

Oracle® Secure Global Desktop

Installation Guide for Release 5.1



E41496-01
October 2013

Oracle® Secure Global Desktop: Installation Guide for Release 5.1

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

Abstract

This guide describes how to install the Oracle Secure Global Desktop software on your system, including how to upgrade an existing installation. The guide also explains how to get started using the software.

Document generated on: 2013-10-08 (revision: 2149)

Table of Contents

Preface	v
1. Audience	v
2. Document Organization	v
3. Documentation Accessibility	v
4. Related Documents	v
5. Conventions	v
1. Installing SGD	1
1.1. Preparing to Install	1
1.1.1. Hardware Requirements for SGD	1
1.1.2. Operating System Modifications	2
1.1.3. Required Users and Privileges	3
1.1.4. Network Requirements	4
1.1.5. Clock Synchronization	5
1.1.6. Creating a Linux Package Repository From an ISO Image	5
1.2. Installing the Main SGD Component	5
1.2.1. How To Install SGD	6
1.3. Installing the SGD Enhancement Module for Microsoft Windows	8
1.3.1. How to Install the SGD Enhancement Module for Microsoft Windows	9
1.4. Installing the SGD Enhancement Module for UNIX and Linux Platforms	9
1.4.1. How To Install the SGD Enhancement Module on Solaris Platforms	10
1.4.2. How To Install the SGD Enhancement Module on Linux Platforms	11
1.4.3. Troubleshooting Installing the UNIX Audio Module on Linux Platforms	11
1.5. Installing the SGD Gateway	12
2. Upgrading SGD	13
2.1. Before You Upgrade	13
2.1.1. Upgrades and Early Access Program Software	13
2.1.2. Conditions for Upgrading	13
2.1.3. Upgrades and Secure Mode Installations	13
2.1.4. Upgrades and Client Access Licenses	14
2.1.5. Before You Upgrade on Oracle Solaris Platforms	14
2.1.6. Upgrades and Your Existing Configuration	14
2.1.7. Upgrades and UNIX Audio	15
2.2. Performing the Upgrade	15
2.2.1. How to Upgrade a Fully Licensed Single-Server Array	15
2.2.2. How to Upgrade a Fully Licensed Multiple-Server Array	15
2.2.3. Upgrading a Customized SGD Installation	16
2.3. Upgrading Other SGD Components	18
2.3.1. How to Upgrade the SGD Enhancement Module for Microsoft Windows	18
2.3.2. How to Upgrade the SGD Enhancement Module for UNIX and Linux Platforms	18
2.3.3. How to Upgrade the SGD Client Automatically	18
2.3.4. How to Upgrade the SGD Client Manually	18
2.3.5. How to Upgrade the SGD Gateway	19
3. Getting Started With SGD	21
3.1. Logging In to SGD	21
3.1.1. How to Log In to SGD	21
3.2. Using the Workspace	24
3.2.1. Running Applications	24
3.2.2. Changing Your Settings	26
3.2.3. Logging Out	26
3.3. SGD Administration Tools	26
3.3.1. The Administration Console	27

3.3.2. The tarantella Command	29
3.4. Creating Users	30
3.4.1. Creating User Profiles and SGD Administrators	31
3.5. Adding Applications to Workspaces	35
3.5.1. How to Assign an Application Object	36
3.5.2. Creating and Assigning an Application Object	41
3.6. Managing SGD	47
3.6.1. Arrays	49
3.6.2. Monitoring Users	50
3.7. Controlling SGD	51
3.7.1. Controlling the SGD Enhancement Module	52
3.8. SGD Network Architecture	53
3.8.1. Client Devices	53
3.8.2. SGD Servers	54
3.8.3. Application Servers	54
3.9. Next Steps	54
3.9.1. What You Need to Tell Users	54
3.9.2. Where to Get More Help	55
4. Removing SGD	57
4.1. Removing SGD	57
4.1.1. How to Remove SGD on Oracle Solaris Platforms	57
4.1.2. How to Remove SGD on Linux Platforms	57
4.1.3. How to Remove the SGD Enhancement Module for Microsoft Windows	57
4.1.4. How to Remove the SGD Enhancement Module for UNIX and Linux Platforms	58
4.1.5. How to Remove the SGD Client on Microsoft Windows Platforms (Manual Installation)	58
4.1.6. How to Remove the SGD Client on Microsoft Windows Platforms (Automatic Installation)	59
4.1.7. How to Remove the SGD Client on UNIX, Linux, and Mac OS X Platforms (Manual Installation)	59
4.1.8. How to Remove the SGD Client on UNIX, Linux, and Mac OS X Platforms (Automatic Installation)	59

Preface

The *Oracle Secure Global Desktop Installation Guide* provides instructions for installing, upgrading, and removing Oracle Secure Global Desktop (SGD). It also provides instructions on how to get started using the software.

1. Audience

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

2. Document Organization

The document is organized as follows:

- [Chapter 1, *Installing SGD*](#) describes how to install SGD.
- [Chapter 2, *Upgrading SGD*](#) describes the requirements and procedures for upgrading from a previous version of SGD.
- [Chapter 3, *Getting Started With SGD*](#) describes how to log in to SGD and get started using the software.
- [Chapter 4, *Removing SGD*](#) describes how to remove SGD.

3. 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>.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

4. Related Documents

The documentation for this product is available at:

<http://www.oracle.com/technetwork/documentation/sgd-193668.html>

For additional information, see the following manuals:

- *Oracle Secure Global Desktop Administration Guide*
- *Oracle Secure Global Desktop User Guide*
- *Oracle Secure Global Desktop Gateway Administration Guide*
- *Oracle Secure Global Desktop Platform Support and Release Notes*
- *Oracle Secure Global Desktop Security Guide*

5. Conventions

The following text conventions are used in this document:

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

Chapter 1. Installing SGD

This chapter describes how to install Oracle Secure Global Desktop (SGD).

SGD contains several installable components:

- The main SGD component installed on *hosts* provides the main functionality of SGD.
- The optional 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.
- The optional component installed on *hosts*, called the SGD Gateway, provides proxy server and load balancing functionality for an array of SGD servers

Topics in this chapter include the following:

- [Section 1.1, “Preparing to Install”](#)
- [Section 1.2, “Installing the Main SGD Component”](#)
- [Section 1.3, “Installing the SGD Enhancement Module for Microsoft Windows”](#)
- [Section 1.4, “Installing the SGD Enhancement Module for UNIX and Linux Platforms”](#)
- [Section 1.5, “Installing the SGD Gateway”](#)

1.1. Preparing to Install

This section describes the things you must know and do before you install Oracle Secure Global Desktop (SGD).

The following topics are covered:

- Hardware requirements
- Operating system modifications required before installing SGD
- System requirements, such as the required users and network ports



Note

Before installing SGD, read the *Oracle Secure Global Desktop Platform Support and Release Notes*. The release notes contain the latest information on supported platforms and known issues.

1.1.1. Hardware Requirements for SGD

Use the following hardware requirements as a guide and not as an exact sizing tool. For detailed help with hardware requirements, contact an [Oracle sales office](#).

The requirements for a server hosting SGD can be calculated based on the *total* of the following:

- What is needed to install and run SGD
- What is needed for each user that logs in to SGD on the host and runs applications

The following are the requirements for installing and running SGD:

- 2 GB of free disk space
- 2 GB of RAM
- 1 GHz processor
- Network adapter card

This is *in addition to* what is required for the operating system itself and assumes the server is used only for SGD.

The following are the requirements to support users who log in to SGD and run applications:

- Minimum 50 MB for each user
- 50 MHz for each user



Caution

The actual CPU and memory requirements can vary significantly, depending on the applications used.

1.1.2. Operating System Modifications

You might have to make some operating system modifications. Without these modifications, SGD might not install properly or operate correctly.

1.1.2.1. Oracle Solaris

The following operating system modifications might be required for Oracle Solaris platforms:

- On Solaris 10 platforms, you must install at least the End User Oracle Solaris distribution to get the libraries required by SGD.

On Solaris 11 platforms, you must install at least the `slim_install` package group.

If you do not install these package groups, SGD may not install.

- When installing on zones, ensure that the required packages are available on the zone.
- The TCP Fusion feature of Oracle Solaris can cause problems with some local socket connections used by SGD. Disable the TCP Fusion feature before you install SGD, as follows:

1. Add the following line at the bottom of the `/etc/system` file.

```
set ip:do_tcp_fusion = 0x0
```

2. Reboot the server.

- On Oracle Solaris 11 platforms, SGD assigns administration privileges to the first entry in the `/etc/user_attr` file which has the `roles=root` attribute. Ensure that you know the credentials for this Oracle Solaris user.

After installation, the SGD Administrator can be configured using the following command:

```
# tarantella object edit --name "o=Tarantella System Objects/cn=Administrator" \  
--user user-name --surname family-name
```


1.1.2.2. Oracle Linux

The following operating system modifications might be required for Oracle Linux platforms:

- The default `/etc/hosts` file for Oracle Linux contains a single entry, which incorrectly maps the host name of the SGD host to the local loopback address, `127.0.0.1`.

Edit the `/etc/hosts` file to remove this mapping, and add a new entry that maps the name of the SGD host to the network IP address of the SGD host. The SGD host name must not be mapped to the local loopback IP address.

- When installing on Oracle Linux 6 platforms, choose the Desktop or Software Development Workstation package group. This ensures that the required packages for the default SGD workspace are installed. Required packages include graphical administration tools, and X clients such as `xterm` and `gnome-terminal`.

Alternatively, you can choose another package group during installation and use the Customize Now option to add the required packages from the Desktops category.

1.1.2.3. 5250 and 3270 Applications

The following modifications might be required to support 5250 and 3270 applications:

- **Linux platforms.** The `libXm.so.3` library is required. This library is available in the OpenMotif 2.2 package.
- **Solaris 11 platforms.** Install the `motif` package, as follows:

```
# pkg install motif
```

1.1.3. Required Users and Privileges

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

The system must have `ttaserv` and `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 displays a message telling you what you need to do. The message includes details of an install script that you can run to create the required users and group.

If you need to create the required users and group manually, the 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 *writable* home directory.

- For security, lock these accounts, for example with the `passwd -l` command.

Create these users with the `useradd` and `groupadd` commands. For example:

```
# groupadd ttaserv
# useradd -g ttaserv -s /bin/sh -d /home/ttasy -m ttasy
# useradd -g ttaserv -s /bin/sh -d /home/ttaserv -m ttaserv
# passwd -l ttasy
# passwd -l ttaserv
```

To check whether the `ttasy` and `ttaserv` user accounts are correctly set up on your system, use the following commands.

```
# su ttasy -c "/usr/bin/id -a"
# su ttaserv -c "/usr/bin/id -a"
```

If your system is set up correctly, the command output should be similar to the following examples.

```
uid=1002(ttaserv) gid=1000(ttaserv) groups=1000(ttaserv)
uid=1003(ttasy) gid=1000(ttaserv) groups=1000(ttaserv)
```

1.1.4. Network Requirements

You must configure your network for use with SGD. The following are the main requirements:

- Hosts must have Domain Name System (DNS) entries that can be resolved by all clients.
- DNS lookups and reverse lookups for a host must always succeed.
- All client devices must use DNS.
- When you install SGD, you are asked for the DNS name to use for the SGD server. The DNS name must meet the following requirements:
 - In a network containing a firewall, use the DNS name that the SGD host is known as *inside* the firewall.
 - Always use fully-qualified DNS names for the SGD host. For example, `boston.example.com`.

The *Oracle Secure Global Desktop 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 HTTP over Secure Sockets Layer (HTTPS) connections between client devices and the SGD web server.
- **3144** - For standard (unencrypted) connections between the SGD Client and the SGD server.
- **5307** - For secure connections between the SGD Client and the SGD server. Secure connections use Secure Sockets Layer (SSL).



Note

For a default installation in secure mode, where you enable SGD security services and use HTTPS, only ports 443 and 5307 must be open in the firewall.

For an installation in standard mode, where connections are not secured, ports 80, 3144, and 5307 must be open in the firewall. This is because the SGD Client initially makes a secure connection on port 5307. After the connection is established, the connection is downgraded to a standard connection on port 3144.

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

- **22** – For X and character applications using Secure Shell (SSH)
- **23** – For Windows, X, and character applications using Telnet
- **3389** – For Windows applications using Windows Remote Desktop Services
- **6010** and above – For X applications

1.1.5. Clock Synchronization

In SGD, an array is a collection of SGD servers that share configuration information. As the SGD servers in an array share information about user sessions and application sessions, it is important to synchronize the clocks on the SGD hosts. Use Network Time Protocol (NTP) software or the `rdate` command to ensure the clocks on all SGD hosts are synchronized.

1.1.6. Creating a Linux Package Repository From an ISO Image

When installing on Linux platforms, you use the `yum` command to ensure that any package dependencies are resolved automatically. This means that `yum` must be configured to use a suitable Linux package repository.

The Oracle Public Yum Server at <http://public-yum.oracle.com> contains instructions on how to set up an online repository.

If an online package repository is not available, you can use the installation ISO image for your operating system as a local package repository.

The following steps describe how to create a local package repository from an Oracle Linux ISO image stored on the SGD host.

1. Log in as superuser (root) on the SGD host.
2. Create a directory for your repository and mount the ISO image. For example:

```
# mkdir /iso
# mount -o loop OracleLinux-R6-version-Server-x86_64-dvd.iso /iso
```

3. Configure `yum` to use the new repository.

Create the following `yum` configuration file called `iso.repo` in the `/etc/yum.repos.d/` directory.

```
[iso]
name=iso
baseurl=file:///iso/
gpgkey=file:///iso/RPM-GPG-KEY
enabled=1
```

1.2. Installing the Main SGD Component

On Oracle Solaris platforms, install SGD with the `pkgadd` command.

On Oracle Linux platforms, install SGD with the `yum` command. To ensure that any package dependencies are resolved automatically, `yum` should be configured to use a suitable Linux package repository. See [Section 1.1.6, “Creating a Linux Package Repository From an ISO Image”](#) if an online repository is not available.

On Linux platforms, SGD is installed in the `/opt/tarantella` directory. On other platforms, you can change the installation directory as follows:

- **Oracle Solaris platforms** – The installation program asks you for the installation directory when you install the software.
- **Oracle Solaris Trusted Extensions platforms** – The installation program asks you for the installation directory when you install the software. You *must* select another installation directory because the `/opt` directory is a read-only directory. You must also install SGD in a labelled zone. Do not install SGD in the global zone.

When you install the main SGD component, you install the SGD web server. The SGD installation program asks you for the TCP port that the SGD web server listens on 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.

You can install SGD in the following ways:

- **Secure mode.** This is the default mode of installation. The installation program does the following:

- Installs a Secure Sockets Layer (SSL) certificate and configures the SGD server for secure connections between client devices and the SGD server.

If you do not specify certificate details during installation, a self-signed SSL certificate is created and installed automatically. Only use a self-signed SSL certificate for test purposes.

- Enables secure intra-array communication for the SGD server. This means that connections between the SGD servers in an array are secure.



Tip

When you install in secure mode, the installation program uses the `tarantella security enable` command to configure and enable secure connections automatically. Firewall forwarding is disabled, so the SGD server can be used with the SGD Gateway and with tablet devices.

See [Enabling Secure Connections \(Automatic Configuration\)](#) for more information about using this command to install an SSL certificate and enable secure connections, or to enable firewall forwarding for an SGD server.

- **Non-secure mode.** The SGD server is not configured for secure connections during installation. Connections can be secured after installation, as described in the [Enabling Secure Connections \(Automatic Configuration\)](#).

Once you install SGD, the SGD server and the SGD web server are running.

1.2.1. How To Install SGD

Before you begin, if you are installing in secure mode ensure you have access to your SSL certificate, and the private key and CA certificate, if needed. The certificates must be in PEM format.

1. Obtain the software.

Download the software from <http://www.oracle.com>, or copy it from the installation media.

Save the software to a temporary directory on the host.

These are the package files:

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

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

3. Install SGD.

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

To install on Oracle Solaris on x86 platforms:

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

To install on Oracle Solaris on SPARC technology platforms:

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



Note

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

To install on Linux platforms:

```
# yum install --nogpgcheck /tempdir/tta-version.i386.rpm
```

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

On Oracle Solaris platforms:

```
# pkginfo -x tta
```

On Linux platforms:

```
# yum list tta
```

5. Start the SGD server.

```
# /opt/tarantella/bin/tarantella start
```

The first time you start the SGD server, the SGD installation 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, including the following:
 - **Install in secure mode?** By default, SGD is installed and configured to use secure connections to the SGD server and secure intra-array communication. Alternatively, SGD can be installed without secure connections.
 - **Certificate file name.** The SSL certificate used to secure connections to the SGD server. If you have your own SSL certificate, enter the path to the certificate file. The path must be readable by the `ttasys` user.

The default setting of `*` means that a self-signed certificate is installed automatically.

- **Private key file name.** If you are using your own SSL certificate, enter the full path to the private key file. The path must be readable by the `ttasys` user.
- **(Optional) Root certificate file name.** If you are using your own SSL certificate, enter the full path to the root CA certificate file. The path must be readable by the `ttasys` user.

This setting is only required if the SSL certificate is signed by an unsupported CA or an Intermediate CA.

- **Peer DNS name.** You must use a fully-qualified Domain Name System (DNS) name. If you are running SGD on a network with a firewall, use the DNS name that the host is known by inside the firewall.
- **TCP ports.** If another process is currently running on the TCP ports used by the SGD web server, the SGD installation program asks you which TCP port to use.
- **Archive logs every week?** By default, SGD archives its log files each week at 3 a.m. on Sunday. The log files are archived in the `/opt/tarantella/var/log` directory.
- 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.
- (Optional) Installs an SSL certificate. For installations in secure mode, the certificate is used to configure the SGD server for secure connections.
- 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 an SGD Pluggable Authentication Module (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.
- Creates a log file, `/tmp/tta_inst.log`. This file contains a copy of the messages displayed during installation.

1.3. Installing the SGD Enhancement Module for Microsoft Windows

The SGD Enhancement Module for Microsoft Windows contains modules for advanced load balancing 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\Oracle\Secure Global Desktop 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 is listed as Secure Global Desktop Load Balancing Service in the Windows Services tool.

The load balancing service starts automatically whenever the Windows host is rebooted.

1.3.1. 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 installation media, the installation program is in the `modules` directory.

Alternatively, download the installation program from an SGD web server from <https://server.example.com>, where `server.example.com` is the name of an SGD server. When the SGD web server Welcome page displays, click Install an Oracle Secure Global Desktop Enhancement Module.

The SGD Enhancement Module installation program is `temwin32.msi`.

3. Install the SGD Enhancement Module.

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

1.4. Installing the SGD Enhancement Module for UNIX and Linux Platforms

The SGD Enhancement Module for UNIX and Linux Platforms contains modules for advanced load balancing, CDM 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 Oracle Solaris platforms, the UNIX audio module can be installed only in the global zone.

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

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

By default, the Enhancement Module is installed in the `/opt/ta_tem` directory. You can change the installation directory as follows:

- **Oracle Solaris platforms** – The installation program asks you for the installation directory when you install the software.
- **Oracle Solaris Trusted Extensions platforms** – The installation program asks you for the installation directory when you install the software. You *must* select another installation directory because the `/opt` directory is a read-only directory. You must also install the Enhancement Module in a labelled zone. Do not install the Enhancement Module in the global zone.
- **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 module and the UNIX audio module, if selected, are running. The CDM module is not running, because this requires additional configuration. The additional configuration needed is described in the *Oracle Secure Global Desktop 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`.

1.4.1. How To Install the SGD Enhancement Module on Solaris Platforms

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

If you are installing from the installation media, the package is in the `modules` directory.

Alternatively, download the installation program from an SGD web server from <https://server.example.com>, where `server.example.com` is the name of an SGD server. When the SGD web server Welcome page displays, click Install an Oracle Secure Global Desktop Enhancement Module.

These are the package files:

- `tem-version.sol-x86.pkg` for Oracle Solaris on x86 platforms
- `tem-version.sol-sparc.pkg` for Oracle Solaris on SPARC technology platforms

where `version` is the SGD version number.

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 Oracle Solaris on x86 platforms:

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

To install on Oracle Solaris on SPARC technology platforms:

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

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

- The installation directory.

- 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.

```
# pkginfo -x tem
```

1.4.2. How To Install the SGD Enhancement Module on Linux Platforms

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

If you are installing from the installation media, the package is in the `modules` directory.

Alternatively, download the installation program from an SGD web server from <https://server.example.com>, where server.example.com is the name of an SGD server. When the SGD web server Welcome page displays, click Install an Oracle Secure Global Desktop Enhancement Module.

The package files are `tem-version.i386.rpm`, where `version` is the SGD version number.

2. Log in as superuser (root) on the host.
3. Install the SGD Enhancement Module.

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

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

```
# rpm -q tem
```

5. Start the Enhancement Module installation program.

```
# /opt/tta_tem/bin/tem start
```

6. Configure settings for the Enhancement Module.

The Enhancement Module installation program presents the following settings that you can accept or change:

- The amount of virtual memory the host has. This is used for load balancing.
- Whether to install the UNIX audio module.

1.4.3. 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 audio module does not install, check the following:

- 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?
- If the `ARCH` environment variable is set in your environment, does it contain the path to a directory that exists on the system?

1.5. Installing the SGD Gateway

Instructions for installing and configuring the SGD Gateway are included in the *Oracle Secure Global Desktop Gateway Administration Guide*.

Chapter 2. Upgrading SGD

This chapter describes the requirements and procedures for upgrading from a previous version of Oracle Secure Global Desktop (SGD).

Topics in this chapter include the following:

- [Section 2.1, “Before You Upgrade”](#)
- [Section 2.2, “Performing the Upgrade”](#)
- [Section 2.3, “Upgrading Other SGD Components”](#)

2.1. Before You Upgrade

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

2.1.1. 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.

2.1.2. Conditions for Upgrading

The supported upgrade paths to this version of SGD are listed in the *Oracle Secure Global Desktop Platform Support and Release Notes*.

If you want to upgrade from any other version of SGD contact Oracle Support.

If you are sure you want to perform an unsupported upgrade, you must create an empty file `/opt/tarantella/var/UPGRADE` before installing the new version of the software. Your SGD installation might not be upgraded correctly.

2.1.3. Upgrades and Secure Mode Installations

SGD is installed by default in *secure mode*. For secure mode installations, an SSL certificate is installed on the SGD server. The SSL certificate can be a self-signed certificate that is generated during installation, or you can use your own certificate.

What happens on upgrade depends on whether the pre-upgrade version of SGD uses secure connections as follows:

- If the pre-upgrade installation is not secure, the upgrade defaults to a secure mode installation. This is the same as for a clean install of SGD.
- If the pre-upgrade installation is secure and uses a self-signed certificate, the upgrade defaults to a secure mode installation and will install a *new* self-signed certificate.



Note

If you are using the SGD server with the SGD Gateway, you must reconfigure your Gateway deployment by installing the new certificate on the Gateway. See the *Oracle Secure Global Desktop Gateway Administration Guide* for details of how to install an SSL certificate on the Gateway.

- If the pre-upgrade installation is secure and uses a certificate supplied by the user, the upgrade defaults to a secure mode installation using the *same* certificate.

2.1.4. Upgrades and Client Access Licenses

Starting with SGD release 4.7, Client Access Licenses (CALs) for non-Windows client devices are no longer stored in a license pool on the SGD server. CALs are now stored in a location on the client device.

Following an upgrade, non-Windows client devices can use temporary CALs issued by the Remote Desktop Session Host. The temporary CALs can be used until the correct CALs have been stored on the client device.

2.1.5. Before You Upgrade on Oracle Solaris Platforms

When you upgrade on Oracle Solaris 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 lines:

```
conflict=nocheck
instance=unique
```

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.

2.1.6. Upgrades and Your Existing Configuration

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

- Your existing local repository, formerly called the Enterprise Naming Scheme (ENS) datastore, is preserved and backed up.

The local repository is the storage area for all the objects in your SGD organizational hierarchy.

The `/opt/tarantella/var/ens` directory is backed up to the `/opt/tarantella/var/ens.oldversion` directory.

The backup is not changed. The existing ENS database might be changed if changes are needed to enable it work with the new version of SGD.

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

This configuration is stored in the `/opt/tarantella/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 `/opt/tarantella/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 `/opt/tarantella/var/serverresources/expect` directory is backed up to `/opt/tarantella/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 by *adding your own files*, such as 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 [Section 2.2.3, “Upgrading a Customized SGD Installation”](#) for advice on how to upgrade these files.

2.1.7. Upgrades and UNIX Audio

Following an upgrade, if you want to use audio for X applications you must also upgrade the SGD Enhancement Module on your UNIX or Linux platform application servers. See [Section 2.3.2, “How to Upgrade the SGD Enhancement Module for UNIX and Linux Platforms”](#) for upgrade instructions.

UNIX audio services might not work correctly if the versions of SGD and SGD Enhancement Module are different.

2.2. Performing the Upgrade

How you upgrade SGD depends 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.

2.2.1. How to Upgrade a Fully Licensed Single-Server Array

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

2.2.2. How to Upgrade a Fully Licensed Multiple-Server Array

All SGD servers in a multiple-server array must run on the same version of the SGD software. This means that to upgrade an array, you must dismantle the array, upgrade each server independently, and then rebuild the array.

1. Make sure no user sessions and application 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
```

Detach only one secondary SGD server at a time. After making the change to the structure of the array, wait until SGD has copied the change to all the SGD servers in the array before making any further changes. Run the `tarantella status` command on the primary SGD server to check the status of the array.

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.

The clocks on all SGD servers must be in synchronization. If the time difference is more than one minute, the array join operation will fail.

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

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

Add only one secondary SGD server at a time. After making the change to the structure of the array, wait until SGD has copied the change to all the SGD servers in the array before making any further changes. Run the `tarantella status` command on the primary SGD server to check the status of the array.

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

2.2.3. 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

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

2.2.3.1. 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 `/opt/tarantella/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.

2.2.3.2. 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:

- `/opt/tarantella/var/log/upgraded.files` – A summary of the changes
- `/opt/tarantella/var/log/customized.list` – A list of any files that an Administrator has edited or added
- `/opt/tarantella/var/log/customizedchanged.list` – A list of any files that an Administrator has edited that were changed by the upgrade

- `/opt/tarantella/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:
 - `/opt/tarantella/var/serverresources.oldversion` for login scripts.
 - `/opt/tarantella/etc/data.oldversion` for other files such as color maps.
- The old, uncustomized version in the `/opt/tarantella/etc/templates.oldversion` directory.
- The new, uncustomized version in the `/opt/tarantella/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 the previous step 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 `/opt/tarantella/etc/templates.oldversion` directory.
- The new version of the standard SGD files in the `/opt/tarantella/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.

2.3. Upgrading Other SGD Components

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

2.3.1. How to Upgrade the SGD Enhancement Module for Microsoft Windows

1. (Optional) If the current version of the SGD Enhancement Module is before version 4.7, remove the current version manually.



Caution

The upgrade process will fail if the current version is not removed manually.

See [Section 4.1.3, "How to Remove the SGD Enhancement Module for Microsoft Windows"](#).

2. Install the new version of the Enhancement Module.

See [Section 1.3.1, "How to Install the SGD Enhancement Module for Microsoft Windows"](#).

2.3.2. How to Upgrade the SGD Enhancement Module for UNIX and Linux Platforms

When you upgrade the SGD Enhancement Module and you install the UNIX audio module, you might see a message that says the UNIX audio module is already running. This message is displayed because the SGD audio driver is currently in use and cannot be stopped. The upgraded SGD audio driver is loaded when you next restart the host.

1. Install the new version of the Enhancement Module.

See [Section 1.4, "Installing the SGD Enhancement Module for UNIX and Linux Platforms"](#).

2.3.3. 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 browser has a supported version of Java Plug-in software and Java technology is enabled

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

See [Section 3.1.1, "How to Log In to SGD"](#).

2.3.4. How to Upgrade the SGD Client Manually

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

1. Install the new version of the SGD Client.

2.3.5. How to Upgrade the SGD Gateway

1. Install the new version of the SGD Gateway.

Instructions for installing and configuring the SGD Gateway are included in the *Oracle Secure Global Desktop Gateway Administration Guide*.

Chapter 3. Getting Started With SGD

This chapter describes how to log in to Oracle Secure Global Desktop (SGD) and get started using the software.

Topics in this chapter include the following:

- [Section 3.1, “Logging In to SGD”](#)
- [Section 3.2, “Using the Workspace”](#)
- [Section 3.3, “SGD Administration Tools”](#)
- [Section 3.4, “Creating Users”](#)
- [Section 3.5, “Adding Applications to Workspaces”](#)
- [Section 3.6, “Managing SGD”](#)
- [Section 3.7, “Controlling SGD”](#)
- [Section 3.8, “SGD Network Architecture”](#)
- [Section 3.9, “Next Steps”](#)

3.1. Logging In to SGD

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

3.1.1. How to Log In to SGD



Note

This section describes how to log in to SGD from a desktop computer. For instructions on how to log in using a tablet device, see [Using a Tablet Device](#) in the *Oracle Secure Global Desktop User Guide*.

To use SGD, you need the SGD Client and a supported browser. Usually the SGD Client is installed automatically when you log in. To perform an automatic installation, the browser must have a supported Java Plug-in software and Java technology must be enabled.

If your browser does not have Java technology, you must manually install the SGD Client and then connect to SGD.

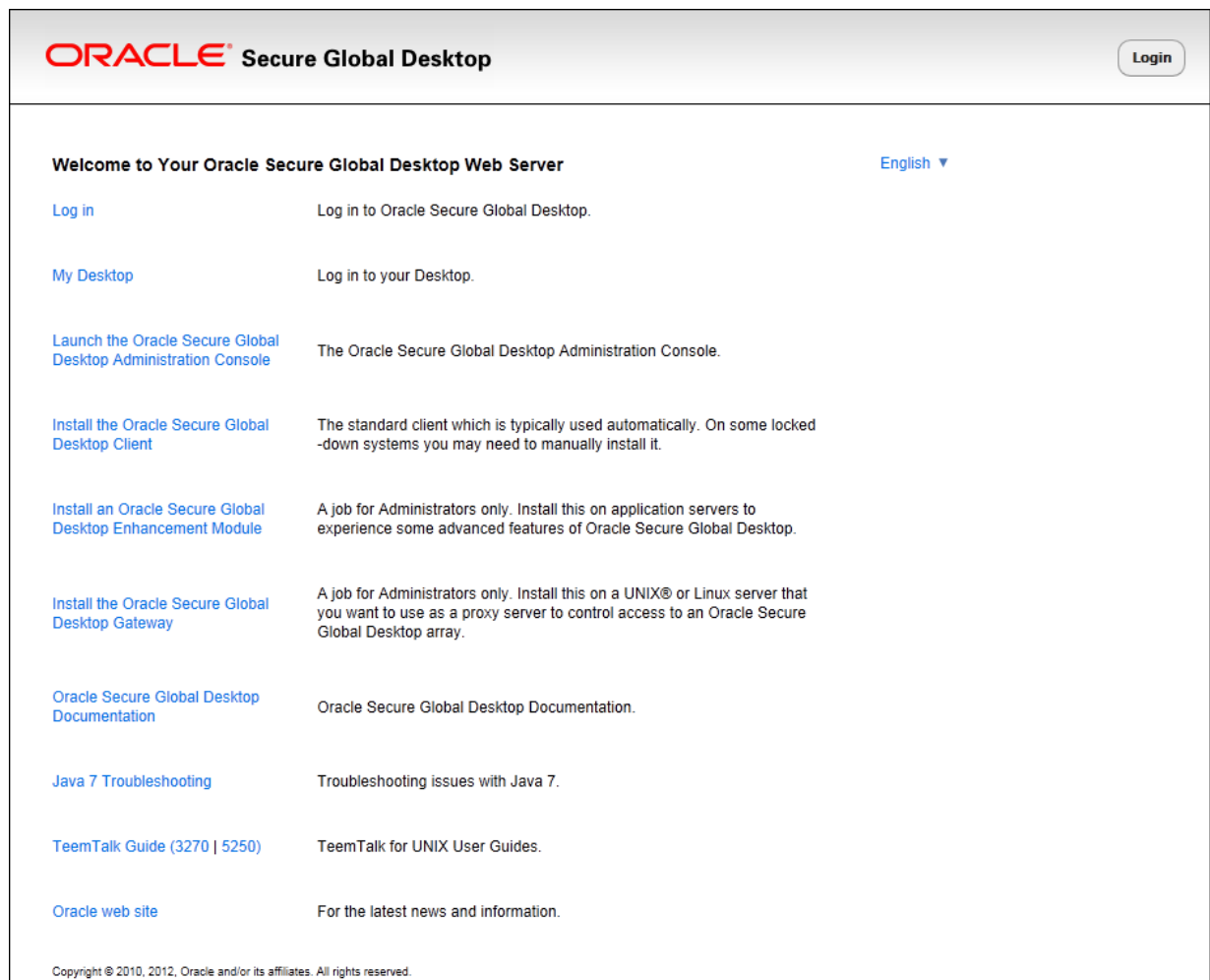
To use SGD with a browser, the browser must have the JavaScript programming language enabled.

If the SGD server uses a Secure Sockets Layer (SSL) certificate signed by an unsupported Certificate Authority (CA), you may see security warning messages when you log in to SGD. See the *Oracle Secure Global Desktop Administration Guide* for information about security warnings and how to avoid them.

1. Using a browser, go to <https://server.example.com> where [server.example.com](#) is the name of an SGD server.

The SGD web server Welcome page is displayed, as shown in [Figure 3.1, “The SGD Web Server Welcome Page”](#).

Figure 3.1. The SGD Web Server Welcome Page



2. (Optional) Select your preferred language.

Select a language from the list near the top of the Welcome page.

The Welcome page is displayed in the selected language.

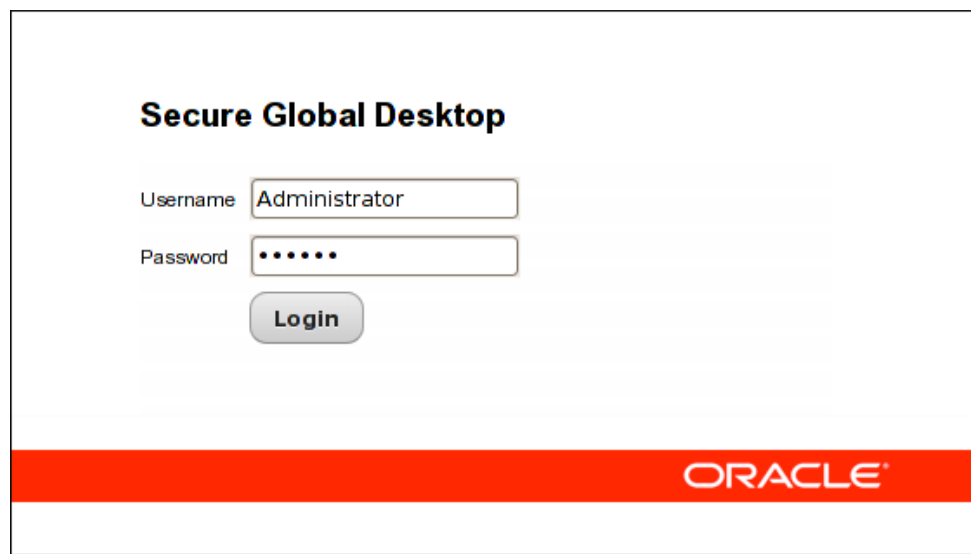
3. Click Login.

The SGD Login Page is displayed, as shown in [Figure 3.2, “The SGD Login Page”](#).

4. Log in.

When you install SGD, SGD creates a default SGD Administrator with the user name “Administrator”. This user authenticates using the password of the UNIX or Linux system root user on the host.

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

Figure 3.2. The SGD Login Page

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

The Untrusted Initial Connection message is displayed. See [Figure 3.3, “An Untrusted Initial Connection message”](#).

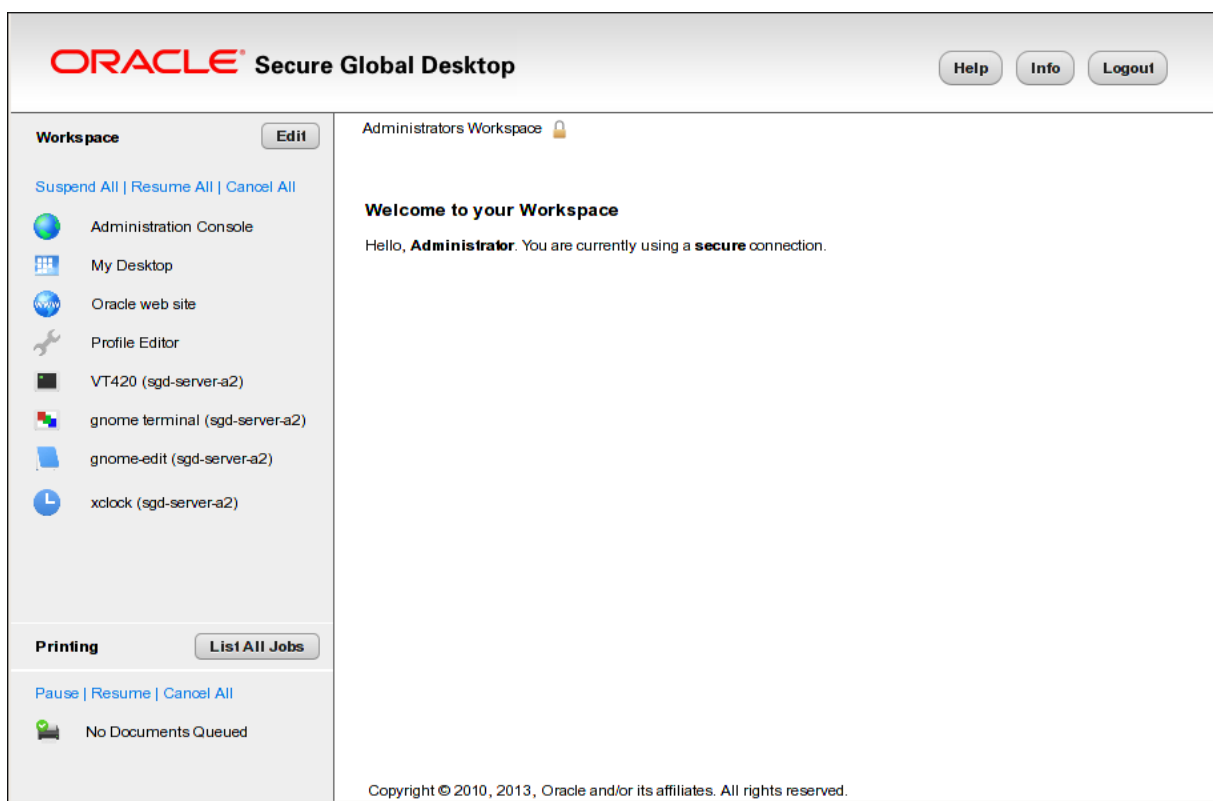
Figure 3.3. An Untrusted Initial Connection message

5. Check the Untrusted Initial Connection message.

The Untrusted Initial Connection message is a security measure to ensure the SGD Client only connects to trusted hosts. The message gives you the opportunity to check the host name and server certificate details before agreeing to the connection. The message is displayed only once for each SGD server to which you connect.

Check that the host details are correct. If they are, click Yes. If they are not, click No.

The workspace for the Administrator user is displayed, as shown in [Figure 3.4, “The Administrator User's Workspace”](#).

Figure 3.4. The Administrator User's Workspace

The SGD Client icon is displayed in the Task bar. See [Figure 3.5, “SGD Client Task Bar Icon”](#).

Figure 3.5. SGD Client Task Bar Icon

3.2. Using the Workspace

The workspace lists the applications and documents you access through SGD, including the SGD administration tools.

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

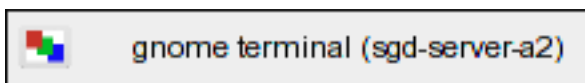


Note

When you use a tablet device, some features of the workspace are changed and how you run applications is different. See [Using a Tablet Device](#) in the *Oracle Secure Global Desktop User Guide*.

3.2.1. Running Applications

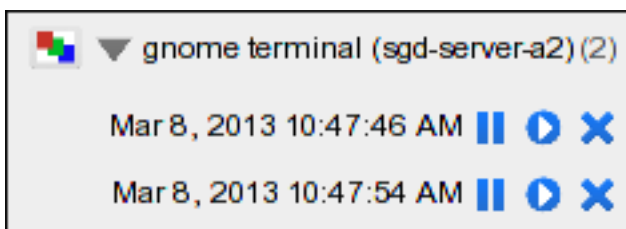
To run an application, click its link on the workspace, as shown in [Figure 3.6, “An Application Link on a Workspace”](#).

Figure 3.6. An Application Link on a Workspace

When you start an application, you might be asked for a user name and password. This is authentication information for the application server which is running the application. These details can be cached securely so you do not need to enter them more than once for each application server.

SGD Administrators configure how applications appear. Some applications might appear full-screen with no window decoration, and others in a window that behaves in the same way as a window on the client device.

When an application is running, a triangle appears in front of the application's name on the workspace and a number appears in brackets after it. The session toolbar also appears below the application name, as shown in [Figure 3.7, “The Session Toolbar”](#).

Figure 3.7. The Session Toolbar

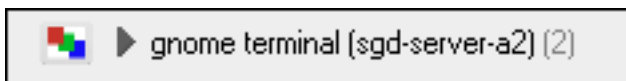
The number in brackets is the number of separate instances of the application you have started. SGD Administrators configure how many simultaneous instances of an application that you can run.

Some applications can be configured to keep running even when they are not displayed. These are “resumable” applications. To close an application's window without ending the application, you *suspend* the application. To display the window again and start using the application, you *resume* the application.

There is a separate session toolbar for each running instance of the application, which you use as follows:

- Click the Suspend button to suspend an application session
- Click the Resume button to resume an application session
- Click the Cancel button to end an application session

Click the triangle to hide and show the session toolbars for the application sessions, as shown in [Figure 3.8, “Hidden Session Toolbars”](#).

Figure 3.8. Hidden Session Toolbars

You can manage all your application sessions at once from the links at the top of the Applications area. You use these links as follows:

- Click Suspend All to suspend all running applications
- Click Resume All to resume all suspended application

- Click Cancel All to end all running or suspended applications

Applications can have one of three resumability settings.

Setting	Description
Never	The application exits when you log out of SGD. You cannot suspend or resume, non-resumable applications.
During the User Session	The application continues to run until you log out of SGD. While you are logged in, you can suspend and resume these applications.
General	The application continues to run even after you have logged out of SGD. When you log in again, click the resume button to display the running application again.

Resumable applications are useful for the following reasons:

- Applications that take a long time to start can be left running, even after you have logged out of SGD.
- You can leave applications running while you travel.
- You can easily recover from browser or other crashes.

3.2.2. Changing Your Settings

If you click the Edit button in the Applications area of the workspace, you can change your settings.

On the Edit Groups tab, you can personalize your workspace by arranging your applications into groups. You decide how and when the groups display. Groups are useful for keeping similar applications together or for hiding applications not used very often. Only an SGD Administrator can add an application to, or remove an application from, the list of applications that are available on a user's workspace.

On the Client Settings tab, you can configure the settings for the SGD Client, for example the proxy server to use. The settings are stored in a profile on the client device.

3.2.3. Logging Out

You must log out of SGD before closing your browser. This enables SGD to shut down any applications that need not run any more and stop the SGD Client.

If you close your browser without logging out, you are not logged out of SGD, because the SGD Client is still running. If you accidentally close the browser, you can only display the workspace by logging in again.

To log out of SGD, click the Logout button on the workspace and click OK when prompted for confirmation.

3.3. SGD Administration Tools

SGD has the following administration tools:

- **Administration Console** – Enables user and user session management, SGD server configuration, and the configuration of applications for SGD users
- **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

The Administration Console and the Profile Editor are available on the workspace of SGD Administrators.

3.3.1. The Administration Console

To display the Administration Console, you can use any browser that is supported by SGD, apart from Safari. See the *Oracle Secure Global Desktop Platform Support and Release Notes* for details of the supported browsers for SGD. The browser must have the JavaScript programming language enabled.

The Administration Console works best when you run it on the primary SGD server in the array.

3.3.1.1. Starting the Administration Console

To start the Administration Console, you click the link on the workspace.

If you want to run the Administration Console without displaying the workspace, you can run it from the following locations:

- <https://server.example.com> and click the Launch the Secure Global Desktop Administration Console link
- <https://server.example.com/sgdadmin>

where server.example.com is the name of an SGD server.

If you run the Administration Console without displaying a workspace, you are prompted to log in as an SGD Administrator.

The Administration Console uses the preferred language for the browser. The current workspace language is not used.

3.3.1.2. Using the Administration Console

When you log in to the Administration Console, the Administration Console opens in Navigation View, as shown in [Figure 3.9, “The Administration Console in Navigation View”](#).

Figure 3.9. The Administration Console in Navigation View

VERSION PREFERENCES LOG OUT HELP

ORACLE Secure Global Desktop User Identity: System Objects / Administrator (Local) Secure Global Desktop Server: sgd-server-a1.example.com

Navigation View

Secure Global Desktop Servers Sessions User Profiles Applications Application Servers Global Settings Caches

Secure Global Desktop Servers

Secure Global Desktop servers are machines running the Secure Global Desktop. By adding at least one other server you create an array. Using an array allows you to distribute load between its servers and increase reliability. One server in the array is the primary server which is responsible for replicating configuration data. Use the Administration Console on the primary server of the array to add additional servers to the array.

Secure Global Desktop Server List (1)

Server	Type	Status	Start Time (BST)	Accepting Connections		User Sessions			Application Sessions		
				Standard	Secure	Standard	Secure	Total	Terminal	Graphical	Total
sgd-server-a1.example.com	Primary Server	Up	2010/06/22 13:25:53	Yes	No	1	0	1	0	0	0

Navigation View is the top-level view that enables you to access the tabs for managing the different areas of SGD. The following table summarizes the tabs available in Navigation View and what they are used for.

Tab	Description
Secure Global Desktop Servers	Managing and configuring SGD servers. This tab is described in more detail in Section 3.6, “Managing SGD” .
Sessions	Managing users' SGD sessions and application sessions. This tab is described in more detail in Section 3.6.2, “Monitoring Users” .
User Profiles	Managing and configuring users' SGD settings. This tab is described in more detail in Section 3.4, “Creating Users” .
Applications	Managing and configuring the applications that users can run through SGD. This tab is described in more detail in Section 3.5, “Adding Applications to Workspaces” .
Application Servers	Managing and configuring the application servers that run the applications displayed through SGD. This tab is described in more detail in Section 3.5, “Adding Applications to Workspaces” .
Global Settings	Configuring settings that apply to SGD as a whole. This tab is described in more detail in Section 3.6, “Managing SGD” .
Caches	Managing the application server passwords that SGD has stored.

SGD is built on the following principles of directory services:

- Users, applications, and application servers are represented by *objects* in a directory. The objects are organized into an *organizational hierarchy* representing your organization.
- Different types of object have different configuration settings, known as *attributes*.
- The *relationships* between objects are important and have meanings.
- Each object is identified using a *unique name*.

SGD includes a number of different object types. When you select an object to work with, the Administration Console changes to Object View. The Administration Console provides links to enable you to switch between Object View and Navigation View, and also an Object History that enables you to switch between the objects you have recently worked with, as shown in [Figure 3.10, “The Administration Console Navigation Links”](#).

Figure 3.10. The Administration Console Navigation Links



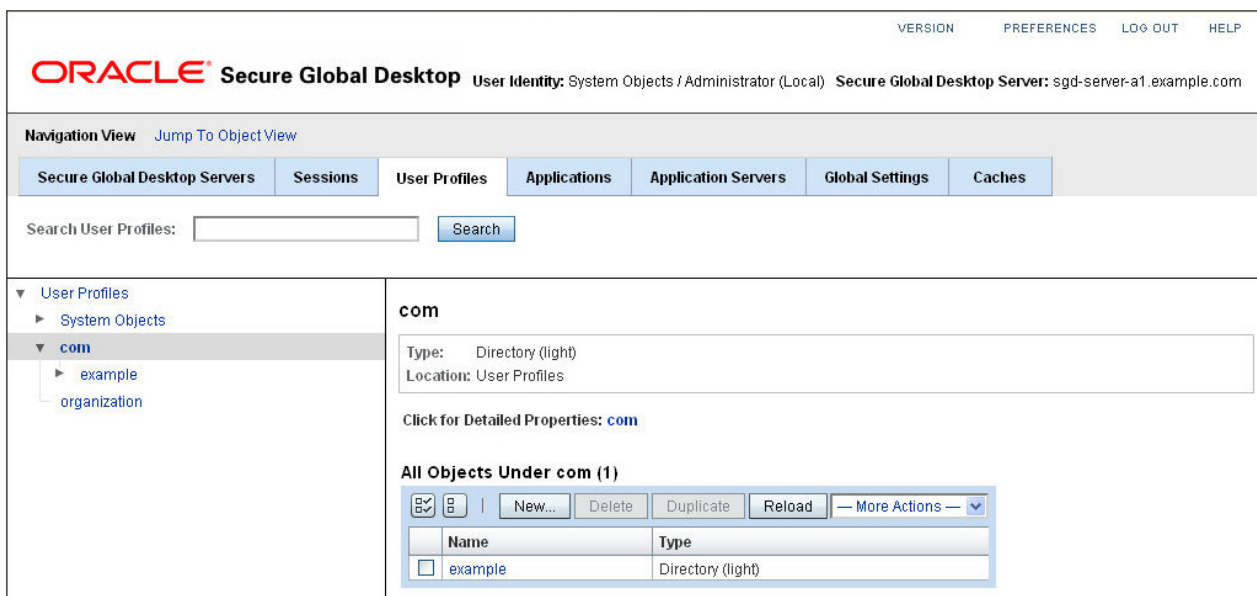


Caution

When using the Administration Console, do not use the browser's Back button. Instead, use the navigation links to move between pages in the Administration Console.

The User Profiles, Applications, and Application Servers tabs are divided into two sections. On the left is the navigation tree and on the right is the content area, as shown in [Figure 3.11, “The Navigation Tree and Content Area”](#). The navigation tree only shows the container objects that are used to structure your organizational hierarchy. As you browse and select objects in the navigation tree, the content area displays a list of objects contained in the selected object.

Figure 3.11. The Navigation Tree and Content Area



Several of the tabs and screens in the Administration Console have a search field. The search is case insensitive and accepts only the * wildcard character. The search results are displayed in a table and are limited to a maximum of 150 hits.

Most tabs in the Administration Console present information in tables. Often the information in a table cell is a link that can be clicked to display further information.

3.3.2. The 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 `/opt/tarantella/bin` before running the command. Alternatively, do the following:

- Add `/opt/tarantella/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 config 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 apply as to which users can use particular `tarantella` commands:

- Commands that control the SGD server and SGD web server can be run only by superuser (root)
- Commands for creating and managing arrays of SGD servers can be run only by 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.

3.4. Creating Users

This section describes how to use the Administration Console to create an SGD user. You do this by creating a user profile object. A user profile is used to control a user's SGD settings, such as whether they can log in to SGD and the applications that they can run. This section also describes how to make a user an SGD Administrator.



Tip

You can configure SGD to use a Lightweight Directory Access Protocol (LDAP) directory for obtaining information about users. If you configure SGD for LDAP integration, you do not have to create user profiles. The *Oracle Secure Global Desktop Administration Guide* has details of how to configure SGD for LDAP integration.

In the Administration Console, the User Profiles tab is where you create and manage user profiles. See [Figure 3.12, “The User Profiles Tab”](#).

Figure 3.12. The User Profiles Tab

The screenshot shows the Oracle Secure Global Desktop Administration Console. At the top, there's a header with 'ORACLE Secure Global Desktop' and 'User Identity: System Objects / Administrator (Local)'. Below this is a navigation bar with tabs: 'Secure Global Desktop Servers', 'Sessions', 'User Profiles', 'Applications', 'Application Servers', 'Global Settings', and 'Caches'. The 'User Profiles' tab is selected. Below the navigation bar is a search bar labeled 'Search User Profiles:'. The main content area is titled 'User Profiles' and shows 'All Objects Under User Profiles (2)'. There's a table with two columns: 'Name' and 'Type'. The table contains two rows: 'com' (Directory (light)) and 'organization' (Directory). Above the table are buttons for 'New...', 'Delete', 'Duplicate', 'Reload', and a 'More Actions' dropdown menu.

By default, this tab contains two “top-level” objects, a Directory object called `organization` (`o=organization` on the command line) and a Directory (light) object called `com` (`dc=com` on the command line). You can rename or delete these objects, or create new top-level objects. You create all the objects you need for managing users within these top-level object types.

You can use other Directory objects to subdivide your organization. For example, you might want to use a Directory (organizational unit) for each department in your organization.

3.4.1. Creating User Profiles and SGD Administrators

In this section, you learn how to create a user profile for yourself, and how to make yourself an SGD Administrator. SGD Administrators always have a user profile. Only SGD Administrators can create user profiles.

Users who occupy the Global Administrators role are SGD Administrators. SGD Administrators can configure SGD using any of the SGD administration tools. Users who do not occupy the Global Administrators role have no administration privileges.

The Global Administrators role is an object in the System Objects organization on the User Profiles tab. The Global Administrators role object is used to assign users administrative privileges and to give them access to the administration tools.

After following these procedures, you can log in to SGD using your UNIX or Linux system user name and password, and run the Administration Console.

You can also use the `tarantella object new_person` command to create a user profile, and the `tarantella role add_member` command to add an SGD Administrator.

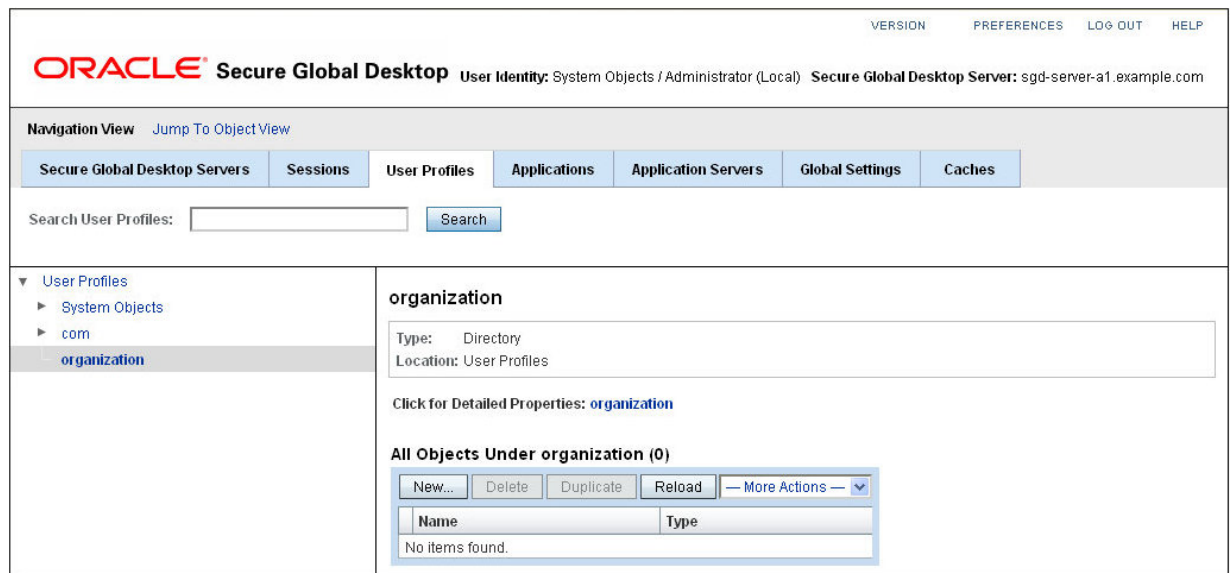
3.4.1.1. How to Create a User Profile

1. In the Administration Console, click the User Profiles tab.
2. Select an object in the organizational hierarchy.

Use the navigation tree to select the organization object, as shown in [Figure 3.13, “The Organization Object Selected”](#).

You can move your user profile to a different location later if needed.

Figure 3.13. The Organization Object Selected



3. Create the user profile object.

- a. In the content area, click New.

The Create a New Object window is displayed.

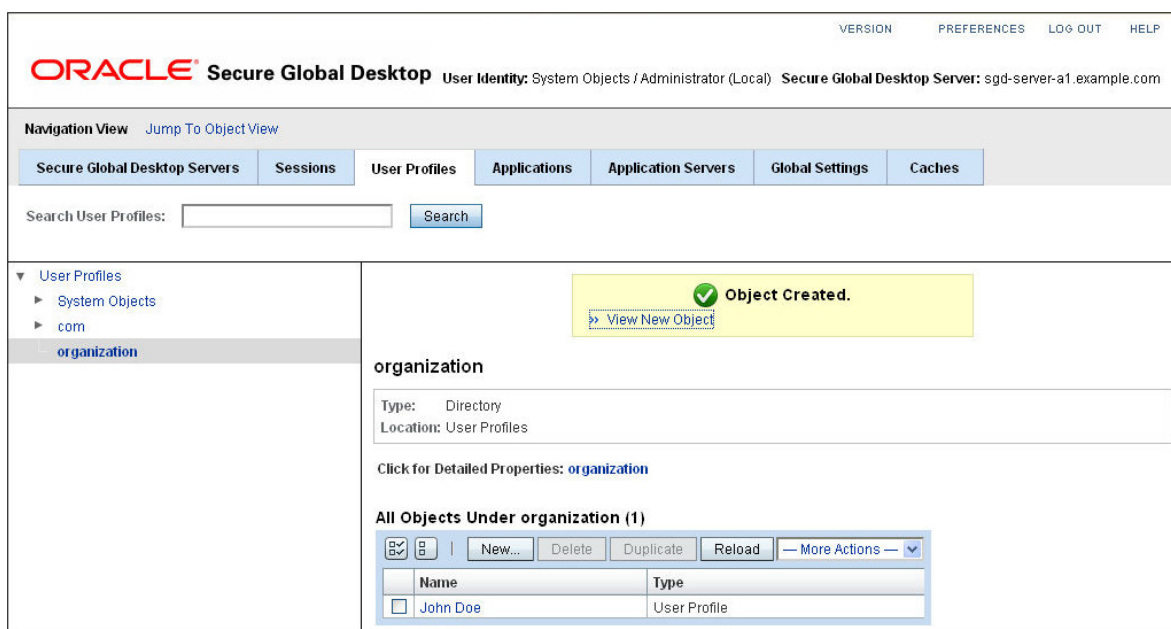
- b. In the Name field, type your name.

For example, [John Doe](#).

- c. Ensure that the User Profile option is selected and click Create.

The Create a New Object window closes and the content area is updated with the new object. See [Figure 3.14, “A Newly-Created User Profile”](#).

Figure 3.14. A Newly-Created User Profile



4. Click the View New Object link.

The General tab for the user profile is displayed in Object View. See [Figure 3.15, “The General Tab for a User Profile”](#).

5. Configure the user profile.

- a. In the Surname field, type your family name.

For example, [Doe](#).

- b. Ensure the Login check box is selected and that the Multiple check box is not selected.

This ensures that you can log in to SGD.

- c. In the User Name field, type your UNIX or Linux system user name.

For example, [jdoe](#).

This attribute can be used to identify and authenticate users.

- d. In the Email Address field, type your full email address.

For example, `john.doe@example.com`.

This attribute can be used to identify and authenticate users.

Figure 3.15. The General Tab for a User Profile

The screenshot shows the Oracle Secure Global Desktop User Identity console. The top navigation bar includes links for VERSION, PREFERENCES, LOG OUT, and HELP. The main header displays the Oracle logo and the text "Secure Global Desktop User Identity: System Objects / Administrator (Local) Secure Global Desktop Server: sgd-server-a1.example.com". Below the header, there is a tabbed interface with tabs for General, Performance, Client Device, Printing, Security, Assigned Applications, Passwords, Tokens, User Sessions, and Application Sessions. The "General" tab is selected, showing the "John Doe - General" profile. The profile details include: Type: User Profile, Location: User Profiles / organization, Designation: Secure Global Desktop Authentication, and Application Authentication. The "Designation" section contains fields for Name (John Doe), Comment (Optional comment field for administrator notes), and Surname (Doe). The "Secure Global Desktop Authentication" section includes a Login checkbox (checked for Enabled, unchecked for Multiple), a Login Name field (jdoe), and an Email Address field (john.doe@example.com). A "Back to top" link is also present.

- e. Click Save.

3.4.1.2. How to Add an SGD Administrator

1. In the Administration Console, click the User Profiles tab.
2. In the navigation tree, click System Objects.

The System Objects table is displayed in the content area, as shown in [Figure 3.16, "The System Objects Table"](#).

Figure 3.16. The System Objects Table

The screenshot shows the Oracle Secure Global Desktop web interface. At the top, there's a header with the Oracle logo and 'Secure Global Desktop'. Below the header, there's a navigation bar with tabs: 'Secure Global Desktop Servers', 'Sessions', 'User Profiles', 'Applications', 'Application Servers', 'Global Settings', and 'Caches'. The 'User Profiles' tab is selected. Below the navigation bar, there's a search field for 'Search User Profiles:' and a 'Search' button. On the left, there's a tree view showing 'User Profiles' expanded, with 'System Objects' selected. The main content area is titled 'System Objects' and shows a table of 'All Objects Under System Objects (8)'. The table has two columns: 'Name' and 'Type'.

Name	Type
Administrator	User Profile
Anonymous Profile	User Profile
Global Administrators	Role
LDAP Profile	User Profile
NT User Profile	User Profile
SecurID User Profile	User Profile
Third Party Profile	User Profile
UNIX User Profile	User Profile

3. In the System Objects table, click the Global Administrators link.

The Members tab is displayed in Object View, as shown in [Figure 3.17, "The Members Tab"](#).

Figure 3.17. The Members Tab

The screenshot shows the Oracle Secure Global Desktop web interface with the 'Members' tab selected. The header and navigation bar are the same as in Figure 3.16. The 'Object View' tab is selected, and the 'Object History' dropdown shows 'Global Administrators'. The main content area is titled 'Global Administrators - Members'. It shows a table with 'Type' and 'Location' columns. Below this, there's a section for 'Editable Members' with a sub-section 'Directly Assigned Member Objects (1)'. This section contains a table with columns 'Member Name', 'Type', and 'Location'.

Member Name	Type	Location
<input type="checkbox"/> Administrator	User Profile	User Profiles / System Objects

4. In the Editable Members table, click Add.

The Add User Assignment window is displayed. See [Figure 3.18, "The Add User Assignment Window"](#).

5. Locate your user profile.

Use the Search field to find your user profile, or browse the navigation tree.

6. Select the check box next to your user profile and click Add.

Figure 3.18. The Add User Assignment Window

ORACLE® Secure Global Desktop

Add User Assignment
Select the object to assign.

Name: Global Administrators
Type: Role
Location: User Profiles / System Objects

Search User Profiles:

▼ User Profiles
 ▶ System Objects
 ▶ com
 organization

organization
Type: Directory
Location: User Profiles

All Objects Under organization (1)

Name	Type
<input checked="" type="checkbox"/> John Doe	User Profile

The Members tab is displayed and your user profile is listed in the Editable Members table. See [Figure 3.19, “Updated Members Tab”](#).

Figure 3.19. Updated Members Tab

ORACLE® Secure Global Desktop User Identity: System Objects / Administrator (Local) Secure Global Desktop Server: sgd-server-a1.example.com

VERSION PREFERENCES LOG OUT HELP

Object View [Jump To Navigation View](#) Object History: Global Administrators ▼

Members **Assigned Applications**

Global Administrators - Members
Type: Role
Location: User Profiles / System Objects

Editable Members

Directly Assigned Member Objects (2)

Member Name	Type	Location
<input type="checkbox"/> Administrator	User Profile	User Profiles / System Objects
<input type="checkbox"/> John Doe	User Profile	User Profiles / organization

3.5. Adding Applications to Workspaces

This section describes how to use the Administration Console to create an application object that can be displayed through SGD, and how to make a link for starting the application appear on a user's workspace.

In the Administration Console, the Applications tab is where you configure the applications that users can run through SGD. See [Figure 3.20, “The Applications Tab”](#). The Application Servers tab is where you configure the application servers that run the applications. See [Figure 3.27, “The Application Servers Tab”](#).

Figure 3.20. The Applications Tab

ORACLE® Secure Global Desktop User Identity: System Objects / Administrator (Local) Secure Global Desktop Server: sgd-server-a1.example.com

Navigation View: Secure Global Desktop Servers Sessions User Profiles Applications Application Servers Global Settings Caches

Search Applications: Search

▼ Applications
► System Objects

Applications

All Objects Under Applications (1 - 15 of 15)

Name	Type
3270	3270 Application
5250	5250 Application
Applications	Group
dtpad (sgd-server-a1)	X Application
dtterm (sgd-server-a1)	X Application
Gnome Terminal (sgd-server-a1)	X Application
Mozilla (sgd-server-a1)	X Application
Oracle web site	Document
SMC (sgd-server-a1)	X Application
StarOffice (sgd-server-a1)	X Application
Unix Desktop	X Application
VT420 (sgd-server-a1)	Character Application
Windows Desktop	Windows Application
xclock (sgd-server-a1)	X Application
My Desktop	Dynamic Application

Page: 1 of 1 Go

Application objects are always contained in the Applications organization (`o=applications` on the command line). Application server objects are always contained in the Application Servers organization (`o=appservers` on the command line).

You can use Directory (organizational unit) objects to subdivide these organizations. For example, you might want to use a Directory object to contain the applications used by a particular department. You can also arrange applications and application servers into Groups.

In SGD, there are links or relationships between user profiles, applications, and application servers. The Administration Console calls these links assignments. Each relationship is managed from an assignment tab. For example, user profile objects have an Assigned Applications tab that shows all the application objects that are assigned to the user. These are the applications that display on a user's workspace. Similarly, application objects have a Hosting Application Servers tab that shows the application servers that can run the application.



Tip

You can configure SGD to use searches of an LDAP directory to assign applications to users. This is called Directory Services Integration (DSI). The *Oracle Secure Global Desktop Administration Guide* has details of how to configure DSI.

3.5.1. How to Assign an Application Object

1. In the Administration Console, click the Applications tab and select the application object.

The General tab is displayed in Object View.

2. Specify the application servers that can run the application.
 - a. Click the Hosting Application Servers tab. See [Figure 3.21, “The Hosting Application Servers Tab”](#).

Figure 3.21. The Hosting Application Servers Tab

The screenshot shows the Oracle Secure Global Desktop web interface. At the top, there's a header with the Oracle logo, 'Secure Global Desktop', and user information: 'User Identity: System Objects / Administrator (Local)' and 'Secure Global Desktop Server: sgd-server-a1.example.com'. Below the header, there's a navigation bar with tabs: 'General', 'Launch', 'Presentation', 'Performance', 'Client Device', 'Printing', 'Hosting Application Servers' (which is selected), 'Assigned User Profiles', and 'Application Sessions'. The main content area is titled 'Notepad - Hosting Application Servers' and includes a description: 'This tab page lists the application servers hosting the selected application.' Below this, there's a section for 'Effective Application Servers' with a table that shows 'No Assignment Found.' Another section, 'Editable Assignments', contains 'Add' and 'Delete' buttons and a table with columns 'Object Name', 'Type', and 'Location', also showing 'No Assignment Found.'

- b. In the Editable Assignments table, click Add.

The Add Application Server Assignment window is displayed. See [Figure 3.22, “The Add Application Server Assignment Window”](#).

- c. Locate the application server.

Use the Search field to find the application server object, or browse the navigation tree.

- d. Select the check box next to the application server object and click Add

If you select more than one application server object, SGD load balances between application servers.

If you select a group object containing application server objects, you select all the application server objects in that group.

Figure 3.22. The Add Application Server Assignment Window

ORACLE® Secure Global Desktop

Add Application Server Assignment
Select the object to assign.

Name: Notepad
Type: Windows Application
Location: Applications

Search Application Servers:

Application Servers

All Objects Under Application Servers (3)

	Name	Type
<input checked="" type="checkbox"/>	rome	Application Server
<input type="checkbox"/>	SGD Broker	Dynamic Application Server
<input type="checkbox"/>	Tarantella server sgd-server-a1	Application Server

The Effective Application Servers table is updated with the selected application server object, as shown in [Figure 3.23, "Updated Hosting Application Servers Tab"](#).

Figure 3.23. Updated Hosting Application Servers Tab

ORACLE® Secure Global Desktop **User Identity:** System Objects / Administrator (Local) **Secure Global Desktop Server:** sgd-server-a1.example.com

VERSION PREFERENCES LOG OUT HELP

Object View [Jump To Navigation View](#) Object History:

General **Launch** **Presentation** **Performance** **Client Device** **Printing** **Hosting Application Servers** **Assigned User Profiles** **Application Sessions**

Notepad - Hosting Application Servers
This tab page lists the application servers hosting the selected application.

Type: Windows Application
Location: Applications

Effective Application Servers

Application Server Name	Type	Location	Assignment Type
rome	Application Server	Application Servers	Direct

Editable Assignments

	Object Name	Type	Location
<input type="checkbox"/>	rome	Application Server	Application Servers

3. Specify the users that see the application on their workspace.
 - a. Click the Assigned User Profiles Tab. See [Figure 3.24, "The Assigned User Profiles tab"](#).

Figure 3.24. The Assigned User Profiles tab

The screenshot shows the Oracle Secure Global Desktop web interface. At the top, there's a header with the Oracle logo and 'Secure Global Desktop' text. To the right of the logo, it says 'User Identity: System Objects / Administrator (Local)' and 'Secure Global Desktop Server: sgd-server-a1.example.com'. Navigation links for 'VERSION', 'PREFERENCES', 'LOG OUT', and 'HELP' are also present.

Below the header, there's a navigation bar with tabs: 'Object View', 'Jump To Navigation View', and 'Object History: Notepad'. The 'Assigned User Profiles' tab is selected.

The main content area is titled 'Notepad - Assigned User Profiles'. Below the title, it says 'This tab page lists the user objects able to launch the selected application.' There's a box showing 'Type: Windows Application' and 'Location: Applications'.

Below this, there's a section titled 'Effective User Profiles'. It contains a table with columns 'User Name', 'Type', 'Location', and 'Assignment Type'. The table has a header row and one data row labeled 'Local Assignments' with the text 'No Assignment Found.' below it.

At the bottom, there's a section titled 'Editable Assignments'. It contains a box with 'Add' and 'Delete' buttons. Below the buttons is a table with columns 'Object Name', 'Type', and 'Location'. The table has a header row and one data row labeled 'No Assignment Found.' below it.

- b. In the Editable Assignments table, click Add.

The Add User Assignment window is displayed, as shown in [Figure 3.25, “The Add User Assignment Window”](#).

- c. Locate the user profile.

Use the Search field to find the user profile, or browse the navigation tree.

You can assign an application object to a user profile or directory object.

If you assign an application object to a directory object, all the user profiles contained in that directory object automatically receive the application. This is called inheritance. Assigning an application object to directory objects is more efficient.

- d. Select the check box next to your user profile and click Add.

Figure 3.25. The Add User Assignment Window

ORACLE® Secure Global Desktop

Add User Assignment
Select the object to assign.

Name: Notepad
Type: Windows Application
Location: Applications

Search User Profiles:

▼ User Profiles
 ▶ System Objects
 ▶ com
organization

organization
 Type: Directory
 Location: User Profiles

All Objects Under organization (1)

	Name	Type
<input checked="" type="checkbox"/>	John Doe	User Profile

The Effective User Profiles table is updated with the selected users. See [Figure 3.26, “Updated Assigned User Profiles Tab”](#).

Figure 3.26. Updated Assigned User Profiles Tab

ORACLE® Secure Global Desktop User Identity: System Objects / Administrator (Local) Secure Global Desktop Server: sgd-server-a1.example.com

Object View [Jump To Navigation View](#) Object History:

General **Launch** **Presentation** **Performance** **Client Device** **Printing** **Hosting Application Servers** **Assigned User Profiles** **Application Sessions**

Notepad - Assigned User Profiles
This tab page lists the user objects able to launch the selected application.

Type: Windows Application
Location: Applications

Effective User Profiles

User Name	Type	Location	Assignment Type
▼ Local Assignments			
John Doe	User Profile	User Profiles / organization	Direct

Editable Assignments

	Object Name	Type	Location
<input type="checkbox"/>	John Doe	User Profile	User Profiles / organization

4. Check that the application appears on your workspace.

You might have to log out and log in using your UNIX or Linux system user name and password to see the application on your workspace.

3.5.2. Creating and Assigning an Application Object

Creating and assigning an application object involves the following steps:

1. Create an application server object.

In this step, you specify the name and location of the application server that runs the application.

See [Section 3.5.2.1, “How to Create an Application Server Object”](#).

2. Create an application object.

In this step, you specify the command that runs when users start the application and how the application is presented.

See [Section 3.5.2.2, “How to Create an Application Object”](#).

3. Assign the application object.

In this step, you assign the application server object to the application object, so that SGD knows where to run the application. Then you assign the application object to an object on the user profiles tab, so that SGD puts a link for the application on a user's workspace.

See [Section 3.5.1, “How to Assign an Application Object”](#).

Only SGD Administrators can create objects and assign them.

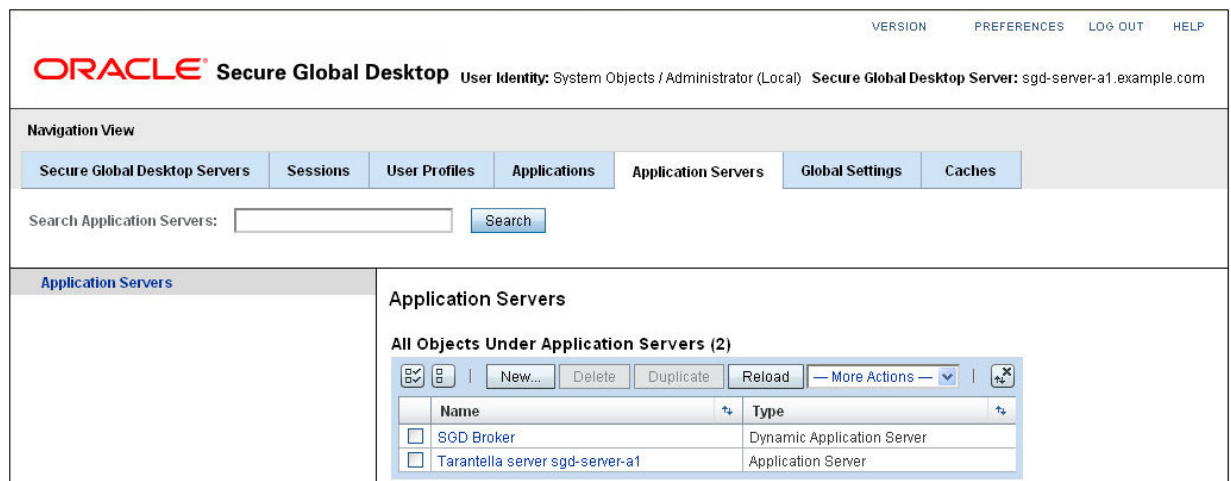
The following procedures describe how to create and assign a Windows application object. The principles are the same for other application types.

On the command line, you can also perform all these steps with the `tarantella object` family of commands.

3.5.2.1. How to Create an Application Server Object

1. In the Administration Console, click the Application Servers tab.

Figure 3.27. The Application Servers Tab



2. Create the application server object.

Create the application server object directly in the Application Servers organization, as shown in [Figure 3.27, “The Application Servers Tab”](#). You can move it to a different location later if needed.

- a. In the content area, click New.

The Create a New Object window is displayed.

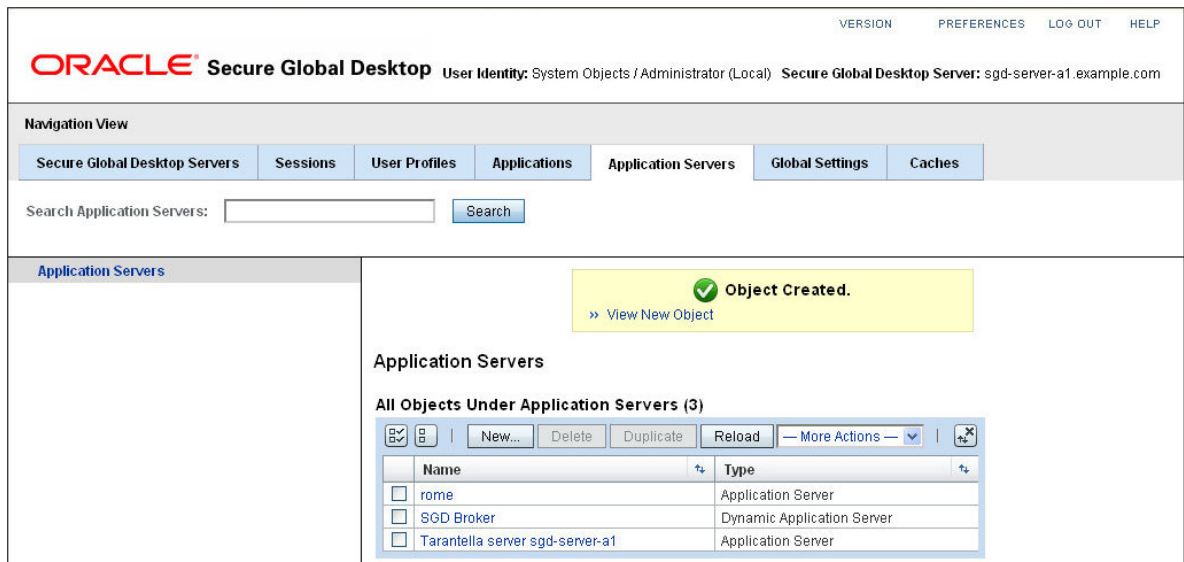
- b. In the Name field, type the name of the application server.

For example, `rome`.

- c. Ensure the Application Server option is selected and click Create.

The Create a New Object window closes and the content area is updated with the new object. See [Figure 3.28, “A Newly-Created Application Server Object”](#).

Figure 3.28. A Newly-Created Application Server Object



3. Click the View New Object link.

The General tab for the application server object is displayed in Object View, as shown in [Figure 3.29, “The General Tab for an Application Server Object”](#).

4. Configure the application server object.

- a. In the Address field, type the fully-qualified Domain Name System (DNS) name of the application server.

For example, `rome.example.com`.

- b. Ensure that the Application Start check box is selected.

This tells SGD that the application server is available to run applications.

- c. In the Domain Name field, type the name of the Microsoft Windows domain.

For example, `rome`.

This attribute is used in the authentication process when users run the application.

Figure 3.29. The General Tab for an Application Server Object

The screenshot shows the Oracle Secure Global Desktop Administration Console interface. At the top, there are navigation links: VERSION, PREFERENCES, LOG OUT, and HELP. Below this, the breadcrumb trail reads: ORACLE® Secure Global Desktop > User Identity: System Objects / Administrator (Local) > Secure Global Desktop Server: sgd-server-a1.example.com. The main content area is titled 'Object View' and includes a 'Jump To Navigation View' link and an 'Object History' dropdown menu currently set to 'rome'. Below this is a tabbed interface with five tabs: General (selected), Performance, Hosted Applications, Application Sessions, and Passwords. The 'General' tab is active, showing the 'rome - General' configuration page. This page includes a 'Save' button and a 'Reset' button. The configuration details are as follows:

- Type: Application Server
- Location: Application Servers
- Designation: Expanded section containing:
 - * Name: rome (text input)
 - Comment: (text area)
 - Optional comment field for administrator notes.
 - Address: rome.example.com (text input) with a 'Test' button.
 - The network address of the application server. Using a DNS name rather than an IP address is recommended.
 - Application Start: ☒ Enabled
 - Whether applications can be started on this application server. You can use this setting, for example, to make an application server temporarily unavailable while you carry out maintenance work.
 - User Assignment: (text area)
 - Optional user assignment to link users to application servers.
 - Maximum Count: (text input)
 - Optional count for the maximum number of applications which can be run on this application server.
- Back to top: (link)
- Application Authentication: (section header)

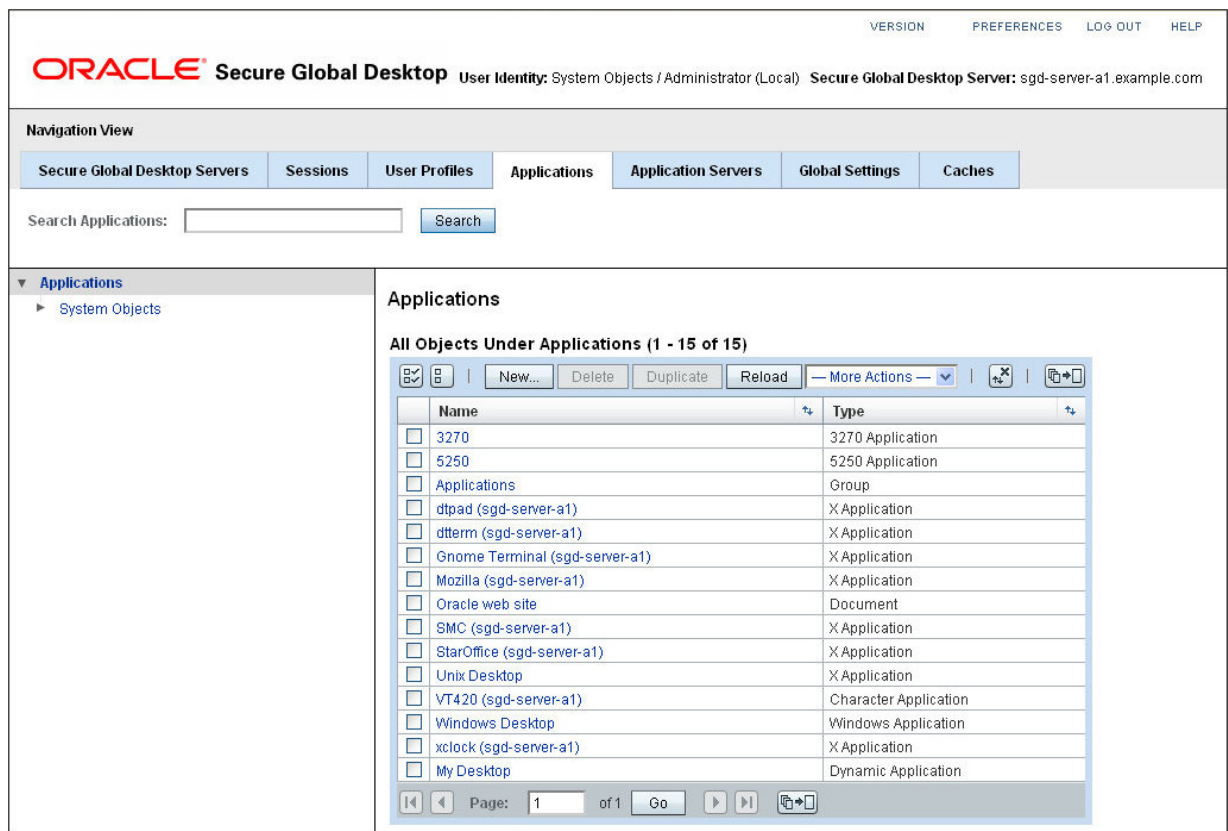
d. Click Save.

3.5.2.2. How to Create an Application Object

The following procedure is an example of how to create a Windows application object.

1. In the Administration Console, click the Applications tab.

Figure 3.30. The Applications Tab



2. Create the application object.

Create the application object directly in the Applications organization, as shown in [Figure 3.30, “The Applications Tab”](#). You can move it to a different location later if needed.

a. In the content area, click New.

The Create a New Object window is displayed.

b. In the Name field, type the name of the application.

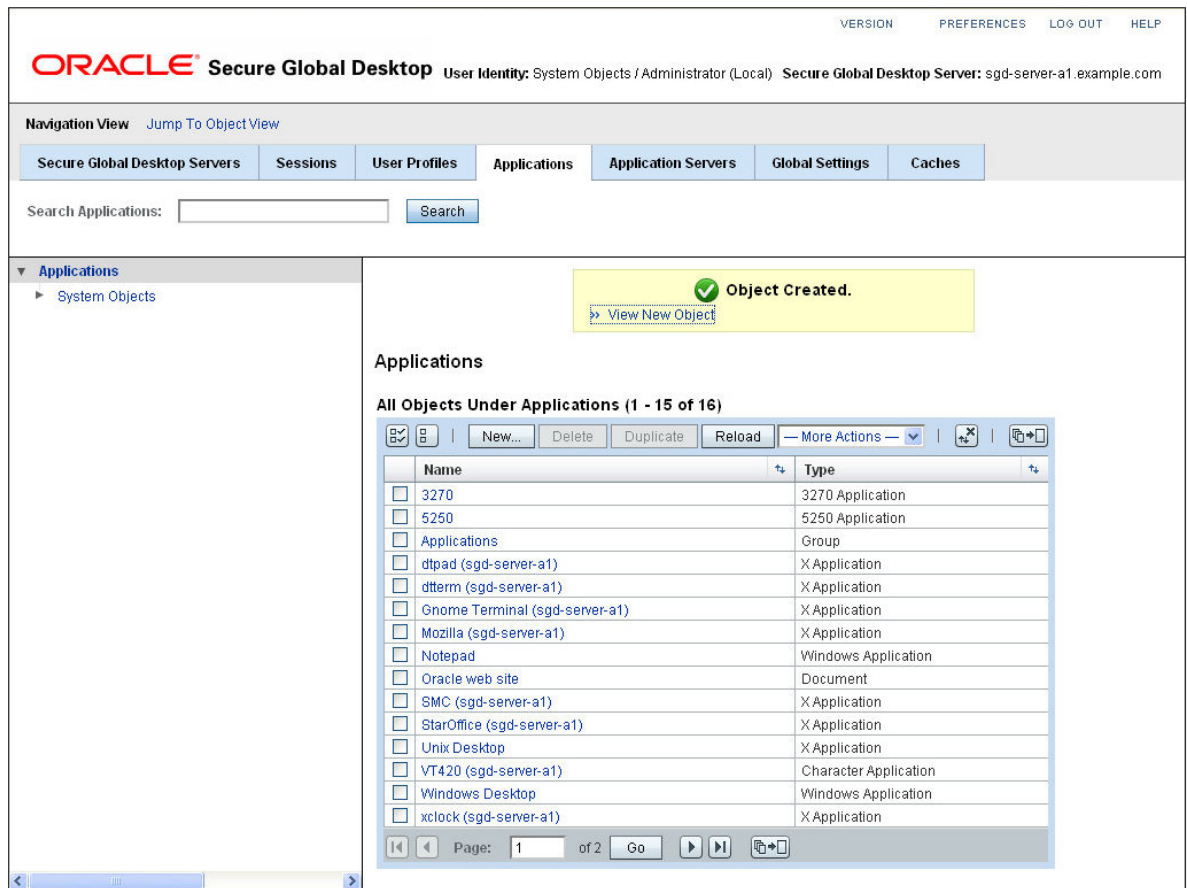
For example, [Notepad](#).

The name you type is used for the application link on the workspace.

c. Ensure that the Windows Application option is selected and click Create.

The Create a New Object window closes and the content area is updated with the new object, as shown in [Figure 3.31, “A Newly-Created Application Object”](#).

Figure 3.31. A Newly-Created Application Object



3. Click the View New Object link.

The General tab for the application object is displayed in Object View.

4. Configure the application.

The configuration settings for a Windows application are described in more detail in the *Oracle Secure Global Desktop Administration Guide*. For this example, the default settings are sufficient, apart from the following configuration.

- a. Click the Launch tab.
- b. In the Application Command field, type the application command.

For Windows desktop sessions, leave this field blank.

To run a particular application, type the full path of the command that runs the application, for example, `C:\Windows\notepad.exe`.

The application must be installed in the same location on all application servers.

- c. Ensure that the SGD Remote Desktop Client check box is selected.

Figure 3.32. The Launch Tab

The screenshot displays the Oracle Secure Global Desktop web interface. At the top, the Oracle logo and 'Secure Global Desktop' text are visible, along with user identity and server information. A navigation bar includes tabs for 'General', 'Launch', 'Presentation', 'Performance', 'Client Device', 'Printing', 'Hosting Application Servers', 'Assigned User Profiles', and 'Application Sessions'. The 'Launch' tab is selected, showing the 'Notepad - Launch' configuration page. This page includes fields for 'Type' (Windows Application), 'Location' (Applications), 'Application Command', 'Arguments for Command', and 'Working Directory'. Below these is the 'SGD Remote Desktop Client' section with checkboxes for 'SGD Remote Desktop Client', 'Console Mode', and 'Enhanced Network Security', each with an 'Enabled' option. A 'Save' button and a 'Reset' button are located at the top right of the configuration area.

- d. Click Save.
5. Click the Presentation tab.
 - a. Configure the Window type.

For a Windows desktop session, select the Kiosk setting from the list.

For an individual application, select the Independent Window setting from the list. You can use the Window Size options to specify the size of the window.

Figure 3.33. The Presentation Tab

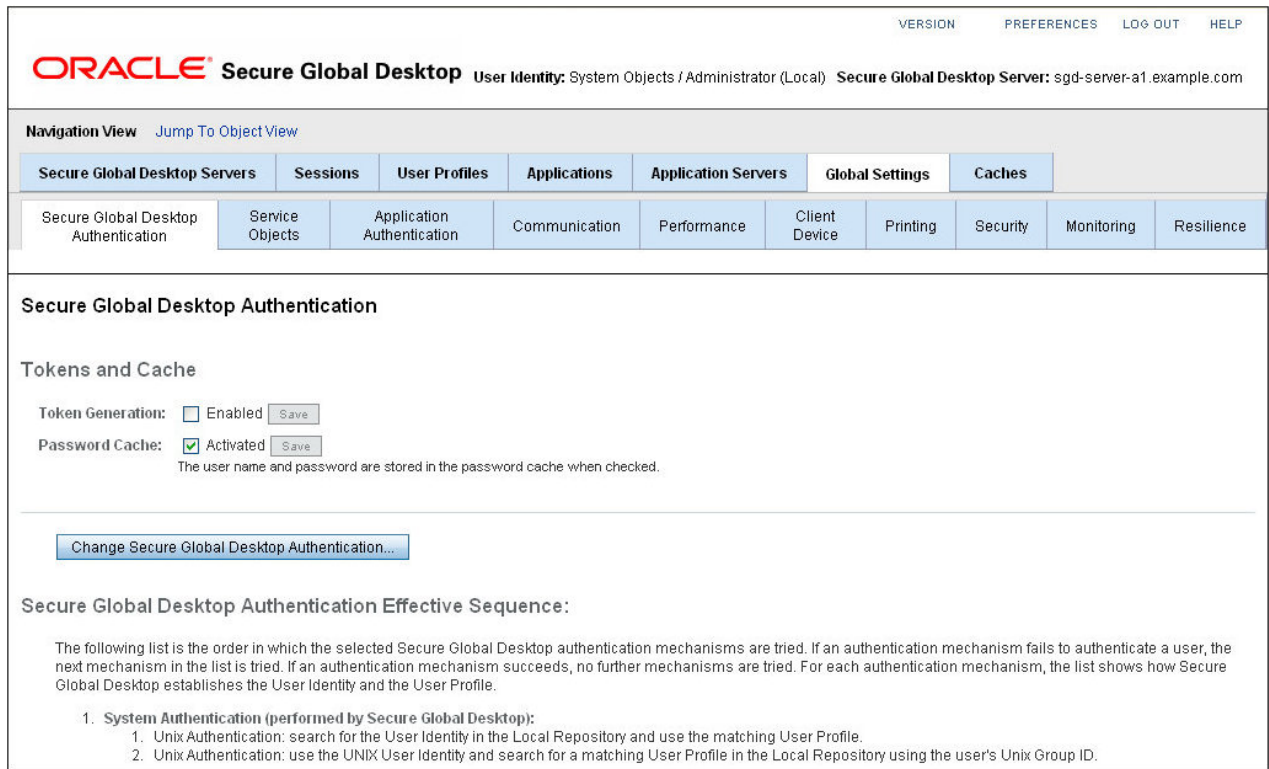
The screenshot shows the Oracle Secure Global Desktop Administration Console interface. At the top, there's a header with the Oracle logo and 'Secure Global Desktop' text. Below this, a breadcrumb trail shows 'System Objects / Administrator (Local)'. The main navigation bar includes tabs for 'General', 'Launch', 'Presentation' (which is selected), 'Performance', 'Client Device', 'Printing', 'Hosting Application Servers', 'Assigned User Profiles', and 'Application Sessions'. The 'Presentation' tab is active, showing settings for the 'Notepad' application. The settings include: 'Type: Windows Application', 'Location: Applications', 'Window Type: Independent Window' (selected from a dropdown), 'SWM Local Window Hierarchy: Needed for Seamless Window Mode compatibility with some Borland applications.', 'Kiosk Mode Escape: [checked] Enable Kiosk Mode Escape', 'Window Manager: [empty text box]', 'Window Size: [unchecked] Client's Maximum Size, [unchecked] RandR Extension, [unchecked] Scale to Fit Window', 'Width: 800 pixels', 'Height: 600 pixels', and 'Color Depth: 24/32-bit - Millions of colors'.

b. Click Save.

3.6. Managing SGD

In the Administration Console, the Global Settings tab is where you configure the settings that apply to SGD as a whole. See [Figure 3.34, "The Global Settings Tab"](#).

Figure 3.34. The Global Settings Tab



ORACLE® Secure Global Desktop User Identity: System Objects / Administrator (Local) Secure Global Desktop Server: sgd-server-a1.example.com

Navigation View [Jump To Object View](#)

Secure Global Desktop Servers Sessions User Profiles Applications Application Servers **Global Settings** Caches

Secure Global Desktop Authentication Service Objects Application Authentication Communication Performance Client Device Printing Security Monitoring Resilience

Secure Global Desktop Authentication

Tokens and Cache

Token Generation: ☐ Enabled [Save](#)

Password Cache: ☒ Activated [Save](#)

The user name and password are stored in the password cache when checked.

[Change Secure Global Desktop Authentication...](#)

Secure Global Desktop Authentication Effective Sequence:

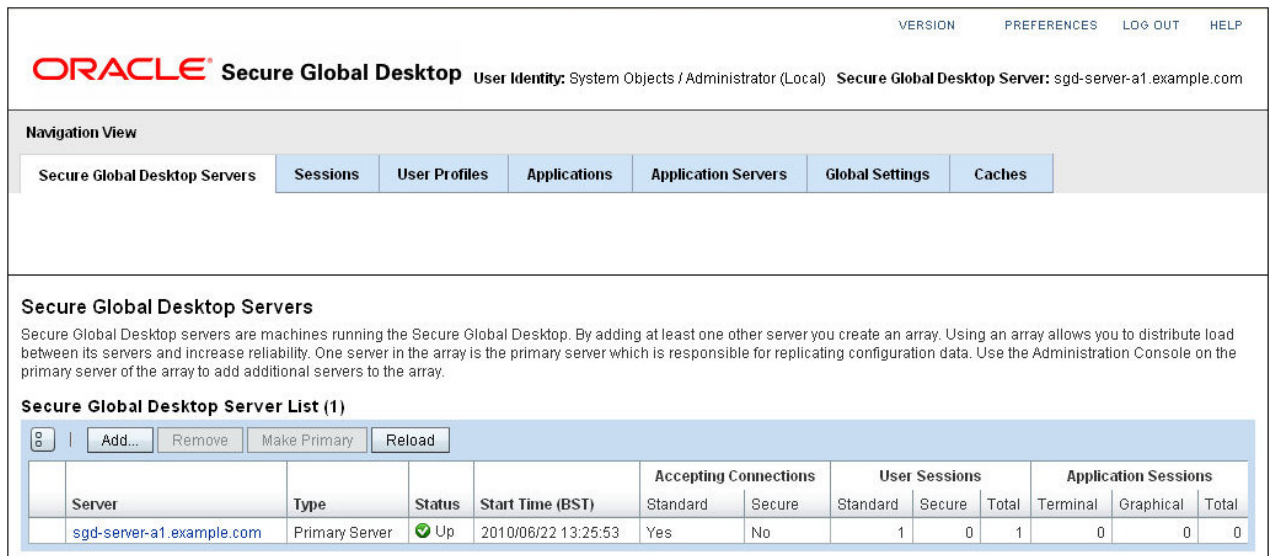
The following list is the order in which the selected Secure Global Desktop authentication mechanisms are tried. If an authentication mechanism fails to authenticate a user, the next mechanism in the list is tried. If an authentication mechanism succeeds, no further mechanisms are tried. For each authentication mechanism, the list shows how Secure Global Desktop establishes the User Identity and the User Profile.

1. System Authentication (performed by Secure Global Desktop):
 1. Unix Authentication: search for the User Identity in the Local Repository and use the matching User Profile.
 2. Unix Authentication: use the UNIX User Identity and search for a matching User Profile in the Local Repository using the user's Unix Group ID.

The Global Settings tab contains other tabs for configuring and managing SGD. For example, the Secure Global Desktop Authentication tab is where you configure how users authenticate to SGD.

In the Administration Console, the Secure Global Desktop Servers tab is where you manage individual SGD servers. See [Figure 3.35, "The Secure Global Desktop Servers Tab"](#).

Figure 3.35. The Secure Global Desktop Servers Tab



ORACLE® Secure Global Desktop User Identity: System Objects / Administrator (Local) Secure Global Desktop Server: sgd-server-a1.example.com

Navigation View

Secure Global Desktop Servers Sessions User Profiles Applications Application Servers Global Settings Caches

Secure Global Desktop Servers

Secure Global Desktop servers are machines running the Secure Global Desktop. By adding at least one other server you create an array. Using an array allows you to distribute load between its servers and increase reliability. One server in the array is the primary server which is responsible for replicating configuration data. Use the Administration Console on the primary server of the array to add additional servers to the array.

Secure Global Desktop Server List (1)

[Add...](#) [Remove](#) [Make Primary](#) [Reload](#)

Server	Type	Status	Start Time (BST)	Accepting Connections		User Sessions			Application Sessions		
				Standard	Secure	Standard	Secure	Total	Terminal	Graphical	Total
sgd-server-a1.example.com	Primary Server	Up	2010/06/22 13:25:53	Yes	No	1	0	1	0	0	0

The Secure Global Desktop Servers tab shows you the status of an SGD server, whether it is running, how many user sessions there are, and how many application sessions the server is hosting.

When you click on the name of an SGD server in the Secure Global Desktop Servers List table, the Administration Console displays further tabs in Object View. You use these tabs to configure and manage the selected SGD server. See [Figure 3.36, “The General Tab for an SGD Server”](#).

Figure 3.36. The General Tab for an SGD Server

The screenshot shows the Oracle Secure Global Desktop Administration Console interface. At the top, there's a header with the Oracle logo and 'Secure Global Desktop' text. Below this, a navigation bar includes 'Object View', 'Jump To Navigation View', and 'Object History: sgd-server-a1.example.com'. A tabbed interface shows 'General', 'Security', 'Performance', 'Protocol Engines', 'User Sessions', and 'Application Sessions'. The 'General' tab is active, displaying configuration for 'sgd-server-a1.example.com - General'. Fields include 'Type: Primary Server', 'External DNS Names: *.sgd-server-a1.example.com', 'User Login: [checked] Allowed', and 'Redirection URL:'. Save and Reset buttons are present at the bottom right.

On the command line, you use the `tarantella config` command to configure global settings and SGD servers. The *Oracle Secure Global Desktop Administration Guide* has details of all the command-line arguments.

3.6.1. Arrays

The Secure Global Desktop Servers tab enables you to group SGD servers together to form an *array*. An array is a collection of SGD servers that share configuration information.

An array contains the following:

- **One primary server** – This server is the authoritative source for global SGD information, and maintains the definitive copy of the organizational hierarchy
- **One or more secondary servers** – The primary server replicates information to these servers

A single, *standalone* server is considered to be the primary server in an array with no secondary servers.

SGD servers in an array might run different operating systems. However, all the array members must run the same version of SGD.

While you are evaluating SGD you are limited to an array containing a maximum of two SGD servers. Once you install a license key, this restriction is removed.

Arrays have the following benefits:

- User sessions and application sessions are load-balanced across the array. To scale more users, simply add more SGD servers to the array.

- With more than one server, there is no single point of failure. You can decommission a server temporarily with the minimum of disruption to your users.
- Configuration information, including all the objects in your organizational hierarchy, is replicated to all array members. All array members have access to all information.

Users see the same workspace and can resume applications no matter which SGD server they log in to.

You add an SGD server to an array by clicking Add in the Secure Global Desktop Servers List table.

3.6.2. Monitoring Users

You can keep track of what your users are doing by monitoring the user sessions and application sessions in progress. User sessions and application sessions are always associated with a user identity and a user profile. The user identity is the unique authenticated identity of the user. The user profile is the SGD user profile object that contains the user's settings.

3.6.2.1. How to Shadow a User's Application Session

If a user is having difficulty with an application, you can use the Administration Console to find the user's application session and then shadow it.

1. Find the user's application session.

In the Administration Console, do one of the following:

- Go to the Application Sessions tab for the user profile object.

This tab lists the application sessions for a user.

- Go to the Application Sessions tab for the application object.

This tab lists the users who are currently running the application.

2. Select the application session in the Application Sessions List table.
3. Start shadowing of the application session.

Click the Shadow button.

The user sees a dialog box, asking whether to allow you to shadow the session. If the user agrees, a new window appears on your screen, showing the running application. Both you and the user can control the mouse pointer and use the application.

4. After fixing the user's problem, end shadowing of the application session.

Close the shadowing window, but do not close the application.

The user sees a dialog box, saying that nobody is currently shadowing the session.

3.6.2.2. User Sessions

A user session begins when a user logs in to SGD and ends when a user logs out. User sessions are hosted by the SGD server the user logs in to. User sessions can be standard sessions or secure sessions. Secure sessions are only available when SGD security services are enabled.

If a user logs in and they already have a user session, the user session is transferred to the new SGD server and the old session ends. This is sometimes called session grabbing, or session moving.

In the Administration Console, you can list user sessions as follows:

- The Sessions tab, in Navigation View, shows all the user sessions that are running on all SGD servers in the array.
- The User Sessions tab for an SGD server shows all the user sessions that are hosted by that server.
- The User Sessions tab for a user profile shows all the user sessions associated with the user profile.

On the Sessions tab and the User Sessions tabs, you can select and end user sessions. On the User Sessions tabs, you can view further details about the user session, for example the information the SGD Client detects about the client device.

On the command line, you use the `tarantella webtopsession` command to list and end user sessions.

3.6.2.3. Application Sessions

An application session begins when a user starts an application and ends when the application exits. Each application session corresponds to an application currently running through SGD. Application sessions can be running or suspended.

An application session can be hosted by any SGD server in the array. This might not be the same SGD server that the user logged in to.

In the Administration Console you can list application sessions as follows:

- The Application Sessions tab for an SGD server shows all the application sessions that are hosted by that server.
- The Application Sessions tab for a user profile shows all the application sessions associated with the user profile.
- The Application Sessions tab for an application server shows all the applications that are running on that application server.

On the Applications Sessions tabs, you can view further details about an application session. You can also end and *shadow* application sessions. With shadowing, you and the user see and interact with the application at the same time.



Note

You can only shadow Windows applications and X applications, and the application sessions must not be suspended.

See [Section 3.6.2.1, “How to Shadow a User's Application Session”](#) for details of how to shadow an application session.

On the command line, you use the `tarantella emulatorsession` command to list, end, and shadow application sessions.

3.7. Controlling SGD

To control SGD from the command line, use the `tarantella start`, `tarantella stop`, and `tarantella restart` commands.

You control an SGD server *and* the SGD web server with the following commands:

- `tarantella start` – Starts the SGD web server and the SGD server
- `tarantella stop` – Stops the SGD web server and the SGD server
- `tarantella restart` – Stops and then restarts the SGD web server and the SGD server

Subcommands for the `tarantella start`, `tarantella stop`, and `tarantella restart` commands enable you to control individual components of SGD, as follows:

- The `sgd` subcommand controls the SGD server. The following example starts SGD services on a host, including printing services.

```
# tarantella start sgd
```

- The `webserver` subcommand controls the SGD web server. The following example stops and then restarts the SGD web server.

```
# tarantella restart webserver
```

See the *Oracle Secure Global Desktop Administration Guide* for more information about the available subcommands and options for the `tarantella stop`, `tarantella start`, and `tarantella restart` commands.

3.7.1. Controlling the SGD Enhancement Module

This section describes how you control the SGD Enhancement Module.

3.7.1.1. 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.

3.7.1.2. Controlling the SGD Enhancement Module for UNIX and Linux Platforms

When you install the SGD Enhancement Module for UNIX and Linux Platforms, the load balancing and UNIX audio 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` 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 `/opt/tta_tem/bin` before running the command. Alternatively, do the following:

- Add `/opt/tta_tem/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 CDM processes
- `tem stopcdm` – Stops the CDM processes
- `tem startaudio` – Starts the UNIX platform audio processes
- `tem stopaudio` – Stops the UNIX platform audio processes

Use the `tem status` command to show the status of the various modules in the Enhancement Module.

3.8. SGD Network Architecture

SGD is built around a three-tier network architecture model, consisting of the following tiers:

- Client devices
- SGD servers
- Application servers

Different tiers can reside on the same host. For example, a single UNIX platform host can act as both an SGD server and an application server, but the tiers remain logically independent.

3.8.1. Client Devices

The first tier contains *client devices*. A client device is a piece of hardware that can communicate with SGD using a browser and the SGD Client.

The browser communicates with the SGD web server on the second tier and displays the workspace to users.

The SGD Client communicates with SGD servers on the second tier and displays the applications that users run.

The Adaptive Internet Protocol (AIP) ensures optimal network usage between the first and second tiers.

3.8.2. SGD Servers

The second tier contains *SGD servers*, which act as a gateway between the first and third tiers. This tier might contain a single SGD server, or many SGD servers configured to form an array.

An SGD server is responsible for the following:

- Authenticating users when they log in to SGD
- Negotiating with application servers to authenticate users when they run applications, prompting users for passwords when necessary
- Causing the SGD Client to display applications
- Keeping track of running applications even after users have logged out, so that they can resume them later

3.8.3. Application Servers

The third tier contains *application servers* that run users' applications.

When a user clicks a link on their workspace, SGD starts the application on an appropriate application server. Output from the application is redirected by the SGD server from the application server to the client device.

When you tell SGD about an application, you include information about all the application servers that can run the application. SGD load balances between the application servers.

3.9. Next Steps

This section describes what you need to tell SGD users and how to view online documentation.

3.9.1. What You Need to Tell Users

The following information is essential to help people use SGD:

- How to log in to SGD.

Users need to know the login URL. Use <https://server.example.com/sgd>, where server.example.com is the name of an SGD server.

Users need to know what user name and password to type to log in to SGD.

SGD supports several mechanisms for authenticating users. The user names and passwords depend on the enabled authentication mechanisms. By default, users can log in with their UNIX or Linux system user name and password.

If your organization prefers not to use Java technology, users need to be shown how to download and install the SGD Client manually.

- How to run applications.

Users need to know how to start and stop applications.

The applications users can access through SGD might run on many different application servers. When a user clicks a link to start an application, SGD might prompt them for a user name and password for the application server. Users need to know what user names and passwords to use.

- Where to get help.

All users have a link to the SGD documentation on their workspace. Click Help.

3.9.2. Where to Get More Help

On the workspace, click Help to view to the online documentation for configuring and running SGD. The online documentation is also available when using the Administration Console.

Documentation in HTML and PDF formats can be accessed from the following locations:

- <https://server.example.com>, where *server.example.com* is the name of an SGD server
- <http://www.oracle.com/technetwork/documentation/sgd-193668.html>

You can also discuss technical issues at the SGD forum at <http://forums.oracle.com/forums/forum.jspa?forumID=914>.

Chapter 4. Removing SGD

This chapter describes how you remove Oracle Secure Global Desktop (SGD).

4.1. Removing SGD

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

4.1.1. How to Remove SGD on Oracle Solaris Platforms

If the SGD server is a member of an array, remove the SGD server from the array. You can use the `tarantella array` command to do this.

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

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



Caution

The `tarantella uninstall` command is the recommended method for removing SGD. This command stops all SGD processes before removing the software. Do not use the `pkgrm` command directly to remove SGD.

4.1.2. How to Remove SGD on Linux Platforms

If the SGD server is a member of an array, remove the SGD server from the array. You can use the `tarantella array` command to do this.

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

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



Caution

The `tarantella uninstall` command is the recommended method for removing SGD. This command stops all SGD processes before removing the software. Do not use the `yum` or `rpm` command directly to remove SGD.

4.1.3. 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.
4. Do one of the following:
 - **On Microsoft Windows XP platforms:** Click Remove.
 - **On Microsoft Windows 7 and Windows 8 platforms:** Click Uninstall.

4.1.4. How to Remove the SGD Enhancement Module for UNIX and Linux Platforms

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

The following commands stop all Enhancement Module processes before removing the software.

On Oracle Solaris platforms:

```
# pkgrm tem
```

On Linux platforms:

```
# rpm -e tem
```



Note

The Enhancement Module installation directory, and some configuration files in this directory, are not removed. The default installation directory for the Enhancement Module is `/opt/tta_tem`.

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

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

1. Remove the SGD Client program.
 - For a system-wide installation:
 - a. In the Windows Control Panel, select Add or Remove Programs.
 - b. Select Oracle Secure Global Desktop Client.
 - c. Do one of the following:
 - **On Microsoft Windows XP platforms:** Click Remove.
 - **On Microsoft Windows 7 and Windows 8 platforms:** Click Uninstall.

- For a user-specific installation:

Delete the SGD Client from wherever it is installed. The default locations are in the user's Home folder, as follows:

On Microsoft Windows XP platforms:

```
C:\Documents and Settings\username\Local Settings\Application Data  
\Programs\Oracle\Secure Global Desktop Client\clients\version
```

On Microsoft Windows 7 and Windows 8 platforms:

```
C:\Users\username\AppData\Local\Programs\Oracle\Secure Global Desktop  
Client\clients\version
```


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

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

1. Remove the SGD Client program.

Delete the SGD Client program from the user's Home folder.

On Microsoft Windows XP platforms, for example:

```
C:\Documents and Settings\username\Local Settings\Temp\Oracle Secure Global Desktop\clients\version
```

On Microsoft Windows 7 and Windows 8 platforms, for example:

```
C:\Users\username\AppData\Local\Temp\Oracle Secure Global Desktop\clients\version
```

The SGD Client program is `tcc.exe`.

4.1.7. How to Remove the SGD Client on UNIX, Linux, and Mac OS X Platforms (Manual Installation)

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

1. Remove the SGD Client program.

Delete the SGD Client program from wherever it is installed.

The default installation directory depends on whether the SGD Client was installed in a user-specified location or in a system-wide location, as follows:

For a user-specific installation, the default locations are:

- **UNIX or Linux platforms:** `$HOME/Oracle Secure Global Desktop/clients/arch/version`
- **Mac OS X platforms:** User-specific installation is not supported on Mac OS X platforms.

For a system-wide installation:

- **UNIX or Linux platforms:** `/opt/Oracle Secure Global Desktop/clients/arch/version`
- **Mac OS X platforms:** `/Applications/Oracle Secure Global Desktop Client/version/Oracle Secure Global Desktop Client.app`

For a system-wide installation on UNIX or Linux platforms, also remove the entry for the SGD Client in the configuration file at `/etc/opt/Oracle Secure Global Desktop/clients.conf`.

The SGD Client program is `ttatcc`.

4.1.8. How to Remove the SGD Client on UNIX, Linux, and Mac OS X Platforms (Automatic Installation)

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

1. Remove the SGD Client program.

Delete the SGD Client program from wherever it is installed. Typically this is the `$HOME/.tarantella/clients/arch/version` directory.

The SGD Client program is `ttatcc`.