



An Oracle White Paper
December, 2011

Design Considerations for Oracle Secure Global Desktop Deployments

Introduction	1
System Requirements and Support	3
Virtualization Support.....	4
Supported Applications and Protocols	4
Networking Requirements.....	5
Microsoft Windows Terminal Services	7
X and Character Applications.....	8
SGD Enhancement Module	10
SGD Web Server	11
SGD Gateway	12
Array Failover.....	15
Supported Versions of Active Directory	16
Supported Versions of SecurID.....	16
SSL Support.....	16
SGD Client	18
Supported Proxy Servers.....	19
Printing Support	19
Supported Smart Cards	20
Appendix A: Oracle Secure Global Desktop Architecture Diagram ..	21
Appendix B: Design Considerations for Distributing Sessions.....	22
Assumptions.....	22
Requirements.....	22
Issues.....	22
Potential Solutions	23

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

- A consistent interface: Users can login to Oracle Secure Global Desktop from virtually any desktop computer in the world simply by going to a URL from a web browser, and have access to their applications and data.
- No client software: IT departments do not need to maintain software on the user's desktop, since the user can access Oracle Secure Global Desktop with any supported web browser. No client software on the desktop device means application updates can be accomplished entirely on the server side, dramatically reducing the time required to roll-out infrastructure updates to users.
- Session mobility: Users can pause, resume or terminate their sessions from the dynamic browser-based Oracle Secure Global Desktop webtop. This includes the ability to suspend a session and then resume it from a different desktop machine in another location (e.g., suspending a session from the office and then resuming it from home). This, combined with

eliminating maintenance of client software on thousands of desktop machines spread across multiple time zones, saves IT departments significant administrative overhead.

- **Simplicity and content control:** Centralized management of the applications and environments a user has access to is simple to use functionality built into 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 metrics 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.

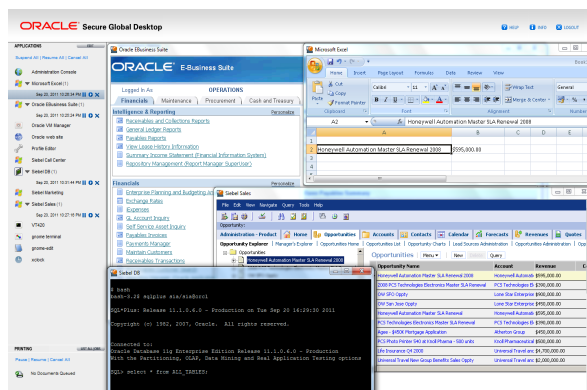


Figure 1. Oracle Secure Global Desktop web Interface and application support.

System Requirements and Support

Use the following hardware requirements as a guide and not as an exact sizing tool. For detailed help with hardware requirements, contact an [Oracle sales office](#).

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

- What is needed to install and run Oracle Secure Global Desktop.
- What is needed for each user that logs in and runs applications.

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

- 2 GB of free disk space
- 2 GB of random-access memory (RAM)
- 1 GHz 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 50 MB memory for each user
- 50 MHz of CPU for each user

Caution - The actual central processing unit (CPU) and memory requirements can vary significantly, depending on the applications used.

TABLE 1. SUPPORTED INSTALLATION PLATFORMS

OPERATING SYSTEM	SUPPORTED VERSIONS
Oracle Solaris OS on SPARC platforms	<ul style="list-style-type: none"> • At least Oracle Solaris 10 10/09 • Trusted Extensions at least Oracle Solaris 10 10/09
Oracle Solaris OS on x86 platforms	<ul style="list-style-type: none"> • At least Oracle Solaris 10 10/09 • Trusted Extensions at least Oracle Solaris 10 10/09
Red Hat Enterprise Linux (32-bit and 64-bit)	5.5
Oracle Linux (32-bit and 64-bit)	5.5

Virtualization Support

The supported installation platforms are also supported 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 (previously called Sun Logical Domains or LDOMs). 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 10 OS. 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 10 OS 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 OS, Linux, HP-UX, and AIX application servers
- Character applications running on Oracle Solaris OS, Linux, HP-UX, and AIX application Servers
- Applications running on IBM mainframe and AS/400 systems
- Web applications, using Hypertext Markup Language (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
- Telnet VT, American National Standards Institute (ANSI)
- TN3270E
- TN5250

Networking Requirements

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

- Hosts must have Domain Name System (DNS) entries that can be resolved by all clients.
- DNS lookups and reverse lookups for a host must always succeed.
- All client devices must use DNS.
- When you install 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: boston.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.

The *Oracle Secure Global Desktop 4.6 Administration Guide* has detailed information about all the ports used by Oracle Secure Global Desktop and how to use the product with firewalls. The following information lists the common ports used. Client devices must be able to make Transmission Control Protocol/Internet Protocol (TCP/IP) connections on the following TCP ports:

- **80** - For Hypertext Transfer Protocol (HTTP) connections between client devices and the Oracle Secure Global Desktop web server. The port number can vary depending on the port selected on installation.
- **443** - For HTTP over Secure Sockets Layer (HTTPS) connections between client devices and the Oracle Secure Global Desktop web server.
- **3144** - For standard (unencrypted) connections between the Oracle Secure Global Desktop Client and the Oracle Secure Global Desktop server.
- **5307** - For secure connections between the Oracle Secure Global Desktop Client and the Oracle Secure Global Desktop server. Secure connections use Secure Sockets Layer (SSL).

Note - The initial connection between an Oracle Secure Global Desktop Client and an Oracle Secure Global Desktop server is **always** secure. After the user logs in, the connection is downgraded to a standard connection. When you first install SGD, TCP ports 3144 and 5307 must be open to connect to SGD. You can configure SGD to always use secure connections.

To run applications, Oracle Secure Global Desktop must be able to make TCP/IP connections to application servers. The types of applications determine the TCP ports that must be open, for example:

- **22** – For X and character applications using Secure Shell (SSH)
- **23** – For Windows, X, and character applications using Telnet
- **3389** – For Windows applications using Windows Terminal Services
- **6010** and above – For X applications

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 (HTTP) or HTTP over Secure Sockets Layer (HTTPS) and Oracle's Adaptive Internet Protocol (AIP). Oracle Secure Global Desktop then connects to the application servers on the user's behalf.

Client devices make the following connections to Oracle Secure Global Desktop servers:

- **HTTP connections:** These are the connections to the Oracle Secure Global Desktop web server, used for Oracle Secure Global Desktop web services, authentication to Oracle Secure Global Desktop, and to display the webtop.
- **AIP connections:** These are the connections between the Oracle Secure Global Desktop Client and an Oracle Secure Global Desktop server, used for displaying applications.

To secure these connections, configure the Oracle Secure Global Desktop web server to be a secure (HTTPS) web server, and enable Oracle Secure Global Desktop security services.

NOTE - The SGD Gateway can be used to provide an increased level of security between client devices and Oracle Secure Global Desktop servers. 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 or the rexec command, 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. This means that all communication is encrypted, and connections to Microsoft Windows application servers are secure.

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.

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.

Microsoft Windows Terminal Services

SGD does not include licenses for Microsoft Windows Terminal Services. If you access terminal server 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.

Oracle Secure Global Desktop supports RDP connections to the following versions of Microsoft Windows:

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003
- Windows 7 Ultimate
- Windows 7 Professional
- Windows Vista Ultimate
- Windows Vista Business
- Windows XP Professional

On Windows 7, Windows Vista, and Windows XP 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 Terminal Services features:

- Audio redirection
- Clipboard redirection
- COM port mapping
- Drive redirection
- 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 44.1 kHz. By default, Oracle Secure Global Desktop 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.

Oracle Secure Global Desktop supports 8-bit, 16-bit, 24-bit, and 32-bit color depths in a Windows Terminal Server session.

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

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

You can only 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.

From Microsoft Windows Server 2003, you can use Transport Layer Security (TLS) for server authentication, and to encrypt Terminal Server communications. Oracle Secure Global Desktop does not support the use of TLS.

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, Telnet, and rexec 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 X11R6.8.2. SGD supports the following X extensions for X applications:

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

- XTEST
- XTTDEV

The following X extensions are not supported:

- KEYBOARD
- RANDR
- XINERAMA
- XVIDEO

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

To use audio for X applications, Linux and UNIX application servers must be running version 4.6 of the SGD Enhancement Module.

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 (UNIX or Linux platforms only)
- Seamless windows (Windows platforms only)
- Audio (UNIX or Linux platforms only)

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

TABLE 2. SUPPORTED INSTALLATION PLATFORMS FOR SGD ENHANCEMENT MODULE

OPERATING SYSTEM	SUPPORTED VERSIONS
Microsoft Windows (64-bit)	Windows Server 2008 R2
Microsoft Windows (32-bit and 64-bit)	Windows Server 2008 Windows Server 2008 R2 Windows Server 2003
Oracle Solaris OS on SPARC platforms	8,9,10, 10 Trusted Extensions
Oracle Solaris OS on x86 platforms	10, 10 Trusted Extensions
Red Hat Enterprise Linux (32-bit and 64-bit)	5
Oracle Linux (32-bit and 64-bit)	5
SUSE Linux Enterprise Server (32-bit and 64-bit)	10,11

SGD Web Server

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

TABLE 3. SGD WEB SERVER COMPONENTS

COMPONENT NAME	SGD VERSION 4.62 COMPONENT VERSION	SGD VERSION 4.50 COMPONENT VERSION	SGD VERSION 4.41 COMPONENT VERSION
Apache HTTP Server	2.2.21	2.2.10	2.2.8
OpenSSL	1.0.0e	0.9.8k	0.9.8g
mod_jk	1.2.32	1.2.27	1.2.25
Apache Jakarta Tomcat	6.0.33	6.0.18	5.0.28
Apache Axis	1.4	1.4	1.2

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 MB.

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)
- 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.

Using the SGD Gateway is an alternative to running your Oracle Secure Global Desktop servers with firewall traversal, also called firewall forwarding.

The SGD Gateway manages load balancing of Hypertext Transfer Protocol (HTTP) connections, so you do not need to use the JavaServer Pages (JSP) technology load balancing page included with Oracle Secure Global Desktop.

The SGD Gateway consists of the following components:

- **Routing proxy:** A Java technology-based application that routes Adaptive Internet Protocol (AIP) data 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.

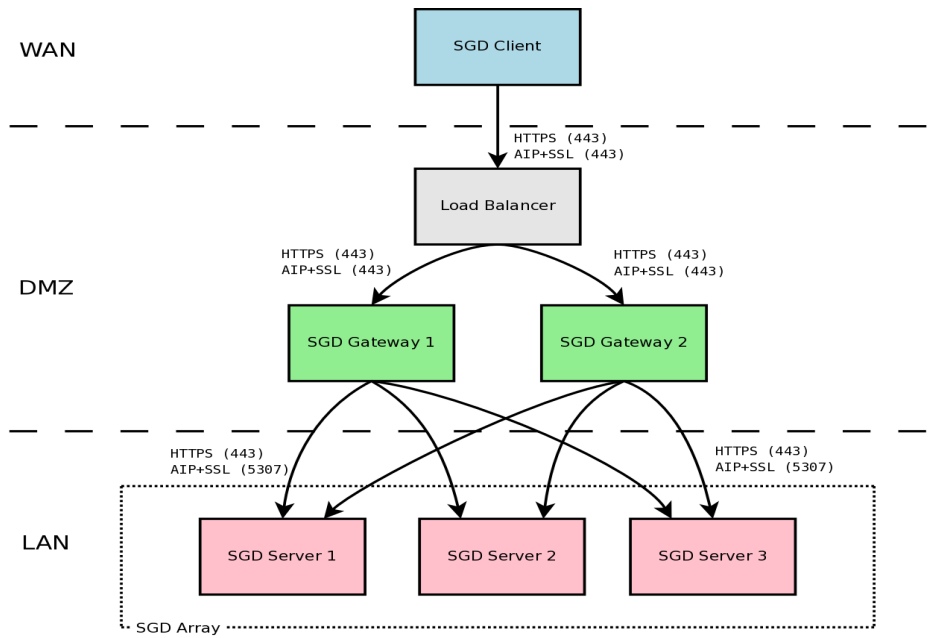


Figure 2. Example Oracle Secure Global Desktop load-balanced deployment

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

TABLE 4. SUPPORTED INSTALLATION PLATFORMS FOR SGD GATEWAY HOST

OPERATING SYSTEM	SUPPORTED VERSIONS
Oracle Solaris OS on SPARC platforms	At least Oracle Solaris 10 10/09
Oracle Solaris OS on x86 platforms	At least Oracle Solaris 10 10/09
Red Hat Enterprise Linux (32-bit and 64-bit)	5.5
Oracle Linux (32-bit and 64-bit)	5.5

By default, the SGD Gateway is configured to support a maximum of 100 simultaneous HTTP connections and 512 simultaneous Adaptive Internet Protocol (AIP) connections. The JVM memory size is optimized for this number of connections. Appendix C of the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide* has details of how to tune the SGD Gateway for the expected number of users.

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

TABLE 5. RETIRED INSTALLATION PLATFORMS FOR SGD GATEWAY HOST

ORACLE SECURE GLOBAL DESKTOP VERSION	PLATFORMS NO LONGER SUPPORTED
4.6x	OpenSolaris (all versions) Red Hat Enterprise Linux 5.0 to 5.4 Oracle Solaris 10 OS up to, and including, 5/09 SUSE Linux Enterprise Server 10
4.50	Not applicable
4.41	Not applicable

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. You must enable secure connections on your Oracle Secure Global Desktop servers. Firewall forwarding must not be enabled.
- **Integrated mode:** Oracle Secure Global Desktop clients must not be configured to access the Oracle Secure Global Desktop servers in Integrated mode.
- **Oracle Secure Global Desktop version:** The Oracle Secure Global Desktop servers must be running at least version 4.5 of Oracle Secure Global Desktop. It is best to use version 4.6 of the SGD Gateway with version 4.6 of Oracle Secure Global Desktop.
- **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 2.2.16. 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 the following 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
- 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

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 4.61 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 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- 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 Directory Server Enterprise Edition version 6.3.1 and 7.0 (formerly Sun Java Directory Server Enterprise Edition)
- Microsoft Active Directory on Windows Server 2003, 2003 R2, 2008, and 2008 R2
- Novell eDirectory version 8.8

Other directory servers might work, but are not supported.

Supported Versions of SecurID

Oracle Secure Global Desktop works with versions 4, 5, 6, and 7 of RSA Authentication Manager (formerly known as ACE/Server). Oracle Secure Global Desktop supports system-generated PINs and user-created PINs.

SSL Support

Oracle Secure Global Desktop supports TLS version 1.0 and SSL version 3.0.

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.509 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.

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 supported browsers and the supported desktop menu systems when the SGD Client is operating in integrated mode.

TABLE 6. SUPPORTED CLIENT PLATFORMS

SUPPORTED CLIENT PLATFORM	SUPPORTED BROWSERS	INTEGRATED MODE SUPPORT
Microsoft Windows 7 (32-bit and 64-bit)	Internet Explorer 8 Mozilla Firefox 3	Microsoft Windows Start Menu
Microsoft Windows Vista (32-bit and 64-bit)	Internet Explorer 7 Internet Explorer 8 Mozilla Firefox 3	Microsoft Windows Start Menu
Microsoft Windows XP Professional (32-bit)	Internet Explorer 7 Internet Explorer 8 Mozilla Firefox 3	Microsoft Windows Start Menu
Oracle Solaris OS on SPARC platforms At least Oracle 10 10/09	Mozilla Firefox 3	Java Desktop System Launch Menu
Oracle Solaris OS on x86 platforms At least Oracle Solaris 10 10/09	Mozilla Firefox 3	Java Desktop System Launch Menu
Oracle Solaris OS Trusted Extensions on SPARC platforms At least Oracle Solaris 10 10/09	Mozilla Firefox 3	Not supported
Oracle Solaris OS Trusted Extensions on x86 platforms At least Oracle Solaris 10 10/09	Mozilla Firefox 3	Not supported
Mac OS X 10.6	Safari 5 Safari 4 Mozilla Firefox 3	Not supported
Red Hat Enterprise Linux 5.5 Desktop (32-bit and 64-bit)	Mozilla Firefox 3	Gnome or KDE Start Menu
Ubuntu 10.04 (32-bit and 64-bit)	Mozilla Firefox 3	Gnome Start Menu

The Oracle Secure Global Desktop Administration Console is not supported on Safari browsers.

Beta versions or preview releases of browsers are not supported.

Browsers must have the JavaScript programming language enabled.

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

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

If Java technology is not available, the SGD Client can be downloaded and installed manually. Manual installation is available for all supported client platforms except Mac OS X. On Microsoft Windows platforms, you need administrator privileges to install the SGD Client.

Java Plugin tool version 1.6 is supported as a plug-in for Java technology.

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 256 colors.

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

- French
- German
- Japanese
- Korean
- 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.

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. At least version 6.52 of Ghostscript must be installed on the Oracle Secure Global Desktop host. 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, at least version 4.0
Oracle Solaris OS on SPARC platforms	Adobe Reader (acroread) GNOME PDF Viewer (gpdf)
Oracle Solaris OS on x86 platforms	GNOME PDF Viewer (gpdf)
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.

Supported Smart Cards

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

Appendix A: Oracle Secure Global Desktop Architecture Diagram

Below is a diagram that illustrates the product architecture for Oracle Secure Global Desktop.

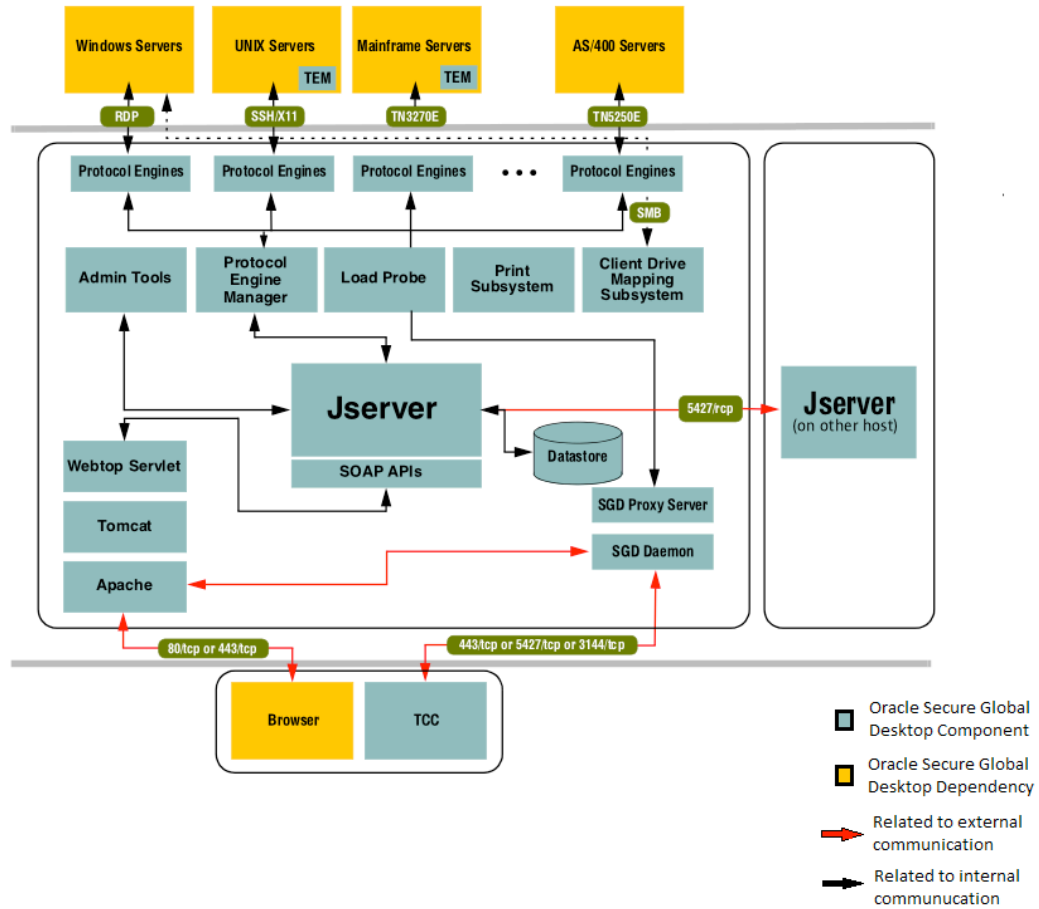


Figure 3. Oracle Secure Global Desktop architecture.

Appendix B: Design Considerations for Distributing Sessions

This section explores some of the issues that need to be considered when attempting to distribute webtop sessions over an Oracle Secure Global Desktop array. In particular it examines the requirements for correct operation of Oracle Secure Global Desktop when using either a Hardware Load Balancer (HWLB), or a software alternative.

Assumptions

The following assumptions have been made about the required end user environment:

- Firewall forwarding mode is in use.
- SSL/HTTPS is being used for all connections.
- The SGD Client being used is the browser-based webtop.
- The user's browser has session cookies and JavaScript enabled.

Requirements

Any solution is required to provide the following:

- 1. There should be a single entry point (that can be bookmarked), that provides access to the Oracle Secure Global Desktop WebTop.
- 2. This entry point should provide some form of load distribution over the members of the array (or a subset of if required).
- 3. If a webtop session already exists, then revisiting the entry point should return the user to the existing session.
- 4. If a member of the array is not functioning, then webtop sessions should not be directed to that server.
- 5. The characteristics of the connection should be preserved if possible and presented to the Oracle Secure Global Desktop server intact (e.g. the connection to the Oracle Secure Global Desktop server should be SSL and any client certificates etc. should still be present).

Issues

When considering any possible solution the following should be reviewed:

- Webtop sessions require server affinity. The current implementation is not mobile between servers. If a session already exists on one member of the array and a webtop request is subsequently directed to a different member of the array this may result in unexpected behavior such as the webtop state being incorrect or a full session-grab being performed resulting in application windows disappearing.
- Adaptive Internet Protocol (AIP) connections must be established to a particular Oracle Secure Global Desktop server and must not have any form of external load distribution performed on them.

- AIP connections are not HTTP based. This means that if an external device removed the SSL wrapper on an AIP connection it is unlikely to be able to interpret the remaining contents.
- When connections made to an Oracle Secure Global Desktop server using a host name (which is part of the URL), that is different than the server's external name, the impact is unknown.
- It is not possible to use virtual hosting for multiple SSL connections to a web server. If it is a requirement to have two SSL based web servers (each with a different DNS name) on the same server then either different ports or different IP addresses must be used.

Potential Solutions

The following sections discuss potential solutions:

Solution 1: Simple Hardware Load Balancer (HWLB)

The most obvious solution would be to simply use a single name (the array name or ANAME), for all of the members of the array, the external names (or ENAME) for each system would be set to this value, only a single certificate is required and it is installed on all of the machines. The HWLB does not require any special features (such as the ability to decode SSL), and the ANAME is simply pointed at the HWLB. The HWLB then simply forwards the incoming connections to members of the array.

Solution Review

- There is no attempt to maintain webtop server affinity.
- The AIP connections will be load balanced and thus cannot be guaranteed to go to the correct server.
- If an attempt is made to decode the SSL traffic on the HWLB then AIP traffic may be affected.

Solution 2: HWLB with persistence capabilities and AIP bypass

We attempt to solve the above issues by using a more sophisticated load balancer that is able to provide persistence of connections over the lifetime of a webtop session, and by bypassing the HWLB for AIP connections. In this configuration we have an ANAME that points to the HWLB and unique ENAMES for each server. The ANAME is used for the initial webtop connection the ENAMES are used for AIP connections and thus go direct to the members of the array. Session persistence for HTTPS connections is provided by the following techniques:

- Using a combination of the client address and the server address.
- Using the SSL session ID.
- Using a HWLB that is capable of decoding the SSL stream and then injecting a cookie into the HTTP system that is used to provide the persistence.

Solution Review for HWLB that use techniques 1 & 2:

- The session persistence is not guaranteed with these techniques (particularly for the long lifetime of typical webtop sessions).

- The name in the URL (the ANAME) is not the same as the ENAME.
- The servers now have to accept SSL connections for two different names. However, it may be possible to overcome this by using the HWLB to direct the ANAME connections to a different server port number. Alternatively a second IP address may be assigned to each server in the array and used for the ANAME traffic.

Solution Review For HWLB that use technique 3 above:

- The SSL connection has been terminated at the HWLB this means that the characteristics of the original connection have been lost (and so this does not meet requirement 5 above).
- Depending upon the capability of the HWLB the ANAME may be presented to the Oracle Secure Global Desktop servers as part of the URL.

Solution 3: HWLB with server based persistence and AIP/webtop bypass

Solution 2 can be extended to use the same bypass technique for the webtop connection and provide persistence through the use of server side scripts. In this configuration the ANAME points to the HWLB. The HWLB selects one of the array members and sends the initial contact request on to that server. This server then executes a small script that:

- Checks to see if the request comes from a browser that already has an active session. If it does then the script performs a HTTP redirect to the ENAME of the specific server.
- If no session exists the script simply performs a HTTP redirect to the ENAME associated with itself.

The script uses a cookie to track the session state (in a similar way to some HWLBs described above). The lifetime of this cookie is the lifetime of the browser session.

This method basically only uses the ANAME and the HWLB to choose the system on the initial connection, and all connections after this point are made directly to the individual servers. There are however two remaining issues with this solution

- If a session has been established to a server that later on becomes unavailable then the persistence mechanism mentioned above will continue to send requests to that server.
- If a HWLB that is not capable of decoding the SSL stream is used then the Oracle Secure Global Desktop servers will need to be able to handle multiple SSL requests to different names.

Issue 1 may be resolved by a minor modification to the persistence mechanism to enable a probe of the server to be made before performing the redirection. Issue 2 may be addressed either by using the HWLB to change the destination port or by adding a second IP address to each of the servers.

Recommended HWLB solution

To provide a simple robust solution it is recommended that a variation of solution 3 be used.

- An SSL capable HWLB is used and responds to requests made to ANAME.

- The request is decoded on the HWLB and then forwarded as a HTTP (not HTTPS) request to the selected server.
- A persistence script is installed on each server in the array, this is the destination of requests that come via the HWLB and performs the persistence/probe/redirect operations described above.

This combination meets all of the requirements and avoids the known issues. It should also be possible to use a less sophisticated HWLB (as described in solution 3 above), however this will require more complex HWLB and server configuration to deal with the dual SSL names issue.

More sophisticated HWLB/SSL accelerators may be used with this solution in a number of configurations:

- Simple pass through. The traffic directed to the ENAMES is simply routed via the device.
- SSL offloading. The SSL decryption is performed by the device with plain text being sent to the back end servers. Note to allow this mode certificates for each ENAME must be installed on the device and the Oracle Secure Global Desktop configuration changed to allow the Oracle Secure Global Desktop SSL process to accept plain text.
- SSL regeneration. As (b) but the connection to the ENAMES is made using a second SSL connection providing external termination of the connections but SSL for the internal connection.

All of the above configurations have been tested using a Sun Secure Application Switch (N1000) system.

Extension to provide software load distribution

A minor modification to the above solution can be made to allow webtop load distribution without a HWLB. One or more members of the array are chosen as array entry points. This system name becomes the ANAME (the script could be installed as the main entry point for the system or a full URL to the script used as the entry point). If the script detects that a session does not already exist (or if the probe fails), then the script creates a randomly ordered list of array members and probes each in turn and when one responds, this is used for the webtop session. This solution is not as robust as that using a HWLB (since it offers no solution if the entry point system is not available, although the DNS entry for ANAME could be changed to point to another system), nor does it make any attempt to take server load into account, however it is a more cost effective solution.

Sample script

A sample implementation of a script that performs the operations described in this document has been created and is included as a sample with Oracle Secure Global Desktop 4.3 and later. The script contains full details of how it can be used and configured. It is recommended that the load balancer script be inserted so that the load balance redirect takes place when the standard.jsp file is loaded. This is easily achieved by modifying the index.jsp file (located in /sgd directory) to include the load balancer script rather than standard.jsp. Instructions on how to do this are provided in the sample script file provided. This sample can be found at the following location:

```
<TTA_INST_DIR>/webserver/tomcat/6.0.29_axis1.4/webapps/sgd/admin/loaddist/swcd.jsp
```



Design Considerations for Oracle Secure
Global Desktop Deployments
December 2011

Authors : Michael Medefesser, Ryder Brooks
Contributing Authors: Mohan Prabhala,
Carmelo Miraglia

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200

oracle.com



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

Copyright © 2011, 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 licensed through X/Open Company, Ltd. 0611

Hardware and Software, Engineered to Work Together