SafeNet Authentication Service
Integration Guide
Using RADIUS and LDAP Protocols for Cisco Secure ACS
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-013144-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>June 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 SAS-SPE and SAS-PCE..................................5
RADIUS Authentication Flow using SAS ...............................................................6
RADIUS Prerequisites...........................................................................................7
Configuring SafeNet Authentication Service.......................................................7
  Synchronizing User Stores to SAS ..................................................................7
  Assigning Authenticator in SAS ........................................................................8
  Configuring Pre-authentication Rules ..............................................................8
  Adding Cisco Secure ACS as an Authentication Node in SAS ......................13
  Checking the SAS RADIUS Server’s IP Address .........................................15
Configuring Cisco ASA.........................................................................................16
  Creating a RADIUS-enabled AAA Server Group ...........................................16
  Adding an IP Address Pool .............................................................................21
  Configuring a Group Policy .........................................................................22
  Configuring a Connection Profile for Network (Client) Access ...................24
Configuring Cisco Secure ACS.............................................................................28
  Configuring Network Devices and AAA Clients .......................................28
  Configuring User and Identity Stores .........................................................29
  Configuring Access Policies .......................................................................31
Running the Solution............................................................................................34
  Using Clientless SSL VPN .............................................................................34
  Using the Cisco AnyConnect Secure Mobility Client ..................................36
Support Contacts..................................................................................................37
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 Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

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

Cisco Secure Access Control Server (ACS) is an access policy control platform that helps you to comply with growing regulatory and corporate requirements. By integrating with your other access control systems, it can 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 authentication, authorization, and accounting (AAA) network security 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 Service in RADIUS mode.
- Deploy two-step authentication using Cisco ASA and Cisco Secure ACS. For example, authenticating with two passwords—the first password can be authenticated by SAS through the LDAP server, and the second password can be authenticated by SAS through the FreeRADIUS server.

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 Service.

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 Service.
Applicability

The information in this document applies to:

- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by Service Providers to deploy instances of SafeNet Authentication Service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version 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 Service – Private Cloud Edition (SAS-PCE)**—Version 3.3.20091.25603
- **Cisco Secure ACS**—Version 5.4.0.46.0a
- **Cisco ASA**—Version 9.2(2)4
- **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 are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

RADIUS-based Authentication using SAS-SPE and SAS-PCE

For both on-premises versions, SAS can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS) or the legacy Microsoft Internet Authentication Service (MS-IAS)**—SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.

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

- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.
For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

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

**RADIUS Authentication Flow using SAS**

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

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

1. A user attempts to log on to Cisco ASA using Active Directory login credentials.
2. Cisco ASA sends the RADIUS request with the user’s Active Directory credentials to Cisco Secure ACS.
3. Cisco Secure ACS sends the RADIUS request with the user’s Active Directory credentials to SAS.
4. SAS sends the LDAP request with the user’s Active Directory credentials to the LDAP server, that is, Microsoft Active Directory.
5. If LDAP authentication succeeds, SAS will send a RADIUS challenge to Cisco Secure ACS. Otherwise, the user will not be granted access.
6. Cisco Secure ACS sends the RADIUS challenge received from SAS to Cisco ASA.
7. Cisco ASA will send the RADIUS challenge to the user, and the RADIUS Challenge will be displayed on user’s screen. The user will send the appropriate response with respect to that RADIUS Challenge.
8. The response will travel through the same channel as specified in steps 1, 2, and 3.
9. SAS will validate the response, and will send back a reply through the same channel in steps 5, 6, and 7.
10. The user is granted or denied access to Cisco ASA based on the RADIUS challenge-response value calculation results from SAS.
RADIUS Prerequisites

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

- End users can authenticate through the Cisco Secure ACS 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 signatures.
- Cisco AnyConnect Secure Mobility Client is installed on the client machine.
- SafeNet MobilePASS is enrolled as an OTP token in SAS.

Configuring SafeNet Authentication Service

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

- Synchronizing User Stores to SAS, page 7
- Assigning Authenticator in SAS, page 8
- Configuring Pre-authentication Rules, page 8
- Adding Cisco Secure ACS as an Authentication Node in SAS, page 13
- Checking the SAS RADIUS Server’s IP Address, page 15

Synchronizing User Stores to SAS

Before SAS can authenticate any user in your organization, you must create a user store in SAS that reflects the users who need to use multi-factor authentication. User records are created in the SAS user store automatically, by synchronizing with your Active Directory /LDAP server using LDAP integration.

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


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

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

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet GOLD
- SMS Token
- MP-1 Software Token
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning Rules” in the SafeNet Authentication Service Subscriber Account Operator Guide to learn how to provision the different authentication methods to the users in the SAS user store.


Configuring Pre-authentication Rules

Just because a user is able to provide a valid, one-time passcode, does not necessarily mean that the user should be granted access to the network. Other conditions such as network access point, group membership, account status, and other attributes might be important in allowing or denying access.

The key advantages of pre-authentication rules are:

- Rules can be applied to LDAP/Active Directory user account attributes.
- Rules can be applied to user accounts maintained in the internal SQL user data source.
- Rules can be applied based on network access points (source IP, Agent).
- Rules can be used to modify the authentication sequence (OTP, LDAP, LDAP + OTP).
- Changes made to user attributes in LDAP or the internal user data source are immediately effective on SafeNet Authentication Service.

In this integration, we will create a rule to modify the LDAP+OTP authentication sequence.
1. Log in to the SAS console with an Operator account.

2. Click the COMMS tab, and then click Authentication Processing.
3. **Under Authentication Processing**, click **Pre-authentication Rules**.

![Pre-authentication Rules](image)

4. **Click New Rule**.

![New Rule](image)
5. Enter the following details, and then click Add below Add New Pre-Auth Rule:

<table>
<thead>
<tr>
<th>Rule Name:</th>
<th>Enter a name for your rule (for example, ldaprule).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter the description of the rule (for example, LDAP rule).</td>
</tr>
</tbody>
</table>
| Filter     | 1. Select LDAP password pass through, and then select Always.  
            2. In the If LDAP authentication fails menu, select reject the authentication.  
            3. In the If LDAP authentication succeeds menu, select force challenge response.  
            4. Click Add on the right side of the screen (see red box in screen below). The following condition is displayed:  
              Always forward request to LDAP. If LDAP authentication fails reject the authentication. If LDAP authentication succeeds force challenge response. |

![Authentication Processing](image-url)
6. Under **Pre-Authentication Rules**, select **Enable Pre-Auth Rules**.

7. Click **Apply** to enable this rule.
Adding Cisco Secure ACS as an Authentication Node in SAS

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

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

2. Click the COMMS tab, and then click Auth Nodes.

3. In the Auth Nodes module, click the Auth Nodes link.
4. Under **Auth Nodes**, click **Add**.

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

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

![Add Auth Node dialog box](image)

The authentication node is added to the system.

![Auth Nodes listing](image)
Checking the SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in Cisco Secure ACS, check the IP address of the SAS RADIUS server. The IP address will be added to Cisco Secure ACS as a RADIUS server later in this document.

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

2. Click the COMMS tab, and then click Auth Nodes.

3. In the Auth Nodes module, click the Auth Nodes link. The SAS RADIUS server details are displayed.
Configuring Cisco ASA

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

- Creating a RADIUS-enabled AAA Server Group, page 16
- Adding an IP Address Pool, page 21
- Configuring a Group Policy, page 22
- Configuring a Connection Profile for Network (Client) Access, page 24

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. Identify AAA server groups by name. Each server group is associated with only one type of server, such as Kerberos, LDAP, NT, RADIUS, SDI, or TACACS+.

1. Open the Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
2. On the Cisco ASDM-IDM Launcher window, complete the following fields, and then click OK.

<table>
<thead>
<tr>
<th>Device IP Address / Name</th>
<th>Enter the IP address of Cisco ASA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter your username on Cisco ASA.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter your password on Cisco ASA.</td>
</tr>
</tbody>
</table>

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

3. On the main window, click the Configuration tab.
4. In the left pane, click the **Remote Access VPN** tab, and then click **AAA/Local Users > AAA Server Groups**.

![Remote Access VPN](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**.

![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 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.)

6. Under **AAA Server Groups**, select the newly created AAA server group (for example, **radiusgroup**).
7. 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.)*
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 the interface to use to reach Cisco Secure ACS.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Name or IP Address</strong></td>
<td>Enter the server name or IP address of Cisco Secure ACS.</td>
</tr>
<tr>
<td><strong>Server Authentication Port</strong></td>
<td>Enter the RADIUS server authentication port (for example, <strong>1812</strong>).</td>
</tr>
<tr>
<td><strong>Server Secret Key</strong></td>
<td>Enter the shared secret key. It should be same as entered in Cisco Secure ACS. Refer to section “Configuring Network Devices and AAA Clients” on page 28.</td>
</tr>
</tbody>
</table>

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

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

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

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

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 > Address Assignment > Address Pools**.

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

5. On the **Add IPv4 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, up to 64 characters (for example, <code>vpnpool</code>).</td>
</tr>
<tr>
<td><strong>Starting IP Address</strong></td>
<td>Enter the first IP address available in the pool. The format of the IP address should be <code>0.0.0.0</code>.</td>
</tr>
<tr>
<td><strong>Ending IP Address</strong></td>
<td>Enter the last IP address available in the pool. The format of the IP address should be <code>0.0.0.0</code>.</td>
</tr>
<tr>
<td><strong>Subnet Mask</strong></td>
<td>Enter the subnet on which this IP pool resides.</td>
</tr>
</tbody>
</table>
6. Click **Apply**.

**Configuring 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.

Configure a group policy, which is present by default, in Cisco ASA.

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**.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
4. In the right pane, for the **DfltGrpPolicy (System Default)** group policy, ensure that in the **Tunneling Protocol** column, **ssl-client** and **ssl-clientless** are added.

![Configuration > Remote Access VPN > Network (Client) Access > Group Policies](image)

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

5. If **ssl-client** and **ssl-clientless** are not added in the **Tunneling Protocol** column, select the **DfltGrpPolicy (System Default)** group policy, click **Edit**, and perform the following steps:

   a. On the **Edit Internal Group Policy** window, click **More Options**.

   ![Edit Internal Group Policy window](image)

   *(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)*
b. Adjacent to **Tunneling Protocols**, select the **Clientless SSL VPN** and **SSL VPN Client** options.

![Image of Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA]

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

c. Click **OK**.

d. 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 also 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.

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 > AnyConnect Connection Profiles**.

![Image of Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA]

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
4. In the right pane, under **Access Interfaces**, 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 each interface (outside and inside), under **SSL Access**, select **Allow Access** and **Enable DTLS**.

   ![Access Interfaces](image)

   *(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](image)

   *(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**, and then complete the following fields:

<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Enter the name of the connection profile (for example, <strong>safenetprofile</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Aliases</strong></td>
<td>Enter the alias for the connection profile (for example, <strong>safenet</strong>).</td>
</tr>
<tr>
<td><strong>AAA Server Group</strong></td>
<td>Select the AAA server group created in the section “Creating a RADIUS-enabled AAA Server Group” on page 16 (for example, <strong>radiusgroup</strong>).</td>
</tr>
<tr>
<td><strong>Client Address Pools</strong></td>
<td>Click <strong>Select</strong> and assign an address pool.</td>
</tr>
<tr>
<td><strong>Group Policy</strong></td>
<td>• Select an appropriate group policy (for example, <strong>DfltGrpPolicy</strong>).</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Enable SSL VPN client protocol</strong>.</td>
</tr>
</tbody>
</table>
7. Click **OK**.
8. On the main window, in the right pane, under **Login Page Setting**, select **Allow user to select connection profile on the login page**.

![Configuration window](image)

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

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

Configuring Cisco Secure ACS for RADIUS authentication requires the following:

- Configuring Network Devices and AAA Clients, page 28
- Configuring User and Identity Stores, page 29
- Configuring Access Policies, page 31

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.

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the network device (Cisco ASA).</td>
</tr>
<tr>
<td>IP</td>
<td>Enter the IP address of the RADIUS client.</td>
</tr>
<tr>
<td>Authentication Options</td>
<td>Select RADIUS.</td>
</tr>
<tr>
<td>Shared Secret</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.

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. On the General tab, complete the following fields, and then click Submit:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name of your identity store (for example, radiusserver).</td>
</tr>
<tr>
<td>Hostname AAA</td>
<td>Enter the IP address of the RADIUS Server.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the secret text shared between Cisco Secure ACS and the RADIUS server.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Enter 1812.</td>
</tr>
</tbody>
</table>

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

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 **match Radius** protocol is pointing to the **Default Network Access** service.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
4. In the left pane, click **Access Policies** > **Access Services** > **Default Device Admin** > **Identity**.

![Access Policies Diagram]

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

5. In the right pane, in the **Identity Source** field, click **Select**.

![Identity Source Selection]

*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*
6. On the **Identity Store** window, select your identity source (for example, **radiusserver**), and then click **OK**.

7. Click **Save Changes**.

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

You can use the following methods to securely connect to Cisco ASA:
- Using Clientless SSL VPN, page 34
- Using the Cisco AnyConnect Secure Mobility Client, page 36

Using 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, including:
- Internal websites
- Web-enabled applications
- NT/Active Directory file shares
- Email proxies, including POP3S, IMP4S, 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 MobilePASS is used as the enrolled OTP token.

1. Open the following URL in a web browser: https://<Public IP Address of Cisco ASA>. The Login window is displayed.

2. Enter your domain username and LDAP password, and then click Login.
   If the login credentials provided are authenticated successfully, the window shown in the next step will appear.
3. Generate a challenge-response from the MobilePASS token, and enter it in the Response field, and then click Continue.
If authentication is successful, the VPN session will be established and 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 MobilePASS is used as the enrolled OTP token.

1. From the Windows Start menu, select 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 the LDAP password.</td>
</tr>
</tbody>
</table>

If LDAP authentication is successful, then the window shown in the next step will appear. Otherwise, authentication will get rejected.
4. Generate a challenge response from the MobilePASS token, and enter it in the **Answer** field, and then click **Continue**.

![Challenge Response Screen](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 Screen](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>
</table>
| **Address**           | SafeNet, Inc.  
4690 Millennium Drive  
Belcamp, Maryland 21017 USA                                                    |
| **Phone**             | United States  
1-800-545-6608                                                                 |
|                       | International  
1-410-931-7520                                                                 |
| **Technical Support Customer Portal** | [https://serviceportal.safenet-inc.com](https://serviceportal.safenet-inc.com)  
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. |