Oracle® Secure Global Desktop

Platform Support and Release Notes for Release 4.7

E26357-02
November 2012

Oracle® Secure Global Desktop: Platform Support and Release Notes for Release 4.7

Abstract

This document describes the new and changed features for Oracle Secure Global Desktop 4.7. It also lists what is supported and the known bugs and issues.

Document generated on: 2012-10-31 (revision: 1250)

Table of Contents

Preface

The *Oracle Secure Global Desktop Platform Support and Release Notes for Release 4.7* provide information about the system requirements and support, and the new features and changes, for this version of Oracle Secure Global Desktop (SGD). This document is written for system administrators.

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, *New Features and Changes* describes the new features and changes for this version of Oracle Secure Global Desktop.
- Chapter 2, *System Requirements and Support* includes details of the system requirements and supported platforms for this version of Oracle Secure Global Desktop.
- Chapter 3, *Known Issues, Bug Fixes, and Documentation Issues* contains information about known issues, bug fixes, and documentation issues for this version of Oracle Secure Global Desktop. Details on providing feedback and reporting bugs are also included.

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 for Release 4.7*
- *Oracle Secure Global Desktop Installation Guide for Release 4.7*
- *Oracle Secure Global Desktop Gateway Administration Guide for Release 4.7*
- *Oracle Secure Global Desktop User Guide for Release 4.7*
- *Oracle Secure Global Desktop Security Guide for Release 4.7*

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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1. New Features and Changes

This chapter describes the new features and changes in Oracle Secure Global Desktop (SGD) Release 4.70.

1.1. New Features in Release 4.70

This section describes the features that are new in the SGD 4.70 release.

1.1.1. Secure Installation by Default

In previous releases of SGD, connections to SGD servers were secured as a post-installation task. In this release, connections to the SGD server can be made secure during installation. This is called installing in *secure mode*.

Secure mode installation uses the `tarantella security enable` command to configure and enable SGD security services automatically. During installation, users can choose to use their own Secure Sockets Layer (SSL) certificate to secure connections.

Secure mode installation also enables secure intra-array communication for the SGD server. This means that connections between the SGD servers in an array are encrypted.

When you install in secure mode, firewall forwarding is disabled. This means that the SGD server can be used with the SGD Gateway.

Installation of SGD without using secure connections is still available.

See Installing SGD for more details about installing in secure mode.

1.1.2. New X Server Implementation

This release incorporates a new X Protocol Engine implementation, based on the X.Org Foundation X Server release X11R7.6.

The new implementation provides enhanced support for multiple monitors and dynamic session resizing. These features are enabled through the use of the RANDR and XINERAMA X extensions.

New attributes have been introduced for configuring RANDR extension support. The RandR Extension (`--array-xrandr-enabled`) attribute enables RANDR support for the array. The Window Size: RandR Extension (`--xrandr`) enables RANDR support for an application object.

SGD now supports the X Keyboard (XKB) X extension. Using XKB enhances globalization support, by providing built-in support for more locales. Legacy keyboard maps and server-side configuration are no longer required to process keyboard input for X applications.

See the Using the RANDR X Extension for more details about configuring applications to use these new features.

1.1.3. Audio Recording for Windows Applications

This release provides support for audio recording in Windows applications displayed through SGD.

The Audio Input (`--array-audioin`) attribute has been introduced to enable audio input for an SGD array.

See the Enabling SGD Audio Services for more details of how to set up audio recording for Windows applications.

1.1.4. Network Level Authentication Support for Windows Applications

This release supports the use of Network Level Authentication (NLA) using CredSSP, for authenticating Windows application users. Using NLA enables users to authenticate themselves before establishing a session on the Windows application server.

The Enhanced Network Security (`--enhancednetworksecurity`) attribute has been introduced to configure NLA for Windows applications. This attribute is enabled by default.

1.1.5. New Virtual Server Broker for Oracle VDI

To provide closer integration with Oracle Virtual Desktop Infrastructure (Oracle VDI) deployments, a new virtual server broker has been introduced. The new broker can be used with Oracle VDI Release 3.3 and later.

The new broker uses the Oracle VDI web services API to authenticate the user, obtain a list of desktops, and to start and stop the desktop. With this broker, SGD and Oracle VDI can be installed on different hosts.

The new broker is called the *VDI broker*. The existing broker for legacy Oracle VDI installations was formerly called the VDI broker, and has been renamed in this release as the *Legacy VDI broker*.

The following table shows broker compatibility with Oracle VDI versions.

Table 1.1. Brokers Used With Oracle VDI

Broker Name	Oracle VDI Version
VDI broker	3.3.2 and 3.4.1
Legacy VDI broker	3.2

The VDI broker provides additional features, such as support for a dedicated certificate truststore, host load balancing, and timeouts.

See VDI Broker for details of how to configure and use the VDI broker.

See Section 3.3.1, “Legacy VDI Broker Documentation Issue” for important information about documentation issues concerning the Legacy VDI broker.

1.2. Changes in Release 4.70

This section describes the changes since the SGD 4.60 release.

1.2.1. SGD Client Installation Changes

The following changes have been made for installation of the SGD Client.

- **Automatic installation.** Default installation directories have changed.

  See Automatic Installation of the SGD Client for details of the changes.

- **Manual installation.** To provide support for shared file systems, Administrators can now install the SGD Client in a system-wide location.

SGD keeps a record of the location of all SGD Clients that you have installed manually.

Manual installation is now supported on Mac OS X platforms.

Default log file locations have changed. On Windows platforms, output is logged to the user's application data folder. On UNIX, Linux, and Mac OS X platforms, output is now logged to the system log location.

1.2.2. Default Connection Method Changes

The Connection Method (`--method`) attribute specifies the mechanism used by the SGD server to access an application server and start an application.

The default Connection Method setting has changed from `telnet` to `ssh`.

The `rexec` setting is no longer available.

1.2.3. New Parameters for User-Defined SGD Broker

New parameters that enable configuration of the chooser page have been introduced for the User-defined SGD broker. The User-defined SGD broker is used with the dynamic launch feature of SGD to enable users to select or specify the application server when starting an application.

The new parameters are as follows:

- `hideAppservers`. The list of application servers is not displayed in the chooser page.
- `checkAppserver`. For user-specified application servers, SGD checks that the application server has been assigned to the application object. If the application server is not assigned to the application object, an error message is shown.

1.2.4. Local Launch No Longer Supported

Support for running an application on Windows client devices (known as local launch) has been removed. The Local Client Launch (`--trylocal`) attribute has been deprecated.

The Local X Server (`localx`) setting is no longer supported for the Window Type (`--displayusing`) attribute.

The Check for Local X Server profile setting is no longer available.

1.2.5. Client Access License Pool Removed

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.

The `tarantella tscal` command used to manage the license pool is no longer available.

Note

When you upgrade an SGD server, any CALs stored in the license pool are removed. Non-Windows client devices can use temporary CALs issued by the Remote Desktop Session Host until the correct CALs are stored on the client device.

See the Microsoft Remote Desktop Services documentation for more details about CAL management.

1.2.6. Changes to Display Attributes for Application Objects

Due to the new XPE implementation introduced in this release, the following display attributes are no longer supported:

- RGB Database (`--xpe-rgbdatabase`). The XPE now has built-in support for X11 color names.
- Euro Character (`--euro`). The euro character is now supported by default.
- Keyboard Map: Locked (`--lockkeymap`).
- Keyboard Map (`--xpe-keymap`). The XKB extension is now used for keyboard maps.
- Keyboard Map (`--keymap`). The XKB extension is now used for keyboard maps.

1.2.7. Removed Features in This Release

See Section 2.5, “Removed Features” for a list of features that have been removed in the 4.70 release.

1.2.8. Documentation Changes

The following documentation changes have been made for this release:

- **Security Guide.** A new manual, the *Oracle Secure Global Desktop Security Guide for Release 4.7*, has been introduced to assist administrators in deploying SGD in a secure manner.
- **Translated documentation.** Localized documentation is now available in the following languages:
  - French
  - Japanese
  - Chinese (Simplified)

1.2.9. Changes to Supported Locales

For this release, the SGD Client and webtop are available in the following supported languages:

- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish
- Chinese (Simplified)
- Chinese (Traditional)

Chapter 2. System Requirements and Support

This chapter includes details of the system requirements and supported platforms for Oracle Secure Global Desktop (SGD) version 4.70.

2.1. SGD Server Requirements and Support

This section describes the supported platforms and requirements for SGD servers.

2.1.1. 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 interface 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.

2.1.2. Supported Installation Platforms for SGD

The following table lists the supported installation platforms for SGD.

Operating System	Supported Versions
Oracle Solaris on SPARC platforms	Solaris 10 8/11 (update 10) Solaris 11 Solaris 10 8/11 (update 10) Trusted Extensions Solaris 11 Trusted Extensions

Operating System	Supported Versions
Oracle Solaris on x86 platforms	Solaris 10 8/11 (update 10) Solaris 11 Solaris 108/11 (update 10) Trusted Extensions Solaris 11 Trusted Extensions
Oracle Linux (32-bit and 64-bit)	5.7 5.8 6.2 6.3

Oracle products certified on Oracle Linux are also certified and supported on Red Hat Enterprise Linux due to implicit compatibility between both distributions. Oracle does not run any additional testing on Red Hat Enterprise Linux products.

2.1.2.1. Operating System Modifications

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

2.1.2.1.1. Oracle Solaris

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

- You must install at least the End User Oracle Solaris distribution to get the libraries required by SGD. If you do not, SGD does not install.
- 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
  ```

2.1.2.1.2. 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 webtop 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.

2.1.2.1.3. 5250 and 3270 Applications

The following modifications are 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
```

2.1.2.2. Virtualization Support

The supported installation platforms for SGD are supported on a Type 1 (bare metal) hypervisor or a Type 2 (hosted) hypervisor, for example Oracle VM VirtualBox, VMWare, or Oracle VM Server for SPARC (previously called Sun Logical Domains or LDoms).

Installation in zones is supported for Oracle Solaris platforms. SGD can be installed either in the global zone, or in one or more non-global zones. Installation in both the global zone and a non-global zone is not supported.

On Oracle Solaris Trusted Extensions platforms, you must install SGD in a labeled zone. Do not install SGD in the global zone.

2.1.2.3. Retirements to Supported SGD Installation Platforms

The following table shows the SGD installation platforms that have been retired.

SGD Version	Platforms No Longer Supported
4.70	Red Hat Enterprise Linux 5.5, 5.6 Oracle Enterprise Linux 5.5, 5.6 Oracle Solaris 10 up to, and including, Solaris 10 9/10 (update 9)
4.60	OpenSolaris (all versions) Red Hat Enterprise Linux 5.0 to 5.4 Solaris 10 OS up to, and including, Solaris 10 5/09 (update 7) SUSE Linux Enterprise Server 10

2.1.3. Supported Upgrade Paths

Upgrades to version 4.70 of SGD are only supported from the following versions:

- Oracle Secure Global Desktop Software version 4.62.913
- Oracle Secure Global Desktop Software version 4.61.915
- Oracle Secure Global Desktop Software version 4.60.911

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

2.1.4. Java Technology Version

The following table shows the JDK versions included with SGD.

SGD Version	JDK Version
4.70	1.6.0_33
4.62	1.6.0_29
4.61	1.6.0_24
4.60	1.6.0_21

2.1.5. 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/ttasys -m ttasys
```

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

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

```
# su ttasys -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(ttasys) gid=1000(ttaserv) groups=1000(ttaserv)
```

2.1.6. 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 for Release 4.7* 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 Transmission Control Protocol/Internet Protocol (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

2.1.7. 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.

2.1.8. SGD Web Server

The SGD web server consists of an Apache web server and a Tomcat JavaServer Pages (JSP) technology container preconfigured for use with SGD.

The SGD web server consists of several components. The following table lists the web server component versions for recent releases of SGD.

Component Name	SGD Version 4.70	SGD Version 4.62	SGD Version 4.61	SGD Version 4.60
Apache HTTP Server	2.2.22	2.2.21	2.2.17	2.2.16
OpenSSL	1.0.0.j	1.0.0.e	1.0.0.d	1.0.0a
mod_jk	1.2.37	1.2.32	1.2.31	1.2.27
Apache Jakarta Tomcat	7.0.29	6.0.33	6.0.32	6.0.29
Apache Axis	1.4	1.4	1.4	1.4

The Apache web server includes all the standard Apache modules as shared objects.

The minimum Java Virtual Machine (JVM) software heap size for the Tomcat JSP technology container is 256 megabytes.

2.1.9. Supported Authentication Mechanisms

The following are the supported mechanisms for authenticating users to SGD:

- Lightweight Directory Access Protocol (LDAP) version 3
- Microsoft Active Directory
- Network Information Service (NIS)
- RSA SecurID

- Web server authentication (HTTP/HTTPS Basic Authentication), including public key infrastructure (PKI) client certificates

2.1.9.1. Supported Versions of Active Directory

Active Directory authentication and LDAP authentication are supported on the following versions of Active Directory:

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

2.1.9.2. Supported LDAP Directories

SGD supports version 3 of the standard LDAP protocol. You can use LDAP authentication with any LDAP version 3-compliant directory server. However, SGD only supports the following directory servers:

- Oracle Internet Directory 11gR1 (all 11.1.1.x.0 releases)
- Oracle Directory Server Enterprise Edition version 11gR1
- Microsoft Active Directory, as shown in Section 2.1.9.1, “Supported Versions of Active Directory”
- Sun Directory Server 6.3 or later

Other directory servers might work, but are not supported.

Novell eDirectory is no longer supported as an LDAP directory server.

2.1.9.3. Supported Versions of SecurID

SGD works with versions 4, 5, 6, and 7 of RSA Authentication Manager (formerly known as ACE/Server).

SGD supports system-generated PINs and user-created PINs.

2.1.10. SSL Support

SGD supports TLS version 1.0 and SSL version 3.0.

SGD supports Privacy Enhanced Mail (PEM) Base 64-encoded X.509 certificates. These certificates have the following structure:

```
-----BEGIN CERTIFICATE-----

...certificate...

-----END CERTIFICATE-----
```

SGD supports the Subject Alternative Name (`subjectAltName`) extension for SSL certificates. SGD also supports the use of the `*` wildcard for the first part of the domain name, for example `*.example.com`.

SGD includes support for a number of Certificate Authorities (CAs). The `/opt/tarantella/etc/data/cacerts.txt` file contains the X.500 Distinguished Names (DNs) and MD5 signatures of all the CA

certificates that SGD supports. Additional configuration is required to support SSL certificates signed by an unsupported CA. Intermediate CAs are supported, but additional configuration might be required if any of the certificates in the chain are signed by an unsupported CA.

SGD supports the use of external hardware SSL accelerators, with additional configuration.

SGD supports the following cipher suites:

- RSA_WITH_AES_256_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_3DES_EDE_CBC_SHA
- RSA_WITH_RC4_128_SHA
- RSA_WITH_RC4_128_MD5
- RSA_WITH_DES_CBC_SHA

2.1.11. Printing Support

SGD supports two types of printing: PDF printing and Printer-Direct printing.

For PDF printing, SGD uses Ghostscript to convert print jobs into Portable Document Format (PDF) files. Your Ghostscript distribution must include the `ps2pdf` program. For best results, install the latest version of Ghostscript on the SGD host.

SGD supports Printer-Direct printing to PostScript, Printer Command Language (PCL), and text-only printers attached to the user's client device. The SGD `tta_print_converter` script performs any conversion needed to format print jobs correctly for the client printer. The `tta_print_converter` script uses Ghostscript to convert from Postscript to PCL. To support this conversion, Ghostscript must be installed on the SGD server. For best results, download and install the additional fonts.

Ghostscript is not included with the SGD software.

2.2. Client Device Requirements and Support

This section describes the supported platforms and requirements for client devices.

2.2.1. Supported Client Platforms

The following table lists the supported client platforms and browsers for the SGD Client.

Caution

The client platform for the SGD Client must be a full desktop operating system. An individual application, such as a browser, is not a supported client platform.

Supported Client Platform	Supported Browsers
Microsoft Windows 7 (32-bit and 64-bit) [a]	Internet Explorer 8 Internet Explorer 9 Mozilla Firefox 3.6, 10.0.3:ESR, 11

Supported Client Platform	Supported Browsers
	Chrome 17
Microsoft Windows XP Professional SP3 (32-bit)	Internet Explorer 7 Internet Explorer 8 Mozilla Firefox 3.6, 10.0.3:ESR, 11 Chrome 17
Oracle Solaris on SPARC platforms Solaris 10 8/11 (update 10), Solaris 11	Mozilla Firefox 3.6, 10.0.3:ESR, 11 Chrome 17
Oracle Solaris on x86 platforms Solaris 10 8/11 (update 10), Solaris 11	Mozilla Firefox 3.6, 10.0.3:ESR, 11 Chrome 17
Oracle Solaris Trusted Extensions on SPARC platforms Solaris 10 8/11 (update 10), Solaris 11	Mozilla Firefox 3.6, 10.0.3:ESR, 11 Chrome 17
Oracle Solaris Trusted Extensions on x86 platforms Solaris 10 8/11 (update 10), Solaris 11	Mozilla Firefox 3.6, 10.0.3:ESR, 11 Chrome 17
Mac OS X 10.6 (latest version) and 10.7 [b]	Safari 5 Mozilla Firefox 3.6, 10.0.3:ESR, 11 Chrome 17
Oracle Linux 5.7, 5.8, 6.2, 6.3 (32-bit and 64-bit)	Mozilla Firefox 3.6, 10.0.3:ESR, 11 Chrome 17
Ubuntu 10.04, 12.04 (32-bit and 64-bit) [c]	Mozilla Firefox 3.6, 10.0.3:ESR, 11 Chrome 17

[a] On 64-bit client platforms, the 32-bit and 64-bit versions of Internet Explorer are supported.

[b] Mac OS X 10.8 is not supported as a client platform.

[c] On 64-bit Ubuntu Linux 12.04 platforms, the `ia32-libs` package is required.

Oracle products certified on Oracle Linux are also certified and supported on Red Hat Enterprise Linux due to implicit compatibility between both distributions. Oracle does not run any additional testing on Red Hat Enterprise Linux products.

The SGD Administration Console is not supported on Safari browsers.

Beta versions or preview releases of browsers are not supported.

Browsers must have the JavaScript programming language enabled.

To support the following functionality, browsers must have Java technology enabled:

- Downloading and installing the SGD Client automatically
- Determining proxy server settings from the user's default browser

If Java technology is not available, the SGD Client can be downloaded and installed manually. Manual installation is available for all supported client platforms.

Java Plug-in software versions 1.6 and 1.7 are supported as a plug-in for Java technology.

Note

For details of known issues when using Java Plug-in software version 1.7, see knowledge document ID 1487307.1 on My Oracle Support (MOS).

For best results, client devices must be configured for at least thousands of colors.

The SGD Client and webtop are available in the following supported languages:

- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish
- Chinese (Simplified)
- Chinese (Traditional)

2.2.1.1. Virtualization Support

The supported client platforms for SGD are supported on a Type 1 (bare metal) hypervisor or a Type 2 (hosted) hypervisor, for example Oracle VM VirtualBox, VMWare, or Oracle VM Server for SPARC (previously called Sun Logical Domains or LDoms).

2.2.1.2. Retirements to Supported Client Platforms

The following table shows the SGD Client installation platforms, browsers, and Java Plugin tools that have been retired.

SGD Version	Platforms No Longer Supported
4.70	Microsoft Windows Vista Red Hat Enterprise Linux 5.5 Desktop Oracle Solaris 10 up to, and including, 9/10 (update 9) Safari 4
4.60	Mac OS X 10.5 OpenSolaris (all versions) Red Hat Enterprise Linux Desktop 5.0 to 5.4 Solaris 10 OS up to, and including, 5/09 (update 7)

SGD Version	Platforms No Longer Supported
	Ubuntu 8 Firefox 2 Internet Explorer 6 Safari 2 Safari 3 Java Plugin tool version 1.5

2.2.2. Supported Proxy Servers

To connect to SGD using a proxy server, the proxy server must support tunneling. You can use HTTP, Secure (SSL) or SOCKS version 5 proxy servers.

For SOCKS version 5 proxy servers, SGD supports the Basic and No Authentication Required authentication methods. No server-side configuration is required.

2.2.3. PDF Printing Support

To be able to use PDF printing, a PDF viewer must be installed on the client device. SGD supports the following PDF viewers by default.

Client Platform	Default PDF Viewer
Microsoft Windows platforms	Adobe Reader, at least version 4.0
Oracle Solaris on SPARC platforms	GNOME PDF Viewer (`gpdf`) Adobe Reader (`acroread`)
Oracle Solaris on x86 platforms	GNOME PDF Viewer (`gpdf`)
Oracle Linux	GNOME PDF Viewer (`gpdf`) Evince Document Viewer (`evince`) X PDF Reader (`xpdf`)
Mac OS X	Preview App (`/Applications/Preview.app`)

Note

The Adobe Reader PDF viewer must support the `-openInNewWindow` command option. The Preview App PDF viewer must support the `open -a` command option.

To be able to use a supported PDF viewer, the application must be on the user's `PATH`.

Support for alternative PDF viewers can be configured in the user's client profile.

2.2.4. Supported Smart Cards

SGD works with any Personal Computer/Smart Card (PC/SC)-compliant smart card and reader supported for use with Microsoft Remote Desktop services.

2.3. SGD Gateway Requirements and Support

This section describes the supported platforms and requirements for the SGD Gateway.

2.3.1. Supported Installation Platforms for the SGD Gateway

The supported installation platforms for the *SGD Gateway host* are shown in the following table.

Operating System	Supported Versions
Oracle Solaris on SPARC platforms	Solaris 10 8/11 (update 10) Solaris 11
Oracle Solaris on x86 platforms	Solaris 10 8/11 (update 10) Solaris 11
Oracle Linux (32-bit and 64-bit)	5.7 5.8 6.2 6.3

Oracle products certified on Oracle Linux are also certified and supported on Red Hat Enterprise Linux due to implicit compatibility between both distributions. Oracle does not run any additional testing on Red Hat Enterprise Linux products.

By default, the SGD Gateway is configured to support a maximum of 100 simultaneous HTTP connections and 512 simultaneous Adaptive Internet Protocol (AIP) connections. The JVM memory size is optimized for this number of connections. Appendix C of the *Oracle Secure Global Desktop Gateway Administration Guide for Release 4.7* has details of how to tune the Gateway for the expected number of users.

2.3.1.1. Virtualization Support

The supported installation platforms for the SGD Gateway are supported on a Type 1 (bare metal) hypervisor or a Type 2 (hosted) hypervisor, for example Oracle VM VirtualBox, VMWare, or Oracle VM Server for SPARC (previously called Sun Logical Domains or LDoms).

On Oracle Solaris platforms, installation in zones is supported. The SGD Gateway can be installed either in the global zone, or in one or more non-global zones. Installation in both the global zone and a non-global zone is not supported.

2.3.1.2. Retirements to Supported Gateway Installation Platforms

The following table shows the SGD Gateway installation platforms that have been retired.

SGD Version	Platforms No Longer Supported
4.70	Oracle Solaris 10 up to, and including, 9/10 (update 9) Red Hat Enterprise Linux 5.5 Oracle Enterprise Linux 5.5

SGD Version	Platforms No Longer Supported
4.60	OpenSolaris (all versions) Red Hat Enterprise Linux 5.0 to 5.4 Solaris 10 OS up to, and including, 5/09 (update 7) SUSE Linux Enterprise Server 10

2.3.2. SGD Server Requirements for the SGD Gateway

The following requirements apply for the SGD servers used with the SGD Gateway:

- **Secure mode.** By default, the SGD Gateway uses secure connections to SGD servers. You must enable secure connections on your SGD servers. Firewall forwarding must not be enabled.

  In a standard installation, an SGD server is configured automatically to use secure connections.

- **SGD version.** The SGD servers must be running at least version 4.5 of SGD. It is best to use version 4.7 of the Gateway.

- **Clock synchronization.** It is important that the system clocks on the SGD servers and the SGD Gateway are in synchronization. Use Network Time Protocol (NTP) software, or the `rdate` command, to ensure that the clocks are synchronized.

2.3.3. Apache Web Server

The Apache web server supplied with the SGD Gateway is Apache version 2.2.22. It includes the standard Apache modules for reverse proxying and load balancing. The modules are installed as Dynamic Shared Object (DSO) modules.

2.3.4. Java Technology Version

The SGD Gateway includes Java Runtime Environment (JRE) version 1.6.0_33.

2.3.5. SSL Support

SSL support for the SGD Gateway is provided by the Java Runtime Environment (JRE) supplied with the Gateway. See the Java Platform documentation for more details.

The SGD Gateway supports Privacy Enhanced Mail (PEM) Base 64-encoded X.509 certificates. These certificates have the following structure:

```
-----BEGIN CERTIFICATE-----

...certificate...

-----END CERTIFICATE-----
```

The SGD Gateway supports the use of external hardware SSL accelerators, with additional configuration.

By default, the SGD Gateway is configured to support the following high grade cipher suites for SSL connections:

- SSL_RSA_WITH_RC4_128_MD5

- SSL_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

The following cipher suites are also supported, but must be configured by the user as shown in the *Oracle Secure Global Desktop Gateway Administration Guide for Release 4.7*.

- SSL_RSA_WITH_DES_CBC_SHA
- SSL_DHE_RSA_WITH_DES_CBC_SHA
- SSL_DHE_DSS_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA

2.4. Application Requirements and Support

This section describes the supported platforms and requirements for displaying applications through SGD.

2.4.1. Supported Applications

You can use SGD to access the following types of applications:

- Microsoft Windows
- X applications running on Oracle Solaris, Linux, HP-UX, and AIX application servers
- Character applications running on Oracle Solaris, Linux, HP-UX, and AIX application servers
- Applications running on IBM mainframe and AS/400 systems
- Web applications, using HTML and Java technology

SGD supports the following protocols:

- Microsoft Remote Desktop Protocol (RDP) at least version 5.2

- X11
- HTTP
- HTTPS
- SSH at least version 2
- Telnet VT, American National Standards Institute (ANSI)
- TN3270E
- TN5250

2.4.2. Supported Installation Platforms for the SGD Enhancement Module

The SGD Enhancement Module is a software component that can be installed on an application server to provide the following additional functionality when using applications displayed through SGD:

- Advanced load balancing
- Client drive mapping (UNIX or Linux platforms only)
- Seamless windows (Windows platforms only)
- Audio (UNIX or Linux platforms only)

The following table lists the supported installation platforms for the SGD Enhancement Module.

Operating System	**Supported Versions**
Microsoft Windows (64-bit)	Windows Server 2008 R2
Microsoft Windows (32-bit and 64-bit)	Windows Server 2008 Windows Server 2003 R2 Windows Server 2003
Oracle Solaris on SPARC platforms	Solaris 8, 9, 10, 11 Solaris Trusted Extensions 10, 11
Oracle Solaris on x86 platforms	Solaris 10, 11 Solaris Trusted Extensions 10, 11
Oracle Linux (32-bit and 64-bit)	5, 6
SUSE Linux Enterprise Server (32-bit and 64-bit)	10, 11

Oracle products certified on Oracle Linux are also certified and supported on Red Hat Enterprise Linux due to implicit compatibility between both distributions. Oracle does not run any additional testing on Red Hat Enterprise Linux products.

On Oracle Solaris Trusted Extensions platforms, only advanced load balancing is supported. Audio and CDM are *not supported*.

Application servers that are not supported platforms for the SGD Enhancement Module can be used with SGD to access a supported application type using any of the supported protocols.

2.4.2.1. Virtualization Support

The supported installation platforms for the SGD Enhancement Module are supported on a Type 1 (bare metal) hypervisor or a Type 2 (hosted) hypervisor, for example Oracle VM VirtualBox, VMWare, or Oracle VM Server for SPARC (previously called Sun Logical Domains or LDoms).

Installation in zones is supported for Oracle Solaris platforms. SGD can be installed in the global zone, or in one or more non-global zones. Installation in both the global zone and a non-global zone is *not supported*.

On Oracle Solaris Trusted Extensions platforms, you must install SGD in a labeled zone. Do not install SGD in the global zone.

2.4.2.2. Retirements to Supported Installation Platforms for the SGD Enhancement Module

The following table shows the installation platforms for the SGD Enhancement Module that have been retired.

SGD Version	Platforms No Longer Supported
4.70	Red Hat Enterprise Linux 5
4.60	OpenSolaris (all versions) Windows Vista Business Windows Vista Professional Windows XP Professional

Note

The SGD Enhancement Module no longer provides functionality that is supported on Windows 7 and Windows XP platforms. These platforms are still supported as an application server platform, see Section 2.4.3, “Microsoft Windows Remote Desktop Services” .

2.4.3. Microsoft Windows Remote Desktop Services

SGD does not include licenses for Microsoft Windows Remote Desktop Services. If you access Remote Desktop Services functionality provided by Microsoft operating system products, you need to purchase additional licenses to use such products. Consult the license agreements for the Microsoft operating system products you are using to determine which licenses you must acquire.

Note

Before Microsoft Windows Server 2008 R2, Remote Desktop Services was called Terminal Services.

SGD supports RDP connections to the following versions of Microsoft Windows:

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003

- Windows 7 SP1
- Windows XP Professional SP3

On Windows 7 and Windows XP platforms, only full Windows desktop sessions are supported. Running individual applications is not supported. Seamless windows are also not supported.

The features supported by SGD depend on whether you connect using RDP or Oracle VM VirtualBox RDP (VRDP), as shown in the following table.

Table 2.1. Comparison of Features Supported by SGD When Using RDP and VRDP

Feature	RDP	VRDP
Audio recording (input audio)	✓	✓
Audio redirection	✓	✓
Clipboard redirection	✓	✓
COM port mapping	✓	✗
Compression	✓	✗
Drive redirection (client drive mapping)	✓	✗
Multi-monitor	✓	✗
Network security (encryption level)	✓	✓
Session directory	✓	✗
Smart card device redirection	✓	✗
Time zone redirection	✓	✗
Windows printer mapping (client printing)	✓	✗

2.4.3.1. Audio Quality

Windows Server 2008 R2 and Windows 7 support audio bit rates of up to 44.1 kHz. By default, SGD supports bit rates of up to 22.05 kHz. To support bit rates of up to 44.1 kHz, in the Administration Console go to the Global Settings, Client Device tab and select the Windows Audio: High Quality option.

2.4.3.2. Audio Recording Redirection

Audio recording redirection is supported for Microsoft Windows Server 2008 R2 and Microsoft Windows 7 application servers.

To record audio in a Windows Remote Desktop Services session, audio recording redirection must be enabled on the application server. By default, audio recording redirection is disabled.

To enable audio recording for Microsoft Windows 7 Enterprise application servers, you also need to add the following registry entry to the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp` key.

```
"fDisableAudioCapture"=dword:00000000
```

2.4.3.3. Color Depth

SGD supports 8-bit, 16-bit, 24-bit, and 32-bit color depths in a Windows Remote Desktop Services session.

32-bit color is available on Windows Server 2008, Windows Server 2008 R2, and Windows 7 platforms. To display 32-bit color, the client device must be capable of displaying 32-bit color.

15-bit color depths are not supported. If this color depth is specified on the Remote Desktop Session Host, SGD automatically adjusts the color depth to 8-bit.

2.4.3.4. Encryption Level

You can only use the Low, Client-compatible, or High encryption levels with SGD. SGD does not support the Federal Information Processing Standards (FIPS) encryption level.

2.4.3.5. Transport Layer Security

From Microsoft Windows Server 2003, you can use Transport Layer Security (TLS) for server authentication, and to encrypt Remote Desktop Session Host communications.

2.4.3.6. Network Level Authentication

If the Remote Desktop Session Host supports Network Level Authentication (NLA) using CredSSP, you can use NLA for server authentication.

2.4.4. X and Character Applications

To run X and character applications, SGD must be able to connect to the application server that hosts the application. SGD supports SSH and Telnet as connection methods. SSH is the best for security.

SGD works with SSH version 2 or later. Because of SSH version compatibility problems, use the same major version of SSH, either version 2 or version 3, on all SGD hosts and application servers.

If you are using SSH to connect to X applications, you must enable X11 forwarding. You can do this either in your SSH configuration or by configuring the application in SGD. The *Oracle Secure Global Desktop Administration Guide for Release 4.7* has details on using SSH with SGD.

SGD supports the X Security extension. The X Security extension only works with versions of SSH that support the `-Y` option. For OpenSSH, this is version 3.8 or later

2.4.4.1. X11 Software

SGD includes an X protocol engine (XPE) implementation based on the X.Org Foundation X Server release X11R7.6.

The XPE implementation is based on the following X.org foundation sources:

- `xorg-server 1.9.3`
- `xrandr 1.3`
- `xkeyboard-config 2.1`

The following versions of X.org dependencies are used:

- `Mesa 7.9.2`
- `pixman 0.20.2`

2.4.4.2. Supported X Extensions

SGD supports the following X extensions for X applications:

- BIG-REQUESTS

- BLINK
- DAMAGE
- DEC-XTRAP
- DOUBLE-BUFFER
- Extended-Visual-Information
- GLX
- MIT-SCREEN-SAVER
- MIT-SHM
- MIT-SUNDRY-NONSTANDARD
- NATIVE-WND
- RDP
- RECORD
- RENDER
- SCO-MISC
- SECURITY
- SGI-GLX
- SHAPE
- SYNC
- TOG-CUP
- X-Resource
- XC-APPGROUP
- XC-MISC
- XFIXES
- XFree86-Bigfont
- XTEST
- XTTDEV
- KEYBOARD
- RANDR
- XINERAMA

The following X extension is *not* supported:

- XVIDEO

2.4.4.3. Character Applications

SGD supports VT420, Wyse 60, or SCO Console character applications

2.4.5. Virtual Desktop Infrastructure

SGD uses a type of object called a *dynamic application server* to represent a virtual server broker (VSB). SGD uses the VSB to obtain a list of application servers that can run an application.

SGD includes brokers that enable you to give users access to desktops provided by an Oracle Virtual Desktop Infrastructure (Oracle VDI) server.

Integration with Oracle VDI is also supported by configuring a Windows application object, as described in the *Oracle Secure Global Desktop Administration Guide for Release 4.7*.

This release of SGD supports the following versions of Oracle VDI:

- Oracle VDI 3.4.1
- Oracle VDI 3.3.2

2.5. Removed Features

The following features have been removed in the 4.70 release:

- **CALs license pool.** Client Access Licenses (CALs) for non-Windows client devices are no longer stored in a license pool on the SGD server. The `tarantella tscal` command used to manage the license pool is no longer available.
- **Local launch.** Support for running an application on Windows client devices (known as local launch) has been removed. The Local Client Launch (`--trylocal`) attribute has been deprecated.

  The `localx` setting is no longer supported for the Window Type (`--displayusing`) attribute.

  The Check for Local X Server profile setting is no longer available.
- **Windows domain authentication.** Windows domain authentication is no longer supported as a method for authenticating SGD users. The Windows Domain Controller (`--login-nt`) attribute has been deprecated.

  Active Directory authentication can be used as an alternative to Windows domain authentication.
- **Using `rexec` to start applications.** `rexec` is no longer supported as an option for the Connection Method (`--method`) attribute.
- **Display attributes.** The following X Protocol Engine (XPE) and X display attributes have been deprecated:
  - RGB Database (`--xpe-rgbdatabase`). The XPE now has built-in support for X11 color names.
  - Euro Character (`--euro`). The euro character is now supported by default.
  - Keyboard Map: Locked (`--lockkeymap`). The XKB extension is now used for keyboard support.
  - Keyboard Map (`--xpe-keymap`). The XKB extension is now used for keyboard support.

- Keyboard Map (`--keymap`). This attribute is now only available using the command line.

2.5.1. Changes in the Next Release of SGD

The following SGD features might not be available in the next release of SGD:

- Supported client platforms and browsers: Ubuntu Linux10.04 and Mac OS X 10.6 may not be supported as client platforms. Support for Mac OS X 10.8 will be added in the next release.

  For browsers, Internet Explorer 7 may not be supported.

- LDAP directory servers: Sun Directory Server may not be supported.
- SGD load-balancing JSP (`swcd.jsp`): The SGD Gateway provides a much better solution for load-balanced deployments.
- Optional use of browser cookies when accessing SGD.
- SecurID authentication: Use the RSA Authentication Agent with third-party authentication instead.
- Integrated mode for the SGD Client.
- The `tarantella cache` command.

Chapter 3. Known Issues, Bug Fixes, and Documentation Issues

This chapter contains information about known issues, bug fixes, and documentation issues for Oracle Secure Global Desktop (SGD). Details on providing feedback and reporting bugs are also included.

3.1. Known Bugs and Issues

This section lists the known bugs and issues for the SGD 4.70 release.

3.1.1. 2205237 – Seamless Windows Display Problems When Restarting a Disconnected Session

Problem: Issues with seamless windows might be encountered when the user restarts a Windows application after closing it down. The problem is seen when the application is hosted on a Windows Server 2008 R2 server.

Cause: A known problem with some versions of the SGD Enhancement Module.

Solution: Ensure that the version of the SGD Enhancement Module running on the Windows application server is the same as the SGD server version.

3.1.2. 6555834 – Java Technology is Enabled For Browser But Is Not Installed On Client Device

Problem: If Java technology is enabled in your browser settings, but Java Plug-in software is not installed on the client device, the SGD webtop does not display. The login process halts at the splash screen.

Cause: SGD uses the browser settings to determine whether to use Java technology.

Solution: Install the Java Plug-in software and create a symbolic link from the browser plug-ins directory to the location of the Java Virtual Machine (JVM) software. Refer to your browser documentation for more information.

3.1.3. 6831480 – Backup Primaries List Command Returns an Error

Problem: Using the `tarantella array list_backup_primaries` command on an SGD server that has been stopped and then detached from an array returns a "Failed to connect" error.

Cause: A known issue.

Solution: Restart the detached SGD server before using the `tarantella array list_backup_primaries` command.

3.1.4. 6863153 – HyperTerminal Application Hangs in a Relocated Windows Desktop Session

Problem: Users running the HyperTerminal application in a Windows desktop session experience problems when they try to resume the desktop session from another client device. The HyperTerminal application is unresponsive and cannot be closed down.

Cause: A known issue with HyperTerminal when resuming Windows desktop sessions from another client device (also called “session grabbing”).

Solution: Close down the HyperTerminal application before you resume the Windows desktop session from another client device.

3.1.5. 6937146 – Audio Unavailable for X Applications Hosted on 64-Bit Linux Application Servers

Problem: Audio might not play in X applications that are hosted on 64-bit Linux application servers. The issue is seen for X applications that are hard-coded to use the `/dev/dsp` or `/dev/audio` device, and the Audio Redirection Library (`--unixaudiopreload`) attribute is enabled.

Cause: A known issue. A 64-bit SGD Audio Redirection Library is not included in the SGD Enhancement Module.

Solution: No known solution at present.

3.1.6. 6942981 – Application Startup is Slow on Solaris Trusted Extensions

Problem: On Oracle Solaris Trusted Extensions platforms, startup times for Windows applications and X applications might be longer than expected.

Cause: By default, the X Protocol Engine attempts to connect to X display port 10. This port is unavailable when using Solaris Trusted Extensions. After a period of time, the X Protocol Engine connects on another X display port and the application starts successfully.

Solution: Do either of the following:

- Change the default minimum display port used by the SGD server.

  Configure the following setting in the `xpe.properties` file in the `/opt/tarantella/var/serverconfig/local` directory on the SGD server:

  ```
  tarantella.config.xpeconfig.defaultmindisplay=11
  ```

  Restart the SGD server after making this change.

- Exclude the unavailable port from use by the X Protocol Engine.

  In the Administration Console, go to the Protocol Engines, X tab for each SGD server in the array and type `-xport` *`portnum`* in the Command-Line Arguments field, where *`portnum`* is the TCP port number to exclude.

  Alternatively, use the following command:

  ```
  $ tarantella config edit --xpe-args "-xport portnum"
  ```

  For example, to exclude X display port 10 from use by the X Protocol Engine:

  ```
  $ tarantella config edit --xpe-args "-xport 6010"
  ```

  The changes made take effect for new X Protocol Engines only. Existing X Protocol Engines are not affected.

3.1.7. 6957820 – SGD Client Hangs When Using Smart Card Authentication for Windows Applications

Problem: When using a smart card to log in to a Windows application session from a Ubuntu Linux 10.04 client device, the SGD Client hangs after the user exits the authenticated application session. The user might not be able to start any further applications or log out from SGD.

Cause: A known issue with version 1.5.3 of PCSC-Lite on Ubuntu client platforms.

Solution: Update to the latest version of PCSC-Lite on the client device.

3.1.8. 6962970 – Windows Client Device Uses Multiple CALs

Problem: A Windows client device is allocated multiple client access licences (CALs). A CAL is incorrectly allocated each time a Windows application is started.

Cause: A known issue if the `HKEY_LOCAL_MACHINE\Software\Microsoft\MSLicensing` key or any of its subkeys are missing from the Windows registry on a client device. This issue affects Microsoft Windows 7 platforms.

Solution: Recreate the missing keys, by starting the Remote Desktop Connection with administrator privileges. See Microsoft Knowledge Base article 187614 for more details.

3.1.9. 6970615 – SecurID Authentication Fails for X Applications

Problem: SecurID authentication for X applications fails when using the RSA Authentication Agent for PAM. The issue is seen with X applications that are configured to use telnet as the Connection Method.

Cause: A known issue when using the RSA Authentication Agent for PAM.

Solution: Configure the X application object to use SSH as the Connection Method.

3.1.10. 7004887 – Print to File Fails for Windows Client Devices

Problem: When users select the Print to File menu option in a Windows application displayed through SGD, the print job remains on hold in the print queue on the client device. The issue is seen on Windows Vista and Windows 7 client devices.

Cause: A known issue with some versions of Windows.

Solution: A workaround for Windows Vista is described in Microsoft Knowledge Base article 2022748.

3.1.11. 12300549 – Home Directory Name is Unreadable For Some Client Locales

Problem: When using client drive mapping in SGD, the name of the user's home directory may include unreadable characters. By default, a user's home directory is mapped to a drive called "My Home".

The issue has been seen on non-Windows client devices configured with a non-English client locale, such as `ja_JP.UTF-8`.

Cause: A known issue for some client locales.

Solution: No known solution at present.

3.1.12. 13068287 – 16-bit Color OpenGL Application Issues

Problem: OpenGL applications, such as three-dimensional graphics programs, do not start or do not display correctly when published through SGD. The issue is seen when the X application object is configured with a 16-bit Color Depth setting.

Cause: A known issue when displaying OpenGL applications using 16-bit color.

Solution: The workaround is to display the application using a 24-bit Color Depth setting.

3.1.13. 13117149 – Accented Characters in Active Directory User Names

Problem: Active Directory authentication fails for user names that contain accented characters, such as the German umlaut character (ü). The issue has been seen when using Windows Server 2003 R2.

The following error is shown in the log output when using the `server/login/info` log filter:

```
javax.security.auth.login.LoginException: Integrity check on decrypted field failed (31)
```

Cause: Active Directory authentication uses the Kerberos authentication protocol. This is a known issue when Kerberos authentication is configured to use DES encryption.

Solution: The workaround is to disable the use of DES encryption in the `krb5.conf` Kerberos configuration file on the SGD server.

Include the following lines in the `[libdefaults]` section of the `krb5.conf` file.

```
  [libdefaults]
    default_tgs_enctypes =  rc4-hmac des3-cbc-sha1 aes128-cts aes256-cts
    default_tkt_enctypes =  rc4-hmac des3-cbc-sha1 aes128-cts aes256-cts
```

3.1.14. 13354844, 14032389, 13257432, 13117470 – Display Issues on Ubuntu Client Devices

Problem: The following display issues might be seen on client devices running Ubuntu Linux.

- The kiosk mode minimize button does not work if you are not using a window manager or if you are using a minimalist window manager, such as `evilwm`.
- The button for toggling between kiosk mode and an Integrated Window display does not work.
- The SGD Client task bar icon is not shown when using the Unity desktop.
- A seamless windows application that should span multiple monitors is instead displayed with scroll bars on a single monitor.

Cause: Known issues when using a Ubuntu Linux client device.

Solution: Use one of the following workarounds.

- To use the kiosk mode window decoration, the window manager must implement the change state protocol from Normal to Iconify. Ensure that you are running a suitable window manager.
- Use the Ctrl+Alt+Break keyboard shortcut to toggle between kiosk mode and an Integrated Window display.
- To show the SGD Client task bar icon, add the SGD Client application to the whitelist for the Unity desktop.

  Start the `dconf-editor` and go to the Desktop → Unity → Panel dialog. Add `Oracle Secure Global Desktop` to the list of applications.
- There is no known solution for the seamless windows issue on multiple monitors.

3.1.15. 13360596 – Pass-Through Authentication Issue With Oracle VDI

Problem: When using the VDI broker with Oracle VDI, an error is displayed when authenticating to the Windows desktop. Users must enter their password every time that they start a desktop.

Cause: A known issue with how SGD caches user credentials for certain configurations of Oracle VDI.

Solution: On the SGD server, edit the application launch script at `/opt/tarantella/webserver/tomcat/tomcat-version/webapps/sgd/applicationLaunch/appLaunch.jsp`.

Locate the following statement, at line 484 in `appLaunch.jsp`:

```
if (chosenCandidate.getUsername() == null)
```

Edit the statement, to read as follows:

```
if (chosenCandidate.getUsername() == null || chosenCandidate.getPassword() == null)
```

3.1.16. 13971245 – Package Removal Issues on Oracle Solaris 11

Problem: SGD might not uninstall cleanly on Oracle Solaris 11 platforms. After uninstalling SGD, entries for SGD packages are still present in the Solaris package database.

Cause: A known issue when you are using the Image Packaging System (IPS) included with Oracle Solaris 11 and you remove SGD.

Solution: The workaround is to use the SGD package database repair script `pkgdbfix.sh` after uninstalling SGD. This script is included in the `/opt/tarantella/etc/data` directory on an SGD server.

Log in as superuser (root) and do the following:

- Uninstall SGD and check for SGD package entries in the Solaris package database.

  ```
  # pkgchk -l tta
  # pkgchk -l tta.2
  ```

- If any package entries are reported using either of the previous commands, repair the package database.

  ```
  # sh pkgdbfix.sh package-instance
  ```

  where *`package-instance`* is the reported package instance, either `tta` or `tta.2`.

3.1.17. 14026511 – VDI Broker Connections Fail After an Oracle VDI Upgrade

Problem: After an Oracle VDI host has been upgraded or reconfigured, users might not be able to connect to their Oracle VDI desktops using the VDI broker.

Cause: When using the VDI broker, connections to the Oracle VDI host are secured using a self-signed SSL certificate for the web services API.

Whenever you reconfigure or upgrade Oracle VDI on a host, the web services self-signed certificate is regenerated and the existing SSL certificate is not preserved. In addition, when you upgrade, the host name (subject) used in the web services SSL certificate might change.

Solution: Use one of the following workarounds:

- Back up the web services certificate keystore on the Oracle VDI host before upgrading or reconfiguring. Restore the keystore from backup after you have made changes to the Oracle VDI installation.

  This process is described in the Oracle VDI documentation.

- Reconfigure the VDI broker as follows:

- Import the web services SSL certificate for *each Oracle VDI host* into the certificate truststore on *each SGD server*. Depending on your configuration, the truststore is either the CA certificate truststore or a dedicated truststore.
- Reconfigure the VDI broker to use the host names that appear in the web services SSL certificates.

  Change the `preferredhosts` and `failoverhosts` settings to use the new host names.

3.1.18. 14021467 – Webtop Language Selection Issue

Problem: Typically, users can select a preferred language from the list on the SGD Welcome Page. They then click Log in to access a webtop in that language.

After selecting a language at the SGD Welcome Page, users may not be able to select a different language for subsequent logins.

Cause: A known issue with caching of the preferred language selection.

Solution: Use one of the following workarounds:

- Clear your browser cache before selecting a different language.
- Locate the following text, at line 66 in the `localeutils.jsp` file:

  ```
    prefLang = (String) pageContext.getAttribute(PREF_LANG, PageContext.SESSION_SCOPE);
  ```

  The `localeutils.jsp` file is in the `/opt/tarantella/webserver/tomcat/`*`tomcat-version`*`/webapps/sgd/resources/jsp` directory on the SGD server.
- Edit the file, to read as follows:

  ```
  if (httpServletRequest.getParameter(LANG_SELECTED) == null)
    prefLang = (String) pageContext.getAttribute(PREF_LANG, PageContext.SESSION_SCOPE);
  ```

3.1.19. 14085800 – Active Directory Aged Password Handling Issue

Problem: Following expiry of their Active Directory password, users are able to update their password when prompted by SGD. However, the updated password is not always stored correctly in the password cache.

This means that some users might be prompted for authentication credentials every time that they start an application hosted on a Windows application server.

The issue is seen when the following are true:

- SGD is configured to automatically try the user's password when logging in to an application server, if the password has been cached. SGD does this by default.
- The Active Directory service object has the password expiry setting (`--check-pwd-policy`) enabled.

Cause: A known issue with how SGD handles aged passwords for Active Directory.

Solution: Use the following workaround.

- Disable the password expiry feature for the service object. For example:

  ```
  $ tarantella service edit --name ad1-east --check-pwd-policy 0
  ```
- Configure the Domain Name attribute for the Windows application object. For example:

```
$ tarantella object edit --name obj --ntdomain east.example.com
```

3.1.20. 14147506 – Array Resilience Fails if the Primary Server is Changed

Problem: Array resilience may fail if you change the primary server while the array is in a repaired state. The array is in a repaired state when the failover stage has completed.

After the recovery stage of array resilience, when uncontactable servers rejoin the array, communications to the other array members may not work.

The issue is seen when secure intra-array communication is enabled for the array.

Cause: A known issue with array resilience when secure intra-array communication is used. By default, secure intra-array communication is enabled for an SGD server.

Solution: No known solution. If possible, avoid changing the array structure during the array resilience process.

3.1.21. 14221098 – Konsole Application Fails to Start on Oracle Linux

Problem: The KDE `Konsole` terminal emulator application fails to start when configured as an X application object in SGD.

The issue is seen when the application is hosted on an Oracle Linux 6 platform.

Cause: A known issue when running `Konsole` on Oracle Linux 6. The issue is caused by the application process forking on start up.

Solution: The workaround is to use the `--nofork` command option when starting `Konsole`.

In the Administration Console, go to the Launch tab for the X application object and enter `--nofork` in the Arguments for Command field.

3.1.22. 14237565 – Page Size Issue When Printing on Non-Windows Client Devices

Problem: Print jobs are not delivered to the client printer in the correct page format. For example, a print job for an A4 page size document is delivered to the client printer as a Letter page size document. Depending on the client printer configuration, this might cause the print job to fail.

The issue is seen when using Linux and Mac OS X client devices.

Cause: A known issue when printing to some non-Windows client devices.

Solution: Some client printers can be configured to ignore the page size format.

A workaround is to use PDF printing when printing from SGD.

3.1.23. 14287570 – Microsoft Windows Server 2003 Applications Limited to 8-Bit Color Depth for Large Screen Resolutions

Problem: For Microsoft Windows Server 2003 applications, the display color depth on the client device is limited to 8-bit for large screen resolutions. The issue is seen when screen resolutions are higher than 1600 x 1200 pixels.

Cause: A known issue with Windows Server 2003 Remote Desktop Services sessions.

Solution: See Microsoft Hotfix 942610 for details of how to increase the color depth to 16-bit.

3.1.24. 14287730 – X Error Messages When Shadowing From the Command Line

Problem: Error messages similar to the following might be seen when shadowing an application session from the command line, using the `tarantella emulatorsession shadow` command.

```
X Error:  BadImplementation
  Request Major code 152 (RANDR)
  Request Minor code 8 ()
  Error Serial #209
  Current Serial #209
```

Shadowing works as expected, despite the error messages.

Cause: A known issue if the X server on the client device does not implement session resizing.

Solution: The errors are benign and can be ignored.

3.1.25. 14404371 – User Input Characters in the Authentication Dialog Are Unreadable

Problem: When a user attempts to enter authentication credentials using the SGD authentication dialog, some input characters might be unreadable. The issue is seen on non-Windows client devices where the user credentials contain multibyte characters, such as European language characters.

The SGD authentication dialog is shown when the user holds down the Shift key when clicking an application link on the webtop.

Cause: A known issue with how the SGD Client sets the font list on some client devices.

Solution: Use the following workaround.

- On the client device, create a font specification file with the following contents:

  ```
  *XmTextField*fontList: -*-*-medium-r-normal-*-*-120-*-*-*-*-*-*
  ```

- Make the fonts available on the client device.

  ```
  # xrdb -merge filename
  ```

  where *`filename`* is the name of the font specification file.

  Alternatively, you can add the font specification to an `.Xresources` file in your home directory.

3.1.26. 14408025 – SGD Client Exits Unexpectedly on Ubuntu Linux

Problem: On Ubuntu Linux 12 client devices, the SGD Client might exit unexpectedly. This means that users have to resume or restart their applications.

Cause: The issue is caused by a missing Enlightened Sound Daemon (ESD) library, `libesd.so`.

Solution: Install the missing library on the client device as follows:

```
# apt-get install libesd0
```

3.1.27. 14472019 – SGD Does Not Start on System Boot Up

Problem: On Oracle Linux 6 platforms, SGD is not started automatically when the SGD host is started up.

When the SGD host is shut down, SGD services are not stopped cleanly.

Cause: The issue is caused by a change in system startup architecture introduced in Oracle Linux 6. This means that the required symbolic links are not created automatically when you install SGD.

Solution: Add a symbolic link as follows:

```
# ln -s /etc/init.d/sun.com-sgd-base /etc/rc3.d/S90sun.com-sgd-base
```

3.2. Bug Fixes in Version 4.70

The following table lists the significant bugs that are fixed in the 4.70 release.

Table 3.1. Bugs Fixed in the 4.70 Release

Reference	Description
14399820	APPLICATION LAUNCHES FAIL WHEN USING SECURID ON APPLICATION SERVER
14377391	SGD CLIENT IN ORACLE LINUX 5.8 SUN RAY SESSION CRASHES ON START UP
14375562	TTATCC DOES NOT INTEGRATE WITH SUN RAY LICENSE STORE
14360939	CLIENT WINDOWS MANAGEMENT FOCUS IS NOT SET CORRECTLY WHEN A WINDOW IS CLOSED
14341167	WARNING MESSAGES SEEN WHEN RESTARTING TARANTELLA ON SOLARIS SPARC SGD SERVER
14324111	NULL POINTER EXCEPTION IN PROXY.CONNECTION.START
14309113	SEAMLESS WINDOWS APPLICATION, MENUS NOT SHOWN PROPERLY ON MULTI MONITOR
14303042	TTATSC CRASHES WHEN VIEWING CERTAIN URLS WITH WIN 7 APPLICATION SERVER (PORT OF 14097708)
14282154	WE SHOULD DOCUMENT HOW TO ENABLE SECURE COOKIES WITH PLAIN TEXT CONNECTIONS
14273752	SGD CLIENT SEGMENTATION FAULTS WHEN LAUNCHING A SEAMLESS WINDOWS APP FROM A UBUNTU 11.10 CLIENT
14272631	REPAINT ISSUE WHEN GRABBING A SESSION TO WINDOWS FROM UBUNTU LINUX
14225437	DOCUMENT VERSIONS OF X11 SOFTWARE
14221098	PROBLEMS RUNNING KONSOLE ON OEL 6.2
14215152	LOGIN BUTTON ON MAIN ENTRY PAGE IS NOT LOCALIZED
14213904	OVERRIDE PROXY SETTING DOES NOT WORK
14203183	LD.SO.1: TTAXTEXTCONV: FATAL: LIBICONV.SO.2: OPEN FAILED
14202226	WINDOWS APPLICATION EXITS WHEN SCREEN SAVER APPEARS IN THE APPLICATION
14202097	CLASSROOM OBJECT FAILS TO LAUNCH WHEN X AUTHORIZATION FOR X DISPLAY IS ENABLED
14194633	COMMAND NOT FOUND ERROR ON TRYING TO SHADOW A CHARACTER OR SUSPENDED APPLICATION FROM CLI
14194487	SEGMENTATION FAULT IS SEEN ON CLOSING A SHADOWED SESSION LAUNCHED WITH --SILENT OPTION
14174406	CLIENTSESSIONOBJECT.FORWARDREQUEST DROPS ONE CONNECTION, TWO IF PEER SSL ENABLED

Reference	Description
14169371	JDEVELOPER CRASHES THE TTAXPE
14169009	MAC OS X CLIENT SEGMENTATION FAULT ON CHANGING PROFILE SETTINGS
14151185	SETUP LOG ERROR FOR 3270 AND 5250 APPLICATIONS CREATED WITH LOCKKEYMAP ARGUMENT
14128209	VARIOUS SEAMLESS WINDOWS TOGGLE PROBLEMS UNDER UNIX
14124560	SGD CLIENT CORE DUMP FOR COMMAND LINE START UP
14124146	ORACLE SGD BANNER IS MISALIGNED
14123398	SGD CLIENT NOSTARTIMMEDIATE FLAG NOT WORKING
14119028	TTATSC USES 100% CPU
14101871	DOC CORRECTION REQUIRED FOR TARANTELLA OBJECT NEW_GROUP
14101499	4.7 PORT OF 13947409 AND REMOVAL OF INSTRUMENTATION
14101480	CAPS LOCK STATE SYNC WHEN KEYBOARD IS JAPANESE PC ON SERVER
14080078	SOLARIS 11: 3270 AND 5250 WILL NOT RUN BECAUSE OF MOTIF DEPENDANCY
14079220	PRTINSTALL MESSAGE MENTIONS CONFIG FILES THAT MIGHT NOT EXIST
14068868	SGD CLIENT CRASHES WHEN DEFAULT URL IS INVALID AND NO PROMPT/ PROFILE/URL ARGS
14064173	PRINTING FROM GNOME EDIT FAILS
14062558	TTATCC DOES NOT LAUNCH ON SOLARIS 11 CLIENT
14058535	DIRECTORY SERVICE UNAVAILABLE ERROR WHEN NO PASSWORD SUPPLIED
14058517	PORT OF 13968262: DUPLICATE SESSION/APP START ISSUES FOR SOME USERS
14053610	UNSAFE DOWNGRADE OF ALL INTERNET EXPLORER TRAFFIC TO HTTP1.0/TLS1.0
14053578	DEFAULT CHARACTER APPLICATION DOES NOT LAUNCH
14051828	APPARENT PROBLEM WITH WIDTH/HEIGHT RETURNED IN EXTENSION EVENT (RANDR)
14042478	SEAMLESS WINDOWS APPLICATION IS REPRESENTED IN TASKBAR USING APP ICON WHEN COLOR DEPTH IS 16/8
14032389	MAXIMISE BACK TO KIOSK MODE NOT WORKING VERY WELL
14032229	UNLOCALIZED MESSAGES IN PROFILE EDIT PAGE
14027702	CLIENTS MAXIMUM SIZE FEATURE IS BROKEN
14025219	SGD NOT PRESERVING APACHE PORT NUMBER ON UPGRADE
14021791	TTWEBTOP WINDOW: CALCULATING FRAME INSETS... MESSAGE IS DISPLAYED ON UBUNTU 12.04
14021492	MISSING ZH_TW TAIWAN KEYBOARD ENTRY IN USER PROFILE
14019019	FILES SHOULD BE OWNED BY ROOT OR BIN NOT TTASERV
14018841	SGDAUDIO DAEMON DOES NOT RUN ON SOLARIS SPARC
14018564	LDAP PASSWORD EXPIRY CHANGE DOES NOT WORK
14006086	RDP SHORTCUT KEYS FOR SCREEN COPY BEHAVIOR ARE INVERTED
14005396	ARRAY IS NOT REPAIRING WHEN PRIMARY IS OUT OF NETWORK

Reference	Description
14004321	SEAMLESS WINDOWS PAINT APPLICATION CANNOT BE MOVED TO RIGHT AFTER RESUMING IT ON MULTI MONITOR SETUP
14002030	WINDOWS LAUNCHES TO A 2008 R2, RDPSEC LAYER, FIPS COMPLIANT FAIL - NO ERROR
14000588	UNLOCALIZED MESSAGES DISPLAYED
13999334	GLOBAL GRAB BY AN APPLICATION CAN LOCK ALL APPLICATION SESSIONS THAT SHARE AN XPE
13997556	NLA ALWAYS ON, EVEN WHEN DISABLED FOR OBJECT
13997183	TTATSC SEGMENTATION FAULTS ON SESSION DIRECTORY REDIRECT
13996950	CANNOT RUN TTATSC MANUALLY WITHOUT LD_LIBRARY_PATH BEING SET
13996443	AN APPLICATION USING RANDR DOES NOT INFLUENCE THE SIZE OF THE SHADOW SESSION
13995625	EXCEPTIONS SEEN WITH MYDESKTOP/AUTOLOGOUT FUNCTIONALITY
13995357	INPUT METHOD IS NOT INVOKED
13991896	TTASHADOW SHOULD BE ROBUST WHEN HAVING A WRONG FONT IN THE DEFAULT FONT PATH
13974978	ESC - NEED A 4.62 REPLACEMENT FOR 4.50 GROUP MATCHES FEATURE
13969843	TTATCC SEGMENTATION FAULTS ON LOG OUT
13969017	LDAP AND AD USERS WITHIN THEIR DN SEE AN EMPTY WEBTOP
13943954	REINSTALL OF SGD THROWS WARNING AFTER UNINSTALL WITHOUT PURGE
13943594	3270 APPLICATION LAUNCHED THROUGH SGD SERVERS GIVES JUNK CHARACTERS
13943378	ADMINISTRATION GUIDE MESSAGE SHOULD BE REMOVED
13943130	ON SILENT SHADOWING, MESSAGES SHOULD BE GIVEN TO ADMIN ON THE STATUS OF THE USER APPLICATION
13940099	SGD CLIENT NOT COMPATIBLE ERROR ON RESTARTING TARANTELLA
13939571	CWM X APPLICATION EXITS ON CLICKING THE SHADOWING WINDOW
13933608	ENHANCEMENT MODULE INSTALLATION THROWS AN ERROR OF NO SUCH FILE OR DIRECTORY
13931179	VDI BROKER ALWAYS DISPLAYS GUEST POOLS
13924905	SGD, LD_LIBRARY_PATH AND SETUID
13920661	ON SUN RAY CHOOSE ZH_TW BIG5 - THE SGD CLIENT CRASHES IN DDPCSCINIT()
13920424	UNINSTALLATION OF SGD FAILS ON ORACLE LINUX BECAUSE OF YUM INSTALL DEPENDENCIES
13920127	GETTING WRONG MESSAGE DURING CONFIGURATION OF SGD SERVER ON SOLARIS 11
13919290	CGI SCRIPTS ARE MISSING EXECUTE PERMISSIONS ON SOLARIS
13918324	SOME ES/IT/PT_BR WEB PAGES ARE INCOMPLETELY LOCALIZED
13896960	XPE MMAP() MEMORY ALLOCATION STILL NEEDED ON SOLARIS
13887082	SGD DIRECTORY SERVICES INTEGRATION USER ATTRIBUTE AUTHENTICATION CACHE BROKEN

Reference	Description
13871529	KIOSK UI CAN APPEAR ON THE WRONG MONITOR
13854955	CLASSROOM OBJECT FAILS TO LAUNCH
13852504	GATEWAY FAILS AND DENIES LOGINS
13849967	SUN RAY REMOTE SCREEN CAPTURE KEY SEQUENCE LOSES EVENTS
13843469	KIOSK APP SPANS ONLY ONE SCREEN AFTER CHANGING THE RESOLUTION OF ONE IN MULTI MONITOR SETUP
13829872	MAC CLIENT GETS POLISH KEYBOARD LOADED FOR FRENCH INPUT
13829754	ALLOW ACCESS TO XKBSETIGNORELOCKMODS FOR MOTIF ACCELERATOR BUGS
13829264	BASIC AUTHENTICATION THIRD PARTY LOG IN DOES NOT WORK WITH TOMCAT 7
13813121	AGED PASSWORD HANDLER TRANSPORT DOES NOT VARY WITH APPLICATION
13810458	CLIENT KEYBOARD LAYOUT OVERRIDE DOES NOT DISPLAY CORRECT TERRITORY
13808564	ADDITIONAL TTAXPE INSTANCE IS STARTED ON LAUNCHING A SHAREABLE APPLICATION
13793464	VDI BROKER LOGS SHOULD INDICATE WHEN THE VDA.CREDENTIAL PROPERTY WAS RECEIVED
13783709	KIOSK DROP DOWN CONTROL IS TOO SLOW
13777898	CORRECT LOGGING AND MAKE IT MORE INFORMATIVE
13768869	TTACPE DUMP CORE PERIODICALLY
13741660	UPGRADE SCRIPTS CANNOT GREP OR COPY OLD PROPERTIES FILE
13721719	REVIEW THE 12296158 CPE FIX
13720573	HTTP STATUS 500 ERROR SEEN WHEN LC_ VARIABLES ARE SET TO C
13707502	TABBING ORDER OF THE UI ELEMENTS OF THE TTATCC PROMPT IS NOT CORRECT
13703100	APPLE KEYBOARD ISSUES
13702339	VDI BROKER: USERS ARE NOT PROMPTED FOR CREDENTIALS WHEN AUTHENTICATION IS DISABLED ON VDI SERVER
13696359	CHANGING THE PREFERRED LANGUAGE TO DE REPLACES EN WITH DE
13680486	SGD CLIENT INSTALLATION WINDOW DOES NOT SHOW THE CONTENTS IN THE PREFERRED LANGUAGE
13635728	AT INSTALL TIME THE SCRIPT CHECKS PORT 80 IS FREE - CHECK 443 AS WELL OR INSTEAD
13635716	CLEAN UP THE END OF INSTALL TEXT
13634040	VDI BROKER DOES NOT DETECT EXPIRED CERTIFICATES UNLESS SEPARATE TRUSTSTORE IS CONFIGURED
13630575	RDP LICENSE POOL: PROFILE SETTING REFERS TO SSGD
13618869	WEBTOP SESSION IDLE TIMEOUT CAN FAIL IN AN ARRAY
13603137	OEL6 SELINUX CONFIGURATION ISSUE CAUSES PROBLEM FOR SGD PRINTING
13596466	ESC: SGD (VDI) SESSION APPEARS TO CRASH WHEN USING PARTICULAR SPREADSHEETS

Reference	Description
13596303	ESC: SGD TTATSC (VDI) SESSION APPEARS TO CRASH WHEN USING PIVOT TABLE IN MICROSOFT EXCEL
13583751	KEYSTORE GEN SCRIPT TEST FAILS ON SERVERRENAME OF EXISTING NODE
13582025	SGD BROKER LISTS APPLICATION SERVERS WHICH ARE DISABLED AS LAUNCH CANDIDATES
13525046	ENSURE ALL WINDOWS 2008 R2 AUDIO AND SESSION DIRECTORY CHANGES ARE IN 4.62
13524320	PORT 13422037 TO 4.7 (AGED PASSWORD HANDLER FAILS IN 4.6)
13520731	CANNOT USE THE SAME BROKER (CONFIGURED DIFFERENTLY) BETWEEN DYNAMIC APP SERVERS
13510249	TARANTELLA PASSCACHE LIST FAILS IN SOME CIRCUMSTANCES WHEN SERVER IS RUNNING
13505639	REMOVE LOCAL LAUNCH
13496613	NUMEROUS TR: WARNING: AN UNESCAPED BACKSLASH MESSAGES INSTALLING SGD ON OEL 6.1
13485736	LDAP SEARCHES FROM THE ADMIN CONSOLE ARE NOT CONFIGURABLE
13474437	MAKE DEVICESERVICE MORE ROBUST
13465649	REMOVE REXEC AND RCMD TRANSPORTS
13465645	NTLA IS DEPRECATED
13457415	SOLARIS 11: CHANGE ADMINISTRATOR PROFILE TO USE A LOGIN NAME WITH A ROOT ROLE
13451793	PORT 13442124 ADMIN CONSOLE FIX TO 4.7
13451320	PORT TTASHADOW LAUNCH FIXES TO 4.7
13441204	PORT OF 13255477 TO 4.7
13432087	MAC MANUAL INSTALLER WILL REPLACE ANY EXISTING SGD CLIENTS
13424293	LICENSE POOL REMOVAL ON UPGRADE TO 4.7
13414544	RFE: NEW BROKER FOR ACCESSING A TARGET PLATFORM AT LAUNCH TIME
13408097	UNIX SGD CLIENT DIALOG BOXES SHOULD BE CENTRED ON THE PRIMARY MONITOR NOT AT 0,0
13407638	WINDOW COLOR PRESENTATION ATTRIBUTE NEEDS REVIEWING
13403026	AUDIO DEVICE DOES NOT BUILD WITH ORACLE LINUX UEK HEADERS
13390651	AUDIO RECORD AND PLAYBACK IS CHOPPY OVER VPN, BETTER WITH COMPRESSION
13386831	VDI 3.3 BROKER DOES NOT PROMPT FOR CREDENTIALS AGAIN WHEN SESSION HAS EXPIRED
13386823	REMOVE ONLINE HELP FROM THE ADMIN CONSOLE
13386804	REMOVE DOCUMENTATION FROM INSTALLATION PACKAGES
13375588	MAKE DEFAULT XCLOCK APPLICATION SCALABLE
13359188	ALLOW READ TIMEOUTS TO BE CONFIGURED IN THE VDI 3.3 BROKER
13359119	VDI 3.3 BROKER SHOULD LOG TO A SEPARATE FILE BY DEFAULT
13354844	KIOSK MINIMISE BUTTON NOT WORKING

Reference	Description
13341364	DO NOT GET LOCKED OUT ERROR AFTER EXHAUSTING FAILED LOGIN ATTEMPTS
13257432	NO SGD CLIENT PANEL CONTROL IN UNITY DESKTOP ON UBUNTU 11.10
13257339	MAC OS X CLIENT UNNECESSARILY VERBOSE ABOUT THE INPUT SERVICE STATE
13248823	TTASHADOW SEGMENTATION VIOLATION
13118977	SEAMLESS WINDOWS: SHOW DESKTOP CAUSING OCCASIONAL VISUAL DEFECTS
13117053	WINDOWS APPLICATION SESSION IS ENDED ON SGD SERVER BUT IS STILL ALIVE AS AN RDP SESSION
13117046	KIOSK APPLICATION APPEARS IN STRANGE POSITIONS ON A DUAL MONITOR SYSTEM (UBUNTU)
13109118	AD USER IS PROMPTED INCORRECTLY BY SGD TO CHANGE PASSWORD
13097388	PORT OF BUG 12310050
13096064	LOAD BALANCED LAUNCHES ASSIGNED INCORRECT PROFILE FOR LDAP/AD USERS
13087707	INSTALLED SGD CLIENT DOES NOT REMEMBER LOCALE
13065305	RANDR: CAUSES PROBLEMS UNDER COMPIZ
13063591	ESC: VDI BROKER TO WINDOWS 7 VRDP PASSTHROUGH AUTHENTICATION FAILS WITH NON UPN USERNAME
13059922	UNABLE TO LIST CONTENTS OF LIGHT DIRECTORIES FROM COMMAND LINE
13038949	CONFIGURED LDAP OPERATION TIMEOUTS ARE NOT WORKING
13028776	ERROR MESSAGE: THE SGD SERVER URL IS INVALID
13013449	UNNECESSARY LIBXPM DEPENDENCY IN TTATSC
13009764	SGD PRINTING SUBSYSTEM DECLARES PCL PRINTER TO BE POSTSCRIPT PRINTER
12967239	LDAP SEARCHES THAT RETURN SIZE LIMIT EXCEEDED ERROR ARE NOT HANDLED CORRECTLY
12961980	CANNOT INSTALL SGD WINDOWS CLIENT AS A NON-ADMIN USER WITHOUT ADMIN PRIVILEGES
12903943	ADMIN CONSOLE LDAP USER SEARCH FILTER DOES NOT WORK WHEN USING OPENLDAP SERVER.
12863967	TTASHADOW REVIEW
12826145	UNIX CDM FAILS FOR USERS WITH UPPER CASE CHARACTERS
12768524	CREATE A MANUAL INSTALLER FOR THE MAC CLIENT
12768473	UPDATE THE WINDOWS CLIENT'S MANUAL INSTALLER
12768449	UPDATE THE UNIX CLIENT'S MANUAL INSTALLATION SCRIPT
12768390	ALLOW CHOICE OF SGD SERVER WHEN THE SGD CLIENT IS STARTED MANUALLY
12768347	SGD CLIENT HELPER SHOULD MAKE USE OF INSTALLED CLIENTS WHERE POSSIBLE.

Reference	Description
12755593	SGD INCORRECTLY REQUIRES GATEWAY NAME TO BE A FULLY-QUALIFIED HOSTNAME
12708195	ESC: ENABLING BILLING SERVICES CAUSES STATUS COMMAND ERROR
12691786	SGD DOCUMENTATION DOES NOT EXPLICITLY STATE SUPPORTED CLIENT REQUIREMENTS
12687906	INCORRECT MESSAGE LOGGED REGARDING ROUTING TOKEN VALIDITY
12667391	CLIENT DRIVE MAPPING: MISLEADING OUT OF MEMORY ERROR MESSAGES WHEN TRYING TO SAVE FILES
12636349	USER NOT PROMPTED FOR AUTHORIZATION IF NLA FAILS
12633214	SGD FAILS TO HANDLE LDAP USER NAMES WITH SPACES AT THE END OF THEIR DNS
12551476	GATEWAY LOGGING DOCUMENTATION IMPROVEMENTS
12542375	CREATE A VIRTUAL SERVER BROKER COMPATIBLE WITH VDI 3.3
12425312	ESC: AUTHENTICATION CONFIGURATION WIZARD: UNABLE TO CREATE A SERVICE OBJECT
12312532	NULL POINTER EXCEPTION WITHIN EXCEPTION HANDLING
12311743	NULL POINTER EXCEPTION WITH FAST LOGIN/LOGOUT CYCLE.
12310344	SUNBT7032412 POTENTIAL INFINITE LOOP IN DYNAMIC LAUNCH
12310034	SUNBT7031082 ESC: APPLICATION MENUS ARE NOT WORKING AS EXPECTED IN SEAMLESS WINDOWS
12309878	SUNBT7030194 ERROR ON DYNAMIC LAUNCH WHEN CREATING A PERMANENT ENS OBJECT
12309725	SUNBT2207875 ESC: X11 APPLICATIONS DO NOT REDRAW CORRECTLY
12309559	SUNBT7028247 JAVA NOT DETECTED CORRECTLY IN INTERNET EXPLORER 9 (WINDOWS 7)
12309384	SUNBT2207614 ESC: SGD 4.50 GATEWAY PROTOCOL TRANSLATION FAILS FROM HTTPS TO HTTP
12309088	SUNBT2207339 ERROR WHEN BUILDING AUDIO DRIVE ON 64-BIT SUSE 11
12308958	SUNBT7024633 ESC: PRINTING FAILS ON SOLARIS WHEN THE USER CN/DN EXCEEDS 149 CHARACTERS
12308892	SUNBT7024122 TARANTELLA STATUS REPORTS INCORRECT SECURITY STATUS
12308632	SUNBT7022398 90-METER SMART CARD STRING BUFFER SIZE AND AUTO-ALLOCATION FIXES
12308362	SUNBT7020722 ESC: UNABLE TO BROWSE AN AD SERVER VIA THE ADMIN CONSOLE
12308030	SUNBT7018972 ESC: OPENSSL COMMAND IN SECURE GLOBAL DESKTOP CANNOT LOAD CONFIG
12307930	SUNBT7018525 SOAP PEER CONNECTIONS ARE NOT ALARMED
12307553	SUNBT7016632 ESC: SGD INSTALLATION FAILS WITH A PERMISSION DENIED ERROR
12307459	SUNBT7016280 DOC: STATEMENT ON ARRAY RECOVER AFTER FAILOVER IS INCORRECT

Reference	Description
12307455	SUNBT7016266 DOC: PATH TO SGD WEBSERVICES.JAR IS INCORRECT
12305483	SUNBT7007439 UTTSC CANNOT USE THE CAL STORED BY SGD
12305187	SUNBT7006408 OBSOLETE CLI STILL AVAILABLE
12305168	SUNBT7006334 INCORRECT SECTION LABEL ON PRESENTATION TAB FOR CHARACTER APPLICATIONS
12305011	SUNBT7005437 AUTOMATIC LOGOUT CAN FAIL WHEN AN APPLICATION IS SUSPENDED/RESUMED
12304276	SUNBT7002124 GATEWAY DOCS NEED CORRECTING FOR CONFIG EDIT COMMANDS THAT ARE A LIST
12304039	SUNBT7000901 PRINTERS AND DRIVES NOT MAPPED FOR WINDOWS APPS
12303980	SUNBT7000586 MULTIPLE DEPENDENCY PROBLEMS WHEN INSTALLING 4.6 ON RHEL 6
12303665	SUNBT2202272 ESC: SINCE UPGRADE TO 4.5, PRINT JOBS INTERMITTENTLY STAY IN PRINT
12303609	SUNBT6998552 USING WEB SERVICES TO CREATE A DYNAMIC APPLICATION SERVER WITH A VSB
12303546	SUNBT2202151 IMPROVE SGD 4.50 COMPATIBILITY WITH WINDOWS SERVER 2008 AND 2008 R2
12302189	SUNBT6990599 LDAP URL FILTER WITHOUT A SEARCH FILTER DOES NOT WORK
12301942	SUNBT6989595 SEPARATOR BARS FOR WEBTOP GROUPS NEED REDUCING IN SIZE
12301940	SUNBT6989592 UPDATE DOCS FOR SPAN MULTIPLE MONITORS OPTION
12301668	SUNBT6988236 WEB.XML FOR ADMINISTRATION CONSOLE STILL REFERS TO SUN
12301484	SUNBT6987242 ACTIVE DIRECTORY CONFIGURATION WRONG AFTER AN UPGRADE
12300978	SUNBT2198455 ESC: RFE: SUPPORT FOR SECURE GLOBAL DESKTOP ENHANCEMENT MODULE
12300864	SUNBT6983054 DYNAMIC DRIVE MAPPING WARNING MESSAGES ONLY IN ENGLISH
12300298	SUNBT6979454 REVIEW DOCUMENTED GHOSTSCRIPT MINIMUM VERSION REQUIREMENTS
12299999	SUNBT6977961 A RUNTIME ERROR HAS OCCURRED WHILE CLICKING ON VERSION
12299915	SUNBT2197077 REVIEW /OPT/TARANTELLA/ETC/DATA/CACERTS.TXT
12299530	SUNBT6975570 CHANGE DEFAULT COLOR DEPTH TO 24/32 FOR WINDOWS APPLICATIONS
12299506	SUNBT6975287 UPGRADE LOG REFERS TO LEGACY TARANTELLA DOCS
12299354	SUNBT6974464 KIOSK APPLICATIONS ON UBUNTU HAVE OS TOOLBARS OVER THE TOP
12298702	SUNBT6971208 DOC NEEDS CORRECTING FOR WINDOWS AUDIO AND SUPPORT FOR HIGHER BITRATES

Reference	Description
12298004	SUNBT2195462 TERMINAL SERVICES CALS NOT STORED IN REGISTRY ON WINDOWS 7/VISTA FOR NON-ADMIN USER
12297905	SUNBT6967170 APPLICATION SESSION RESUMABILITY TIMEOUTS NEED CLARIFICATION
12297901	SUNBT6967158 CDE DOES NOT COME UP FOR SOME LOCALIZED ENVIRONMENT FROM SGD
12297796	SUNBT2195370 SECURITY ENABLE WITH A THAWTE TEST CERT FAILS TO ACCEPT ROOT OR INTERMEDIATE CERTIFICATE
12297749	SUNBT2195328 ESC: AUDIO CANNOT BE HEARD WITH WIN2008 R2 AS THE APPLICATION SERVER
12296804	SUNBT6961989 NON-ASCII CHARACTERS ARE NOT RETURNED TO THE LOGIN BOX
12296679	SUNBT6961333 SGD CLIENT INSTALL DIRECTORY: ORACLE REBRANDING NEEDED
12296343	SUNBT2194331 CAPSLOCK ON FRENCH KEYBOARD GIVES CAPITALISED ACCENTED CHRS
12294323	SUNBT2192822 ESC: DISABLE AUTOCOMPLETE ON LOGIN PAGE TO PREVENT BROWSER CREDENTIALS CACHING
12292967	SUNBT6945810 INTEGRATING SGD WITH ORACLE INTERNET DIRECTORY AS AN LDAP BACKEND
12291675	SUNBT6941088 PRINTING TROUBLESHOOTER NEEDS TO COVER RDP SETTINGS
12261595	SUNBT6802404 GATEWAY DOES NOT REPORT IF PORTS ARE IN USE
12260830	SUNBT6799048 CLOCK SKEWING ON GATEWAY SERVERS CAUSES SESSION LAUNCH FAIL
12218812	SUNBT6632783 MAC OS X SGD CLIENT FAILS TO RUN FROM COMMAND LINE

3.3. Documentation Issues in Release 4.70

This section lists the known documentation issues for the 4.70 release.

3.3.1. Legacy VDI Broker Documentation Issue

The Legacy VDI Broker is a virtual services broker that enables SGD to request a desktop from a local Oracle VDI 3.2 installation.

Because the SGD 4.70 release does not support Oracle VDI version 3.2, the description and configuration procedures for the Legacy VDI broker that are included in the published documentation are not applicable for this release of SGD.

3.3.2. Secure Mode Installation and Firewall Forwarding

The published documentation does not clearly state that in a secure mode installation, firewall forwarding is disabled for the SGD server.

The note in Installing the Main SGD Component in the *Oracle Secure Global Desktop Installation Guide for Release 4.7* should read as follows:

"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.

See the *Oracle Secure Global Desktop Administration Guide for Release 4.7* 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."

3.3.3. Incorrect Windows Registry Key Path for Enhancement Module

In the Windows Applications Do Not Close Down topic in the *Oracle Secure Global Desktop Administration Guide for Release 4.7*, the stated path for the Windows registry key is incorrect.

The correct path is as follows:

```
HKEY_LOCAL_MACHINE\Software\Oracle\Enhancement Module for Windows
```

On 64-bit Windows platforms, the path is as follows:

```
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Oracle\Enhancement Module for Windows
```

3.4. Providing Feedback and Reporting Problems

This section provides information about how to provide feedback and contact support for the Oracle Secure Global Desktop product.

To report a bug in the software or to ask a question, please contact the Secure Global Desktop Software Team and Community Forum. Posting on the Secure Global Desktop Software Team and Community Forum does not guarantee a response. If you need a fix for a bug, and have an Oracle Premier Support Agreement, you should open a case with Oracle Support at https://support.oracle.com.

If you are reporting a bug, please provide the following information where applicable:

- Description of the problem, including the situation where the problem occurs, and its impact on your operation.
- Machine type, operating system version, browser type and version, locale and product version, including any patches you have applied, and other software that might be affecting the problem.
- Detailed steps on the method you have used, to reproduce the problem.
- Any error logs or core dumps.

3.4.1. Contacting Oracle Specialist Support

If you have an Oracle Customer Support Identifier (CSI), first try to resolve your issue by using My Oracle Support at https://support.oracle.com. Your Oracle Premier Support CSI does not cover customization support, third-party software support, or third-party hardware support.

If you cannot resolve your issue, open a case with the Oracle specialist support team for technical assistance on break/fix production issues. The responding support engineer will need the following information to get started:

- Your Oracle Customer Support Identifier.
- The product you are calling about.

- A brief description of the problem you would like assistance with.

If your CSI is unknown, find the correct Service Center for your country (http://www.oracle.com/us/support/contact-068555.html), then contact Oracle Services to open a non-technical service request (SR) to get your CSI sorted. Once you have your CSI, you can proceed to open your case through My Oracle Support.