SafeNet Authentication Service
Integration Guide

Using SAS as an Identity Provider for Better MDM
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012923-001, Rev. B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>November 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>
<tr>
<td>Contents</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>Better MDM Authentication Flow using SAS-SPE and SAS-PCE</td>
<td>5</td>
</tr>
<tr>
<td>Better MDM Authentication Flow using SAS</td>
<td>6</td>
</tr>
<tr>
<td>Configuring SafeNet Authenticator Service SAML</td>
<td>6</td>
</tr>
<tr>
<td>Configuring SAS as an Identity Provider for Better MDM</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>11</td>
</tr>
<tr>
<td>Synchronizing Users Stores to SAS</td>
<td>11</td>
</tr>
<tr>
<td>Authenticator Assignment in SAS</td>
<td>11</td>
</tr>
<tr>
<td>Enabling SAML User Authentication in SAS</td>
<td>12</td>
</tr>
<tr>
<td>Associating SAS Users with the SAML Service Provider</td>
<td>14</td>
</tr>
<tr>
<td>Configuring a Secured Application with Better MDM</td>
<td>14</td>
</tr>
<tr>
<td>Adding a Mobile Device to the Devices List</td>
<td>14</td>
</tr>
<tr>
<td>Creating a New Application Policy</td>
<td>17</td>
</tr>
<tr>
<td>Adding and Deploying a Secured Application</td>
<td>21</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>26</td>
</tr>
<tr>
<td>SAML Login to the Better MDM Management Console</td>
<td>26</td>
</tr>
<tr>
<td>SAML Login to a Secured Application with Better MDM</td>
<td>28</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>30</td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

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

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.

Better MDM offers an all-in-one mobile security platform that seamlessly integrates with any existing mobility solution. Better MDM provides enterprises with complete endpoint visibility, security, and control, with real-time, self-protecting advanced mobile threat detection and prevention. With Better MDM, CSOs and security administrators gain mobile application visibility and risk-based intelligence, and can add security controls to any app outside of a secured container to satisfy any existing security infrastructure requirements. Better MDM does this quickly and automatically without any coding or wrapping.

This document describes how to:


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

Better MDM can be configured to support multi-factor authentication in several modes. 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 – Service Provider Edition (SAS-SPE)**—A server version used by Service Providers to deploy instances of SafeNet Authentication Service.
Environment

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

- **SafeNet Authentication Service**—SafeNet’s on-premises authentication service
- **Better MDM**

Audience

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

BETTER MDM Authentication Flow using SAS-SPE and SAS-PCE

SafeNet Authentication Service 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 AD FS infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for AD FS.

For more information on how to install and configure the SafeNet Authentication Service Agent for AD FS, refer to the SafeNet Support Portal.
Better MDM Authentication Flow using SAS

SafeNet Authentication Service communicates with a large number of Service Providers and cloud-based service solutions using the SafeNet AD FS agent.

The image below describes the dataflow of a multi-factor authentication transaction for Better MDM (exchange server).

1. A user attempts to log on to Better MDM using an OTP authenticator.
2. Better MDM sends a SAML request with the user’s credentials to SafeNet Authentication Service for validation.
3. The SAS authentication reply is sent back to the Better MDM.
4. The user is granted or denied access to the Better MDM based on the OTP value calculation results from SAS.

Configuring SafeNet Authentication Service SAML

The SAS Management Console settings are used to establish SafeNet Authentication Service (SAS) as the Identity Provider for Better MDM.

To configure SAS SAML:

1. On the SAS Management Console, click VIRTUAL SERVER > COMMS.

2. Click SAML Service Providers > SAML 2.0 Settings. The SAML 2.0 Settings are displayed, as shown in the example below.
3. A SAS Identity Provider certificate should be downloaded locally, as it will be needed in the section “Configuring SAS as an Identity Provider for Better MDM” below.

### Configuring SAS as an Identity Provider for Better MDM

In order to configure SAS as an Identity Provider for Better MDM, a new SAS realm must be added through the Better MDM Management Console. Thereafter, it is added to the login page automatically.

**To configure SAS as an Identity Provider for Better MDM:**

1. Log in to the Better MDM Management Console.

(The screen image above is from Better MDM. Trademarks are the property of their respective owners.)
2. Click the **ENTERPRISE INTEGRATIONS** tab.

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

The **Enterprise Connectors** list is displayed.

(The screen image above is from Better MDM. Trademarks are the property of their respective owners.)
3. From the **Enterprise Connectors** list:
   a. Set SafeNet’s **IAM/SSO** connector to **ON** by clicking the **ON/OFF** button to the right of the **SafeNet** icon.
   b. Click the **+ Add New Realm** below the **SafeNet** icon to add a new realm. The **New Realm** window is displayed.

   ![Enterprise Connectors](image)

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

4. Complete the fields on the **New Realm** window as follows, and then click **Save**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly Name</td>
<td>Enter a new realm name (for example, SafeNetDemos).</td>
</tr>
<tr>
<td>Identity Provider SSO URL</td>
<td>Enter the SAS Idp Redirect login URL (for example, <a href="https://SAS.SafeNetDemos.com/idp/profile/SAML2/Redirect/SSO">https://SAS.SafeNetDemos.com/idp/profile/SAML2/Redirect/SSO</a>).</td>
</tr>
<tr>
<td>Identity Provider Logout URL</td>
<td>Enter the SAS Idp logout URL (for example, <a href="https://SAS.SafeNetDemos.com/idp/signout.jsp">https://SAS.SafeNetDemos.com/idp/signout.jsp</a>).</td>
</tr>
<tr>
<td>Upload Certificate</td>
<td>Click <strong>Browse</strong> and then upload the SAS Idp certificate (which can be downloaded from the SAS console).</td>
</tr>
</tbody>
</table>
5. Click **Close** to close the **New Realm** window. The realm is added below the **SafeNet** icon, and SAS is now configured as an Identity Provider for Better MDM.
Configuring SafeNet Authentication Service

To deploy multi-factor authentication using SAS with Better MDM using SAML authentication, do the following:

- Synchronizing Users Stores to SAS
- Authenticator Assignment in SAS

Synchronizing Users Stores to SAS

Before SAS can authenticate any user in your organization, you must create a user store in SAS that contains the users requiring the use of 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.

Authenticator Assignment in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users authenticating through Better MDM.

The following authenticators are supported:

- eToken PASS
- SMS tokens
- MP-1
- GrIDsure
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning** – Assign an authenticator to users one by one.
- **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 the “Provisioning Rules” section of the SafeNet Authentication Service - Subscriber Account Operator Guide to learn how to provision the different authentication methods to users in the SafeNet Authentication Service user store.


Enabling SAML User Authentication in SAS

An organization’s user accounts must be configured to authenticate to Better MDM using SafeNet Authentication Service.

6. On the SafeNet Authentication Service Management Console, click VIRTUAL SERVER > COMMS.

7. Click SAML Service Providers > SAML 2.0 Settings. The SAML 2.0 Settings are displayed, as shown in the example below.

8. Click Add.
9. On the **Add SAML 2.0 Settings** window, complete the following fields:

10. In the **Friendly Name** field, enter a name for the Better MDM service provider (for example, BetterMDM).

11. In the **SAML 2.0 Metadata** field, select **Create New Metadata File**.

<table>
<thead>
<tr>
<th>Entity ID</th>
<th>Enter the Better Id shown in the Better MDM Management Console (<a href="https://sfnt.bettermdm.com">https://sfnt.bettermdm.com</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Enter the Better Assertion URL shown in the Better MDM Management Console (<a href="https://sfnt.bettermdm.com/init/saml_response">https://sfnt.bettermdm.com/init/saml_response</a>).</td>
</tr>
</tbody>
</table>

12. Click **Apply**. Better MDM is now added as a SAML service provider.
Associating SAS Users with the SAML Service Provider

Users in the SAS user store must be associated with the appropriate SAML service provider (the SAML login ID for Better MDM should be user’s email address). This is done by using a pre-defined SAML provisioning rule that will automatically associate a group (or groups) of users to the specific SAML Service Provider. For more information on using SAML provisioning rules, see the SafeNet Authentication Service Administration Guide at http://www2.safenet-inc.com/sas/implementation-guides.html.

NOTE: This process is common for all SAML Service Providers. Readers that have already configured a different SAML Service Provider may need to repeat the process, making sure that the users are associated with multiple SAML Service Providers.

Configuring a Secured Application with BETTER MDM

In order to configure a secured application with Better MDM and authenticate to it using SAS SAML, the following needs to be executed:

- Adding a Mobile Device to the Devices List, on page 14
- Creating a New Application Policy, on page 17
- Adding and Deploying a Secured Application, on page 21

Adding a Mobile Device to the Devices List

To add a mobile device to the Devices list:

1. Log in to the Better MDM Management Console.

2. Click the Devices tab.

(The screen image above is from Better MDM. Trademarks are the property of their respective owners.)
3. On the **Devices** window, click **+Add** to add a mobile device.

4. On the **Register Device** window, enter the following information, and then click **Register Device**:
Platform | Select the Android/IOS according to the preferred device.
---|---
Email | Enter the requested user’s email.
Authentication | Select Basic.
Single Token Use | Leave the option set to OFF.

![Register Device](image)

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

5. IOS and Android devices must be registered before the device is registered in Better MDM’s Management Console (follow the email instructions sent to the device):

- **Android device** – The Better MDM application must be installed and logged in.
- **IOS device** – A secured profile must be added (no application is required to be installed).

The device was added to the **Devices** list.
Creating a New Application Policy

To create a new application policy:

1. Log in to the Better MDM Management Console.
2. Click the **POLICIES & PROFILES** tab.

![Image](image1.png)

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

3. Click the **Application Policy** tab.

![Image](image2.png)

*(The screen image above is from Better MDM. Trademarks are the property of their respective owners.)*
4. Click **Add Application Policy**.

![Image of Better MDM interface](image.png)

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

5. On the **Add Policy** window complete the following fields, and then click **Add**:

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>App Authentication</strong></td>
<td>Set this option to <strong>ON</strong>.</td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
<td>Select <strong>SafeNet Authentication Manager</strong>.</td>
</tr>
<tr>
<td><strong>In Browser</strong></td>
<td>Leave this option set to <strong>OFF</strong>.</td>
</tr>
</tbody>
</table>
(The screen image above is from Better MDM. Trademarks are the property of their respective owners.)
The application policy is now added.

![App Policy Screen](image)

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

Adding and Deploying a Secured Application

1. Log in to the Better MDM Management Console.

![Login Screen](image)

(The screen image above is from Better MDM. Trademarks are the property of their respective owners.)
2. Click the **APPS** tab.

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

3. Click **Add** to add an application.

(The screen image above is from Better MDM. Trademarks are the property of their respective owners.)
4. On the **Add Application** window, perform the following steps, and then click **Add**:
   c. In the left pane, select the relevant operating system and then search for the desired app (for example, Salesforce).
   d. Click the + button next to the app to add it to the **Selected Apps** list (you may add as many applications, from different operating systems, as you want).
   e. Under **App Settings**, click the ON/OFF button to turn on the **Secure (In-House Apps Only)** feature.
   f. Under **Policy Settings**, in the **Policies** field, select the policy that was created in the Creating a New Application Policy section, and then select the group of users that the policy will apply to (leave this field set to **Default** to apply to all users).

(The screen image above is from Better MDM. Trademarks are the property of their respective owners.)
5. Verify that the requested application has been added to the **Enterprise App Store**. Wait a few minutes until the application is wrapped by Better MDM (time may vary according to the size of the application).

(The screen image above is from Better MDM. Trademarks are the property of their respective owners.)
6. After the application is ready (wrapped), select the preferred way in which to publish it to the mobile device.
   a. Click the **Action** button and select either **Push** or **Download**.

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

   b. Click the **Distribute** tab, and then click **Email** or **SMS** under **Send Via**.

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

Your application is now published to your mobile device, and is secured by Better MDM and SAS SAML authentication.
Running the Solution

SAS SAML authentication is available in the following Better MDM solutions:

- SAML Login to the Better MDM Management Console, on page 26.


SAML Login to the Better MDM Management Console

1. Bob tries to log in to the Better MDM Management Console by browsing to his unique organizational URL (for example, sfnt.bettermdm.com).

2. In order to use SAS SAML login, Bob chooses to log in with his organization’s SafeNet login link.

3. The browser redirects Bob to the SAS SAML login page. Bob must use his SAS token to authenticate.
4. After authenticating successfully, Bob is redirected to the Better MDM Management Console.

(The screen image above is from Better MDM. Trademarks are the property of their respective owners.)
SAML Login to a Secured Application with Better MDM

Before starting, make sure the secured application (configured in the section Configuring a Secured Application with BETTER MDM, on page 14) appears on your device screen (including the small Better MDM lock icon).

1. Bob wants to launch the Salesforce Classic application, which is secured by Better MDM.

2. Bob taps the app to launch it. He is redirected to a browser.

3. On the SAS SAML login page, Bob is prompted to enter his token credentials.
4. After authenticating successfully, the requested app is launched.

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