SafeNet Authentication Service
Integration Guide

Using SAS as an IDP of F5 BIG-IP APM
Document Information

<table>
<thead>
<tr>
<th>Product Version</th>
<th>3.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Part Number</td>
<td>007-012670-001, Rev. A</td>
</tr>
<tr>
<td>Release Date</td>
<td>August 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.

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

Introduction .................................................................................................................. 4
  Third-Party Software Acknowledgement .................................................................. 4
  Overview .................................................................................................................... 4
  Audience ................................................................................................................... 4
  Prerequisites ............................................................................................................ 5
Security Assertion Markup Language ......................................................................... 5
Authentication Flow ..................................................................................................... 5
Configure an Identity Provider .................................................................................... 7
Configurations on BIG-IP APM ................................................................................. 8
  Configuring BIG-IP APM as a Service Provider ..................................................... 9
  Configuring SAS as an Identity Provider ................................................................. 11
  Associating an Identity Provider Connector with the Service Provider Service .......... 13
  Configuring the Webtop ............................................................................................. 14
  Configuring the Webtop Links .................................................................................. 15
  Configuring the Access Profile ................................................................................ 16
  Editing the Access Profile ....................................................................................... 17
  Adding SAML Authentication .................................................................................... 18
  Adding a Webtop ........................................................................................................ 20
  Configuring the Virtual Server ................................................................................ 21
Configuring SAS to Use SAML-based User Federation .......................................... 24
  Enabling SAML User Authentication ..................................................................... 24
  Associating SAS Users with the SAML Service Provider ....................................... 26
Running the Solution ................................................................................................. 26
  Logging On Based on Tokens Assigned .................................................................. 27
  After Successful Authentication .............................................................................. 28
Appendix ..................................................................................................................... 30
  DNS and NTP Settings on the BIG-IP System .......................................................... 30
Support Contacts ........................................................................................................ 31
Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as F5 Networks® BIG-IP Access Policy Manager (APM).

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

BIG-IP APM is a flexible, high-performance access and security solution that provides unified global access to your applications and network. By converging and consolidating remote access, LAN access, and wireless connections within a single management interface, and providing easy-to-manage access policies, BIG-IP APM helps you free up valuable IT resources and scale cost-effectively.

BIG-IP APM protects your public-facing applications by providing policy-based, context-aware access to users while consolidating your access infrastructure. It also provides secure remote access to corporate resources, such as Microsoft Exchange, SharePoint, and VDI, from all networks and devices.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

The image above displays a sample Access Policy set in Access Policy Manager. To increase the security of resources behind APM, features of APM are used along with SAML authentication from SafeNet Authentication Service (SAS) to make resources available securely to authenticated users.

Audience

This document is targeted to system administrators familiar with the F5 BIG-IP APM management portal and who are interested in adding SAML authentication capabilities using SAS.
Prerequisites

- SAS should be configured, and a user account can be selected on the Assignment tab.
- A user must have an IP address for the local traffic virtual server.
- A user must have administrator privileges on the BIG-IP management portal.
- SAS and Exchange Server must be reachable from BIG-IP.
- A user must have a token enrolled with SAS; for example, Password, MobilePASS, GrIDSure, or SMS token.
- BIG-IP APM and SAS are up and running, and that a user has an Administrator and Operator account on APM and SAS, respectively.
- To successfully perform the instructions provided in this guide, you need the following:
  - SafeNet Authentication Service 3.3.2
  - F5 BIG-IP APM version 11.4.1
  - Exchange Server 2010 (OWA or any resource configured and running)

NOTE: The instructions provided in this guide have been tested in the following environments:
- SafeNet Authentication Service 3.3.2 Cloud
- F5 BIG-IP APM version 11.4.1 on Amazon Cloud
- Exchange Server 2010 on a publically accessible machine

Security Assertion Markup Language

Security Assertion Markup Language (SAML) is a standard for exchanging authentication and authorization data between security domains. SAML is an XML-based protocol that uses security tokens (information packets) containing assertions to pass information about a principal (usually an end user) between an identity provider and a web service. SAML enables web-based scenarios, including single sign-on (SSO) authentication. SAML is supported by F5 BIG-IP APM. In this SAML scenario, BIG-IP APM is the service provider and SafeNet Authentication Service (SAS) is the identity provider. BIG-IP APM implements the authentication result determined by SAS.

Authentication Flow

The address of a local traffic virtual server created on BIG-IP APM is provided to a user. When the user browses to the virtual server, the secure access to the BIG-IP APM using SAS with SAML happens as explained below:

1. Bob, a user, wants to log in to F5 virtual server. Bob leverages the single sign-on capabilities embedded in the organization’s SAS solution.
2. The SAS portal collects Bob's credentials and passes them to SAS for authentication. SAS evaluates Bob's credentials and returns accept or reject response to the external portal.
3. The external portal uses the response from SAS to return *accept* or *error* assertion to the F5 virtual server.
4. After successful SAML authentication, the user gets access to a Webtop with predefined resources.
5. The user can click on the desired Webtop links to access resources.
Configure an Identity Provider

The SAS Administrator Console settings are used to establish SAS as the identity provider for BIG-IP APM.

To configure SAS as an identity provider:

1. In the SAS Administrator Console, click Virtual Server, and then click the COMMS tab.

2. Click SAML Service Providers > SAML 2.0 Settings. The SAML 2.0 settings are displayed, as shown in the screen below.

3. Download the SafeNet-Idp-Metadata.xml file using the configured URL against Entity ID (https://idp1.cryptocard.com/idp/shibboleth) and save it to your local machine. This file is required when creating the new SAML identity provider in BIG-IP APM.
Configurations on BIG-IP APM

A virtual server is created on BIG-IP, on which an Access Policy is applied. To set up the virtual server, log in to the management portal of APM as a BIG-IP administrator. Configure BIG-IP with the SAML service provider, external IDP connectors, access profile, Webtop, and virtual server.

NOTE: If the virtual server and Webtop are already configured on BIG-IP APM, skip these configuration steps. Configure the Service Provider and IDP Connector, and edit the access profile, accordingly.

To access the management portal of F5 BIG-IP APM:

1. Browse to the public DNS/public IP of the BIG-IP APM Amazon instance.
2. Click Proceed anyway.
3. Enter administrator login credentials and then click Log in.
On successful authentication, you are logged in as an administrator in the management portal.

_configuring BIG-IP APM as a Service Provider_

A service provider is a system that relies on information provided by an identity provider. Based on an assertion from an identity provider, a service provider grants or denies access to protected services.

When you use APM as a SAML service provider, APM consumes the SAML assertions (claims) and validates their trustworthiness. After successfully verifying the assertion, APM creates session variables from the assertion contents. In an Access Policy, you can use these session variables to control access to resources. Based on the values of session variables, you can create multiple branches in the policy, assigning different resources on each branch. When it runs, the Access Policy follows a branch depending on the values of session variables.

To configure BIG-IP as a service provider:

1. In the F5 management portal, click **Main > Access Policy > SAML > BIG-IP as SP**.
2. In the right corner of the window, click **Create**.

3. On the **Create New SAML SP Service** window, click **General Settings** in the left pane and then complete the following fields:

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the service provider; for example, <strong>SASasIDP</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entity ID</strong></td>
<td>Enter the URL of the virtual server.</td>
</tr>
</tbody>
</table>

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

4. Click **OK**.
Configuring SAS as an Identity Provider

The BIG-IP system is used as the SAML service provider. It sends authentication requests to and receives assertions from SAS (identity provider).

To configure SAS as an Identity Provider:

1. In the F5 management portal, click **Main > Access Policy > SAML > BIG-IP as SP.**

   (The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

2. Click the **External IdP Connectors** tab.

   (The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

3. In the right corner of the window, click **Create > From Metadata.**

   You will create an identity provider from the metadata you downloaded in the section “Configure an Identity Provider” on page 7.

   (The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
4. On the **Create New SAML IdP Connector** window, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Select File</strong></td>
<td>Enter the path of the downloaded metadata file.</td>
</tr>
<tr>
<td><strong>Identity Provider Name</strong></td>
<td>Enter an appropriate name for the Identity Provider.</td>
</tr>
</tbody>
</table>

5. Click **OK**.

The External Identity Provider Connector is added and displayed in the list. You can edit the connector, if required, and verify the values.
Associating an Identity Provider Connector with the Service Provider Service

After the local Service Provider service and the external Identity Provider connector are added, bind the Identity Provider connector with the Service Provider service.

1. In the F5 management portal, click **Main > Access Policy > SAML > BIG-IP as SP**.
2. Select the Service Provider service and then click **Bind/Unbind IdP Connectors**.

3. On the **Edit SAML IDP** window, click **Add New Row**.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
4. In the **SAML IdP Connectors** column, select the Identity Provider connector; for example, `/Common/SAS`.

![Edit SAML IDP's that use this SP](image)

*(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)*

5. Click **Update** and then click **OK**.

**Configuring the Webtop**

When a user is allowed access based on an Access Policy, that user is typically assigned a Webtop. A Webtop is the successful endpoint for a Web application or a network access connection.

**To create a Webtop:**

1. Click **Access Policy > Webtops > Webtop List**.

![Access Policy](image)

*(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)*
2. In the right corner of the screen, click **Create**.

3. Complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the Webtop.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select <strong>Full</strong>.</td>
</tr>
</tbody>
</table>

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

4. Click **Finished**.

**Configuring the Webtop Links**

Webtop links are the links to the resources, such as OWA, that are being added to the Webtop. After successful SAML authentication, the links to the resources will be displayed on the assigned Webtop.

To create the Webtop links:

1. Click **Access Policy > Webtops > Webtop Links**.
2. On the right corner of the screen, click **Create**.
3. Complete the **New Webtop Link** fields as described below:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the Webtop link; for example, OWA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>(Optional) Type a description for this link.</td>
</tr>
<tr>
<td>Link Type</td>
<td>Select either <strong>Application URL</strong> or <strong>Hosted Contents</strong>. For example, if your resource is an application, select <strong>Application URL</strong>.</td>
</tr>
<tr>
<td>Application URL</td>
<td>This field is available for selection only when <strong>Application URL</strong> is selected as the <strong>Link Type</strong>. Specify the URL of the application.</td>
</tr>
<tr>
<td>Hosted File</td>
<td>This field is available for selection only when <strong>Hosted Contents</strong> is selected as the <strong>Link Type</strong>. Specify the hosted file.</td>
</tr>
</tbody>
</table>
4. Click **Finished**.

### Configuring the Access Profile

The access profile acts as the brain of the solution. It is where you define the criteria for granting access to the various servers, applications, and other resources on your network.

**To create an access profile:**

1. Click **Access Policy > Access Profiles**.
2. Under **General Properties**, specify a name for the profile; for example, **SAS_SAML_Profile**.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
3. Under **Language Settings**, select a language in the **Factory Builtin Languages** list and then click the << button to move the selected language to the **Accepted Languages** list.

![Language Settings](image)

*(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)*

4. Click **Finished**.

**Editing the Access Profile**

Using an Access Policy, you can define a sequence of checks to enforce the required level of security on a user system before a user is granted access to servers, applications, and other resources on your network.

An Access Policy can also include authentication checks to authenticate a user before access is granted to the network resources. The access profile can be edited as per requirements.

A sample Access Policy looks like this:

![Access Policy](image)

*(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)*

**To edit the access profile:**

1. On the **Main** tab of the navigation pane, expand **Access Policy > Access Profiles**.
2. In the **Access Profiles List**, find the Access Policy you want to edit and then click **Edit** in the **Access Policy** column.

   The Visual Policy editor opens in a new window or a new tab, depending on your browser settings. This is the new blank policy that you have just created.
3. On a rule branch of the Access Policy, click the + symbol to add an action.

   The Add Item window appears. Click the + symbol to add SAML authentication and Webtop assignments.

   (The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

   **Adding SAML Authentication**

   You can add authentication to an Access Policy using AAA servers (Authentication, Authorization, and Accounting) or client certificates.

   If a user is successfully authenticated, that user continues on the **Successful** branch. A user who is not successfully authenticated continues on the **Fallback** branch.

   **To add SAML authentication after the logon page:**

   1. Click the + symbol after **Start**.

   (The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
2. On the Authentication tab, select SAML Auth, and then click Add Item.

3. Under SAML Authentication SP, select the configured SAML service provider; for example, /Common/SASasIDP.

4. Click Save.
Adding a Webtop

When a user is successfully authenticated, they are presented with a Webtop containing customized resources.

To add a Webtop:

1. Click the + symbol in the Successful branch of SAML Auth.

2. On the Assignment tab, select Advanced Resource Assign, and then click Add Item.


5. Select the Webtop Links and Webtop tabs to define each item.

![Webtop Links and Webtop tabs](image)

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

6. Click **Update** for the expression. The Resource Assignment window becomes active.

7. Click **Save**.

### Configuring the Virtual Server

When using BIG-IP APM, virtual servers are configured with specific settings for network access connections or web application access. The IP address assigned to a host virtual server is the one that is typically exposed to the Internet.

With the Access Policy Manager, you can configure a remote access connection to one or more internal web applications. Using web applications, you create an Access Policy and local traffic virtual server so that end users can access internal web applications through a single external virtual server.

**To create a virtual server for secure connection:**

1. On the **Main** tab of the navigation pane, expand Local Traffic and then click **Virtual Servers**.

![Virtual Servers](image)

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

2. Click **Create**.
3. Complete the **New Virtual Server** fields as described below:

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the virtual server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
<td>For <strong>Type</strong>, select <strong>Host</strong>. In the <strong>Address</strong> field, enter the virtual server host IP address.</td>
</tr>
<tr>
<td><strong>Service Port</strong></td>
<td>Select <strong>HTTPS</strong>.</td>
</tr>
<tr>
<td><strong>HTTP Profile</strong></td>
<td>Select <strong>HTTP</strong>.</td>
</tr>
<tr>
<td><strong>SSL Profile (Client)</strong></td>
<td>Select the client SSL profile to use with this virtual server.</td>
</tr>
<tr>
<td><strong>SSL Profile (Server)</strong></td>
<td>If your web application server is using HTTPS services, select the server SSL profile to use with this virtual server.</td>
</tr>
<tr>
<td><strong>Access Profile</strong></td>
<td>Select the access profile to associate with this virtual server. You must create an access profile before you define the virtual server as there is no default access profile available.</td>
</tr>
<tr>
<td><strong>Rewrite Profile</strong></td>
<td>If you are creating a virtual server to use with web applications, select the rewrite profile.</td>
</tr>
</tbody>
</table>

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
4. Click **Finished**.
Configuring SAS to Use SAML-based User Federation

Before configuring an F5 BIG-IP APM instance as a SAML service provider for SAS, ensure that the organization’s user accounts have been created on the SAS virtual server. This can be done using one of the following methods:

- **Automatically**—by synchronizing with your Active Directory/LDAP server using the SAS LDAP Synchronization Agent
- **Manually**—by using the Create User shortcut
- **Manually**—by importing one or more user records using a flat file

For further information on adding users to SAS, refer to the SAS documentation at: [http://www2.safenet-inc.com/sas/implementation-guides.html](http://www2.safenet-inc.com/sas/implementation-guides.html)

Enabling SAML User Authentication

An organization’s user accounts must be configured to authenticate F5 BIG-IP APM using SAS.

1. On the **SAS Administrator Console**, click **Virtual Server**, and then click the **COMMS** tab.
2. Click **SAML Service Providers > SAML 2.0 Settings**. The SAML 2.0 Settings are displayed, as shown in the screen below.

3. Click **Add**.

4. Complete the SAML details as described below:

   | Friendly Name | Enter a name for the BIG-IP APM service provider. |
   | Destination | For **Type**, select **Host**. In the **Address** field, enter the virtual server host IP address. |
   | SAML 2.0 Metadata | Select **Create New Metadata file**. |
   | Entity ID | Enter the URL of the F5 BIG-IP APM virtual server you use to log in. |

5. Click **Apply**.
Associating SAS Users with the SAML Service Provider

Users in the SAS user store must be associated with an appropriate SAML service provider. This can be achieved using a pre-defined SAML provisioning rule that will automatically associate a group (or groups) of users to the specific SAML service provider. For more information on using SAML provisioning rules, see the SafeNet Authentication Service Administration Guide. The SAS documentation can be found at: http://www2.safenet-inc.com/sas/implementation-guides.html

**NOTE:** This process is common for all the SAML service providers. If you have already configured a different SAML service provider, repeat the process to make sure that the users are associated with multiple SAML service providers.

To associate a SAS user with the SAML Service Provider:

1. On the **Assignment** tab, select a user in the SAS virtual server.
2. Under **SAML Services**, click **Add**.
3. Complete the SAML Service details as described below:

<table>
<thead>
<tr>
<th>Service</th>
<th>Select <strong>Service for SAML Service Provider</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML Login ID</td>
<td>Select a login ID.</td>
</tr>
</tbody>
</table>

4. Click **Add**.

Running the Solution

Once the BIG-IP local traffic virtual server is configured with an appropriate Access Policy, the administrator provides the users with the address of BIG-IP local traffic virtual server.

If you have an enrolled token (such as OTP, GrIDsure, SMS, or MP), browse to the virtual server. On the SAS login window, enter the credentials for the SAML authentication.

Proceed according to the steps configured in the Access Policy.

A user can be assigned several types of SAS-supported tokens. This section provides guidance on how to run the solution for one of the token types, the GrIDsure token.
Logging On Based on Tokens Assigned

GrIĐsure Token

If a user is assigned a GrIĐsure token, that user needs to select a grid pattern as a password.

1. Browse to the local traffic virtual server configured in APM. You are redirected to the SAS login portal.
2. On the login window, enter your User Name and then click Login.

3. In the Password field, enter the numbers in the grid that correspond to your selected GrIĐsure pattern and then click Login.
After Successful Authentication

If the credentials are valid, authentication will be successful. Otherwise, authentication will fail and the user will not be allowed access to resources.

1. On successful SAML authentication, the Webtop assigned in the Access Policy is displayed.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
2. Click on the Webtop link (for example, OWA in the screen above). The resource page is displayed for the user to provide credentials for the exchange server.

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

DNS and NTP Settings on the BIG-IP System

For BIG-IP APM, you must have DNS and NTP settings configured. To configure these settings, use the following procedures.

**Configuring DNS**

Configure DNS on the BIG-IP system to point to the corporate DNS server. DNS lookups go out over one of the interfaces configured on the BIG-IP system, not the management interface. The management interface has its own separate DNS configuration.

The BIG-IP system must have a route to the DNS server. The Route configuration is done on the Main tab. Expand Network and then click Routes. For specific instructions on configuring a route on the BIG-IP system, see the BIG-IP online help or documentation.

1. On the Main tab, click System > Configuration.
2. On the Device menu, click DNS.
3. In the Address field, in the DNS Lookup Server List row, enter the IP address of the DNS server.
4. Click Add.
5. Click Update.

**Configuring NTP**

For authentication to work properly, you must configure NTP on the BIG-IP system.

1. On the Main tab, click System > Configuration.
2. On the Device menu, click NTP.
3. In the Address field, enter the fully-qualified domain name (or the IP address) of the time server that you want to add to the Address List.
4. Click Add.
5. Click Update.
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>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>