SafeNet Authentication Manager
Integration Guide

SAM using RADIUS Protocol with Oracle Secure Global Desktop
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012562-001, Rev. B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>October 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

Third-Party Software Acknowledgement...............................................................4
Description.............................................................................................................4
Applicability..........................................................................................................4
Environment .........................................................................................................5
Audience................................................................................................................5
RADIUS-based Authentication using SAM ............................................................5
RADIUS Authentication Flow using SAM............................................................6
RADIUS Prerequisites..........................................................................................6
Configuring SafeNet Authentication Manager......................................................7
  - Synchronizing User Stores to SafeNet Authentication Manager .......................7
  - Configuring SAM’s Connector for OTP Authentication.......................................7
  - Token Assignment in SAM ...............................................................................8
  - Adding Oracle Secure Global Desktop as a RADIUS Client in IAS/NPS ............8
  - SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration ....................10
Configuring Oracle Secure Global Desktop.........................................................11
  - Configuring an SGD Server to Act as a RADIUS Client..................................11
  - Configuring Oracle Secure Global Desktop for Two-Factor Authentication ......14
  - Configuring Tomcat to Trust Web Server Authentication..............................22
Running the Solution ............................................................................................23
Appendix: Performing Java Settings .....................................................................25
Support Contacts ....................................................................................................27
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.

Description

SafeNet Authentication Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

Oracle Secure Global Desktop (SGD) 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 applications and desktop environments residing in the data center.

Oracle Secure Global Desktop can be configured to communicate with SAM through the RADIUS protocol. This integration enables strong two-factor authentication for users accessing protected resources.

This document describes how to:

- Configure Oracle Secure Global Desktop to work with SafeNet Authentication Manager in RADIUS mode.

It is assumed that the Oracle Secure Global Desktop environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager installation modes, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

Oracle Secure Global Desktop can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with SafeNet Authentication Manager.

Applicability

The information in this document applies to SafeNet Authentication Manager, a server version of SAM that is used to deploy the solution on-premises in the organization.
Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Manager 8.2 HF 493** - A server version of SAM that is used to deploy the solution on-premises in the organization.
- **Oracle Secure Global Desktop version 4.7 and 5.1**

Audience

This document is targeted to system administrators who are familiar with Oracle Secure Global Desktop and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Manager.

RADIUS-based Authentication using SAM

SafeNet’s OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SafeNet Authentication Manager (SAM).

SAM’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS, providing strong authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*. 
RADIUS Authentication Flow using SAM

SafeNet Authentication Manager communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Oracle Secure Global Desktop.

1. A user attempts to log on to Oracle Secure Global Desktop using an OTP token.
2. Oracle Secure Global Desktop sends a RADIUS request with the user’s credentials to SafeNet Authentication Manager for validation.
3. The SAM authentication reply is sent back to Oracle Secure Global Desktop.
4. The user is granted or denied access to Oracle Secure Global Desktop based on the OTP value calculation results from SAM and is connected to Oracle Secure Global Desktop.

RADIUS Prerequisites

To enable SafeNet Authentication Manager to receive RADIUS requests from Oracle Secure Global Desktop, ensure the following:

- End users can authenticate from the Oracle Secure Global Desktop environment with a static password before configuring Oracle Secure Global Desktop to use RADIUS authentication.
- Ports 1812/1813 are open to and from Oracle Secure Global Desktop.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and the RADIUS client for encryption, decryption, and digital signature purposes.
Configuring SafeNet Authentication Manager

The deployment of multi-factor authentication using SAM with Oracle Secure Global Desktop using the RADIUS protocol requires the following:

- Synchronizing User Stores to SafeNet Authentication Manager, page 7
- Configuring SAM’s Connector for OTP Authentication, page 7
- Token Assignment in SAM, page 8
- Adding Oracle Secure Global Desktop as a RADIUS Client in IAS/NPS, page 8
- SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration, page 10

Synchronizing User Stores to SafeNet Authentication Manager

SAM manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (stand-alone) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Configuring SAM’s Connector for OTP Authentication

SafeNet Authentication Manager is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications, including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected the Simplified OTP-only configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The Simplified OTP-only configuration is as follows:

- **Connectors** - SAM Connector for OTP Authentication is installed
- **SAM Back-end Service** - Activated on this server; scheduled to operate every 24 hours
In addition, the SAM default policy is set as follows:

- OTP support (required for OTP) is selected in the **Token Initialization** settings.
- The **SAM Connector for OTP Authentication** is set, by default, to enable enrollment of OTP tokens without requiring changes in the TPO settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

**Token Assignment in SAM**

SAM supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through Oracle Secure Global Desktop.

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- MobilePASS
- SafeNet eToken 3400

Tokens can be assigned to users as follows:

- **SAM Management Center**: Management site used by SAM administrators and help desk for token enrollment and lifecycle management.
- **SAM Self-Service Center**: Self-service site used by end users for managing their tokens.
- **SAM Remote Service**: Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

**Adding Oracle Secure Global Desktop as a RADIUS Client in IAS/NPS**

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in Oracle Secure Global Desktop.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in Oracle Secure Global Desktop.

Oracle Secure Global Desktop must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Oracle Secure Global Desktop for authentication.

---

**NOTE:** This document assumes that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

The details below refer to NPS, and are very similar to IAS.
To add a RADIUS client:

2. On the NPS web console, in the left pane, expand RADIUS Clients and Servers, right-click RADIUS Clients and then click New.

3. On the New RADIUS Client window, complete the following fields on the Settings tab:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable this RADIUS client</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Friendly name</td>
<td>Enter a RADIUS client name.</td>
</tr>
<tr>
<td>Address (IP or DNS)</td>
<td>Enter the IP address or DNS of Oracle Secure Global Desktop.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>Enter the shared secret for the RADIUS client. The value must be the same when configuring the RADIUS server in Oracle Secure Global Desktop.</td>
</tr>
<tr>
<td>Confirm shared secret</td>
<td>Re-enter the shared secret to confirm it.</td>
</tr>
</tbody>
</table>

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

Oracle Secure Global Desktop is added as a RADIUS client in NPS.

**SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration**

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) as Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

SAM’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*. 
Configuring Oracle Secure Global Desktop

Configuring Oracle Secure Global Desktop to support multi-factor authentication using RADIUS protocol requires the following:

- Configuring an SGD Server to Act as a RADIUS Client, page 11
- Configuring Oracle Secure Global Desktop for Two-Factor Authentication, page 14
- Configuring Tomcat to Trust Web Server Authentication, page 22

The Apache web server is configured to use SGD. The objective is to instruct Apache to authenticate against an existing RADIUS database.

Configuring an SGD Server to Act as a RADIUS Client

The integration of SAM with SGD using 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 NAS in the authentication chain and hits off the RADIUS server for authentication and accounting requests.

Install the mod_auth_radius Module

1. Download the mod_auth_radius-1.5.8.tar package from the following site:
   http://freeradius.org/mod_auth_radius/

   Since Apache 2.x is being used underneath SGD, you must obtain the correct version of the mod_auth_radius package.

2. Extract the mod_auth_radius package to obtain the mod_auth_radius.c file.

   ```bash
   [root@oracle Downloads]# 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
   
   [root@oracle Downloads]# ls
   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. Go to the directory where the mod_auth_radius package is extracted.
4. Run the following command to copy the mod_auth_radius-2.0.c file to the Apache root directory.

   ```bash
   cp mod_auth_radius-2.0.c /opt/tarantella/webserver/apache/2.2.25_openssl-1.0.0k_jk1.2.37
   ```

5. Build mod_auth_radius-2.0.c.

   Go to the location `/opt/tarantella/webserver/apache/2.2.25_openssl-1.0.0k_jk1.2.37` and complete the following:
   - For 32-bit OS, 32-bit libraries should be installed.
   - Open the config_vars.mk file from this location: `/opt/tarantella/webserver/apache/2.2.25_openssl-1.0.0k_jk1.2.37/build`
   - Modify the CC and CPP values as mentioned below and save the file:

     ```bash
     CC = gcc
     ```
CPP= gcc –E

Now, run this command:

../bin/apxs/ –i –a –c mod_auth_radius-1.5.8/mod_auth_radius-2.0.c

• For 64-bit OS, 32-bit libraries should be installed as all other files in Apache are of 32-bit.

Open the config_vars.mk file from this location: /opt/tarantella/webserver/apache/2.2.25_openssl-1.0.0k_jk1.2.37/build

Modify the CC and CPP values as mentioned below and save the file:

CC = gcc –m32
CPP= gcc –E

NOTE: The -m32 tag is used to compile the module in 32-bit. Ensure that gcc compiler is installed before running the command.

The common package, which includes the above library files, is glibc. The package may be different depending upon the operating system.

Run this command:

../bin/apxs/ –i –a –c mod_auth_radius-1.5.8/mod_auth_radius-2.0.c

The above command adds the following line in the httpd.conf file located at

/opt/tarantella/webserver/apache/{version}/conf/:

LoadModule radius_auth_module modules/mod_auth_radius-2.0.so

Configuring Apache for RADIUS Authentication

Configure the RADIUS server details that specify where Apache will forward authentication requests.

1. Go to the location /opt/tarantella/webserver/apache/{version}/conf/.

2. Open the httpd.conf file. At the end of the file create a section and configure for the mod_auth_radius module as explained below:

```c
# 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, and shared secret for the web client, and the 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.
3. You can protect the area of the website; for example, alias /sgd created in the previous step. Add a section in the httpd.conf file and configure it as follows:

```xml
SetEnvIf Request_URI "\.(cab|jar|gif|der|class|png)"  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>

<LocationMatch "/sgdadmin">
  Order Allow,Deny
  Allow from env=sgd_noauth_ok
  AuthType Basic
  Allow from all
</LocationMatch>
```

Each of these directives is explained below:

<table>
<thead>
<tr>
<th>Directive</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthType</td>
<td>This module requires basic authentication.</td>
</tr>
<tr>
<td>AuthName</td>
<td>The contents of this string are included in the password prompt presented to the user.</td>
</tr>
<tr>
<td>AuthBasicAuthoritative</td>
<td>This directive ensures that other authentication types are not used for this particular site area.</td>
</tr>
<tr>
<td>AuthRadiusAuthoritative</td>
<td>This directive tells Apache to consider all RADIUS responses authoritative; that is, the RADIUS responses are &quot;the final answer&quot; for authentication.</td>
</tr>
<tr>
<td>AuthRadiusCookieValid</td>
<td>This 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. The server will take the lower of the two values, the AddRadiusCookieValid directive set here and the AddRadiusCookieValid directive set in the previous step, and set the cookie to expire at that interval.</td>
</tr>
<tr>
<td>AuthRadiusActive</td>
<td>This turns on RADIUS authentication globally for the site.</td>
</tr>
<tr>
<td>Require valid-user</td>
<td>This directive ensures that only valid users can access the site. All the authentication requests are processed on the RADIUS server.</td>
</tr>
</tbody>
</table>

4. Restart the SGD web server using the following command:

   /opt/tarantella/bin/tarantella restart
Configuring Oracle Secure Global Desktop for Two-Factor Authentication

For details on various user synchronization methods and authentication details, refer to:
http://docs.oracle.com/cd/E41492_01/E41495/E41495.pdf

1. In a web browser, open this URL: https://<name of SGD server>/
2. On the welcome window, click the Launch the Oracle Secure Global Desktop Administrator Console link and log in.

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)
3. On the **Oracle SGD Administrator Console** window, perform the following steps:
   
   a. Click the **Global Settings** tab.
   
   b. Click the **Secure Global Desktop Authentication** tab.
   
   c. Click **Change Secure Global Desktop Authentication**.

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)
4. On the **Step 1: Overview** window, read the overview, and then click **Next**.

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)
5. On the **Step 2: Third-Party / System Authentication** window, select the following authentication types, and then click **Next**:

- Third-Party Authentication
- System Authentication

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

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)
7. On the **Step 4: System Authentication – Repositories** window, select **Unix**, and then click **Next**.

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)
8. On the **Step 4.1: Unix Authentication – User Profile** window, select the following, and then click **Next**:
   - Search Unix User ID in Local Repository
   - Search Unix Group ID in Local Repository

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)
On the **Step 5: LDAP Repository Details** window, click **Next**.

(The screen image above is from Oracle® software. Trademarks are the property of their respective owners.)
10. On the **Step 5: Review Selections** window, review the authentication configuration, and then click **Finish**.

![Step 5: Review Selections](image)

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

**Configuring Tomcat to Trust Web Server Authentication**

1. Edit the Tomcat configuration file, `server.xml`, which is located at:
   ```
   /opt/tarantella/webserver/tomcat/7.0.42_axis1.4/conf/
   ```
2. Modify the **Coyote/JK2 AJP 1.3 Connector** configuration 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 `server.xml` file.
4. Restart the SGD web server using the following command:
   ```
   /opt/tarantella/bin/tarantella restart
   ```
Running the Solution

Before running this solution, ensure that:

- Oracle Secure Global Desktop client is installed.
- The SGD server certificate is installed on all client machines to avoid certificate warnings.

For this solution, the SafeNet eToken 3400 is used as the enrolled OTP token.

1. Start the Oracle Secure Global Desktop application.

2. On the Oracle Secure Global Desktop window, perform the following steps:
   a. Select Define a new server by URL.
   b. In the URL field, enter the URL of your SGD server.
   c. Click Connect.

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

3. On the Windows Security window, enter your user name and the generated OTP passcode, and then click OK.

   (The screen image above is from Windows® software. Trademarks are the property of their respective owners.)
On successful authentication, the user is logged in to its workspace.

(The screen images above are from Oracle® software. Trademarks are the property of their respective owners.)
Appendix: Performing Java Settings

Java shows certain warning messages before connecting to the Oracle Secure Global Desktop server. To avoid these warnings, perform the following steps on the client machine:

1. Open the **Java Control Panel**.
2. Click the **Security** tab.
3. Set **Security Level** to **Medium**.
4. Click **Edit Site List**, and then add the SGD URL in the exception list.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
5. On the Java Control Panel, click the **Advanced** tab.

6. Under **Java Plug-in**, clear the option **Enable the next-generation Java Plug-in (Requires browser restart)**.

7. Click **OK**.
Support Contacts

If you encounter a problem while installing, registering, or operating this product, please 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><strong>Address</strong></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><strong>Phone</strong></td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support Customer Portal</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td></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>