SafeNet Authentication Manager
Integration Guide

Using RADIUS Protocol for Cisco Secure ACS
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012887-001, Rev. B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>April 2015</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland  21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
Contents

Third-Party Software Acknowledgement ................................................................. 4
Description .............................................................................................................. 4
Applicability ............................................................................................................ 5
Environment .......................................................................................................... 5
Audience ................................................................................................................. 5
RADIUS-based Authentication using SAM ......................................................... 5
RADIUS Authentication Flow using SAM ............................................................ 6
Prerequisites .......................................................................................................... 6
Configuring SafeNet Authentication Manager ...................................................... 7
  Synchronizing User Stores to SafeNet Authentication Manager ......................... 7
  Configuring SAM’s Connector for OTP Authentication .................................... 7
  Token Assignment in SAM .................................................................................. 8
Adding Cisco Secure ACS as a RADIUS Client in IAS/NPS ............................... 8
SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration ..................... 10
Configuring Cisco ASA ......................................................................................... 11
  Creating AAA Server Groups ........................................................................ 11
  Adding an IP Address Pool ................................................................................ 17
  Adding a Group Policy ..................................................................................... 19
  Configuring a Connection Profile for Network (Client) Access ....................... 21
  Configuring a Connection Profile for Clientless SSL VPN Access .................. 25
Configuring Cisco Secure ACS .......................................................................... 30
  Configuring Network Devices and AAA Clients .......................................... 30
  Configuring User and Identity Stores ............................................................. 31
  Configuring Access Policies .......................................................................... 33
Running the Solution ............................................................................................ 36
  Using the Clientless SSL VPN ....................................................................... 36
  Using the Cisco AnyConnect Secure Mobility Client .................................. 38
Support Contacts .................................................................................................. 39
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Cisco Secure ACS.

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 Secure Access Control Server (ACS) is an access policy control platform that helps you comply with growing regulatory and corporate requirements. By integrating with your other access control systems, it helps improve productivity and contain costs. It supports multiple scenarios simultaneously, including:

- **Device administration**: Authenticates administrators, authorizes commands, and provides an audit trail
- **Remote access**: Works with VPN and other remote network access devices to enforce access policies
- **Wireless**: Authenticates and authorizes wireless users and hosts, and enforces wireless-specific policies
- **Network admission control**: Communicates with posture and audit servers to enforce admission control policies

Cisco Secure ACS uses two distinct protocols for AAA services—Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS+).

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 that stops attacks before they spread through the network.

Cisco ASA can be used as a security solution for both the small and large networks.

This document describes how to:

- Configure Cisco Secure ACS to work with SafeNet Authentication Manager in RADIUS mode.

It is assumed that the Cisco Secure ACS 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 Secure ACS 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 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 Secure ACS**—Version 5.4.0.46.0a
- **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 Secure ACS and Cisco ASA, and are interested in adding multi-step and 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 SafeNet Authentication Manager (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 Secure ACS.

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 will send a TACACS request to Cisco Secure ACS. Otherwise, the user will not be granted access.
5. The SAM authentication reply is sent back to the Cisco Secure ACS.
6. Cisco Secure ACS 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.

Prerequisites

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

- End users can authenticate through the Cisco Secure ACS and Cisco ASA environment with a static password before configuring Cisco Secure ACS to use RADIUS authentication.
- Ports 1812/1813 are open to and from Cisco Secure ACS.
- 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 the RADIUS client for encryption, decryption, and digital signature purposes.
- Cisco AnyConnect Secure Mobility Client is installed on the client machine.
- SafeNet e-Token PASS is already enrolled as an OTP token in SAM.
Configuring SafeNet Authentication Manager

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

- Synchronizing User Stores to SafeNet Authentication Manager, page 7
- Configuring SAM’s Connector for OTP Authentication, page 7
- Token Assignment in SAM, page 8
- Adding Cisco Secure ACS as a RADIUS Client in IAS/NPS, page 8
- SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration, page 10

Synchronizing User Stores to SafeNet Authentication Manager

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 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*.

**Token Assignment in SAM**

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

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 help desk 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 Secure ACS 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 Secure ACS.

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 Secure ACS.

Cisco Secure ACS must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Cisco Secure ACS for authentication.
NOTE: It is assumed 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.

To add a RADIUS client:

2. From the NPS web console, in the left pane, 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 DNS)</td>
<td>Enter the IP address or DNS of Cisco Secure ACS.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>Enter the shared secret for the RADIUS client. The value must be the same when configuring the RADIUS server in Cisco Secure ACS.</td>
</tr>
<tr>
<td>Confirm shared secret</td>
<td>Re-enter the shared secret to confirm it.</td>
</tr>
</tbody>
</table>
4. Click OK.

Cisco Secure ACS is added as a RADIUS client in NPS.

**SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration**

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.

The following is required to configure Cisco ASA for two-step and multi-factor authentication:

- Creating AAA Server Groups, page 11
- Adding an IP Address Pool, page 17
- 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 25

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 TACACS+ external AAA servers for authentication.

Create two server groups; for example, adgroup and tacacsgroup. The adgroup must be configured with the external LDAP server using the LDAP protocol, and tacacsgroup should be configured with the external TACACS server using the TACACS+ 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 Remote Access VPN > 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**.

![Screenshot of the AAA Server Groups section](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 is added in 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 LDAP.</td>
</tr>
</tbody>
</table>

![Screenshot of the 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 the **AAA Server Groups** section, select the newly created server group; for example **adgroup**.

![Configuration window](image)

*(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**.

![Server addition 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**. 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 the LDAP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name or IP Address</td>
<td>Enter the IP address 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. <strong>sAMAccountName</strong> 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>-----------------</td>
<td>-----------------------------------------------------------------------------------------------------------</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 TACACS-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 Remote Access VPN > AAA/Local Users > AAA Server Groups.

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

5. On the Add AAA Server Group window, complete the following fields, and then click OK. This newly created AAA server group is added in the list under the AAA Server Group section.

<table>
<thead>
<tr>
<th>AAA Server Group</th>
<th>Enter a server group name; for example, tacacsgroup.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select TACACS+</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, **tacacsgroup**.

7. Under the **Servers in the Selected Group** section, click **Add**.
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 will use to reach Cisco ACS and the RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name or IP Address</td>
<td>Enter the IP address that Cisco ASA will use to reach Cisco ACS.</td>
</tr>
<tr>
<td>Server Secret Key</td>
<td>Enter the secret key shared between Cisco ASA and Cisco ACS.</td>
</tr>
</tbody>
</table>

9. Click Apply.

Adding an IP Address Pool

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

To add an IP address pool:

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

![Image: Add IP Pool window]

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

4. On the **Add IP Pool** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter the name of the address pool. The length can be up to 64 characters; for example, <strong>vpnpool</strong>.</td>
</tr>
<tr>
<td><strong>Starting IP Address</strong></td>
<td>Enter the first IP address available for this IP pool. The format of the IP address should 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 this IP pool. The format of the IP address should be <strong>0.0.0.0</strong>.</td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td>Enter the subnet on which this IP pool resides.</td>
</tr>
</tbody>
</table>

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

5. 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 Configuration.
4. In the right pane, click Add.
5. 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. Clear Tunneling Protocols and then select the following:
      • Clientless SSL VPN
      • SSL VPN Client
6. Click **Apply**.

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

To configure a connection profile:

1. Open the Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
2. On the main window, click Configuration. Then, in the left pane, click Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile.

3. 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, under the SSL Access column, select Allow Access and Enable DTLS.

4. In the right pane, under Connection Profiles, click Add.
5. 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>Name</th>
<th>Enter the name of the connection profile; for example, <strong>safenetprofile</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aliases</td>
<td>Enter the alias for the connection profile; for example, <strong>safenet</strong>.</td>
</tr>
<tr>
<td>AAA Server Group</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>Client Address Pools</td>
<td>Click <strong>Select</strong> and assign an address pool.</td>
</tr>
<tr>
<td>Group Policy</td>
<td>• Select an appropriate group policy; for example, <strong>safenetpolicy</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Enable SSL VPN client protocol</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Fill in the <strong>DNS Server</strong> detail.</td>
</tr>
</tbody>
</table>

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
6. 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, **tacacsgroup**.
   c. Click **OK**.

*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*
7. On the main window, in the right pane, perform the following steps:
   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.

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

8. Click **Apply**.
Configuring a Connection Profile for Clientless SSL VPN Access

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

![Cisco ASDM Configuration Window]

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

3. In the right pane, in the Customization objects list, select DfltCustomization, and then click Assign. The DfltCustomization template will be used for the login page and main SSL portal.

4. On the Assign GUI Customization: DfltCustomization window, ensure that a group policy (for example, safenetpolicy) or connection profile (for example, safenetprofile), or both are selected. Click OK.

![Assign GUI Customization Window]

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
5. On the main window, click **Configuration**. In the left pane, click **Clientless SSL VPN Access > Connection Profile**.

   ![Diagram of Remote Access VPN](image)

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

6. In the right pane, under **Connection Profiles**, select a profile (for example, **safenetprofile**), and then click **Edit**.

   ![Connection Profiles](image)

   *(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*
7. On the **Edit Clientless SSL VPN Connection Profile: safenetprofile** window, in the left pane, click **Basic**. In the right pane, complete the following fields:

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

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

8. In the left pane, click **Advanced > Secondary Authentication**.
9. In the right pane, in the **Server Group** field, select an appropriate server group; for example, **tacacsgroup**.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
10. In the left pane, select **Clientless SSL VPN**.

11. In the right pane, perform the following steps:
   a. 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.

12. Click **OK**.

13. Click **Apply**.
Configuring Cisco Secure ACS

Cisco Secure ACS is an authentication, authorization, and accounting (AAA) access control server. Cisco Secure ACS provides access control to network access servers (NAS) through AAA, an architectural framework for configuring a set of three independent security functions consistently.

Cisco Secure ACS uses two distinct protocols for AAA services—Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS+).

To configure Cisco Secure ACS for RADIUS authentication, you must do the following:

- Configuring Network Devices and AAA Clients, page 30
- Configuring User and Identity Stores, page 31
- Configuring Access Policies, page 33

Configuring Network Devices and AAA Clients

It is important to remember that a device should be in the ACS repository before AAA requests from that device will be accepted. Add an AAA client to the ACS database and enable communications using the TACACS+ or RADIUS protocol.

**To configure network devices and AAA clients:**

1. Log on to Cisco Secure ACS.
2. On the main window, in the left pane, click Network Resources > Network Devices and AAA Clients.

![Network Resources Menu](image)

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

3. In the right pane, click Create.
4. Complete the following fields, and then click **Submit**:

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter a name for the network device (Cisco ASA).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP</strong></td>
<td>Enter the IP address of the network device (Cisco ASA).</td>
</tr>
<tr>
<td><strong>Authentication Options</strong></td>
<td>Select TACACS+.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the secret text shared between Cisco ASA and Cisco Secure ACS.</td>
</tr>
</tbody>
</table>

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

**Configuring User and Identity Stores**

Cisco Secure ACS manages your network devices and other ACS clients by using the ACS network resource repositories and identity stores. When a host connects to the network through Cisco Secure ACS requesting access to a particular network resource, Cisco Secure ACS authenticates the host and decides whether the host can communicate with the network resource.

To authenticate and authorize a user or host, Cisco Secure ACS uses the user definitions in identity stores. There are two types of identity stores:

- **Internal**: Identity stores that Cisco Secure ACS maintains locally (also called local stores) are called internal identity stores. For internal identity stores, Cisco Secure ACS provides interfaces for you to configure and maintain user records.

- **External**: Identity stores that reside outside of Cisco Secure ACS are called external identity stores. Cisco Secure ACS requires configuration information to connect to these external identity stores to perform authentication and obtain user information.

For authentication (second-step authentication), in this integration, we will use external identity stores, that is, a RADIUS Identity Server.
To configure external identity store:

1. Log on to Cisco Secure ACS.

2. On the main window, in the left pane, click Users and Identity Stores > External Identity Stores > RADIUS Identity Servers.

3. In the right pane, click Create.

4. In the right pane, on the General tab, complete the following fields, and then click Submit:

   - **Name**: Enter a name of your identity store (for example, radiusserver).
   - **Hostname AAA**: Enter the IP address of the identity store.
   - **Shared Secret**: Enter the secret text shared between Cisco Secure ACS and the RADIUS server.
   - **Authentication Port**: Enter 1812.
Configuring Access Policies

In Cisco Secure ACS, policy drives all activities. Policies consist mainly of rules that determine the action of the policy. You create access services to define authentication and authorization policies for requests. A global service selection policy contains rules that determine which access service processes an incoming request.

To configure access policies:

1. Log on to Cisco Secure ACS.
2. On the main window, in the left pane, click Access Policies > Access Services > Service Selection Rules.

3. In the right pane, make sure that a rule is added in which TACACS protocol is pointing to the Default Device Admin service.
4. In the left pane, click **Access Policies > Access Services > Default Device Admin > Identity.**

5. In the right pane, in the **Identity Source** field, click **Select.**
6. On the **Identity Store** window, select your identity source (for example, `radiusserver`), and then click **OK**.

   ![Identity Store Window](image)

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

7. Click **Save Changes**.
Running the Solution

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

- Using the Clientless SSL VPN, page 36
- Using the Cisco AnyConnect Secure Mobility Client, page 38

Using the Clientless SSL VPN

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
- Microsoft Web App to Exchange Server 2010 in 8.4(2) and later
- Application Access (smart tunnel or port forwarding access to other TCP-based applications)

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

To use clientless SSL VPN:

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 password associated with your domain user name.</td>
</tr>
<tr>
<td>2nd Username</td>
<td>Enter your SAM user ID.</td>
</tr>
<tr>
<td>2nd Password</td>
<td>Generate an OTP using SafeNet eToken PASS and enter it in this field.</td>
</tr>
</tbody>
</table>
3. **Click Login.**

If the login credentials provided are authenticated successfully, you are logged in. You can access the service and application configured.
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. 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 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 enter it in this field.</td>
</tr>
</tbody>
</table>

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
If authentication is successful, the VPN session will be established and you will see the following message on your system.

![VPN Connected to ciscoasa.safenet.com](image)

(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 SafeNet Customer Support. SafeNet 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 SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></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><strong>Technical Support</strong></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 SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>