ORACLE
Secure Global
Desktop

Deployment Considerations for Oracle Secure Global Desktop

ORACLE WHITE PAPER | APRIL 2018

Table of Contents

Introduction

The architecture described in this document demonstrates the design and testing of Oracle Secure Global Desktop deployments. It is intended to help IT departments plan an application deployment strategy with confidence that the configuration will meet their IT and business needs.

One of the biggest challenges IT organizations face today is how to provide users with access to their specific workspaces (applications and desktops) from any location around the globe at a moment's notice, reliably, securely? and with no performance degradation. In addition, administrators need to centrally administer access to individual workspaces across multiple locations worldwide. This is not always easy. For many customers, they have addressed these problems for thousands of employees by deploying workspaces using Oracle Secure Global Desktop. Some of the features that make Oracle Secure Global Desktop an ideal solution to these problems are:

- **Security**: All connections are encrypted and secured and all resources are protected from unauthorized use;
- **A consistent user interface**: Users can login to Oracle Secure Global Desktop from virtually any device in the world simply by going to a URL from a web browser and have access to their workspaces from anywhere;
- **Client software:** IT departments do not need to maintain software on the user's desktop, as long as the browser supports Java or Java WebStart. The user can access Oracle Secure Global Desktop with any supported web browser;
- **Clients never enter your network and data never leaves the data center:** Many IT departments chose VPN to provide encrypted access to resources over the network. With VPN the client device is being brought into your network and has access to data and can copy it to the client device. With SGD the client never enters your network and all the data stays in the data center; users simply and securely interact with provisioned applications and the data;
- **Session mobility:** Users can pause, resume or terminate their sessions from the dynamic browser-based Oracle Secure Global Desktop workspace. This includes the ability to suspend a session and then resume it from a different device in another location (e.g., suspending a session on a PC from the office and then resuming it on a tablet device from home). This, combined with eliminating maintenance of client software on thousands of desktop machines spread across multiple time zones, can save IT departments significant administrative overhead;
- **Simplicity and content control:** Centralized management of the applications and environments that a user has access to is built-in to Oracle Secure Global Desktop. Load-balanced pools of application servers allow the addition, removal or modification of servers to be completely transparent to end users;
- **Performance:** The Adaptive Internet Protocol (AIP) used by Oracle Secure Global Desktop, combined with Intelligent Array Routing (IAR), and various other performance features, allows for excellent performance even over high-latency WAN links. This is crucial since IT departments have large numbers of users distributed around the world accessing multiple applications for their daily work;
- **Monitoring:** By creating user defined Oracle Secure Global Desktop alerts in Oracle Enterprise Manager Grid Control, an IT department can continually monitor several deployment metrics such as 1) daily peak resource usage, 2) number of users, and 3) performance, via a simple dashboard that can be shared with executive management and operations teams.

System Requirements and Support

The version of Oracle Secure Global Desktop (SGD) that is current at the time this document is released is 5.4.

Use the following hardware requirements as a guide and not as an exact sizing tool. For detailed help with hardware requirements, contact your local Oracle sales office.

The requirements for a server hosting Oracle Secure Global Desktop can be calculated based on the following (please note, client requirements are different and are covered later in this document):

- Requirements to install and run Oracle Secure Global Desktop;
- Requirements for each user that logs in and runs applications.

The following are the requirements for installing and running Oracle Secure Global Desktop:

- 2GB of free disk space;
- 2GB of random-access memory (RAM);
- 1GHz processor;
- Network interface card (NIC).

This is in addition to what is required for the operating system itself and assumes the server is used only for Oracle Secure Global Desktop. The following are the requirements to support users who log in to Oracle Secure Global Desktop and run applications:

- Minimum 80MB memory for each user;
- 50MHz of CPU for each user.

A typical user with ten applications in the workspace and running two applications requires about 80MB of memory. For a 500 user deployment, where a typical user has two running applications, a total of 40GB memory and 5-15GHz CPU would be required. A typical application uses between 10-30MHz CPU, but actual CPU usage depends on the application. Busy applications can use between 50-100MHz CPU.

TABLE 1. SUPPORTED INSTALLATION PLATFORMS

OPERATING SYSTEM	SUPPORTED VERSIONS
ORACLE SOLARIS ON SPARC PLATFORMS	ORACLE SOLARIS 10 [AT LEAST VERSION 8/11 (UPDATE 10)] ORACLE SOLARIS 11 TRUSTED EXTENSIONS VERSIONS OF THE ABOVE
ORACLE SOLARIS ON X86 PLATFORMS	ORACLE SOLARIS 10 [AT LEAST VERSION 8/11 (UPDATE 10)] ORACLE SOLARIS 11 TRUSTED EXTENSIONS VERSIONS OF THE ABOVE
ORACLE LINUX (64-BIT ONLY)	7 (AT LEAST VERSION 7.0) 6 (AT LEAST VERSION 6.2) 5 (AT LEAST VERSION 5.8)

Virtualization Support

Installation is also supported on platforms hosted on a Type 1 (bare metal) hypervisor or a Type 2 hypervisor, for example Oracle VM VirtualBox, Oracle VM Server for x86, or Oracle VM for SPARC . Issues reported on 3rd party hypervisors will be tested on the appropriate Oracle hypervisors and if the problem cannot be reproduced, the customer will need to contact their virtualization vendor for assistance.

Installation in zones is supported for Oracle Solaris platforms. Oracle Secure Global Desktop 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 Oracle Secure Global Desktop in a labeled zone. Do not install Oracle Secure Global Desktop in the global zone.

Supported Applications and Protocols

You can use Oracle Secure Global Desktop 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.

Oracle Secure Global Desktop supports the following protocols for accessing applications:

- 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;

Networking Requirements

Oracle Secure Global Desktop is a 3-tier architecture: client – SGD Gateway/Server – Application Server.

When using Oracle Secure Global Desktop, client devices never connect directly to application servers. Instead they connect to Oracle Secure Global Desktop using Hypertext Transfer Protocol over SSL or TLS (HTTPS) and Oracle's Adaptive Internet Protocol (AIP). Oracle Secure Global Desktop then connects to the application servers on the user's behalf.

You must configure your network for use with Oracle Secure Global Desktop. The following are the main requirements:

- Oracle recommends the use of the SGD Gateway, which means the client only needs to be able to resolve the hostname(s) of the gateway systems, otherwise every SGD server host must have a Domain Name System (DNS) entry 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 Oracle Secure Global Desktop, you are asked for the DNS name to use for the Oracle Secure Global Desktop server. The DNS name must meet the following requirements:
  - In a network containing a firewall, use the DNS name that the Oracle Secure Global Desktop host is known as **inside** the firewall;
  - Always use fully-qualified DNS names for the Oracle Secure Global Desktop host. For example: us.example.com.

By default, Oracle Secure Global Desktop uses a query class of ANY for DNS lookups. Some firewall configurations might block this class of DNS lookups. This can lead to problems, for example when configuring Active Directory authentication using the Administration Console.

For commands where the Domain Name System (DNS) name of an Oracle Secure Global Desktop server must be specified (such as 'tarantella array join'), a warning message is shown if the fully- qualified DNS name is not used.

To be able to connect to Oracle Secure Global Desktop through a proxy server, client devices might need to be configured with the address and port number of the proxy servers. You might also need to configure Oracle Secure Global Desktop to give clients information about server-side proxy servers.

The Oracle Secure Global Desktop Administration Guide (available from http://www.oracle.com/technetwork/documentation/sgd-193668.html) has detailed information about all the ports used by Oracle Secure Global Desktop and how to use the product with firewalls.

Oracle recommends the use of the SGD Gateway explained in more detail further down. The gateway can be separate from the SGD server infrastructure and positioned in a DMZ. The gateway exposes only port 443 (and port 80 with redirect to 443) and encapsulates all traffic (HTTP and AIP) in SSL. When you use the SGD Gateway, client devices do NOT connect directly to Oracle Secure Global Desktop servers.

The connections between Oracle Secure Global Desktop servers and application servers are used to start applications on the application server, and to send and receive data from the application, such as key presses and display updates.

The level of security between Oracle Secure Global Desktop and your application servers depends on the types of application server and the protocols they use.

When connecting using the Telnet protocol, all communication and passwords are transmitted unencrypted. For secure connections to UNIX or Linux system application servers, use Secure Shell (SSH). SSH encrypts all communications between Oracle Secure Global Desktop hosts and encrypts passwords before they are transmitted. By default, Oracle Secure Global Desktop secures X displays using X authorization to prevent users from accessing X displays they are not authorized to access.

Windows applications use the Microsoft Remote Desktop (RDP) protocol. Connections are protected by RDP or TLS security with Network Level Authentication (NLA).

The level of security depends on the type of web server used to host the web application, as follows:

» **HTTP web servers** – All communication is unencrypted;
» **HTTPS web server** – All communication is encrypted.

For secure connections to web application servers, use HTTPS web servers.

Microsoft Windows Remote Desktop Services

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

Oracle Secure Global Desktop is tested against and supports RDP connections to the following versions of Microsoft Windows:

» Windows Server 2012, 2012 R2, 2016;
» Windows Server 2008, 2008 R2;
» Windows 7 SP1;
» Windows 8, 8.1;
» Windows 10.

Oracle continually monitors and tests Oracle Secure Global Desktop with later versions of Microsoft Windows and updates supported platforms accordingly.

Oracle Secure Global Desktop has also been successfully tested against Windows 2003 and 2003 R2, but these operating systems are no longer supported by Microsoft. On Windows 7, Windows 8 and Windows 10 platforms, only full Windows desktop sessions are supported. Running individual applications is not supported. Seamless windows are also not supported when connecting to these operating systems.

Oracle Secure Global Desktop supports the following Windows Remote Desktop Services features:

» Audio recording;
» Audio redirection;
» Clipboard redirection;

- Serial port mapping;
- Compression;
- Drive redirection;
- Multi-monitor;
- Network security (encryption level);
- Session directory;
- Smart card device redirection;
- Time zone redirection;
- Windows printer mapping.

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

Oracle Secure Global Desktop supports 8-bit, 16-bit, and 32-bit color depths in a Windows Remote Desktop Server session.

15-bit color depths are not supported. If this color depth is specified on the Remote Desktop Server, Oracle Secure Global Desktop automatically adjusts the color depth to 8-bit.

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

X and Character Applications

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

Oracle Secure Global Desktop 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 Oracle Secure Global Desktop 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 Oracle Secure Global Desktop.

Oracle Secure Global Desktop 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.

Oracle Secure Global Desktop includes an X server, based on X11R7.6. SGD supports the following X extensions for X applications:

- BIG-REQUESTS;
- Composite;
- DAMAGE;
- DOUBLE-BUFFER;
- GLX;
- Generic Event Extension;
- MIT-SCREEN-SAVER;
- MIT-SHM;
- NATIVE-WND;
- Present;
- RANDR;
- RDP;
- RECORD;
- RENDER;
- SCO-MISC;

» SGI-GLX;
» SHAPE;
» SYNC;
» X-Resource;
» XC-MISC;
» XFIXES;
» XINERAMA;
» XInputExtension;
» XKEYBOARD;
» XTEST;
» XTTDEV.

By default, Oracle Secure Global Desktop runs an Input Method (IM) for UNIX platform applications for all locales except C and POSIX.

SGD Enhancement Module

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

» Advanced load balancing;
» Client drive mapping (required for UNIX or Linux application servers only);
» Seamless windows (applies to Windows application servers only);
» Audio (required for UNIX or Linux application servers only).

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

TABLE 2. SUPPORTED INSTALLATION PLATFORMS FOR SGD ENHANCEMENT MODULE

OPERATING SYSTEM	SUPPORTED VERSIONS
MICROSOFT WINDOWS (64-BIT)	WINDOWS SERVER 2008 R2, 2012 R2
ORACLE SOLARIS ON SPARC PLATFORMS	ORACLE SOLARIS 10 8/11 (UPDATE 10) OR LATER ORACLE SOLARIS 11 TRUSTED EXTENSIONS VERSIONS OF THE ABOVE
ORACLE SOLARIS ON X86 PLATFORMS	ORACLE SOLARIS 10 8/11 (UPDATE 10) OR LATER ORACLE SOLARIS 11 TRUSTED EXTENSIONS VERSIONS OF THE ABOVE
ORACLE LINUX (32-BIT AND 64-BIT)	5, 6, 7

The OS versions are those that have been tested and Oracle monitors and updates the list periodically.

SGD Web Server

The SGD web server consists of an Apache web server and a Tomcat JavaServer Pages (JSP) technology container pre-configured for use with Oracle Secure Global Desktop. Oracle is committed to security and provides regular updates to the SGD web server components. The table lists the versions current at the time of publication.

TABLE 3. SGD WEB SERVER COMPONENTS

COMPONENT NAME	SGD VERSION 5.4 COMPONENT VERSION AT TIME OF RELEASE
APACHE HTTP SERVER	2.4.29
OPENSSL	1.0.2N
APACHE TOMCAT	7.0.82

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 256MB.

Supported Authentication Mechanisms

The following are the supported mechanisms for authenticating users to Oracle Secure Global Desktop:

- Lightweight Directory Access Protocol (LDAP) version 3;
- Microsoft Active Directory;
- Network Information Service (NIS);
- Microsoft Windows Domains;
- RSA SecurID;
- Web server authentication (HTTP/HTTPS Basic Authentication), including public key infrastructure (PKI) client certificates.

SGD Gateway

The SGD Gateway is a proxy server designed to be deployed in front of an Oracle Secure Global Desktop array in a demilitarized zone (DMZ). This enables the Oracle Secure Global Desktop array to be located on the internal network of an organization. Additionally, all connections can be authenticated in the DMZ before any connections are made to the Oracle Secure Global Desktop servers in the array.

The SGD Gateway can manage load balancing of Hypertext Transfer Protocol (HTTP) connections on behalf of Oracle Secure Global Desktop servers.

The SGD Gateway consists of the following components:

- Routing proxy: A Java technology-based application that routes Adaptive Internet Protocol (AIP) data connections and websocket connections to an Oracle Secure Global Desktop server. Keystores in the routing proxy contain the certificates and private keys used to secure connections for the SGD Gateway. The routing proxy uses routing tokens to manage AIP connections. A routing token is a signed, encrypted message that identifies the origin and destination Oracle Secure Global Desktop server for a route.
- Reverse proxy: An Apache web server, configured to operate in reverse proxy mode. The reverse proxy also performs load balancing of HTTP connections.

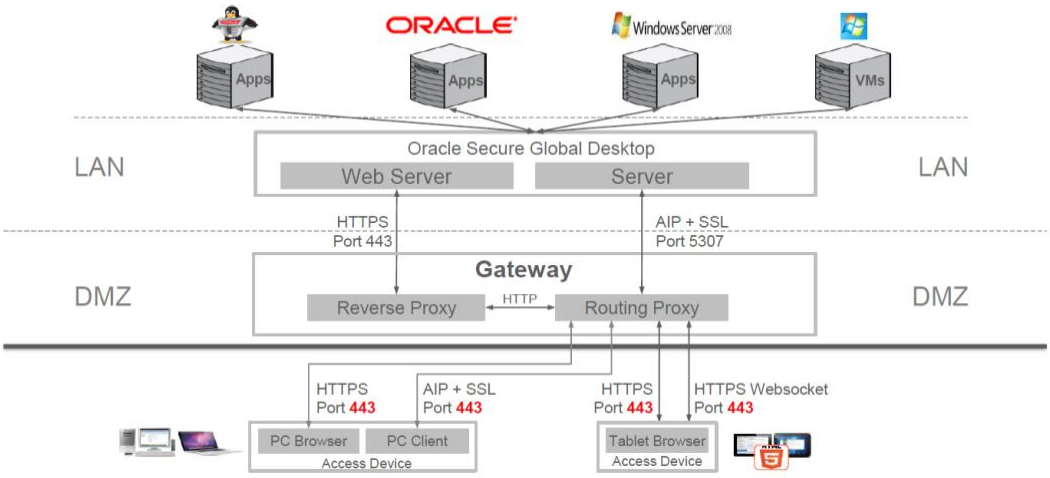

Figure 2. Example Oracle Secure Global Desktop deployment using SGD gateway

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

TABLE 4. SUPPORTED INSTALLATION PLATFORMS FOR SGD GATEWAY SERVER

OPERATING SYSTEM	SUPPORTED VERSIONS
ORACLE SOLARIS ON SPARC PLATFORMS	ORACLE SOLARIS 10 [AT LEAST VERSION 8/11 (UPDATE 10)] ORACLE SOLARIS 11
ORACLE SOLARIS ON X86 PLATFORMS	ORACLE SOLARIS 10 [AT LEAST VERSION 8/11 (UPDATE 10)] ORACLE SOLARIS 11
ORACLE LINUX (64-BIT ONLY)	5 (AT LEAST VERSION 5.8) 6 (AT LEAST VERSION 6.2) 7 (AT LEAST VERSION 7.0)

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

The following requirements apply for the Oracle Secure Global Desktop servers used with the SGD Gateway:

- Secure mode: By default, the SGD Gateway uses secure connections to Oracle Secure Global Desktop servers. Firewall forwarding must not be enabled;
- Oracle Secure Global Desktop version: It is best to use the same (or higher) version of the SGD Gateway as that of the Oracle Secure Global Desktop server;
- Clock synchronization: It is important that the system clocks on the Oracle Secure Global Desktop 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.

The Apache web server supplied with the SGD Gateway is Apache version 2.2.31. It includes the standard Apache modules for reverse proxying and load balancing. The modules are installed as Dynamic Shared Object (DSO) modules.

The SGD Gateway supports all the cipher suites available in the Java Virtual Machine. The following cipher suites are enabled by default:

- 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.

Other cipher suites can be configured by the administrator, as shown in the *Oracle Secure Global Desktop Gateway Administration Guide*

Array Failover

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

Array failover is disabled by default for an Oracle Secure Global Desktop array.

When array failover is enabled for an array, the array repairs itself automatically following the loss of the primary server.

In array failover, a secondary server in the array is upgraded automatically to become the primary server.

Oracle Secure Global Desktop supports automatic recovery of an array after failover.

The process of failover, followed by recovery of the original array formation is called *array resilience*.

Array join operations are now only permitted if the clock on the server joining the array is in synchronization with the other servers in the array. If the time difference is more than one minute, the array join operation fails.

Supported Versions of Active Directory

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

» Windows Server 2008;
» Windows Server 2008 R2;
» Windows Server 2012;
» Windows Server 2012 R2;
» Windows 2016.

Supported LDAP Directories.

Oracle Secure Global Desktop supports version 3 of the standard LDAP protocol. You can use LDAP authentication with any LDAP version 3-compliant directory server. However, Oracle Secure Global Desktop 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 on Windows Server 2008, 2008 R2, 2012 and 2012 R2 and 2016.

Other directory servers might work, but are not supported.

Supported Versions of SecurID

Oracle Secure Global Desktop 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.

Oracle Secure Global Desktop supports system-generated PINs and user-created PINs.

Supported Versions of Oracle Identity Management

Oracle Secure Global Desktop works with the following versions of Oracle Identity Management:

» Oracle Identity Management 11gR2 (11.1.2.x).

SSL Support

Oracle Secure Global Desktop supports TLS versions 1.0, 1.1, and 1.2.

Oracle Secure Global Desktop supports Privacy Enhanced Mail (PEM) Base 64-encoded X.509 certificates. These certificates have the following structure.

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

...certificate...

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

Oracle Secure Global Desktop supports the Subject Alternative Name (subjectAltName) extension for SSL certificates.

Oracle Secure Global Desktop also supports the use of the * wildcard for the first part of the domain name, for example *.example.com.

Oracle Secure Global Desktop 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 Oracle Secure Global Desktop 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.

Oracle Secure Global Desktop supports the use of external hardware SSL accelerators, with additional configuration.

Oracle Secure Global Desktop 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.

SGD Client

The following table lists the supported client platforms for the SGD Client. Also included are the latest tested and supported browsers.

TABLE 6. SUPPORTED CLIENT PLATFORMS

SUPPORTED CLIENT PLATFORM	TESTED BROWSERS
Microsoft Windows 10 (32-bit and 64-bit)	Edge 20 Mozilla Firefox 45ESR and 48RR Chrome 53

Microsoft Windows 8, 8.1 (32-bit and 64-bit) in desktop mode only	Internet Explorer 10, 11 Mozilla Firefox 38.3 ESR, 41.0.1 Chrome 52
Microsoft Windows 7 (32-bit and 64-bit)	Internet Explorer 10, 11 Mozilla Firefox 38.3 ESR, 41.0.1 Chrome 53
Sun Ray Software on Oracle Solaris (x86 and SPARC platforms): Oracle Solaris 10 8/11 (update 10) or later Oracle Solaris 11	Mozilla Firefox 31.0 (Solaris 10) Mozilla Firefox 38.2.1 (Solaris 11)
Sun Ray Software on Oracle Linux (32-bit and 64-bit): Oracle Linux 5 Oracle Linux 6	Mozilla Firefox Chrome
Oracle Linux (32-bit and 64-bit): Oracle Linux 5 Oracle Linux 6 Oracle Linux 7	Mozilla Firefox 38.3.0 ESR, 41.0.2 Chrome
Ubuntu Linux 14.04, 16.04 (32-bit and 64-bit)	Mozilla Firefox 31.5 ESR, 48.0.1 Chrome 52
Mac OS X 10.9, 10.10, 10.11, 10.12, 10.13	Safari 7, 8, 9, 10 Mozilla Firefox Chrome
Apple iPad on: iOS 7, 8, 9, 10	Safari
Google Nexus 7 and Google Nexus 10 on: Android 5.11 Android 6	Chrome
Acer Chromebook and HP Chromebook on: Chrome OS 38.0	Chrome

The Oracle Secure Global Desktop Administration Console is not supported on Safari browsers, Mac OS X or iPad client devices.

Beta versions or preview releases of browsers are not supported.

Browsers must have the JavaScript programming language enabled, and must be configured to accept cookies.

Oracle Secure Global Desktop can either use a Java plug-in or Java Web Start technology to initially install the native client; both versions 1.7 and 1.8 are supported on the client. Version 1.8 is recommended. Once the native client has been installed on the users system, Java is no longer required.

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

On tablet devices such as the iPad, Oracle Secure Global Desktop uses an HTML5 based client to display applications and/or desktops, within a separate browser tab (i.e. via the Safari browser). The Oracle Secure Global Desktop workspace is also accessed on iPad's safari browser.

When users start more than one user session using the same client device and browser, the user sessions join rather than the new session ending the existing session. For user sessions to join in this way, the browser must be configured to allow permanent cookies. If permanent cookies are not allowed, user sessions always end and this might cause application windows to disappear.

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;
- Simplified Chinese;
- Traditional Chinese.

Supported Proxy Servers

To connect to Oracle Secure Global Desktop 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, Oracle Secure Global Desktop supports the Basic and No Authentication Required authentication methods. No server-side configuration is required.

For HTTP proxy servers, Oracle Secure Global Desktop 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.

Printing Support

Oracle Secure Global Desktop supports two types of printing: PDF printing and Printer-Direct printing.

- For PDF printing, Oracle Secure Global Desktop 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.
- Oracle Secure Global Desktop supports Printer-Direct printing to PostScript, Printer Command Language (PCL), and text-only printers attached to the user's client device. The Oracle Secure Global Desktop 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 Oracle Secure Global Desktop server. For best results, download and install the additional fonts.

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

TABLE 7. SUPPORTED PDF VIEWERS

CLIENT PLATFORM	DEFAULT PDF VIEWER
Microsoft Windows platforms	Adobe Reader
Oracle Linux	GNOME PDF Viewer (**gpdf**) Evince Document Viewer (**evince**) X PDF Reader (**xpdf**)
Mac OS X	Preview App (**/Applications/Preview.app**)

The default printer driver used for Portable Document Format (PDF) printing from Windows application servers is HP Color LaserJet 2800 Series PS. On tablet computers, the browser plug-in is used to display PDF files.

Supported Smart Cards

Oracle Secure Global Desktop works with Personal Computer/Smart Card (PC/SC)-compliant smart cards and readers supported for use with Microsoft Remote Desktop Services

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

April 2018

Oracle is committed to developing practices and products that help protect the environment

Integrated Cloud Applications & Platform Services