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

<table>
<thead>
<tr>
<th>Document Product Number</th>
<th>007-012474-001, Revision A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>September 2014</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.
## Contents

Preface .............................................................................................................................. 4  
Support Contacts ............................................................................................................ 4  

CHAPTER 1 Introduction ................................................................................................. 5  
Overview ........................................................................................................................... 5  
IBM ISAM for Web 7 and SafeNet SAS Solution Overview .................................................... 5  
Administrator Prerequisites ............................................................................................. 6  
Configuration Components .............................................................................................. 6  
  Solution Flow .................................................................................................................. 6  
Prerequisite Tasks ........................................................................................................... 7  

CHAPTER 2 SAS EAI Agent Installation and Configuration ............................................. 8  
SAS EAI Agent Overview ................................................................................................. 8  
Installing the SAS EAI Agent ......................................................................................... 8  
Deploying the WAR File ................................................................................................. 9  
Configuring the SAS EAI Agent ..................................................................................... 10  

CHAPTER 3 IBM ISAM for Web 7.0 Basic Configuration .................................................. 12  
Configuring IBM ISAM for Web 7.0 ............................................................................. 12  

CHAPTER 4 SAS Configuration ....................................................................................... 18  
Configuring SAS ............................................................................................................. 18  

CHAPTER 5 Running the Solution ................................................................................... 19  
Logging On to the Protected Resource ............................................................................ 19
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 1: Support Contacts

<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></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>
CHAPTER 1
Introduction

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, see:

Organizations using IBM ISAM for Web to protect their resources can now implement the SafeNet Authentication Service (SAS) solution for powerful two-factor authentication (2FA).

IBM ISAM for Web 7 and SafeNet SAS Solution Overview

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

This software utilizes IBM WebSEAL’s External Authentication Interface (EAI) for two-factor authentications. 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, it’s a custom J2EE application (for example, SafeNetWebSeal) deployed on the same physical server or an external J2EE server (Apache Tomcat 7xx). The application receives the request, then collects the user’s LDAP credentials and verifies them on a configured LDAP server (LDAP and 2FA credentials verification can be split into two stages via configuration). It then sends the collected credentials to the cloud/on-premises SafeNet Authentication Server (SAS) using a highly encrypted (1024-bit) payload over SOAP protocol. SAS then sends back an encrypted authenticated response. Upon successful 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.
Administrator Prerequisites

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

- IBM Security Access Manager for Web 7.0
- SafeNet Authentication Service, Cloud, or SPE/PCE (on-premises)
  This guide uses SAS Cloud as an example but the solution can also be implemented on SAS SPE/PCE.
- SafeNet Authentication Service EAI Agent

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

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 the user.

**Prerequisite Tasks**

- Install the following:
  - IBM ISAM for Web 7.0
  - SafeNet Authentication Service EAI Agent
- Create an account in SAS Cloud.
  For more information, go to: http://www.safenet-inc.com/request-information/
- Ensure that a Microsoft environment is available for client installation.
SAS EAI Agent Overview

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

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

The procedures in this document are based on Linux Red Hat versions 5.9 and 6.4 x64.

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

- “Installing the SAS EAI Agent” – see below
- “Deploying the WAR File” – page 9
- “Configuring the SAS EAI Agent” – page 10

Installing the SAS EAI Agent

To install 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

To deploy the WAR file:

1. Go to the Apache management console: http://localhost:8080

2. On the right side, click the Manager App button.

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

4. Click Deploy.
5. After deployment, open the Application Manager and ensure that, in the **Running** column, the /SafenetWebseal application has the value of **true**.

6. To test the app, click the /SafenetWebseal hyperlink. The agent login screen opens.

### 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.

```
; ----------------------------- 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.
CHAPTER 3
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 is used with two junctions. 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 there is a reverse proxy already configured for a protected web application.
2. Log on to the **IBM Security Web Gateway Appliance** console.
3. Click **Secure > Reverse Proxy**.

4. Select the reverse proxy and then click **Edit**.

5. On the **Authentication** tab, add a new **Trigger URL**: `/eai/SafenetWebseal/Login`

6. Add a new **Authentication Level** called **ext-auth-interface**.
7. Log in to ISAM from 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 TcmodbsvaBRrxl
   - pdadmin sec_master> acl modify unauth set group webseal-servers Tgmdbsrxl
   - dpadmin sec_master> acl modify unauth set user sec_master TcmodbsvaBRrxl
   - pdadmin sec_master> acl modify unauth set any-other Trx
   - pdadmin sec_master> acl modify unauth set unauthenticated Trxc

8. Attach the ACL you created previously to the eai application (object).
   For example: `pdadmin sec_master> acl attach <object name/reverse proxy>/eai unauth`

9. Select the reverse proxy, and then select Manage > Junction Management.
10. Perform the following steps to create a new junction in which SAS EAI server is the junction server:

   a. Select **New > Standard Junction**.

   ![Standard Junction Creation](image)

   b. On the **Junction** tab, add a **Junction Point Name**.

   c. Under **Junction Type**, select **TCP**.

   d. Click the **Servers** tab, and then click **New**.

   e. In the **Hostname** box, enter the SAS EAI agent server information.

   f. In the **Virtual Host** box, add the path to the login folder: `/SafenetWebseal/Login`

   ![Servers Configuration](image)

   g. Click **Save**. You will be returned to the **Reverse Proxy** page.
11. Do the following to configure redirection to the EAI agent:

   a. Select **Secure > Reverse Proxy**.

   b. Click the reverse proxy, and then select **Manage > Management Root**.

   c. In the **Management Root** list, click **login.html**.

   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'
```

f. Click Save.

12. Deploy and restart the reverse proxy.
CHAPTER 4
SAS Configuration

This chapter explains how to use the SAS console to configure an Auth Node for the agent.

Configuring SAS

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. Click **Virtual Server > Comms**.
3. Under **Auth Nodes**, select **Auth Node** and then click **Add**.
4. Enter the following information:
   - **Agent Description**
   - **Low IP Address In Range**: IP Address of the SAS EAI agent
   - Ensure that **FreeRADIUS Synchronization** is not selected since this is a web service agent
5. Click **Save**.
CHAPTER 5
Running the Solution

Logging On to the Protected Resource

To log on to the protected resource:

1. In your browser, open the URL of the reverse proxy of the WebSEAL protected resource.
   You are redirected to the SafeNet Authentication application for logon.

2. Enter your user name and LDAP password, and then click the arrow button.
   You are prompted to enter a one-time password (OTP). Depending on your configuration, you may need to enter a PIN together with the OTP.

3. Enter your OTP. You are redirected to the WebSEAL protected resource.

   NOTE: Depending on your token type, you may need to generate an OTP.