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, Linux, Solaris and mainframe servers. Oracle Secure Global Desktop works with a wide range of popular client devices, including Windows PCs, Macs, Linux PCs, 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. Applications types supported include Microsoft Windows (via RDP), UNIX/Linux X- Windows, character terminal (e.g. “VT420”), tn3270, and tn5250.

Most commonly, SGD is viewed as a having a “three-tier architecture”, with client computers representing tier 1, the SGD server(s) being tier 2, and application servers tier 3. Clients (tier 1) connect to the SGD server(s) (tier 2), which in turn launches proxied connections to tier 3.

Clients connect to the SGD server and the SGD server proxies / connects to the application server tier using native protocols appropriate to the application type (e.g. RDP for RDP/Windows applications, SSH/X11 for X-Windows applications, etc.).

Users never connect directly to the application server tier. This allows the application servers to be isolated from internet access, except through the SGD server.

Q: What is the latest available version?

A: Version 5.2 is the latest version as of June 2015. Details can be found here.

Q: Where can I find documentation?

A: he 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: For the latest version of SGD the list of supported operating systems 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.

Note that this does not necessarily specify application server operating systems. This is because SGD uses standard protocols to connect to the application servers, and the application server operating system isn’t something that SGD is dependent on, provided that the hosting application server behaves in a predictable way. For example, it probably doesn’t matter if the X-Windows application you’re publishing is hosted on Solaris 10, or a Linux distribution, or OpenSolaris. But it will matter if the hosting operating system isn’t a UNIX work-alike, like OpenVMS. There are usually ways to deal with such differences.

Where application server operating systems are relevant is when installing an Enhancement Module. Enhancement modules 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).

Note that X-Windows applications which require some extensions not supported by SGD may not always work. For a list of X-Windows extensions supported by SGD, see Supported X Extensions.

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: 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 process, and minor differences between versions or distributions are usually not a problem. The exception to this is the audio-redirection drivers for UNIX/Linux servers. However, that said, Oracle support cannot guarantee an unsupported platform will operate properly. For unsupported platforms, Oracle Support will only offer assistance on a best-effort basis. If you have questions or concerns, please contact your Oracle sales or support representative.

Q: How do I get support?

A: If you're entitled to SGD Support of any kind (a license purchase includes 1 year of Basic Support), you should use it. If you do not have contracted support, you may be able to get your questions answered elsewhere – See Oracle Secure Global Desktop Community

Q: How is Oracle Secure Global Desktop licensed?

A: Secure Global Desktop 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;
- Both 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, Solaris, UNIX and Mainframe
Part # TTWI9-LCO-NUP = $150/- List Price per License.	**Part # TTAI9-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.

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

A: This is a difficult question to answer, as there are a great 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. As was mentioned, AIP measures the available network bandwidth available, and adjusts its behaviors 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), will send a rather large amount of packets at the beginning of a session to profile the available bandwidth and network latency, so be sure to allow any testing to run long enough for AIP to “train” to the detected bandwidth.

All that said, a 56Kbps unshared network connection is usually considered minimally adequate for accessing a typical graphical application, with a 128Kbps client connection recommended.

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 well be appropriate.

A: 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 VPN?

A: In general terms, a VPN, (Virtual Private Network), 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 between 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. Typically this provides some form of 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 any computer they desire. This introduces the 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 the following documentation links:

- Connections between SGD Client and SGD Server(s);
- Connections between SGD Servers in an Array;

- Connections between SGD Server(s) and Application Server(s);
- Connections between SGD Server(s) and "Other" Services.

Note that, technically, there are two ports used by the SGD client - one port for http and one for AIP. In most cases, firewall traversal is used to provide a single port connection between the SGD Client and SGD Server. An alternative to firewall traversal is the SGD Secure Gateway, which provides an alternative single-port mechanism. See Oracle Secure Global Desktop Gateway Administration Guide for more details.

Q: What is firewall traversal and how do I enabled it?

A: As mentioned, the connection between the SGD client and SGD server requires two separate ports, one for http and one for AIP. The ports are as follows.

Source	Destination	Port	Description
Client	SGD Server	80/tcp	Standard, unencrypted HTTP requests and responses.Used to display workspaces and for web services.
Client	SGD Server	443/tcp	Secure, encrypted HTTPS requests and responses. Used to display workspaces and for web services.
Client	SGD Server	3144/tcp	Standard, unencrypted AIP connections. Used for control and application display updates.
Client	SGD Server	5307/tcp	SSL-based secure, encrypted AIP connections. Used for control and application display updates.

Client web browsers connect over either port 80, or port 443, while the SGD Client Component connects over 3144 or 5307, depending on whether encryption is enabled or not on the respective protocols.

Note that even when using unencrypted AIP connections for a client, the first connection is always secure (that is, on 5307, unless firewall traversal is enabled).

When the connection between the client and the SGD server is on a wide area network or other network connections that may include firewalls, the ports required by AIP (either 3144 or 5307) are usually blocked. While it's sometimes possible to change firewall configurations to allow these connections, there's a better way.

Most firewall configuration allows port 443 connections to take place, if they're properly encrypted. SGD Firewall Forwarding places both protocols on port 443, with the SGD SSL Proxy acting as the end-point for communications. The SSL Proxy examines the packet headers to determine their true destination - the web server or SGD, and sends the packets to the appropriate destination.

Firewall forwarding requires security to be enabled on both http and AIP connections.

To enable firewall forwarding in SGD, you can set it up automatically (subject to certain restrictions) with a single command: the *tarantella security enable* command. For more information, see Enabling Secure Connections (Automatic Configuration.).

If unable to use automatic configuration, firewall traversal can be setup using manual methods: see Enabling Secure Connections (Manual Configuration).

Similar to the firewall forwarding technique is the SGD Secure Gateway. First available in Version 4.50, the Secure Gateway is an alternative to firewall traversal; that is, you either configure firewall traversal or a Secure Gateway, not both. The Secure Gateway is designed to be installed on one or more dedicated servers deployed in front of SGD servers, typically in the DMZ, allowing the SGD server/array to be installed in an internal network.

An example of a simple Secure Gateway deployment can be found here.

The Secure Gateway performs the functions of a traditional reverse proxy, as well as an AIP router. It can also perform load-balancing, and multiple gateways can be installed to avoid a single point of failure. For more information on the Secure Gateway, see Gateway Administration Guide.

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

A: Yes, Zones support is for SGD installed in either Global Zone or 1 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 fully supported, but 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, of course, the virtualized operating system instance in one of the tested and supported operating systems listed for the particular SGD release (See SGD Server Requirements and Support, Virtualization Support).

Q: How 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 only 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 VDI solution would. It is based on the server-based computing concept where SGD simply picks the applications from application server (which can be Linux, Windows, Mainframe, Oracle Solaris, etc) and the user will be able to access that application using any supported browser.

A list of supported browsers can be found here.

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, IP address they are logged in from, session time, and many 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 ready cloud 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 to users with applications.

Q: Does SGD support CentOS?

A: No. It may work but Oracle cannot assist if there is an OS issue.

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 completely unnecessary.

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

A: Not directly. 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 will be 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.

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

A: There is no need to install any client software for using SGD, and yes, you can access SGD without Java.

Secure Global Desktop can be accessed using browsers installed on your PCs or tablets. By default, your browser need to be configured to enable Java and JavaScript, and it must be configured to accept cookies.

However, there are two options for using SGD without Java.

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.

   You can refer here for more details.

2) Use the native SGD client. Besides the auto-downloaded Java based client, there is also a non-Java based native SGD client for Windows, Linux, and Mac, which can be downloaded and installed manually from the SGD web server page.

   To use the native client, users need to launch the SGD client first, then enter the SGD server URL, such as *https://xxx.xxx.xxx/sgd* into the SGD client, and finally log into SGD workspace as usual.

   You can refer here and here for more details.

ORACLE

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