SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for SonicWALL Secure Remote Access
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms’ resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2015 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-012744-001, Rev. B
Release Date: June 2016
Contents

Third-Party Software Acknowledgement .............................................................................. 4
Description .......................................................................................................................... 4
Applicability ....................................................................................................................... 5
Environment ....................................................................................................................... 5
Audience .............................................................................................................................. 5
SAML Authentication using SafeNet Authentication Service Cloud .................................. 5
SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE66
SAML Authentication Flow using SafeNet Authentication Service ..................................... 6
SAML Prerequisites .......................................................................................................... 6
Configuring SonicWALL Secure Remote Access ................................................................. 7
  Importing SAS Certificate .............................................................................................. 7
  Creating a Realm ........................................................................................................... 10
  Creating a User ............................................................................................................. 14
  Applying Configuration Changes .................................................................................. 16
Configuring SafeNet Authentication Service ................................................................... 17
  Synchronizing Users Stores to SafeNet Authentication Service .................................... 17
  Assigning an Authenticator in SafeNet Authentication Service .................................... 17
  Adding SonicWALL Secure Remote Access as a Service Provider (SP) in SafeNet Authentication Service ................................................................. 18
  Enabling SAML Services in SafeNet Authentication Service ......................................... 21
Running the Solution ........................................................................................................ 27
Support Contacts ............................................................................................................. 29
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as SonicWALL Secure Remote Access.

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 Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

SonicWALL Secure Remote Access (SRA) appliances extend secure remote networking over an SSL VPN to potentially thousands of locations—providing anytime, anywhere access. The encrypted SSL VPN tunnel protects the transmitted data. In addition, as an added layer of protection, granular access controls allow the administrator to delegate access privileges to different individuals or groups so that they can access only specific, defined resources. SonicWALL SRA appliances integrate seamlessly with virtually any firewall.

This document describes how to:


(The screen image above is from Dell®. Trademarks are the property of their respective owners.)
• Configure SAML authentication in SonicWALL Secure Remote Access using SafeNet Authentication Service as an identity provider.

It is assumed that the SonicWALL Secure Remote Access environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

SonicWALL Secure Remote Access can be configured to support multi-factor authentication in several modes. The SAML authentication will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet's cloud-based authentication service
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by Service providers to deploy instances of SafeNet Authentication Service
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version 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 Service**—SafeNet's cloud-based authentication service
- **SonicWALL Secure Remote Access 11.0**

Audience

This document is targeted to system administrators who are familiar with SonicWALL Secure Remote Access, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

SAML Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (SAS) Cloud provides a service for SAML authentication that is already implemented in the SAS Cloud environment and can be used without any installation.
SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service (SAS) comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)**—An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.

- **SafeNet Authentication Service – Private Cloud Edition (PCE)**—An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, SAS can be integrated with the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

For more information on how to install and configure the SafeNet Authentication Service Agent for Shibboleth, refer to the SafeNet Support Portal.

**SAML Authentication Flow using SafeNet Authentication Service**

SafeNet Authentication Service (SAS) communicates with a large number of service providers and cloud-based services solutions using the SAML protocol.

The image below describes the dataflow of a multi-factor authentication transaction for SonicWALL Secure Remote Access.

1. A user attempts to log on to SonicWALL Secure Remote Access. The user is redirected to SafeNet Authentication Service. SAS collects and evaluates the user’s credentials.

2. SAS returns a response to SonicWALL Secure Remote Access, accepting or rejecting the user’s authentication request.

**SAML Prerequisites**

To enable SafeNet Authentication Service (SAS) to receive SAML authentication requests from SonicWALL Secure Remote Access, ensure that the end users can authenticate from the SonicWALL Secure Remote Access environment with a static password.
Configuring SonicWALL Secure Remote Access

To add SafeNet Authentication Service (SAS) as an Identity Provider in SonicWALL Secure Remote Access:

- Import SAS certificate
- Creating a realm
- Creating a user
- Applying configuration changes

Importing SAS Certificate

The SAS certificate is imported on the SonicWALL SRA appliance so that a trust can be established between SAS and the SonicWALL appliance. Use the SAS certificate that was downloaded in the Downloading SAS Certificate section on page 16.

1. Open the SonicWALL Management Console and log in as an administrator.
2. On the Secure Mobile Access Management Console window, in the left pane, under System Configuration, click SSL Settings.

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)
3. In the right pane, on the SSL Settings tab, under CA certificates, click the first Edit link.

![SSL Settings](image)

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

4. In the right pane, under Filters, click New.

![CA Certificates](image)

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)
5. In the right pane, select **Certificate file**, and then click **Choose File** to browse and select the downloaded SAS certificate.

![Import CA Certificate](image)

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

6. Click **Import**.

The SAS certificate is imported successfully.
Creating a Realm

A realm references an authentication server and determines which access agents are provisioned to users and which endpoint control restrictions are imposed.

1. Open the SonicWALL Management Console.
2. On the Secure Mobile Access Management Console window, in the left pane, under User Access, click Realms.

3. In the upper right corner of the window, click the New realm link.
4. On the **Configure Realm** window, in the **General** tab, complete the following details:
   a. In the **Name** field, enter a name for the realm.
   b. In the **Authentication server** field, click **New**.

   ![Configure Realm Window](image)

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

c. Under **Authentication directory**, select **CA SiteMinder**, and then click **Continue**.

   ![New Authentication Server Window](image)

   *(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*
d. On the **Configure Authentication Server** window, complete the details as specified below, and then click **Save**.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the authentication server; for example, <strong>SAS Cloud SAML</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Appliance ID</strong></td>
<td>Enter a unique <strong>Entity ID</strong> of the SonicWALL Secure Remote Access appliance. Note that this <strong>Entity ID</strong> will be required while configuring SAS.</td>
</tr>
</tbody>
</table>
| **Server ID** | Enter the SAS **Entity ID**.  
To obtain the SAS Entity ID, perform the following steps:  
1. Log in to the SAS console with an Operator account.  
2. Click the **COMMS** tab and then select the **SAML Service Providers** module.  
3. Click the **SAML 2.0 Settings** link.  
4. Copy the **Entity ID**.  
5. Paste the **Entity ID** in the **Server ID** field. |
| **Authentication service URL** | Enter the SAS **Identity Provider HTTP-Redirect login URL**.  
To obtain the URL, the steps are similar to the steps specified for Server ID. |
| **Logout Service URL** | Enter the SAS **Identity Provider logout URL**.  
To obtain the URL, the steps are similar to the steps specified for Server ID. |
| **Trust the following certificate** | Select the imported SAS certificate.  
To import a SAS certificate, refer to “Importing SAS Certificate” on page 7. |

---

*The screen image above is from Dell®. Trademarks are the property of their respective owners.*
5. On the Configure Realm window, the newly created authentication server is populated in the Authentication Server field. Click Next > Finish.

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

A realm is created and its details are displayed.

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)
Creating a User

A user is an individual who needs access to resources on the corporate network. After creating users on the SonicWALL Secure Remote Access appliance, you can reference them in an Access Control Rule to permit or deny access to resources.

1. Open the SonicWALL Management Console.
2. On the Secure Mobile Access Management Console window, in the left pane, under Security Administration, click Users & Groups.


(The screen image above is from Dell®. Trademarks are the property of their respective owners.)
4. On the **Add Mapped Account** window, complete the details as specified below, and then click **Save**.

<table>
<thead>
<tr>
<th><strong>Select realm</strong></th>
<th>Select the realm you created using “Creating a Realm” on page 10.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User type</strong></td>
<td>Select <strong>User</strong>.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>Enter the name of the user. The user name must be same as specified in SAS.</td>
</tr>
<tr>
<td><strong>Display name</strong></td>
<td>Enter the name of the user for display.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter the description of this mapped account.</td>
</tr>
</tbody>
</table>

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)
Applying Configuration Changes

After you have made the configuration changes, you need to apply them in the system.

1. Open the SonicWALL Management Console.
2. On the Secure Mobile Access Management Console window, in the upper right corner, click the Pending changes link.

3. On the Apply Pending Changes window, click Apply Changes.

4. Click Close.
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with SonicWALL Secure Remote Access using SAML authentication requires:

- Synchronizing Users Stores to SafeNet Authentication Service, page 17
- Assigning an Authenticator in SafeNet Authentication Service, page 17
- Adding SonicWALL Secure Remote Access as a Service Provider (SP) in SafeNet Authentication Service. page 18
- Enabling SAML Services in SafeNet Authentication Service, page 21

Synchronizing Users Stores to SafeNet Authentication Service

Before SafeNet Authentication Service (SAS) can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

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

For further details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning an Authenticator in SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users authenticating through SonicWALL Secure Remote Access.

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS tokens
- MP-1 software token
- GrIDsure
- MobilePASS

Authenticators can be assigned to users in two ways:
• **Manual provisioning**—Assign an authenticator to users one at a time.

• **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning” in the *SafeNet Authentication Service - Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.


**Adding SonicWALL Secure Remote Access as a Service Provider (SP) in SafeNet Authentication Service**

Add a service provider entry in the SafeNet Authentication Service (SAS) **SAML Service Providers** module to prepare it to receive SAML authentication requests from SonicWALL Secure Remote Access. You will need the Issuer ID and assertion consumer URL location of SonicWALL Secure Remote Access.

**To add SonicWALL Secure Remote Access as a Service Provider in** SafeNet Authentication Service:

1. Log in to the SafeNet Authentication Service console with an Operator account.

2. Click the **COMMS** tab, and then click **SAML Service Providers**.

![SafeNet Authentication Service console](image-url)
3. In the **SAML Service Providers** module, click the **SAML 2.0 Settings** link.

4. Click **Add**.

5. Under **Add SAML 2.0 Settings**, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Friendly Name</strong></td>
<td>Enter the SonicWALL Secure Remote Access name.</td>
</tr>
<tr>
<td><strong>SAML 2.0 Metadata</strong></td>
<td>Select <strong>Create New Metadata File</strong>.</td>
</tr>
<tr>
<td><strong>Entity ID</strong></td>
<td>Enter the Service Provider Entity ID.</td>
</tr>
<tr>
<td></td>
<td>This value must be same as <strong>Appliance ID</strong> you entered while creating a realm. See “Creating a Realm” on page 10.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Enter the following URL: <strong>https://&lt;Public IP of SonicWALL SRA Appliance&gt;/saml2ssoconsumer</strong></td>
</tr>
</tbody>
</table>
NOTE: The remaining options are used to customize the appearance of the logon page presented to the user. For more information on logon page customization, refer “Configure SAML Service” in the SAML Configuration Guide: http://www2.safenet-inc.com/sas/implementation-guides/sas-on-prem/SAS-QS-SAML.pdf

Under **Return Attributes**, add the following attributes, and then click **Apply**:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/claims/EmailAddress">http://schemas.xmlsoap.org/claims/EmailAddress</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/claims/CommonName">http://schemas.xmlsoap.org/claims/CommonName</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td>principal</td>
<td>According to ThirdParty Product Requirements</td>
</tr>
</tbody>
</table>

SonicWALL Secure Remote Access is added as a service provider in the system.
Enabling SAML Services in SafeNet Authentication Service

After SonicWALL Secure Remote Access has been added to SafeNet Authentication Service (SAS) as a service provider, the users should be granted permission to use this service provider with SAML authentication.

There are two methods to enable the user to use the service provider:

- Manually, one user at a time, using SAML Services module
- Automatically, by defining groups of users, using SAML Provisioning Rules
Using the SAML Services Module

Manually enable a single user to authenticate against one or more configured SAML Service providers.

1. Log in to the SafeNet Authentication Service console with an Operator account.

2. Click the ASSIGNMENT tab, and then search for the required user.

3. Click the appropriate user in the User ID column.
4. Click **SAML Services**.

5. Click **Add**.

6. Under **Add SAML Service**, do the following:
   
e. From the **Service** menu, select the SonicWALL Secure Remote Access service provider.
   
f. In **SAML Login ID** field, select the type of login ID (User ID, E-mail, or Custom) to be sent as a UserID to SonicWALL Secure Remote Access in the response.
   
g. Click **Add**.
The user can now authenticate to SonicWALL Secure Remote Access using SAML authentication.

<table>
<thead>
<tr>
<th>Index</th>
<th>SAML Service</th>
<th>User ID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SonicWALL</td>
<td></td>
<td>Active</td>
</tr>
</tbody>
</table>

**Using SAML Provisioning Rules**

Use this module to enable groups of users to authenticate to SAML service providers.

1. Log in to the SafeNet Authentication Service console with an Operator account.

2. Click the POLICY tab, and then click **Automation Policies**.
3. Click the **SAML Provisioning Rules** link.

4. Click **New Rule**.

5. Configure the following fields, and then click **Add**:

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Enter a name for the rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User is in container</td>
<td>Users affected by this rule must be in the selected container.</td>
</tr>
<tr>
<td>Groups</td>
<td>The <strong>Virtual Server groups</strong> box lists all groups. Click the user groups that will be affected by the rule, and then click the right arrow to move it to the <strong>Used by rule</strong> box.</td>
</tr>
<tr>
<td>Parties</td>
<td>The <strong>Relying Parties</strong> box lists all service providers. Click the service providers that the groups of users will authenticate to, and then click the right arrow to move it to <strong>Rule Parties</strong> box.</td>
</tr>
<tr>
<td>SAML Login ID</td>
<td>Select User ID. This is the User ID that will be returned to the Service Provider in the SAML assertion.</td>
</tr>
</tbody>
</table>
### Add SAML Auto-create Rule

<table>
<thead>
<tr>
<th>Rule Name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User is in container:</td>
<td>Default ▼</td>
</tr>
<tr>
<td>Groups Filter:</td>
<td>Search</td>
</tr>
</tbody>
</table>

**Groups:**
- DA_Group
- DA_Users
- WSAllowAddSlackAccess
- WSAllowComputerAccess
- WSAllowHomePageLinks
- WSAllowShareAccess
- WSManagedGroups
- WSRemoteAccessUsers
- WSRemoteWebAccessUsers

**Virtual Server groups:**

**Used by rule:**

**Parties:**

**Relying Parties**
- SonicWall

**Rule Parties**

**SAML Login ID:**
- User ID □ E-mail □
Running the Solution

The SonicWALL WorkPlace portal is used to verify this integration solution. The WorkPlace portal provides dynamically personalized access to the web-based (HTTP) resources. It also gives users access from their web browsers to files and folders on Windows file servers, and to TCP/IP resources through Secure Mobile Access agents that can be provisioned from WorkPlace.

For this integration, the SafeNet GrIDsure token is configured for authentication with the SAS solution.

NOTE: While running the solution, if any Java or Security warning is shown, click Allow.

1. In a web browser, open the SonicWALL Secure Mobile Access Workspace URL: https://<Appliance public IP>
2. Click Continue to this website.
3. In the Log in to field, select an appropriate realm, and then click Next.

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

4. In User Name field, enter your user name, and then click Login.

5. In the Password field, enter your Personal Identification Pattern (PIP), and then click Login.
If authentication is successful, the user will be allowed access to the resources configured on Workplace.

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

**NOTE:** If you are using SonicWALL for the first time, you will need to install the Secure Endpoint Manager. When you are logged in to WorkPlace, you will get an option to install the Secure Endpoint Manager. For more information, refer to the SonicWALL documentation.
## 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 Gemalto Customer Support. Gemalto 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 Gemalto 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>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto, 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</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></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 Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>