SafeNet Authentication Service 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: 007-013607-001, Rev. A
Release Date: September 2016
Contents

Third-Party Software Acknowledgement ................................................................. 4
Description .................................................................................................................. 4
Applicability .................................................................................................................. 4
Environment .................................................................................................................. 5
Audience ....................................................................................................................... 5
RADIUS-based Authentication using SafeNet Authentication Service Cloud ............... 5
RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE .......................................................... 6
RADIUS Authentication Flow using SafeNet Authentication Service ......................... 6
RADIUS Prerequisites ............................................................................................... 7
Configuring SafeNet Authentication Service .............................................................. 7
  Creating Users Stores in SafeNet Authentication Service ........................................... 7
  Assigning an Authenticator in SafeNet Authentication Service ............................... 8
  Adding F5 BIG-IP Access Policy Manager as an Authentication Node in SafeNet Authentication Service .................................................. 8
  Checking the SafeNet Authentication Service RADIUS Address ........................... 10
Configuring F5 BIG-IP Access Policy Manager ......................................................... 12
  Accessing the F5 BIG-IP APM Management Portal ............................................... 12
  Configuring the RADIUS Server ............................................................................ 13
  Creating a Webtop .................................................................................................. 15
  Configuring the Webtop Links ............................................................................... 16
  Creating an Access Profile ..................................................................................... 17
  Configuring the Access Profile ............................................................................. 18
  Configuring the Virtual Server ............................................................................. 25
Running the Solution .................................................................................................. 28
Appendix A: Configuring DNS and NTP on the BIG-IP System ................................ 29
Appendix B: Modifying the Login Page for a GrIdsure Token ................................... 30
Support Contacts ....................................................................................................... 35
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 Service (SAS) delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

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, F5 BIG-IP APM helps you free up valuable IT resources and scale cost-effectively.

F5 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.

This document describes how to:

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

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

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet’s cloud-based authentication service
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by Service Providers to deploy instances of SafeNet Authentication Service
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version 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 Service – Private Cloud Edition (SAS-PCE)**
- **F5 BIG-IP Access Policy Manager—Version 12.0**
- **Exchange Server 2010** (OWA or any resource configured and running)

**NOTE:** This Guide is applicable for both BIG-IP VE and BIG-IP hardware appliance.

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 Service (SAS).

RADIUS-based Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (SAS) Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.

  ![RADIUS Protocol](image)

- **Local RADIUS hosted on-premises**—A RADIUS agent that is implemented in the existing customer’s RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.

  ![RADIUS Protocol](image)
This document demonstrates the solution using the SAS cloud hosted RADIUS service.

For more information on how to install and configure SAS Agent for IAS/NPS, refer to:

For more details on how to install and configure FreeRADIUS, refer to the SafeNet Authentication Service FreeRADIUS Agent Configuration Guide.

**RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE**

For both on-premises versions, SafeNet Authentication Service (SAS) can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS) or the legacy Microsoft Internet Authentication Service (MS-IAS)**—SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.

  For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to the following document:

- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

**RADIUS Authentication Flow using SafeNet Authentication Service**

SafeNet Authentication Service communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the data flow 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 using an OTP authenticator.
2. F5 BIG-IP Access Policy Manager sends a RADIUS request with the user’s credentials to SafeNet Authentication Service (SAS) for validation.
3. The SAS authentication reply is sent back to the F5 BIG-IP Access Policy Manager.
4. The user is granted or denied access to the F5 BIG-IP Access Policy Manager based on the OTP value calculation results from SAS.

**RADIUS Prerequisites**

To enable SafeNet Authentication Service (SAS) 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.

**Configuring SafeNet Authentication Service**

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with F5 BIG-IP Access Policy Manager using RADIUS protocol requires the following:

- Creating Users Stores in SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 8
- Adding F5 BIG-IP Access Policy Manager as an Authentication Node in SafeNet Authentication Service, page 8
- Checking the SafeNet Authentication Service RADIUS Address, page 10

**Creating Users Stores in SafeNet Authentication Service**

Before SafeNet Authentication Service (SAS) can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

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

For additional details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.
Assigning an Authenticator in SafeNet Authentication Service

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

The following authenticators are supported:
- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet Gold
- SMS Token
- MP-1 Software Token
- MobilePASS
- GrIDsure Authentication

Authenticators can be assigned to users in two ways:
- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.


Adding F5 BIG-IP Access Policy Manager as an Authentication Node in SafeNet Authentication Service

Add a RADIUS entry in the SafeNet Authentication Service (SAS) **Auth Nodes** module to prepare it to receive RADIUS authentication requests from F5 BIG-IP Access Policy Manager. You will need the IP address of F5 BIG-IP Access Policy Manager and the shared secret to be used by both SAS and F5 BIG-IP Access Policy Manager.
1. Log in to the SAS console with an Operator account.

2. Click the COMMS tab and then select Auth Nodes.

3. In the Auth Nodes module, click the Auth Nodes link.

4. Under Auth Nodes, click Add.
5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent Description</strong></td>
<td>Enter a description of the agent (for example, <strong>BIG-IP RADIUS Agent</strong>).</td>
</tr>
<tr>
<td><strong>Host Name</strong></td>
<td>Enter the IP address of the BIG-IP server.</td>
</tr>
<tr>
<td><strong>Low IP Address In Range</strong></td>
<td>Enter value in this field only if there is a pool of IP addresses. Otherwise, enter the same IP address as specified in the <strong>Host Name</strong> field.</td>
</tr>
<tr>
<td><strong>High IP Address In Range</strong></td>
<td>Enter value in this field if there is a pool of IP addresses. Otherwise, enter the same IP address as specified in the <strong>Host Name</strong> field.</td>
</tr>
<tr>
<td><strong>Exclude from PIN change requests</strong></td>
<td>Do not select anything.</td>
</tr>
<tr>
<td><strong>Configure FreeRADIUS Synchronization</strong></td>
<td>Select this option.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td><strong>Confirm Shared Secret</strong></td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>

The authentication node is added to the system.

**Checking the SafeNet Authentication Service RADIUS Address**

Before adding SafeNet Authentication Service (SAS) as a RADIUS server in F5 BIG-IP Access Policy Manager, check its IP address. The IP address will then be added to F5 BIG-IP Access Policy Manager as a RADIUS server at a later stage.
1. Log in to the SAS console with an Operator account.

![SAS console interface](image1)

2. Click the COMMS tab, and then select Auth Nodes.

![SAS COMMS interface](image2)

3. In the Auth Nodes module, click the Auth Nodes link. The SAS RADIUS server details are displayed.

![SAS Auth Nodes interface](image3)
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 Policy, 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 12
- Configuring the RADIUS Server, page 13
• Creating a Webtop, page 15
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.

![Management Portal](image)

(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 APM as a client. Use the same shared secret in both the RADIUS server configuration and in the APM configuration.

1. On the management portal console, on the **Main** tab, click **Access Policy > AAA Server > RADIUS**, and then click the ![icon](image).
2. Complete the following fields, and then click **Finished**.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the RADIUS server (for example, SAS_OWA_Policy_aa_srv).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
<td>Select <strong>Authentication</strong>.</td>
</tr>
<tr>
<td><strong>Server Connection</strong></td>
<td>If you have a single RADIUS server, select <strong>Direct</strong>, else, select <strong>Use Pool</strong>.</td>
</tr>
<tr>
<td><strong>Server Address</strong></td>
<td>Enter the IP address of the RADIUS server, which can be found in the <strong>Auth nodes</strong> section on the <strong>COMMS</strong> tab of your SAS server.</td>
</tr>
<tr>
<td><strong>Authentication Service Port</strong></td>
<td>Enter the authentication service port. SAS works on the default port number 1812.</td>
</tr>
<tr>
<td><strong>Secret</strong></td>
<td>Enter a shared secret for the RADIUS server.</td>
</tr>
<tr>
<td><strong>Confirm Secret</strong></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.)
Creating 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 > Webtops > Webtop List**, and then click the [icon.

![Access Policy screenshot](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>Name</th>
<th>Enter a name for the Webtop.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Full.</td>
</tr>
</tbody>
</table>

![Webtop configuration settings](image)

*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, such as Rupiwebtop, 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.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the Webtop link.</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 URL or Hosted Contents. For example, if your 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 URL 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>
<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>

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
Creating 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. On the management portal console, on the Main tab, click **Access Policy > Access Profiles > Access Profiles List**, and then click the icon.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the profile (for example, SAS_OWA_Policy).</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.

   ![Language Settings](image)

   *(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 requirements.

The following is a sample Access Policy:

![Access Policy](image)

*(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 19
• Editing the Access Profile, page 20
- Adding a Logon Page, page 21
- Adding RADIUS Authentication, page 22
Viewing Access Policy

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


2. On the Access Profile List tab, in the Name column, click the access profile (for example, SAS_OWA_Policy) that you created earlier in step 2 of "Creating an Access Profile" on page 17.

3. Click the Access Policy tab.
Editing the Access Profile

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

![Access Policy](image)

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

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

![Access Profile](image)

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

The Visual Policy editor is displayed.

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

   ![Start](image)

   *(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.

   ![Logon](image)

   *(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.

   ![Properties](image)

   *(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.

   ![Customization Image](image)

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

**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:

A logon page action and an 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, that 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 22
- Adding a Webtop, page 23

**Adding RADIUS Authentication after the Logon Page**

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

   ![Logon Page Image](image)

   *(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**.

(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, **SAS_OWA_Policy_aa_srv**), and then click **Save**.

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

**Adding a Webtop**

When a user is successfully authenticated, they are 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**.

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

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

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

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

   (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 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 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>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 HTTPS.</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>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Profile</td>
<td>Select HTTP.</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:

| Access Profile | 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. |
| Connectivity Profile | If you are creating a virtual server to use with web applications, select the connectivity profile. |

(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

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

To fetch a grid for the user, the administrator needs to configure several settings on the BIG-IP management portal. For these settings, refer to “Appendix B: Modifying the Login Page for a GrIDsure Token”, page 30.

When an administrator completes the configuration, the Get Grid button is displayed on the local traffic virtual server login screen.

1. Browse to the local traffic virtual server configured in APM.
2. On the login window, enter your username, and then click Get Grid.

3. In the Password field, enter your Personal Identification Pattern (PIP), and then click Logon. The credentials are forwarded to the RADIUS server for authentication.

4. After successful authentication with the RADIUS server, the Webtop assigned to the Access Policy is displayed. Click the Webtop (for example, Safenet Page).

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
Appendix A: 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, refer to 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.

Appendix B: Modifying the Login Page for a GrIDsure Token

If the user is assigned a GrIDSure token, the user needs to enter the selected grid pattern as the password. To fetch a grid for the user, the administrator needs to do some settings in the BIG-IP management portal.

Log in to BIG-IP as an administrator and perform the following steps so that a user having a GrIDsure token can log in to the virtual server.

Current authentication methods are created and applied to the access policy.

1. On the management portal console, on the Main tab, click Access Policy > Customization > Advanced.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
2. In the View field, select Advanced Customization, and then in the middle pane, under Customization Settings, expand Access Profiles.

![Customization Settings](image1)

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

3. Under Access Profiles, expand the access profile that you want to customize (for example, /Common/SAS_OWA_Policy).

![Access Profiles](image2)

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

4. Under the access profile (for example, /Common/SAS_OWA_Policy), click Access Policy > Logon Pages.

![Logon Pages](image3)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
5. Expand the Logon Page, and then double-click logon.inc.

6. Double-click logon.inc to open it and then perform the following steps to update the content:
   a. Search for the following line:
      ```
      <? include_customized_page("logout", "session_expired.js"); ?>
      ```
   b. Add the following content below the line mentioned above in step a:
      ```
      //------GrIDsure beginning-----
      var BlackShieldServerLocation = "Change to Org's Unique Self-Service URL from SAS";
      // BlackShieldServerLocation URL might look like the following:
      var form = document.getElementById(globalFormId); function getChallenge(userName){
      var challengeImg = document.getElementById("challengeImage");
      challengeImg.src = BlackShieldServerLocation + "+getChallengeImage=true&userName=" + userName + "+noCache=" + new Date().toString();
      var challengeDiv = document.getElementById("challengeImageDiv");
      challengeDiv.style.display="block"; challengeDiv.style.visibility="visible";
      }
      //------GrIDsure end------
      ```
   c. Search for the following content:
      ```
      <tr id="submit_row">
        <td class="credentials_table_unified_cell">
          <input type=submit class="credentials_input_submit" value="%[logon]">
        </td>
      </tr>
      ```
      ```
d. Replace the content mentioned above in step c with the following content:

  `<tr id="submit_row">
  <?
  if($GLOBALS["label_position"] == "above"){
  ?>
  <td class="credentials_table_unified_cell">
  <input type=submit class="credentials_input_submit" value="%[logon]">
  <input id="BSID_challengeButton" type="button" name="grid" value='Get Grid' title='Get Grid' onClick="getChallenge(form.input_1.value)">
  </td>
  <?
  }else{
  ?>
  <td class="credentials_table_label_cell"></td>
  <td class="credentials_table_field_cell">
  <input type=submit class="credentials_input_submit" value="%[logon]">$
  <input id="BSID_challengeButton" type="button" name="grid" value='Get Grid' title='Get Grid' onClick="getChallenge(form.input_1.value)">
  </td>
  <?}
  </tr>

f. Replace the content mentioned above in step e with the following content:

  }else{
  ?>
  <td class="credentials_table_label_cell"></td>
  <td class="credentials_table_field_cell">
  <input type=submit class="credentials_input_submit" value="%[logon]">$
  <input id="BSID_challengeButton" type="button" name="grid" value='Get Grid' title='Get Grid' onClick="getChallenge(form.input_1.value)">
  </td>
  <?}
  }
  ?>
  </tr>

g. Search for the following content:

  `<td colspan=2 id="credentials_table_footer">`
h. Replace the content mentioned above in step g with the following content:

```html
<td colspan=2 id="credentials_table_footer" >
<\/td>
```

```html
<div id="challengeImageDiv" style="visibility:hidden;display:none;"> <img id="challengeImage" src=""/></div>
</td>
```

```
</td>
```

i. Save the file.
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><strong>Address</strong></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><strong>Phone</strong></td>
<td>United States 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 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.