide, such as IPsec tunneling, VPN, 802.1x authentication, and network connectivity. Instead,
these capabilities are provided by the platform on which the Oracle Virtual Desktop Client is running, so
choosing a platform for an Oracle Virtual Desktop Client dictates the security capabilities available.

In fact, using the platform for the underlying client security can provide benefits beyond what the Sun Ray
Client provides, such as expanded VPN capabilities. And, beyond security considerations, the platform can
provide additional network connectivity options such as wireless or cellular.

Here are some additional security considerations for Oracle Virtual Desktop Clients:

- **Clipboard sharing** - Clipboard sharing is the ability for the user to copy and paste text between an
  application running in an Oracle Virtual Desktop Client session and an application running on the local
desktop. By default, this feature is disabled. For the copy and paste functionality to work, the clipboard
service must be enabled on the Sun Ray server and clipboard sharing must be enabled on the Oracle
Virtual Desktop Clients. You can use the `utdevadm` command or the Security page of the Admin GUI
to enable the clipboard service. See [How to Enable the Clipboard Service for Oracle Virtual Desktop
Clients](#) in the *Administration Guide* for details.

  - **Note**
    
The clipboard service is not available on Sun Ray servers running Oracle Solaris
    Trusted Extensions.

- **Secure profile entries** - By default, security-sensitive profile entries, such as the client key, are not
  shown in the profile file. If you deselect this check box in the Advanced tab, all profile file entries are
  shown in the profile file.
Chapter 3. Sun Ray Server Security

This chapter describes the security considerations for the Sun Ray server.

3.1. Operating System

You can install Sun Ray Software on a server running the Oracle Solaris or Oracle Linux operating system, and Sun Ray Software gains all the security-related benefits from those operating systems. To gain more security at the operating system level, Sun Ray Software is also supported on Oracle Solaris with Trusted Extensions. For more information about what additional configuration steps are required when using Oracle Solaris with Trusted Extensions, see Installing and Configuring in the Administration Guide.

3.2. Installation

Here are other security-related considerations when installing a Sun Ray server:

- **Secure by default** - When using the utsetup installation program to install Sun Ray Software, the Sun Ray Software is automatically activated. When activated, security-related policy settings are set to default values, which try to maintain a good balance between security and usability. If more relaxed settings are appropriate for the particular deployment, then you must specifically adjust those settings. Conversely, you can adjust the settings the other way if you require enhanced security. See Chapter 4, Client-to-Server Security for details.

If you do not use utsetup for installation, Sun Ray Software is activated on the server by using the utconfig, utadm, or utstart command.

- **Preserving data before upgrade** - Before you upgrade a Sun Ray server, you need to back up the configuration data to a utpreserve tar file. This tar file contains sensitive information, so make sure to use sufficient security precautions when copying or storing this file. See How to Preserve Sun Ray Software Configuration Data in the Administration Guide for details.

- **Cloning installations** - When cloning a Sun Ray server using the utsetup command, make sure to use sufficient security precautions when copying or storing the *.utdialog_responses.props files, because they may contain passwords. See How to Clone a Sun Ray Server in the Administration Guide for details.

- **Restricting Oracle Linux privileges** - Oracle Linux comes preconfigured with liberal administrative privileges for non-root users. These privileges should not be made available to users who log in using a Sun Ray Client. To prevent this, see How to Limit Administrative Privileges for Non-root Users (Oracle Linux) in the Administration Guide.

3.3. Administration

This section describes the administration privilege requirements for the Sun Ray Software tools and how to secure access to the Sun Ray Software Administration GUI (Admin GUI).

3.3.1. Administration Privilege Requirements

Access to the Sun Ray Software commands require root access to the Sun Ray server. Currently, there is no delegated administration mode for the command line, meaning there is no way to assign privileges to specific users to run specific commands.

Similarly, there is no delegated administration mode for the Sun Ray Software Admin GUI. Anyone who is granted access to the Admin GUI has access to the entire Admin GUI and all the administration tasks you
can perform from it. See Administrative Name and Password in the Administration Guide for information about managing the Admin GUI password.

Although there is no way to provide access to specific areas of the Admin GUI, you can enable more users beyond the admin user to access the Admin GUI. See Section 3.3.2, “Admin GUI” for details.

3.3.2. Admin GUI

There are various security considerations when using the Sun Ray Software Admin GUI, including accessing, session timeout, and auditing.

Accessing

- **SSL security** - You can configure the Admin GUI to require access through SSL, which encrypts the data between the browser and the Admin GUI web server. Enabling SSL is strongly recommended and is enabled by default during the Sun Ray Software installation (“Enable secure connections?” question). Post installation, you can enable or disable SSL with the `utconfig -w` command.

  SSL also provides authentication of the server. By default, the Admin GUI web server is configured with a self-signed certificate that can cause browsers to show a warning when contacting the server, but you can install other certificates if that is preferred. You can also configure the Admin GUI web server to require client certificates for additional security.

- **Local or Remote Access** - You can configure the Admin GUI to accept connections only from the local system. Local access is likely to be more secure than allowing connections from outside the server. Remote access to the Admin GUI is disabled by default during the Sun Ray Software installation (Enable remote server administration?). Post installation, you can enable or disable remote access to the Admin GUI with the `utconfig -w` command.

  • **Multiple administration accounts** - By default, only the Sun Ray Software admin user account can be used to access the Admin GUI. However, you can configure any valid UNIX user ID to be able to access the Admin GUI and administer Sun Ray services. To do this, you need to add the user to the `utadmin` authorized user list with the `utadminuser` command and configure the appropriate authentication permissions through the PAM framework using the `utadmingui` PAM service name.

  See Administration Tool (Admin GUI) in the Administration Guide for details.

Session Timeout

By default, if your Admin GUI session is inactive for 30 minutes, you must log in again. You can increase or decrease the timeout value depending on your security requirements. See How to Change the Admin GUI Timeout for details.

Auditing

There may be times when you need to determine how or when an administrative action was performed with the Admin GUI. Activities performed with the Admin GUI are recorded by messages sent to syslog, which by default are appended to the `/var/opt/SUNWut/log/messages` file. The text portion of messages begins with the string `utadt::`. The format and content of other messages in this file are generally highly volatile, but the format of the `utadt::` messages are considered stable.

See How to Audit Admin GUI Sessions for details.
Chapter 4. Client-to-Server Security

This chapter describes the security aspects of the interactions between the desktop clients and the Sun Ray server.

4.1. Network Topology

Sun Ray Software supports various network configurations, but a shared network is recommended. A shared network is where the Sun Ray server and desktop clients are part of a Local Area Network (LAN) or Wide Area Network (WAN) and where network services such as DHCP and DNS are already provided by existing servers. The same security considerations for standard shared networks apply to a shared network used for a Sun Ray environment. See Planning a Sun Ray Network Environment in the Administration Guide for details.

4.2. Network Traffic

Securing network traffic between the desktop clients and the Sun Ray server can be accomplished through firewalls, switches, and network encryption.

- For firewalls, consider the list of ports and protocols used for Sun Ray Software. See Ports and Protocols in the Administration Guide for details.

- Use switched network gear for the last link to the desktop clients. This configuration makes it very difficult for a malicious PC user or network snooper 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 desktop client is plugged directly into the wall jack, then it becomes virtually impossible for communications between the server and the client to be intercepted.

- Use the ARCFOUR encryption algorithm and the Digital Signature Algorithm (DSA) authentication scheme that Sun Ray Software provides to protect data between Sun Ray servers and their desktop clients. It is recommended that you enable and configure encryption and authentication based on your site's requirements, unless you are confident that your network is secure and performance is an issue. See Encryption and Authentication in the Administration Guide for details on how to enable and disable encryption and authentication in a Sun Ray environment.

4.3. Appliance Link Protocol (ALP)

Sun Ray Clients and Oracle Virtual Desktop Clients use the Appliance Link Protocol (ALP) to connect to a Sun Ray server. ALP provides some limited security features, which can be administered at the Sun Ray server level. For example, ALP can encrypt keystroke and display traffic between the desktop client and the Sun Ray server, but it does not encrypt USB device traffic.

After the desktop client is authenticated and connected to the Sun Ray server via ALP, the Sun Ray Windows connector, when used, provides access to the Windows desktop via RDP. The RDP connection can and should occur entirely within the data center.

4.4. Client Access Policy

This section describes the security considerations for client access.

4.4.1. Oracle Virtual Desktop Clients Access

Sun Ray Software enables you to specify whether the Sun Ray server should accept connections from Oracle Virtual Desktop Clients. The default access policy disallows Oracle Virtual Desktop Client
connections. To enable access for Oracle Virtual Desktop Clients, you can use the \texttt{-u} option of the \texttt{utpolicy} command or the System Policy page of the Admin GUI. See \textit{How to Enable Access for Oracle Virtual Desktop Clients} for details.

4.4.2. Client Authentication

Each Sun Ray Client or Oracle Virtual Desktop Client instance can provide a unique authentication value when connecting to a Sun Ray server. You can configure the Sun Ray server to require or not require such a value and to respond in a variety of ways if there is a conflict with the client's expected authenticator value. You can configure client authentication through the \texttt{utcrypto} and \texttt{utkeyadm} commands or the corresponding options in the Security Policy page of the Admin GUI.

New Sun Ray Clients with the factory firmware installed do not provide an authentication value. This is intended to assure that the client's authentication value is not exposed prior to its deployment at the customer site.

For detailed information about client authentication, see \textit{Client-Server Security} in the \textit{Administration Guide}.

4.5. Session Access Policy

This section describes the security considerations for session access.

4.5.1. Access Without Smart Cards

If you access a Sun Ray session without a smart card, the session is bound to that client and it cannot be hotdesked to another client. However, the non-smart card mobility (NSCM) feature makes the session mobile, which binds the session to the authenticated user name that started it and enables the user to hotdesk to another client. You can enable the NSCM feature through the \texttt{utpolicy} command or the System Policy page of the Admin GUI.

When the NSCM feature is enabled, the NSCM login greeter also provides access to an underlying stationary session through the Exit option of the Options menu. The Exit option is intended to allow users who don't have a user account on the Sun Ray server to initiate a remote X login to another server and gain access to a user account. The Exit option is enabled by default, but you can disable it by using the \texttt{-d} option of the \texttt{utpolicy} command or the System Policy page of the Admin GUI.

For detailed information about the NSCM feature, see \textit{Hotdesking} in the \textit{Administration Guide}.

4.5.2. Access Using Smart Cards

Sun Ray Software automatically provides smart card services, such as smart card authentication, through the PC/SC-lite API. Smart card services include interoperability with the integrated smart card readers on Sun Ray Clients and the client computers running Oracle Virtual Desktop Clients. External USB readers connected to Sun Ray Clients and Oracle Virtual Desktop Clients are supported through the CCID handler, which can be downloaded separately.

For details about the smart card services provided with Sun Ray Software and the CCID IFD Handler, see \textit{Smart Card Services} in the \textit{Administration Guide}.

For details about additional smart card configuration when using the Windows connector, see \textit{Smart Cards} in the \textit{Administration Guide}.

4.5.3. Authenticated Sessions

This section describes the security considerations for authenticated sessions.
User Authentication

User authentication for Sun Ray sessions is controlled by a dedicated Authentication Manager. The Authentication Manager implements site-wide access policies for identifying and authenticating users on the desktop clients. An important piece of this process includes tokens, which are authentication keys used to identify what type of session is provided to a user based on the configured policy and consequently what login scheme is presented to the user. The Authentication Manager also provides an audit trail of the actions of users who have been granted administrative privileges for Sun Ray services.

You can use the Security page of the Admin GUI to change the policy for session authentication, including what type of sessions users are presented. And, you can use the Tokens page of the Admin GUI to manage and register tokens. See Sessions Overview in the Administration Guide for details.

Sun Ray Software uses the site's existing User Directory for user identification and authentication, which is configured through the Sun Ray server's available PAM modules and Name Service Switch file (/etc/nsswitch.conf). The PAM configuration used for user authentication is based on the type of session being requested:

- When logging in to a smart card session or a non-mobile session, authentication is performed by the session's X display manager, using the PAM configuration defined for that display manager.

- When logging in to an NSCM session, authentication is performed by a pair of NSCM login greeter sessions. By default, the NSCM PAM configuration is copied from the authentication rules for the X display manager when the Sun Ray server is activated during the installation. If you modify the X display manager's PAM configuration after the Sun Ray server is installed and activated, you must also make the same modifications to the NSCM PAM configuration. The NSCM PAM configuration is located in the utgulogin ('get username' service) and the utnsclogin (authentication service) sections of the PAM configuration file.

Desktop Screen Locking

Most desktop operating systems provide their own screen locking mechanism, which the user can invoke manually or it will occur automatically after a certain period of inactivity. When a desktop screen is locked either manually or automatically, the Sun Ray session is disconnected and it requires authentication to re-access the session again.

Note

Locking an Oracle Linux desktop locks only the desktop and does not disconnect the session. If a new user needs to use a Sun Ray Client where the desktop is locked, the user must reset the client to disconnect the session and make the client available for use. For Oracle Linux desktops, using the utdetach command is recommended as an alternative to locking the screen.

When unlocking a smart card session or a non-mobile session, the PAM configuration used for user authentication depends on whether or not the Remote Hotdesk Authentication (RHA) feature is enabled (described in Section 4.5.3, “Remote Hotdesk Authentication (RHA)”).

- RHA is enabled - Authentication at the screen lock is performed by a separate RHA greeter session for greater security. By default, the RHA PAM configuration is copied from the authentication rules for the X screen lock when the Sun Ray server is activated during the installation. If you modify the X screen lock's PAM configuration after the Sun Ray server is installed and activated, you must also make the same modifications to the RHA PAM configuration. The RHA PAM configuration is located in the uthotdesk section of the PAM configuration file.

- RHA is disabled - Authentication at the screen lock is performed by the session's X display screen lock, using the PAM configuration defined for that screen lock program.
When unlocking an NSCM session, authentication is performed by a pair of NSCM login greeter sessions. By default, the NSCM PAM configuration is copied from the authentication rules for the X display manager when the Sun Ray server is activated during the installation. If you modify the X display manager's PAM configuration after the Sun Ray server is installed and activated, you must also make the same modifications to the NSCM PAM configuration. The NSCM PAM configuration is located in the `utgulogin` ('get username' service) and the `utnsclogin` (authentication service) sections of the PAM configuration file.

### Remote Hotdesk Authentication (RHA)

One of the unique aspects of Sun Ray Software is the ability to "hotdesk" from one client to another. Hotdesking, or session mobility, is the ability for a user to remove a smart card, insert it into any other client within a failover group, and have the user's session "follow" the user, enabling the user to have instantaneous access to the user's windowing environment and current applications from multiple clients.

By default, when a user hotdesks, the desktop's screen lock is activated and the user is forced to authenticate again. However, screen locks are inherently insecure in a number of ways. Remote Hotdesk Authentication (RHA) is designed to provide a more secure hotdesk environment instead of the 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 and applications cannot interfere with the authentication. From a user's perspective, there is minimal change if Remote Hotdesk Authentication is enabled.

When RHA is enabled and a reconnection is attempted, the Sun Ray Software creates a temporary new session for the client and uses that session to present an authentication login greeter to the user. This RHA greeter looks very similar to the non-smart card mobile (NSCM) login greeter. After the user successfully authenticates through the greeter, the temporary session is dismissed and the user's existing session is connected to the client.

For environments where the in-session screen lock provides acceptable security or where no hotdesk authentication is desired, you can configure Sun Ray Software to disable the RHA security feature.

RHA is enabled for smart cards by default, and non-smart card mobility (NSCM) automatically provides similar protection as RHA. Authentication does not apply to anonymous Kiosk Mode.

See [Remote Hotdesk Authentication (RHA)](#) in the Administration Guide on how to disable or enable remote hotdesk authentication for smart cards.

### 4.5.4. Unauthenticated Sessions With Kiosk Mode

By default, kiosk mode is disabled. If you enable kiosk mode, be aware that kiosk mode bypasses the system login mechanism, so 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.

### Kiosk User Accounts

All computer applications must run under some type of user account and kiosk sessions are no different. To enable real users to access applications without requiring the need to authenticate to the underlying operating system of the Sun Ray Software, kiosk mode manages a pool of local user accounts. If the kiosk service determines that an administrator has configured the system policy or the current token ID to run a kiosk session, unauthenticated access to the system is granted.
While kiosk user accounts do not correspond to a real user, their role in kiosk mode allows a real user to use the applications defined by the administrator in an unauthenticated manner. Without a kiosk user account, a kiosk session cannot run.

See Kiosk User Accounts in the Administration Guide for details, including ways to limit the impact a kiosk user can have on the system and prevent unauthenticated access from becoming uncontrolled access.

### 4.5.5. External Peripherals

Sun Ray Software provides the ability for users to access external peripherals connected to a Sun Ray Client or Oracle Virtual Desktop Client, either by using the device mapping feature with an Oracle Solaris or Oracle Linux desktop or by using the USB device redirection feature with Windows desktop sessions. Connecting external peripherals presents an inherent security risk, which may include unintended access to data. For example, when using USB device redirection with Windows Server 2003 R2 or Windows Server 2008 R2 platforms, USB devices to a Sun Ray Client client are accessible and visible to all desktops running on the Windows system.

For details about the security implications with external peripherals, see Peripherals Overview for device mapping or USB Device Redirection in the Administration Guide.

By default, access to external devices are enabled. You can disable access to external devices with the `utdevadm` command or from the Security page of the Admin GUI. For details, see Enabling and Disabling Device Services in the Administration Guide.

For additional details about accessing external peripherals connected to a client computer running Oracle Virtual Desktop Client, see the Oracle Virtual Desktop Client User's Guide.
Chapter 5. Server-to-Server Security

This chapter describes the security aspects of the interaction between servers in a failover group.

5.1. Sun Ray Data Store

The content of the Sun Ray data store is generally readable, but data store content can be modified only by a properly authenticated client of the data store. During the Sun Ray Software installation, you are prompted to specify a password for the admin user, which is created to access both the data store and the Admin GUI.

You can modify the Sun Ray data store password after installation by using the utpw command or the Data Store Password page of the Admin GUI. You must coordinate this password change on each server within the failover group.

5.2. Group Manager

The Group Manager component of the Sun Ray Authentication Manager daemon is responsible for recognizing servers as belonging to the same failover group. Failover group membership is dictated by a "group signature", which is like a password that is requested during the Sun Ray Software installation. 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.

Server-discovery requests are the only unsigned network traffic accepted by the Group Manager. All other network traffic received by the Group Manager that fails a validation test against the group signature is discarded. So, the Group Manager maintains group status and connectivity information only on the basis of reports from members of its own failover group.

You can modify the group signature after installation by using the utgroupsig command. In order to put the new group signature into effect, you must coordinate the change on each server within the failover group followed by a warm restart of all servers in the group.

5.3. Failover Group Network Service

The utrcmd network service provides a remote command execution facility that allows members of a failover group to perform group-wide administrative actions. Requests are accepted only on the basis of a demonstrated knowledge of the same group signature used by the Group Manager, and only a specific small number of commands are made available through this service.
Sun Ray Software provides a number of desktop connectors to provide Windows desktops to users, including the Windows connector.

6.1. Enhanced Windows Authentication With Windows Connector

To help secure all data being transferred to and from the Windows server when using the Windows connector, Sun Ray Software also supports the built-in RDP encryption that uses the RC4 cipher, which encrypts data of varying size with a 56-bit or a 128-bit key. Enhanced authentication options are also provided, which include TLS/SSL (with optional server verification) and Network Level Authentication (NLA) using CredSSP. For NLA, Kerberos authentication is used by default, but NT LAN Manager (NTLM) authentication is also provided.

All the available enhanced authentication options protect the Windows session from malicious users and software before a full session connection is established. See Network Security in the Administration Guide for details.

6.2. VMware View Manager Authentication

The default SSL certificate created from the VMware View Manager installation must be imported into the Sun Ray server to enable SSL connections to desktops. See How to Enable SSL Connections to the View Connection Server in the Administration Guide for details.