

Frequently Asked Questions Oracle Secure Global Desktop

Introduction

Oracle Secure Global Desktop is a secure remote access solution for cloud-hosted enterprise applications and hosted desktops running on Microsoft Windows, Oracle Linux and other Linux Distributions, Oracle Solaris and mainframe servers. Oracle Secure Global Desktop works with a wide range of popular client devices, including Windows PCs, Macs, Linux PCs, Chromebooks and tablets such as the Apple iPad and Android- based devices. The software gives users the ability to work securely from nearly any device, virtually anywhere, while providing administrators the tools they need to control access to applications and desktop environments resident in the data center.

Questions and Answers

Q What is Oracle Secure Global Desktop

A: Oracle Secure Global Desktop (SGD) is software that enables remote users to securely access and run centralized applications, using the web browser on their supported device. Supported application types include Microsoft Windows (via RDP), UNIX/Linux X- Windows, character terminal (e.g. "VT420"), tn3270, and tn5250.

SGD is a three-tier architecture. Client devices (Tier 1) connect to SGD servers (Tier 2) which connect to the application servers (Tier 3), where applications and desktops are hosted. This secure architecture isolates the application servers, which typically reside in the Cloud or data center, from direct connections from client devices that access from the Internet. The SGD servers connect to application servers through standard protocols, such as RDP and X11, meaning that existing application servers can be used with little or no installation and configuration.

Q What is the latest available version?

A: Version 5.4 is the latest version as of April 2018. Details can be found [here](#).

Q Where can I find documentation?

A: The documentation collection can be found at [Oracle Secure Global Desktop Documentation](#) page

Q Where can I find the software?

A: SGD can be downloaded from the [Oracle Secure Global Desktop downloads](#) page.

Q What operating systems does SGD run on?

A: The list of supported operating systems for the latest version of SGD can be found [here](#).

Q What application types are supported?

A: For the latest version of SGD, the supported application types (and associated protocols) can be found [here](#).

SGD uses customizable Expect scripts and standard protocols to connect to application servers. The default scripts enable SGD to connect to Linux, Oracle Solaris, Unix and Windows servers without modification and they can be customized to connect to application servers running less common operating systems, like OpenVMS.

Q What are SGD Enhancement Modules?

A: [Enhancement Module](#) install on application servers to provide additional functionality and are completely optional. They provide:

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

Q Where can I find the Enhancement Modules?

A: The simplest way is to browse to the SGD server landing page from the application server console and locate the link **Install an Oracle Secure Global Desktop Enhancement Module**. Clicking on the link will take you

to a download page, where you can download and install the appropriate module.

Q How do users authenticate to application servers?

A: Unix based application servers are accessed via ssh or telnet by providing username and password credentials asked from the user. These credentials can be stored in an encrypted password cache so the user would only have to provide the credentials once. Credentials can also be stored in the password cache by an administrator, thus allowing a user access to an application server without having to know credentials at all.

If ssh does not allow authentication via passwords and only permits private keys, the user can provide the ssh private key to the native SGD client or to the HTML5 client in order to authenticate to the server to launch an application. The private keys will not be uploaded to the SGD server infrastructure, but will remain only on the users computer.

Q What clients are supported?

A: The list of clients supported by the latest version of SGD can be found [here](#).

Q I have a client / server operating system / application server operating system not on your list - will this work?

A: It depends on the nature of the differences in your operating system / configuration. They will often work if they're substantially similar to a supported platform. This list of platforms is simply those that have been through Oracle Quality Assurance testing processes.

Q How do I get support?

A: The purchase of an SGD license includes one year of Basic Support. If you do not have contracted support, you may be able to get your questions answered by querying the [Oracle Secure Global Desktop Community](#).

Q How is Oracle Secure Global Desktop licensed?

A: SGD is licensed using Oracle's Named- User Plus licensing model, by feature used, on an array-wide basis. The features are based on **the type of application** being accessed. The two types of access are:

- UNIX/Linux X11/ANSI terminal/5250/3270;
- Windows / RDP.

There are currently two types of licenses sold:

- Windows Applications Only;
- All Platforms, including Windows applications and UNIX/Linux/ANSI terminal/5250/3270 applications.

Details of the two licensing models are as follows:

Type 1	Type 2
Oracle Secure Global Desktop License Named User Plus for Microsoft Windows Only	Oracle Secure Global Desktop License Named User Plus for Microsoft Windows, AS/400, Oracle Solaris, UNIX and Mainframe
Part # TTW19-LCO-NUP = \$150/- List Price per License.	Part # TTA19-LCO-NUP = \$250/- List Price per License.
First Year Support: \$33 (22% of list price)	First Year Support: \$55 (22% of list price)

Q What is AIP?

A: Adaptive Internet Protocol (AIP) is the protocol used between the SGD server and an SGD client to deliver an application over a network connection, and is designed to provide optimal application behavior and responsiveness when delivered by SGD. AIP is an adaptive protocol meaning that it adapts to changing network conditions. It measures network bandwidth, network latency, client performance, and application behavior to determine the best strategy for optimizing perceived performance at the client computer. AIP is covered by patent number 6362836, and is described [here](#).

Q How much bandwidth does AIP require (or what is the bandwidth requirement to access the SGD server)?

A: There are many variables that impact network bandwidth. These include screen size, color depth, application behavior, display complexity, frequency of screen refreshes, and the like. Graphical applications tend to have a high initial requirement, as the initial screen is displayed, after which, the bandwidth demands are far smaller. User think-time and idle time are often used in bandwidth calculations to artificially reduce bandwidth averages. Therefore, protocols which state the bandwidth required as an average over time must be viewed with some skepticism, because while 20Kb on average might be technically accurate, a user who connects over a 20Kb unshared connection is unlikely to have acceptable performance. Yet 10 users on a 200Kb shared network connection may experience adequate performance. The best way to determine the requirements for a particular installation is to simulate the network environment, and

measure the actual application behavior under constrained conditions.

A common error in benchmarking AIP is to use an unconstrained network connection. AIP measures the available network bandwidth and adjusts its behavior accordingly. If you test on a 100Mbps network connection, AIP will detect that, and will invoke relatively few optimizations. If you measure the bandwidth consumed under such conditions, you may conclude that AIP requires a very large amount of bandwidth. However, if the client connection were constrained to, for example, 48Kbps, AIP will adjust its optimization techniques accordingly, to “fit” within the available bandwidth, and to deliver the best interactive response.

Also be aware that AIP, with certain exceptions, can send a rather large number of packets at the beginning of a session to profile the available bandwidth and network latency. Be sure to allow any testing to run long enough for AIP to “train” to the detected bandwidth.

For accessing a typical graphical application, a 128Kbps client connection is recommended. A 56Kbps unshared network connection is usually considered minimally adequate.

Q Can I constrain how much bandwidth AIP consumes?

A: Yes, bandwidth limits can be applied to users, or groups of users. This is not generally necessary, but when users are using applications which can demand high amounts of bandwidth, such as streaming video / animations, this may be appropriate.

See [The X Application Uses Too Much Bandwidth](#) and [SGD Uses Too Much Network Bandwidth](#). Also see: [Improving the Performance of Windows Applications](#) and [Improving the Performance of Java Desktop System Desktop Sessions or Applications](#).

Q How is SGD different from Virtual Private Network (VPN)?

A: In general terms, a VPN creates a virtual communications circuit as a component of a larger network. As this relates to how SGD is used, the common use of a VPN is to create a tunnel from a client computer to a private network, using the Internet as the carrier of this tunnel. This is commonly used to allow a computer (user) to access the private network facilities of their company from a remote location, using the Internet as the physical transport of this tunnel. This allows them to access computers and services held within the private network, which are not otherwise exposed to the public Internet.

This typically requires some form of VPN client software on the client computer, and a VPN concentrator at the border of the private network. The solution uses authentication and encryption (IPSec, commonly), so that eavesdroppers cannot intercept or alter the data as it traverses those public links.

A key point is that the VPN tunnel provides network “presence” of the remote computer. This allows applications present on the remote computer to access computers and services on the private network as though the client computer were on the same network as these internal hosts, because, in effect, they are. These applications may include web browsers, accessing internal web servers and e-mail clients and accessing internal mail servers. Using the appropriate emulation software installed on the private computer, the client can also access other application types, such as Windows (via the RDP protocol) and X-Windows (using X11) running on computers in the private network.

One way in which SGD is different is that it doesn’t provide network presence to the remote computer. The client connects to the SGD server, which itself is local to the private network. The SGD server then proxies the client connection to the appropriate application server. The client computer never needs direct access to the internal network. In the case of a traditional VPN, the user can browse the internal networks, and can communicate directly with other computers. This introduces the potential for malware, such as a trojan or worm, infecting the client computer. Such a malicious program, installed on the users’ computer can connect directly to these internal systems, and perhaps infect them or steal data. This is why some VPN solutions have techniques such as endpoint validation to ensure that connected clients have appropriate virus scanners, firewalls, and/or patch levels installed. As SGD doesn’t provide client network access, such techniques are unnecessary to protect internal systems.

Q What network ports does SGD use / require to be open?

A: The network ports used by SGD are described in: [Connections between SGD Client and SGD Server\(s\)](#).

Q What is the SGD Gateway and how do I use it?

A: The SGD Gateway is an independent component that sits between clients and SGD servers, providing single-port access for IPv4 and IPv6 client devices. Firewall-friendly port 443 is used by default. Oracle recommends the use of the SGD Gateway.

The SGD Gateway can either be installed on its own server, which can be in a different security zone, like the DMZ, providing additional security and load-balancing capabilities, or it can be installed on the same host as the SGD server, creating a self-contained system that services IPv4 and IPv6 clients through a single port.

An example of a simple Secure Gateway deployment can be found [here](#).

Q Does SGD support IPv6?

A: The SGD Gateway supports IPv6, and as such can provide secure access to your data center. The SGD servers, which establish connectivity to the third-tier application servers still require IPv4. With SGD Gateway and SGD servers you can make resources that still depend on IPv4 securely accessible via IPv6.

Q Can SGD be installed using Oracle Solaris containers / zones?

A: Yes, Zones support is for SGD installed in either global zone or one or more non-global zones, but not both at the same time. See [Supported Installation Platforms for SGD - Virtualization Support](#).

There are some additional caveats:

- For UNIX Application Servers, Client Drive Mapping depends on NFS support, and since NFS is restricted to global zones, then UNIX CDM can only be supported in a global zone;
- There have been confirmed reports that installing the SGD Server in a global zone with non-global zones active may cause intermittent application launch issues. If zones are in use, you may wish to consider installing SGD in a non-global zone, as this seems to alleviate the problem. Note that the installation in the global zone remains supported, however, you may wish to consider this when planning a new installation.

Q Is Secure Global Desktop supported on virtual machines?

A: Yes, Secure Global Desktop is supported on virtual machine instances under Type 1 and Type 2 hypervisors, provided the virtualized operating system instance is one of the tested and supported operating systems listed for the particular SGD release. See [SGD Server Requirements and Support, Virtualization Support](#).

Q Is it possible to integrate thin clients with an SGD environment?

A: SGD cares only about supported operating systems and browser version. A user can use any supported browser to access applications via SGD. You need to ensure that the

thin client will support a browser from the supported list of browsers. It's also important to understand that SGD does not contain a hypervisor, like solutions (e.g. VDI). With a server-based computing design, SGD simply picks the applications from application server (which can be Linux, Windows, Mainframe, Oracle Solaris, etc) and this allows the user to access the selected applications using any supported browser.

A list of supported browsers can be found [here](#).

Additionally, Oracle works with [StratoDesk](#), the maker of NoTouchOS, a thin client OS which can:

- Change a Windows PC with various 3rd party software and need for constant patching and antivirus into a secure, thin client-type appliance;
- Centralize management with inheritance, configuration, updating, reporting, helpdesk support, and cover the endpoints and help eliminate the need for third party client software;
- Work on existing thin clients of various types;
- unify the end user look and feel, and the system administrator look and feel, over different devices;
- Support Oracle Secure Global Desktop.

Q Can SGD discover dynamic, virtualized application servers?

A: SGD can provision special application server objects that can communicate with Oracle VM VirtualBox (vboxwebsrv) and Oracle VM Manager (version >3.4.x) web service APIs to dynamically display a list of guest VMs with which to establish a secure connection. This allows for a one-time setup to support changing virtualized environments.

Q What is the level of the traceability of users' activities?

A: There are various kinds of log filters available with SGD where logs can be generated for user activity. You can easily trace the user login time, which server they logged into, the IP address they are logged in from, session time, and more. See [Using Log Filters for Auditing](#).

Q Is the SGD platform cloud ready or do we need other components like Oracle Cloud Application Foundation for cloud deployments?

A: SGD is a cloud-ready access solution. If there is a public cloud or private cloud environment, where applications are being accessed by a user, SGD can be installed on top of it to provide access.

Q Does SGD support CentOS?

A: No. While it may work, it is not supported by Oracle.

Q How do I size an SGD server?

A: SGD server sizing is based on amount of memory consumed per user and CPU usage per user. Below are the details:

- 80MB memory per user;
- 50MHz CPU per user.

SGD servers can be installed either on Oracle Linux or Oracle Solaris systems. Below are the requirements for installing and running SGD:

- 2GB of free disk space;
- 2GB of random-access memory (RAM);
- 1GHz processor;
- Network interface card (NIC);
- Minimum two SGD servers should be deployed to achieve HA.

Please refer to [this sizing document](#) for SGD which will assist you in designing the environment.

Q If applications are Linux based, will they require Windows CAL licenses?

A: No, for Linux-based applications, the Windows CAL licenses are unnecessary.

Q Is it possible to use SGD to reduce the cost of Microsoft licenses?

A: SGD does not provide any capability to bypass Windows or application licensing requirements. However, since SGD makes it easy to publish applications from any supported platform (e.g., Linux) to any supported device (e.g., a tablet, a Mac, and so on), you have the tools to provide users with easy access to low or no cost alternative applications, or mix-and-match traditional commercial and open source applications, as necessary.

Q Does SGD support viewing a Mac OS X desktop or server?

A: To use an application server with SGD it needs to support either the X or RDP protocols.

If your Mac OS X applications are purely X11-based, you can access them through SGD without additional software. Otherwise, you will need something to export the Mac desktop to either RDP or X.

Q Will SGD replace the 2-factor authentication service we currently use?

A: No. SGD should be considered as an additional security control, rather than a replacement for your existing 2-factor authentication service. While SGD does effectively provide the functionality of a secure gateway to the protected resources and data-in-transit is encrypted using the SSL protocol, the primary function of the service is to limit the risk of data leakage from data centers and enable your IT infrastructure to meet tougher security and compliance requirements.

The product suite [VISULOX](#) by Oracle Partner Amitego provides add-on solutions to SGD, including 2-factor authentication integrated into the SGD authentication flow.

Q Do I need to install special software to use SGD? Can I access SGD without Java?

A: SGD can be accessed using browsers installed on your PCs or tablets. By default, your browser needs to be configured to enable JavaScript, and it must be configured to accept cookies.

If Java is installed on the client, there is no need to manually install the native client software for using SGD. If the Java plugin is enabled in the Browser, SGD will be installed and/or launched automatically. In cases where the browser does not support the Java plugin, or has it disabled, Java WebStart will be used to install and/or launch SGD.

In case the client computer does not have Java, there are two options for using SGD:

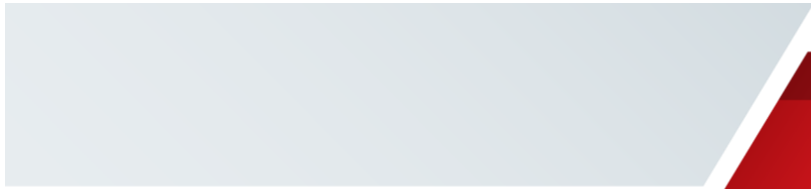
- 1) Access using a supported HTML5 web browser. Currently, this is Chrome, Firefox and Chromebook (Chrome OS). The SGD HTML5 client is a non-Java implementation and users don't need plugins or JRE on the client side.

More details are can be found [here](#).

- 2) Manual install of the native SGD client. This option allows the use of the native SGD client for Windows, Linux, and Mac, which can be downloaded and installed manually from the SGD web server page.

Once the native client is installed it will be launched via a registered URL schema handler.

Additional information can be found [here](#) and [here](#).







Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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

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

