SafeNet Authentication Manager
Integration Guide

Using RADIUS Protocol for Cisco ASA
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012965-001, 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
SafeNet Authentication Manager............................................................................................................................... 4
Cisco ASA................................................................................................................................................................. 4
Applicability............................................................................................................................................................... 4
Environment ............................................................................................................................................................. 5
Audience.................................................................................................................................................................... 5
RADIUS-based Authentication using SAM .............................................................................................................. 5
RADIUS Authentication Flow using SAM................................................................................................................... 6
RADIUS Prerequisites.............................................................................................................................................. 6
Configuring SafeNet Authentication Manager........................................................................................................ 7
  Synchronizing User Stores with SAM..................................................................................................................... 7
  Configuring SAM’s Connector for OTP Authentication.......................................................................................... 7
  Assigning an Authenticator in SAM........................................................................................................................ 8
  Adding Cisco ASA as a RADIUS Client in IAS/NPS.............................................................................................. 9
  Configuring SAM’s OTP Plug-in for Microsoft RADIUS Client ............................................................................ 10
Configuring Cisco ASA............................................................................................................................................ 11
  Creating a RADIUS-enabled AAA Server Group................................................................................................... 11
  Adding an IP Address Pool.................................................................................................................................... 14
  Adding a Group Policy.......................................................................................................................................... 15
  Configuring a Connection Profile for Network (Client) Access........................................................................... 17
  Configuring a Connection Profile for Clientless SSL VPN Access....................................................................... 21
Running the Solution ............................................................................................................................................... 24
  Using Clientless SSL VPN Access....................................................................................................................... 24
  Using the Cisco AnyConnect Secure Mobility Client.......................................................................................... 26
  Using the Cisco VPN Client (IPsec)...................................................................................................................... 27
Support Contacts....................................................................................................................................................... 29
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet 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 Manager

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 ASA

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

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Cisco ASA using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Manager.
- Configure Cisco ASA to work with SafeNet Authentication Manager 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 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 additional information on SafeNet Authentication Manager installation modes, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

Cisco ASA can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with SafeNet Authentication 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**—Version 8.2 (HF 493)
- **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 ASA, 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 SafeNet Authentication Manager (SAM).

SAM's OTP plug-in for Microsoft RADIUS Client works with either Microsoft’s IAS or NPS, and provides 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 ASA.

1. A user attempts to log on to Cisco ASA using an OTP authenticator.
2. Cisco ASA sends a RADIUS request with the user’s credentials to SAM for validation.
3. The SAM authentication reply is sent back to Cisco ASA.
4. 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 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 the RADIUS client for encryption, decryption, and digital signatures.
- Cisco AnyConnect Secure Mobility Client is installed on the client machine.
- Cisco VPN client is installed on the client machine.
- SafeNet eToken PASS is already enrolled as an OTP token in SAM.
Configuring SafeNet Authentication Manager

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

- Synchronizing User Stores with SAM, page 7
- Configuring SAM’s Connector for OTP Authentication, page 7
- Assigning an Authenticator in SAM, page 8
- Configuring a Connection Profile for Network (Client) Access, page 9
- Configuring a Connection Profile for Clientless SSL VPN Access, page 10

Synchronizing User Stores with SAM

SAM manages and maintains OTP token information in its data store, including the token’s status and user assignment, and the OTP algorithm used to generate the OTP. 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 (Token Policy Object) 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 an Authenticator in SAM

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

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 through:

- **SAM Management Center**—Management site used by SAM administrators and help desk 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 ASA 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 ASA.

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 ASA.

Cisco ASA must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Cisco ASA 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.

2. From the NPS web console, expand RADIUS Clients and Servers, right-click RADIUS Clients, and then click New.

(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 name for the RADIUS client.</td>
</tr>
<tr>
<td>Address (IP or DNS)</td>
<td>Enter the Cisco ASA IP address or DNS.</td>
</tr>
<tr>
<td>Manual/Generate</td>
<td>Select <strong>Manual</strong>.</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 ASA.</td>
</tr>
<tr>
<td>Confirm shared secret</td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>

4. Click **OK**. Cisco ASA 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 either Microsoft’s IAS or NPS, and provides 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 RADIUS authentication with SAM requires the following:

- Creating a RADIUS-enabled AAA Server Group, page 11
- Adding an IP Address Pool, page 14
- Adding a Group Policy, page 15
- Configuring a Connection Profile for Network (Client) Access, page 17
- Configuring a Connection Profile for Clientless SSL VPN Access, page 21

Creating a RADIUS-enabled AAA Server Group

To use an external AAA server for authentication, authorization, or accounting, you must first create at least one AAA server group per AAA protocol, and add one or more servers to each group. Each server group is specific to one type of server, such as Kerberos, LDAP, NT, RADIUS, SDI, or TACACS+.

For this integration, we will use an external AAA server for authentication and one server group, configured with an external RADIUS server with RADIUS protocol.

1. Launch the Cisco Adaptive Security Device Manager (ASDM).
2. Click the Configuration tab.
3. In the left pane, click Remote Access VPN.
4. Click AAA/Local Users > AAA Server Groups.

5. Adjacent to the AAA Server Groups window, click Add.

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
6. 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 name for the AAA Server Group (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.)

7. Under **AAA Server Groups**, select the newly created AAA server group.

8. Adjacent to the **Servers in the Selected Group** window, click **Add**.

(The screen image above is from Cisco®, Trademarks are the property of their respective owners.)
9. 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 the interface to use to reach the RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Name or IP Address</strong></td>
<td>Enter a server name or IP address to use to reach the RADIUS server.</td>
</tr>
<tr>
<td><strong>Server Authentication Port</strong></td>
<td>Enter the RADIUS server’s authentication port; for example, <strong>1812</strong>.</td>
</tr>
<tr>
<td><strong>Server Secret Key</strong></td>
<td>Enter the shared secret that will be used between Cisco ASA and the RADIUS server.</td>
</tr>
</tbody>
</table>

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

10. Click **Apply**.
Adding an IP Address Pool

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

1. Launch the Cisco Adaptive Security Device Manager (ASDM).
2. Click the Configuration tab.
3. Click Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools.
4. Click Add.
5. On the Add IPv4 Pool window, complete the following fields, and then click OK.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter the name of the address pool, up to 64 characters (for example, vnppool).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting IP Address</td>
<td>Enter the first IP address available in the pool (for example, 8.8.8.1).</td>
</tr>
<tr>
<td>Ending IP Address</td>
<td>Enter the last IP address available in the pool (for example, 8.8.8.25).</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the subnet on which this IP pool resides (for example, 255.255.255.0).</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. 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.

   ![Cisco ASDM Group Policies](image)

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

4. Click **Add**.

   ![Add Group Policy](image)

   *(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)*
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. Adjacent to **Tunneling Protocols**, deselect **Inherit**.
   
d. Select the following:
      - Clientless SSL VPN
      - SSL VPN Client
      - IPsec IKEv1
      - IPsec IKEv2 (optional)
      - L2TP/IPsec (optional)

   ![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.

A connection profile identifies a default group policy for the connection, which contains protocol-specific connection parameters, including 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.

Configuring a Connection Profile for AnyConnect

1. Launch the Cisco Adaptive Security Device Manager (ASDM).
2. Click the Configuration tab.

4. Under Access Interfaces, complete the following steps:
   a. Select Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below.
   b. For each interface (outside and inside), under SSL Access, select Allow Access and Enable DTLS.
   c. For each interface (outside and inside), under IPsec Access, select Allow Access and Enable DTLS.

SafeNet Authentication Manager: Integration Guide
Using RADIUS Protocol for Cisco ASA
Document PN: 007-012965-001, Rev. B, Copyright © 2015 SafeNet, Inc., All rights reserved.
5. Under **Connection Profiles**, click **Add**.

![Connection Profiles screenshot](image)

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

6. On the **Add AnyConnect Connection Profile** window, click **Basic**, and then 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>radiusgroup</em>).</td>
</tr>
<tr>
<td></td>
<td>This will be the authentication method that will be associated with this profile.</td>
</tr>
<tr>
<td><strong>Client Address Pools</strong></td>
<td>Click <strong>Select</strong> and assign an address pool; for example, <em>vpnpool</em>.</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>
<tr>
<td></td>
<td>• Select <strong>Enable IPsec client protocol</strong> (optional).</td>
</tr>
<tr>
<td></td>
<td>• Fill in the <strong>DNS Server</strong> detail.</td>
</tr>
</tbody>
</table>

![Add AnyConnect Connection Profile screenshot](image)

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

7. Click **OK**.
8. On the **AnyConnect Connection Profiles** window, verify these options are selected:
   - (Optional) Under **Access Interfaces**: Bypass interface access lists for inbound VPN sessions
   - Under **Login Page Setting**: Allow user to select connection profile on the login page

   ![Connection Profile Configuration](image)

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

9. Click **Apply**.

### Configuring a Connection Profile for IPsec (IKEv1)

1. Launch the Cisco Adaptive Security Device Manager (ASDM).
2. Click the **Configuration** tab.
3. Click **Remote Access VPN > Network (Client) Access > IPsec(IKEv1) Connection Profiles**.

   ![Remote Access VPN Configuration](image)

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

4. Under **Access Interfaces**, for each interface (outside and inside), select **Allow Access**.

   ![IPsec Access Interfaces](image)

   *(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)*
5. Under **Connection Profiles**, select the profile that you created (for example, `safenetprofile`), and then click **Edit**.

![Connection Profiles Table](image)

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

6. Click **Basic**, complete the following fields, and then click **OK**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-shared key</td>
<td>Enter the name of the pre-shared key.</td>
</tr>
<tr>
<td>Server Group</td>
<td>Select an appropriate server group (for example, <code>radiusgroup</code>).</td>
</tr>
<tr>
<td>Client Address Pools</td>
<td>Click <strong>Select</strong> and assign an address pool; for example, <code>vpnpool</code>.</td>
</tr>
<tr>
<td>Group Policy</td>
<td>Select an appropriate group policy (for example, <code>safenetpolicy</code>).</td>
</tr>
<tr>
<td>Enable IPsec protocol</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Enable L2TP over IPsec protocol</td>
<td>(Optional) Select this option.</td>
</tr>
</tbody>
</table>

![Basic Configuration](image)

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

7. Click **Apply**.

![Advanced Configuration](image)
Configuring a Connection Profile for Clientless SSL VPN Access

1. Launch the Cisco Adaptive Security Device Manager (ASDM).
2. Click the Configuration tab.

![Cisco Adaptive Security Device Manager](image1)

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

4. Under Customization Objects, select the DfltCustomization template, and then click Assign. This template will be used for the Login page and the main SSL portal page.

![Cisco Configuration](image2)

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

5. On the Assign GUI Customization window, select either a Group Policy (for example, safenetpolicy) or a Connection Profile (for example, safenetprofile), and then click OK.

![Assign GUI Customization](image3)

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

7. Click **Remote Access VPN > Clientless SSL VPN Access > Connection Profiles**.

8. Under **Connection Profiles**, select the profile that you created earlier (for example, **safenetprofile**), and then click **Edit**.

9. Click **Basic**, complete the following fields, and then click **OK**:

<table>
<thead>
<tr>
<th><strong>AAA Server Group</strong></th>
<th>Select an appropriate server group (for example, <strong>radiusgroup</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Group</strong></td>
<td>Select an appropriate DNS server group.</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 clientless SSL VPN protocol</strong></td>
<td>Select this option.</td>
</tr>
</tbody>
</table>
10. On the **Edit Clientless SSL VPN Connection Profile** window, in the left pane, click **Advanced > Clientless SSL VPN**.

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
11. Complete the following steps, and then click OK:
   a. In the Login and Logout Page Customization menu, verify that DfltCustomization is selected.
   b. Under Connection Aliases, verify the safenet alias is set to Enabled.

![Login and Logout Page Customization Menu]

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

12. Click Apply.

### Running the Solution

Before running the RADIUS server integration solution, a corresponding RADIUS client must be added in NPS. You can use the following methods to securely connect to Cisco ASA:

- Using Clientless SSL VPN Access, page 24
- Using the Cisco AnyConnect Secure Mobility Client, page 26
- Using the Cisco VPN Client (IPsec), page 26

In each method described below, the SafeNet eToken PASS is used as the enrolled OTP token.

#### Using Clientless SSL VPN Access

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, including:

- Internal web sites
- 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.
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>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Select an appropriate group alias; for example, safenet.</td>
</tr>
<tr>
<td>USERNAME</td>
<td>Enter your SAM user ID.</td>
</tr>
<tr>
<td>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.)

3. Click Login.

After successful authentication, you will be logged in. You can now access the service and configured application.

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

To securely connect to Cisco ASA, the Cisco AnyConnect Secure Mobility Client can be used. The Cisco AnyConnect Secure Mobility Client provides remote users with secure VPN connections to 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**.

![Cisco AnyConnect Secure Mobility Client](image)

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

3. Complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Select an appropriate group alias; for example, safenet.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter your SAM user ID.</td>
</tr>
<tr>
<td>Password</td>
<td>Generate an OTP using SafeNet eToken PASS and enter it in this field.</td>
</tr>
</tbody>
</table>

![Cisco AnyConnect](image)

(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 Cisco ASA](image)

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

The Cisco VPN Client provides remote users with a secure VPN connection to Cisco ASA using IPsec protocol. In this solution, the SafeNet eToken PASS is used as the enrolled OTP token.

1. From the Windows Start menu, select All Programs > Cisco System VPN Client > VPN Client.
2. Click New.

![Cisco VPN Client](image)

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

3. On the Create New VPN Connection Entry window, complete the following fields, and then click **Save**:

<table>
<thead>
<tr>
<th>Connection Entry</th>
<th>Enter a unique name for the connection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>(Optional) Enter a description for the connection.</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the hostname or IP address of the remote VPN server.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Select <strong>Group Authentication</strong>, and then complete the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Name</strong>—Enter the name of the connection profile or tunnel group to which you belong (for example, safenetprofile). This entry is case-sensitive.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Password</strong>—Enter the shared secret of your connection profile or tunnel group. This entry is case-sensitive.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Confirm Password</strong>—Re-enter the shared secret.</td>
</tr>
</tbody>
</table>

![Create New VPN Connection Entry](image)

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
4. Select the new connection entry (for example, Safenet), and then click Connect.

![Connection Entry](image)

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

5. Complete the following fields, and then click OK.

<table>
<thead>
<tr>
<th>Username</th>
<th>Enter your SAM user ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Generate an OTP using SafeNet eToken PASS and enter it in this field.</td>
</tr>
</tbody>
</table>

When the credentials are authenticated, secure VPN connection to Cisco ASA is made.

![Connected](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 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
</tbody>
</table>
|                         | 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.