SafeNet Authentication Manager
Integration Guide

Using SafeNet Authentication Manager as an Identity Provider for F5 BIG-IP Access Policy Manager
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Document Part Number:** 007-012671-001, Rev. B  
**Release Date:** October 2016
# Contents

Third-Party Software Acknowledgement .................................................................................. 4
Description ............................................................................................................................... 4
Applicability .............................................................................................................................. 5
Environment ............................................................................................................................... 5
Audience .................................................................................................................................... 5
SAML Authentication using SafeNet Authentication Manager ............................................. 5
Authentication Flow using SafeNet Authentication Manager .................................................. 5
SAML Prerequisites .................................................................................................................. 6

Configuring SafeNet Authentication Manager ..................................................................... 6
  Synchronizing User Stores to SafeNet Authentication Manager ........................................... 7
  Assigning Tokens in SafeNet Authentication Manager ....................................................... 7
  Configuring SafeNet Authentication Manager as an Identity Provider ............................ 8
  Exporting the SafeNet Authentication Manager Certificate and Downloading Metadata .... 10
  Configuring SafeNet Authentication Manager for SAML-based User Federation ............. 11

Configuring F5 BIG-IP Access Policy Manager .................................................................. 14
  Accessing the F5 BIG-IP APM Management Portal ......................................................... 14
  Configuring BIG-IP APM as a Service Provider ............................................................... 15
  Configuring SafeNet Authentication Manager as an Identity Provider ............................ 16
  Associating an Identity Provider Connector with the Service Provider Service ................ 18
  Configuring the Webtop List ............................................................................................... 19
  Configuring the Webtop Links ............................................................................................ 21
  Configuring an Access Profile ............................................................................................ 22
  Modifying the Access Profile ............................................................................................. 22
  Adding SAML Authentication ............................................................................................. 23
  Adding a Webtop .................................................................................................................. 25
  Configuring the Virtual Server ........................................................................................... 26

Running the Solution ............................................................................................................... 30
  After Successful Authentication ....................................................................................... 31

Appendix: Configuring DNS and NTP on the BIG-IP System ............................................. 32
  Configuring DNS ................................................................................................................ 32
  Configuring NTP .................................................................................................................. 33

Support Contacts .................................................................................................................... 33
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third party software, such as F5 BIG-IP Access Policy 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.

Description

SafeNet Authentication Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

F5 BIG-IP Access Policy Manager (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 image above displays a sample access policy set in Access Policy Manager (APM). To increase the security of resources behind APM, features of APM are used along with the Security Assertion Markup Language (SAML) authentication from SafeNet Authentication Manager (SAM) to make resources available securely to the authenticated users.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in F5 BIG-IP Access Policy Manager using SafeNet tokens managed by SafeNet Authentication Manager.
- Configure SAML authentication in F5 BIG-IP Access Policy Manager using SafeNet Authentication Manager as an identity provider.
It is assumed that the F5 BIG-IP Access Policy Manager environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

F5 BIG-IP Access Policy Manager can be configured to support multi-factor authentication in several modes. The SAML authentication will be used for the purpose of working with SafeNet Authentication Manager.

**Applicability**

The information in this document applies to:

- **SafeNet Authentication Manager**—A server version of SAM 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 Manager—Version 8.2
- F5 BIG-IP Access Policy Manager—Version 12.0

**Audience**

This document is targeted to system administrators who are familiar with F5 BIG-IP Access Policy Manager, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Manager (SAM).

**SAML Authentication using SafeNet Authentication Manager**

SafeNet Authentication Manager (SAM) provides a SAML authentication option that is already implemented in the SAM environment and can be used without any installation.

**Authentication Flow using SafeNet Authentication Manager**

SafeNet Authentication Manager (SAM) communicates with a large number of service providers and cloud-based services solutions using the SAML protocol.
The image below describes the dataflow of a multi-factor authentication transaction for F5 BIG-IP Access Policy Manager.

1. A user attempts to log on to F5 BIG-IP Access Policy Manager. The user is redirected to SafeNet Authentication Manager (SAM). SAM collects and evaluates the user's credentials.
2. SAM returns a response to F5 BIG-IP Access Policy Manager, accepting or rejecting the user's authentication request.

**SAML Prerequisites**

To enable SafeNet Authentication Manager (SAM) to receive SAML authentication requests from F5 BIG-IP Access Policy Manager, ensure the following:

- SAM should be installed and configured.
- 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.
- SAM must be reachable from BIG-IP.
- A user must have a token enrolled with SAM (for example, **OTP token**).
- BIG-IP APM and SAM are up and running, and a user has an Administrator and Operator account on APM and SAM, respectively.
- To successfully perform the instructions provided in this guide, you need the following:
  - SafeNet Authentication Manager—Version 8.2
  - F5 BIG-IP APM version—Version 12.0

**Configuring SafeNet Authentication Manager**

Using SafeNet Authentication Manager (SAM) as an identity provider for F5 BIG-IP Access Policy Manager requires the following:

- Synchronizing User Stores to SafeNet Authentication Manager, page 7
- Assigning Tokens in SafeNet Authentication Manager, page 7
Synchronizing User Stores to SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) manages and maintains tokens information in its data store, including the tokens status and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Assigning Tokens in SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) supports a number of token methods that can be used as a second authentication factor for users authenticating through F5 BIG-IP Access Policy Manager.

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- SafeNet GOLD
- SMS tokens
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)
- SafeNet eToken 3400
- SafeNet eToken 3500
Tokens can be assigned to users as follows:

- **SAM Management Center**—Management site used by SAM administrators and helpdesk personnel for token enrollment and lifecycle management.
- **SAM Self-Service Center**—Self-service site used by end users for managing their tokens.
- **SAM Remote Service**—Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet’s tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

### Configuring SafeNet Authentication Manager as an Identity Provider

To use F5 BIG-IP Access Policy Manager as a service provider and SafeNet Authentication Manager (SAM) as an identity provider, SAM must be configured as an identity provider.

1. From the Windows **Start** menu, click **Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
2. Click the **Action** tab and then click **Cloud Configuration**.

3. On the **Info for Service Provider** tab, in the **Domain URL** field, enter the web address of the SAM portal server.

   ![Cloud Settings](image)

   The remaining fields are generated according to the Domain URL that was entered.
4. Click OK.

Exporting the SafeNet Authentication Manager Certificate and Downloading Metadata

SafeNet Authentication Manager’s certificate is shared between SAM and F5 BIG-IP Access Policy Manager. The certificate will be used to sign the authentication requests.

1. From the Windows Start menu, click Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager.

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

2. Click the Action tab, and then click Cloud Configuration.
3. On the **Info for Service Provider** tab, perform the following steps:
   a. Click **Export Certificate** and save the certificate file. The certificate file will be imported into F5 BIG-IP Access Policy Manager later.
   b. Click **Download Metadata** for Downloading Metadata and save it. This metadata will be imported into F5 BIG-IP Access Policy Manager later.
   c. Copy the values of the **Sign-in page URL**, **Sign-out page URL**, and **Change password URL** fields, and then save them in a text file. These URLs will be required while configuring F5 BIG-IP Access Policy Manager.

4. Click **OK**.

### Configuring SafeNet Authentication Manager for SAML-based User Federation

SafeNet Authentication Manager’s Token Policy Object (TPO) policies include application authentication settings for SAML service providers. These settings are used by SAM’s portal to communicate with service providers.

For general portal configuration, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

**To edit the TPO for SAM’s portal configuration:**

1. Open the **Token Policy Object Editor** for the appropriate group. See the *SafeNet Authentication Manager 8.2 Administrator’s Guide* for more information.
2. In the left pane, click **Protected Application Settings > User Authentication**.

![Screen image of Protected Application Settings](image1)

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

3. In the right pane, double-click **Application Authentication Settings**.

4. On the **Application Authentication Settings Properties** window, perform the following steps:
   a. Select **Define this policy setting**.
   b. Select **Enabled**.
   c. Click **Definitions**.

![Screen image of Application Authentication Settings Properties](image2)

*(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)*
5. On the Application Authentication Settings window, in the left pane, right-click Application Authentication Settings, and then select Create a new profile.

6. Right-click the new profile, and then rename it to a user-friendly name.

7. Click the new profile.

8. In the right pane, double-click on the following policies, and enter the appropriate information:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Issuer</td>
<td>Enter the virtual server address or entity ID. The value should be the F5 BIG-IP virtual server URL.</td>
</tr>
<tr>
<td>SAM issuer</td>
<td>Enter entity ID of the SAM as SAM issuer (Entity ID in Metadata of SAM)</td>
</tr>
<tr>
<td>Application’s login URL</td>
<td>Enter https://&lt;F5 virtual server&gt;/saml/sp/profile/post/sls.</td>
</tr>
</tbody>
</table>


The following is an example of the completed policy settings in the Application Authentication Settings window:

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
10. Click OK until all of the Token Policy Object Editor windows are closed.

Configuring F5 BIG-IP Access Policy Manager

Add SafeNet Authentication Manager (SAM) as an Identity Provider in F5 BIG-IP Access Policy Manager.

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 as the SAML service provider, with external identity provider connectors, an access profile, a Webtop, and the virtual server.

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

Accessing the F5 BIG-IP APM Management Portal

1. In a web browser, open the DNS/Public IP of the BIG-IP APM Amazon instance.
2. On the login window, enter the administrator login credentials, and then click Log in.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
After the successful authentication, you will be logged in to the F5 BIG-IP APM 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.

1. On the management portal console, 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, in the left pane, click General Settings, and then in the right pane, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the service provider (for example, SAMasIDP).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity ID</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 SafeNet Authentication Manager as an Identity Provider

The BIG-IP system is used as the SAML service provider. It sends authentication requests to SafeNet Authentication Manager (an identity provider) and, in turn, receives assertions from SAM.

To configure SAM as an Identity Provider:

1. On the management portal console, 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.

![Image of External IdP Connectors tab](image-url)

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

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

You create an identity provider from metadata that you downloaded in step 3 (b) of “Exporting the SafeNet Authentication Manager Certificate and Downloading Metadata” on page 10.

![Image of Create New SAML IdP Connector](image-url)

*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>Select File</td>
<td>Enter the path of the downloaded metadata file.</td>
</tr>
<tr>
<td>Identity Provider Name</td>
<td>Enter an appropriate name for the identity provider.</td>
</tr>
</tbody>
</table>

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

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

![External Identity Provider Connector](image)

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

**Associating an Identity Provider Connector with the Service Provider Service**

Bind the Identity Provider Connector with the Service Provider service.

1. On the management portal console, click **Main > Access Policy > SAML > BIG-IP as SP**.
2. On the **Local SP Services** tab, select the SP service (for example, **SAMsiDP**) that you created earlier in step 3 of “Configuring BIG-IP APM as a Service Provider” on page 15, and then click **Bind/Unbind IdP Connectors**.

![Local SP Services](image)

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
3. On the **Edit SAML IDP’s that use this SP** window, click **Add New Row**.

   ![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.)*

4. In the **SAML IdP Connectors** column, select the Identity Provider Connector (for example, `/Common/SAM`).

   ![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**.

6. Click **OK**.

**Configuring the Webtop List**

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.
1. On the management portal console, click **Main > Access Policy > Webtops > Webtop List.**

![Access Policy](image1)

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

2. On the right corner of the screen, click **Create.**

3. Complete the following fields, and then click **Finished.**

<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>

![Access Policy](image2)

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

Webtop links are the links to the resources that are added to the Webtop.

After successful SAML authentication, the links to the resources will be displayed on the assigned Webtop.

1. On the management portal console, click **Main > Access Policy > Webtops > Webtop Links**.
2. On the right corner of the screen, click **Create**.
3. Complete the following fields, and then click **Finished**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the Webtop link (for example, Rupiwebtop).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Type a description for this link.</td>
</tr>
<tr>
<td>Link Type</td>
<td>Select either Application URI or Hosted Contents. For example, if your resource is an application, select Application URI.</td>
</tr>
<tr>
<td>Application URI</td>
<td>Enter the application URL. This field is available only when Application URI is selected as the Link Type.</td>
</tr>
<tr>
<td>Hosted File</td>
<td>Enter the hosted file name. This field is available for only when Link Type is selected as Hosted Contents.</td>
</tr>
<tr>
<td>Caption</td>
<td>Enter the caption. By default, the caption is same as the Webtop link name, but you can modify it as per your preferred configuration.</td>
</tr>
</tbody>
</table>

(4) Click **Finished**.
Configuring an Access Profile

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

1. Click **Access Policy > Access Profiles**.
2. Under **General Properties**, complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the profile (for example, <strong>SAM_SAML_Profile</strong>).</td>
</tr>
<tr>
<td>Profile Type</td>
<td>Select <strong>All</strong>.</td>
</tr>
</tbody>
</table>

![General Properties](image)

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

3. Under **Language Settings**, in the **Factory Builtin Languages** list, select a language, 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**.

Modifying 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.
Below is the structure of a sample Access Policy.

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

1. On the management portal console, on the **Main** tab, click **Access Policy > Access Profiles**.

2. On the **Access Profile List** tab, search for the Access Policy you want to modify, and then in the **Access Policy** column, click **Edit** for the Access Policy.

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

The Visual Policy editor is displayed. This is the new blank policy that you have just created.

3. On the Visual Policy editor, on a rule branch of the Access Policy, click the + icon to add an action.

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

4. The **Add Item** window is displayed. Click the + symbol to add **SAML authentication** and **Webtop assignment**.

**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:

1. On the visual policy editor, click the + icon 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**.

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

3. On the **Properties** tab, in the **AAA Server** field, select the configured SAML service provider (for example, /Common/SAMasIDP).

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

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. On the Visual Policy editor, click the + icon in the Successful branch of SAML Auth.

   ![Visual Policy Editor](image)

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

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

   ![Assignment Tab](image)

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


   ![Properties Tab](image)

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

5. Click the **Webtop Links** tab, and then select the webtop link from the list.

![Webtop Links](image)

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

6. Click the **Webtop** tab, and then select a webtop from the list, and then click **Update**.

![Webtop](image)

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

7. Click **Save**.

![Save](image)

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

**Configuring the Virtual Server**

When using BIG-IP APM, virtual servers are configured with specific settings for the 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.
1. On the management portal console, on the **Main** tab, click **Local Traffic > Virtual Servers**.

   ![Management Portal Console Screenshot](image1)

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

2. Click **Create**.

3. Under **General Properties**, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the virtual server.</td>
</tr>
<tr>
<td><strong>Destination Address/Mask</strong></td>
<td>Enter the host IP address of the virtual server.</td>
</tr>
<tr>
<td><strong>Service Port</strong></td>
<td>Select HTTPS.</td>
</tr>
</tbody>
</table>

   ![General Properties Screenshot](image2)

   *(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)*
4. Under **Configuration**, complete the following fields:

<table>
<thead>
<tr>
<th>HTTP Profile</th>
<th>Select HTTP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Profile (Client)</td>
<td>Select the client SSL profile to use with this virtual server.</td>
</tr>
<tr>
<td>SSL Profile (Server)</td>
<td>If your web application server is using HTTPS services, select the server SSL profile to use with this virtual server.</td>
</tr>
</tbody>
</table>

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
5. Under **Access Policy**, complete the following fields:

<table>
<thead>
<tr>
<th><strong>Access Profile</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connectivity Profile</strong></td>
<td>If you are creating a virtual server to use with web applications, select the Connectivity profile.</td>
</tr>
</tbody>
</table>

6. **Click Finished.**
Running the Solution

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

If you have an enrolled token (for example, **OTP Token**), browse to the virtual server. You will be redirected to the SAM portal for login. Provide the login credentials for SAML authentication.

Proceed according to the steps configured in the Access Policy.

In the steps below, the SafeNet eToken 3400 is used as the enrolled OTP token.

1. Browse to the local traffic virtual server configured in APM.
2. On the **User Identification** window, enter your username, select the security level, and then click **OK**.

3. On the eToken 3400, click **PRESS**. An OTP is generated by the token.
4. In the web browser, on the **OTP Authentication** window, in the **OTP Authentication Code** field, enter the generated OTP, and then click **OK**.

### 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.

*(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)*
On successful SAML authentication, the Webtop assigned in the Access Policy is displayed. Click on the Webtop link (for example, Safenet Page).

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

The resource page is displayed for the user.

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

Appendix: Configuring DNS and NTP on the BIG-IP System

For BIG-IP APM, you need to configure the DNS and NTP.

**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 Gemalto Customer Support. Gemalto 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 Gemalto 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>
</table>
| **Address**                    | Gemalto  
4690 Millennium Drive  
Belcamp, Maryland  21017 USA |
| **Phone**                      | United States  
1-800-545-6608  
International  
1-410-931-7520 |
Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base. |