Deployment Considerations for Oracle Secure Global Desktop
Introduction ........................................................................................................... 1
System Requirements and Support ................................................................. 3
Virtualization Support ....................................................................................... 4
Supported Applications and Protocols ......................................................... 4
Networking Requirements ................................................................................ 5
Microsoft Windows Remote Desktop 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 .............................................................................................. 20
Supported Smart Cards .................................................................................. 20
Appendix A: Oracle Secure Global Desktop Product Architecture........ 21
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 workspaces (applications and desktops) 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 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:

- **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 anywhere access to their workspaces.

- **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 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 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 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):

- 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:

- 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 10 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**

<table>
<thead>
<tr>
<th>OPERATING SYSTEM</th>
<th>SUPPORTED VERSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Solaris OS on SPARC platforms</td>
<td>Solaris 10 update 10, Solaris 10 update 11,</td>
</tr>
<tr>
<td></td>
<td>Solaris 11, 11.1</td>
</tr>
<tr>
<td></td>
<td>Trusted Extensions versions of the above</td>
</tr>
<tr>
<td>Oracle Solaris OS on x86 platforms</td>
<td>Solaris 10 update 10, Solaris 10 update 11,</td>
</tr>
<tr>
<td></td>
<td>Solaris 11, 11.1</td>
</tr>
<tr>
<td></td>
<td>Trusted Extensions versions of the above</td>
</tr>
<tr>
<td>Oracle Linux (32-bit and 64-bit)</td>
<td>5.8, 5.9, 6.2, 6.3, 6.4</td>
</tr>
</tbody>
</table>
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: 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.

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. 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.
Note - The connections between an Oracle Secure Global Desktop Client and an Oracle Secure Global Desktop server is always secure. When you first install SGD, TCP ports and 5307 must be open to connect to SGD.

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, 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 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 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 SP1
- Windows XP Professional SP3

On Windows 7 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 Remote Desktop Services features:

- Audio recording
- Audio redirection
- Clipboard redirection
- COM 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 bit rates of up to 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.


32-bit color is available on 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 Remote Desktop 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, 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
- 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
• KEYBOARD
• RANDR
• XINERAMA

The following X extensions are not supported:
• XVIDEO

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 (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>
<thead>
<tr>
<th>TABLE 2. SUPPORTED INSTALLATION PLATFORMS FOR SGD ENHANCEMENT MODULE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OPERATING SYSTEM</strong></td>
<td><strong>SUPPORTED VERSIONS</strong></td>
</tr>
<tr>
<td>Microsoft Windows (64-bit)</td>
<td>Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2003</td>
</tr>
<tr>
<td>Oracle Solaris OS on SPARC platforms</td>
<td>Solaris 8, 9, 10, 11, 11.1</td>
</tr>
<tr>
<td></td>
<td>Trusted Extensions versions of the above</td>
</tr>
<tr>
<td>Oracle Solaris OS on x86 platforms</td>
<td>Solaris 10, 11, 11.1</td>
</tr>
<tr>
<td></td>
<td>Trusted Extensions versions of the above</td>
</tr>
<tr>
<td>Oracle Linux (32-bit and 64-bit)</td>
<td>5, 6</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (32-bit and 64-bit)</td>
<td>10, 11</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>TABLE 3. SGD WEB SERVER COMPONENTS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>COMPONENT NAME</strong></td>
<td><strong>SGD VERSION 5.0 COMPONENT VERSION</strong></td>
</tr>
<tr>
<td>Apache HTTP Server</td>
<td>2.2.24</td>
</tr>
<tr>
<td>OpenSSL</td>
<td>1.0.0.k</td>
</tr>
<tr>
<td>mod_jk</td>
<td>1.2.37</td>
</tr>
<tr>
<td>Apache Jakarta Tomcat</td>
<td>7.0.37</td>
</tr>
<tr>
<td>Apache Axis</td>
<td>1.4</td>
</tr>
</tbody>
</table>

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

### TABLE 4. SUPPORTED INSTALLATION PLATFORMS FOR SGD GATEWAY HOST

<table>
<thead>
<tr>
<th>OPERATING SYSTEM</th>
<th>SUPPORTED VERSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Solaris OS on SPARC platforms</td>
<td>- Solaris 10 update 10, Solaris 10 update 11, Solaris 11, 11.1</td>
</tr>
<tr>
<td></td>
<td>- Trusted Extensions versions of the above</td>
</tr>
<tr>
<td>Oracle Solaris OS on x86 platforms</td>
<td>- Solaris 10 update 10, Solaris 10 update 11, Solaris 11, 11.1</td>
</tr>
<tr>
<td></td>
<td>- Trusted Extensions versions of the above</td>
</tr>
<tr>
<td>Oracle Linux (32-bit and 64-bit)</td>
<td>5.8, 5.9, 6.2, 6.3, 6.4</td>
</tr>
</tbody>
</table>

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. 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: 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 2.2.24. 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_EXPORT_WITH_RC4_40_MD5`

The following cipher suites are also supported, but must be configured by the user, as shown in the Oracle Secure Global Desktop Gateway Administration Guide:

- `SSL_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 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 11gR1
- Oracle Internet Directory 11gR1 (all 11.1.1.x.0 releases)

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.500 Distinguished Names (DNs) and MD5 signatures of all the CA certificates that SGD supports. Additional configuration is required to support SSL certificates signed by an unsupported CA. Intermediate CAs are supported, but additional configuration might be required if any of the certificates in the chain are signed by an unsupported CA.

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>
<thead>
<tr>
<th>SUPPORTED CLIENT PLATFORM</th>
<th>SUPPORTED BROWSERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS 6.x on Apple iPad 2, 3, 4, mini</td>
<td>Safari</td>
</tr>
<tr>
<td>Microsoft Windows 8 (32-bit and 64-bit) Desktop mode only</td>
<td>Internet Explorer 10, Mozilla Firefox 17.0.2:ESR, 18, Chrome 24</td>
</tr>
<tr>
<td>Microsoft Windows 7 (32-bit and 64-bit)</td>
<td>Internet Explorer 9, Internet Explorer 8, Mozilla Firefox 17.0.2:ESR, 18, Chrome 24</td>
</tr>
<tr>
<td>Microsoft Windows XP Professional SP3 (32-bit)</td>
<td>Internet Explorer 7, 8, Mozilla Firefox 17.0.2:ESR, 18, Chrome 24</td>
</tr>
<tr>
<td>Sun Ray Software on Oracle Solaris (X86 and SPARC platforms) Solaris 10 update 10, 10 update 11, Solaris 11, 11.1</td>
<td>Mozilla Firefox 17.0.2:ESR, 18, Chrome 24</td>
</tr>
<tr>
<td>Sun Ray software on Oracle Linux (32-bit and 64-bit) Oracle Linux 5.8, 5.9, 6.2, 6.3, 6.4</td>
<td>Mozilla Firefox 17.0.2:ESR, 18, Chrome 24</td>
</tr>
<tr>
<td>Mac OS X 10.7 and 10.8</td>
<td>Safari 5, Mozilla Firefox 17.0.2:ESR, 18, Chrome 24</td>
</tr>
<tr>
<td>Oracle Linux 5.8, 5.9, 6.2, 6.3, 6.4 (32-bit and 64-bit)</td>
<td>Mozilla Firefox 17.0.2:ESR, 18, Chrome 24</td>
</tr>
<tr>
<td>Ubuntu 10.04 and 12.04 (32-bit and 64-bit)</td>
<td>Mozilla Firefox 17.0.2:ESR, 18, Chrome 24</td>
</tr>
</tbody>
</table>

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

Beta versions or preview releases of browsers are not supported.

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

Java Plugin tool version 1.6 and 1.7 is supported as a plug-in for Java technology.

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 webtop (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 256 colors.

The SGD Client and webtop 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.
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>
<thead>
<tr>
<th>CLIENT PLATFORM</th>
<th>DEFAULT PDF VIEWER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows platforms</td>
<td>Adobe Reader, at least version 4.0</td>
</tr>
<tr>
<td>Oracle Solaris OS on SPARC platforms</td>
<td>Adobe Reader (acroread)</td>
</tr>
<tr>
<td></td>
<td>GNOME PDF Viewer (gpdf)</td>
</tr>
<tr>
<td>Oracle Solaris OS on x86 platforms</td>
<td>GNOME PDF Viewer (gpdf)</td>
</tr>
<tr>
<td>Linux</td>
<td>GNOME PDF Viewer (gpdf)</td>
</tr>
<tr>
<td></td>
<td>Evince Document Viewer (evince)</td>
</tr>
<tr>
<td></td>
<td>X PDF Reader (xdpdf)</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>Preview App (/Applications/Preview.app)</td>
</tr>
</tbody>
</table>

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 any Personal Computer/Smart Card (PC/SC)-compliant smart card and reader supported for use with Microsoft Remote Desktop services.
Figure 3. Oracle Secure Global Desktop architecture.