Sun Secure Global Desktop 4.31 Installation Guide

Sun Microsystems, Inc.
www.sun.com

Part No. 820-1087
May 2007, Revision 01

Please
Recycle

Contents

Preface

The *Sun Secure Global Desktop 4.31 Installation Guide* provides instructions for installing, upgrading, and removing Sun Secure Global Desktop Software. This document is written for system administrators.

Using UNIX Commands

This document might not contain information on basic UNIX® commands and procedures such as shutting down the system, booting the system, and configuring devices. Refer to your system documentation for this information. This document does, however, contain information about specific Secure Global Desktop commands.

Shell Prompts

Shell	Prompt
C shell	*machine-name*%
C shell superuser	*machine-name*#
Bourne shell and Korn shell	$
Bourne shell and Korn shell superuser	#

Typographic Conventions

Typeface*	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your .login file. Use ls -a to list all files. % You have mail.
AaBbCc123	What you type, when contrasted with on-screen computer output	% **su** Password:
AaBbCc123	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the *User's Guide*. These are called *class* options. To delete a file, type **rm** *filename*.

* **The settings on your browser might differ from these settings.**

Related Documentation

The documents listed as online are available at:

`http://www.sun.com/documentation`

Application	Title	Part Number	Format	Location
Release Notes	*Sun Secure Global Desktop Software 4.31 Release Notes*	820-1086-10	HTML PDF	Online Software CD and online
Administration	*Sun Secure Global Desktop Software 4.31 Administration Guide*	801-1088-10	HTML	Online

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Sun at:

docfeedback@sun.com

Please include the following document title and part number in the subject line of your email:

Sun Secure Global Desktop 4.31 Installation Guide, part number 820-1087.

CHAPTER 1

Preparing to Install

This chapter describes the things you must know and do before you install Sun Secure Global Desktop Software (SGD).

Topics in this chapter include:

Release Notes

Before installing SGD, read the *Sun Secure Global Desktop Software 4.31 Release Notes*. The release notes contain important information about this version of SGD, including the following:

- Hardware requirements.
- Supported installation platforms.
- Operating system modifications. If you do not make the required modifications, SGD might not install.
- Known issues and bugs with installation.

Secure Global Desktop Web Server

When you install SGD, you install the Secure Global Desktop Web Server. The SGD Web Server is an Apache web server that is pre-configured for use with SGD.

When you install SGD, the SGD installation program asks you for the TCP port on which the SGD Web Server listens for HTTP connections. This is usually TCP port 80. If another process is listening on that port, the installation program asks you to choose another port.

Required Users and Privileges

To install SGD, you must have superuser (root) privileges.

The system must have `ttaserv` and a `ttasys` users and a `ttaserv` group before you can install SGD.

The `ttasys` user owns all the files and processes used by the SGD server. The `ttaserv` user owns all the files and processes used by the SGD Web Server.

The SGD server does not require superuser (root) privileges to run. The SGD server starts as the root user and then downgrades to the `ttasys` user.

If you try to install the software without these users and group in place, the installation program stops without making any changes to the system and tells you what you need to do.

Following are the requirements:

- The user names must be `ttaserv` and `ttasys`.
- The group name must be `ttaserv`.
- You can use any user identification number (UID) or group ID (GID) you want. The UID and GID can be different.
- Both users must have `ttaserv` as their primary group.
- Both users must have a valid shell, for example `/bin/sh`.
- Both users must have a home directory.
- For security, lock these accounts, for example with the `passwd -l` command.

One way to create these users is with the `useradd` and `groupadd` commands, for example:

```
# groupadd ttserv
# useradd -g ttaserv -s /bin/sh -d /home/ttasys ttasys
# useradd -g ttaserv -s /bin/sh -d /home/ttaserv ttaserv
# passwd -l ttasys
# passwd -l ttaserv
```

Application Connection Methods

To run applications, SGD must be able to connect to the application server that hosts the application. Typically this is done using either Telnet or Secure Shell (SSH). Enable one of these services before installing the SGD. SSH is the best for security.

If you are using SSH, you must enable X11 forwarding. You can do this either in your SSH configuration or by configuring the application in SGD. The *Sun Secure Global Desktop Software 4.31 Administration Guide* has details on using SSH with SGD.

Port Requirements

The *Sun Secure Global Desktop Software 4.31 Administration Guide* has detailed information about all the ports used by SGD and how to use SGD with firewalls. The following information lists the common ports used.

Client devices must be able to make TCP/IP connections to SGD on the following TCP ports:

- **80** - For HTTP connections between client devices and the SGD Web Server. The port number can vary depending on the port selected on installation.
- **443** - For HTTPS connections between client devices and the SGD Web Server.
- **3144** - For standard (unencrypted) connections between client devices and SGD.
- **5307** - For secure (SSL-based) connections between client devices and SGD.

Note – The initial connection between a client device and SGD is *always* secure. After the user logs in to SGD, the connection is downgraded to a standard connection. When you first install SGD, TCP ports 3144 and 5307 must be open to connect to SGD. You can configure SGD to always use secure connections.

To run applications, SGD must be able to make TCP/IP connections to application servers. The types of applications determine which TCP ports must be open, for example:

- **22** - For X and character applications using SSH
- **23** - For Windows, X, and character applications using Telnet
- **3389** - For Windows applications using Windows Terminal Services
- **6010** and above - For X applications

CHAPTER 2

Installing Sun Secure Global Desktop Software

This chapter describes how to install SGD.

If you are upgrading, read the upgrade instructions in Chapter 3 *before* installing the software.

SGD contains several installable components:

- The component installed on *hosts* provides the main functionality of SGD.
- The component installed on *application servers*, called an SGD Enhancement Module, provides additional functionality for SGD, for example to enable users to access the drives on their client device.
- The component installed on *client devices* enables users to connect to an SGD server.

Topics in this chapter include the following:

Installing Secure Global Desktop

On Solaris™ Operating System (Solaris OS) platforms, install SGD with the `pkgadd` command.

On Linux platforms, install SGD with the `rpm` command.

By default, SGD is installed in the `/opt/tarantella` directory. On Solaris OS platforms, the installation program asks you for the installation directory when you install the software. On Linux platforms, you can choose a different installation directory by using the `--prefix` option with the `rpm` command when you install the software.

Once you install SGD, the SGD server and the SGD Web Server are running.

▼ How To Install Secure Global Desktop

1. **Obtain the software.**

   Download the software from `http://www.sun.com` or copy it from the CD-ROM.

   Save the software to a temporary directory on the host.

   These are the package files:

   - `tta-`*version*`.sol-x86.pkg` for Solaris OS on x86 platforms
   - `tta-`*version*`.sol-sparc.pkg` for Solaris OS on SPARC® technology platforms
   - `tta-`*version*`.i386.rpm` on Linux platforms

2. **Log in as superuser (root) on the host.**

3. **Install Secure Global Desktop.**

   If the package file is compressed, you must expand it before installing.

   To install on Solaris OS on x86 platforms:

```
# pkgadd -d /tempdir/tta-version.sol-x86.pkg
```

   To install on Solaris OS on SPARC technology platforms:

```
# pkgadd -d /tempdir/tta-version.sol.sparc.pkg
```

Note – On Solaris OS platforms, if the installation fails with a `pwd: cannot determine current directory!` error message, change to the `/tmp` directory and try again.

   To install on Linux platforms:

```
# rpm -Uvh /tempdir/tta-version.i386.rpm
```

4. **Verify that the SGD package is registered in the package database.**

   On Solaris OS platforms:

```
# pkginfo | grep -i tta
```

   On Linux platforms:

```
# rpm -qa | grep -i tta
```

5. **Start the SGD server.**

```
# /install-dir/bin/tarantella start
```

   The first time you start the SGD server, the SGD Setup program runs. This program does the following:

   - Asks you to agree to the Software License Agreement.
   - Presents a list of recommended settings that you can accept or change. If a web server is currently running on TCP port 80, SGD Setup asks you which TCP port to use for the SGD Web Server.
   - Installs and configures the software. This includes creating an organizational hierarchy with some sample applications, and making the UNIX or Linux system `root` user an SGD Administrator.
   - Adds a file to the system startup directory to ensure that the SGD server and the SGD Web Server start when the system reboots. For example, if you install the software in run level 3, the file is in the `/etc/rc3.d` directory and named `*sun.com-sgd-base`.
   - Modifies root's `crontab` to archive the SGD log files weekly.
   - On Linux platforms only, adds a SGD PAM configuration file, `/etc/pam.d/tarantella`. This is copied from the existing `/etc/pam.d/passwd` file. If this file does not exist, the PAM configuration file is not created.

Installing the SGD Enhancement Module for Microsoft Windows

The SGD Enhancement Module for Microsoft Windows contains modules for advanced load balancing, client drive mapping, and seamless windows. When you install the Enhancement Module, you can choose which of these modules to install.

By default, the Enhancement Module is installed in the `C:\Program Files\Tarantella\Enhancement Module` directory, but the installation program asks you for the installation directory.

After installation, the load balancing service is running. The load balancing service starts automatically whenever the Windows host is rebooted.

▼ How to Install the SGD Enhancement Module for Microsoft Windows

1. **Log in to the Windows host as a user with administrator privileges.**
2. **Save the Enhancement Module installation program to a temporary directory on the host.**

   If you are installing from the CD-ROM, the installation program is in the `EnhancementModules` directory.

   Alternatively, download the installation program from an SGD Web Server from `http://server.example.com`. When the SGD Web Server Welcome page displays, click Install a Sun Secure Global Desktop Enhancement Module.

   The SGD Enhancement Module installation program is `temwin32.exe`.
3. **Install the SGD Enhancement Module.**

   Double-click `temwin32.exe` and follow the instructions on the screen.

Installing the SGD Enhancement Module for UNIX/Linux

The SGD Enhancement Module for UNIX/Linux contains modules for advanced load balancing, client drive mapping and UNIX audio.

The UNIX audio module of the Enhancement Module is optional and is not installed by default. If you choose to install the UNIX audio module, the SGD audio driver is installed in the kernel of the operating system.

On Solaris OS platforms, the UNIX audio module can be installed only in the global zone.

On Linux platforms, the UNIX audio module can be installed only if your kernel version is 2.4.20 or later. The SGD audio driver is compiled before it is installed in the kernel. To compile the audio driver, the following must be available on the host:

- Header files for your Linux kernel version
- GNU Compiler Collection (GCC)
- `make` utility
- `soundcore` kernel module

On Solaris OS platforms, install the Enhancement Module with the `pkgadd` command.

On Linux platforms, install the Enhancement Module with the `rpm` command.

On Solaris OS and Linux platforms, the Enhancement Module is installed in the `/opt/tta_tem` directory by default. On Solaris OS platforms, the installation program asks you for the installation directory when you install the software. On Linux platforms, you can choose a different installation directory by using the `--prefix` option with the `rpm` command when you install the software.

After installation, the advanced load balancing and UNIX audio (if selected) modules are running. The client drive mapping module is not running because this requires additional configuration which is described in the *Sun Secure Global Desktop Software 4.31 Administration Guide*.

The Enhancement Module installation program adds a file to the system startup directory to ensure that the Enhancement Module starts when the system reboots. For example, if you install the software in run level 3, the file is in the `/etc/rc3.d` directory and named `*sun.com-sgd-em`.

▼ How To Install the SGD Enhancement Module for UNIX/Linux

1. **Save the SGD Enhancement Module to a temporary directory on the host.**

   If you are installing from the CD-ROM, the package is in the `EnhancementModules` directory.

   Alternatively, download the package from an SGD Web Server from `http://server.example.com`. When the SGD Web Server Welcome page displays, click Install a Sun Secure Global Desktop Enhancement Module.

   These are the package files:

   - `tem-`*version*`.sol-x86.pkg` for Solaris OS on x86 platforms
   - `tem-`*version*`.sol-sparc.pkg` for Solaris OS on SPARC technology platforms
   - `tem-`*version*`.i386.rpm` on Linux platforms

2. **Log in as superuser (root) on the host.**

3. **Install the SGD Enhancement Module**

   If the package file is compressed, you must expand it before installing.

   To install on Solaris OS on x86 platforms:

```
# pkgadd -d /tempdir/tem-version.sol-x86.pkg
```

   To install on Solaris OS on SPARC technology platforms:

```
# pkgadd -d /tempdir/tem-version.sol-sparc.pkg
```

   To install on Linux platforms:

```
# rpm -Uvh tem-version.i386.rpm
```

   When you install, the Enhancement Module installation program presents the following settings that you can accept or change:

   - The installation directory (Solaris OS platforms only).
   - The amount of virtual memory the host has. This is used for load balancing.
   - Whether to install the UNIX audio module.

4. **Verify that the Enhancement Module package is registered in the package database.**

   On Solaris OS platforms:

```
# pkginfo | grep -i tem
```

   On Linux platforms:

```
# rpm -qa | grep -i tem
```

Troubleshooting Installing the UNIX Audio Module on Linux Platforms

On Linux platforms, if the UNIX audio module does not install, the SGD Enhancement Module installation program asks you whether to cancel the installation or to continue the installation without installing the UNIX audio module. If the UNIX platform module does not install, check the following:

- Is the Linux kernel version 2.4.20 or later?
- Are the header files for your Linux kernel version installed?

- Do the version numbers of the header files and the Linux kernel match?
- Does the GCC version match the version used to compile the Linux kernel?
- Does the `dmesg` utility reveal any other errors?

Installing the SGD Client

The SGD Client is usually installed automatically when a user connects to an SGD server using a web browser with Java technology enabled. Follow these instructions only if you want to *manually* install the SGD Client.

You do not need superuser (root) or administrator privileges to install the SGD Client.

On Microsoft Windows platforms, the SGD Client is installed in the `C:\Program Files\Sun\Secure Global Desktop Client` directory by default, but you can choose a different installation directory when you install the software. A shortcut for the SGD Client is added to the Windows Start Menu.

On UNIX and Linux platforms, the SGD Client is installed in the `$HOME/bin` directory by default, but you can choose a different installation directory when you install the software.

▼ How to Install the SGD Client Manually on Microsoft Windows Platforms

1. **In a web browser, go to an SGD Web Server.**

   For example, `http://server.example.com`.

   The SGD Web Server Welcome page displays.

2. **(Optional) Select your preferred language.**

   Click one of the flags at the top of the Welcome page.

   The Welcome page displays in the selected language.

3. **Click Install the Sun Secure Global Desktop Client.**

   The Sun Secure Global Desktop Client page displays.

4. **Download the SGD Client installation program.**
   Click Download the Secure Global Desktop Client for Microsoft Windows.
   Save the installation program to a temporary directory on the PC.
   The SGD Client installation program is `sgdcwin-`*lang*`.exe`.
5. **Change to the temporary directory and install the SGD Client.**
   Double-click `sgdcwin-`*lang*`.exe` and follow the instructions on the screen.

▼ How to Install the SGD Client Manually on Solaris OS and Linux Platforms

1. **In a web browser, go to an SGD Web Server.**
   For example, `http://server.example.com`
   The SGD Web Server Welcome page displays.
2. **(Optional) Select your preferred language.**
   Click one of the flags at the top of the Welcome page.
   The Welcome page displays in the selected language.
3. **Click Install the Sun Secure Global Desktop Client.**
   The Sun Secure Global Desktop Client page displays.
4. **Download the SGD Client tar file.**
   Click Download the Secure Global Desktop Client for *platform*.
   Save the tar file to a temporary directory on the host.
   Tar file names indicate a platform, as follows:
   - `sgdci3so.tar` for Solaris OS on x86 platforms
   - `sgdcspso.tar` for Solaris OS on SPARC technology platforms
   - `sgdci3li.tar` for Linux platforms
5. **Change to the temporary directory and extract the tar file.**

```
$ cd /tempdir
$ tar xvf tarfile
```

6. **Install the SGD Client.**

```
$ sh sgdc/install
```

Follow the instructions on the screen.

Logging in Using the SGD Client

- On UNIX and Linux platforms, you start the SGD Client with the `ttatcc` command.
- On Microsoft Windows platforms, you can either start the Client as part of the installation or click Start ⇒ Programs ⇒ Sun Secure Global Desktop ⇒ Login.

The first time you start the SGD Client, it asks for the following information:

- The URL of the SGD server to which it connects. This is usually `http://server.example.com/sgd`.
- The proxy settings to use. The settings can be determined from your default web browser (requires Java technology) or you can enter them.

Installing the SGD Native Client

The SGD Native Client is no longer being developed. Install the SGD Native Client only if you are using the *classic* webtop.

You do not need superuser (root) or administrator privileges to install the SGD Native Client.

When you install the SGD Native Client, you can choose where it is installed or accept the default location:

- The `C:\Program Files\Tarantella\Sun Secure Global Desktop Native Client` directory on Microsoft Windows platforms.
- The `$HOME/bin` directory on UNIX and Linux platforms.

▼ How to Install the SGD Native Client for Microsoft Windows

1. **Save the SGD Native Client installation program to a temporary directory on the PC.**

   If you are installing from the CD-ROM, the installation program is in the `NativeClients` directory.

   Alternatively, download the installation program from an SGD Web Server from `http://server.example.com`. When the SGD Web Server home page displays, click Install the Sun Secure Global Desktop Classic Native Client.

   The SGD Native Client installation program is `tncwin32.exe`.

2. **Install the SGD Native Client.**

   Double-click `tncwin32.exe` and follow the instructions on the screen.

▼ How to Install the SGD Native Client for UNIX/Linux

1. **Save the SGD Native Client tar file to a temporary directory on the client device.**

   If you are installing from the CD-ROM, the installation program is in the `NativeClients` directory.

   Alternatively, download the tar file from an SGD Web Server from `http://server.example.com`. When the SGD Web Server Welcome page displays, click Install the Sun Secure Global Desktop Classic Native Client.

   SGD Native Client tar files are named according to the platform:

   - `tnci3so.tar` for Solaris OS on x86 platforms
   - `tncspso.tar` for Solaris OS on SPARC technology platforms
   - `tnci3li.tar` for Linux platforms

2. **Change to the temporary directory and extract the tar file.**

```
$ cd /tempdir
$ tar xvf tarfile
```

3. **Install the SGD Native Client.**

```
$ sh ttwebtop/install
```

▼ How to Install the SGD Native Client for Mac OS X

1. **Save the SGD Native Client disk image file to a temporary directory on the client device.**

   If you are installing from the CD-ROM, the installation program is in the `NativeClients` directory.

   Alternatively, download the installation program from an SGD Web Server from `http://server.example.com`. When the SGD Web Server Welcome page displays, click Install the Sun Secure Global Desktop Classic Native Client.

   The SGD Native Client installation program is `tncppdw.dmg`.

2. **Open (mount) the disk image.**

   Drag the Secure Global Desktop Native Client application to your desktop or hard drive.

CHAPTER 3

Upgrading Sun Secure Global Desktop Software

This chapter describes the requirements and procedures for upgrading from a previous version of SGD.

Topics in this chapter include the following:

Before You Upgrade

This section describes the things you must know and do before upgrading.

Upgrades and Early Access Program Software

Upgrades to or upgrades from Early Access Program (EAP) software releases of SGD are not supported. EAP software releases must always be a fresh installation.

Conditions for Upgrading

Upgrades to this version of SGD are only supported from the following versions:

- Sun Secure Global Desktop Software version 4.3
- Sun Secure Global Desktop Software version 4.2

- Tarantella Secure Global Desktop version 3.44 (Japanese locale only)
- Tarantella Secure Global Desktop version 3.42

If you want to upgrade from any other version of SGD, or from Tarantella Enterprise 3 version 3.3 or earlier, contact Sun Support.

You can upgrade from SGD version 3.42 or 3.44 only if *both* of the following are true:

- The server is fully licensed.
- You have a valid maintenance subscription *or* you bought the right to upgrade.

Note – A valid maintenance subscription means you installed sufficient maintenance license keys for your product license keys before trying to upgrade. If you bought the right to upgrade, you must install the Right to Upgrade license key before trying to upgrade.

Upgrades and License Keys

If you upgrade from SGD version 4.1 or earlier, your license keys are upgraded when you install the software. Sun Support does not know what you new license keys are. Use the `tarantella license list` command to list your new license keys. *Make a note of them and keep them somewhere safe.*

Before You Upgrade on Solaris OS Platforms

When you upgrade on Solaris OS platforms, the `pkgadd` command performs several checks and asks you to confirm the changes before installing the package. You can create an administration file that instructs `pkgadd` to bypass these checks and install the package without user confirmation.

To avoid user interaction, the administration file must contain the following line:

```
conflict=nocheck
```

When you upgrade SGD, use the `pkgadd -a` *adminfile* command to specify the administration file.

If you do not specify an administration file when you upgrade, the SGD installation program creates one for you and gives you the option to quit the installation so that you can run the `pkgadd` command again with the `-a` *adminfile* option.

Before You Upgrade From Version 4.2 on Linux Platforms

On Linux platforms, if you are upgrading from SGD version 4.2, you must manually remove all the optional SGD software packs *before* upgrading.

To list all installed SGD software packs:

```
# rpm -qa | grep -i tta
```

The following are the optional SGD software packs:

Package	SGD Software Pack Name
`ttasecure`	Security Pack
`tta3270`	Mainframe Connectivity Pack
`tta5250`	AS/400 Connectivity Pack
`ttafandr`	Andrew X fonts
`ttafhang`	Hangul X fonts
`ttaficl`	ICL X fonts
`ttaforie`	Oriental X fonts
`ttafscot`	SCO Term X fonts

To remove all optional SGD software packs:

```
# rpm -e package ...
```

Upgrades and Your Existing Configuration

When you upgrade, the following changes are applied to your existing configuration:

- Your existing Enterprise Naming System (ENS) database is preserved and backed up.

  The ENS database is the storage area for all the objects in your SGD organizational hierarchy.

  The *install-dir*`/var/ens` directory and backed up to the *install-dir*`/var/ens.`*oldversion* directory.

The backup is not changed and the existing ENS database is changed only if new objects essential to the running of SGD are needed.

- The SGD server configuration and the SGD global configuration are preserved but *not* backed up.

  This configuration is stored in the *install-dir*`/var/serverconfig` directory.

  This configuration is changed only if new properties files need to be added or new attributes need to be added to existing properties.

- All the server resources files in the *install-dir*`/var/serverresources` directory are replaced.

  These files are not normally edited as they control how SGD works.

- Your SGD login scripts are preserved and backed up.

  The *install-dir*`/var/serverresources/expect` directory is backed up to *install-dir*`/var/serverresources/expect.`*oldversion*`.`

- Your customized SGD files are backed up but they are *not upgraded*.

  You can customize SGD by *changing the files* found in a standard installation, for example webtop themes, or by *adding your own files*, for example login scripts.

  You have to upgrade these files manually.

  When you install the new version of SGD, the installation program warns you if files exist that might need to be upgraded manually. See "Upgrading a Customized SGD Installation" on page 22 for advice on how to upgrade these files.

Upgrading Secure Global Desktop

How you upgrade SGD depends on whether you are upgrading an evaluation version or a fully licensed version of SGD, and on whether you are upgrading a single-server or multiple-server array. If you have customized SGD, you might have to upgrade your customized files manually.

Upgrading Evaluation Versions of SGD

If an SGD server does not have a license key installed, or belong to an array that is fully licensed, the SGD server is in evaluation mode. After 30 days the evaluation period expires and the SGD server is in expired evaluation mode.

Upgrade an SGD server in evaluation mode or expired evaluation mode by installing the next version of the software.

An SGD server that was in expired evaluation mode remains in expired evaluation mode after the upgrade. You cannot log in to an SGD server when it is in expired evaluation mode.

To license a server when it is in expired evaluation mode, you must either use the `tarantella license add` command to add a valid license key, or join the server to an array that is already fully licensed.

▼ How to Upgrade a Fully Licensed Single-Server Array

1. **Make sure no webtop and emulator sessions are running in the array, including suspended sessions.**
2. **Upgrade the server by installing the new version of SGD.**

▼ How to Upgrade a Fully Licensed Multiple-Server Array

As the SGD servers in an array share configuration information, they must all run on the same version (4.3x) of the software. This means that to upgrade a multiple-server array, you must dismantle the array, upgrade each server independently, and then rebuild the array.

1. **Make sure no webtop and emulator sessions are running in the array, including suspended sessions.**
2. **Dismantle the array.**

   On the *primary SGD server*, detach the secondary SGD servers from the array:

```
# tarantella array detach --secondary server
```

Caution – Detach only one secondary SGD server at a time. Wait for the array change to be copied to all members of the array before detaching any more SGD servers. You can tell that this has happened when the `tarantella status` command returns the same result when you run it on *each array member*.

   When a secondary SGD server is detached from an array, it loses its license keys and, temporarily, you might not be able to log in to SGD on this host.

3. **Upgrade the primary SGD server by installing the new version of the software.**

4. **Upgrade the secondary SGD servers by installing the new version of the software.**

5. **Rebuild the array.**

   On the *primary SGD server*, add the secondary SGD servers to the array:

```
# tarantella array join --secondary server
```

Caution – Add only one secondary SGD server at a time. Wait for the array change to be copied to all members of the array before adding any more SGD servers. You can tell that this has happened when the `tarantella status` command returns the same result when you run it on *each array member*.

When a secondary SGD server is added to an array, it gains any license keys installed on the primary SGD server.

Upgrading a Customized SGD Installation

When you upgrade, the SGD installation program preserves the customized files it finds, but it does not upgrade them. These files have to be manually upgraded. Two sets of files might need to be upgraded:

- **SGD Web Server files** - Web application files and files used to configure the SGD Web Server.
- **SGD server files** - Files used by the SGD server, such as login scripts, and files used for the *classic webtop*.

Two types of customized files might need attention after you have upgraded:

- **Customized files** - Files found in a standard SGD installation that have been changed by an SGD Administrator.
- **Bespoke files** - Files your organization created and added to an SGD installation.

Upgrading Customized SGD Web Server Files

When you upgrade, the SGD installation program backs up any *customized* SGD Web Server files it detects. Backed-up files and their locations are listed in the *install-dir*`/var/log/webservercustomized.list` log file.

To upgrade the customized files, use utilities such as `diff` and `patch` to compare and merge the differences between the backed-up files and the files in the standard SGD installation.

The SGD installation program copies any *bespoke* SGD Web Server files it finds into the new installation. These files are not changed.

Upgrading Customized SGD Server Files

When you upgrade, the SGD installation program backs up the customized and bespoke SGD server files it detects and produces the following log files:

- *install-dir*`/var/log/upgraded.files` - A summary of the changes.
- *install-dir*`/var/log/customized.list` - A list of any files that an Administrator has edited or added.
- *install-dir*`/var/log/customizedchanged.list` - A list of any files that an Administrator has edited that were changed by the upgrade.
- *install-dir*`/var/log/docrootjava.log` - A list of new or modified Java™ technology files from the original installation.

Use these log files to identify the files that need to be manually upgraded.

▼ How to Manually Upgrade Customized SGD Server Files

1. **Create a copy of the customized file.**
2. **Identify the changes made between SGD versions.**

   The `customizedchanged.list` log file lists the customized files that have to be manually upgraded. For each file listed in this log file, your system will have three versions of the file:

   - The old, customized version in one of the following directories:
     - *install-dir*`/var/docroot.`*oldversion* for classic webtop files.
     - *install-dir*`/var/serverresources.`*oldversion* for login scripts.
     - *install-dir*`/etc/data.`*oldversion* for other files such as color maps.
   - The old, uncustomized version in the *install-dir*`/etc/templates.`*oldversion* directory.
   - The new, uncustomized version in the *install-dir*`/etc/templates` directory.

   Use a utility such as `diff` to compare the old, uncustomized file with the new, uncustomized file. This highlights the changes made between SGD versions.
3. **Apply the changes to the customized file.**

   Use a utility such as `patch` to apply the changes identified in Step 2 to the copy of your customized file.
4. **Copy the upgraded customized file into the correct location in the new SGD installation.**

▼ How to Manually Upgrade Bespoke SGD Server Files

1. **Create a copy of the bespoke file.**
2. **Identify the changes made between SGD versions.**

   The `docrootjava.log` and `customized.list` log files list the bespoke files that might have to be manually upgraded.

   The only way to upgrade bespoke files is to compare versions of the standard SGD files to identify changes that have taken place and then apply those changes to your bespoke files.

   Use a utility such as `diff` to compare the old, uncustomized file with the new, uncustomized file. This highlights the changes made between SGD versions.

   To identify the changes, compare the following files:

   - The old version of the standard SGD files in the *install-dir*`/etc/templates.`*oldversion* directory.
   - The new version of the standard SGD files in the *install-dir*`/etc/templates` directory.
3. **Apply the changes to the bespoke file.**

   Use a utility such as `patch` to apply the changes identified in Step 2 to the copy of your bespoke file.
4. **Copy the upgraded bespoke file into the correct location in the new SGD installation.**

Upgrading Other SGD Components

This section describes how you upgrade the SGD Enhancement Module, the SGD Client, and the SGD Native Client.

▼ How to Upgrade the SGD Enhancement Module for Microsoft Windows

1. **Remove the previous version of the SGD Enhancement Module.**

   See "How to Remove the SGD Enhancement Module for Microsoft Windows" on page 34.

2. **Install the new version of the SGD Enhancement Module.**

   See "How to Install the SGD Enhancement Module for Microsoft Windows" on page 8.

▼ How to Upgrade the SGD Enhancement Module for UNIX/Linux

- **Install the new version of the Enhancement Module.**

  See "How To Install the SGD Enhancement Module for UNIX/Linux" on page 9.

▼ How to Upgrade the SGD Client Automatically

The SGD Client can only be upgraded automatically if *both* of the following are true:

- The previous version of the SGD Client was installed automatically.
- The user's web browser has a supported Java Plug-in tool and Java technology is enabled.

1. **Close any existing web browser sessions.**
2. **Start a new web browser session.**
3. **Log in to SGD.**

   See "How to Log in to Secure Global Desktop" on page 27.

▼ How to Upgrade the SGD Client Manually

Follow this procedure only if the previous version of the SGD Client was installed manually.

- **Install the new version of the SGD Client.**

  See "How to Install the SGD Client Manually on Solaris OS and Linux Platforms" on page 12.

▼ How to Upgrade the SGD Native Client

- **Install the new version of the SGD Native Client.**

  See "Installing the SGD Native Client" on page 13.

Note – Older versions of the Native Client for Microsoft Windows might be installed in different locations to the current version. This might mean that the previous version is not removed when you upgrade and might have to be removed manually.

CHAPTER 4

Getting Started With Sun Secure Global Desktop Software

This chapter describes how to log in to SGD and get started using the software.

Topics in this chapter include the following:

Getting Started

This section describes how to log in to SGD and introduces the SGD administration tools.

▼ How to Log in to Secure Global Desktop

To use SGD, you need the SGD Client and a supported web browser. The SGD Client is usually installed automatically when you log in. To perform an automatic installation, the web browser must have a supported Java Plug-in tool and Java technology must be enabled. If you are using Internet Explorer on Microsoft Windows Vista platforms, you must also add the URL of the SGD server to the list of Trusted Sites in Internet Explorer's Security Settings.

If your web browser does not have Java technology, you must manually install the SGD Client and then connect to SGD. See "Installing the SGD Client" on page 11.

1. **Using a web browser, go to an SGD Web Server.**

   For example, `http://server.example.com`.

   The Secure Global Desktop Web Server Welcome page displays.

2. **(Optional) Select your preferred language.**

   Click one of the flags at the top of the Welcome page.

   The Welcome page displays in the selected language.

3. **Click Login.**

   If a Java technology security message displays, click Run to install the SGD Client.

   The Untrusted Initial Connection message displays.

   The Untrusted Initial Connection message is a security measure to ensure the SGD Client only connects to trusted hosts. The message displays only once for each SGD server to which you connect.

4. **Check the Untrusted Initial Connection message.**

   Check that the name of the host in the message is correct.

   If yes, click Yes.

   If no, click No.

   The Secure Global Desktop login page displays.

   The login page might take a while to display the first time you visit it.

5. **Log in.**

   Type Administrator for the Username and the superuser (root) password for the Password.

   SGD supports several mechanisms for authenticating users. By default, any user with an account on the host can log in to SGD using their UNIX or Linux system username and password.

   When you are logged in, the SGD webtop displays.

   The webtop lists the applications and documents you access through SGD. It also enables access to the SGD online documentation and the SGD administration tools.

   The webtop lists some sample applications that the SGD installation program found on the host so that you can start using SGD.

Once you configure SGD, you might want to tell users to log in by going to `http://server.example.com/sgd`. This displays the SGD login page.

Online Documentation

On the webtop, click Help to display the *Secure Global Desktop 4.31 Administration Guide*. This is the online documentation for configuring and running SGD. Read all of the "Getting started" section as this covers the essential information to help you get started with SGD.

SGD Administration Tools

SGD has several tools for administration:

- **Object Manager** - Enables creation and configuration of objects representing the people, applications, and application servers in your organization. It also enables creation of webtops for SGD users.
- **Array Manager** - Enables configuration of global settings for SGD and settings for individual SGD servers.
- **Configuration Wizard** - Similar to Object Manager but enables creation of objects quickly using the most common settings. You can also delete objects.
- **Session Manager** - Enables management of users' webtop and application sessions.
- **Profile Editor** - Enables definition of settings for the SGD Client for the users in your organization.
- `tarantella` **command** - Enables control and configuration of SGD from the command line.

All of the SGD administration tools, apart from the `tarantella` command, are available on the webtop of SGD Administrators.

`tarantella` command

The `tarantella` command is a script installed in the *install-dir*`/bin` directory. By default, *install-dir* is `/opt/tarantella`. As this script is not on the standard PATH, you must use the full path each time you run the command, or change to *install-dir*`/bin` before running the command. Alternatively:

- Add *install-dir*`/bin` to the PATH, for example:

  ```
  PATH=$PATH:/opt/tarantella/bin; export PATH
  ```

- Create an alias, for example:

  ```
  alias t=/opt/tarantella/bin/tarantella
  ```

The `tarantella` command is actually a family of commands, each of which can have its own set of subcommands. You always run the subcommands through the `tarantella` command, for example:

```
# tarantella license list
```

Help is available for every command by using the `--help` command line argument.

Many commands are designed so that you can build scripts around them.

The following restrictions on which users can use particular `tarantella` commands exist:

- Commands that control the SGD server and SGD Web Server can be run only by superuser (root).
- Commands for running Array Manager and Object Manager, and for creating arrays, can only be run SGD Administrators.
- All other commands can be run by any user in the `ttaserv` group.

Use the `usermod -G` command to make a user a member of the `ttaserv` group. The `ttaserv` group does not have to be the user's primary or effective group.

Controlling SGD

You control SGD from the command line using the `tarantella` command.

You control an SGD server using a `tarantella` command as follows:

- `tarantella start` - Starts SGD services on a host, including printing services.
- `tarantella stop` - Stops SGD services on a host, prompting if users are currently connected.
- `tarantella restart` - Stops and then restarts SGD services on a host.

You control the SGD Web Server using the `tarantella webserver` command as follows:

- `tarantella webserver start` - Starts the SGD Web Server.
- `tarantella webserver stop` - Stops the SGD Web Server.
- `tarantella webserver restart` - Stops and then restarts the SGD Web Server.

Controlling the SGD Enhancement Module

This section describes how you control the SGD Enhancement Module.

Controlling the SGD Enhancement Module for Microsoft Windows

When you install the SGD Enhancement Module for Microsoft Windows, the load balancing service starts immediately. The load balancing service also starts automatically whenever the Windows host is rebooted.

▼ How to Manually Control the Load Balancing Service

Use the following procedure to manually stop and start the load balancing service on a Windows host.

1. **Log in to the Windows host as a user with administrative privileges.**
2. **In the Windows Control Panel, click Administrative Tools.**
3. **Click Computer Management.**
4. **In the tree, expand Services and Applications.**
5. **Click Services.**
6. **Double-click the Tarantella Load Balancing Service.**
7. **Click Stop or Start to stop or start the service.**

Controlling the SGD Enhancement Module for UNIX/Linux

When you install the SGD Enhancement Module for UNIX/Linux, the load balancing and UNIX audio (if installed) processes start immediately. The client drive mapping processes have to be started manually because extra configuration is required.

Whenever the host is rebooted, all the Enhancement Module processes are started automatically.

On UNIX and Linux platforms, you can control the Enhancement Module processes manually with the `tem` command. The `tem` command is a script installed in the *install-dir*`/bin/tem` directory. By default, *install-dir* is `/opt/tta_tem`. As this script is not on the standard PATH, you must use the full path each time you run the command, or change to *install-dir*`/bin` before running the command. Alternatively:

- Add *install-dir*`/bin` to the PATH, for example:

  ```
  PATH=$PATH:/opt/tta_tem/bin; export PATH
  ```

- Create an alias, for example:

  ```
  alias em=/opt/tta_tem/bin/tem
  ```

You control the Enhancement Module processes manually by running the following commands as superuser (root):

- `tem start` - Starts the load balancing processes.
- `tem stop` - Stops the load balancing processes.
- `tem startcdm` - Starts the client drive mapping processes.
- `tem stopcdm` - Stops the client drive mapping processes.
- `tem startaudio` - Starts the UNIX platform audio processes.
- `tem stopaudio` - Stops the UNIX platform audio processes.

Evaluating SGD

By default, SGD installs in a 30-day evaluation mode. During the evaluation period, the following restrictions apply:

- The size of an array is limited to two SGD servers.
- The number of users that can log in or have running applications is limited to five.

After 30 days, the SGD server no longer allows users to log in.

To continue using SGD, you must add a license key. You can add license keys in the following places:

- On the License Properties panel in Array Manager.
- On the command line:

```
# tarantella license add license-key
```

CHAPTER 5

Removing Sun Secure Global Desktop Software

This chapter describes how you remove SGD.

Removing Secure Global Desktop

To remove SGD, you remove the components installed on hosts, on application servers, and on client devices.

▼ How to Remove SGD

1. **Log in as superuser (root) on the SGD host.**
2. **Remove SGD.**

```
# tarantella uninstall --purge
```

Caution – The `tarantella uninstall` command is the only supported method for removing SGD. This command stops all SGD processes before removing the software. Do not use the `pkgrm` or `rpm` commands directly to remove SGD.

▼ How to Remove the SGD Enhancement Module for Microsoft Windows

1. **Log in to the Windows host as a user with administrator privileges.**
2. **In the Windows Control Panel, select Add or Remove Programs.**
3. **Select Secure Global Desktop Enhancement Module for Windows.**
4. **Click Remove.**

▼ How to Remove the SGD Enhancement Module for UNIX/Linux

1. **Log in as superuser (root) on the application server.**
2. **Remove the Enhancement Module:**

   On Solaris OS platforms:

```
# pkgrm tem
```

   On Linux platforms:

```
# rpm -e tem
```

▼ How to Remove the SGD Client on Microsoft Windows Platforms (Manual Installation)

Follow these instructions only if the SGD Client was installed manually.

1. **In the Windows Control Panel, select Add or Remove Programs.**
2. **Select Sun Secure Global Desktop Client.**
3. **Click Remove.**

▼ How to Remove the SGD Client on Microsoft Windows Platforms (Automatic Installation)

Follow these instruction only if the SGD Client was installed automatically.

- **Remove the SGD Client program.**

  Delete the SGD Client program from the user's Home folder. Typically this is the `C:\Documents and Settings\`*username*`\Local Settings\Temp\tcc\`*version* folder.

  The SGD Client program is `tcc.exe`.

▼ How to Remove the SGD Client on UNIX, Linux and Mac OS X Platforms

- **Remove the SGD Client program.**

  Delete the SGD Client program from wherever it is installed. Typically this is either the `$HOME/.tarantella/tcc/`*version* directory or the `$HOME/bin` directory.

  The SGD Client program is `tcc`.

▼ How to Remove the SGD Native Client on Microsoft Windows Platforms

1. **In the Windows Control Panel, select Add or Remove Programs.**
2. **Select Sun Secure Global Desktop Native Client.**
3. **Click Change/Remove.**

▼ How to Remove the SGD Native Client on UNIX, Linux and Mac OS X Platforms

- **Remove the SGD Native Client program.**

  Delete the SGD Client program from wherever it is installed. Typically this is the `$HOME/bin` directory.

  The SGD Native Client program is `ttwebtop` on UNIX and Linux platforms and `tncppdw.dmg` on Mac OS X platforms.