SafeNet Authentication Service
Push OTP 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:** 007-013573-001, Rev. A  
**Release Date:** September 2016
Contents

Third-Party Software Acknowledgement ............................................................................ 4
Description .......................................................................................................................... 4
Applicability .......................................................................................................................... 5
Environment .......................................................................................................................... 5
Audience ................................................................................................................................. 5
RADIUS-based Authentication using SafeNet Authentication Service Cloud ...................... 5
RADIUS Authentication Flow using SafeNet Authentication Service ................................. 6
RADIUS Prerequisites .......................................................................................................... 6
Push OTP 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
  Enabling the Software Token Push OTP Setting ................................................................. 11
  Enabling the Allowed Targets Policy ................................................................................ 12
Configuring F5 BIG-IP Access Policy Manager ................................................................. 13
  Accessing the F5 BIG-IP APM Management Portal ............................................................ 14
  Configuring the Active Directory Server .......................................................................... 15
  Configuring the RADIUS Server ...................................................................................... 17
  Creating a Webtop .............................................................................................................. 19
Configuring the Webtop Links ............................................................................................ 20
  Creating an Access Profile ................................................................................................. 21
  Configuring the Access Profile (Simple Mode) ................................................................. 22
  Configuring the Access Profile (Hybrid Mode) ................................................................. 34
  Configuring the Virtual Server ......................................................................................... 53
Running the Solution ............................................................................................................ 57
  Running the Solution (Simple Mode) ................................................................................ 57
  Running the Solution (Hybrid Mode) ................................................................................ 60
Appendix: Configuring DNS and NTP on the BIG-IP System ............................................ 64
Support Contacts ................................................................................................................. 65
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 (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.

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 APM using the SafeNet Push one-time password (OTP) solution managed by SafeNet Authentication Service.
- Configure F5 BIG-IP APM 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 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 Access Policy Manager**—Version 12.0

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 the following RADIUS topology that supports Push OTP tokens:

**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.

This document demonstrates the solution using the SAS cloud hosted RADIUS service.
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 dataflow of a multi-factor authentication transaction for F5 BIG-IP Access Policy Manager.

1. A user attempts to log on to F5 BIG-IP Access Policy Manager using a Push 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. 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 Access Policy Manager.
5. The user is granted or denied access to 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 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.
• On the client machine, set the RADIUS timeout value at least 60 seconds.

**Push OTP Prerequisites**

In order to use SafeNet Authentication Service (SAS) Push OTP you will need:

• **SafeNet Authentication Service configured to enable Push OTP**

• MobilePASS that is supported on the following OS platforms:
  - MobilePASS+ (Push OTP support)
    - Android 4.x and 5.x
    - iOS 7+

**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 8

• Enabling the Software Token Push OTP Setting, page 10

• Enabling the Allowed Targets Policy, page 12

**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:

- 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 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 click **Auth Nodes**.

![Auth Nodes](image1)

3. In the **Auth Nodes** module, click the **Auth Nodes** link, and then click **Add**.

![Auth Nodes](image2)

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

   - **Auth Node Name**: Enter a host description.
   - **Resource Name**: Enter a resource name which will identify in a push notification which authentication node it relates to.
   - **Low IP Address In Range**: Enter the IP address of the host that will authenticate with SAS.
   - **Exclude from PIN change requests**: Do not select this option.
   - **Configure FreeRADIUS Synchronization**: Select this option.
   - **Shared Secret**: Enter the shared secret key.
   - **Agent Description**: Re-enter the shared secret key.
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.

2. Click the **COMMS** tab, and then click **Auth Nodes**.

![Auth Nodes](image)
3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.

![Auth Nodes](image)

**Auth Nodes:**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth Nodes</td>
<td>Create and configure SafeNet Authentication Service Authentication Nodes</td>
</tr>
</tbody>
</table>

Using the RADIUS protocol over the Internet provides limited security of the traffic between the organization’s data center and the authentication service. For improved security and for alternatives to RADIUS traffic, refer to the recommendations included in the SafeNet Authentication Service Administrator Guide.

<table>
<thead>
<tr>
<th>Primary RADIUS Server IP</th>
<th>64.26.164.56:1812</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary SafeNet Authentication Service Agent DNS</td>
<td>safetagent.safenetservices.com:443</td>
</tr>
<tr>
<td>Secondary SafeNet Authentication Service Agent DNS</td>
<td>safetagent.safenetservices.com:443</td>
</tr>
<tr>
<td>Max. Auth Nodes</td>
<td>10</td>
</tr>
</tbody>
</table>

No Records

---

**Enabling the Software Token Push OTP Setting**

To use Push OTP authentication, the Software Token Push OTP setting must be enabled in the SafeNet Authentication Service (SAS) token policy.

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

2. Click the **POLICY** tab, and then click **Token Policies**.

![Policy Tab](image)
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 SafeNet Authentication Service (SAS) console with an Operator account.
2. Click the **POLICY** tab, and then select **Token Policies**.

![Image of Token Policies](image)

3. In the **Token Policies** module, click the **Allowed Targets Settings** link.

![Image of Allowed Targets Settings](image)

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

### 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 APM management portal as the 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 14
- Configuring the Active Directory Server, page 15
- Configuring the RADIUS Server, page 17
- Creating a Webtop, page 19
- Configuring the Webtop Links, page 20
- Creating an Access Profile, page 21
- Configuring the Access Profile (Simple Mode), page 22
- Configuring the Access Profile (Hybrid Mode), page 34
- Configuring the Virtual Server, page 53

Accessing the F5 BIG-IP APM Management Portal

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

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

Configuring the Active Directory Server

1. On the management portal console, on the Main tab, click Access Policy > AAA Servers > Active Directory, and then click the icon.
2. Under **General Properties**, complete the following fields, and then click **Finished**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the authentication server.</td>
</tr>
<tr>
<td><strong>Domain Name</strong></td>
<td>Enter the domain name of the Active Directory server.</td>
</tr>
<tr>
<td><strong>Server Connection</strong></td>
<td>Select <strong>Use pool</strong> or <strong>Direct</strong> based on your preferred configuration.</td>
</tr>
<tr>
<td><strong>Domain Controller</strong></td>
<td>Enter the IP address of the Active Directory server.</td>
</tr>
<tr>
<td><strong>Admin Name</strong></td>
<td>Enter an administrator name that has Active Directory administrative permissions.</td>
</tr>
<tr>
<td><strong>Admin Password</strong></td>
<td>Enter an administrator password for the server.</td>
</tr>
<tr>
<td><strong>Verify Admin Password</strong></td>
<td>Re-enter the administrator password.</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 users to access their resources through a RADIUS server that you configure in the Access Policy Manager (APM).

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.

(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, SAS_OWA_Policy_aa_srv).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Select Authentication.</td>
</tr>
<tr>
<td>Server Connection</td>
<td>If you have a single RADIUS server, select Direct, else, select Use Pool.</td>
</tr>
<tr>
<td>Server Address</td>
<td>Enter the IP address of the RADIUS server, which can be found in the Auth nodes section on the COMMS tab of your SAS server.</td>
</tr>
<tr>
<td>Authentication Service Port</td>
<td>Enter the authentication service port. SAS works on the default port number 1812.</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.)
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.

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>

(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 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.

![Screen Image](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><strong>Name</strong></th>
<th>Enter a name for the Webtop link.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Type a description for this link.</td>
</tr>
<tr>
<td><strong>Link Type</strong></td>
<td>Select either <strong>Application URL</strong> or <strong>Hosted Contents</strong>. For example, if your resource is an application, select <strong>Application URL</strong>.</td>
</tr>
<tr>
<td><strong>Application URL</strong></td>
<td>Enter the URL of the application. This field is available only when <strong>Application URL</strong> is selected as the <strong>Link Type</strong>.</td>
</tr>
<tr>
<td><strong>Hosted File</strong></td>
<td>Specify the hosted file name. This field is available only when <strong>Hosted Contents</strong> is selected as the <strong>Link Type</strong>.</td>
</tr>
<tr>
<td><strong>Caption</strong></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>

![Form](image)

(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**, in the **Factory Builtin Languages** list, select a language, 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 (Simple Mode)**

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.

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

The following is a sample Access Policy for two–step authentication:

![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 23
- Editing the Access Profile, page 24
- Adding a Logon Page, page 25
- Adding Active Directory Authentication, page 26
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:

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

![Access Policy](image1)

(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 **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 21.

![Access Profiles List](image2)

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

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

![Access Policy](image3)

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


   (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) you want to edit.

   (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 the user will enter its username and password. To add a logon page on the local traffic virtual server, perform the following steps:

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

![Start + icon](image)

2. On the **Logon** tab, select **Logon Page**, and then click **Add Item**.

![Logon tab selection](image)

3. On the **Properties** tab, in the **Name** field, enter a name for the logon page.

![Properties tab](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.png)

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

5. **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.

1. **Click the + icon after Logon Page.**

   ![Logon Page Image](image.png)

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

![Authentication Tab](image1)

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

3. On the **Properties** tab, in the **Server** field, select the configured AD server, and then click **Save**.

![Properties Tab](image2)

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

### Adding RADIUS Authentication

Adding RADIUS authentication requires:

- Adding a Second Logon Page for RADIUS Authentication, page 28
- Adding Variable Assign, page 29
- Adding RADIUS Authentication, page 31
- Adding a Webtop, page 32
Adding a Second Logon Page for RADIUS Authentication

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

2. On the Logon tab, select Logon Page, and then click Add Item.

3. On the Properties tab, perform the following steps:
   a. In the Name field, enter a name for the logon page.
   b. In the table, for the password variable type, in the Read Only column, select Yes.
5. On the Customization window, 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.
   d. Click **Save**.

   ![Customization Window]

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

**Adding Variable Assign**

1. On the **Visual Policy** editor, click the + icon after the second logon page.

   ![Access Policy]

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

2. On the **Assignment** tab, select **Variable Assign**, and then click **Add Item**.
3. On the **Variable Assign** window, click **Add new entry**, and then click **change**. A popup window is displayed.

![Variable Assign Window](image1)

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

4. On the popup window, perform the following steps:
   a. On the left side, in the dropdown list, select **Custom Variable**.
   b. In the box, enter the following string:
      
      ```
      session.logon.last.password
      ```
   c. On the right side, in the dropdown list, select **Text**
   d. In the **Text** field, enter **1**.
   e. Click **Finished**.
   f. Click **Save**.

![Custom Variable Window](image2)

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

1. On the Visual Policy editor, click the + icon after Variable Assign.

2. On the Authentication tab, select RADIUS Auth, and then click Add Item.
3. On the **Properties** tab, in the **AAA Server** field, select the configured RADIUS server (for example, **SAS_OWA_Policy_aa_srv**).

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

   ![Properties Tab](image)

   - **Name:** RADIUS Auth
   - **AAA Server:** None
   - **Show Extended Error:** Disabled
   - **Max Logon Attempts Allowed:** 3

4. Click **Save**.

**Adding a Webtop**

When users are 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**.

   *(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.

![Properties tab](image)

(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.

![Webtop Links tab](image)

(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](image)

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

6. Click Save.

![Webtop tab](image)

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

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.

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

The following is a sample Access Policy for two–step authentication:

Configuring the access profile for Hybrid Mode requires:

- Viewing Access Policy, page 35
- Editing the Access Profile, page 36
- Adding a Logon Page, page 37
- Adding Active Directory Authentication, page 39
- Adding SafeNet Two-Factor Authentication Method, page 40
- Adding a Logon Page to the Mobile Branch, page 43
- Adding Variable Assign to the Mobile Branch after Logon Page, page 44
- Adding RADIUS Authentication to the Mobile Branch after Variable Assign, page 46
- Adding a Webtop to the Mobile Branch after RADIUS Authentication, page 48
- Adding Logon Page to the Manual Branch, page 49
- Adding RADIUS Authentication to the Manual Branch after Logon Page, page 50
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:


   (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 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 21.

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

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**.

   ![Image of 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 you want to edit.

   ![Image of Access Profiles List](image)

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

   The Visual Policy editor will be displayed.

   ![Image of Visual Policy Editor](image)

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

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 the user will enter its username and password. To add a logon page on the local traffic virtual server, perform the following steps:

1. On the Visual Policy editor, click the + icon after Start.

2. On the Logon tab, select Logon Page, and then click Add Item.

3. On the Properties tab, perform the following steps:
   a. In the Name field, enter a name for the logon page.
   b. In the table, in the Type column, select text, password, and radio variable types.
   c. Click in the Values column of the radio variable type.
4. Click **Add Option**, and then perform the following steps:
   a. In the **Value** column, enter **mobile**.
   b. In the **Text** column, enter **Use mobile to auto send passcode**.

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

5. Click **Add Option**, and then perform the following steps, and then click **Finished**:
   a. In the **Value** column, enter **manual**.
   b. In the **Text** column, enter **Enter passcode manually**.

   (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.)
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.

1. Click the + icon after Logon Page.

2. On the Authentication tab, select AD Auth, and then click Add Item.
3. On the **Properties** tab, in the **Server** field, select the configured AD server, and then click **Save**.

![Properties tab screenshot](image)

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

**Adding SafeNet Two-Factor Authentication Method**

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

![Visual Policy editor screenshot](image)

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

2. Click the **General Purpose** tab, select **Empty**, and then click **Add Item**.

![General Purpose tab screenshot](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 the name for the Safenet two-factor authentication method.

![Properties tab](image)

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

4. Click the **Branch Rule** tab, and then perform the following steps:
   a. Click **Add Branch Rule**.
   b. In the **Name** field, enter **manual**.
   c. Click **change**.

![Branch Rules tab](image)

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

5. Click the **Advanced** tab, and then enter the following expression:

```plaintext
expr { mcget {session.logon.last.safenet} ] == "manual" }
```

![Advanced tab](image)

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

6. Click **Finished**.
7. Click Add Branch Rule, and then perform the following steps:
   a. In the Name field, enter mobile.
   b. Click change.

8. Click the Advanced tab, enter the following expression, and then click Finished.
   \[ \text{expr} \{ \text{mcget\{(session.logon.last.safenet\)}} == \text{"mobile"} \} \]

9. Click Save.
Adding a Logon Page to the Mobile Branch

1. On the Visual Policy editor, click the + icon in the Mobile branch of Safenet Two-Factor Auth Method.

![Diagram](image1.png)

(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 Panel](image2.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 Name field, enter a name for the logon page.

![Properties Panel](image3.png)

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

4. In the table, for the password variable type, in the Read Only column, select Yes.
5. On the Customization window, 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.
   d. Click Save.

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

Adding Variable Assign to the Mobile Branch after Logon Page

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

   ![Visual Policy Editor](image)
   (The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
2. On the Assignment tab, select **Variable Assign**, and then click **Add Item**.

3. On the **Variable Assign** window, click **Add new entry**, and then click **change**. A popup window is displayed.
4. On the popup window, perform the following steps:
   a. On the left side, in the dropdown list, select **Custom Variable**.
   b. In the box, enter the following string:
      
      `session.logon.last.password`
   c. On the right side, in the dropdown list, select **Text**
   d. In the **Text** field, enter 1.
   e. Click **Finished**.
   f. Click **Save**.

   ![Popup Window](image)

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

**Adding RADIUS Authentication to the Mobile Branch after Variable Assign**

1. On the **Visual Policy** editor, click the `+` icon after **Variable Assign**.

   ![Visual Policy Editor](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**).

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

4. Click **Save**.
Adding a Webtop to the Mobile Branch after RADIUS Authentication

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.)


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


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.

**Adding Logon Page to the Manual Branch**

1. On the **Visual Policy** editor, click the + icon in the **Manual branch** of **Safenet Two-factor Auth Method**.

   ![Image](image1.png)

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

2. On the **Authentication tab**, select **AD Auth**, and then click **Add Item**.

   ![Image](image2.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 **Server** field, select the configured AD server, and then click **Save**.

![Properties tab screenshot](image)

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

**Adding RADIUS Authentication to the Manual Branch after Logon Page**

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

![Visual Policy editor screenshot](image)
2. On the **Authentication** tab, select **RADIUS Auth**, and then click **Add Item**.

3. On the **Properties** tab, in the **AAA Server** field, select the configured RADIUS server (for example, **SAS_OWA_Policy_aa_srv**).
4. Click **Save**.

**RADIUS Auth** will be listed in the Visual Policy editor.

![Diagram of Access Policy](image)

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

**Adding a Webtop to the Manual Branch**

When users are 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**.

![Diagram of Access Policy](image)

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

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

![Diagram of Assignment Tab](image)

*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**.

![Diagram of Properties Tab](image)

*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.

![Webtop Links Tab](image)

*(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 on **Update**.

![Webtop Tab](image)

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

6. Click **Save**.

![Resource Assignment](image)

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

---

**Configuring the Virtual Server**

When using BIG-IP APM, virtual servers are configured with specific settings for 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 Servers Tab](image1.png)

*(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 virtual server.</th>
</tr>
</thead>
<tbody>
<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>

![General Properties](image2.png)

*(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:

<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 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 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, GridSecure, 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 (Simple Mode)

1. Browse to the local traffic virtual server configured in APM.
2. On the login window, enter your user name 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. You will be redirected to the second login page for push OTP authentication, enter your user name and then click Logon

![Second Login Page](image)

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
4. On the registered mobile device, tap **APPROVE** to accept the OTP request.

5. On the **TOKEN AUTHENTICATION** screen, enter **Token PIN**, and then tap **Continue** to send the approval with OTP to SAS.

(The screen image above is from F5 Networks® software. Trademarks are the property of their respective owners.)
6. A success message is displayed on the 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, a success message is displayed (if the Authentication Success Message option is enabled in the Access Policy). Click on the Click here to continue link.

2. The Webtop assigned in the Access Policy is displayed. Click on the Webtop link.
The resource page is displayed to provide credentials for the exchange server.

![Image of resource page]

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

**Running the Solution (Hybrid Mode)**

1. Browse to the local traffic virtual server configured in APM.
2. On the login window, enter your user name and Active Directory password, and then select any of the following options:
   - Use mobile to autosend passcode
   - Enter passcode manually

![Image of login window]

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

---

**NOTE:** In this scenario, Use mobile to autosend passcode is selected.
3. You will be redirected to the second logon page for the push OTP authentication. Enter your username, and then click Logon.

4. On the mobile device, tap APPROVE to accept the OTP request.
5. On the TOKEN AUTHENTICATION screen, enter **Token PIN**, and then tap **Continue** to send the approval with OTP to SAS.

6. A success message is displayed on the mobile device.

![MobilePASS+ Token Authentication Screen]

**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, a success message is displayed (if the Authentication Success Message option is enabled in the Access Policy). Click the Click here to continue link.

![Successful RADIUS authentication with SAS server!!](image)

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

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

![Webtop](image)

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

The resource page will be displayed to provide credentials for the exchange server.

![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, 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.
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>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>