SafeNet Authentication Service
Integration Guide

Using SAS with Web Application Proxy
Document Information

Document Part Number | 007-012656-001, Revision 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 |
<p>| Email | <a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a> |</p>
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>4</td>
</tr>
<tr>
<td>Single Sign-On Data Flow Scenario</td>
<td>4</td>
</tr>
<tr>
<td>The Environment</td>
<td>5</td>
</tr>
<tr>
<td>Configuring WAP to Use ADFS for Pre-Authentication</td>
<td>6</td>
</tr>
<tr>
<td>- Publish a Web Application in WAP</td>
<td>12</td>
</tr>
<tr>
<td>Configuring the MFA Agent</td>
<td>16</td>
</tr>
<tr>
<td>Configuring the AD FS Authentication Policy</td>
<td>17</td>
</tr>
<tr>
<td>Running the WAP SAML Authentication Solution</td>
<td>18</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>19</td>
</tr>
</tbody>
</table>
Overview

This document provides guidance for setting up and managing SafeNet Authentication Service (SAS) as an identity provider for web applications using ADFS 3.0 (bundled with Windows Server 2012 R2) and SafeNet Authentication Agent for ADFS.


NOTE: This document assumes that WAP is already configured and working with AD users and static passwords prior to implementing SafeNet Authentication Service strong authentication.

Single Sign-On Data Flow Scenario

1. Bob, a user, wants to log in to his organization’s published application by WAP. Bob leverages the single sign-on capabilities embedded in the organization’s SafeNet Authentication Service (SAS) solution. After Bob’s AD credentials are authenticated, SAS collects and evaluates Bob’s credentials.

2. SAS returns a response to WAP to accept or reject Bob’s credentials for authentication.
The Environment

1. User attempts to access a Web Application

2. WAP is configured to address ADFS for SAML authentication

3. MFA is configured on ADFS forwarding to SAS as 2nd authentication

4. After successful login on both ADFS and SAS, user is authenticated to the Web Application
Configuring WAP to Use ADFS for Pre-Authentication

To configure WAP as a Relying Party Trust in ADFS:

1. In the Server Manager, click **Tools > AD FS Management**.
2. In the pane, expand **AD FS > Trust Relationships**. Right-click **Relying Party Trusts** and then click **Add Relying Party Trust**.

   (The screen image above is Active Directory Federation Services software. Trademarks are the property of their respective owners.)

   The Add Relying Party Trust Wizard opens.

3. On the **Welcome** window, click **Start**.

   (The screen image above is Active Directory Federation Services software. Trademarks are the property of their respective owners.)

4. In the **Select Data Source** window, select the **Enter data about the relying party manually** option, and then click **Next**.
5. In the **Specify Display Name** window enter the following details:
   a. **Display name** - enter a name for this relying party (for example, **WAP**).
   b. **Notes** - enter a description.
   c. Click **Next**.

6. In the **Choose Profile** window, select the **AD FS profile** radio button, and click **Next**.
7. In the **Configure Certificate** window, click **Next**.

8. In the **Configure URL** window, click **Next**.

**NOTE:** This document refers to a standalone web application, therefore no protocol is configured. In cases where other secured web applications are required, the relevant protocol must be configured.
9. In the **Configure Identifiers** window, enter the following details:
   
a. **Relying party trust identifier** - enter the URL of the published application (e.g: https://iis.integ.com/app1/).

b. Click **Add**, and then click **Next**.

10. In the **Configure Multi-factor Authentication Now?** Window, click **Next**. (MFA will be configured later on).
11. In the Choose Issuance Authorization Rules window, select the Permit all users to access this relying party radio-button, and then click Next.

12. In the Ready to Add Trust window, review the settings, and then click Next to save your relying party trust information.
13. In the **Finish** window, ensure that **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** option is **not** selected, and then click **Close**.
Publish a Web Application in WAP


2. On the Welcome window, click Next.

3. In the left pane, click Preauthentication, and then select the Active Directory Federation Services (AD FS) option. Click Next.
4. In the left pane, click **Relying Party**. From the list of relying parties (taken from the AD FS server), select the relying party for the application that you want to publish (use the same relying party created in the section “Configuring WAP to Use ADFS for Pre-Authentication” on page 6), and then click **Next**.
5. In the left pane, click **Publishing Settings**, and then complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter an application name. This name is used only in the list of published applications in the Remote Access Management console.</td>
</tr>
<tr>
<td>External URL</td>
<td>Enter the external URL for this application. For example: <a href="https://iis.integ.com/app1/">https://iis.integ.com/app1/</a></td>
</tr>
<tr>
<td>External certificate</td>
<td>The selected certificate must fit the external URL. As each certificate has a URL, ensure that the selected certificate is the same as the configured external URL.</td>
</tr>
<tr>
<td>Backend server URL</td>
<td>Enter the URL of the backend server. This value is automatically entered when you enter the external URL, and you must change it only if the backend server URL is different.</td>
</tr>
</tbody>
</table>

(The screen image above isActive Directory Federation Services software. Trademarks are the property of their respective owners.)

6. In the left pane, click **Confirmation**. Review the settings and then click **Publish**.

**NOTE:** You can copy the PowerShell command to set up other published applications.
7. In the left pane, click **Results** Verify that the application was published successfully.

8. Click **Close**.
Configuring the MFA Agent

1. Run the MFA agent.
2. On the Policy tab, select the Enable/Disable Agent and Pre Generate Challenge options.
3. On the Communications tab, enter your SAS server IP address or name (and port if non-causal is used).
4. Click Apply. Enabling the agent registers the SafeNet MFA Adapter with AD FS and enables it at the global policy level.
5. Under Authentication Test, click Test to test authentication from the agent to the authentication server.
6. Under Server Status Check, click Test to test that the authentication server is online.
7. Click OK to close the window.
Configuring the AD FS Authentication Policy

1. Open the AD FS Management Console.
2. Right-click **Authentication Policies** and select **Edit Global Primary Authentication**.
3. Select the **Primary** tab. Verify that **Form Authentication** is selected for both **Extranet** and **Intranet**.
4. Select the **Multi-factor** tab.
   a. Under **Users/Groups**, add those that you want the MFA to take control of.
   b. Under **Locations**, select **Extranet** and/or **Intranet**, according to your preferred configuration.
   c. Ensure that **SafeNet Multi Factor Authentication (SMFA)** is selected as an additional authentication method.
   d. Click **OK**.

SafeNet Authentication Service is now configured as an identity provider for AD FS (and for WAP).
Running the WAP SAML Authentication Solution

After WAP is configured to use SafeNet Authentication Service as its identity provider (through AD FS), and SafeNet Authentication Service is configured to use AD FS as a SAML service provider, users can log in to WAP.

NOTE: The AD FS server time and the SAS server time must be NTP synchronized, as a difference of more than two (2) seconds will cause a failure.

To log in to a WAP-published application:

1. From the Internet, browse to https://iis.integ.com/app1 (this address refers to your organization WAP server and not directly to the IIS server where the application is configured, as you are supposed to connect from the Internet and not from inside the organization).

2. You will be redirected to your domain login page. Enter your organization credentials and then click Sign in.

3. After successful login, the SafeNet Authentication login window is displayed. Enter your SafeNet Authentication Service credentials and then click Submit.

4. After another successful login, you will be redirected to your requested web application.
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</td>
</tr>
<tr>
<td></td>
<td>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></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>