SafeNet Authentication Service
Integration Guide

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

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

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

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

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

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

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

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

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

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

**Document Part Number:** 007-012884-001, Rev. D  
**Release Date:** November 2015
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 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 Service in RADIUS mode.

It is assumed that the Cisco Secure ACS environment is 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 (SAS)**—SafeNet's cloud-based authentication service
- **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 (SAS)**—SafeNet's cloud-based authentication service
- **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
- **SafeNet VPN Client for Cisco AnyConnect**—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 Cloud

SAS Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.
- **Local RADIUS hosted on-premises**—A RADIUS agent that is implemented in the existing customer’s RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.

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

For more information on how to install and configure SAS Agent for IAS/NPS, refer to: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

For more details on how to install and configure FreeRADIUS, refer to the SafeNet Authentication Service FreeRADIUS Agent Configuration Guide.

---

### 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.
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 data flow of a multi-factor authentication transaction for Cisco Secure ACS.

1. A user attempts to log on to Cisco Secure ACS using an OTP authenticator.
2. Cisco Secure ACS sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
3. The SAS authentication reply is sent back to the Cisco Secure ACS.
4. The user is granted or denied access to the Cisco Secure ACS based on the OTP 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 from the Cisco Secure ACS environment with a static password before configuring the 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 RADIUS client for encryption, decryption, and digital signatures.
- Cisco AnyConnect Secure Mobility Client is installed on the client machine.
- SafeNet VPN client for Cisco AnyConnect is installed on the client machine.
- SafeNet eToken PASS and MP-1 tokens are already 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 the following:

- Creating Users Stores in SAS, page 9
- Assigning an Authenticator in SAS, page 10
- Adding Cisco Secure ACS as an Authentication Node in SAS, page 10
- Checking the SAS RADIUS Address, page 13

Creating Users Stores in SAS

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

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

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

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

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Cisco 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
- GrIDsure Authentication

Authenticators can be assigned to users in two ways:

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

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

Adding Cisco 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 both SAS and Cisco Secure ACS.

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

2. Click the COMMS tab, and then select Auth Nodes.
3. In the **Auth Nodes** module, click the **Auth Nodes** link.

![Auth Nodes](image)

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

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

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

![Add Auth Nodes](image)

The authentication node is added to the system.

![Auth Nodes](image)
Checking the SAS RADIUS Address

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

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

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

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

For this integration, Cisco ASA is used for the SSL VPN connection.

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

- Creating AAA Server Groups, page 14
- ADDING AN IP ADDRESS POOL, page 22
- Adding a Group Policy, page 23
- Configuring a Connection Profile for Network (Client) Access, page 25
- Configuring a Connection Profile for Clientless SSL VPN Access, page 29
- Configuring a Connection Profile for Clientless SSL VPN Access for GrIDsure, page 34

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. adgroup must be configured with the external LDAP server using LDAP protocol, and tacacsgroup should be configured with the external TACACS server using 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. In the left pane, click the Remote Access VPN tab, and then click AAA/Local Users > AAA Server Groups.

3. In the right pane, under the AAA Server Groups section, click Add.
4. On the Add AAA Server Group window, complete the following fields, and then click OK. This newly created AAA server group will be added to the list under the AAA Server Group section.

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

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

5. On the main window, in the right pane, under the AAA Server Groups section, select the newly created server group; for example adgroup.

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

![Servers in the Selected Group](image)

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

7. On the **Add AAA Server** window, complete the following fields, and then click **OK**. This newly created AAA server will be added to the list under the **Servers in the Selected Group** section.

<table>
<thead>
<tr>
<th><strong>Interface Name</strong></th>
<th>Select an appropriate interface that Cisco ASA uses in order to reach the LDAP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Name or IP Address</strong></td>
<td>Enter the IP address of the LDAP server that Cisco ASA uses in order to reach the LDAP server.</td>
</tr>
<tr>
<td><strong>Base DN</strong></td>
<td>Enter the location in the LDAP hierarchy where the server must begin to search.</td>
</tr>
<tr>
<td><strong>Naming Attribute(s)</strong></td>
<td>Enter the Relative Distinguished Name attribute(s) that uniquely identifies an entry on the LDAP server. <strong>sAMAccountName</strong> is the default attribute in the Microsoft Active Directory.</td>
</tr>
<tr>
<td><strong>Login DN</strong></td>
<td>Enter the Distinguished Name with enough privileges in order to be able to search users in the LDAP server.</td>
</tr>
<tr>
<td><strong>Login Password</strong></td>
<td>Enter the password for the Distinguished Name account.</td>
</tr>
</tbody>
</table>
8. 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**. In the left pane, click the **Remote Access VPN** tab, and then click **AAA/Local Users > AAA Server Groups**.

![Cisco ASDM Configuration](image)

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

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

![AAA Server Groups](image)

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
4. On the **Add AAA Server Group** window, complete the following fields, and then click **OK**. This newly created AAA server group will be added to the list under the **AAA Server Group** section.

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

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

5. On the main window, in the right pane, under the **AAA Server Groups** section, select the newly created server group; for example, **tacacsgroup**.

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

![Server Selection Screen](image)

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

7. 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><strong>Interface Name</strong></th>
<th>Select an appropriate interface that Cisco ASA uses in order to reach Cisco ACS and then the RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Name or IP Address</strong></td>
<td>Enter the IP address that Cisco ASA uses in order to reach Cisco ACS.</td>
</tr>
<tr>
<td><strong>Server Secret Key</strong></td>
<td>Enter the secret key shared between Cisco ASA and Cisco ACS.</td>
</tr>
</tbody>
</table>

![Add AAA Server Window](image)

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

8. 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. In the left pane, click the Remote Access VPN tab, and then click Network (Client) Access > Address Assignment > Address Pools.

   ![Add Address Pool](image1)

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

3. In the right pane, click Add.

   ![Add IPv4 Pool](image2)

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

4. 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>Name</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>Starting IP Address</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>Ending IP Address</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>Subnet Mask</td>
<td>Enter the subnet on which this IP pool resides.</td>
</tr>
</tbody>
</table>
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**. 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.)
3. In the right pane, click **Add**.

![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.)

4. 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**

![Add Internal Group Policy](image)

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

5. Click **Apply**.
Configuring a Connection Profile for Network (Client) Access

A connection profile consists of a set of records that determines tunnel connection policies. These records identify the servers to which the tunnel user is authenticated, as well as the accounting servers, if any, to which connection information is sent. They also identify a default group policy for the connection, and they contain protocol-specific connection parameters. 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. In the left pane, click the Remote Access VPN tab, and then click Network (Client) Access > AnyConnect Connection Profiles.
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:
   
c. In the left pane, click **Advanced > Secondary Authentication**.

d. In the right pane, in the **Server Group** field, select an appropriate server group; for example, **tacacsgroup**.

e. 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.

![Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles](image)

(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. In the left pane, click the Remote Access VPN tab, and then click Clientless SSL VPN Access > Portal > Customization.

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

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 the main SSL portal.

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

(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**.

![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, perform the following steps:
   a. In the left pane, click **Basic**.
   b. In the right pane, complete the following fields:

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

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

d. 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.)*
e. In the left pane, click **Advanced > Clientless SSL VPN**.

f. In the right pane, in the **Login and Logout Page Customization** field, select **DfltCustomization**. Then, under **Connection Aliases**, select an appropriate alias (for example, **safenet**), and then select the option in the **Enabled** column.

8. Click **OK**.

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

For GrIDsure authentication in Clientless SSL VPN, create one more template with different login page settings; that is, the Login Page will show the GET grid button.

Create a copy (DfltCustomizationgridsure) of the default customization template (DfltCustomization).

To configure a clientless SSL VPN for GrIDsure:

1. Open the Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.

2. On the main window, click Configuration. In the left pane, click the Remote Access VPN tab, and then click Clientless SSL VPN Access > Portal > Customization.

3. In the right pane, in the Customization objects list, select Dfltcustomizationgridsure, and then click Edit.
4. On the **Edit Customization Object** window, perform the following steps:
   a. In the left pane, click **Logon Page > Logon Form**.
   b. In the right pane, under **Username and Password**, clear **Show internal password**.
   c. In the left pane, click **Logon Page > Informational Panel**.
   d. In the right pane, select **Display informational panel**.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
e. Copy the following GrIDsure code, paste it in the Text field, and then click OK.

**NOTE:** In the GrIDsure code, you will need to specify the gridMaker URL. For details on how to obtain the gridMaker URL, refer to the section Obtaining a Grid URL in Appendix.

```html
//URL of the BlackShield ID Self Service page

function showGrid()
{
    var obj=document.getElementById('login_message_text');
    if(obj)
    {
        obj.innerHTML="Please enter your OTP";
        var uname=document.getElementById('username');
        if(uname)
        {
            if (uname.value == "")
            {
                alert("User name required");
            }
            else
            {
                obj.innerHTML += '<br><br><img border="1" src="' + gridMakerURL + uname.value + '">
                
                uname.readOnly=true;
                uname.style.backgroundColor='gray'
            }
        }
    }
    var obj=document.getElementsByName("Login");
    if(obj)
    {
        obj[0].parentNode.innerHTML += '<INPUT type="button" name="getOTP" value="Get Grid" onclick="showGrid()">';
    }
```
obj=document.getElementById("password_field");
if(obj)
{
    obj.innerHTML="Password";
}
</script>

5. On the main window, in the right pane, in the **Customization objects** list, select **Dfltcustomegridsure**, and then click **Assign**.

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

7. On the main window, click **Apply**.

8. To verify if the **Dfltcustomegridsure** template is assigned to the clientless SSL VPN, perform the following steps:
   a. On the main window, in the left pane, click **Clientless SSL VPN Access > Connection Profiles**.
      
      *(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*

SafeNet Authentication Service: Integration Guide
Using RADIUS Protocol for Cisco Secure ACS
Document PN: 007-012884-001, Rev. D, Copyright © 2015 Gemalto, Inc., All rights reserved.
b. In the right pane, select your connection profile (for example, `safenetprofile`), and then click **Edit**.

c. On the **Edit Clientless SSL VPN Connection Profile: safenetprofile** 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.)

d. In the right pane, in the **Login and Logout Page Customization** field, select `Dfltcustomizationgridsure`.

e. Click **OK**.
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+).

Configuring Cisco Secure ACS for RADIUS authentication requires the following:

- Configuring Network Devices and AAA Clients, page 39
- Configuring User and Identity Stores, page 40
- Configuring Access Policies, page 42

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.
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 an 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. 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 identity store.</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>
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**.

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

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

- Using Clientless SSL VPN, page 45
- Using Clientless SSL VPN with GrIDsure Authentication, page 46
- Using the Cisco AnyConnect Secure Mobility Client, page 48
- Using the SAS Agent for Cisco AnyConnect, page 50

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. 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 a 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>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 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 SAS 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 Clientless SSL VPN with GrIDsure Authentication**

The SafeNet GrIDsure flexible authentication method allows an end user to generate a one-time password without the requirement for hardware tokens or software applications.

In this solution, the SafeNet GrIDsure is used as the enrolled OTP token. Note that an appropriate customization page should be selected in configuration while using GrIDsure authentication.

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><strong>GROUP</strong></td>
<td>Select an appropriate group alias; for example, <em>safenet</em>.</td>
</tr>
<tr>
<td><strong>USERNAME</strong></td>
<td>Enter your domain user name.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter password associated with your domain user name.</td>
</tr>
<tr>
<td><strong>2nd Username</strong></td>
<td>Enter your SAS user ID.</td>
</tr>
</tbody>
</table>
3. Click **Get Grid**.

4. Using the grid, enter the PIP in the 2nd **Password** field.

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

When the authentication is successful, you are logged in.

![SSL VPN Service](image1)

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

**Using the Cisco AnyConnect Secure Mobility Client**

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

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

1. Start the **Cisco AnyConnect Secure Mobility Client** application from **Start > All Programs > Cisco > Cisco AnyConnect Secure Mobility Client**.
2. 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](image2)

(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 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 SAS 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>
If authentication is successful, the VPN session will be established and you will see the following message on your system.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
Using the SAS Agent for Cisco AnyConnect

Organizations may wish to integrate software-based two-factor authentication tokens with the Cisco AnyConnect Client to simplify the login process for users, thus eliminating the need to copy and paste a one-time password from one application to another.

With the SAS Agent for Cisco AnyConnect, the ability to integrate software-based two-factor authentication tokens with Cisco AnyConnect becomes a reality.

In this solution, the SafeNet MP-1 token is used as the enrolled OTP token.


2. On the Connection tab, in the Connect to field, enter the fully qualified domain name or IP address for Cisco ASA, and then click Select.

3. Complete the following fields, and then click Connect:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group</strong></td>
<td>Select an appropriate group alias; for example, safenet.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Enter your domain user name.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password associated with your domain user name.</td>
</tr>
<tr>
<td><strong>Token</strong></td>
<td>Select an appropriate MP-1 token.</td>
</tr>
<tr>
<td><strong>Pin</strong></td>
<td>Enter PIN for the selected MP-1 token.</td>
</tr>
</tbody>
</table>
NOTE: On the Connection tab, “Token and Pin” combination is displayed as the second authentication method, for which configuration is done in Windows Registry after installing SafeNet Cisco AnyConnect Agent. For details, refer to the section “Configuring SafeNet Cisco AnyConnect Agent Registry Key” on page 54.
If authentication is successful, the VPN session will be established.
Appendix

Obtaining a Grid URL

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

2. Click the SELF-SERVICE tab, and then click Self-service Policy.

3. Copy the Self Service Unique URL. For example:

4. Replace the ss.safenet-inc.com to grid.safenet-inc.com:

5. Append the following text in the Self Service Unique URL:
   ?getChallengeImage=true&userName=

Now you will have the grid maker URL as follows:
Verifying the Grid URL

To test the URL from the above section, add a test username after userName in the URL and then paste it in the browser to see if you are getting a grid.

For example, enroll a GRIDsure token to user alice and then browse to this address:


If it shows a grid, the URL is valid; otherwise, verify if the link or self-service unique URL is correct.

Configuring SafeNet Cisco AnyConnect Agent Registry Key

In the Windows Registry, you specify where the MP-1 token list will appear and what password field(s) will be used when the one-time password is submitted to the server.

On the Windows XP/Vista/7 (32 bit) machine, the SoftTokenInclusion key in Windows Registry is located at:

\HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\CiscoAnyClientPlugin

On the Windows XP/Vista/7 (64 bit) machine, the SoftTokenInclusion key in Windows Registry is located at:

\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CRYPTOCard\CiscoAnyClientPlugin
The default value of the **SoftTokenInclusion** key is: **ALL+ALL+1**;

The definition of **ALL+ALL+1** is as follows:

“**Connect To** “+”**Group Profile** “+”**Field Position** to display MP-1 and submit one-time password”

For example, assume that the value of the **SoftTokenInclusion** key is: **ciscoasa.safenet.com+safenet+1**;

Explanation of the example above:

- This will work when connecting to **ciscoasa.safenet.com**
- MP-1 token detection will only show up using the “**safenet**” group profile
- It will display the MP-1 token detection in the first field

Below are the examples of changing the MP-1 token detection to a different field.

**ALL+ALL+1**

Display MPs in the first username field and submit one-time password to the first password field. This is the default setting after installing the SafeNet Cisco AnyConnect, and the SAS Software Tools. This option is used if the authentication is going against SAS.
**ALL+ALL+2**

Display MPs in the second username field and submit one-time password (OTP) to the second password field. This option is used if dual authentication is required.

**Example:** Microsoft Password [top], then SAS [Bottom]

```plaintext
NOTE: In this integration (Using RADIUS Protocol for Cisco Secure ACS), ALL+ALL+2 is used.
```
**ALL+ALL+3**

Display MPs in the first and second username fields and submit one-time password to the first and second password fields. This setting is used if there needs to be authentication against two SAS. This would be an odd case as this setting would rarely be used.

Multiple options can be appended to the **SoftTokenInclusion** key.

Here is an example:

Value of the **SoftTokenInclusion** Registry key: “ALL+Corporate+1;ALL+safenet+2;ALL+CRYPTOCARD+3;”

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Gemalto, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland  21017 USA</td>
</tr>
<tr>
<td><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><strong>Customer Portal</strong></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>