SafeNet Authentication Service
Push OTP Integration Guide

Using RADIUS Protocol 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:** 007-013352-001, Rev. A  
**Release Date:** November 2015
## Contents

Third-Party Software Acknowledgement ........................................................................... 4
Description ............................................................................................................................... 4
Applicability ............................................................................................................................. 4
Environment .............................................................................................................................. 5
Audience ................................................................................................................................. 5
RADIUS-based Authentication using SAS Cloud ............................................................... 5
RADIUS Authentication Flow using SAS ............................................................................... 6
RADIUS Prerequisites ............................................................................................................ 6
Push OTP Prerequisites ......................................................................................................... 7
Configuring SafeNet Authentication Service ...................................................................... 7
  Creating Users Stores in SAS ............................................................................................... 7
  Assigning an Authenticator in SAS ...................................................................................... 7
  Adding SonicWALL Secure Remote Access as an Authentication Node in SAS ............... 8
Checking the SAS RADIUS Server’s IP Address ................................................................. 10
Enabling the Software Token Push OTP Setting ................................................................. 11
Enabling the Allowed Targets Policy .................................................................................... 12
Configuring the On-Premise NPS Server ............................................................................ 14
Configuring SonicWALL Secure Remote Access ................................................................. 17
  Creating an LDAP Authentication Server ......................................................................... 17
  Creating a RADIUS Authentication Server ...................................................................... 20
Creating a Realm ................................................................................................................... 22
Creating a User ...................................................................................................................... 24
Applying Configuration Changes ........................................................................................ 25
Running the Solution ............................................................................................................. 26
Support Contacts .................................................................................................................. 29
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto 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 appliances extend secure remote networking over an SSL VPN to potentially thousands of locations, to provide anytime, anywhere access. The encrypted SSL VPN tunnel protects the transmitted data.

This document describes how to:

- Configure SonicWALL Secure Remote Access to work with SafeNet Authentication Service in RADIUS mode.

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 RADIUS protocol will be used for the purpose of working with the SafeNet Authentication Service Push OTP solution.

The primary objective of the Push OTP solution is to reduce the friction around two-factor authentication, and provide users with an improved two-factor authentication experience.

It is likely that most users already own and always carry a device that can be used as a second factor of authentication. Using the mobile phone as an authenticator replaces the need for a user to carry any additional hardware. So, with Push OTP, a user can:

- Receive authentication requests in real-time via push notifications to his or her smart phone.
- Assess the validity of the request with the information displayed on the screen.
- Respond quickly with a one-tap response to approve or deny the authentication.

Applicability

The information in this document applies to:

- SafeNet Authentication Service (SAS)—SafeNet's cloud-based authentication service
- MobilePASS+ application
Environment

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

- **SafeNet Authentication Service (SAS)**
- **SonicWALL Secure Remote Access**—Version 10.7

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.

RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.

- **Local RADIUS hosted on-premises**—A RADIUS agent that is implemented in the existing customer’s RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.

This document demonstrates the solution using the SAS cloud hosted RADIUS service.

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

For more details on how to install and configure FreeRADIUS, refer to the *SafeNet Authentication Service FreeRADIUS Agent Configuration Guide*. 
RADIUS Authentication Flow using SAS

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

SonicWALL Secure Remote Access does not directly support a cloud RADIUS server. To overcome this, an intermediate on-premises RADIUS server is used (IAS/NPS server in our case), which can connect to both SonicWALL Secure Remote Access and SAS Cloud RADIUS server.

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 using a Push OTP authenticator.
2. SonicWALL Secure Remote Access sends a RADIUS request with the user’s credentials to the on-premises RADIUS server, which in-turn forwards it to SafeNet Authentication Service for validation.
3. SAS identifies the user or mobile device, and detects that the OTP field is empty. Then:
   - SAS will directly trigger a Push OTP authentication request.
   - The user receives a push notification on the configured mobile device to indicate there is a login request pending.
   - The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request (approving will require providing the token’s PIN code).
4. The SAS authentication reply is sent back to SonicWALL Secure Remote Access.
5. The user is granted or denied access to SonicWALL Secure Remote Access based on the OTP value calculation results from SAS.

RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from SonicWALL Secure Remote Access, ensure the following:

- End users can authenticate from the SonicWALL Secure Remote Access environment with a static password before configuring SonicWALL Secure Remote Access to use RADIUS authentication.
- Ports 1812/1813 are open to and from SonicWALL Secure Remote Access.
- 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 RADIUS client for encryption, decryption, and digital signatures.
- On the client machine, set the RADIUS timeout value at least 60 seconds.
Push OTP Prerequisites

In order to use SAS Push OTP you will need:

- SAS configured to enable Push OTP
- MobilePASS which is supported on the following OS platforms:
  - MobilePASS+ (Push OTP support)
    - Android 4.x, 5.x
    - iOS 7+

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with SonicWALL Secure Remote Access using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 7
- Adding SonicWALL Secure Remote Access as an Authentication Node in SAS, page 8
- Checking the SAS RADIUS Server’s IP Address, page 10
- Enabling the Software Token Push OTP Setting, page 10
- Enabling the Allowed Targets Policy, page 12

Creating Users Stores in SAS

Before 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 additional 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 SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through SonicWALL Secure Remote Access.

The following authenticators are supported:
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 Rules” 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 an Authentication Node in SAS**

Add a RADIUS entry in the SAS **Auth Nodes** module to prepare it to receive RADIUS authentication requests from SonicWALL Secure Remote Access. You will need the IP address of SonicWALL Secure Remote Access and the shared secret to be used by both SAS and SonicWALL Secure Remote Access.

1. Log in to the SAS console with an Operator account.

2. Click the **COMMS** tab, and then select **Auth Nodes**.

![Authenticators module in SafeNet Authentication Service](image-url)
3. In the **Auth Nodes** module, click the **Auth Nodes** link.


5. In the **Add Auth Nodes** section, complete the following fields, and then click Save:

   - **Auth Node Name**: Enter a host description.
   - **Resource Name**: Enter a resource name which will identify in a push notification which authentication node it relates to.
   - **Low IP Address In Range**: Enter the IP address of the host or the lowest IP address in a range of addresses that will authenticate with SAS.
   - **Configure FreeRADIUS Synchronization**: Select this option.
   - **Shared Secret**: Enter the shared secret key.
   - **Confirm Shared Secret**: Re-enter the shared secret key.

The authentication node is added to the system.
Checking the SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in SonicWALL Secure Remote Access, check its IP address. The IP address will then be added to SonicWALL Secure Remote Access as a RADIUS server at a later stage.

1. Log in to the SAS console with an Operator account.

2. Click the COMMS tab, and then select Auth Nodes.

3. In the Auth Nodes module, click the Auth Nodes link. The SAS RADIUS server details are displayed.
Enabling the Software Token Push OTP Setting

To use Push OTP authentication, the setting must be enabled in the SAS token policy.

1. Log in to the SAS console with an Operator account.

2. Click the POLICY tab, and then select Token Policies.

3. In the Token Policies module, click the Software Token Push OTP Setting link.

4. Select Enable Push OTP communication with MobilePass+, and then click Apply.
Enabling the Allowed Targets Policy

For Push OTP to be permitted during authentication the user must have a MobilePASS+ token enrolled and this policy must be enabled.

The settings to enable this policy will determine which OS targets are presented to users during the self-enrollment of MobilePASS tokens. You can restrict the targets on which MobilePASS+ or MobilePASS 8 tokens are allowed to be activated or enrolled.

1. Log in to the SAS console with an Operator account.

2. Click the **POLICY** tab, and then select **Token Policies**.
3. In the **Token Policies** module, click the **Allowed Targets Settings** link.

![Token Policies](image)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token Templates</td>
<td>Edit the templates used to customize token operation. Templates are applied during token initialization.</td>
</tr>
<tr>
<td>Token Passcode Processing Policy</td>
<td>Set how the server will evaluate passcodes and support offline authentication.</td>
</tr>
<tr>
<td>Server-side PIN Policy</td>
<td>Set or modify the global server-side PIN policy.</td>
</tr>
<tr>
<td>Global or Groups PIN Change</td>
<td>Trigger a &quot;Global or Groups PIN Change on next use&quot;</td>
</tr>
<tr>
<td>Temporary Password Policy</td>
<td>Set or modify the length, complexity, change frequency, randomness, and lifetime of static passwords.</td>
</tr>
<tr>
<td>Synchronization</td>
<td>Set inner and outer window synchronization parameters.</td>
</tr>
<tr>
<td>SMS/OTP</td>
<td>Set the number of OTPs to be sent in a single SMS message, as well as delivery mode and content.</td>
</tr>
<tr>
<td>Software Token Push OTP Settings</td>
<td>Enable Push OTP communication with MobilePASS.</td>
</tr>
<tr>
<td>Token File Creation Policy</td>
<td>Set the default location for token file creation.</td>
</tr>
<tr>
<td>Allowed Targets Settings</td>
<td>Set the allowed targets to software tokens.</td>
</tr>
<tr>
<td>MobilePASS Devices</td>
<td>Set and format download, installation, and removal messages for SafeNet Authentication Service MP tokens devices.</td>
</tr>
<tr>
<td>Third-Party Application Options</td>
<td>Set authentication options for third-party tokens, such as GridSure and RADIUS.</td>
</tr>
</tbody>
</table>

4. On the **MobilePASS** tab, select the desired targets to allow for each MobilePASS application, and then click **Apply**.

![MobilePASS](image)
Configuring the On-Premise NPS Server

Configure an on-premises NPS server, which will act as a proxy server. The SonicWALL appliance will send the authentication request to this server. This server in turn will forward the request to SAS for authentication.

To configure NPS as a proxy server:

2. From the NPS web console, expand RADIUS Clients and Servers, right-click Remote RADIUS Server Groups, and then click New.

3. On the New Remote RADIUS Server Group window, in the Group name field, enter a name for the group. Then, click Add.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
4. On the **Add RADIUS Server** window, on the **Address** tab, in the **Server** field, enter the IP address of the SAS Cloud RADIUS server.

![Add RADIUS Server dialog box]

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

5. On the **Authentication/Accounting** tab, in the **Shared secret** field, enter a shared secret text. Enter the same secret text in the **Confirm shared secret** field.

![Add RADIUS Server dialog box]

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
6. On the **Load Balancing** tab, in the **Weight** field, enter 100. Then, click **OK**. A new group is added.

![Load Balancing tab screenshot](image_url)

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

7. From the NPS web console, expand **RADIUS Clients and Servers**, right-click **RADIUS Clients** and then click **New**.

![NPS web console screenshot](image_url)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
8. On the **New RADIUS Client** window, complete the following fields and click on **OK**.

<table>
<thead>
<tr>
<th><strong>Enable this RADIUS Client</strong></th>
<th>Select this check box.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Friendly name</strong></td>
<td>Enter a name for the remote client.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Enter the IP address of the remote client (SonicWALL appliance).</td>
</tr>
<tr>
<td><strong>Manual/Generate</strong></td>
<td>Select <strong>Manual</strong>.</td>
</tr>
<tr>
<td><strong>Shared secret</strong></td>
<td>Enter the shared secret for the RADIUS client. This entry must match the shared secret that was used when the RADIUS server was configured in SonicWALL Secure Remote Access.</td>
</tr>
<tr>
<td><strong>Confirm shared secret</strong></td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>

9. Restart the **Network Policy Server**.

---

**Configuring SonicWALL Secure Remote Access**

To configure SonicWALL Secure Remote Access for RADIUS authentication requires:

- Creating an LDAP Authentication Server, page 17
- Creating a RADIUS Authentication Server, page 20
- Creating a Realm, page 22
- Creating a User, page 24
- Applying Configuration Changes, page 25

To perform these configuration settings, log in to the SonicWALL Secure Remote Access appliance with administrator credentials.

**Creating an LDAP Authentication Server**

Create an LDAP authentication server for verifying domain credentials.

1. Open the **SonicWALL Management Console** in web browser (for example, https://<Internal IP address or FQDN of Appliance>:8443).
2. On the login page, enter the credentials, and then click **Login**.

4. In the upper right corner of the window, click the New… link.

5. Under Authentication directory, select LDAP, and then click Continue.
6. 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 LDAP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary LDAP Server</strong></td>
<td>Enter the IP address of the LDAP server.</td>
</tr>
<tr>
<td><strong>Login DN</strong></td>
<td>Enter the login DN of the user with enough privileges. (for example, <strong>CN=Administrator,CN=Users,DC=safenetdemos,DC=com</strong>).</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password of the above user.</td>
</tr>
<tr>
<td><strong>Search base</strong></td>
<td>Enter the search base where it should look for users. (for example, <strong>CN=Users,DC=safenetdemos,DC=com</strong>).</td>
</tr>
</tbody>
</table>

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

Create a RADIUS authentication server for verifying domain credentials.

1. Open the SonicWALL Management Console in a web browser (for example: https://<Internal IP address or FQDN of Appliance>:8443).
2. On the login page, enter the credentials, and then click Login.

4. In the upper right corner of the window, click the New... link.
5. Under **Authentication directory**, select **RADIUS**, and then click **Continue**.

![Authentication directory](image)

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

6. 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 RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary RADIUS Server</strong></td>
<td>Enter the IP address of the NPS server (on-premises RADIUS server) followed by the port number. The format is <code>&lt;IP address&gt;:&lt;port number&gt;</code>. The port number should be either 1812 or 1645.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret value. The shared secret must be same as on the NPS server.</td>
</tr>
<tr>
<td><strong>Connection timeout</strong></td>
<td>Change it to at least 60 sec.</td>
</tr>
</tbody>
</table>

![Configure Authentication Server](image)

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

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

To create a realm:

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, on the **General** tab, complete the following details:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the Realm.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Server</strong></td>
<td>Select the LDAP authentication server created previously.</td>
</tr>
</tbody>
</table>

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

5. Click **Advanced** to expand it, and then complete the following details:

| **Secondary authentication server** | Select the RADIUS server created above. |
| **Usernames must match** | Select this option if the username is same in Active Directory and SAS. |

6. Click **Finish**. 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 your network. After creating users on the SonicWALL Secure Remote Access appliance, you can refer them in an Access Control Rule to permit or deny access to resources.

To create a user:

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>Select realm</th>
<th>Select the realm that was created previously.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User type</td>
<td>Select <strong>User</strong>.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the name of the user. The user name must be same as specified in SAS.</td>
</tr>
<tr>
<td>Display name</td>
<td>Enter the name of the user for display.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of this mapped account.</td>
</tr>
</tbody>
</table>

![Add Mapped Account](image)

*(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.

**To apply configuration changes:**

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.

![SonicWALL Management Console](image)

*(The screen image above is from Dell®. Trademarks are the property of their respective owners.)*
3. On the **Apply Pending Changes** window, click **Apply Changes**.

![Apply Pending Changes](image.png)

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

The changes are applied and a message is displayed.

![Apply Pending Changes](image.png)

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

4. Click **Close**.

### Running the Solution

The user is enrolled with a **MobilePass** token.

1. In a web browser, open the SonicWALL Secure Mobile Access Workspace:
   
   https://<SonicWALL SRA Appliance Public IP>

2. In the **Log in to** field, select the configured realm, and then click **Next**.

![MobilePass Token](image.png)

(The screen image above is from Dell®. Trademarks are the property of their respective owners.)
3. Enter your domain credentials, and then click Login.

4. Now, for RADIUS authentication, enter only your username, and then click Login.

5. An authentication notification is received on the registered mobile device. Tap Approve.
6. Enter the token PIN, and then tap **Continue**.

If the PIN is valid, the token will generate an OTP and will send it automatically.

-Autosend passcode was successful.-
On successful authentication, you will be successfully logged in to WorkPlace.

![SonicWALL | Aventail WorkPlace](image)

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

### 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>
</tbody>
</table>
| **Customer Portal**      | 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.