SafeNet Authentication Service
Integration Guide

SAS EAI Agent for IBM Security Access Manager for Web 7.0
Document Information

Document Part Number | 007-012650-001, Rev A
---|---
Release Date | July 2014

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>
</table>
| Mail | SafeNet, Inc.  
4690 Millennium Drive  
Belcamp, Maryland 21017, USA |
| Email | TechPubs@safenet-inc.com |
## Contents

- **Introduction** .................................................................................................................. 4
- **Third-Party Software Acknowledgement** ........................................................................ 4
- **Overview** .......................................................................................................................... 4
- **Solution Overview** ......................................................................................................... 4
- **Solution Flow** ................................................................................................................... 5
- **Prerequisites** .................................................................................................................... 5
- **Configuration Components** ............................................................................................. 6
- **SAS EAI Agent Installation and Configuration** ................................................................. 6
  - **SAS EAI Agent Overview** ............................................................................................. 6
  - **Installing the SAS EAI Agent** ..................................................................................... 7
  - **Deploying the WAR File** ............................................................................................. 7
  - ** Configuring the SAS EAI Agent** ................................................................................. 9
- **IBM ISAM for Web 7.0 Basic Configuration** .................................................................. 10
  - **Configuring IBM ISAM for Web 7.0** ...................................................................... 10
- **SAS Configuration** .......................................................................................................... 16
- **Running the Solution** ...................................................................................................... 16
- **Support Contacts** ............................................................................................................ 17
Introduction

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.

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.

Overview

IBM® Security Access Manager (ISAM) for Web 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.

For more information, refer to IBM Security Identity Manager V6.0.0 documentation.

Organizations using IBM ISAM for Web to protect their resources can now implement the SafeNet Authentication Service (SAS) solution for powerful two-factor authentication.

Solution Overview

Authentication is the process of proving that a user is who he or she claims to be. The Access System allows you to configure authentication rules in the policy domains and policies that protect your resources. Authentication rules, in turn, contain authentication schemes. Authentication schemes provide the methods for performing verification of the user's identity.

This software utilizes IBM WebSEAL's External Authentication Interface (EAI) for two-factor authentication. When a user tries to access a protected application, WebSEAL intercepts the request based on a defined set of rules and redirects the login request to an appropriate authentication destination; in this case, a custom J2EE application (SafeNet WebSeal) deployed on the same physical server or an external J2EE server (Apache Tomcat 7xx).

The application receives the request and then collects the user’s LDAP credentials and verifies them on a configured LDAP server (LDAP and two-factor credentials verification can be split into two stages via configuration). It then sends the collected credentials to SafeNet Authentication Server (SAS) using a highly encrypted (1024-bit) payload over SOAP protocol. SAS then sends back an encrypted authenticated response. On successful two-factor authentication, the response is returned to WebSEAL with some special response headers, which WebSEAL translates into a successful authentication. WebSEAL adds an authentication header to the ongoing request and forwards the request to the protected resource.
Solution Flow

The following diagram shows the environment required to implement an IBM ISAM for Web 7.0 solution using SafeNet Authentication Service:

In this example, the user wants to connect to the WebSEAL server.

1. The user tries to access the protected resource.
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 access to user.

Prerequisites

To successfully configure and implement the solution, the administrator must be familiar with the following:

- IBM Security Access Manager for Web 7.0
- SafeNet Authentication Service, cloud or on-premises
  This guide uses SAS Cloud as an example, but the solution can also be implemented on SAS PCE/SPE (on-premises).
- SafeNet Authentication Service EAI agent
The following prerequisite tasks must also be completed:

- Ensure the prerequisites required for installing the IBM Security Access Manager (ISAM) components are met. Refer to the following link:
  stl_preq_prod.html

- Install the following:
  - IBM ISAM for Web 7.0
  - SafeNet Authentication Service EAI agent

- Create an account in SAS Cloud.
  For more information, refer to: http://www.safenet-inc.com/request-information/

- Ensure that a Microsoft environment is available for client installation.

Configuration Components

The environment components are:

- IBM Security Access Manager for Web 7.0
- SafeNet Authentication Service EAI Agent
- SafeNet hardware or software token that has been assigned or provisioned to a user

SAS EAI Agent Installation and Configuration

SAS EAI Agent Overview

The SAS EAI agent must be installed on a Linux machine. The following versions of Linux are supported:

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

For this guide, Red Hat versions 5.9 and 6.4 x64 were used.

To prepare the SafeNet SAS EAI agent, perform the following steps:

- Install the agent.
- Deploy the WAR file.
- Configure the agent.
Installing the SAS EAI Agent

To install the SAS EAI Agent:
1. Install Java Runtime Environment (JRE).
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

To deploy the WAR file:
1. Go to the Apache management console: `http://localhost:8080`
2. On the right side of the window, click the Manager App button.

3. Under WAR file to deploy, do the following:
   a. Click Browse to locate and select the following file:
      `/usr/local/safenet/webseal/SafenetWebseal.war`
   b. Click Deploy.
4. After deployment, open **Application Manager** and ensure that, in the **Running** column, the `/SafenetWebseal` application has the value set to **true**.

5. To test the app, click the `/SafenetWebseal` hyperlink. The agent login window is displayed.
Configuring the SAS EAI Agent

The SAS EAI agent configuration file can be found at /usr/local/safenet/webseal/ini.

The file JCryptoWrapper.ini is the configuration file that 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
  ```

- Default LDAP credentials are included in the file.

  ```ini
  ; ------------------------------------------ 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
  ```

  Update the default LDAP credentials to those required by your Active Directory.
IBM ISAM for Web 7.0 Basic Configuration

This chapter explains the steps needed to configure IBM ISAM for Web 7.0 with a basic configuration so that the user can authenticate to the protected web application using the SAS EAI agent.

Configuring IBM ISAM for Web 7.0

IBM ISAM for Web 7.0 is configured with default options. In the following example, a reverse proxy with two junctions is used. One junction is the protected web application, and the other is the SafeNet WebSEAL external authentication agent.

To configure IBM ISAM for Web 7.0:

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

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

![Secure and Reverse Proxy screen](image)

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

4. Select your reverse proxy, and then click Edit.

![Reverse Proxy settings screen](image)

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

5. Click the Authentication tab.
   a. Under Trigger URL, click New and add `/eai/SafenetWebseal/Login`.
   c. Click Save.
6. Log in to ISAM for the web command line interface, and create the following ACL for unauthenticated users:

- `pdadmin sec_master> acl create unauth`
- `pdadmin sec_master> acl modify unauth set group iv-admin TcmedbsvaBRrxl`
- `pdadmin sec_master> acl modify unauth set group webseal-servers Tgmdbsrxl`
- `dpdadmin sec_master> acl modify unauth set user sec_master TcmedbsvaBRrxl`
- `pdadmin sec_master> acl modify unauth set any-other Trx`
- `pdadmin sec_master> acl modify unauth set unauthenticated Trxc`

7. Attach the ACL you created in the previous step to the EAI application (object).

   For example: `pdadmin sec_master> acl attach <object name/reverse proxy>/eai unauth`

8. 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.)
9. Do the following to create a new junction in which the SAS EAI server is the junction server:
   a. Click **New > Standard Junction**.

   ![Screen image of Junction Management](image)

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

   b. On the **Junction** tab, complete the following fields:

<table>
<thead>
<tr>
<th>Junction Point Name</th>
<th>Enter a name for the junction point.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Junction Type</td>
<td>Select TCP.</td>
</tr>
</tbody>
</table>
c. Click the **Servers** tab, and then click **New**, complete the following fields:

<table>
<thead>
<tr>
<th>Hostname</th>
<th>Enter the SAS EAI agent server information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Host</td>
<td>Add the path to the login folder: /SafenetWebseal/Login</td>
</tr>
</tbody>
</table>

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

d. Click **Save**.

10. On the **Reverse Proxy** window, do the following to configure redirection to the EAI agent:

a. Click **Secure > Reverse Proxy**.

b. Select your reverse proxy, and then select **Manage > Management Root**.

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)
c. In the **Management Root** list, select `login.html`.

![Screen image of Management Root list](image1)

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

**d.** Click **File > Open**.

**e.** In the first `<script>` tag, add the following script to redirect to the reverse proxy that holds the SAS EAI agent:

```javascript
document.cookie = 'ISAMOriginalURL=' + encodeURIComponent(window.location) + '; Path=/;
location.href = '/eai/SafenetWebseal/Login'
```

![Screen image of reverse proxy management](image2)

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

**f.** Click **Save**.

11. Deploy and restart the reverse proxy.
SAS Configuration

After the SAS EAI agent has been configured as a junction server, the SAS EAI agent IP must be added as an Auth Node to your organization.

To configure the SAS agent Auth Node:

1. Log in to the SAS Console.
2. Select VIRTUAL SERVER > COMMS.
3. Under Auth Nodes, select Auth Node and then click Add.
4. Enter the following information:

<table>
<thead>
<tr>
<th>Description</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Description</td>
<td>Enter a description of the agent.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the IP address of the SAS EAI agent.</td>
</tr>
<tr>
<td>FreeRADIUS Synchronization</td>
<td>Ensure that this option is not selected.</td>
</tr>
</tbody>
</table>

5. Click Save.

Running the Solution

To log on to the protected resource:

1. Open a browser and go to the URL of the reverse proxy of the WebSEAL protected resource.
2. On the SafeNet Authentication logon window, enter your user name and LDAP password, and then click the arrow icon.

NOTE: Depending on your token type, you may need to generate an OTP.
3. When prompted, enter a one-time password (OTP). Depending on your configuration, you may need to enter a PIN along with the OTP.

Upon successful login, 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 phone support is available to you.

**Table 1: Support Contacts**

<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</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>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>