Oracle® Secure Global Desktop

Platform Support and Release Notes for Release 5.2

April 2015
E51729-03

Oracle Legal Notices

Abstract

This document describes the new and changed features for this release of Oracle Secure Global Desktop. Information on supported platforms and known bugs and issues are included.

Document generated on: 2015-07-07 (revision: 3955)

Table of Contents

Preface

The *Oracle Secure Global Desktop Platform Support and Release Notes* 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 Related Documents

The documentation for this product is available at:

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

4 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 5.2.

1.1 New Features in Release 5.2

This section describes the features that are new in the SGD 5.2 release.

1.1.1 Plug-ins for Oracle Enterprise Manager

Plug-ins for Oracle Enterprise Manager are now available which enable SGD Administrators to monitor and diagnose issues with SGD array and SGD Gateway deployments.

This release can be used with the following plug-ins:

- Enterprise Manager Plug-in for Oracle Secure Global Desktop
- Enterprise Manager Plug-in for Oracle Secure Global Desktop Gateway

See the Oracle Enterprise Manager Cloud Control Plug-ins page for the released documentation for these plug-ins.

1.1.2 Single Sign-On Integration with Oracle Access Manager

SGD now integrates with Oracle Access Manager. The single sign-on feature of Oracle Access Manager can be used for the following:

- Authenticating to an SGD server
- Authenticating to a remote application started from the SGD workspace

Single sign-on for an SGD server can be enabled from the Administration Console, or by using the `tarantella sso` command.

A new attribute, Single Sign-on (`--ssoauth`), for application objects enables single sign-on when authenticating to a remote application.

See Single Sign-On Authentication in the *Oracle Secure Global Desktop Administration Guide* for more details on configuring and using single sign-on with SGD.

1.1.3 New Commands for Installing SGD Patches

New commands have been introduced to simplify the process of installing software updates (*patches*) for an SGD installation.

- The `tarantella patch` command is for applying patches to an SGD server.

  See tarantella patch in the *Oracle Secure Global Desktop Administration Guide*.

- The `gateway patch` command is for applying patches to an SGD Gateway.

  See gateway patch in the *Oracle Secure Global Desktop Gateway Administration Guide*.

1.1.4 Password Preferences for Users

The SGD workspace now includes a Password Preferences tab. Password preferences enable users to control whether SGD saves their passwords in the application server password cache. Users can choose

to always save passwords, save passwords for the duration of the user session only, or to never save passwords.

The current password preferences setting is shown on the workspace when a user logs in to SGD.

See User Management of the Password Cache for more details on how to configure the password preferences feature.

See Password Preferences for details of how users can set password preferences from the SGD workspace.

1.1.5 Role-Based Administration of SGD

Additional role objects for SGD Administrators have been introduced for this release. The new roles offer different levels of administration privileges and access control to the Administration Console.

The available new roles are:

- Session Administrators
- Session Viewers
- Global Viewers
- Enterprise Manager Agents

These role objects are created automatically when you install SGD.

See SGD Administrators in the *Oracle Secure Global Desktop Administration Guide*.

1.2 Changes in Release 5.2

This section describes the changes for the SGD 5.2 release.

1.2.1 Changes to Supported SGD Installation Platforms

The following is a summary of the main changes for this release:

- **Retirement of 32-bit platforms.** Support for installing the following SGD software components on 32-bit platforms is no longer available.
  - The main SGD component
  - The SGD Gateway

  Administrators can install these software components on 64-bit platforms.
- **Application server platforms.** New packages for the SGD Enhancement Module have been introduced for Oracle Linux and Oracle Solaris platforms. The packages are for a specific operating system (OS) version. The packages provide PulseAudio support for the UNIX audio module.

  Windows Server 2012R2 has been added as a supported installation platform for the Enhancement Module. Some legacy releases of Windows Server, such as Windows Server 2003 have been retired as supported platforms.
- **Client platforms.** Windows XP has been retired as a supported client platform.

Chrome OS has been added as a supported client platform. This means that SGD can now be used with Chromebook devices.

The tablet workspace can now be used with Firefox browsers running on Windows client platforms.

See Chapter 2, *System Requirements and Support* for full details of the supported installation platforms for this release.

1.2.2 Retirement of rpm Command for Installation on Linux Platforms

Use of the `rpm` command is no longer recommended when installing the SGD Gateway or the SGD Enhancement Module on Linux platforms.

To install these software components on Linux platforms, Administrators should use the `yum` command. For example, to install the Gateway:

```
# yum install --nogpgcheck SUNWsgdg-version.x86_64.rpm
```

Using `yum` means that all package dependencies are resolved automatically.

See Installing the SGD Enhancement Module for UNIX and Linux Platforms in the *Oracle Secure Global Desktop Installation Guide* and Performing the Installation in the *Oracle Secure Global Desktop Gateway Administration Guide*.

1.2.3 Secure Array Joins Using the Administration Console

The Administration Console can now be used to add an SGD server to an array that uses secure intra-array communication. In previous releases, array join operations for secure arrays were done from the command line.

1.2.4 Required Users for SGD Server and SGD Gateway Hosts

The following changes have been made for required user and group accounts on SGD and SGD Gateway hosts:

- **SGD hosts.** Required users are now created automatically when you install SGD on Linux platforms.

  In previous releases, the `ttaserv` and `ttasys` users and a `ttaserv` group were required on the Linux host before installing SGD.

- **Gateway hosts.** The Gateway now requires an `sgdgsys` user and a `sgdgserv` group.

  The required user and group are created automatically when you install the Gateway on Linux platforms. On Oracle Solaris platforms, you are prompted to run a script to create the required user and group manually.

  File ownerships for a Gateway installation are now `sgdgsys`:`sgdgserv`, to reflect the new user and group.

1.2.5 Changes to Gateway Commands

The `gateway status` command has been extended to provide a summary of connections through the Gateway. A new command, `gateway connection`, can be used to display detailed connection statistics.

The `tarantella gateway token` command has been introduced to help to diagnose connection issues in a Gateway deployment. You run this command on an SGD server in the array.

See the *Oracle Secure Global Desktop Gateway Administration Guide* for details of these commands.

1.2.6 Changes for SecurID Authentication

The following changes have been made for users authenticating to SGD using SecurID:

- Configuration for SecurID authentication has changed, due to a new implementation using the RSA Java API.

  Administrators now use a properties file, `rsa_api.properties`, to specify SecurID settings such as the location of the RSA Authentication Manager configuration file and logging levels.

  Note that if you are upgrading SGD, SecurID authentication will be disabled automatically and you are prompted to reconfigure SecurID authentication using the new configuration procedure. See SecurID Authentication in the *Oracle Secure Global Desktop Administration Guide* for more details of the configuration changes.

- SGD can now use an LDAP directory server to establish the user identity when a user logs in using SecurID authentication.

See Section 2.1.4.3, “Supported Versions of SecurID” for RSA Authentication Manager versions supported by this release.

1.2.7 Password Types for Password Cache Entries

You can now specify a password type when you create a new password cache entry. The password type is used by SGD to organize entries in the password cache.

See tarantella passcache in the *Oracle Secure Global Desktop Administration Guide*.

1.2.8 Changes for UNIX Audio

The following changes have been made to SGD audio services for X applications running on a UNIX or Linux platform application server.

- Users can now record audio in an X application.

  A new attribute, Unix Audio Input (`--array-unixaudioin`), enables UNIX audio recording for the array.

- The UNIX audio module now supports PulseAudio on Oracle Linux 6 and Oracle Solaris 11 platforms. Open Sound System (OSS) is still supported for legacy platforms. Administrators are prompted for the required emulation during installation of the Enhancement Module. See Section 2.4.2, “Supported Installation Platforms for the SGD Enhancement Module” for the supported installation platforms for the UNIX audio module.

  PulseAudio is the preferred audio emulation mode for SGD. For legacy OSS applications, you can use the PulseAudio OSS wrapper script, `padsp`, to ensure compatibility with PulseAudio.

  On supported platforms for the Enhancement Module, PulseAudio works with ALSA applications and GStreamer applications, with no extra configuration required.

See Audio in the *Oracle Secure Global Desktop Administration Guide* for more details on configuring and using audio for X applications.

1.2.9 Changes to Supported Proxy Authentication Methods

This release adds support for using the following authentication methods when connecting to SGD through an HTTP proxy server.

- Negotiate (NTLM authentication only)
- Digest
- NTLM

This means that clients configured for Integrated Windows Authentication (IWA) can now be used.

See Section 2.2.2, “Supported Proxy Servers” for more details of the supported proxy authentication methods.

1.2.10 Support for Microsoft Hyper-V

This release adds limited support for connecting from SGD to a system hosted by a Hyper-V service on a Windows Server 2012 R2 host. See Section 2.4.6, “Microsoft Hyper-V” for details of supported versions.

The enhanced session mode feature of Hyper-V is supported for Windows Server 2012 R2 and Windows 8.1 virtual machines.

See Integrating SGD With Microsoft Hyper-V in the *Oracle Secure Global Desktop Administration Guide* for details of how to configure SGD to access a Hyper-V guest.

1.2.11 Client Configuration Changes for Multi-Monitor Kiosk Mode Applications

For multi-monitor displays without RANDR, desktop size configuration has changed when displaying kiosk mode applications.

The `virtual` value is no longer available for the `<KioskArea>` client setting. Use the Span Multiple Monitors (Kiosk Mode) option in the Client Settings tab to display a kiosk mode application on all monitors.

See Configuring Desktop Size for Kiosk Mode Applications in the *Oracle Secure Global Desktop Administration Guide*.

1.2.12 Changes for Audit Logging

Audit logging is now enabled by default when you install SGD. This feature uses the `*/*/*auditinfo` log filter.

1.2.13 Language Selection List on Login Dialog

The workspace language can now be selected using a drop-down list on the SGD login dialog.

1.2.14 Performance Improvements for Windows Applications

Performance improvements have been made for SGD applications that use the Microsoft Remote Desktop Protocol (RDP). The changes result in a smoother display and lower bandwidth usage when running Windows applications.

1.2.15 Changes to Default Attribute Settings of Application Objects

The default attribute settings for new X application and Windows application objects have changed, as follows:

- **Color Depth:** X application objects now use 24-bit color (millions of colors). Windows application objects use 24/32-bit color (millions of colors).
- **Window Size:** For application objects with a Window Type of Independent Window (`--independent`), the default window size is now 1024 x 768 pixels.

1.2.16 Retirement of Load-Balancing JSP Technology Page

The SGD JavaServer Pages (JSP) technology page for load balancing of user sessions is no longer included in the SGD software.

Administrators can use the SGD Gateway to support user session load balancing. See the *Oracle Secure Global Desktop Gateway Administration Guide*.

Chapter 2 System Requirements and Support

This chapter includes details of the system requirements and supported platforms for Oracle Secure Global Desktop (SGD) Release 5.2.

2.1 SGD Server Requirements and Support

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

2.1.1 Supported Installation Platforms for SGD

Table 2.1, “Supported Installation Platforms for SGD” lists the supported installation platforms for SGD.

Table 2.1 Supported Installation Platforms for SGD

Operating System	Supported Versions
Oracle Solaris on SPARC platforms	Solaris 10 [at least version 8/11 (update 10)] Solaris 11 Trusted Extensions versions of the above
Oracle Solaris on x86 platforms	Solaris 10 [at least version 8/11 (update 10)] Solaris 11 Trusted Extensions versions of the above
Oracle Linux (64-bit only)	5 (at least version 5.8) 6 (at least version 6.2)

Note

This table shows the installation platforms that Oracle has tested with this release of SGD. For up to date information on supported platforms, see knowledge document ID 1416796.1 on My Oracle Support (MOS).

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.

2.1.1.1 Virtualization Support

SGD is supported and can be installed in an Oracle virtualized environment. If you encounter a problem when using an unsupported virtualization environment, you may be asked to demonstrate the issue on a non-virtualized operating system to ensure the problem is not related to the virtualization product.

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.

2.1.1.2 Retirements to Supported SGD Installation Platforms

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

SGD Version	Platforms No Longer Supported
5.2	Oracle Linux (32-bit platforms)

2.1.1.3 Network Requirements

IPv6 network addresses are not supported. See the *Oracle Secure Global Desktop Installation Guide* for details of network requirements for SGD.

2.1.2 Supported Upgrade Paths

Upgrades to version 5.2 of SGD are only supported from the following versions:

- Oracle Secure Global Desktop Software version 5.1
- Oracle Secure Global Desktop Software version 5.0
- Oracle Secure Global Desktop Software version 4.71
- Oracle Secure Global Desktop Software version 4.63

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

2.1.3 Third Party Components for SGD

SGD includes the following third party components:

- **Java technology.** This release of SGD includes Java 8 update 31.
- **SGD web server components.** 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 this release of SGD.

Component Name	Version
`Apache HTTP Server`	2.2.29
`OpenSSL`	1.0.1l
`Apache Tomcat`	7.0.57

  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.

2.1.4 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

2.1.4.1 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
- Windows Server 2012
- Windows Server 2012 R2

2.1.4.2 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 Unified Directory 11gR1 (11.1.1.x), 11gR2 (11.1.2.x)
- Oracle Internet Directory 11gR1 (11.1.1.x), 11gR2 (11.1.2.x)
- Oracle Directory Server Enterprise Edition 11gR1 (11.1.1.x)
- Microsoft Active Directory, as shown in Section 2.1.4.1, “Supported Versions of Active Directory”

Other directory servers might work, but are not supported.

2.1.4.3 Supported Versions of SecurID

SGD works with the following versions of RSA Authentication Manager (formerly known as ACE/Server).

- 7.1 SP2, 7.1 SP3, 7.1 SP4
- 8.0, 8.1

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

2.1.4.4 Supported Versions of Oracle Identity Management

SGD works with the following versions of Oracle Identity Management:

- Oracle Identity Management 11gR2 (11.1.2.x)

2.1.5 SSL Support

SGD supports TLS versions 1.0, 1.1, and 1.2

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

2.1.6 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 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.

To print from a UNIX or Linux system application server using CUPS (Common UNIX Printing System), the version of CUPS must be at least 1.4.2.

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 tables list the supported client platforms and browsers for the SGD Client.

- **Desktop platforms:** For supported desktop client platforms, see Table 2.2, “Supported Desktop Client Platforms for SGD”.
- **iPad tablet devices:** For supported iPad tablet devices, see Table 2.3, “Supported iPad Client Devices for SGD”.
- **Android tablet devices:** For a list of Android tablet devices which have been tested with SGD, see Table 2.4, “Android Client Devices Tested With SGD”.
- **Chrome OS devices:** For a list of Chrome OS devices which have been tested with SGD, see Table 2.5, “Chrome OS Client Devices Tested With SGD”.

Caution

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

Table 2.2 Supported Desktop Client Platforms for SGD

Supported Client Platform	Supported Browsers	Notes
Microsoft Windows 8, 8.1 (32-bit and 64-bit)	Internet Explorer 10, 11 Mozilla Firefox 31.5 ESR, 34 Chrome	Windows 8 is supported in desktop mode only. "Metro" mode is not supported. On 64-bit Windows 8 platforms, the 32-bit version of the Java Plug-in software is required. HTML5 client is supported for Firefox browsers. If the SGD server uses an untrusted certificate, add the server URL as a permanent security exception in Firefox. HTML5 client is supported for Chrome browsers. To use Java plug-in software with Chrome version 42 and later, users must enable NPAPI support on the `chrome://flags` settings page.
Microsoft Windows 7 (32-bit and 64-bit)	Internet Explorer 10, 11 Mozilla Firefox 31.5 ESR, 34 Chrome	On 64-bit client platforms, the 32-bit and 64-bit versions of Internet Explorer are supported. HTML5 client is supported for Chrome browsers. To use Java plug-in software with Chrome version 42 and later, users must enable NPAPI support on the `chrome://flags` settings page.

Supported Client Platform	Supported Browsers	Notes
Sun Ray Software on Oracle Solaris (x86 and SPARC platforms): • Solaris 10 8/11 (update 10) or later • Solaris 11	Mozilla Firefox	On Solaris 11 and 11.1 platforms, the `motif` package is required.
Sun Ray Software on Oracle Linux (32-bit and 64-bit): • Oracle Linux 5 • Oracle Linux 6	Mozilla Firefox Chrome	On 64-bit Linux client platforms, additional packages may be required. See Compatibility Libraries Required on 64-bit Linux Platforms.
Oracle Linux (32-bit and 64-bit): • Oracle Linux 5 • Oracle Linux 6	Mozilla Firefox 31.5 ESR, 34 Chrome	On 64-bit Linux client platforms, additional packages may be required. See Compatibility Libraries Required on 64-bit Linux Platforms.
Ubuntu Linux 12.04, 14.04 (32-bit and 64-bit)	Mozilla Firefox 31.5 ESR, 34 Chrome	On 64-bit Linux client platforms, additional packages may be required. See Compatibility Libraries Required on 64-bit Linux Platforms.
Mac OS X 10.9, 10.10	Safari 7, 8 Mozilla Firefox Chrome	HTML5 client is supported for Chrome browsers. To use Java plug-in software with Chrome version 42 and later, users must enable NPAPI support on the `chrome://flags` settings page.

Note

This table shows the client platforms and browser versions that Oracle has tested with this release of SGD. For up to date information on supported client platforms and browser versions, see knowledge document ID 1950093.1 on My Oracle Support (MOS).

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.

iPad Client Platforms

Table 2.3 Supported iPad Client Devices for SGD

Supported Devices	Operating System	Supported Browsers	Notes
Apple iPad	iOS 7	Safari	Private browsing mode is not

Supported Devices	Operating System	Supported Browsers	Notes
	iOS 8		supported for Safari browsers.

Android Client Platforms

Note

Oracle has tested SGD with the following preferred models of Android devices. Other devices may work with SGD, but have not been tested.

Table 2.4 Android Client Devices Tested With SGD

Device Name	Operating System	Supported Browsers	Notes
Google Nexus 7 Google Nexus 10	Android 4.0.3 and later Android 5	Chrome	Android 5 devices must support WebSocket technology.

Chrome OS Client Platforms

Note

Oracle has tested SGD with the following preferred models of Chrome OS devices. Other devices may work with SGD, but have not been tested.

Table 2.5 Chrome OS Client Devices Tested With SGD

Device Name	Operating System	Supported Browsers
Acer Chromebook HP Chromebook	Chrome OS 38.0	Chrome

Browser Requirements

- The SGD Administration Console is not supported on Safari browsers, either on Mac OS X or iPad client devices.
- Beta versions or preview releases of browsers are not supported.
- Browsers must be configured to accept cookies.
- Browsers must have the JavaScript programming language enabled.

Java Technology Requirements

- On *desktop computer platforms*, browsers must have Java technology enabled to support the following functionality:
  - 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 desktop platforms.

- On *tablet device platforms*:
  - Java technology is not required on the browser
  - Manual installation of the SGD Client is not supported

Java Plug-in software versions 1.7 and 1.8 are supported as a plug-in for Java technology.

For Chrome version 42 and later, Java Plug-in software is disabled by default. Users can enable Java Plug-in software by going to the `chrome://flags` page and enabling NPAPI support. See Enabling NPAPI in Chrome Version 42 and later for more details.

Note

For details of known issues when using Java Plug-in software versions 1.7 and 1.8, 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 workspace are available in the following supported languages:

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

2.2.1.1 Compatibility Libraries Required on 64-bit Linux Client Platforms

The Linux version of the SGD Client is a 32-bit binary. To run on a 64-bit Linux client platform, 32-bit compatibility libraries may be required on the client device.

You can install the required packages on the client device as follows:

Oracle Linux 6 platforms

```
# yum install openmotif.i686 libXt.i686 libxkbfile.i686 libXpm.i686 libstdc++.i686 \
 libXinerama.i686 libXcursor.i686 libXdmcp.i686 libXrandr.i386
```

Oracle Linux 5 platforms

```
# yum install libXrandr.i686
```

Ubuntu Linux 14.04 platforms

```
$ sudo apt-get install libstdc++6:i386 libxpm4:i386 libxinerama1:i386 libxcursor1:i386 \
```

```
libxkbfile1:i386 libxt6:i386 libxm4:i386 libxrandr2:i386
```

Ubuntu Linux 12.04 platforms

```
$ sudo apt-get install ia32-libs libxrandr2:i386 libxkbfile1:i386 libmotif4:i386
```

See Table 2.2, “Supported Desktop Client Platforms for SGD” for details of the supported Linux client platforms.

2.2.1.2 Virtualization Support

SGD is supported and can be installed in an Oracle virtualized environment. If you encounter a problem when using an unsupported virtualization environment, you may be asked to demonstrate the issue on a non-virtualized operating system to ensure the problem is not related to the virtualization product.

2.2.1.3 Network Requirements

IPv6 network addresses are not supported. See the *Oracle Secure Global Desktop Installation Guide* for details of network requirements for SGD.

2.2.1.4 Retirements to Supported Client Platforms

The following table shows the SGD Client installation platforms and browsers that have been retired for this release.

SGD Version	Platforms No Longer Supported
5.2	Windows XP
	Mac OS X 10.7, 10.8
	Ubuntu 10.04
	iOS 6

2.2.2 Supported Proxy Servers

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

SOCKS proxy servers: SGD supports the following authentication methods.

- Basic
- Anonymous (no authentication required)

HTTP proxy servers: SGD supports the following authentication methods.

- Negotiate (for NTLM authentication only)
- Digest
- NTLM
- Basic
- Anonymous (no authentication required)

For the Negotiate method you must use a Windows client device and must start the SGD Client manually.

If the HTTP proxy server supports multiple authentication methods, the SGD Client selects a method automatically. The selected method is based on the order of preference shown in the above list. Negotiate has the highest order of preference, Basic has the lowest order of preference.

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
Sun Ray Software on Oracle Solaris (SPARC platforms)	GNOME PDF Viewer (`gpdf`) Adobe Reader (`acroread`)
Sun Ray Software on Oracle Solaris (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.

On Windows 8 platforms, the Reader app is not supported as a PDF viewer.

On tablet devices, the browser plug-in is used to display PDF files.

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 Table 2.6, “Supported Installation Platforms for the SGD Gateway”.

Table 2.6 Supported Installation Platforms for the SGD Gateway

Operating System	Supported Versions
Oracle Solaris on SPARC platforms	Solaris 10 [at least version 8/11 (update 10)]

Operating System	Supported Versions
	Solaris 11
Oracle Solaris on x86 platforms	Solaris 10 [at least version 8/11 (update 10)] Solaris 11
Oracle Linux (64-bit only)	5 (at least version 5.8) 6 (at least version 6.2)

Note

This table shows the installation platforms that Oracle has tested with this release of SGD. For up to date information on supported platforms, see knowledge document ID 1416796.1 on My Oracle Support (MOS).

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.

Note

If your users connect to SGD from a tablet device, using the SGD Gateway is the only supported method of firewall traversal.

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

2.3.1.1 Virtualization Support

The SGD Gateway is supported and can be installed in an Oracle virtualized environment. If you encounter a problem when using an unsupported virtualization environment, you may be asked to demonstrate the issue on a non-virtualized operating system to ensure the problem is not related to the virtualization product.

Installation in zones is supported for Oracle Solaris platforms. 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 for this release.

SGD Version	Platforms No Longer Supported
5.2	Oracle Linux (32-bit platforms)

2.3.2 Network Requirements

IPv6 network addresses are not supported. See the *Oracle Secure Global Desktop Gateway Administration Guide* for details of network requirements for the SGD Gateway.

2.3.3 SGD Server Requirements for the SGD Gateway

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

- **Firewall forwarding.** Firewall forwarding must not be enabled for SGD servers used with the Gateway.
- **SGD version.** Always use version 5.2 of SGD with version 5.2 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.

2.3.4 Third Party Components for the SGD Gateway

The SGD Gateway includes the following third party components:

- **Apache web server.** The Apache web server supplied with the SGD Gateway is Apache version 2.2.29.

  The web server includes the standard Apache modules for reverse proxying and load balancing. The modules are installed as Dynamic Shared Object (DSO) modules.
- **Java technology.** The SGD Gateway includes Java 8 update 31.

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*.

- 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)
- 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) [1]

Table 2.7, “Supported Installation Platforms for the SGD Enhancement Module” lists the supported installation platforms for the SGD Enhancement Module.

Table 2.7 Supported Installation Platforms for the SGD Enhancement Module

Operating System	Supported Versions
Microsoft Windows (64-bit)	Windows Server 2008 R2, 2012 R2
Oracle Solaris on SPARC platforms	Solaris 10 8/11 (update 10) or later Solaris 11 Trusted Extensions versions of the above
Oracle Solaris on x86 platforms	Solaris 10 8/11 (update 10) or later Solaris 11 Trusted Extensions versions of the above
Oracle Linux (32-bit and 64-bit)	5 6

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*.

For best results, ensure that the version of the Enhancement Module is the same as the SGD server version.

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 SGD Enhancement Module is supported and can be installed in an Oracle virtualized environment. If you encounter a problem when using an unsupported virtualization environment, you may be asked to demonstrate the issue on a non-virtualized operating system to ensure the problem is not related to the virtualization product.

[1] PulseAudio audio module is supported on Oracle Linux 6 and Oracle Solaris 11 platforms only.

Installation in zones is supported for Oracle Solaris platforms. The Enhancement Module 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 the Enhancement Module in a labeled zone. Do not install in the global zone.

2.4.2.2 Retirements to Supported SGD Enhancement Module Installation Platforms

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

SGD Version	Platforms No Longer Supported
5.2	Windows Server 2008
	SUSE Linux Enterprise Server 10, 11
	Oracle Solaris 8, 9 (on SPARC platforms)

2.4.2.3 Network Requirements

IPv6 network addresses are not supported. See the *Oracle Secure Global Desktop Installation Guide* for details of network requirements for SGD.

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 2012, 2012 R2 [2]
- Windows Server 2008, 2008 R2
- Windows Server 2003, 2003 R2
- Windows 7 SP1
- Windows 8, 8.1

On Windows 7 and Windows 8 platforms, only full Windows desktop sessions are supported. Running individual applications is not supported. Seamless windows are also not supported.

SGD supports RDP connections to virtual machines (VMs) running on Oracle VM VirtualBox and Microsoft Hyper-V.

[2] Includes Windows Hyper-V guests on Windows Server 2012 R2.

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 2.8 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

Some Windows Server platforms 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

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 set the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\fDisableAudioCapture` registry subkey to `0`.

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.

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

With Microsoft Windows Server, 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 most secure connection method.

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* 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.

To print from a UNIX or Linux system application server using CUPS, the version of CUPS must be at least 1.4.2.

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 1.4.1`
- `xkeyboard-config 2.9`

The following versions of X.org dependencies are used:

- `Mesa 9.2.5`
- `pixman 0.32.4`
- `freetype 2.4.9`
- `fontconfig 2.11.1`

2.4.4.2 Supported X Extensions

SGD supports the following X extensions for X applications:

- BIG-REQUESTS
- Composite
- DAMAGE
- DOUBLE-BUFFER

- GLX
- Generic Event Extension
- MIT-SCREEN-SAVER
- MIT-SHM
- RANDR
- RECORD
- RENDER
- SGI-GLX
- SHAPE
- SYNC
- X-Resource
- XC-MISC
- XFIXES
- XINERAMA
- XInputExtension
- XKEYBOARD
- XTEST

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*.

This release of SGD has been tested with version 3.5.1 of Oracle VDI.

2.4.6 Microsoft Hyper-V

This release of SGD supports connections to a Microsoft Hyper-V guest running on a Windows Server 2012 R2 host.

Integration with Microsoft Hyper-V is supported by configuring a Windows application object, as described in the *Oracle Secure Global Desktop Administration Guide*.

The enhanced session mode feature of Hyper-V can be used with Windows Server 2012 R2 and Windows 8.1 virtual machines.

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 5.2 release.

3.1.1 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 workspace 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.

3.1.2 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.

3.1.3 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.

3.1.4 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: On Oracle Linux 6 platforms, you can use the `padsp` PulseAudio OSS wrapper script to ensure compatibility with PulseAudio.

3.1.5 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.

3.1.6 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.

3.1.7 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.

3.1.8 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 has been seen on Windows 7 client devices.

Cause: A known issue with some versions of Windows.

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

3.1.9 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.

3.1.10 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 for SGD on Linux platforms, 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.

3.1.11 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
```

3.1.12 13354844, 14032389, 13257432, 13117470, 16339876 – 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.
- Terminal windows, such as a VT420 application, may not be sized correctly.

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.
- To ensure that VT420 terminal windows are sized correctly, you may need to install the required fonts. For example, on Ubuntu Linux 12.04 client platforms install the following font packages:

```
$ sudo apt-get install xfonts-traditional
$ sudo apt-get install xfonts-100dpi
$ sudo apt-get install xfonts-75dpi
```

3.1.13 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.

3.1.14 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.

3.1.15 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.

3.1.16 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.

Ensure that the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\AllowHigherColorDepth` registry entry described in the Microsoft hotfix procedure is set to `1`.

3.1.17 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.

3.1.18 14690706 – Display Issues on a Tablet Device When the RANDR X Extension is Disabled

Problem: The user experience on a tablet device may be poor if the RANDR X extension is disabled for the application. For example, you may notice that a desktop application does not fill the screen if you rotate the display.

Cause: A known issue if the RANDR X extension is disabled for the application. The RANDR extension provides enhanced display support for applications.

Solution: Enable the RANDR extension for the application object. This is described in the Enabling the RANDR Extension for Applications section in the *Oracle Secure Global Desktop Administration Guide*.

3.1.19 15903850 – Printing From a Tablet Device Fails Sometimes

Problem: Tablet device users may not be able to print from some applications.

Error messages such as the following may be seen:

```
Nov 27, 2012 11:56:59 AM com.oracle.sgd.webserver.printing.PrintServlet processRequest
SEVERE: Exception occurred in servlet javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid
certification path to requested target
```

The issue is seen when the print job and the user session are hosted on different SGD servers in the array. This situation may occur in the following scenarios:

- When an SGD server in the array is also used as an application server.
- When application session load balancing is used for the array.

Cause: This is a certificate trust issue. One or more SGD servers in the array are secured using an untrusted SSL certificate, such as a self-signed certificate.

Solution: On each SGD server, import the SSL certificates from the other array members into the CA certificate truststore. This process is described in the The CA Certificate Truststore section in the *Oracle Secure Global Desktop Administration Guide*.

The SSL certificate for an SGD server is at `/opt/tarantella/var/tsp/cert.pem`.

The CA certificate truststore for an SGD server is at `/opt/tarantella/bin/jre/lib/security/cacerts`.

3.1.20 16003643, 17043257 – Currency Symbols Are Not Displayed Correctly on a Tablet Device

Problem: When running SGD applications on an iPad or Android tablet, currency symbols such as pound (£), euro (€), and yen (¥) may not display correctly.

Cause: A known issue with displaying extended characters, such as currency symbols, on a tablet device.

Solution: No known solution. Where possible, use characters that are available on a US English keyboard.

3.1.21 16244748 – SGD Client Does Not Install When Using a Sun Ray Client

Problem: When using a Sun Ray Client to log in to SGD, the SGD Client may not install. The issue has been seen when the Sun Ray server is using the scbus v2 smart card bus protocol.

Cause: A known issue if the Sun Ray server is using the scbus v2 protocol.

Solution: A workaround is to disable smart card services on the Sun Ray server host. For example, on Oracle Solaris platforms use the following command:

```
# svcadm disable pcscd
```

3.1.22 16275930 – Unable to Access SGD Servers When Using the SGD Gateway

Problem: When connecting through an SGD Gateway, users are unable to access the SGD servers in the array. When they attempt to log in to an SGD server or use the Administration Console, their browser is redirected to an error page.

The issue is seen when the Gateway is configured as follows:

- The port used for incoming connections is not the default port, port 443.
- Connections between the Gateway and the SGD servers in the array are not secure.

These settings are usually configured during installation of the Gateway.

Cause: A known issue with this specific Gateway configuration.

Solution: Use the following workaround.

On the Gateway host, edit the `opt/SUNWsgdg/httpd/`*`apache-version`*`/conf/extra/gateway/httpd-gateway.conf` file.

Locate the `ProxyPassReverse` directive. For example:

```
ProxyPassReverse / http://gw.example.com:80/
```

Change the port number for the `ProxyPassReverse` directive, as follows:

```
ProxyPassReverse / http://gw.example.com:port-num/
```

where *`port-num`* is the port number used by the Gateway for incoming connections.

3.1.23 16310420 – External Keyboard Issue for iPad Tablets

Problem: When using an external keyboard with an iPad tablet, some keys may have no effect in SGD applications.

Examples of keys that may not work include modifier keys such as Alt and Ctrl, and function keys.

Cause: A known issue when using an external keyboard with an iPad tablet.

Solution: Use the on-screen keyboard to enter the missing keystroke.

For example, to enter the key combination Ctrl+C:

- Display the on-screen keyboard and tap the Ctrl key.

  This key is shown when you tap the `main` key.

- Use the external keyboard to enter the C character.

3.1.24 16420093, 17559489 – Log In Process Fails for Mac OS X Users

Problem: Users on Mac OS X platforms are unable to log in to SGD. Downloading of the SGD Client fails and the login process does not complete.

Cause: The issue is seen when Mac OS X users have not enabled Java Plug-in software for their browser. On other client platforms, warning prompts are usually shown in this case.

On some Safari browsers, the issue may still be seen after enabling Java Plug-in software. This is due to the Safe Mode feature of Safari.

Solution: Users must enable Java plug-in software on the client browser before logging in to SGD.

For example, on Safari browsers ensure that the Enable Java content in browser option is checked. This option is disabled by default on Safari browsers.

On some Safari browsers, additional configuration may be required. Enable the Run in Unsafe Mode option in the Manage Website Settings section of the Security tab.

3.1.25 16613748 – Unable to Generate Mobile Configuration Profiles For Some SGD Gateway Deployments

Problem: For some SGD Gateway deployments, Administrators may not be able to generate the `.mobileconfig` configuration profiles used for secure connections to tablet devices. The `mobile_profile_create.sh` script used to generate the configuration profiles fails.

The issue is seen when unencrypted connections are used between the SGD Gateway and the SGD servers in the array. In this scenario, the SGD servers are configured to use standard, unencrypted connections.

Cause: When security is disabled on an SGD server, the following directories required for the `.mobileconfig` configuration profiles are deleted:

- `/opt/tarantella/var/tsp/certs`. When generating configuration profiles, SSL certificates must be copied to this directory.
- `/opt/tarantella/var/docroot/certs`. The generated configuration profiles are stored in this directory.

Solution: Create the required directories manually on the primary SGD host:

```
# mkdir -p /opt/tarantella/var/tsp/certs/gateway
# mkdir -p /opt/tarantella/var/tsp/certs/array
# chown -R  ttasys:ttaserv /opt/tarantella/var/tsp/certs
# mkdir /opt/tarantella/var/docroot/certs
# chown root:ttaserv /opt/tarantella/var/docroot/certs
```

You can then generate the configuration profiles as described in How to Configure the SGD Gateway for Connections From Tablet Devices Using Untrusted Certificates in the *Oracle Secure Global Desktop Gateway Administration Guide*.

3.1.26 16814553 – Multiple Authentication Prompts When Accessing My Desktop Using a Safari Browser

Problem: Users may see multiple authentication prompts when they try to access the My Desktop application, either from the SGD web server Welcome page or by going to the My Desktop URL.

The issue is seen when the following apply:

- Web authentication is the authentication mechanism for SGD.
- A Safari browser is used to access SGD, from a Mac OS X or iOS client device.

Cause: A known issue with the Safari browser.

Solution: No known solution. The user is logged in to SGD after negotiating the authentication prompts.

3.1.27 16854421 – Unexpected Text Characters When Using Android Client

Problem: When using an Android tablet to enter text in an application displayed through SGD, the displayed text may sometimes not match the input character.

For example, the character following a period (`.`) may always be displayed in upper case.

Cause: This issue is caused by the predictive text features of Android. By default, auto-capitalization and auto-correction are enabled for an Android keyboard.

Solution: Turn off Auto-Capitalization and Auto-Correction for the Android keyboard. See your Android documentation for details of how to do this.

3.1.28 17601578 – Poor User Experience When Displaying Applications on Mac OS X Platforms

Problem: Users on some Mac OS X platforms may experience screen refresh and other performance issues when displaying SGD applications.

Cause: This issue is caused by the App Nap power-saving feature introduced in Mac OS X 10.9.

Solution: Turn off the App Nap feature for the SGD Client, as follows:

- Locate the SGD Client application in Finder and Command-click the application name.
- Choose the Get Info option, then select the Prevent App Nap check box.

3.1.29 19875716 – Application Close Issues When Using Safari Browser on iOS 8

Problem: On the tablet workspace, the following user interface features for closing an application may not work correctly when using the Safari browser on iOS 8 client devices:

- The Close icon on the drop-down toolbar.
- The Close button on the Application Disconnected dialog. This dialog is shown when you tap the close window decoration on an application window.

Cause: A known issue with some versions of the Safari browser.

Solution: A workaround is to close the browser tab that displays the running application.

3.1.30 19996614 – Audio is Not Played on a Linux Client Device

Problem: Audio output from applications is not played on a Linux client device.

Cause: This issue is due to missing ESD library dependencies on some Linux client platforms.

Solution: The workaround is to install the required libraries and restart the pulseaudio daemon, as follows:

Oracle Linux 6 platforms:

```
# yum install pulseaudio-esound-compat esound-libs.i686
$ pulseaudio -k
```

Ubuntu Linux 14.04 platforms:

```
$ sudo apt-get install pulseaudio-esound-compat libesd0:i386
$ pulseaudio -k
```

Ubuntu Linux 12.04 platforms:

```
$ sudo apt-get install pulseaudio-esound-compat
$ pulseaudio -k
```

3.1.31 20421590 – Lock File Issues With Oracle Access Manager WebGate

Problem: Single sign-on authentication does not work when using some versions of the Oracle Access Manager WebGate 11gR2.

Cause: The WebGate is unable to create lock files on the SGD host.

This is caused by changes in the file locking implementation, introduced in version 11.1.2.2.0 of the WebGate.

Solution: In the `webgate.conf` configuration file for the WebGate, set the value of the `WebGateLockFileDir` directive. This directive specifies the location to create WebGate lock files.

The value must be a directory that is writeable by the `ttaserv` system user. For example, `/opt/tarantella/webserver/apache/`*`apache-version`*`/logs`.

3.1.32 20220383 – Proxy Authentication Dialog Issue

Problem: When users connect to SGD through a proxy server, the proxy authentication dialog does not display the authentication method or authentication realm used by the proxy server. This can cause confusion when the proxy server supports multiple authentication methods, and users have different credentials for different authentication methods.

Cause: A known issue when using a proxy server that is configured to use multiple authentication methods.

Solution: No known solution at this time.

3.1.33 20463642 – Credential Caching Issues for HTTP Proxy Authentication on Windows Clients

Problem: When users connect to SGD through an HTTP proxy server from a Windows client device, cached credentials are not used as expected.

The following issues have been seen:

- For Basic or Digest authentication methods, cached credentials are not used. The user is always prompted to enter credentials, regardless of whether credentials have previously been cached.
- For NTLM or Negotiate methods, cached domain credentials are not used. If the domain requested by the proxy server does not match the domain used to log in to Windows, the user is prompted for

credentials. The SGD Client does not attempt to use alternative domain credentials stored in Windows Credential Manager.

Cause: Known issues when connecting to SGD through an HTTP proxy server from a Windows client device.

Solution: No known solution at this time.

3.1.34 20676754 – Legacy Settings Present in SGD Gateway Setup Program

Problem: In release 5.2, the SGD Gateway setup program incorrectly shows an option on whether to configure secure connections between the Gateway and the SGD servers in the array. The same option is shown when using the `gateway config create` command.

This is a legacy option that is no longer required. In release 5.2, the Gateway selects the required security level automatically for connections to SGD servers in the array.

Cause: A known issue with the release version of SGD 5.2.

Solution: Accept the default setting for the secure connections option in the Gateway setup program. The issue will be fixed in a future software update.

3.1.35 20693954 – Audio Recording Issue for Linux Clients

Problem: Audio recorded from a Linux client device by the `audiorecord` command running on an Oracle Solaris application server is not recorded correctly. White noise is heard on playback.

Cause: The default audio format for `audiorecord` is u-law. When recording from a Linux client device, this audio format is not recorded correctly by the SGD UNIX audio input service.

Solution: Change the audio format used by the `audiorecord` command. Specify the linear encoding option, as follows:

```
audiorecord -e linear audio-file
```

where `audio-file` is the output file name.

3.1.36 20506611 – Enhancement Module Installation Issue on Oracle Linux UEK R3

Problem: Installation of the SGD Enhancement Module may fail on Oracle Linux versions which use the Unbreakable Enterprise Kernel Release 3 (UEK R3) kernel.

The error message `Unable to locate source tree` is shown during installation.

Cause: The Enhancement Module installation program is unable to locate the kernel headers for the UEK R3 kernel.

Solution: Use the following command to install the required kernel header packages:

```
# yum install kernel-uek-devel-$(uname -r)
```

3.1.37 20678796 – Mac OS X Client Device Uses Multiple CALs

Problem: Connections to a Windows application server from a Mac OS X client device may use more client access licenses (CALs) than expected. The issue is seen when using both the SGD Client and the Microsoft Remote Desktop Client on the same Mac OS X client device.

Cause: A known issue when using SGD with some versions of the Microsoft Remote Desktop Client that are downloaded from the Mac App Store.

Such versions of the Microsoft Remote Desktop Client may not store CALs in the default shared directory location used by the SGD Client: `/Users/Shared/Microsoft/Crucial RDC Server Information`.

Solution: No known solution at present.

3.2 Bug Fixes in Version 5.2

The following table lists the significant bugs that are fixed in the 5.2 release.

Table 3.1 Bugs Fixed in the 5.2 Release

Reference	Description
20625580	FAILURE TO PROCESS A PRINT JOB CAN PREVENT JSERVER FROM STARTING
20594916	TTASWM.EXE SPINS ON WINDOWS 2012R2 WHEN STARTED FROM A NON-SGD LOGIN
20547500	CAPS LOCK ON CLIENT NOT REFLECTED IN SGD-HOSTED WINDOWS XP DESKTOP
20380879	HANGUL AND HANJA KEYS ARE REVERSED ON A WINDOWS CLIENT
20344134	SECURE ARRAY PEER SOAP CONNECTIONS NEED A CONFIGURABLE TIMEOUT VALUE
20344079	X11 BELL DOES NOT WORK AFTER UPGRADE FROM 4.6
20172841	DRAGGING QT DESIGNER 3.3 DIALOG BOX CONTROLS IN CLIENT WINDOW MANAGEMENT MODE LEAVES A TRAIL
20095450	XPE MISSING PATCH TO BASE INTERNAL SERVER START TIME AT ZERO
20094561	XPE PART OF THE FORCE3BUTTONMOUSE PATCH IS MISSING
20093956	XPE CANNOT FIND FONT ENCODINGS FILES, IF SGD INSTALL DIRECTORY IS NOT DEFAULT
20068741	XAIP PERFORMANCE TEST CAUSES HTML5 CLIENT LOCKUPS ON ANDROID 5 DEVICES
20005147	HANGUL AND HANJA KEYS ON KOREAN PC106 KEYBOARD DO NOT WORK
19957512	COPY AND PASTING PRODUCES CORRUPTED CHARACTERS
19951617	ALL OBJECTS IN ADMIN CONSOLE APPEAR EMPTY WHEN OBJECT DELETE COMMAND IS RUN WITHOUT A VALUE
19913235	RECURSIVE FIND IN LINUX CLIENT HOME DIRECTORY CAUSES TERMINAL TO HANG
19821584	"THE DATABASE ROOTED AT: /OPT/TARANTELLA/VAR/ENS HAS BECOME CORRUPT" ERROR SHOWN
19815339	EMULATORSESSION SHADOW COMMAND DOES NOT ACCEPT ANY ARGUMENTS AND DOES NOT SET EXIT STATE
19786967	GNOME-SESSION ON OPENSUSE 13 CRASHES TTAXPE
19730151	CORRUPT PASSWORD CACHE FILE CAN CRASH SGD SERVER
19717933	WINDOWS SESSION FREEZES ON LOGIN SCREEN BUT APPLICATIONS REMAIN ACTIVE

Reference	Description
19644071	ADD SUPPORT FOR IOS8
19635090	WORKSPACE BUTTONS SHOULD SET IE=EDGE META INFO
19579558	STOP USING SHA-1 FOR CERTIFICATE SIGNATURES
19543926	UNABLE TO SUCCESSFULLY LAUNCH A SOLARIS 10 CDE DESKTOP
19530415	SGD ENHANCEMENT MODULE INSTALL AND NON-DEFAULT UMASK HANDLING
19524048	COPY/PASTE TO CLIENT FROM WINDOWS 2008R2 FAILS AFTER DESKTOP RESIZE USING XRANDR
19466534	SLOW PERFORMANCE WITH LARGE FILES USING CLIENT DRIVE MAPPING ON LINUX PLATFORMS
19464483	SUPPORT COPYING AND CUSTOMIZATION OF THE SGD WORKSPACE
19446980	WORKSPACE GROUP UPDATE USER INTERFACE ON CHROME BROWSER CAN BE UNRELIABLE
19438994	WORKSPACE IS UNABLE TO USE A SESSION TOKEN TO JOIN A USER SESSION
19362594	WORKAROUND TO START KIOSK MODE APPLICATION ON A SECONDARY MONITOR
19335113	INCREASE DEFAULT RESOLUTION FOR INDEPENDENT WINDOW APPLICATIONS TO 1024X768
19285409	CHANGE DEFAULT COLOR DEPTH FOR X APPLICATIONS TO 24 OR 8/24 BPP
19274698	FAIL-FAST LOGIC IN PREFLIGHT CHECKS CAN CAUSE UNNECESSARY ISSUES
19261911	INDEPENDENT WINDOW MODE XFCE DESKTOP LOSES CONTENTS OR DISAPPEARS WHEN RESIZED
19260585	INFINITE LOOP IN TOMCAT WHEN VIRTUAL SERVER BROKER CANNOT BE LOADED
19173034	ADD CHROMEBOOK CLIENT SUPPORT FOR SECURE GLOBAL DESKTOP
19165309	CHANGE OUTDATED TERM "NT DOMAIN" IN WINDOWS APPLICATION AUTHENTICATION DIALOG
19164767	ENTER KEY GENERATES WRONG KEYSYM ON MAC CLIENT
19158037	WINDOWS DRIVE MAPPING FAILING WITH WINDOWS 8.1 AND 2012R2.
19150260	CANNOT INTERACT WITH FIREFOX MENUS UNDER SOLARIS
19141020	SGD CLIENT EVENTS SENT TO WEBSERVER IN THIN WORKSPACE
19129550	DISPLAY UNDER MENUS NOT REDRAWN USING RDP 5.2 (WINDOWS SERVER 2003)
19078969	PEMANAGER CRASH ON APPLICATION LAUNCH WHEN APPLICATION SERVER ADDRESS ATTRIBUTE IS BLANK
19076777	CORRECTLY PASS X SERVER MOUSE GRABS TO THE CLIENT DEVICE
19071549	SUPPORT HYPER-V VIRTUAL MACHINE CONNECTIONS
18994939	SEND RDP BITMAPS TO THE CLIENT DEVICE
18977225	X APPLICATIONS WITH NO BACKGROUND CAN RENDER POORLY
18977186	STRANGE CHARACTERS APPEAR IN DIGIT FIELD OF X APPLICATION
18815048	EXECPE SORT ENVIRONMENT VARIABLE SUBSTITUTE ISSUE
18777683	PATCH.LOG IS ROTATED AND DATA WILL BE LOST

Reference	Description
18773785	AIP REDRAW HINT IS NOT ALWAYS HONORED BY SGD CLIENT
18717142	SUPPORT AUTHENTICATION TO WINDOWS 2012 R2 ACTIVE DIRECTORY
18705210	FINER CONTROL OVER AUTOCOMPLETE IN FORMS
18688883	MAC APPLICATION BUNDLE SHOULD START WITH -PROMPT ARGUMENT
18675963	PORT ESCALATION FIX FOR WSVEVENT READER
18669362	SSL DAEMON GENERATES DOUBLE BYTES WHEN CONNECTIONS RECEIVED FROM GATEWAY
18663011	STOP SETTING TOS FIELD (QUALITY OF SERVICE PARAMETERS) ON IP PACKETS
18497439	UNIX/MAC CLIENTS SHOULD HONOUR INITIAL FOCUS HINT
18467797	SGD AUDIO OUTPUT CRACKLES AND CLICKS
18391292	LANGUAGE SELECTION IN SGD LOGIN PAGE
18320241	SUPPORT RDP FRAME MARKERS THROUGH SGD (AVOID TILING EFFECTS)
18314177	TTASSL PROCESS SPINS ON A DECOMPRESSION ERROR
18305404	INTERMITTENT WORKSPACE ITEM LAUNCH FAILURE
18273837	GATEWAY STOPS ACCEPTING WEBSOCKET CONNECTIONS AFTER CONNECTION FAILURES
18243152	CLIENT DRIVE MAPPING STOPS WORKING AFTER CLIENT NETWORK RECONNECTIONS
18237573	CLIENT DOES NOT IDENTIFY DISCONNECTS WHEN USING AN SGD GATEWAY
18197560	KEEP LAUNCH CONNECTION OPEN GRAYED OUT WHEN USING TELNET AS CONNECTION METHOD
18193547	MISLEADING MESSAGE WHEN JAVA NOT AVAILABLE ON CLIENT
18188255	WEBSOCKET HTTP HEADER CHECKING IN GATEWAY IS CASE-SENSITIVE
18186719	USERS UNABLE TO LOGIN TO SGD VIA THE GATEWAY AFTER ABOUT TWO WEEKS
18181729	WINDOWS APPLICATION LAUNCH FAILURE WITH SPACES IN WORKING DIRECTORY
18174959	KEY REPETITION DOES NOT WORK WHEN WINDOWS MANAGEMENT KEYS ARE ENABLED
18174496	CHANGE IN LANGUAGE DOES NOT TAKE EFFECT UNLESS COOKIES ARE CLEARED
18148581	NUMERIC KEYPAD DOES NOT WORK WITH HTML5 CLIENT
18130177	XTEST KEYBOARD DEVICE HAS WRONG KEYMAP LOCALE
18130151	UNABLE TO SET THE FOCUS ON CLIENT WINDOW MANAGEMENT WINDOWS
18130083	ENABLE SOFTWARE CURSORS FOR X APPLICATIONS
18122970	UNABLE TO PRE-POPULATE DOMAIN VALUE WHEN USING HTML5 CLIENT
18090070	CLIENT WINDOW MANAGEMENT APPLICATION GOES BLANK WHEN A WINDOW IS CLOSED
18062622	SELECTING KEYBOARD LAYOUT IN USER PROFILE GENERATES INCORRECT KEYCODES ON UBUNTU CLIENT
18055385	ADD SUPPORT FOR INTERNET EXPLORER 11

Reference	Description
17993225	SGD GATEWAY CONNECTION RESETS, SOMETIMES WITH ERROR, SOMETIMES WITH EMPTY FRAME
17993069	BUG IN NFS READDIR PRIMITIVE CAUSES DIRECTORY LISTING TO HANG
17909288	XML PARSING ERRORS IN THE SERVER LEAVE THREADS WAITING ON TOMCAT
17897177	APACHE REDIRECTION DOES NOT WORK WITH NON-STANDARD SSL PORTS
17896235	CANNOT USE SELF SIGNED CERTICATES FOR SECURE LDAP CONNECTION ON SOLARIS 11
17895412	PRINTER UNINSTALL TRIES REMOVAL TWICE AND DISPLAYS INCORRECT INFORMATION ON SOLARIS 11
17865040	NO ERROR SHOWN IF "MY DESKTOP<SUFFIX>" EXISTS, BUT "MY DESKTOP" DOES NOT
17804055	APPLICATION CANNOT BE STARTED AFTER SHADOWING ANOTHER APPLICATION
17803553	EVENTS FOR CLIENT KEY REPEATS ARE IN THE WRONG ORDER
17803379	SGD CLIENT CRASHES ON WINDOWS CLIENT DEVICES
17768321	ADD SERVER REPORTING CAPABILITIES TO ADMINISTRATION CONSOLE, OR SIMILAR
17705395	ABILITY TO RELOCATE THE SGD CLIENT ARCHIVES OUTSIDE A SECURED WEB PATH
17555509	REMOVE INVALID HTML ALT ATTRIBUTE FROM ANCHOR ELEMENTS
17534933	EMULATOR SESSION SHADOW COMMAND IS MISSING
17531295	SHADOWING FAILS ON SOLARIS 11
17390680	SUPPORT FOR NTLM AUTHENTICATION WHEN CONNECTING TO SGD THROUGH PROXY
17289706	DETECTION OF SWISS FRENCH KEYBOARD LAYOUT SEEMS TO FAIL
17277413	SGD REQUIRES COMPONENTS THAT ARE NOT LISTED IN THE RPM
17269834	STYLES SHOULD NOT BE DUPLICATED IN THE LOCALIZED VERSIONS OF STYLESHEETS
16939518	CREATE A DEDICATED USER AND GROUP FOR THE GATEWAY
16928078	CONNECTION INFORMATION RETURNED BY TARANTELLA STATUS COMMAND DISPLAYS SERVER'S PEERDNS NAME INSTEAD OF EXTERNAL NAME
16897490	PULL-DOWN HEADER IS BLANK OTHER THAN MINIMISE/RESTORE/CLOSE BUTTONS ON LINUX CLIENTS
16839079	SOLARIS PACKAGES DO NOT CHECK ARCHITECTURE BEFORE INSTALL
16748391	BATCHED CONFIG EDIT OPERATIONS CAN FAIL DURING UPGRADE
16680079	SGD CLIENT INSTALLERS SHOULD HAVE UPGRADE CODE CHANGED ON MAJOR VERSIONS
16671558	MAC CLIENT FAILS TO GET CORRECT INPUT LANGUAGE FOR WINDOWS APPLICATION SERVER
16634591	SGD PROBLEMS WITH GNOME/DBUS APPLICATIONS
16520340	GATEWAY STATUS PROVIDES NO USEFUL INFORMATION

Reference	Description
16356068	ON SOLARIS 11 MAKE ALL SYSTEM ADMINISTRATORS WITH ROLES=ROOT SGD ADMINISTRATORS
16355754	SOMETIMES APPLICATION FAILS TO LAUNCH WHEN OPENING MULTIPLE APPLICATIONS SIMULTANEOUSLY
16241757	TARANTELLA SECURITY DISABLE COMMAND PRINTS USER PROMPT BUT DOES NOT WAIT FOR USER INPUT
16023267	NO APPLICATIONS SHOWN ON WORKSPACE IF ONE APPLICATION HAS A MISCONFIGURED APPLICAITON SERVER ASSIGNMENT
16002868	TARANTELLA OBJECT NEW_ORG COMMAND REQUIRES A WEBTOP THEME
15992013	ERROR "FAILED TO START MYDESKTOP" IS AN IMAGE
15984645	SUPPORT FOR AUDIO USING ALSA OR PULSEAUDIO, INSTEAD OF OSS
14826359	INDEPENDENT WINDOW X APPLICATION IS SUSPENDED ON CLOSING, THOUGH CLOSE ACTION IS SET TO "END SESSION"
14408344	RANDR KIOSK APPLICATION DOES NOT SPAN ALL MONITORS ON UNIX AND SOLARIS CLIENTS
14404371	DURING APPLICATION AUTHENTICATION, NON-ENGLISH INPUT CHARACTERS ARE GARBLED
14375629	INCORRECT FONT SELECTED BY SOLARIS CLIENT
14244277	SPECIAL KEYS (COPY, CUT, PASTE) ON SUN KEYBOARD DO NOT WORK
14021467	LANGUAGE SELECTION ON LOGIN PAGE DOES NOT WORK FROM SECOND LOGIN
13971245	PKGRM DOES NOT CLEAN UP /VAR/SADM/INSTALL/CONTENTS ON SOLARIS 11
13897352	APACHECTL IN GATEWAY USES AN INCORRECT PATH TO HTTPD.CONF FILE
13843515	PULL-DOWN HEADER IS NOT CENTERED FOR A UNIX KIOSK APPLICATION ON A MULTI-MONITOR SETUP
13640907	ADMINISTRATION CONSOLE SHOULD SUPPORT PEER CERTIFICATE VERIFICATION
13474208	BLEEDTHROUGH AFFECT SEEN WITH GIMP APPLICATION
12669137	OPTIMISE UPDATE OF LAUNCH DETAILS FOR UNIX VERSION OF SGD CLIENT
12642777	ENHANCING ADMINISTRATIVE EXPERIENCE WITH MAXWEBTOPSESSIONS PARAMETER
12299764	ENABLE RDP 6 BITMAP DECODE VECTOR OPTIMIZATIONS
12298300	REQUEST FOR A STANDARDIZED APPLICATION MONITORING INTERFACE FOR SGD
12244407	ROUTING PROXY TOKEN SHOULD INCLUDE PROTOCOL PATH TO SGD SERVER

3.3 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 provide feedback or to ask a general question, you can post to the Secure Global Desktop Software Community Forum. Forums are Community-monitored and posting to the Secure Global Desktop Software Community Forum does not guarantee a response from Oracle. If you need to report an issue and

have an Oracle Premier Support Agreement, you should open a case with Oracle Support at https://support.oracle.com.

If you are reporting an issue, 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.

3.3.1 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.