SafeNet Authentication Manager
Integration Guide

Using RADIUS Protocol 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: 007-012607-001, Rev. B
Release Date: November 2016
Contents

Third-Party Software Acknowledgement ........................................................................................................... 4
Description .......................................................................................................................................................... 4
Applicability ..................................................................................................................................................... 5
Environment .................................................................................................................................................... 5
Audience ........................................................................................................................................................... 5
RADIUS-based Authentication using SafeNet Authentication Manager .......................................................... 5
RADIUS Authentication Flow using SafeNet Authentication Manager .......................................................... 6
RADIUS Prerequisites ..................................................................................................................................... 6
Configuring SafeNet Authentication Manager ................................................................................................. 7
  Synchronizing Users Stores to SafeNet Authentication Manager ................................................................. 7
  Configuring SafeNet Authentication Manager’s Connector for OTP Authentication .............................. 8
  Assigning a Token in SafeNet Authentication Manager ............................................................................. 8
  Adding F5 BIG-IP Access Policy Manager as a RADIUS Client in IAS/NPS ............................................. 9
  Configuring SafeNet Authentication Manager’s OTP Plug-In for Microsoft RADIUS Client .................. 10
Configuring F5 BIG-IP Access Policy Manager ............................................................................................. 11
  Accessing the F5 BIG-IP APM Management Portal ................................................................................. 11
  Configuring the RADIUS Server ................................................................................................................ 12
  Configuring a Webtop .................................................................................................................................... 14
  Configuring the Webtop Links ....................................................................................................................... 15
  Creating an Access Profile ........................................................................................................................... 16
  Configuring the Access Profile .................................................................................................................... 17
  Configuring the Virtual Server .................................................................................................................... 24
Running the Solution ....................................................................................................................................... 27
  After Successful Authentication .................................................................................................................. 28
Appendix: Configuring DNS and NTP on the BIG-IP System ....................................................................... 29
  Configuring DNS ......................................................................................................................................... 29
  Configuring NTP ......................................................................................................................................... 29
Support Contacts .............................................................................................................................................. 30
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 screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)

This document describes how to:

- Deploy multi-factor authentication (MFA) options in F5 BIG-IP Access Policy Manager using SafeNet one-time password (OTP) tokens managed by SafeNet Authentication Manager.
- Configure F5 BIG-IP Access Policy Manager to work with SafeNet Authentication Manager in RADIUS mode.

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, and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager installation modes, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.
F5 BIG-IP Access Policy Manager can be configured to support multi-factor authentication in several modes. RADIUS protocol 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 8.2 HF 493**—A server version of SAM that is used to deploy the solution on-premises in the organization.
- **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).

RADIUS-based Authentication using SafeNet Authentication Manager

SafeNet’s OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SafeNet Authentication Manager (SAM).

SAM’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS, providing strong authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*. 
RADIUS Authentication Flow using SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the dataflow of a multi-factor authentication transaction for F5 BIG-IP Access Policy Manager.

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, a login screen appears. The user enters the login credentials. On successful RADIUS authentication, the user is granted access to the predefined resources.

1. A user enters the user name and token code on the login screen of the virtual server.
2. The Access Policy set for the virtual server on APM is checked for the next operation.
3. The credentials are passed on to the SAM server for RADIUS authentication.
4. After successful authentication, the user is granted access to a Webtop with predefined resources.

The user can click on the desired Webtop links to access resources.

RADIUS Prerequisites

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

- End users can authenticate from the F5 BIG-IP Access Policy Manager environment with a static password before configuring the F5 BIG-IP Access Policy Manager to use RADIUS authentication.
- Ports 1812/1813 are open to and from F5 BIG-IP Access Policy Manager.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.
- 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.
• NPS/RADIUS server 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.

The instructions provided in this guide have been tested in the following environments:
- SafeNet Authentication Manager version 8.2 on a publicly accessible machine.
- F5 BIG-IP APM version 12.0 on Amazon Cloud.

Configuring SafeNet Authentication Manager

The deployment of multi-factor authentication using SafeNet Authentication Manager with BIG-IP APM using the RADIUS protocol requires the following:
- Synchronizing Users Stores to SafeNet Authentication Manager, page 7
- Configuring SafeNet Authentication Manager’s Connector for OTP Authentication, page 8
- Assigning a Token in SafeNet Authentication Manager, page 4
- Adding F5 BIG-IP Access Policy Manager as a RADIUS Client in IAS/NPS, page 9
- Configuring SafeNet Authentication Manager’s OTP Plug-In for Microsoft RADIUS Client, page 10

Synchronizing Users Stores to SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, 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
Configuring SafeNet Authentication Manager’s Connector for OTP Authentication

SafeNet Authentication Manager (SAM) is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications, including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected the Simplified OTP-only configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The Simplified OTP-only configuration is as follows:

- **Connectors**—SAM Connector for OTP Authentication is installed
- **SAM Back-end Service**—Activated on this server; scheduled to operate every 24 hours

In addition, the SAM default policy is set as follows:

- OTP support (required for OTP) is selected in the Token Initialization settings.
- The SAM Connector for OTP Authentication is set, by default, to enable enrollment of OTP tokens without requiring changes in the Token Policy Object (TPO) settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

Assigning a Token in SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) supports a number of OTP authentication 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.

Adding F5 BIG-IP Access Policy Manager as a RADIUS Client in IAS/NPS

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in BIG-IP APM.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in BIG-IP APM.

BIG-IP APM must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize BIG-IP APM for authentication.

**NOTE:** This document assumes that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager (SAM).

The details below refer to NPS, and are very similar to IAS.

2. On the Network Policy Server web console, expand RADIUS Clients and Servers, right-click RADIUS Clients, and then click New.

![Network Policy Server](image)

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

3. On the New RADIUS Client window, on the Settings tab, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable this RADIUS client</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Friendly name</td>
<td>Enter a friendly name for the RADIUS server.</td>
</tr>
<tr>
<td>Address (IP or DNS)</td>
<td>Enter the IP address or DNS of BIG-IP APM.</td>
</tr>
</tbody>
</table>
### Shared secret
Enter the shared secret for the RADIUS client. This entry must match the shared secret that was used when the RADIUS server was configured in BIG-IP APM.

### Confirm shared secret
Re-enter the shared secret.

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

4. Click **OK**.

   BIG-IP APM is added as a RADIUS client in NPS.

### Configuring SafeNet Authentication Manager’s OTP Plug-In for Microsoft RADIUS Client

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) as Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

SafeNet Authentication Manager’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*. 
Configuring 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 the RADIUS server, access profile, Webtop, and the virtual server.

**NOTE:** If the virtual server and Webtop are already configured on BIG-IP APM, skip the configuration steps for the virtual server and Webtop. Configure the RADIUS server and edit the Access Profile accordingly.

Configuring F5 BIG-IP Access Policy Manager for the simple mode requires:

- Accessing the F5 BIG-IP APM Management Portal, page 11
- Configuring the RADIUS Server, page 12
- Configuring a Webtop, page 14
- Configuring the Webtop Links, page 15
- Creating an Access Profile, page 16
- Configuring the Access Profile, page 17
- Adding RADIUS Authentication, page 21
- Configuring the Virtual Server, page 24

**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.

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

Configuring the RADIUS Server

RADIUS authentication allows you to authenticate and authorize your users to access their resources through a RADIUS server that you configure in the Access Policy Manager.

NOTE: Ensure that the RADIUS server is configured to recognize the Access Policy Manager as a client. Use the same shared secret in both the RADIUS server configuration and in the Access Policy Manager configuration.

1. On the management portal console, on the Main tab, click Access Policy > AAA Servers > RADIUS, and then click the icon.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
2. Complete the following fields, and then click **Finished**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the RADIUS server. For example, (SAM_OWA_Policy_aa_srv).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Select <strong>Authentication</strong>.</td>
</tr>
<tr>
<td>Server Connection</td>
<td>If you have a single RADIUS server, select <strong>Direct</strong>, else, select <strong>Use Pool</strong>.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Enter the IP address of the RADIUS server (IP of NPS server).</td>
</tr>
<tr>
<td>Authentication Service Port</td>
<td>Enter the authentication service port. The NPS server works on the default port number <strong>1645</strong>.</td>
</tr>
<tr>
<td>Secret</td>
<td>Enter the shared secret for the RADIUS server.</td>
</tr>
<tr>
<td>Confirm Secret</td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>

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

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

1. On the management portal console, on the Main tab, click Access Policy > Webops > Webtop List, and then click the icon.

2. 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 Full.</td>
</tr>
</tbody>
</table>
Configuring the Webtop Links

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

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

1. On the management portal console, on the Main tab, click Access Policy > Webtops > Webtop Links, and then click the icon.

![Image of the management portal console with the Webtops menu selected.](image)

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

2. Complete the following fields, and then click Finished.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the Webtop link (for example, Rupiwebtop).</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the link.</td>
</tr>
<tr>
<td>Link Type</td>
<td>Select either Application URL or Hosted Contents. For example, if your</td>
</tr>
<tr>
<td></td>
<td>resource is an application, select Application URL.</td>
</tr>
<tr>
<td>Application URI</td>
<td>Enter the URL of the application. This field is available only when Application URI is selected as the Link Type.</td>
</tr>
<tr>
<td>Hosted File</td>
<td>Specify the hosted file name. This field is available only when Hosted Contents is selected as the Link Type.</td>
</tr>
</tbody>
</table>
Creating an Access Profile

The 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. On the management portal console, on the Main tab, click Access Policy > Access Profiles > Access Profiles List, and then click the icon.

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

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

(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 << to move the selected language to the **Accepted Languages** list.

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

4. Click **Finished**.

**Configuring 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 Policy can be edited as per the requirements.

The following is a sample Access Policy:

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

- Viewing Access Policy, page 18
- Editing the Access Profile, page 19
- Adding a Logon Page, page 20
- Adding RADIUS Authentication, page 21

**Viewing Access Policy**

Another way to view the AAA (Authentication, Authorization, and Accounting) servers and resources assigned in an Access Policy can be as follows:

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

2. On the **Access Profile List** tab, in the **Name** column, click the access profile (for example, **SAM_OWA_Policy**) that you created earlier in step 2 of “Creating an Access Profile” on page 16.

3. Click the **Access Policy** tab.

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

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

2. On the **Access Profile List** tab, in the **Access Policy** column, click **Edit** for the Access Policy (for example, **SAM_OWA_Policy**) that you want to edit.

3. On the Visual Policy editor, on a rule branch of the Access Policy, click the **+** icon to add an actions, such as, logon page, RADIUS authentication, and Webtop assignments.
Adding a Logon Page

The first page for a user will be a logon page where they will enter their username and password. To add a logon page on the local traffic virtual server, perform the following steps:

1. In 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 Logon tab, select Logon Page, 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 Name field, enter a name for the logon page.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
4. Under **Customization**, perform the following steps:
   a. In the **Language** field, select a language.
   b. In the **Form Header Text** field, edit the header text as per your preferred configuration.
   c. Enter names for the input fields as per your preferred configuration.

5. Click **Save**.

**Adding RADIUS Authentication**

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

For server authentication, the following two Access Policy items are required to be added in the following order:
- Logon page action
- AAA server action

The logon page action presents a user with a logon page with customizable fields and text. When the user specifies credentials (for example, a user name and a password), these credentials are passed to the specified AAA server in the AAA server action. If a user is successfully authenticated, the user continues on the Successful branch. A user who is not successfully authenticated continues on the Fallback branch.

Adding RADIUS authentication requires:
- Adding RADIUS Authentication after the Logon Page, page 21
- Adding a Webtop, page 23

**Adding RADIUS Authentication after the Logon Page**

1. On the **Visual Policy** editor, click the + icon after the **Logon Page**.

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

![Screen Image](image1.png)

*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 RADIUS server (for example, `SAM_OWA_Policy_aa_srv`).

![Screen Image](image2.png)

*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, the user is presented with a Webtop containing customized resources.

1. On the **Visual Policy** editor, click the **+** icon in the **Successful** branch of **RADIUS Auth**.

   (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**.

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

3. On the **Properties** tab, under **Resource Assignment**, click **Add new entry**, and then under **Expression**, click **Add/Delete**.

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

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

   (The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
5. Click the **Webtop** tab, select a webtop from the list, and then click **Update**.

![Webtop tab screenshot](Image)

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

6. The **Resource Assignment** window becomes active. 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.

1. On the management portal console, on the **Main** tab, click **Local Traffic > Virtual Servers > Virtual Server List**, and then click the **Virtual Servers** icon.

![Virtual Server List screenshot](Image)

*(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)*
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 virtual server.</td>
</tr>
<tr>
<td>Destination Address/Mask</td>
<td>Enter the host IP address of the virtual server.</td>
</tr>
<tr>
<td>Service Port</td>
<td>Select <strong>HTTPS</strong>.</td>
</tr>
</tbody>
</table>

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

3. Under **Configuration**, complete the following fields:

<table>
<thead>
<tr>
<th>Profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Profile</td>
<td>Select <strong>HTTP</strong>.</td>
</tr>
<tr>
<td>SSL Profile (Client)</td>
<td>Select the client SSL profile to use it 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 it 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.)
4. Under **Access Policy**, complete the following fields:

<table>
<thead>
<tr>
<th><strong>Access Profile</strong></th>
<th>Select the access profile to associate it with the 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 it with web applications, select the connectivity profile.</td>
</tr>
</tbody>
</table>

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

5. Click **Finished**.

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

Once the BIG-IP local traffic virtual server is configured with an appropriate Access Policy, and a corresponding RADIUS client is added in SafeNet Authentication Manager (SAM), the administrator provides users with the address of BIG-IP local traffic virtual server.

If you have an enrolled token (for example, OTP token), browse to the virtual server, and then on the login window, enter the username and token code.

Proceed according to the steps configured in the Access Policy.

In the below steps, 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 login window, in the Username field, enter your username.

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

3. On the eToken 3400, click PRESS. The token generates an OTP.

4. On the login window, in the Password field, enter the generated OTP, and then click Logon. The credentials are passed to the RADIUS server for authentication.
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.

![Access Policy Diagram](image)

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

On successful RADIUS authentication, the Webtop assigned in the Access Policy is displayed. Click on the Webtop link (for example, Safenet Page).

![Webtop Page](image)

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

The resource page is displayed.

![Resource Page](image)

(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>
<tbody>
<tr>
<td>Address</td>
<td>Gemalto</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>
</tbody>
</table>
|                           | 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.