SafeNet Authentication Service
Integration Guide

Oracle Secure Desktop Using SAS RADIUS OTP Authentication
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012547-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>May 2014</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
## Contents

Introduction ................................................................................................................................. 4
  Third-Party Software Acknowledgement ................................................................................. 4
  Overview ................................................................................................................................ 4
Solution Flow ............................................................................................................................... 4
Preparation and Pre-requisites ..................................................................................................... 5
Checklists .................................................................................................................................. 5
Configuration ............................................................................................................................... 6
  Configuring Apache to Act as a RADIUS Client ...................................................................... 6
  Configuring Communication between Apache and the NPS/RADIUS Server ......................... 7
  Configuring LDAP Authentication on SGD ............................................................................. 9
Configuring Communication between SAS and the RADIUS Server ........................................ 14
  Configuring a SAS Auth Node and Encryption Key ................................................................. 14
Configuring the NPS/IAS Agent ................................................................................................. 16
Synchronizing User Stores .......................................................................................................... 17
Configuring SAS ......................................................................................................................... 17
  Prerequisites ........................................................................................................................... 17
  SGD Authentication ................................................................................................................ 17
  Configuring Tomcat to Trust Web Server Authentication ....................................................... 18
Solution Dataflow ....................................................................................................................... 18
Running the Solution ................................................................................................................... 19
  Installing the SGD Client ....................................................................................................... 19
  Running the Solution with a MobilePASS Token ................................................................. 21
Troubleshooting ......................................................................................................................... 25
  bin/apxs command failed with rc=65536 ............................................................................. 25
  Wrong ELF class: ELFCLASS64 ......................................................................................... 25
Support Contacts ......................................................................................................................... 26
Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Oracle Secure Global Desktop.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Overview

This document provides guidance for setting up and managing SafeNet Authentication Service (SAS) to protect Oracle Secure Global Desktop (SGD) using RADIUS OTP authentication. It covers the implementation of this process, and facilitates easy installation and configuration for RADIUS authentication with SGD.

Oracle Secure Global Desktop provides secure remote access to applications running on Windows, Linux, Solaris, and Mainframe servers from a wide variety of popular client devices, including Windows and Linux PCs, Macs, and tablets, such as the Apple iPad and Android-based devices. Oracle Secure Global Desktop provides users with the ability to work from anywhere, and gives administrators the control and security needed when providing access to a variety of applications and desktop environments residing in the data center.

The goal of this document is to provide guidance for setting up a RADIUS OTP-based authentication solution in Oracle Secure Global Desktop (SGD) environment.

Solution Flow

1. The user attempts to access the following site: http://<SGDServerURL>/
2. The user is prompted for their user name and password.
3. The user generates a one-time passcode on their token and enters it into the Password prompt.
4. Apache routes the credentials to the NPS server via mod_auth_radius.
5. The NPS server forwards the request to the SAS server.
6. If the credentials match what SAS expects, the server will tell Apache to grant access.
Preparation and Pre-requisites

NOTE: This document assumes that the SGD 5.1 environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

The SGD 5.1 installation includes the following third-party components:

- **Java technology.** This release of SGD includes Java 6, Update 65.

- **SGD web server components.** The SGD web server consists of an Apache web server and Tomcat JavaServer Pages (JSP) technology container preconfigured for use with SGD.

The SGD web server consists of several components. The following table lists the web server component versions for this release of SGD.

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache HTTP Server</td>
<td>2.2.25</td>
</tr>
<tr>
<td>OpenSSL</td>
<td>1.0.0k</td>
</tr>
<tr>
<td>mod_jk</td>
<td>1.2.37</td>
</tr>
<tr>
<td>Apache Tomcat</td>
<td>7.0.42</td>
</tr>
<tr>
<td>Apache Axis</td>
<td>1.4</td>
</tr>
</tbody>
</table>

The Apache web server includes all of the standard Apache modules as shared objects.

Checklists

For establishing the required flow of authentication, the user must perform these tasks in the following sequence:

1. Install SGD.
2. Configure Apache to act as a RADIUS Client.
3. Configure NPS Client.
5. Configure LDAP on SGD.
6. Configure RADIUS Communication between SGD and NPS.
7. Configure NPS/IAS Agent.
8. Synchronize AD and SAS.
10. Enroll a token in SAS.
11. Install SGD Client.
Configuration

When configuring Secure Global Desktop to support multi-factor authentication, for the purpose of working with SafeNet Authentication Service, the RADIUS protocol will be used.

The deployment of multi-factor authentication support using SafeNet Authentication Service with SGD 5.1 requires completion of the following steps:

- Configure SGD Server running on Apache to act as a free-radius client.
- Configure RADIUS communication between Apache and RADIUS/NPS Server.
- Configure RADIUS communication between the RADIUS/NPS Server and SafeNet Authentication Service using NPS/IAS Plugin.

The SGD web server consists of an Apache web server preconfigured for use with SGD. The objective is to instruct Apache to authenticate against an existing RADIUS database.

The integration of SGD (Apache) and RADIUS authentication can be done in various ways. One method is based on a piece of code (mod_auth_radius) from the open source freeradius.org project. In effect, Apache becomes a RADIUS client occupying the traditional position of the NAS in the authentication chain and hits off the RADIUS server for authentication and accounting requests.

Configuring Apache to Act as a RADIUS Client

1. Download mod_auth_radius-1.5.8.tar package from the following site:
   http://freeradius.org/mod_auth_radius/
2. Extract the package mod_auth_radius to obtain the mod_auth_radius.c file.

   [root@oracleDownloads]# tar -xvf mod_auth_radius-1.5.8.tar
   mod_auth_radius-1.5.8/
   mod_auth_radius-1.5.8/Makefile
   mod_auth_radius-1.5.8/README
   mod_auth_radius-1.5.8/.htaccess
   mod_auth_radius-1.5.8/httpd.conf
   mod_auth_radius-1.5.8/index.html
   mod_auth_radius-1.5.8/mod_auth_radius-2.0.c
   mod_auth_radius-1.5.8/mod_auth_radius.c
3. Retrieve mod_auth_radius.

   Since Apache 2.x is being used underneath SGD 5.1, you must obtain the correct version of the mod_auth_radius package. You can download the correct version, mod_auth_radius-2.0.c, from freeradius.org.

   Copy the downloaded package, mod_auth_radius-2.0.c, to Apache’s root directory.

   317 cp mod_auth_radius-2.0.c /opt/tarantella/webserver/apache/2.2.25_openssl-1.0.8k_jkl2.37
   318 cd /opt/tarantella/webserver/apache/2.2.25_openssl-1.0.8k_jkl2.37
4. Build mod_auth_radius-2.0.c.

   As SGD has already built and installed Apache with dynamic modules, to use mod_auth_radius as a dynamic module, use apxs as:

   bin/apxs -l -a -c mod_auth_radius-2.0.c

   This should have added a line in the Apache /opt/tarantella/webserver/apache/(version)/httpd.conf file:

   LoadModule auth_radius_module modules/mod_auth_radius-2.0.so
Configuring Communication between Apache and the NPS/RADIUS Server

NOTE: It is assumed that NPS Server is configured and working with AD authentication.

Configuring NPS Client

To define an SGD server as a RADIUS client:

1. From the NPS Server Management Console, right-click the RADIUS Clients folder and select New RADIUS Client.
2. On the New RADIUS Client screen, provide the following information:

<table>
<thead>
<tr>
<th>Friendly name</th>
<th>Enter a friendly name for the device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Enter the client address of the SGD server.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>Select Manual and then enter the shared secret for communication with the remote RADIUS client.</td>
</tr>
<tr>
<td>Confirm shared secret</td>
<td>Enter the shared secret to confirm it.</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft®, Inc. software. Trademarks are the property of their respective owners.)

3. Click OK.
Configuring Apache (Free RADIUS Client)

In this procedure, you will provide NPS server details that specify where authentication requests will be forwarded by Apache.

1. To configure Apache for RADIUS authentication, you must create a section with specific configuration directives for the `mod_auth_radius` module. At the end of `httpd.conf`, create a section like the following example and configure it as explained:

   ```
   #
   # radius_auth_module add
   #
   Alias /sgd "/opt/tarantella/webserver/tomcat/7.0.42_axis1.4/webapps/sgd"
   
   <IfModule radius auth module>
   AddRadiusAuth 172.25.12.173:1812 1111 5:3
   AddRadiusCookieValid 0
   </IfModule>
   ```

   - The `AddRadiusAuth` directive tells Apache to authenticate against RADIUS. You specify the name/IP address of the RADIUS server, port, shared secret for the web client, and timeout period Apache should wait before giving up and assuming no response will be sent.
   - The `AddRadiusCookieValid` directive specifies, in minutes, the length of time that the cookie sent in the response to the end user from the web client is valid. Setting this value to zero (0) signifies that the cookie will be valid forever.


   The initial configuration is now complete. The next step is to define the areas of the website that need protection. To control access when using `httpd.conf`, add the section to the file and configure it as follows:

   ```
   SetEnvIf Request_URI "^\.(cab|jar|gif|der|class)$" sgd_noauth_ok
   
   <LocationMatch "/sgd"/>
   Order Allow,Deny
   Allow from env=sgd_noauth_ok
   AuthType Basic
   AuthName "SafeNet Authentication"
   AuthBasicAuthoritative off
   AuthRadiusAuthoritative on
   AuthRadiusCookieValid 15
   AuthRadiusActive On
   Require valid-user
   Satisfy any
   </LocationMatch>
   ```

   The following definitions provide an explanation of each of these directives:

   - **AuthType**: This module requires basic authentication.
   - **AuthName**: The contents of this string are included in the password prompt presented to the user.
   - **AuthBasicAuthoritative**: This directive ensures that other authentication types are not used for this particular site area.
   - **AuthRadiusAuthoritative**: This directive tells Apache to consider all RADIUS responses authoritative; that is, the RADIUS responses are "the final answer" for authentication.
• **AuthRadiusCookieValid**: The server will choose the lower of the two values (AddRadiusCookieValid set in previous step) and set the cookie to expire at that interval. This value is in minutes.

• **AuthRadiusActive**: This turns on RADIUS authentication globally for the site.

• **Require valid-user**: This directive ensures that only valid users can access the site. All the authentication requests are processed on RADIUS Server.

3. Restart the web server.
   `/opt/tarantella/bin/tarantella restart`

4. Test the RADIUS authentication.
   • When attempting to access the server, you will be prompted for your user name and password.
   • Verify if authentication is successful using AD credentials.

---

**Configuring LDAP Authentication on SGD**

NOTE: For more details on various user synchronization methods and authentication details, refer to the following link:

http://docs.oracle.com/cd/E41492_01/E41495/E41495.pdf

To enable LDAP authentication:

1. Open a browser and go to https://server.example.com, where server.example.com is the name of an SGD server. The SGD web server **Welcome** window is displayed, as shown in the example below:

   ![Welcome window](image-url)

   *(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)*
2. In the SGD Administration Console, the **Navigation View** is displayed.

![Oracle SGD Administration Console](image1)

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)

3. Click the **Global Settings** tab, and then click the **Secure Global Desktop Authentication** tab. Click the **Change Secure Global Desktop Authentication** button.

![Oracle SGD Global Settings](image2)

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)
4. On the **Secure Global Desktop Authentication Configuration** window, click **Next**.

![Secure Global Desktop Authentication Configuration](image)

*Background Knowledge*

When a user logs in, the Secure Global Desktop server tries to authenticate the user based on the given credentials (typically username and password) using different authentication mechanisms, for example LDAP.

The authentication mechanisms are tried in a fixed order until one authentication mechanism is able to authenticate the user. In case of a successful authentication, the following things happen:

1. A User Identity is created. A User Identity is a unique runtime identifier for that user.
2. A User Profile is associated to the user. A User Profile is a set of configuration data and is found in the Local Repository.

If none of the authentication mechanisms is able to authenticate the user, the login fails.

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)

5. Under **Third-Party/System Authentication**, select the **System Authentication** check box and then click **Next**.

![Secure Global Desktop Authentication Configuration](image)

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)
6. Under **System Authentication - Repositories**, select the **LDAP/Active Directory** check box, and then click **Next**.

![Secure Global Desktop Authentication Configuration](image)

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)

7. Under **LDAP Repository Details**, configure the LDAP directory details, and then click **Next**.

<table>
<thead>
<tr>
<th><strong>Repository Type</strong></th>
<th><strong>Select LDAP.</strong></th>
<th>(Select this option even if you are using a Microsoft Active Directory server for LDAP authentication.)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>URLs</strong></td>
<td>Enter the URL of one or more LDAP directory servers.</td>
<td></td>
</tr>
<tr>
<td><strong>User Name</strong></td>
<td>Enter your LDAP user name.</td>
<td></td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter your LDAP password.</td>
<td></td>
</tr>
</tbody>
</table>
8. **Under Review Selections**, verify the authentication configuration, and then click **Finish**.

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)
Configuring Communication between SAS and the RADIUS Server

To allow the NPS server to communicate with SAS, install the SAS NPS/IAS Agent on the NPS server.

NOTE: For more information on how to install and configure SAS NPS/IAS Agent for NPS, refer to the following link:

Configuring a SAS Auth Node and Encryption Key

In the event that the SAS server is not installed on the same machine as NPS, the following steps must be performed:

1. Log in to the SAS console as the account operator.
2. Click Virtual Servers > Comms > Authentication Processing.
3. Click the Authentication Agent Settings link, and then select Download to download the encryption key file. This file will be needed in step 3 of “Configuring the NPS/IAS Agent” on page 16.
4. Click **Virtual Servers > Comms > Auth Nodes**.

5. Click the **Auth Nodes** link and select **Add**. Complete the **Auth Notes** tab as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent Description</strong></td>
<td>Enter a description for this node.</td>
</tr>
<tr>
<td><strong>Host Name</strong></td>
<td>Enter a host name.</td>
</tr>
<tr>
<td><strong>Low IP Address in Range</strong></td>
<td>Enter the low IP address for this range.</td>
</tr>
<tr>
<td><strong>High IP Address in Range</strong></td>
<td>Enter the high IP address for this range. (The low and high IP addresses can be the same since the node is referencing a single machine.)</td>
</tr>
<tr>
<td><strong>Exclude from PIN change requests</strong></td>
<td>Do not select this check box.</td>
</tr>
</tbody>
</table>

![Auth Nodes](image_url)
Configuring the NPS/IAS Agent

1. From the Start menu, open the NPS/IAS Configuration Tool.
2. On the NPS/IAS Settings tab, under Agent Activation, select the Enable to activate the plugin.

3. If a SAS server is not installed on the same machine as the NPS, a key encryption file needs to be loaded (the key file that was downloaded in step 3 on page 14).
4. On the Communications tab, in the Location (IP:Port) field, enter the SAS server IP address.
5. Click Apply.
6. Click OK.
Synchronizing User Stores

Before SafeNet Authentication Service can authenticate any user in AD, you must create a user store in the service that reflects the users that would need to use multi-factor authentication.

User entries/records are created in a SafeNet Authentication Service user store using a number of methods:

- Manually—one user at a time, using the Create User shortcut.
- Manually—by importing one or more user records using a flat file.
- Automatically—by synchronizing with your Active Directory / LDAP server using the SAS LDAP Synchronization Agent.

For working with Microsoft AD, LDAP synchronization is preferred.

For further information on adding users to SAS, refer to product documentation at the following location:

http://www2.safenet-inc.com/sas/implementation-guides.html

Configuring SAS

Prerequisites

- SAS-PCE server is already installed.
- A subscriber account exists.
- Users with the same user name as in Linux/UNIX are added to the account.
- Users should have a token provisioned in SAS.

SGD Authentication

SGD has two stages to user authentication:

- Stage 1: Users authenticate to an SGD server to log in to SGD.
- Stage 2: Users authenticate to an application server to run an application.
Configuring Tomcat to Trust Web Server Authentication

To configure the Tomcat component of the SGD web server to trust the web server's authentication:

1. Edit the Tomcat configuration file, which is located at:
   
   /opt/tarantella/webserver/tomcat/7.0.42_axis1.4/conf/server.xml

2. Amend the configuration of the Coyote/JK2 AJP 1.3 Connector to add a `tomcatAuthentication="false"` attribute to the `<Connector>` element as follows:

   ```
   <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" allowTrace="false" tomcatAuthentication="false">
   ```

3. Save the file.

4. Restart the SGD Web Server.

Solution Dataflow

1. The client browser submits a page request for `http://<SGDServerURL>/sgd`

2. Apache sees that the directory is secured and sends an **Authorization Required** request (with spaces for the user name and password) to the end user.

3. The user responds to the authentication request with his credentials. The browser sends the response and the same page request again to Apache.
4. Apache receives the user's response and hands it off to `mod_auth_radius`. The module sees that a cookie is not present (since this is the user's first request). It constructs a RADIUS request and transmits it to the RADIUS/NPS server.

5. The NPS/IAS plug-in installed on the RADIUS server forwards the request to SAS.

6. The SAS server performs the authentication and sends its response back to the RADIUS server.

7. The RADIUS server sends its response back to `mod_auth_radius`.

8. Next, `mod_auth_radius` interprets the RADIUS server's decision. If the authentication was deemed successful, the module sends a cookie with the public and private information hidden using MD5. If the authentication was unsuccessful, the module returns an Access Denied message.

9. Even if the web browser sends the cookie with another request, as long as `mod_auth_radius` recognizes the cookie as valid, it will not send another request to the RADIUS server.

Running the Solution

Installing the SGD Client

SGD can be set for automatic installation or the SGD Client can be manually downloaded. SGD requires JRE installation in the browser:

1. Open your browser and enter the URL of the SGD server (https://oracle.linux/).

2. Click Install the Oracle Secure Global Desktop Client.

   ![Oracle Secure Global Desktop](https://oracle.linux)

   Log in to Oracle Secure Global Desktop.

   Log in to your Desktop.

   The Oracle Secure Global Desktop Administration Console.

   The standard client which is typically used automatically. On some locked-down systems you may need to manually install it.

   *(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)*
3. Under **Microsoft Windows**, click the **Download the Secure Global Desktop Client for Microsoft Windows** link.

![Secure Global Desktop](https://oracle/oracle)

<table>
<thead>
<tr>
<th>Component versions: 5.10.901</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac OS X</td>
</tr>
<tr>
<td>- Download the Secure Global Desktop Client for Mac OS X, OracleSecureGlobalDesktopClient.dmg, to a temporary directory on your Mac.</td>
</tr>
<tr>
<td>- Double-click OracleSecureGlobalDesktopClient.dmg to open the installer disk image.</td>
</tr>
<tr>
<td>- In the window that appears, double-click the Oracle Secure Global Desktop Client.pkg package to install the Secure Global Desktop Client.</td>
</tr>
<tr>
<td>- Follow the instructions on your screen.</td>
</tr>
<tr>
<td>Microsoft Windows</td>
</tr>
<tr>
<td>- Download the Secure Global Desktop Client for Microsoft Windows, sgdesktop-em.msi, to a temporary directory on your PC.</td>
</tr>
<tr>
<td>- Double-click sgdesktop-em.msi to install the Secure Global Desktop Client.</td>
</tr>
<tr>
<td>- Follow the instructions on your screen.</td>
</tr>
<tr>
<td>Linux x86 32-bit</td>
</tr>
<tr>
<td>- Download the Secure Global Desktop Client for Linux x86 32-bit, sgdesktop1.tar, to a temporary directory on your system.</td>
</tr>
<tr>
<td>- At a command prompt, extract the tar file by typing <code>tar xvf sgdesktop1.tar</code>.</td>
</tr>
<tr>
<td>- Install the Client by typing <code>sudo /install</code>.</td>
</tr>
<tr>
<td>- Follow the instructions on your screen.</td>
</tr>
<tr>
<td>Solaris™ Operating System (Solaris OS) on x86 platforms</td>
</tr>
<tr>
<td>- Download the Secure Global Desktop Client for Solaris OS on x86 platforms, sgdesktop2.tar, to a temporary directory on your system.</td>
</tr>
<tr>
<td>- At a command prompt, extract the tar file by typing <code>tar xvf sgdesktop2.tar</code>.</td>
</tr>
</tbody>
</table>

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)

4. Click **Run**.

5. When the Setup Wizard opens:
   a. Click **Next**.
   b. Click **Install for Everyone**.
   c. Click **Install**.

![Secure Global Desktop Client](https://oracle/oracle)

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)
Running the Solution with a MobilePASS Token

A user, Bob, has been assigned an MP-1 token in SAS, which will be used to authenticate against SGD.

1. Enter the URL of your SGD server, and then click Connect if logging in through SGD Client as shown:

![ SGD Client Login Screen ]

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)

2. The URL opens and the user is prompted for their user name and password. Generate an OTP and enter it in the Password field.

![ OTP Entry Screen ]

3. Click OK.
4. If the user’s credentials are valid, a session is established and the user is redirected to their workspace.

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)

5. You must now authenticate against the application server. To do so, click on any application in the Workspace pane (for example, My Desktop).

6. On the login window, enter your user name and password for accessing the application server, and then click OK.

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)
7. If the credentials are verified, the Windows Desktop is displayed.

8. To end the My Desktop session, close the Windows Desktop window, and then click **OK** to confirm.
9. You will be returned to the Oracle Workspace window, which will show, in the left pane, the last opened session as Windows Desktop.

![Image of Oracle Workspace](https://example.com/oracle-workspace.png)

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)

10. To log out of SGD, close or suspend the applications, and then click the **Logout** button.

![Image of SGD Logout](https://example.com/sgd-logout.png)

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)
11. Click **OK** to confirm.

![Image of Oracle Secure Global Desktop](image-url)

*(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)*

**Troubleshooting**

**bin/apxs command failed with rc=65536**

To resolve this issue:

- Provide `tag="CC"` for compiling `mod_auth_radius-2.0.c`.
- Check for missing header files `md5.h` and `e_os2.h` in the `openssl` package and copy them to the Apache root directory.

**Wrong ELF class: ELFCLASS64**

On 64-bit Linux systems, this issue is due to a `mod_auth_radius.2.0` that has been built for 64-bit, whereas all the files in the Apache root directory/module are, by default, 32-bit.

- Check for 32-bit libraries or install them
- Provide the `–m32` tag when compiling and linking `mod_auth_radius-2.0.c`.
Support Contacts

If you encounter a problem while installing, registering, or operating this product, make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Table 1: Support Contacts

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td>Phone</td>
<td>United States 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>