Sun Ray Enterprise Server Software 1.1 Product Notes

901 San Antonio Road
Palo Alto, , CA 94303-4900
USA 650 960-1300 Fax 650 969-9131

Part Number 806-4576-10
April 2000, Revision A

Please Recycle

CHAPTER 1

Sun Ray Software

The *Sun Ray Enterprise Server Software 1.1 Product Notes* provide instructions for Sun Ray™ server software, release 1.1.

Firmware Upgrades

The firmware version must be the same on all servers in the failover group that have firmware upgrade enabled.

Firmware Upgrade Procedure

▼ To Upgrade the Sun Ray Software Version for a Group

1. **Disable firmware upgrade on all members of the failover group.**

2. **Install the new software on each server in the failover group, enabling upgrade.**

   As each Sun Ray appliance connects to an upgraded server, it downloads the new firmware version once.

Installation Guide Errata

The following changes apply to the *Sun Ray Enterprise Server Software 1.1 Installation Guide* (part number 805-7916).

What Does Full Cluster Mean?

The *Sun Ray Enterprise Server Software 1.1 Installation Guide* states that a *full cluster* install of the Solaris™ 2.6 or Solaris 7 operating environment is required.

Full cluster means that either the *Entire Distribution plus OEM support* or the *Entire Distribution* software group is checked in the Select Software window during the Solaris software installation.

Administrator's Guide Errata

The following changes apply to the *Sun Ray Enterprise Server Software 1.1 Administrator's Guide* (part number 805-7915).

Chapter 1, Sun Ray System Overview

Remove the section "Sun Enterprise 10000 Server Support Provided."

Chapter 2, Sun Ray Software and Hardware Requirements

In section "Disk Space," replace Table 2-3 with the following:

TABLE 1–1 Sun Ray Server Software Disk Space Requirements

Product	Default Installation Path	Requirements

Sun Ray core software	`/`
	`/opt`
	`/var`
		1 MB
		8 MB
		1 MB + log files

LDAP client libraries	`/usr`	350 K
Sun™ Directory Services 3.1	`/opt/SUNWconn` The default location for the directory database is `/var`.	■ Requires JDK 1.1.x ■ 25 MB disk space in `/opt` ■ 2.0 MB in `/var` ■ 0.4 MB in `/etc` You must allow enough disk space for the database. 1,000 entries require roughly 1.5 MB of disk space, 64 MB of RAM, and 128 MB of swap.
Sun WebServer™ 2.1	`/usr`	■ Software—9.5 MB and 2 MB disk space for documents and log files. ■ Memory—64 MB minimum, 96 MB is recommended.
JRE 1.2.1	`/opt`	26.5 MB

Chapter 3, Configuring the Software

In the procedure “To Run the Configuration Script,” Steps 7 through 9 should be replaced with the following:

7. Answer the failover group prompt.

```
# Configure this server for a failover group (y/[n])
```

8. Answer the prompt for `groupSignature`.

If you are in a group environment then the `groupSignature` must be the same for all group members. A group of 1 is valid. This prevents unintended results when additional browsers are brought online.

9. After the script has completed, check in `/var/tmp/utconfig.`<*date-format*>`.log` to see if there were any errors.

10. Once completed successfully, see “Testing the Installation and Configuration” on page 47.

Chapter 4, SSL Certificate Configuration

Secure Sockets Layer

Substitute the following table for Table 4-2 in the guide:

TABLE 1–2 Required Information

Information	example	Comment
RootCA user	*rcauser*	Existing user, or new one.
RootCA directory	*/var/certs*	
RootCA Distinguished Name	`cn=`*rcauser*`,o=`*fun*`,c=`*we*	Simplified for table.
RootCA password	*rcapass*	Requested to enable login as the RootCA user.
Sun Ray server root password	*rootpass*	Root password of Sun Ray server.
Web server domain name	*eng.fun.com*	
*Web server IP address	*192.144.31.118*	
*Web server Distinguished Name	`ou=`*eng*`,o=`*fun*`,l=`*lapland*`,st=`*bliss*`,c=`*we*	Every attribute except the common name. Simplified for table.
*Web server certificate directory	*/var/certs/ 192.144.31.118*	Directory is the IP address of the web server.
*Key package password	*keypass*	Requested to create the RootCA credentials.

TABLE 1–2 Required Information *(continued)*

Information	example	Comment
*Encryption password	*encpass*	Requested when configuring the web server's certificate.

* Additional values must be provided for each failover Sun Ray server.

Configuring SSL on the Primary Sun Ray Server

Replace Steps 4 through 7 of the procedure "To Configure SSL on the Primary Sun Ray Server" with the following:

4. Become the RootCA user and run the `crca` script to create the RootCA credentials:

```
# su rcauser
$ /usr/bin/crca
```

The `crca` script asks for the following:

- RootCA distinguished name (cn=*rcauser*,o=*fun*,st=*bliss*,c=*we*)
- RootCA directory (*/var/certs*)
- Key package password (*keypass*)
- Key package password again (*keypass*)
- To store the credentials in the name server (`y`)
- Sun Ray server root password (*rootpass*)

5. Create the web server certificate directory and set permissions and ownership:

```
$ mkdir /var/certs/192.144.31.118
$ chmod 700 /var/certs/192.144.31.118
$ chown rcauser /var/certs/192.144.31.118
```

6. Run the `sslgencrd` script to generate the web server certificate:

```
$ /usr/http/bin/sslgencrd -r rcauser -d /var/certs/192.144.31.118 -i 192.144.31.118
```

The `sslgencrd` script asks for the following:

- Web server (`httpd`) host name (press Return)
- Web server domain name (*eng.fun.com*)
- Web server DN without common name (ou=*eng*,o=*fun*,l=*laffland*,st=*bliss*,c=*we*)
- Encryption password (*encpass*)
- Encryption password again (*encpass*)
- Key package password (*keypass*)

7. Install the web server certificate as superuser:

```
$ exit
# /usr/http/bin/sslstore -i 192.144.31.118 -p /var/certs/192.144.31.118 0
```

Note - In the above command, the last character is a zero.

The `sslstore` script requests the encryption password:

```
/usr/bin/skilogin; Enter host key package password: encpass
```

Note - Type the encryption password, *encpass*, not the key package password.

Troubleshooting SSL Configuration

The procedure “To Remove All SSL Information” does not remove all SSL information. The following procedure removes files to enable reconfiguration.

▼ To Remove SSL Database

1. **Log in or use the `rlogin` command to become superuser on the Sun Ray server.**
2. **Stop both the `cryptorand` server and the `skiserv` server:**

```
# /etc/init.d/cryptorand stop
# /etc/init.d/skiserv stop
```

3. **Remove the Federated Naming Service directory:**

```
# rm -rf /var/fn
```

4. **Change to the RootCA directory:**

```
# cd /var/certs
```

5. **Remove the web server certificate directory, files, and subdirectories from the RootCA directory:**

```
# rm -rf new_cred_list keypkgs certs 192.144.31.118
```

6. **Start both the** `cryptorand` **server and the** `skiserv` **server:**

```
# /etc/init.d/cryptorand start
# /etc/init.d/skiserv start
```

Reconfigure SSL according to "Configuring SSL on the Primary Sun Ray Server" on page 56 of this document, starting with Step 4.

Note - You do not need to create the RootCA user again.

Accessing the Sun Ray Server Through SSL

The following information was omitted from Chapter 4 of the *Sun Ray Enterprise Server Software 1.1 Administrator's Guide*:

After configuring the Sun Ray server with an SSL certificate and enabling SSL, type the following URL to access the administration application:

`https://`*servername*`:`*port*

Where *servername*:*port* is the host name and port of the Sun Ray web server. By default, the port is 1660.

Chapter 6, Administering the Sun Ray System

Replace the step in the procedure “To Restart the Session Manager” with the following:

1. **If the Session Manager exits and does not automatically restart, stop and start the `utsvc` daemons by typing:**

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

Chapter 8, Managing Sun Ray 1 Appliances

In the section “Interpreting Failover Group Status Information,” replace the second paragraph with the following:

For example, in Figure 8-9 there is one public network and two Sun Ray interconnect fabrics. Sunray5 (a) has the potential for failover for all of the Sun Ray appliances that reside on the 192.168.128.0 network. On the 192.168.140.0 network (e) the network appliances are not intended for failover and considered completely private to Sunray5 (a).

In the section “Interpreting Failover Group Status Information,” replace the fourth paragraph with the following:

The network/netmask headings (xxx.xxx.xxx.x/24) refer to all of the networks that are observed. Group membership is represented by the group icon. Other Sun Ray servers visible on the screen may also be members of another group. You can see that information by selecting a different server which refreshes the broadcasted information and reveals other groups. Multiple groups can use same network IDs for their private interconnect fabrics. For example, the group Sunray5 and Sunray11 are using a specific network. The connection only exists between those two servers.

In the section “Example Configurations,” replace the second item in the legend with the following:

2. Private network (192.168.128.0)

Viewing System Status

In the section “Viewing System Status,” the Status Summary frame has been redesigned Status Summary as shown in Figure 1–1. The frame layout has changed in order to enhance usability.

Note - The Policy field, showing which policy is currently is in use, has been removed from the Summary Status frame.

To view group and local policies, go to the Admin->Policy screen and click the associated radio button to view the policy.

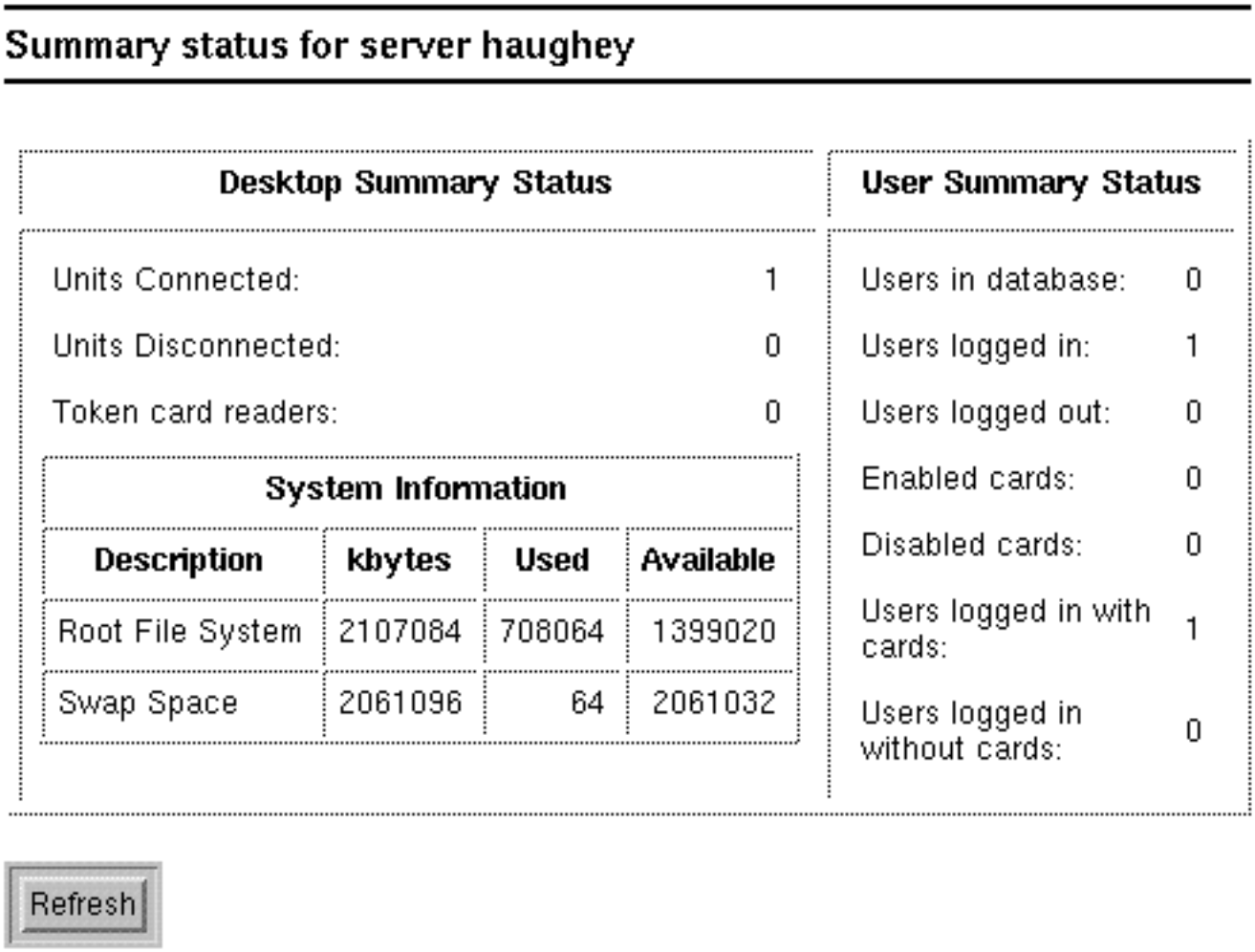

Figure 1–1 Redesigned Status Summary Frame

Replace Table 8-2 with the following:

TABLE 1–3 System Status Frame Field Descriptions

Options	Description
DeskTop Summary Status	
Units attached	Total number of Sun Ray 1 appliances attached to the interconnect fabric.
Units logged in	Total number of Sun Ray 1 appliances logged into of the Sun Ray server.
Units logged out	Total number of Sun Ray 1 appliances logged off of the.Sun Ray server.
Token card readers	Total number of Sun Ray 1 appliances designated as token card readers attached to the interconnect fabric.
User Summary Status	
Users in database	Total number of users in the LDAP database.
Users logged in	Total number of users logged in to the system.
Users logged out	Total number of users who have logged off in a specified time frame.
Inactive sessions	Total number of inactive sessions.
Enabled cards	Total number of enabled smart cards.
Disabled cards	Total number of disable smart cards.
Users logged in with cards	Total number of users logged in with smart cards.
Users logged in without cards	Total number of users logged in not using smart cards.
System Information	
Root File System	Total, used and available disk space available for the Sun Ray server.
Swap Space	Total, used and available swap space available for the Sun Ray server.
Memory	Total, used and available memory available for the Sun Ray server.

View Current Desktop Frame

In the section, Listing Currently Connected Desktops," the View Current Desktop frame has been modified. It now contains a server column as shown in Figure 1–2.

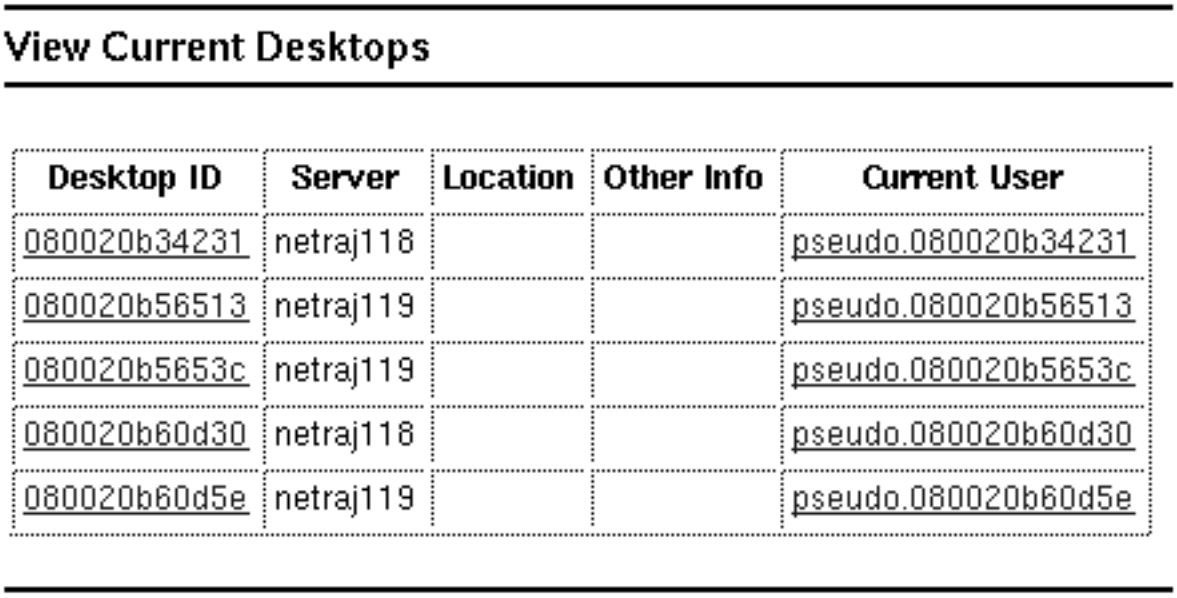

Figure 1–2 Redesigned View Current Desktops Frame

Examining Log Files

In the section "Examining Log Files," the string `""The date last modified:" $date "` has been removed from the log files in the web-based administration software. Disregard this line in Figures 8-11 through 8-14.

Chapter 10, Removing the Sun Ray Software

In the procedure, To Unconfigure the Sun Ray Server Software, the output screen in Step 8 contains the CGI username incorrectly entered as `utadmin`. The default CGI username is *www*.

Replace the output screen in Step 8 with the following one:

```
Enter UT admin web server instance name [utadmin]:

Delete CGI username account ([y]/n)y
```

(continued)

(Continuation)

```
# Enter CGI username [www)]: www

About to un-configure the following software products:

Sun Directory Services 3.1
Sun Web Server 2.1
Sun Ray enterprise server 1.1

Continue ([y]/n)y
```

Unconfiguring the Sun Ray Server Software

In the procedure “To Unconfigure the Sun Ray Server Software,” replace Step 9 with the following:

9. After the script has completed, check in `/var/tmp/utconfig.`<*date-format*>`.log` to see if there were any errors where <*date-format*> is in the format *year_month_day_hour:min:sec*.

Uninstalling the Sun Ray Software

In the procedure “To Uninstall the Sun Ray Software,” replace Step 4 with the following:

4. After the script has completed, check in `/var/tmp/utinstall.`<*date-format*>`.log` to see if there were any errors where <*date-format*> is in the format *year_month_day_hour:min:sec*.

Appendix A, Troubleshooting

In the section “Server Questions,” the answer to the question below should be replaced with the following:

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

A: The Sun Ray server has exhausted the number of pseudo terminals defined. If a system does not have enough pseudo terminals defined, users can not bring up a shell window and will not be able to login. For example, a network consists of 50 Sun Ray 1 appliances and the `pty` entry is set to 40. When the 41st user tries to open

a shell window, this error message displays. As `root`, edit the `/etc/systems` file `pt_cnt` value to increase the number of available pseudo terminals.

```
# vi /etc/systems
```

For 50 users, change the `pt_cnt` entry to five times the number of users:

```
set pt_cnt=250
```

Note - You must reboot.

For additional information see “Setting System Parameters on page 62.

Appendix C, The Green Newt Cursor

Appendix C, The Green Newt Cursor, contains an incorrect reference to the *Sun Ray Enterprise Server Software 1.0 Administrator's Guide* and *Installation Guide*. These references should refer to the Sun Ray Enterprise Server Software 1.1 release.

Removing Log Files

The Administration application log files can grow to an unmanageable size in three distinct locations—`authmgr`, Sun WebServer, and `adminlog`. Periodically removing log files from these areas is necessary.

Note - Logging to messages files and to the `admin_log` file does not commence until after the interface is configured; that is, after the `utadm -a` <*interface*> command is run.

Administration and Authentication Logs

Both the administration and authentication manager log files are located in `/var/opt/SUNWut/log`.

These message files use the following syntax:

- `admin_log`
- `admin_log.`<*n*> where <‘*n*’> is a number => 1
- `auth_log`

- `auth_log.`<*n*> where <‘*n*’> is a number => 1

Caution - Never delete the currently active log file (either `admin_log` or `auth_log`). Use the `rm` command to delete the other log files.

A messages file used by all the administration tools and Sun Ray services is archived daily. This message file uses the following syntax:

- `messages`
- `messages.`<*n*> where <‘*n*’> is a number => 1

You can remove these log files using the `rm` command.

Sun WebServer Log Files

The Sun WebServer log files are located in `/var/http/instance_name/websites/default_site/logs.` The `instance_name` variable is the name of the web server instance supplied to `utconfig.` The default name is `utadmin`.

The SWS log files use the following syntax:

- `http_log_clf`
- `http_log_clf.`<*n*> where <‘*n*’> is a number => 1

The Sun WebServer maintains a symbolic link (`http_log_clf`) to the active Sun WebServer log file. The symbolic link is also linked to one of the other `http_log_clf.x` files. You should not delete the symbolic link or the log file the symbolic link points to or logging may be disrupted.

The `utglpolicy` Command

The `utglpolicy` command is used to get or set the global `utpolicy` options. Normally, setting global policies is done using the Sun Ray administration tool.

The `utglpolicy` command syntax has changed and is now identical to the command syntax for `utpolicy` with the exception of the `-i {clear|soft}` and the `-t list` policy options, which are not supported by `utglpolicy`.

Note - Do not use the `-i {clear|soft}` and the `-t list` options in `utglpolicy`.

SYNOPSIS:	`/opt/SUNWut/sbin/utglpolicy` [*utpolicy-options*]
DESCRIPTION:	`utglpolicy` with no options gets the global `utpolicy` options.
	`utglpolicy` [*utpolicy-options*] provides a command line alternative for the administrator to set a valid global `utpolicy` options in the database.
EXAMPLE:	To set a global policy:

```
# /opt/SUNWut/sbin/utglpolicy -a -r card -z pseudo -t clear -t add:080020a8e723
```

Previously, `utglpolicy` required a `-g` (get) or `-s` (set) option with the *utpolicy-options* in quotes.

Note - Do not use the old syntax.

The `utpolicy` Command

The `utpolicy` command is used to configure multiple terminal readers. For example, assume an environment has four token readers and you execute `utpolicy` for a second time and do not use the `-t` option. You may intend to only change the card, but, once the policy is invoked, the terminal readers disappear. To correct this, execute another invocation of your chosen policy using the `-t` option. This causes the appropriate readers to appear.

The Zero Administration Policy

In the Sun Ray Enterprise Server Software 1.1, the Zero Administration policy assumes that all servers are part of a default group that includes the `-g` option, which allows automatic session selection. In effect, if servers are physically connected over the Sun Ray Interconnect fabric, they are part of a failover group.

Local Policies for Group Configurations (After Using `utconfig`)

In this scenario, you have issued `utconfig` and you have chosen to be a group-of-one. Later, you choose to become a member of a larger group on the primary failover server. You choose not to execute `utconfig` for a second time. For a group environment, execute `utconfig` and select group environment when

prompted. Next, use `utreplica` on the primary server and perform the same steps on the secondary. For more information on how to use the `utreplica` command, refer to the section “Using the `utreplica` Command” on page 23 of this document and Chapter 2 in the *Sun Ray Enterprise Server Software 1.1 Advanced Administrator’s Guide*. When you select group, you are prompted to set a group signature. After a group is established, you can preserve the database. Refer to the steps below.

▼ To Preserve the Current Database (Primary Failover Server)

Select this procedure if you are changing from an administered non-group environment to a group environment and want to preserve the database. If you do not want to preserve the database, refer to “To Remove the Current Database (Primary Failover Server)” on page 19 below. You must also manually change the signature, change the local policy, and execute `utreplica`. The `utreplica` command automatically restarts the Authentication Manager.

1. **Use `utgroupsig` to set the failover signature.**

2. **Modify the `auth.props` file entry (*useLocalPolicy*=) to a value of false.**

```
useLocalPolicy=false
```

Note - You must execute this command to preserve the database.

3. **Run the `utreplica` command for the primary and other group members (for example, group1, group2, and so on).**

▼ To Remove the Current Database (Primary Failover Server)

Select this procedure if you do not want to preserve the database. Essentially, this procedure removes the existing configuration.

1. **Remove the existing configuration.**

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

2. **Run** `utconfig`**.**

3. **Answer Y to the group prompt.**

4. **Provide a group signature name.**
   Record this name for later use with all secondary failover servers.

Note - Any `groupSignature` names must be identical for both the primary and secondary failover servers.

---

5. **Run** `utreplica -p` **or** `-s`**.**

`utgstatus` Command

Since the publication of the *Sun Ray Enterprise Server Software 1.1 Administrator's Guide*, the `utgstatus` command has been added.

The `utgstatus` command allows the user to view the failover group status information for the local server or for a named server. If you issue the command with no arguments, local server information is displayed; if you issue the command with arguments, information for the named server is displayed. An example of the command syntax is shown below. The `-s` argument is used for nonlocal servers. For additional information, refer to the `utgstatus` man page.

```
# /opt/SUNWut/sbin/utgstatus   [-s <server_name>]
```

Note - The label (T) following a server name, viewed in the output from the `utgstatus` command, designates the server as a "trusted" member of a failover group.

Advanced Administrator's Guide Errata

The following changes apply to the *Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide* (part number 805-4181-10).

Chapter 2, Failover

Setting Up Class C Addresses

The note in this section incorrectly states that 256 Class C addresses are available. The correct number of addresses is 254. Zero (0) is network address and 255 is the broadcast address.

Under the section “Client Addresses,” replace the first two sentences of the fourth paragraph with the following:

When a Sun Ray appliance resets, it sends a DHCP broadcast request on its network interface. Each DHCP server on the network receives the broadcast and responds with an IP address allocated from its non-overlapping range of addresses described above.

Group Manager Configuration Section

In paragraph 1 in “Group Manager Configuration,” the `gmSignatureFile` entry is not commented out in the `auth.props` file. If it is commented out, no signature file is configured. Uncomment the line (in the quoted box). A corrected line entry is shown below:

```
gmSignatureFile = /etc/opt/SUNWut/gmSignature
```

Multicasting

Multicasting should be turned on in the switches to enable failover functionality. If multicasting is enabled, the multicast address specified in the `multicastAddress` property of `/etc/opt/SUNWut/auth.props` is used to communicate with other servers in the failover group.

If multicasting is not available in the switches, then the `enableMulticast` property of `/etc/opt/SUNWut/auth.props` should be set to `false`.

These settings control group maintenance messages on the Sun Ray interconnect interfaces as well as the LAN interface. All members of the group must be configured the same way for the failover functionality to be operational.

Setting Up a Trusted Group

Replace the note on selecting passwords at the bottom of the page in this section with the following note:

Note - For additional security, use long passwords and signatures of at least eight characters—two or more alphabetic and one or more non-alphabetic.

Coexistence With Clustering

There is currently no relationship between the Sun Ray enterprise server software 1.1 and the Sun Cluster 2.2 software environment. They should be able to coexist on the same servers, but this is not a verified configuration.

LDAP Replication Defined

The online SunDS documentation contains some further background reading on the LDAP replication mechanism utilized in Sun Directory Services 3.1.

HTML online documents can be found on the server on which you installed `SUNWconn` at the following location:

`/opt/SUNWconn/ldap/docs/locale/C/help/admin`

The specific HTML document giving the most comprehensive explanation of LDAP replication is:

<*servername*>`:/opt/SUNWconn/ldap/docs/locale/C/help/admin/datasstext.html`

Group/LDAP Password

Once a group password is established within a failover group, any change to the password locally replicates the new password to all the databases. The password in the database is then out of synchronization with the local password on each server.

To bring the utilities and the Authentication Manager back into synchronization with the database, you must change the password on each individual server that is part of the failover group.

To change the password initially, use the administration GUI or `utpw` on the command line. Subsequent changes to the password on the other servers in the group must be made using the command line interface.

▼ To Change the Local Password

1. **Manually log in to each group server and type:**

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

You are prompted for the new password.

Note - You must restart services after changing the password.

▼ To Restart Services

1. Type:

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

Using the `utreplica` Command

The `utreplica` command is a configuration utility that enables you to manage and configure a group of servers. This command works in conjunction with the `utconfig` command. The `utreplica` command performs configuration of the Sun Ray LDAP server to enable replication of administered data from a designated primary server to each secondary server in a failover group. The command syntax depends on whether you are configuring the primary server or a secondary server for administered group membership.

The `utreplica` command syntax has changed since the *Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide* was published. The new syntax is shown below:

```
# /opt/SUNWut/sbin/utreplica -p secondary-server [secondary-server]...
```

Use this command only on Sun Ray servers that have been configured for administration by the `utconfig` command.

Note - The `utreplica` command must be run on the primary server first and then on each secondary server.

Note - To add an additional secondary server, you must perform `utreplica -u` and reconfigure your primary and secondary servers. If you try to add a secondary server without doing this, the server will not be added and you will not receive an error message.

Note - For this command to work, all servers in the group must be configured with the same group manager signature.

For additional information on the `utreplica` command and its options, refer to the `utreplica` man page.

`utreplica` Password

The `utreplica` command no longer requires `@(UTPASSWD)` when configuring a server for failover.

Primary Failover Servers and Setting Local Policies

A primary server cannot have `useLocalPolicy=true.` Essentially, this is an override in the `auth.props` file (in expert mode). It is possible to run a server within a group that will not adhere to group policies. This situation could be a security issue, and, in addition, Sun is restricting its use to secondary and not primary servers. If you do make this change, the global administration tools on primary servers may not work across the group. The policy you receive may not be the policy you intended; rather, it is a result of interaction between the tool and utility.

Note - The LDAP and failover domains should be the same.

Note - Configuring and modifying policies should be conducted on primary failover servers, not the secondaries.

The `utreplica` command sets or defines the LDAP domain. Use `utgroupsig` to configure the failover domain.

Known Problems

The following section documents existing problems and known solutions (workarounds).

Sun Ray Enterprise Servers and `bootp`

Some external software that configures bootp and DHCP services may interfere with the proper functioning of the Sun Ray enterprise server software. Refer to the *Sun Ray Enterprise Server Software 1.1 Administrator's Guide.*

In most situations, the `bootp` daemon is not needed. In the case where only standard `bootp` services are required, try the following workaround.

Workaround: Edit the `/etc/init.d/dhcp` file and add the `-b` option to the `DHCPOPTIONS` line. For more information, see the `dhcpconfig` and `in.dhcpd` man pages.

In the situation where more than standard `bootp` is needed, you may have to remove the external software.

Workaround: Remove the offending service from the Sun Ray server.