SafeNet Authentication Service
Push OTP Integration Guide
Using RADIUS Protocol for F5 BIG-IP APM
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.

© 2015 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. 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: 007-013348-001, Rev. A
Release Date: November 2015
Contents

Third-Party Software Acknowledgement ................................................................. 5
Description ............................................................................................................. 5
Applicability .......................................................................................................... 6
Environment .......................................................................................................... 6
Audience ................................................................................................................. 6
RADIUS-based Authentication using SAS Cloud .................................................. 6
RADIUS Authentication Flow using SAS ............................................................... 7
RADIUS Prerequisites ......................................................................................... 8
Push OTP Prerequisites ....................................................................................... 8
Configuring SafeNet Authentication Service ...................................................... 8
  Creating Users Stores in SAS ............................................................................. 8
  Assigning an Authenticator in SAS ................................................................. 9
  Adding F5 BIG-IP APM as an Authentication Node in SAS ......................... 9
Checking the SAS RADIUS Server’s IP Address .............................................. 11
Enabling the Software Token Push OTP Setting ............................................. 12
Enabling the Allowed Targets Policy ............................................................ 14
Configuring F5 BIG-IP APM ........................................................................... 16
  Configuring the Active Directory Server ..................................................... 18
  Configuring the RADIUS Server ................................................................. 19
  Creating a Webtop ......................................................................................... 21
  Configuring the Webtop Links ..................................................................... 22
Creating an Access Profile .............................................................................. 23
Editing the Access Profile .............................................................................. 23
Adding a Logon Page ...................................................................................... 25
Adding Active Directory Authentication ....................................................... 26
Adding RADIUS Authentication .................................................................. 28
Adding a Webtop ............................................................................................ 30
Configuring the Virtual Server .................................................................... 31
Running the Solution ....................................................................................... 34
  Running the Solution for Push OTP Tokens – Simple Mode ...................... 34
  Running the Solution for Push OTP Tokens – Hybrid Mode ....................... 37
Appendix ............................................................................................................. 41
  DNS and NTP Settings on the BIG-IP System ......................................... 41
Modifying Second Login Page for Push OTP Token .................................. 42
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 APM.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Service 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.

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.

This document describes how to:

- Configure F5 BIG-IP APM to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the F5 BIG-IP APM environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

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

The primary objective of the Push OTP solution is to reduce the friction around two-factor authentication, and provide users with an improved two-factor authentication experience.

It is likely that most users already own and always carry a device that can be used as a second factor of authentication. Using the mobile phone as an authenticator replaces the need for a user to carry any additional hardware. So, with Push OTP, a user can:

- Receive authentication requests in real-time via push notifications to his or her smart phone.
- Assess the validity of the request with the information displayed on the screen.
- Respond quickly with a one-tap response to approve or deny the authentication.
Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet’s cloud-based authentication service
- **MobilePASS+ application**

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service (SAS)**
- **F5 BIG-IP APM**—Version 11.4.1
- **Exchange Server 2010**

Audience

This document is targeted to system administrators who are familiar with F5 BIG-IP APM, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

RADIUS-based Authentication using SAS Cloud

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.

- **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.
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: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

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

**RADIUS Authentication Flow using SAS**

SafeNet Authentication Service 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 APM.

1. A user attempts to log on to F5 BIG-IP APM using a Push OTP authenticator.
2. F5 BIG-IP APM sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
3. SAS identifies the user or mobile device, and detects that the OTP field is empty. Then:
   - SAS will directly trigger a Push OTP authentication request.
   - The user receives a push notification on the configured mobile device to indicate there is a login request pending.
   - The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request (approving will require providing the token’s PIN code).
4. The SAS authentication reply is sent back to F5 BIG-IP APM.
5. The user is granted or denied access to F5 BIG-IP APM based on the OTP value calculation results from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from F5 BIG-IP APM, ensure the following:

- End users can authenticate from the F5 BIG-IP APM environment with a static password before configuring F5 BIG-IP APM to use RADIUS authentication.
- Ports 1812/1813 are open to and from F5 BIG-IP APM.
- 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.
- On the client machine, set the RADIUS timeout value at least 60 seconds.

Push OTP Prerequisites

In order to use SAS Push OTP you will need:

- SAS configured to enable Push OTP
- MobilePASS which is supported on the following OS platforms:
  - MobilePASS+ (Push OTP support)
    - Android 4.x, 5.x
    - iOS 7+

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with F5 BIG-IP APM using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 8
- Assigning an Authenticator in SAS, page 9
- Adding F5 BIG-IP APM as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS Server’s IP Address, page 9
- Enabling the Software Token Push OTP Setting, page 11
- Enabling the Allowed Targets Policy, page 14

Creating Users Stores in SAS

Before 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 SAS

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 APM.

The following authenticators are supported:

- MobilePASS+

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 APM as an Authentication Node in SAS

Add a RADIUS entry in the SAS Auth Nodes module to prepare it to receive RADIUS authentication requests from F5 BIG-IP APM. You will need the IP address of F5 BIG-IP APM and the shared secret to be used by both SAS and F5 BIG-IP APM.

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>Auth Node Name</strong></td>
<td>Enter a description of the agent; for example, <strong>BIG-IP RADIUS Agent</strong>.</td>
</tr>
<tr>
<td><strong>Resource Name</strong></td>
<td>Enter a resource name which will identify in a push notification which</td>
</tr>
<tr>
<td></td>
<td>authentication node it relates to.</td>
</tr>
<tr>
<td><strong>Low IP Address In Range</strong></td>
<td>Specify this field only if there is a pool of IP addresses. Otherwise,</td>
</tr>
<tr>
<td></td>
<td>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>Specify this field if there is a pool of IP addresses. Otherwise, enter</td>
</tr>
<tr>
<td></td>
<td>the same IP address as specified in the <strong>Host Name</strong> field.</td>
</tr>
<tr>
<td>**Exclude from PIN change</td>
<td>Do not select anything.</td>
</tr>
<tr>
<td>requests**</td>
<td></td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret that was used when the RADIUS server was configured</td>
</tr>
<tr>
<td></td>
<td>on BIG-IP.</td>
</tr>
<tr>
<td><strong>Agent Description</strong></td>
<td>Enter a description of the agent; for example, <strong>BIG-IP RADIUS Agent</strong>.</td>
</tr>
</tbody>
</table>

The authentication node is added to the system.

### Checking the SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in F5 BIG-IP APM, check its IP address. The IP address will then be added to F5 BIG-IP APM as a RADIUS server at a later stage.

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. The SAS RADIUS server details are displayed.

### Enabling the Software Token Push OTP Setting

To use Push OTP authentication, the setting must be enabled in the SAS token policy.

1. Log in to the SAS console with an Operator account.
2. Click the **POLICY** tab, and then select **Token Policies**.

3. In the **Token Policies** module, click the **Software Token Push OTP Setting** link.

4. Select **Enable Push OTP communication with MobilePass+**, and then click **Apply**.
**Enabling the Allowed Targets Policy**

For Push OTP to be permitted during authentication the user must have a MobilePASS+ token enrolled and this policy must be enabled.

The settings to enable this policy will determine which OS targets are presented to users during the self-enrollment of MobilePASS tokens. You can restrict the targets on which MobilePASS+ or MobilePASS 8 tokens are allowed to be activated or enrolled.

1. Log in to the SAS console with an Operator account.

2. Click the **POLICY** tab, and then select **Token Policies**.
3. In the **Token Policies** module, click the **Allowed Targets Settings** link.

![Token Policies](image)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token Templates</td>
<td>Edit the templates used to customize token operation. Templates are applied during token initialization.</td>
</tr>
<tr>
<td>Token Passcode Processing Policy</td>
<td>Set how the server will evaluate passcodes and support offline authentication.</td>
</tr>
<tr>
<td>Server-side PIN Policy</td>
<td>Set or modify the global server-side PIN policy.</td>
</tr>
<tr>
<td>Global or Groups PIN Change</td>
<td>Trigger a “Global or Groups PIN Change on next use.”</td>
</tr>
<tr>
<td>Temporary Password Policy</td>
<td>Set or modify the length, complexity, change frequency, randomness, and lifetime of static passwords.</td>
</tr>
<tr>
<td>Synchronization</td>
<td>Set inner and outer window synchronization parameters.</td>
</tr>
<tr>
<td>SMS/OTP</td>
<td>Set the number of OTPs to be sent in a single SMS message, as well as delivery mode and content.</td>
</tr>
<tr>
<td>Software Token Push OTP Settings</td>
<td>Enable Push OTP communication with MobilePASS.</td>
</tr>
<tr>
<td>Token File Creation Policy</td>
<td>Set the default location for token file creation.</td>
</tr>
<tr>
<td>Allowed Targets Settings</td>
<td>Set the allowed targets to software tokens.</td>
</tr>
<tr>
<td>MobilePASS Devices</td>
<td>Set and format download, installation, and removal messages for SafeNet Authentication Service MobilePASS devices.</td>
</tr>
<tr>
<td>Third-Party Authentication Options</td>
<td>Set authentication options for third-party tokens, such as Gridsure and RADIUS.</td>
</tr>
</tbody>
</table>

4. On the **MobilePASS** tab, select the desired targets to allow for each MobilePASS application, and then click **Apply**.

![Allowed Targets Settings](image)
Configuring F5 BIG-IP APM

A virtual server is created on BIG-IP, on which an Access Policy is applied. To set up the virtual server, log in to the management portal of APM as a BIG-IP administrator. Configure 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.

To access the management portal of F5 BIG-IP APM:
1. Browse to the public DNS/public IP of the BIG-IP APM Amazon instance.
2. Enter administrator login credentials, and then click Log in.

On successful authentication, you are logged in as an administrator in the management portal.
Configuring the Active Directory Server

1. Go to **Main > Access Policy > AAA Server > Active Directory** and then click the [+] sign in the right corner of the window.

2. Under **General Properties**, complete the details, and then click **Finished**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the authentication server you are creating.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>Enter the Windows Domain name. You must enter the FQDN.</td>
</tr>
<tr>
<td>Domain Controller Pool Name</td>
<td>Enter the Active Directory server configured with this role.</td>
</tr>
<tr>
<td>Admin Name</td>
<td>Enter an administrator name that has Active Directory administrative permissions.</td>
</tr>
<tr>
<td>Admin Password</td>
<td>Enter the administrative password for the server.</td>
</tr>
<tr>
<td>Verify Admin Password</td>
<td>Enter the administrative password for the server again.</td>
</tr>
</tbody>
</table>

(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. Click Main > Access Policy > AAA Server > RADIUS and then click the [+] sign in the right corner of the window.
2. Complete the details as described below, and then click **Finished**:

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the RADIUS server; for example, <strong>SAS_OWA_Policy_aa_srv</strong>.</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>. Otherwise, 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 the shared secret for the RADIUS server.</td>
</tr>
<tr>
<td><strong>Confirm Secret</strong></td>
<td>Enter the shared secret again.</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, that user is typically assigned a Webtop. A Webtop is the successful endpoint for a Web application or a network access connection.

To create a Webtop:

1. Click **Access Policy > Webtops > Webtop List** and then click the [+] sign in the right corner of the window.

2. Complete the details as described below, and then click **Finished**:

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

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

To create the Webtop links:

1. Click **Access Policy > Webtops > Webtop Links** and then click the [+] sign in the right corner of the window.
2. Complete the **New Webtop Link** fields as described below.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the Webtop link; for example, OWA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>(Optional) Type a description for this link.</td>
</tr>
<tr>
<td>Link Type</td>
<td>Select either Application URL or Hosted Contents. For example, if your resource is an application, select Application URL.</td>
</tr>
<tr>
<td>Application URL</td>
<td>This field is available only when Application URL is selected as the Link Type. Specify the URL of the application.</td>
</tr>
<tr>
<td>Hosted File</td>
<td>This field is available only when Hosted Contents is selected as the Link Type. Specify the hosted file.</td>
</tr>
<tr>
<td>Caption</td>
<td>By default, the caption is same as the Webtop link name; however, it may be changed to a unique value if desired.</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

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

1. Click **Access Policy > Access Profiles > Create**.
2. Specify a name for the profile; for example, **SAS_OWA_Policy**.
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.
4. Click **Finished**.

Editing the Access Profile

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

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

This guide is mainly focused on two-step authentication—first AD authentication and then second authentication with the OTP push notification.

A sample Access Policy for two-step authentication looks like this:
Another way to view the AAA (Authentication, Authorization, and Accounting) servers and resources assigned to an Access Policy can be as follows:

1. Click **Access Policy > Access Profiles**.
2. From the **Access Profiles** list, select **Access Profile**.
3. Click the **Access Policy** tab.

To edit the Access Profile:

1. On the **Main** tab of the navigation pane, expand **Access Policy > Access Profiles**.
2. In the **Access Profiles List**, find the Access Policy you want to edit and then click **Edit** in the **Access Policy** column. The Visual Policy editor opens in a new window or a new tab, depending on your browser settings. This is the new blank policy that you have just created.
3. On a rule branch of the access policy, click the plus symbol “+” to add an action.
The Add Item window appears. Click the + symbol to add a logon page, RADIUS authentication, and Webtop assignments.

Adding a Logon Page

The first page for a user will be a logon page where the user will enter its 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 + symbol after Start.


3. Click Add Item.

4. In the Name field, enter a name for the Logon Page.
5. In the **Language** field, select the language.

6. Edit the **Form Header Text** field and the name of the **Input** fields, if required.

7. Click **Save**.

## Adding Active Directory Authentication

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

Typically, for server authentication, two Access Policy items will need 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.

**To add Active Directory authentication after the first logon page:**

1. Click the + symbol after the **Logon Page**.
2. On the **Authentication** tab, select **AD Auth**, and then click **Add Item**.
3. In the **Server** field, select the configured AD server, and then click **Save**.

![Image of the Server field with AD Auth selected]

**Adding RADIUS Authentication**

**To add RADIUS authentication after the second logon page:**

1. Click the + symbol after the second **Logon Page**.
2. On the **Authentication** tab, select **RADIUS Auth**, and then click **Add Item**.

![Screen Shot](image)

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

3. Select the configured RADIUS server; for example, **SAS_OWA_Policy_aa_srv**.

![Properties](image)

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

4. Click **Save**.
Adding a Webtop

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

To add a Webtop:

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

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


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

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

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

7. Click **Save**.

**Configuring the Virtual Server**

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

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

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

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

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
2. Click Create.
3. Complete the **New Virtual Server** fields as described below.

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

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

Once the BIG-IP local traffic virtual server is configured with an appropriate Access Policy, and a corresponding Auth Node is added in SAS, the administrator provides users with the address of BIG-IP local traffic virtual server.

If you have an enrolled token (OTP, GridSure, SMS, and MobilePASS, etc.), browse to the virtual server and enter the username and token code on the login window.

Proceed according to the steps configured in the Access Policy.

Running the Solution for Push OTP Tokens – Simple Mode

1. Browse to the local traffic virtual server configured in APM.
2. On the login window, enter your **Username** and active directory **Password**, and then click **Logon**.

   ![Login Window](image)

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

3. User is redirected to the second logon page for push OTP authentication, enter your **Username** and then click **Logon** without entering any **Password**.

   ![Second Logon Page](image)

4. On the mobile device, tap **APPROVE** to accept the OTP request.
5. Enter Token PIN and tap **Continue** to send the approval with OTP to SAS.

6. The message **“Autosend passcode was successful.”** is displayed on the end user's mobile device.

"Autosend passcode was successful."
After Successful Authentication

For all the above token types, the user’s credentials are passed to the RADIUS server defined in the Access Policy for authentication. If the credentials are valid, authentication will be successful. Otherwise, authentication will fail and the user will not be allowed access to resources.

1. On successful authentication with the RADIUS server, the following message is displayed (if the Authentication Success Message option is enabled in the Access Policy).

2. Click the Click here to continue link. The Webtop assigned in the Access Policy is displayed.

3. Click the Webtop link (for example, OWA in the screen below). The resource page is displayed for the user to provide credentials for the exchange server.
Running the Solution for Push OTP Tokens – Hybrid Mode

1. Browse to the local traffic virtual server configured in APM.
2. On the login window, enter your **Username** and active directory **Password**, and then click **Logon**.
3. User is redirected to the second logon page for push OTP authentication. Select **Use my mobile to autosend a passcode**, and then click **Submit**.
4. Wait on this window till the end user approves the authentication request on his/her mobile device.

5. On the mobile device, tap **APPROVE** to accept the OTP request.
6. Enter **Token PIN** and tap **Continue** to send the approval with OTP to SAS.

7. The message “**Autosend passcode was successful.**” is displayed on the end user's mobile device.
After Successful Authentication

For all the above token types, the user’s credentials are passed to the RADIUS server defined in the Access Policy for authentication. If the credentials are valid, authentication will be successful. Otherwise, authentication will fail and the user will not be allowed access to resources.

1. On successful authentication with the RADIUS server, the following message is displayed (if the Authentication Success Message option is enabled in the Access Policy).

2. Click the **Click here to continue** link. The Webtop assigned in the Access Policy is displayed.

3. Click the Webtop link (for example, **OWA** in the screen below). The resource page is displayed for the user to provide credentials for the exchange server.

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

DNS and NTP Settings on the BIG-IP System

For BIG-IP APM, you must have DNS and NTP settings configured.

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.

Modifying Second Login Page for Push OTP Token

Customizing the logon page’s header and input filed text:

1. Log in to F5 BIG-IP.
3. Click Edit in front of the created access policy.
4. Click on the second Logon Page to edit action properties.

5. Under the Customization section, update the fields as described below.

<table>
<thead>
<tr>
<th>Form Header Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Welcome &lt;br&gt; For security reasons, we require additional information to verify your account.”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logon Page Input Field #1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logon Page Input Field #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter your passcode to sign in</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logon Button</th>
</tr>
</thead>
<tbody>
<tr>
<td>Submit</td>
</tr>
</tbody>
</table>
6. Click Save.

**Customizing the logon page to provide Hybrid options on the page:**

To select Push OTP options on the logon page, change the code of default logon page. An example of the modified F5 BIG-IP APM logon page can be downloaded from Inquire (DOW4047).

Log in to BIG-IP as an administrator and perform the following steps to update the logon page.

The following changes are made based on the assumption that the Push OTP authentication is provided on the second logon page and that the **Username** field is set to **Read-only**.

1. Log in to F5 BIG-IP.
2. Click **Access Policy > Customization > Advanced**.
3. In the **Edit Mode** field, select **Advanced**.
4. Expand **Access Profiles**.
5. Expand the **End User SSL VPN** portal page.
6. Click **Access Policy > Logon Pages**.
7. Under **Logon Pages**, expand the first logon page.
8. Select **logon.inc** and update the content as explained below.

   a. Look for the following line:

   ```html
   <? include_customized_page("logout", "session_expired.js"); ?>
   ```

   Then, add the following functions before the line above:

   ```javascript
   function yesnoCheck() {
     var yesno = document.getElementById("yesCheck");
     var noVar = document.getElementById("noCheck");
   }
   ```
var yesNoDiv = document.getElementById("ifYes");
if (yesno.checked) {
    yesNoDiv.style.display = "block";
    yesNoDiv.style.visibility = "visible";
} else if (noVar.checked){
    yesNoDiv.style.display = "none";
    yesNoDiv.style.visibility = "hidden";
}

function testScript()
{
    var msg = document.getElementById("msgYes");
    msg.style.display = "block";
    msg.style.visibility = "visible";
    msg.style.color = 'blue';
}

b. Look for the following function and go to where function ends:
foreach( $fields_settings as $id=>$field_settings )
{
}

Then, copy the below content:

?>
<tr>
 <td colspan=2 class="credentials_table_unified_cell" >
     <label for="text">I want to :</label>
     <input type="radio" name="otgotp" id="noCheck" onClick="yesnoCheck()" value='1' > Use my mobile to autosend a passcode<br>
     <input type="radio" name="otgotp" id="yesCheck" onClick="yesnoCheck()" value='2' > Enter a passcode manually

     </td>
 </tr>

<tr>
 <td colspan=2 class="credentials_table_unified_cell" >
     <div id="ifYes" style="visibility:hidden; display:none;">Enter your passcode to sign in</div>
     <input type=password name=password class="credentials_input_password"  value="" id="input_2" autocomplete="off" autocapitalize="off">
 </td>
</tr>

<tr>
 <td colspan=2 class="credentials_table_unified_cell" >
     <div id="msgYes" style="visibility:hidden; display:none;"><label for="message">A login request from Gemalto has been sent. <br> Please check your mobile device.</label></div>
 </td>
</tr>
c. Look for the following content:

```php
<tr id="submit_row">
  <td class="credentials_table_unified_cell"><input type=submit class="credentials_input_submit" value="%[logon]"></td>
</tr>
```

Then, replace with the following content:

```php
<tr id="submit_row">
  <td class="credentials_table_unified_cell" onclick="yesnoCheck();"><input type=submit class="credentials_input_submit" value="%[logon]"></td>
</tr>
```

d. Look for the following content:

```php
<table id="main_table" class="logon_page">
  <tr>
    <td colspan=2 id="credentials_table_header" ><? print( $formHeader ); ?></td>
  </tr>
</table>
```

Then, replace with the following content:

```php
<table id="main_table" class="logon_page">
  <tr>
    <td colspan=2 id="credentials_table_header" onclick="yesnoCheck();"><input type=submit class="credentials_input_submit" value="%[logon]" onsubmit="javascript: return masterSubmit(this);" autocomplete="off"></td>
  </tr>
</table>
```
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, Inc. 4690 Millennium Drive 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>
<tr>
<td><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>