SafeNet Authentication Service
Integration Guide

Using SAS EAI Agent for IBM Security Access Manager for Mobile 8
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-013075-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>May 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
Solution Flow using SAS .......................................................................................... 5
Configuring SafeNet Authentication Service ............................................................ 6
  Assigning an Authenticator in SAS ........................................................................ 6
Installing and Configuring the SAS EAI Agent .......................................................... 7
  SAS EAI Agent Overview ....................................................................................... 7
  Installing the SAS EAI Agent ................................................................................. 7
  Deploying the WAR File ......................................................................................... 8
  Configuring the SAS EAI Agent ............................................................................ 9
Configuring IBM ISAM for Mobile 8 ....................................................................... 10
  Creating the EAI Junction ...................................................................................... 10
  Configuring the Reverse Proxy ............................................................................. 14
  Configuring the Secure Mobile Policy .................................................................. 15
  Assigning the Policy to the Protected Resource .................................................... 17
  Configuring the Authentication Mobile Policy ...................................................... 18
Running the Solution ............................................................................................... 21
Support Contacts ...................................................................................................... 22
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as IBM Security Access Manager for Mobile 8.

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.

IBM® Security Access Manager (ISAM) for Mobile 8 provides an integrated security management platform for authentication services, access control, authorization services, identity mapping, web single sign-on, entitlements, and audit services across the enterprise resources. IBM Security Access Manager for Web provides integrated, policy-based security management for the extended enterprise that enables customers, business partners, employees, suppliers, and distributors to securely access enterprise resources in a trusted manner.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in IBM Security Access Manager for Mobile 8 using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure IBM Security Access Manager for Mobile 8 to work with SafeNet Authentication Service EAI Agent.

It is assumed that the IBM Security Access Manager for Mobile 8 environment is already configured and working with static passwords prior to implementing multi-factor authentication using 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 – Private Cloud Edition (SAS-PCE)
- SafeNet Authentication Service EAI Agent
- IBM Security Access Manager for Mobile 8—Version 8.0.0.5

Audience

This document is targeted to system administrators who are familiar with IBM Security Access Manager for Mobile 8, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

Solution Flow using SAS

The image below describes the environment required to implement an IBM ISAM 8 solution using SafeNet Authentication Service:

1. The user attempts to access the protected resource. (In this example, the WebSEAL server.)
2. The WebSEAL EAI redirects the user to SafeNet Authentication Application (SAA).
3. SAA collects LDAP credentials from the user.
4. SAA validates the LDAP credentials against a configured LDAP server.
5. The user is prompted for a one-time password (OTP).
6. The user generates and provides the OTP.
7. Upon successful OTP validation, WebSEAL’s required EAI headers are added to the response.
8. WebSEAL detects the headers in the response and grants the user access to the protected resource.
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with IBM Security Access Manager for Mobile 8 using EAI Agent requires the following:

- Assigning an Authenticator in SAS, see below

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 IBM Security Access Manager for Mobile 8.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet Gold
- SMS Token
- MP-1 Software Token
- GrIDsure Authentication
- 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.

Installing and Configuring the SAS EAI Agent

SAS EAI Agent Overview

The SAS EAI Agent must be installed on Linux. The following versions are supported:

- RHEL 5.9
- RHEL 6.4
- SLES 10
- SLES 11

**NOTE:** Red Hat versions 5.9 and 6.4 x64 were used at the time this document was written.

For this integration, the following procedures are required to prepare the SafeNet SAS EAI agent:

- Installing the SAS EAI Agent, page 7
- Deploying the WAR File, page 8
- Configuring the SAS EAI Agent, page 9

Installing the SAS EAI Agent

1. Install JRE (Java Runtime Environment).
2. Install Apache Tomcat.
3. Install the agent using the rpm command: `rpm -ivh <file_name>`
   The agent is installed in `/usr/local/safenet/webseal`. 
Deploying the WAR File

2. Click Manager App.

3. Under WAR file to deploy, click Browse, and then select the following file: /usr/local/safenet/webseal/SafenetWebseal.war.
4. Click **Deploy**.

5. After deployment, open the **Manager App** page again, and verify that the **Running** value for the `/SafenetWebseal` application is **true**.

![Tomcat Web Application Manager](image-url)

*The screen image above is from The Apache Software Foundation. Trademarks are the property of their respective owners.*

6. Click the `/SafenetWebseal` hyperlink to test the app. The agent login screen is displayed.

### Configuring the SAS EAI Agent

The SAS EAI agent configuration file, `JCryptoWrapper.ini`, is located in `/usr/local/safenet/webseal/ini`. `JCryptoWrapper.ini` contains all the relevant configurations for the agent. The following describes some of the main configuration keys.

- **PrimaryServer** is the IP of the primary BSID server.

```ini
;Primary BSID Server Data. Do not change PrimaryWebServiceRelativePath
PrimaryProtocol=http
PrimaryServer=192.168.40.124
PrimaryServerPort=80
PrimaryWebServiceRelativePath=/TokenValidator/TokenValidator.asmx
```

- To enable LDAP authentication before OTP authentication, set the **USE_SPLIT_AUTH** value to `1`.

```ini
;When this is set to 1, user will be first asked to enter LDAP Credentials.
;And on LDAP validation success user will proceed to enter OTP
USE_SPLIT_AUTH=1
```
The default LDAP credentials are included in this configuration file. Update the default LDAP credentials to those required by your Active Directory.

```
;------------------------ LDAP Settings
LDAP_SERVER=192.168.40.124
LDAP_PORT=389
LDAP_AUTH_DN=CN=Administrator,CN=Users,DC=AUTHDOMAIN,DC=LOCAL
LDAP_AUTH_PASSWORD=
LDAP_BASE_DN=DC=AUTHDOMAIN,DC=LOCAL
LDAP_USER_BASE_DN=CN=Users,DC=AUTHDOMAIN,DC=LOCAL
```

### Configuring IBM ISAM for Mobile 8

To configure IBM ISAM for Mobile 8 so that users can authenticate to the protected web application using the SAS EAI agent requires:

- Creating the EAI Junction, page 10
- Configuring the Reverse Proxy, page 14
- Configuring the Secure Mobile Policy, page 15
- Assigning the Policy to the Protected Resource, page 17
- Configuring the Authentication Mobile Policy, page 18

### Creating the EAI Junction

IBM ISAM for Mobile 8 is configured with default options. In the following example, a reverse proxy with junctions is used. One junction is the protected web application, and the other is the SafeNet WebSEAL external authentication agent.

1. Ensure that a reverse proxy is already configured for a protected web application.
2. Log on to the IBM Security Mobile Gateway Appliance console.

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

4. Select the reverse proxy, and then click Manage > Junction Management.

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)
5. Click **New > Standard Junction**.

6. Under **Junction Point Name**, specify a name for the junction, and under **Junction Type**, select **TCP**.
7. Click the **Servers** tab, and then click on **New**. The **Add TCP or SSL Servers** window is displayed.

8. Complete the following fields, and then click **Save**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hostname</strong></td>
<td>Enter the IP address of the EAI server.</td>
</tr>
<tr>
<td><strong>TCP or SSL Port</strong></td>
<td>Select the port that the ISAM will use to access the EAI server.</td>
</tr>
<tr>
<td><strong>Virtual Host</strong></td>
<td>Enter <code>/SafenetWebseal/Login</code>.</td>
</tr>
<tr>
<td><strong>Virtual Host Port</strong></td>
<td>Select the port that the ISAM will use to access the EAI server.</td>
</tr>
<tr>
<td><strong>Local Address</strong></td>
<td>Select the reverse proxy IP address.</td>
</tr>
<tr>
<td><strong>Query Contents</strong></td>
<td>Enter <code>/cgi-bin/query_contents</code>.</td>
</tr>
<tr>
<td><strong>Treat URL as case insensitive</strong></td>
<td>Select this check box.</td>
</tr>
</tbody>
</table>

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)
9. Click the Identity tab, and then verify all of the check boxes under **HTTP Header Identity Information** are selected.

![Image of IBM Security Access Manager](image)

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

10. Click **Save**.

### Configuring the Reverse Proxy

Configure the triggering URL and the external authentication for the reverse proxy.

1. In the IBM Security Mobile Gateway Appliance console, select **Secure Web Settings > Manage > Reverse Proxy**.

![Image of IBM Security Access Manager](image)

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

2. Select the reverse proxy, and then click **Edit**.

3. Click the **Authentication** tab.
4. Complete the following, and then click **Save**:

<table>
<thead>
<tr>
<th>Trigger URL</th>
<th>Click <strong>New</strong>, and then add the EAI junction URL that you created in the previous procedure. The ISAM supports regular expressions.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Levels</td>
<td>Click <strong>New</strong>, and then add <strong>ext-auth-interface</strong>.</td>
</tr>
</tbody>
</table>

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

**Configuring the Secure Mobile Policy**

To use the redirect mechanism, create an access control policy and assign it to the relevant resource. The access control policy will create a grade based on a predefined context vector, and will be used to define the access policy.

1. In the IBM Security Mobile Gateway Appliance console, select **Secure Mobile Settings > Policy > Access Control**.

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)
2. Click the create policy icon 📝. The create policy window is displayed.

3. Configure the access control policy. Use the required urn for the http redirect authentication mechanism.

4. Click Save.
Assigning the Policy to the Protected Resource

Now you can assign the access control policy that you created in “Configuring the Secure Mobile Policy” to the protected resource.

1. In the IBM Security Mobile Gateway Appliance console, select **Secure Mobile Settings > Access Control > Resources**.

2. Select the protected resource, and then click **Attach**.

3. Select the policy that you created in “Configuring the Secure Mobile Policy,” and then click **OK**.

4. Click **Publish**.

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)
5. Click **Publish** to confirm the action.

![Image: IBM Security Access Manager console]

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

### Configuring the Authentication Mobile Policy

Now you can configure the HTTP redirect mechanism.

1. In the IBM Security Mobile Gateway Appliance console, select **Secure Mobile Settings > Policy > Authentication**.

![Image: IBM Security Access Manager console]

*(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)*
2. Click ☐ to create a new authentication policy.
3. Complete the following fields, and then click Save:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the policy name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>Enter the urn identifier: urn:ibm:security:authentication:asf:http-redirect-softtoken</td>
</tr>
<tr>
<td>Workflow Steps</td>
<td>Click Add Step, and then select HTTP Redirect.</td>
</tr>
</tbody>
</table>

4. Click Mechanisms, and then select HTTP Redirect.
5. Click Modify Authentication Mechanism.

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)
6. Click the **Properties** tab.

7. Complete the following details, and then click **Save**:

<table>
<thead>
<tr>
<th>Redirect URL</th>
<th>Enter https://&lt;EAI Agent IP&gt;:Port/eai/SafenetWebseal/Login.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success Credential Attribute Name</td>
<td>Enter httpRedirectAuthCompleted.</td>
</tr>
<tr>
<td>Success Credential Attribute Value</td>
<td>Set this value to <strong>true</strong>.</td>
</tr>
</tbody>
</table>

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

Log on to the protected resource to check the configured solution.

1. Open a web browser and enter the URL for the reverse proxy of the WebSEAL protected resource. You are redirected to the SafeNet Authentication application to log in.

2. On the login page, enter your **User Name** and **LDAP Password**, and then click the arrow icon.

3. You are prompted to enter a **One Time Password** (OTP). Enter your OTP, and then click the arrow icon.
   (Depending on the configuration, you may also need to enter a PIN with the OTP.)

After successful authentication, you are redirected to the WebSEAL protected resource.
**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 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 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></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>