SafeNet Authentication Service
Push OTP Integration Guide

Using LDAP and RADIUS Protocol for Cisco ASA
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>Applicability</td>
</tr>
<tr>
<td>Environment</td>
</tr>
<tr>
<td>Audience</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAS Cloud</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SAS</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
</tr>
<tr>
<td>Push OTP Prerequisites</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
</tr>
<tr>
<td>Creating Users Stores in SAS</td>
</tr>
<tr>
<td>Assigning an Authenticator in SAS</td>
</tr>
<tr>
<td>Adding Cisco ASA as an Authentication Node in SAS</td>
</tr>
<tr>
<td>Checking the SAS RADIUS Server’s IP Address</td>
</tr>
<tr>
<td>Enabling the Software Token Push OTP Setting</td>
</tr>
<tr>
<td>Enabling the Allowed Targets Policy</td>
</tr>
<tr>
<td>Configuring Cisco ASA</td>
</tr>
<tr>
<td>Creating AAA Server Groups</td>
</tr>
<tr>
<td>Adding a Group Policy</td>
</tr>
<tr>
<td>Configuring a Connection Profile for Clientless SSL VPN Access</td>
</tr>
<tr>
<td>Running the Solution</td>
</tr>
<tr>
<td>Support Contacts</td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Cisco 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 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:

- 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 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)**
- **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 SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

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

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

This document demonstrates the solution using the SAS cloud-hosted RADIUS service.

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

For more information on how to install and configure FreeRADIUS, refer to the **SafeNet Authentication Service FreeRADIUS Agent Configuration Guide**.
RADIUS Authentication Flow using SAS

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

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

1. A user attempts to log on to Cisco ASA using an Active Directory password and OTP.
2. Cisco ASA sends the LDAP request with the user’s Active Directory credentials to the LDAP server, that is, Microsoft Active Directory.
3. If successfully authenticated, Cisco ASA sends a RADIUS request to SafeNet Authentication Service for validation. Otherwise, the user will not be granted access.
4. SAS identifies the user or mobile device, and detects that the OTP field is having one character. 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).
5. The SAS authentication reply is sent back to Cisco ASA.
6. The user is granted or denied access to Cisco ASA based on the OTP value calculation results from SAS.

RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Cisco ASA, 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. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.
- On the client machine, set the RADIUS timeout value at least 60 seconds.
Push OTP Prerequisites

In order to use SAS Push OTP you will need:

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

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Cisco ASA using RADIUS protocol requires:

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding Cisco ASA as an Authentication Node in SAS, page 8
- Checking the SAS RADIUS Server’s IP Address, page 10
- Enabling the Software Token Push OTP Setting, page 12
- Enabling the Allowed Targets Policy, page 13

Creating Users Stores in SAS

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

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

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


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

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through 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 Cisco ASA as an Authentication Node in SAS

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

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.

![Auth Nodes module](image.png)

4. Under **Auth Nodes**, click **Add**.

![Add Auth Node](image.png)

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>Auth Node Name</strong></td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td><strong>Resource Name</strong></td>
<td>Enter a resource name which will identify in a push notification which</td>
</tr>
</tbody>
</table>
authentication node it relates to.

<table>
<thead>
<tr>
<th><strong>Low IP Address In Range</strong></th>
<th>Enter the IP address of the host that will authenticate with SAS.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure FreeRADIUS Synchronization</strong></td>
<td>Select this option.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td><strong>Confirm Shared Secret</strong></td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>

The authentication node is added to the system.

Checking the SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in Cisco ASA, check the IP address. The IP address will then be added to Cisco ASA as a RADIUS server at a later stage.

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

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

---

SafeNet Authentication Service: Push OTP Integration Guide
Using LDAP and RADIUS Protocol for Cisco ASA

Document PN: 007-013354-001, Rev. A, Copyright © 2015 Gemalto, Inc., All rights reserved.
3. In the **Auth Nodes** module, click the **Auth Nodes** link.

The SAS RADIUS server details are displayed.
Enabling the Software Token Push OTP Setting

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

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

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

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

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

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

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

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

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

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

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

---

**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 21
- Configuring a Connection Profile for Clientless SSL VPN Access, page 22
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 have been 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 the 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**.
4. In the right pane, under the **AAA Server Groups** section, 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**. This newly created AAA server group will be added to the list under the **AAA Server Group** section.

<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 the **AAA Server Groups** section, select the newly created server group (for example **adgroup**).

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

7. Under the **Servers in the Selected Group** section, 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. This newly created AAA server will be added to the list under the Servers in the Selected Group section.

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

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

9. Click Apply.
Creating the RADIUS-enabled AAA Server Group and its Servers

1. Open the 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 the AAA Server Groups section, 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**. This newly created AAA server group will be added to the list under the **AAA Server Group** section.

<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>Protocol</td>
<td>Select <strong>RADIUS</strong>.</td>
</tr>
</tbody>
</table>

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

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

![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**. This newly created AAA server is added in the list under the **Servers in the Selected Group** section.

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Select an appropriate interface that Cisco ASA uses in order to reach to the SAS RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name or IP Address</td>
<td>Enter the IP address of the SAS RADIUS server.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specifies the length of time, in seconds, that 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>Server Authentication Port</td>
<td>Enter 1812.</td>
</tr>
<tr>
<td>Server Secret Key</td>
<td>Enter the secret key shared between Cisco ASA and the SAS RADIUS server. Refer step 5 in “Adding Cisco ASA as an Authentication Node in SAS,” on page 8.</td>
</tr>
</tbody>
</table>

![Image]

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

9. 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.

1. Launch the Cisco Adaptive Security Device Manager (ASDM).
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. Adjacent to Tunneling Protocols, clear Inherit.
   d. Select the following:
      - Clientless SSL VPN
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.

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 **Clientless SSL VPN Access > Connection Profiles**.

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

5. In the right pane, under **Connection Profiles**, click **Add**.

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
6. On the **Add Clientless SSL VPN Connection Profile** window, in the left pane, click **Basic**.

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

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

7. Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter the name of the connection profile (for example, <em>safenetprofile</em>).</td>
</tr>
<tr>
<td><strong>Aliases</strong></td>
<td>Enter the alias for the connection profile (for example, <em>safenet</em>).</td>
</tr>
<tr>
<td><strong>AAA Server Group</strong></td>
<td>Select an appropriate AAA server group (for example, <em>adgroup</em>). 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, <em>safenetpolicy</em>).</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Enable SSL VPN client protocol</strong>.</td>
</tr>
</tbody>
</table>
8. On the **Add Clientless SSL VPN Connection Profile** window, in the left pane, click **Advanced > Secondary Authentication**.

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

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

9. 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**.

10. In the left pane, click **Clientless SSL VPN**.
11. In the right pane, in the **Login and Logout Page Customization** field, click **Manage**.

12. On **Configure GUI Customization Objects** window, select an appropriate customization template (for example **DfltCustomization**), and then click **Edit**.

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
13. On **Edit Customization Object** window, under **Group Policies**, select an appropriate group policy (for example, **safenetpolicy**).

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

14. In left pane, under **Logon Page**, select **Logon Form**.

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

![Edit Customization Object](image1.png)

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

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

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

![Configure GUI Customization Objects](image2.png)

*(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)*
18. On the Add Clientless SSL VPN Connection Profile window, in the right pane, in the Login and Logout Page Customization field, make sure an appropriate template (for example, DfltCustomization) is selected, and then click **OK**.
19. On the main window, in the right pane, perform the following steps, and then click **Apply**.
   
a. Under **Login Page Setting**, select **Allow user to select connection profile on the login page**.
   
b. Under **Connection Profiles**, in the connection profile list, select the check box in the **Enabled** column for your connection profile.

![Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles](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. Open the following URL in a web browser: **https://<Public IP Address of Cisco ASA>**
2. On the **SSL VPN Service** window, complete the following fields:

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

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

3. Click **Login**.

Cisco ASA will evaluate the LDAP credential first. If LDAP authentication succeeds, the RADIUS request will be forwarded to SAS, and SAS will trigger a Push OTP authentication request. The user receives a push notification on the configured mobile device.
4. Tap **APPROVE**.

![MobilePASS+](image)

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

![MobilePASS+](image)
The successful sent message is received 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 are logged in. You 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, Inc.</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>