SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for MobileIron
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:** 007-013073-001, Rev. B

**Release Date:** June 2016
Contents

Third-Party Software Acknowledgement ................................................................. 4
Description .................................................................................................................. 4
Applicability .............................................................................................................. 4
Environment .............................................................................................................. 4
Audience .................................................................................................................... 5
SAML Authentication using SafeNet Authentication Service Cloud ................................ 5
SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE5
SAML Authentication Flow using SafeNet Authentication Service ..................................... 6
SAML Prerequisites .................................................................................................... 6
Configuring MobileIron ............................................................................................... 6
    Configuring the BYOD Portal .................................................................................. 7
    Downloading the SAS Metadata ........................................................................... 8
    Downloading the SafeNet Identity Provider Certificate ........................................... 8
Configuring SafeNet Authentication Service ............................................................... 9
    Synchronizing Users Stores to SafeNet Authentication Service ............................... 9
    Assigning an Authenticator in SafeNet Authentication Service .............................. 9
    Adding MobileIron as a Service Provider (SP) in SafeNet Authentication Service .... 10
    Enabling SAML Services in SafeNet Authentication Service .................................... 14
Running the Solution ................................................................................................ 19
Support Contacts ....................................................................................................... 28
Third-Party Software Acknowledgement

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

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.

MobileIron BYOD Portal is a SaaS-based solution that can enhance and extend an organization’s existing mobile device management (MDM) investment. With the MobileIron BYOD Portal, administrators can create a custom, self-service device management experience, which allows end users to easily register and manage their corporate-connected devices.

This document describes how to:

- Configure SAML authentication in MobileIron using SafeNet Authentication Service as an identity provider.

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

MobileIron 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
- **MobileIron Core Admin Portal**—Core 7.5.1.0, Build 37
- **MobileIron BYOD Portal**—Version 2014.12.22C
- iOS Device—iPhone 4S
- iOS Version—Version 8.1.3

**Audience**

This document is targeted to system administrators who are familiar with MobileIron, 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 MobileIron.

1. A user attempts to log on to MobileIron. The user is redirected to SafeNet Authentication Service. SAS collects and evaluates the user's credentials.
2. SAS returns a response to MobileIron, accepting or rejecting the user's authentication request.

SAML Prerequisites

To enable SafeNet Authentication Service to receive SAML authentication requests from MobileIron, ensure the following:

1. The end users can authenticate through the MobileIron environment with a static password.
2. The MobileIron BYOD Portal and MobileIron core appliance should be configured, and end user mobile device registration should be working with a static password.
3. The MobileIron Core-connected cloud should be configured with the appropriate policy for iOS device users to push the Mobile@Work app onto iOS devices after successful device registration using the BYOD portal.

Configuring MobileIron

To add SafeNet Authentication Service (SAS) as an Identity Provider in MobileIron:

- Configuring the BYOD Portal, page 7
- Downloading the SAS Metadata, page 8
- Downloading the SafeNet Identity Provider Certificate, page 8
Configuring the BYOD Portal

1. Log in to the MobileIron BYOD portal configured for SafeNet (https://safenet.byodportal.com/admin) as an admin user. The **BYOD Portal** window is displayed.

   ![BYOD Portal Window](image)

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

2. Click **SAML Settings / SSO** tab in the left pane.

3. On the **SAML Settings / SSO** window, complete the following fields, and then click **Save Your Changes**.

<table>
<thead>
<tr>
<th>Enable SAML SSO</th>
<th>Select On.</th>
</tr>
</thead>
</table>
   | SSO iDP URL     | Enter the SAML identity provider URL. For example:  
   |                 | https://idp1.cryptocard.com/idp/profile/SAML2/Redirect/SSO |
   | x.509 Certificate| Copy the iDP certificate and paste it in this window. Make sure you include the BEGIN CERTIFICATE and END CERTIFICATE tags. |
   | Logout URL      | Enter the URL to redirect the user to after logging out of the application. For example:  
   |                 | https://idp1.cryptocard.com/idp/signout.jsp |
Downloading the SAS Metadata

1. Browse to the https://idp1.cryptocard.com/idp/shibboleth URL.
2. The SAS metadata will automatically download. Save it locally on your machine.

Downloading the SafeNet Identity Provider Certificate

1. Browse to the https://cloud.safenet-inc.com/console/cert/idp.crt URL.
2. The SafeNet IDP Certificate will automatically download. Save it locally on your machine.
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with MobileIron using SAML authentication requires:

- Synchronizing Users Stores to SafeNet Authentication Service, page 9
- Assigning an Authenticator in SafeNet Authentication Service, page 9
- Adding MobileIron as a Service Provider (SP) in SafeNet Authentication Service, page 10
- Enabling SAML Services in SafeNet Authentication Service, page 14

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 MobileIron.

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 MobileIron 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 MobileIron. You will need the Issuer ID and assertion consumer URL location of MobileIron.

**To add MobileIron 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.

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>Friendly Name</th>
<th>Enter the MobileIron name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML 2.0 Metadata</td>
<td>Select Create New Metadata File.</td>
</tr>
<tr>
<td>Entity ID</td>
<td>Enter the service provider IssuerID/EntityID. For example: byodportal-sso</td>
</tr>
<tr>
<td>Location</td>
<td>Enter the Assertion Consumer URL. For example: <a href="https://www.byodportal.com/byodapp/manage/saml_consume.php?target=STZ_I0DsrSIUBMVe9z_K9g">https://www.byodportal.com/byodapp/manage/saml_consume.php?target=STZ_I0DsrSIUBMVe9z_K9g</a></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-QSSAML.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>
</tbody>
</table>
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname  According to ThirdParty Product Requirements

http://schemas.xmlsoap.org/claims/CommonName  According to ThirdParty Product Requirements

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier  According to ThirdParty Product Requirements

principal  According to ThirdParty Product Requirements

---

**Return Attributes**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://schemas.microsoft.com/ws/2006/04/identity/claims/uid">http://schemas.microsoft.com/ws/2006/04/identity/claims/uid</a></td>
<td>UID</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/windowsaccountname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/windowsaccountname</a></td>
<td>SAML Login ID</td>
</tr>
<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>Email address</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/samaccountname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/samaccountname</a></td>
<td>Name</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/commonname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/commonname</a></td>
<td>Given name</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/username">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/username</a></td>
<td>Name</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>Custom...</td>
</tr>
</tbody>
</table>

**Add attribute**

---

MobileIron is added as a service provider in the system.
Enabling SAML Services in SafeNet Authentication Service

After MobileIron 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:
   a. From the Service menu, select the MobileIron service provider.
   b. In SAML Login ID field, select the type of login ID (User ID, E-mail, or Custom) to be sent as a UserID to MobileIron in the response.
   c. Click Add.
The user can now authenticate to MobileIron using SAML authentication.

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>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rule Name</strong></td>
<td>Enter a name for the rule.</td>
</tr>
<tr>
<td><strong>User is in container</strong></td>
<td>Select a container from the menu. Users affected by this rule must be in the selected container.</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td>The <strong>Virtual Server groups</strong> window lists all groups. Click the user group(s) that will be affected by the rule, and then click the right arrow to move the group(s) to the <strong>Used by rule</strong> window.</td>
</tr>
<tr>
<td><strong>Parties</strong></td>
<td>The <strong>Relying Parties</strong> window lists all service providers. Click the service provider(s) that the group(s) of users will authenticate to, and then click the right arrow to move the service provider(s) to <strong>Rule Parties</strong> window.</td>
</tr>
<tr>
<td><strong>SAML Login ID</strong></td>
<td>Select <strong>User ID</strong>. The User ID will be returned to the service provider in the SAML assertion.</td>
</tr>
</tbody>
</table>
Running the Solution

Check the configured solution after successfully configuring the MobileIron for SAML authentication.

In this solution, the user will register her personally owned iOS device using the BYOD portal. After successful device registration, the Mobile@Work app will be pushed onto the registered device, according to the policy defined by the administrator for iOS devices on MobileIron Core.

The user is enrolled with a GrIDsure token.

1. Open the web browser and enter the user device registration URL (https://safenet.byodportal.com/reg) on the iOS device to register her personal device.

1. The user is redirected to the SAS Login page. Enter the username in User Name field, and then click Login.
2. The challenge grid is displayed. In the **Password** field, enter the characters from the grid that correspond to your PIP (personal identification pattern), and then click **Login**.

3. After successful authentication, tap the blue box to register the device.

*(The screen image above is from MobileIron®. Trademarks are the property of their respective owners.)*
4. Select **My Device**, select **I Agree to the Terms**, and then tap **Let’s Register**.

5. On the **Profile Service** screen, tap **Install** to enter the device into the SafeNet encrypted profile service.
6. Enter the iOS device passcode (if configured).

7. Tap Install.

(The screen image above is from MobileIron®. Trademarks are the property of their respective owners.)
Following two screens will be displayed during the profile installation.

8. Tap Install.

*MOBILE DEVICE MANAGEMENT*

Installing this profile will allow the administrator at “https://m.mobileiron.net/safenet/c/i/mdm/mdm.html?c=1073741846” to remotely manage your iPhone.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPhone.

*(The screen image above is from MobileIron®. Trademarks are the property of their respective owners.)*
9. Tap **Trust**.

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

10. Tap **Done**.

(The screen image above is from MobileIron®. Trademarks are the property of their respective owners.)
The device is now registered with the SafeNet MobileIron server.

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

11. The configured policy for the iOS device on the SafeNet MobileIron server is ready to push the app onto the device. Tap **Install** to install the MobileIron app.

(The screen image above is from MobileIron®. Trademarks are the property of their respective owners.)
12. When the MobileIron app is installed on device, the **MobileIron** icon is displayed. Tap the **MobileIron** icon to open the app.

![MobileIron icon on iPhone screen](image1.png)

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

When the app opens for the first time, it will verify the device and user associated with it.

![MobileIron verifying screen](image2.png)

*(The screen image above is from MobileIron®. Trademarks are the property of their respective owners.)*
13. Tap Allow.

![Connection established](image)

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

14. A connection is established with SafeNet’s MobileIron server. Tap the > arrow to view the connection status.

![Connection status](image)

(The screen images above are from MobileIron®. 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>
<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>