SafeNet Authentication Manager
Integration Guide
Using SAM as an Identity Provider for PingFederate
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-013150-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>June 2015</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
SAML Authentication using SAM ..................................................................................................................5
Authentication Flow using SAM ..................................................................................................................5
SAML Prerequisites..................................................................................................................................6
Configuring SafeNet Authentication Manager............................................................................................6
  Synchronizing User Stores to SAM .............................................................................................................7
  Assigning Tokens in SAM ............................................................................................................................8
  Configuring SAM as an Identity Provider ...................................................................................................9
  Downloading the SAM Metadata ...............................................................................................................11
  Exporting the PingFederate Metadata .........................................................................................................12
  Configuring SAM for SAML-based User Federation ..............................................................................15
Configuring PingFederate ............................................................................................................................17
Running the Solution ..................................................................................................................................34
Appendix: Deploying PingFederate Quick-Start Applications .......................................................................36
Support Contacts..........................................................................................................................................36
Third-Party Software Acknowledgement

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

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.

PingFederate is a full-featured federation server that provides identity management, web single sign-on, and API security for customers, partners, and employees. Users can securely access the applications they require with a single identity using any device. Supporting all of the current identity standards including SAML, WS-Federation, WS-Trust, OAuth, and OpenID Connect, PingFederate is recognized as a leading federation product today that also future-proofs your business for tomorrow.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in PingFederate using SafeNet tokens managed by SafeNet Authentication Manager.
- Configure SAML authentication in PingFederate using SafeNet Authentication Manager as an identity provider.

It is assumed that the PingFederate environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

In this guide, PingFederate is shown deployed as a service provider (SP). This guide provides instructions specifically for configuring PingFederate quickly to run with accompanying web applications, which demonstrate Internet SSO (also called browser-based SSO). PingFederate provides preconfigured demo applications to test quick-start scenarios for both identity provider (IdP)-initiated SSO and SP-initiated SSO. This guide also helps you to configure SAM as an IdP to access protected pages of SP quick-start applications.

PingFederate 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 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**—Version 8.2 (HF 679)
- **PingFederate**—Version 7.3.0
- **PingFederate Quick-Start Demo Apps**—Version 1.1

Audience

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

SAML Authentication using SAM

SAM provides a SAML authentication option that is already implemented in the SAM environment and can be used without any installation.

![SAML Authentication Diagram](image)

Authentication Flow using SAM

SafeNet Authentication Manager 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 PingFederate.

![Authentication Flow Diagram](image)

1. A user attempts to log on to PingFederate. The user is redirected to SafeNet Authentication Manager (SAM). SAM collects and evaluates the user’s credentials.

2. SAM returns a response to PingFederate, accepting or rejecting the user’s authentication request.
SAML Prerequisites

To enable SafeNet Authentication Manager to receive SAML authentication requests from PingFederate, ensure that the end users can authenticate from the PingFederate environment with a static password.

The PingFederate quick-start demo applications should be deployed and configured. Refer to “Appendix: Deploying PingFederate Quick-Start App,” page 36, for more information.

Configuring SafeNet Authentication Manager

Using SAM as an identity provider for PingFederate requires the following:

- Synchronizing User Stores to SAM, page 7
- Assigning Tokens in SAM, page 8
- Configuring SAM as an Identity Provider, page 9
• Downloading the SAM Metadata, page 11
• Exporting the PingFederate Metadata, page 12
• Configuring SAM for SAML-based User Federation, page 15

Synchronizing User Stores to SAM

SAM manages and maintains token information in its data store, including the token status 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
Assigning Tokens in SAM

SAM supports a number of token methods that can be used as a second authentication factor for users authenticating through PingFederate.

The following tokens are supported:

- eToken PASS
- SafeNet GOLD
- SafeNet eToken 3400
- SafeNet eToken 3500
- eToken NG-OTP
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)

Tokens can be assigned to users as follows:

- **SAM Management Center**—Management site used by SAM administrators and help desk personnel 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’s tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*. 
Configuring SAM as an Identity Provider

To use PingFederate as a service provider and SAM as an identity provider, SAM must be configured as an identity provider.

1. From the Windows Start menu, click Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager.

(See the screen image above for reference. Trademarks are the property of their respective owners.)

2. Click the Action tab, and then select Cloud Configuration.
3. On the **Info for Service Provider** tab, type the web address of the SAM portal server in the **Domain URL** field.

![Image of Cloud Settings window](image.png)

The remaining fields are generated according to the Domain URL that was entered.

4. Click **OK**.
Downloading the SAM Metadata

The SAM metadata is shared between SAM and PingFederate.

1. From the Windows **Start** menu, click **Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager**.

   ![Screen Image](image1.png)

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

2. Click the **Action** tab, and then select **Cloud Configuration**.

   ![Screen Image](image2.png)
3. On the **Info for Service Provider** tab, click **Download Metadata** and save the metadata file. This metadata file will be imported into PingFederate later.

![Cloud Settings](image)

**Exporting the PingFederate Metadata**

1. Open the PingFederate administrative console using the following URL:
   
   https://<DNS_NAME or IP Address of PingFederate Server>:9999/pingfederate/app

   where DNS_NAME is a fully-qualified name of the machine running the PingFederate server.

2. Under **ADMINISTRATIVE FUNCTIONS**, click **Metadata Export**.

![PingFederate Configuration](image)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
3. On the **Metadata Role** tab, select **I am the Service Provider (SP)**, and then click **Next**.

![Metadata Role tab](image)

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

4. On the **Metadata Mode** tab, select **Use a connection for metadata generation**, and then click **Next**.

![Metadata Mode tab](image)

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

5. On the **Connection Metadata** tab, perform the following steps:
   
   a. Select the connection (for example, **SAM**) for which you want to create metadata. You will create a connection in “Configuring PingFederate” on page 17. On selecting the connection, the remaining fields are automatically populated.

   b. Click **Next**.

   ![Connection Metadata tab](image)

   *(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
6. On the Metadata Signing tab, in the Signing Certificate field, select a certificate, and then click Next.

7. Click Export, and then save the PingFederate metadata file.

8. Click Done.
Configuring SAM for SAML-based User Federation

SAM's Token Policy Object (TPO) policies include application authentication settings for SAML service providers. These settings are used by SAM's portal to communicate with service providers.

For general portal configuration, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

To edit the Token Policy Object for SAM’s portal configuration:

1. Open the Token Policy Object Editor for the appropriate group. See the SafeNet Authentication Manager 8.2 Administrator’s Guide for more information.
2. In the left pane, click Protected Application Settings > User Authentication.
3. In the right pane, double-click Application Authentication Settings.
4. On the Application Authentication Settings Properties window, perform the following steps:
   a. Select Define this policy setting.
   b. Select Enabled.
   c. Click Definitions.
5. On the Application Authentication Settings window, right-click Application Authentication Settings, and then select Create a profile from metadata.

![Application Authentication Settings window](image)

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

6. Browse and select the PingFederate metadata you exported (see “Exporting the PingFederate Metadata” on page 12).

7. In the left pane, right-click the new profile, and then rename it to a user-friendly name (for example, PF).

8. In the left pane, click the new profile.

9. In the right pane, double-click on the following policies, and then enter the appropriate information:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Issuer</td>
<td>Enter the Entity ID of PingFederate (for example, PF-DEMO).</td>
</tr>
<tr>
<td>SAM issuer</td>
<td>Enter a unique SAM ID to be identified in SAML authentication. This entity ID should match the entity ID of the SAM metadata file.</td>
</tr>
<tr>
<td>Application’s login URL</td>
<td>Enter the PingFederate Consumer Assertion URL. The format of the URL is https://&lt;PingFederate Server IP&gt;:9031/sp/ACS.saml2.</td>
</tr>
<tr>
<td>Audience URI</td>
<td>Enter the PingFederate entity ID. It should match the entity ID in the Application Issuer field.</td>
</tr>
<tr>
<td>User mapping</td>
<td>Select AccountName.</td>
</tr>
</tbody>
</table>
10. Enable the appropriate authentication methods for your organization. See the *SafeNet Authentication Manager Version 8.2 Administrator’s Guide* for detailed information about authentication methods.

The following is an example of the completed policy settings in the **Application Authentication Settings** window:

![Application Authentication Settings](image1.png)

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

11. Click **OK** until all of the **Token Policy Object Editor** windows are closed.

### Configuring PingFederate

Add SafeNet Authentication Manager as an identity provider in PingFederate.

1. Log in to the PingFederate administrative console as an administrator using the following URL:
   
   `https://<DNS_NAME_or_IP_of_PingFederate_Server>:9999/pingfederate/app`
   
   where DNS_NAME is a fully-qualified name of the machine running the PingFederate server.

2. Under **IDP CONNECTIONS**, click **Create New**.

![PingFederate Interface](image2.png)

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
3. On the **Connection Type** tab, select **Browser SSO Profiles**, and then click **Next**.

4. On the **Connection Options** tab, ensure that **Browser SSO** is selected, and then click **Next**.

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

On the **Import Metadata** tab, click **Browse**, select the SAM metadata you downloaded in “
5. Downloading the SAM Metadata on page 11, and then click **Next**.

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
6. On the **Metadata Summary** tab, click **Next**.

![Metadata Summary Tab](image)

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

7. On the **General Info** tab, the **Partner's Entity ID**, **Connection Name**, and **Base URL** fields are populated from the metadata file. You can change **Connection Name**, as this is an identifier for this connection. Click **Next**.

![General Info Tab](image)

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

8. On the **Browser SSO** tab, click **Configure Browser SSO**.

![Browser SSO Tab](image)

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
9. On the SAML Profiles tab, select SP-Initiated SSO and SP-Initiated SLO (enabled after selecting SSO profiles), and then click Next.

10. On the User-Session Creation tab, click Configure User-Session Creation.

11. On the Identity Mapping tab, select the Account Mapping option, and then click Next.
12. On the **Attribute Contract** tab, a set of user attributes is displayed that the IdP will send in the assertion. Click **Next**.

![Attribute Contract tab](image)

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

13. On the **Target Session Mapping** tab, map an adapter instance for each target application on your system. Click **Map New Adapter Instance**.

![Target Session Mapping tab](image)

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

14. On the **Adapter Instance** tab, in the **ADAPTER INSTANCE** field, select **SP Adapter**, and then click **Next**.

![Adapter Instance tab](image)

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
15. On the **Adapter Data Store** tab, select the **Use only the attribute available in the SSO Assertion** option, and then click **Next**.

   ![Adapter Data Store Tab](image1.png)

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

16. On the **Adapter Contract Fulfillment** tab, for each of the attributes, complete the following steps, and then click **Next**.
   
   a. In the **SOURCE** column, select **Assertion**.
   
   b. In the **VALUE** column, select **SAML_SUBJECT**.

   ![Adapter Contract Fulfillment Tab](image2.png)

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

17. On the **Issuance Criteria** tab, click **Next**.

   ![Issuance Criteria Tab](image3.png)

   *(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
18. On the **Summary** tab, click **Done**. You are returned to the **Target Session Mapping** tab.

![Target Session Mapping Tab](Image)

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

19. On the **Target Session Mapping** tab, click **Next**.

![Target Session Mapping Tab](Image)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
20. On the **Summary** tab, review the configured session settings, and then click **Done**. You are returned to the **User-Session Creation** tab.

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

21. On the **User-Session Creation** tab, click **Next**.

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

![Configure Protocol Settings]

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

23. On the SSO Service URLs tab, perform the following steps, and then click Next:
   a. In the BINDING column, select POST.
   c. In the ACTION column, click Add.

![SSO Service URLs]

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

24. On the SLO Service URLs tab, perform the following steps, and then click Next:
   a. In the BINDING column, select POST.
   c. In the RESPONSE URL column, do not enter anything.
   d. In the ACTION column, click Add.

![SLO Service URLs]

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
25. On the **Allowable SAML Bindings** tab, select **POST**, and then click **Next**.

![Image of Allowable SAML Bindings tab](image)

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

26. On the **Default Target URL** tab, in the **Default Target URL** field, enter `https://<PingFederate IP Address>:9031/quickstart-app-sp/go`, and then click **Next**.

![Image of Default Target URL tab](image)

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

27. On the **Signature Policy** tab, select **Use SAML-standard signature requirements**, and then click **Next**.

![Image of Signature Policy tab](image)

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
28. On the **Encryption Policy** tab, select **None**, and then click **Next**.

29. On the **Summary** tab, click **Done**. You are returned to the **Protocol Settings** tab.

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
30. On the **Protocol Settings** tab, click **Next**.

![Protocol Settings](image1.png)

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

31. On the **Summary** tab, click **Done**. You are returned to the **Browser SSO** tab.

![Summary](image2.png)

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

32. On the **Browser SSO** tab, click **Next**.

![Browser SSO](image3.png)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
33. On the **Credentials** tab, click **Configure Credentials**.

![Configure Credentials](image)

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

34. On the **Digital Signature Settings** tab, define the private key/certificate that will be used to sign assertions and SLO messages for this SP. Perform the following steps, and then click **Next**:

a. In the **Signing Certificate** field, select your PingFederate server’s signing certificates that you will use to sign SAML requests, responses, and assertions.

b. In the **Signing Algorithm** field, select **RSA SHA256**.

![Digital Signature Settings](image)

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

35. On the **Signature Verification Settings** tab, click **Manage Signature Verification Settings**.

![Signature Verification Settings](image)

*The screen image above is from PingFederate®. Trademarks are the property of their respective owners.*
36. On the Trust Model tab, select Unanchored, and then click Next.

![Trust Model Tab](image)

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

37. On the Signature Verification Certificate tab, in the Primary field, select the partner certificate, and then click Next.

![Signature Verification Certificate Tab](image)

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

38. On the Summary tab, click Done. You are returned to the Signature Verification Settings tab.

![Summary Tab](image)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
39. On the **Signature Verification Settings** tab, click **Next**.

![Signature Verification Settings tab](image)

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

40. On the **Summary** tab, review the credentials configurations, and then click **Done**. You are returned to the **Credentials** tab.

![Summary tab](image)

*(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)*
41. On the **Credentials** tab, click **Next**.

![Credentials tab screenshot](image1.png)

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

42. On the **Activation & Summary** tab, in the **Connection Status** field, select **Active**, and then click **Save**.

![Activation & Summary tab screenshot](image2.png)

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

In the PingFederate quick-start demo application, the service provider quick-start application provides a service provider web page to access the SP-initiated SSO. Ensure that you have deployed the quick-start components and started the PingFederate server.

For this integration, the SafeNet MP token is configured for authentication with the SAM solution.

1. Open the following URL in a web browser: 
   https://<DNS_NAME or IP>:9031/quickstart-app-sp/go
   where DNS_NAME or IP is the fully-qualified name or IP address of the machine running the PingFederate server.

2. In the IdP Partner field, select the identity provider that you have already configured (for example, SAM), and then click Single Sign-On.

   "My Service Provider Quick-Start Application"

   Welcome! This Service Provider (SP) provides single-sign-on access to local resources via a remote Identity Provider (IdP). The button below takes you to the IdP login page or the SP target-resource page depending on your authentication status at the IdP.

   IdP Partner: SAM
   Single Sign-On

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

3. You are redirected to the SAM Login page. In the Username field, enter your user name, and then click OK. The OTP Authentication page is displayed.

   "User Identification"

   Enter your username, select the computer's security level, and click 'OK.'
4. Generate an OTP using the SafeNet token.

5. In the **OTP Authentication Code** field, enter the generated OTP, and then click **OK**.

After successful authentication, you are logged in. The page that displays represents the protected "target" resource of the SSO transaction.

(The screen image above is from PingFederate®. Trademarks are the property of their respective owners.)
Appendix: Deploying PingFederate Quick-Start Applications

This section describes how to deploy the PingFederate quick-start components. After installing PingFederate, configure the PingFederate server and deploy the demo applications.

1. Download the PingFederate Quick-Start Demo application from:
2. If you have not already done so, install the PingFederate server.
3. From the quick-start distribution directory, copy the following files into the
   `<pf_install_dir>/pingfederate/server/default/deploy` directory in your PingFederate installation:
   - quickstart-app-idp.war
   - quickstart-app-sp.war
   - json-simple-1.1.jar
   - pf-referenceid-adapter-1.0.jar
4. From the quick-start distribution directory, copy the `data.zip` file into:
   `<pf_install_dir>/pingfederate/server/default/data/drop-in-deployer`
5. Stop and restart the PingFederate server if it is running.

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>
<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</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</td>
</tr>
<tr>
<td></td>
<td>manage incidents, get the latest software upgrades, and access the SafeNet Knowledge</td>
</tr>
<tr>
<td></td>
<td>Base.</td>
</tr>
</tbody>
</table>