SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol (NPS Agent v2.0) for Cisco ASA
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:** 007-013545-001, Rev. A

**Release Date:** July 2016
# Contents

Third-Party Software Acknowledgement .............................................................. 4
Description ........................................................................................................ 4
Applicability ...................................................................................................... 4
Environment ..................................................................................................... 4
Audience ........................................................................................................... 5
RADIUS-based Authentication using SafeNet Authentication Service Cloud .......................................................... 5
RADIUS Authentication Flow using SafeNet Authentication Service .............................................................. 5
RADIUS Prerequisites ..................................................................................... 6
Push OTP Prerequisites ................................................................................... 6
Configuring SafeNet Authentication Service ..................................................... 6
  Creating Users Stores in SafeNet Authentication Service ............................... 7
  Assigning an Authenticator in SafeNet Authentication Service .................... 7
  Adding NPS Agent as an Authentication Node in SafeNet Authentication Service ........................................... 8
  Enabling the Software Token Push OTP Setting ........................................... 9
  Enabling the Allowed Targets Policy ............................................................. 11
Configuring NPS Agent v2.0 ........................................................................... 12
  Configuring NPS Agent v2.0 to Support Push OTP ..................................... 13
  Configuring the RADIUS Attribute for NPS Agent v2.0 ............................ 14
Configuring Cisco ASA ..................................................................................... 15
  Creating AAA Server Groups .................................................................... 15
  Adding a Group Policy .............................................................................. 22
  Configuring a Connection Profile for Clientless SSL VPN Access .................. 23
Running the Solution ....................................................................................... 31
Support Contacts ............................................................................................. 34
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Cisco Adaptive Security Appliance (ASA).

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

Description

SafeNet Authentication Service (SAS) delivers a fully automated, versatile, and strong authentication-as-a-service solution.

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

Cisco Adaptive Security Appliance (ASA) is a security device that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities. It provides a proactive threat defense to stop attacks before they spread through the network.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Cisco ASA using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure Cisco ASA to work with SafeNet Authentication Service in RADIUS mode.

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

Cisco ASA can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

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

Environment

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

- SafeNet Authentication Service (SAS)
- SafeNet Network Policy Server Agent—Version 2.0
- Cisco ASA—Version 9.2 (2.4)
- Cisco Adaptive Security Device Manager (ASDM)—Version 7.3(1)101
Audience

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

RADIUS-based Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (SAS) Cloud with the Network Policy Server (NPS) agent v2.0 provides a RADIUS mode topology, **Local RADIUS hosted on-premises** in which an NPS agent is implemented in the existing customer’s RADIUS environment. The NPS agent forwards the RADIUS authentication requests to the SAS cloud environment. The NPS agent can be implemented on a Microsoft NPS/IAS server.

This document demonstrates the solution using the SAS cloud and on-premises NPS agent environment.

For more information on how to install and configure SAS Agent for IAS/NPS, refer to, **SAS NPS Agent v2.0 Configuration Guide** (http://www2.gemalto.com/sas-downloads/zip/nps-agent.zip).

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

RADIUS Authentication Flow using SafeNet Authentication Service

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

The image below describes the data flow of a multi-factor authentication transaction for Cisco ASA.

1. A user attempts to log on to Cisco ASA using an OTP authenticator.
2. Cisco ASA sends an LDAP request with the user’s Active Directory (AD) credentials to the LDAP server, that is, Microsoft AD server.

3. If successfully authenticated, Cisco ASA sends a RADIUS request to IAS/NPS server.

4. The NPS agent (installed on the IAS/NPS server), forwards the credentials to SafeNet Authentication Service (SAS) for validation using the SAS Authentication API.

5. SAS identifies the user or mobile device, and detects that the OTP field is single character. Then:
   - SAS will directly trigger a Push OTP authentication request.
   - The user receives a push notification on the configured mobile device to indicate that 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).

6. The SAS authentication reply is sent back to the NPS agent.

7. The NPS agent forwards the reply to the Cisco ASA.

8. The user is granted or denied access to the Cisco ASA based on the OTP value calculation results from SAS.

RADIUS Prerequisites

To authenticate to Cisco ASA with RADIUS protocol using NPS and the SAS NPS Agent v2.0, ensure the following:

- End users can authenticate from the Cisco ASA environment with a static password before configuring Cisco ASA to use RADIUS authentication.
- Ports 1812/1813 are open to and from Cisco ASA.
- A shared secret key has been selected and configured on both Cisco ASA and NPS. 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.

Push OTP Prerequisites

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

- SAS configured to enable Push OTP
- MobilePASS+ application

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Cisco ASA using RADIUS protocol requires the following:

- Creating Users Stores in SafeNet Authentication Service, page 7
- Assigning an Authenticator in SafeNet Authentication Service, page 7
• Adding NPS Agent as an Authentication Node in SafeNet Authentication Service, page 7
• Enabling the Software Token Push OTP Setting, page 9
• Enabling the Allowed Targets Policy, page 11

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 Cisco ASA.

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 NPS Agent as an Authentication Node in SafeNet Authentication Service

Add an Authentication Node entry in the SafeNet Authentication Service (SAS) **Auth Nodes** module to prepare it to receive authentication requests from the NPS Agent.

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

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent Description</strong></td>
<td>Enter a host description.</td>
</tr>
<tr>
<td><strong>Host Name</strong></td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td><strong>Low IP Address In Range</strong></td>
<td>Enter the IP address of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td><strong>Configure FreeRADIUS Synchronization</strong></td>
<td>Do not select this option.</td>
</tr>
</tbody>
</table>

The authentication node is added to the system.

---

**Enabling the Software Token Push OTP Setting**

Enable the Push OTP settings in the SafeNet Authentication Service (SAS) token policy to use Push OTP authentication.

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

   ![Policy Tab](image)

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

   ![Token Policies Module](image)

4. Select **Enable Push OTP communication with MobilePass+** , and then click **Apply**.

   ![Software Token Push OTP Setting](image)
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.
3. In the Token Policies module, click the Allowed Targets Settings link.

![Token Policies](image)

4. Under Allowed Target Settings, on the MobilePASS tab, select the desired targets to allow for each MobilePASS application for this virtual server, and then click Apply.

### Configuring NPS Agent v2.0

Configuring NPS Agent v2.0 requires the following:

- Configuring NPS Agent v2.0 to Support Push OTP, page 13
- Configuring the RADIUS Attribute for NPS Agent v2.0, page 14
Configuring NPS Agent v2.0 to Support Push OTP

On the **SAS – NPS Configuration Management** window, on the NPS Settings tab, select Push OTP Enabled.

For basic agent's configurations, refer to "Configuring SafeNet Authentication Service Agent for NPS" in **SAS NPS Agent v2.0 Configuration Guide** (http://www2.gemalto.com/sas-downloads/zip/nps-agent.zip).
Configuring the RADIUS Attribute for NPS Agent v2.0

Configure the NPS agent to send a specific RADIUS attribute to SafeNet Authentication Service (SAS), which in turn will send the user system IP address in the push notification that is received on the user's mobile.

In this solution, the RADIUS attribute *(Calling-Station-Id (31))* is defined in the registry settings of the system on which the NPS Agent is installed.

1. On the Registry Editor window, click HKEY_LOCAL_MACHINE > SOFTWARE > CRYPTOCard > AuthRadius.

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

<table>
<thead>
<tr>
<th>Registry String Value Name</th>
<th>Value Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>RequiredUserIpAttribute</td>
<td>31</td>
</tr>
<tr>
<td>SendUserIP</td>
<td>1</td>
</tr>
</tbody>
</table>

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

3. Close the Registry Editor, and then restart the system.

**Configuring Cisco ASA**

For this integration, Cisco ASA is used for the SSL VPN connection.

Configuring Cisco ASA for two-step and multi-factor authentication requires the following:

- Creating AAA Server Groups, page 15
- Adding a Group Policy, page 22
- Configuring a Connection Profile for Clientless SSL VPN Access, page 23

**Creating AAA Server Groups**

To use an external AAA server, you must first create at least one AAA server group per AAA protocol, and add one or more servers to each group. AAA server groups are identified by names. Each server group is associated with only one type of server, such as Kerberos, LDAP, NT, RADIUS, SDI, or TACACS+.

For this integration, LDAP and RADIUS external AAA servers are used for authentication.
You will need to create two server groups (for example, `adgroup` and `radiusgroup`). `adgroup` must be configured with the external LDAP server using the LDAP protocol, and `radiusgroup` must be configured with the external RADIUS server using the RADIUS protocol.

Creating the LDAP-enabled AAA Server Group and its Servers

1. Open Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
2. On the main window, click **Configuration**.
3. In the left pane, click the **Remote Access VPN** tab, and then click **AAA/Local Users > AAA Server Groups**.

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

4. In the right pane, under **AAA Server Groups**, click **Add**.

   (The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
5. On the **Add AAA Server Group** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>AAA Server Group</th>
<th>Enter a server group name (for example, adgroup).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select <strong>LDAP</strong>.</td>
</tr>
</tbody>
</table>

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

6. On the main window, in the right pane, under **AAA Server Group**, the newly created AAA server group is listed. Select the newly created server group.

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

7. Under **Servers in the Selected Group**, click **Add**.

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
8. On the **Add AAA Server** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Interface Name</strong></th>
<th>Select an appropriate interface that Cisco ASA uses in order to reach the LDAP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Name or IP Address</strong></td>
<td>Enter the IP address of the LDAP server that Cisco ASA uses in order to reach the LDAP server.</td>
</tr>
<tr>
<td><strong>Base DN</strong></td>
<td>Enter the location in the LDAP hierarchy where the server must begin to search.</td>
</tr>
<tr>
<td><strong>Naming Attribute(s)</strong></td>
<td>Enter the Relative Distinguished Name attribute(s) that uniquely identifies an entry on the LDAP server. <strong>sAMAccountName</strong> is the default attribute in the Microsoft Active Directory.</td>
</tr>
<tr>
<td><strong>Login DN</strong></td>
<td>Enter the Distinguished Name (DN) with enough privileges in order to be able to search users in the LDAP server.</td>
</tr>
<tr>
<td><strong>Login Password</strong></td>
<td>Enter the password for the DN account.</td>
</tr>
</tbody>
</table>

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

9. The newly created AAA server will be added under **Servers in the Selected Group**. Click **Apply**.
Creating the RADIUS-enabled AAA Server Group and its Servers

1. Open Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
2. On the main window, click **Configuration**.
3. In the left pane, click the **Remote Access VPN** tab, and then click **AAA/Local Users > AAA Server Groups**.

![Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups](image)

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

4. In the right pane, under **AAA Server Groups**, click **Add**.

![Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups](image)

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
5. On the **Add AAA Server Group** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>AAA Server Group</th>
<th>Enter a server group name (for example, <code>radiusgroup</code>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol</strong></td>
<td>Select <strong>RADIUS</strong>.</td>
</tr>
</tbody>
</table>

![Add AAA Server Group window](image)

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

6. On the main window, in the right pane, under **AAA Server Groups**, the newly created AAA server group is listed. Select the newly created server group (for example, `radiusgroup`).

![Configuration window](image)

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
7. Under **Servers in the Selected Group**, click **Add**.

![Add AAA Server](image)

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

8. On the **Add AAA Server** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Interface Name</strong></th>
<th>Select an appropriate interface that Cisco ASA uses in order to reach the NPS RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Name or IP Address</strong></td>
<td>Enter the IP address of the NPS RADIUS server.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>Specifies the time period (in seconds) ASA waits for a response from the primary server. Enter timeout, for example, 90 seconds. <strong>NOTE</strong>: This timeout value should be 60 or more than 60 Seconds.</td>
</tr>
<tr>
<td><strong>Server Authentication Port</strong></td>
<td>Enter <strong>1812</strong>.</td>
</tr>
<tr>
<td><strong>Server Secret Key</strong></td>
<td>Enter the secret key shared between Cisco ASA and the NPS server.</td>
</tr>
</tbody>
</table>

![Add AAA Server Window](image)

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

9. The newly created AAA server group is added under **Servers in the Selected Group**. Click **Apply**.
Adding a Group Policy

A group policy is a set of user-oriented attribute/value pairs for connections that are stored either internally (locally) on the device or externally on a RADIUS server. A connection profile uses a group policy that sets terms for user connections after the tunnel is established. Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute for each user.

2. Click the Configuration tab.
3. In the left pane, click Remote Access VPN.

5. Click Add.

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
6. On the Add Internal Group Policy window, perform the following steps, and then click OK.
   a. In the Name field, enter a name for the group policy (for example, safenetpolicy).
   b. Click More Options.
   c. In the Tunneling Protocols field, clear Inherit and select Clientless SSL VPN.

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

7. Click Apply.

**Configuring a Connection Profile for Clientless SSL VPN Access**

A connection profile consists of a set of records that determines tunnel connection policies. These records identify the servers to which the tunnel user is authenticated, as well as the accounting servers, if any, to which connection information is sent. They also identify a default group policy for the connection, and they contain protocol-specific connection parameters. Connection profiles include a small number of attributes that pertain to creating the tunnel itself. Connection profiles include a pointer to a group policy that defines user-oriented attributes.

2. On the main window, click Configuration.
3. In the left pane, click the **Remote Access VPN** tab, and then click **Clientless SSL VPN Access > Connection Profiles**.

4. In the right pane, under **Access Interfaces**, select **Allow Access** for **outside** and **inside** interfaces.

5. Under **Connection Profiles**, click **Add**.
6. On the **Add Clientless SSL VPN Connection Profile** window, in the left pane, click **Basic**, and then in the right pane, complete the following fields:

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter the name of the connection profile (for example, <strong>safenetprofile</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aliases</strong></td>
<td>Enter the alias for the connection profile (for example, <strong>safenet</strong>).</td>
</tr>
<tr>
<td><strong>AAA Server Group</strong></td>
<td>Select an appropriate AAA server group (for example, <strong>adgroup</strong>). This will be the first authentication method associated with the connection profile.</td>
</tr>
<tr>
<td><strong>DNS</strong></td>
<td>Enter the appropriate DNS details.</td>
</tr>
<tr>
<td><strong>Group Policy</strong></td>
<td>Select an appropriate group policy (for example, <strong>safenetpolicy</strong>).</td>
</tr>
<tr>
<td><strong>Clientless SSL VPN protocol SSL VPN client protocol</strong></td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

![Add Clientless SSL VPN Connection Profile](image)

*(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)*
In the left pane, click **Advanced > Secondary Authentication**, and then in the right pane, perform the following steps:

a. In **Server Group** field, select an appropriate server group (for example, `radiusgroup`).

b. Select **Use Primary username**.

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

7. In the left pane, click **Advance > Clientless SSL VPN**.
8. In the right pane, in the **Login and Logout Page Customization** field, click **Manage**.

9. On the **Configure GUI Customization Objects** window, select an appropriate customization template (for example, **DfltCustomization**), and then click **Edit**.
10. On the Edit Customization Object window, in the right pane, under Group Policies, select an appropriate group policy (for example, safenetpolicy).

11. In left pane, click Logon Page > Logon Form.

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
12. In right pane, change the value of the **Secondary Password Prompt** field to an appropriate text (for example, **Passcode**).

![Edit Customization Object](image1)

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

13. Click **OK** to close the **Edit Customization object** window.

14. Click **OK** to close the **Configure GUI Customization Objects** window.

![Configure GUI Customization Objects](image2)

*(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)*
15. On the **Add Clientless SSL VPN Connection Profile** window, in the right pane, in the **Login and Logout Page Customization** field, ensure that an appropriate template (for example, **DfltCustomization**) is selected, and then click **OK**.

*The screen image above is from Cisco®. Trademarks are the property of their respective owners.*
16. On the main window, in the right pane, perform the following steps, and then click **Apply**.
   c. **Under Login Page Setting**, select **Allow user to select connection profile on the login page**.
   d. **Under Connection Profiles**, in the connection profile list, in the **Enabled** column, select the check box for your connection profile.

![Configuration window](image)

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

Running the Solution

Clientless SSL VPN creates a secure remote-access VPN tunnel to Cisco ASA using a web browser without requiring a software or hardware client. It provides secure and easy access to a broad range of web resources and both web-enabled and legacy applications from almost any device that can connect to the Internet via HTTP. They include:

- Internal websites
- Web-enabled applications
- NT/Active directory file shares
- Email proxies, including POP3S, IMAP4S, and SMTPS
- Application Access (smart tunnel or port forwarding access to other TCP-based applications)
Before running this solution, ensure that Cisco ASA is configured for two-step authentication.

For this integration, the user is enrolled with a Push OTP token on the SAS cloud and is using an Android device.

1. In a web browser, open the following URL:
   
   https://<Public IP Address of Cisco ASA>

2. On the **SSL VPN Service** window, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GROUP</strong></td>
<td>Select an appropriate group alias (for example, safenet).</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Enter your domain user name or SAS user ID.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password associated with your domain user name.</td>
</tr>
<tr>
<td><strong>Passcode</strong></td>
<td>Enter one character.</td>
</tr>
</tbody>
</table>

3. Click **Login**.

   Cisco ASA will first evaluate the LDAP credential. If the LDAP authentication succeeds, the RADIUS request will be forwarded to SAS, and then SAS will trigger a Push OTP authentication request. You will receive a push notification on the configured mobile device.
4. On the registered mobile device, tap **APPROVE**.
   If you configured the radius attribute 31, the User IP will appear in the push notification.

![MobilePASS+](image)

5. Enter the **token PIN**, and then tap **Continue** to send the approval with OTP to SAS.

![Token Authentication](image)
You will receive a success sent message on the configured mobile device.

After successful authentication on SAS, you will be redirected to access the web page.

If the login credentials provided are authenticated successfully, you will be able to log in and can access the configured service and application.

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

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></td>
</tr>
<tr>
<td>Customer Portal</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>