SafeNet Authentication Manager
Integration Guide

Using RADIUS Protocol for Cisco ISE
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms’ resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2015 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-013384-001, Rev. A
Release Date: January 2016
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAM</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SAM</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Manager</td>
<td>7</td>
</tr>
<tr>
<td>Synchronizing Users Stores to SAM</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SAM’s Connector for OTP Authentication</td>
<td>7</td>
</tr>
<tr>
<td>Assigning a Token in SAM</td>
<td>8</td>
</tr>
<tr>
<td>Adding Cisco ISE as a RADIUS Client in IAS/NPS</td>
<td>8</td>
</tr>
<tr>
<td>Configuring SAM’s OTP Plug-In for Microsoft RADIUS Client</td>
<td>10</td>
</tr>
<tr>
<td>Configuring Cisco ASA</td>
<td>11</td>
</tr>
<tr>
<td>Creating AAA Server Groups</td>
<td>11</td>
</tr>
<tr>
<td>Adding an IP Address Pool</td>
<td>18</td>
</tr>
<tr>
<td>Adding a Group Policy</td>
<td>19</td>
</tr>
<tr>
<td>Configuring a Connection Profile for Network (Client) Access</td>
<td>21</td>
</tr>
<tr>
<td>Configuring a Connection Profile for Clientless SSL VPN Access</td>
<td>26</td>
</tr>
<tr>
<td>Configuring Cisco ISE</td>
<td>31</td>
</tr>
<tr>
<td>Configuring Network Devices</td>
<td>31</td>
</tr>
<tr>
<td>Configuring External Identity Sources</td>
<td>34</td>
</tr>
<tr>
<td>Configuring an Authentication Policy</td>
<td>37</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>39</td>
</tr>
<tr>
<td>Using the Clientless SSL VPN</td>
<td>39</td>
</tr>
<tr>
<td>Using the Cisco AnyConnect Secure Mobility Client</td>
<td>41</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>42</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 ISE.

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 Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

Cisco Identity Service Entity (ISE)

Cisco ISE is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. The unique architecture of Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can then use that information to make proactive governance decisions by tying identity to various network elements including access switches, wireless LAN controllers (WLCs), Virtual Private Network (VPN) gateways, and data center switches. Cisco ISE is a key component of the Cisco Security Group Access Solution.

Cisco Adaptive Security Appliance (ASA)

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

Cisco ASA is valuable and flexible in a way that it can be used as a security solution for both small and large networks.

This document describes how to:

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

It is assumed that the Cisco ISE and Cisco ASA environments are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager, and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager installation modes, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

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

Applicability

The information in this document applies to:

- SafeNet Authentication Manager—A server version of SAM that is used to deploy the solution on-premises in the organization.
Environment

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

- **SafeNet Authentication Manager 8.2 HF 493**—A server version of SAM that is used to deploy the solution on-premises in the organization.
- **Cisco ISE**—Version 1.4.0.253
- **Cisco ASA**—Version 9.2(2)4
- **Cisco Adaptive Security Device Manager (ASDM)**—Version 7.3(1)101
- **Cisco Secure Mobility Client**—Version 3.1.04072

Audience

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

RADIUS-based Authentication using SAM

SafeNet's OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SAM.

SAM's OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS, providing strong authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*. 
**RADIUS Authentication Flow using SAM**

SafeNet Authentication Manager 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 ISE.

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 Cisco ISE. Otherwise, the user will not be granted access.
4. Cisco ISE sends RADIUS request with the user’s credentials to SafeNet Authentication Manager for validation.
5. The SAM authentication reply is sent back to Cisco ISE.
6. Cisco ISE in turn sends the reply back to Cisco ASA.
7. The user is granted or denied access to Cisco ASA based on the OTP value calculation results from SAM.

**RADIUS Prerequisites**

To enable SafeNet Authentication Manager to receive RADIUS requests from Cisco ISE, ensure the following:

- End users can authenticate from the Cisco ISE environment with a static password before configuring the Cisco ISE to use RADIUS authentication.
- Ports 1812/1813 are open to and from Cisco ISE.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.
Configuring SafeNet Authentication Manager

The deployment of multi-factor authentication using SAM with Cisco ISE using the RADIUS protocol requires the following:

- Synchronizing Users Stores to SAM, page 7
- Configuring SAM’s Connector for OTP Authentication, page 7
- Assigning a Token in SAM, page 4
- Adding Cisco ISE as a RADIUS Client in IAS/NPS, page 8
- Configuring SAM’s OTP Plug-In for Microsoft RADIUS Client, page 10

Synchronizing Users Stores to SAM

SAM manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Configuring SAM’s Connector for OTP Authentication

SafeNet Authentication Manager is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications, including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected the Simplified OTP-only configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The Simplified OTP-only configuration is as follows:

- Connectors—SAM Connector for OTP Authentication is installed
- SAM Back-end Service—Activated on this server; scheduled to operate every 24 hours

In addition, the SAM default policy is set as follows:

- OTP support (required for OTP) is selected in the Token Initialization settings.
The SAM Connector for OTP Authentication is set, by default, to enable enrollment of OTP tokens without requiring changes in the Token Policy Object (TPO) settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

Assigning a Token in SAM

SAM supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through Cisco ISE.

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- SafeNet GOLD
- SMS tokens
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)
- SafeNet eToken 3400
- SafeNet eToken 3500

Tokens can be assigned to users as follows:

- **SAM Management Center**—Management site used by SAM administrators and helpdesk personnel for token enrollment and lifecycle management.
- **SAM Self-Service Center**—Self-service site used by end users for managing their tokens.
- **SAM Remote Service**—Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet’s tokens and service portals, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

Adding Cisco ISE as a RADIUS Client in IAS/NPS

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in Cisco ISE.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in Cisco ISE.
Cisco ISE must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Cisco ISE for authentication.

**NOTE:** This document assumes that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager. The details below refer to NPS, and are very similar to IAS.

1. Click **Start > Administrative Tools > Network Policy Server**.
2. From the NPS web console, expand **RADIUS Clients and Servers**, right-click **RADIUS Clients**, and then click **New**.

![Network Policy Server](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
3. On the New RADIUS Client window, complete the following fields on the Settings tab:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable this RADIUS client</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Friendly name</td>
<td>Enter a RADIUS client name.</td>
</tr>
<tr>
<td>Address (IP or FQDN)</td>
<td>Enter the Cisco ISE IP address or FQDN.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>Enter the shared secret for the RADIUS client. This entry must match the shared secret that was used when the RADIUS server was configured in Cisco ISE.</td>
</tr>
<tr>
<td>Confirm shared secret</td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>

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

4. Click OK.

Cisco ISE is added as a RADIUS client in NPS.

Configuring SAM’s OTP Plug-In for Microsoft RADIUS Client

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) as Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

SAM’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS server. When configured, users who access their
network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

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 11
- Adding an IP Address Pool, page 18
- Adding a Group Policy, page 19
- Configuring a Connection Profile for Network (Client) Access, page 21
- Configuring a Connection Profile for Clientless SSL VPN Access, page 26

Creating AAA Server Groups

If you want 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 name. Each server group is associated with only one type of server, such as Kerberos, LDAP, NT, RADIUS, SDI, or TACACS+.

For this integration, we will use LDAP and RADIUS external AAA servers for authentication.

Create two server groups (for example, adgroup and radiusgroup). The adgroup server group must be configured with the external LDAP server using LDAP protocol, and the radiusgroup server group must be configured with the external RADIUS server using RADIUS protocol.

Creating an 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 the Configuration tab.
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 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**.

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

![Add AAA Server Group](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, the newly created AAA server group is added in the list under **AAA Server Groups**. 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 **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.</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. <em>sAMAccountName</em> is the default attribute in the Microsoft Active Directory.</td>
</tr>
<tr>
<td><strong>Login DN</strong></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><strong>Login Password</strong></td>
<td>Enter the password for the Distinguished Name account.</td>
</tr>
</tbody>
</table>

![Add AAA Server window](image1)

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

9. The newly created AAA server will be added in the list 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 the Configuration tab.
3. In the left pane, click the Remote Access VPN tab, and then click AAA/Local Users > AAA Server Groups.

![Cisco ASA Configuration Screen](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.

![Cisco ASA AAA Server Groups Screen](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, <strong>radiusgroup</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select <strong>RADIUS</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, the newly created AAA server group is added in the list under **AAA Server Group**. 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 **Servers in the Selected Group**, click **Add**.

![Add AAA Server window](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>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Select an appropriate interface that Cisco ASA uses in order to reach Cisco ISE.</td>
</tr>
<tr>
<td>Server Name or IP Address</td>
<td>Enter the Cisco ISE IP address.</td>
</tr>
<tr>
<td>Server Authentication Port</td>
<td>Enter the 1812.</td>
</tr>
<tr>
<td>Server Secret Key</td>
<td>Enter the secret key shared between Cisco ASA and Cisco ISE.</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 is added in the list under **Servers in the Selected Group**. Click **Apply**.
Adding an IP Address Pool

Cisco ASA can use address pools for assigning IP addresses to remote access clients.

1. Open Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
2. On the main window, click the **Configuration** tab.
3. In the left pane, click the **Remote Access VPN** tab, and then click **Network (Client) Access > Address Assignment > Address Pools**.

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

4. In the right pane, click **Add**.

   (The screen image above is from Cisco. Trademarks are the property of their respective owners.)
5. On the **Add IPv4 Pool** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter the name for the address pool. The length can be up to 64 characters (for example, <code>vpnpool</code>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Starting IP Address</strong></td>
<td>Enter the first IP address available for the IP pool. The format of the IP address must be <strong>0.0.0.0</strong>.</td>
</tr>
<tr>
<td><strong>Ending IP Address</strong></td>
<td>Enter the last IP address available for the IP pool. The format of the IP address must be <strong>0.0.0.0</strong>.</td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td>Enter the subnet mask on which the IP pool resides.</td>
</tr>
</tbody>
</table>

6. 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. The 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 individually for each user.

**To add a group policy:**

1. Open the Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
2. On the main window, click the **Configuration** tab.
3. In the left pane, click the **Remote Access VPN** tab, and then click **Network (Client) Access > Group Policies**.

![Remote Access VPN](image)

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

4. In the right pane, click **Add**.

![Group Policies](image)

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the group policy (for example, safenetpolicy).</th>
</tr>
</thead>
<tbody>
<tr>
<td>More Options</td>
<td>Click <strong>More Options</strong> to expand the window and then do the following in the <strong>Tunneling Protocols</strong> field:</td>
</tr>
<tr>
<td></td>
<td>1. Clear <strong>Inherit</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Select <strong>Clientless SSL VPN</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Select <strong>SSL VPN Client</strong>.</td>
</tr>
</tbody>
</table>

![Add Internal Group Policy window](image)

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

6. Click **Apply**.

**Configuring a Connection Profile for Network (Client) 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.

1. Open Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
2. On the main window, click the **Configuration** tab.
3. In the left pane, click the **Remote Access VPN** tab, and then click **Network (Client) Access > AnyConnect Connection Profiles**.

![Remote Access VPN](image1)

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

4. In the right pane, under **Access Interface**, perform the following steps:
   
a. Select **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below**.
   
b. In the table, for **outside** and **inside** interfaces, in the **SSL Access** column, select **Allow Access** and **Enable DTLS**.

![Access Interfaces](image2)

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

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

![Connection Profiles](image3)

*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*
6. On the **Add AnyConnect Connection Profile** window, in the left pane, click **Basic**. In the right pane, 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 for the connection profile (for example, <strong>safenetprofile</strong>).</td>
</tr>
<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>Client Address Pools</strong></td>
<td>Click <strong>Select</strong> and then assign an address pool.</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>Enable SSL VPN client protocol</strong></td>
<td>Select this option.</td>
</tr>
<tr>
<td><strong>DNS Server</strong></td>
<td>Enter the DNS server detail.</td>
</tr>
</tbody>
</table>

*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*
7. On the **Add AnyConnect Connection Profile** window, perform the following steps:
   a. In the left pane, click **Advanced > Secondary Authentication**.
   b. In the right pane, in the **Server Group** field, select an appropriate server group (for example, **radiusgroup**).
   c. Click **OK**.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
8. On the main window, in the right pane, perform the following steps, and then click **Apply**:
   a. Under **Access Interfaces**, select **Bypass interface access lists for inbound VPN sessions**.
   b. Under **Login Page Setting**, select **Allow user to select connection profile on the login page**.
   c. Under **Connection Profiles**, in the connection profile list, select the check box in the **SSL Enabled** column for your connection profile.

   ![Configuration page screenshot](image)

   *(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*
Configuring a Connection Profile for Clientless SSL VPN Access

1. Open Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
2. On the main window, click the Configuration tab.
3. In the left pane, click the Remote Access VPN tab, and then click Clientless SSL VPN Access > Portal > Customization.

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

4. In the right pane, under Customization objects, select the DfltCustomization template, and then click Assign. The template will be used for the Login page and the main SSL portal.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
5. On the **Assign GUI Customization: DfltCustomization** window, select a **Group Policy** (for example, `safenetpolicy`), or **Connection Profile** (for example, `safenetprofile`), or both, and then click **OK**.

6. On the main window, click the **Configuration** tab.

7. In the left pane, click **Clientless SSL VPN Access > Connection Profile**.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
8. In the right pane, under **Connection Profiles**, in the connection profile list, select the check box in the **Enabled** column for your connection profile (for example, **safenetprofile**), and then click **Edit**.

9. On the **Edit Clientless SSL VPN Connection Profile: safenetprofile** window, in the left pane, click **Basic**.

10. In the right pane, complete the following fields:

<table>
<thead>
<tr>
<th>AAA Server Group</th>
<th>Select an appropriate AAA server group (for example, <strong>adgroup</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Group</td>
<td>Select an appropriate DNS server group.</td>
</tr>
<tr>
<td>Group Policy</td>
<td>Select an appropriate group policy (for example, <strong>safenetpolicy</strong>).</td>
</tr>
<tr>
<td>Enable clientless SSL VPN protocol</td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
11. In the left pane, click **Advanced > Secondary Authentication**.

12. In the right pane, in the **Server Group** field, select an appropriate server group (for example, **radiusgroup**).

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
13. In the left pane, click **Advanced > Clientless SSL VPN**, and then perform the following steps:
   a. In the right pane, in the **Login and Logout Page Customization** field, select **DfltCustomization**.
   b. Under **Connection Aliases**, select an appropriate alias (for example, **safenet**), and then select the option in the **Enabled** column.
   c. Click **OK**.
   d. Click **Apply**.

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

Configuring Cisco ISE for RADIUS authentication requires the following:

- Configuring Network Devices, page 31
- Configuring External Identity Sources, page 34
- Configuring an Authentication Policy, page 37

Configuring Network Devices

A network device is an authentication, authorization, and accounting (AAA) client through which AAA service requests are attempted, for example, switches, routers, and so on. The network device definition enables Cisco ISE to interact with the network devices that are configured. A network device that is not defined cannot receive AAA services from Cisco ISE.

1. Open the following URL in a web browser:

   https://<Management IP Address of Cisco ISE>/admin

2. On the Identity Services Engine login window, enter the username and password, and then click Login.

   (The screen image above is from Cisco. Trademarks are the property of their respective owners.)
3. On the Cisco ISE dashboard, click **Administration > Network Resources > Network Devices.** Then, in the right pane, click **Add.**

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
4. Complete the following fields and then click **Submit**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the network device (for example, <strong>Cisco_ASA</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the client (ASA). This field includes the IP address and subnet masks that are associated with the device. A single address or a range, the routable IP address should be one with which the Cisco ISE appliance can communicate.</td>
</tr>
<tr>
<td>Authentication Settings</td>
<td>Select to expand the <strong>Authentication Settings</strong> section.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret same as entered in step 8 of “Creating the RADIUS-enabled AAA Server Group and its Servers”, on page 15.</td>
</tr>
</tbody>
</table>

![Network Devices Section](image)

*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*
The network device is added and listed in the network devices list.

Configuring External Identity Sources

Cisco ISE integrates with external identity sources to validate credentials in user authentication functions. Cisco ISE supports any RADIUS RFC 2865-compliant server as an external identity source. RADIUS identity sources can work with any RADIUS token server that is used to authenticate the user.

1. On the Cisco ISE dashboard, click Administration > Identity Management > External Identity Sources.
2. In left pane, click **RADIUS Token**.

![Image 1](image1.png)
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)

3. In the right pane, click **Add**.

4. On the **General** tab, in the **Name** field, enter a name for the RADIUS server (for example, **SAM_RADIUS_Server**).

![Image 2](image2.png)
(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
5. Click the **Connection** tab, complete the following fields, and then click **Submit**.

<table>
<thead>
<tr>
<th><strong>Host IP</strong></th>
<th>Enter the IP address of the primary SAM RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret same as entered in step 3 of &quot;Adding Cisco ISE as a RADIUS Client in IAS/NPS&quot;, on page 8.</td>
</tr>
<tr>
<td><strong>Authentication Port</strong></td>
<td>Enter the port number on which the SAM RADIUS server is listening. The default port number is <strong>1812</strong>.</td>
</tr>
</tbody>
</table>

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

The RADIUS token identity source is added and listed in the RADIUS Token Identity Sources list.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
Configuring an Authentication Policy

Authentication policies define the protocols that Cisco ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

1. On the Cisco ISE dashboard, click Policy.
2. Select Default Rule and then click Edit.
3. Click the plus (+) sign in the default policy.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
4. In the **Identity Source** field, select an appropriate identity source (for example, `SAM_RADIUS_Server`).

5. Click **Done**.

*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*
6. **Click Save.** A successful message is displayed.

Running the Solution

You can use the following methods to securely connect to Cisco ASA through Cisco ISE:

- Using the Clientless SSL VPN, page 39
- Using the Cisco AnyConnect Secure Mobility Client, page 41

Using the Clientless SSL VPN

The 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.

In this solution, the SafeNet eToken PASS is used as the enrolled OTP token.

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.</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>Enter the password associated with your domain user name.</td>
</tr>
</tbody>
</table>

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
2nd Username | Enter your SAM user ID.
---|---
2nd Password | Generate an OTP using SafeNet eToken PASS and then enter it in this field.

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

3. Click **Login**.

If the login credentials are validated, you are provided access to the service and application.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
Using the Cisco AnyConnect Secure Mobility Client

The Cisco AnyConnect Secure Mobility Client provides remote users with secure VPN connections to the Cisco ASA using the Secure Socket Layer (SSL) protocol and the Datagram TLS (DTLS) protocol. AnyConnect provides remote end users with the benefits of a Cisco SSL VPN client, and supports applications and functions that are unavailable to a clientless, browser-based SSL VPN connection.

In this solution, the SafeNet eToken PASS is used as the enrolled OTP token.

1. Start the Cisco AnyConnect Secure Mobility Client application from Start > All Programs > Cisco > Cisco AnyConnect Secure Mobility Client.

2. On the Cisco AnyConnect Secure Mobility Client window, in the VPN field, enter the fully qualified domain name or IP address for Cisco ASA, and then click Connect.

3. Complete the following fields and then click OK.

<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.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password associated with your domain user name.</td>
</tr>
<tr>
<td>Second Username</td>
<td>Enter your SAM user ID.</td>
</tr>
<tr>
<td>Second Password</td>
<td>Generate an OTP using SafeNet eToken PASS and then enter it in this field.</td>
</tr>
</tbody>
</table>

If authentication is successful, the VPN session is established, and the following message is displayed.

(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>