SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Cisco Identity Services Engine
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.
# Contents

Third-Party Software Acknowledgement .................................................................................. 4
Description .......................................................................................................................... 4
Applicability ....................................................................................................................... 5
Environment ....................................................................................................................... 5
Audience ............................................................................................................................ 5
RADIUS-based Authentication using SAS Cloud ................................................................. 6
RADIUS-based Authentication using SAS-SPE and SAS-PCE ........................................... 7
RADIUS Authentication Flow using SAS ............................................................................. 7
RADIUS Prerequisites ....................................................................................................... 8
Configuring SafeNet Authentication Service ...................................................................... 8
  Creating Users Stores in SAS .......................................................................................... 8
  Assigning an Authenticator in SAS .................................................................................. 9
  Adding Cisco Identity Services Engine as an Authentication Node in SAS .................... 10
  Checking the SAS RADIUS Server’s IP Address ............................................................. 12
Configuring Cisco ASA ..................................................................................................... 13
  Creating AAA Server Groups ......................................................................................... 13
  Adding an IP Address Pool .............................................................................................. 19
  Adding a Group Policy .................................................................................................... 21
  Configuring a Connection Profile for Network (Client) Access ....................................... 23
  Configuring a Connection Profile for Clientless SSL VPN Access ................................... 27
  Configuring a Connection Profile for Clientless SSL VPN Access for GrIDsure ................ 32
Configuring Cisco Identity Services Engine ...................................................................... 37
  Configuring Network Devices ......................................................................................... 37
  Configuring External Identity Sources ............................................................................ 41
  Configuring Policy .......................................................................................................... 45
Running the Solution .......................................................................................................... 47
  Using Clientless SSL VPN .............................................................................................. 47
  Using Clientless SSL VPN with GrIDsure Authentication ............................................... 49
  Using the Cisco AnyConnect Secure Mobility Client ...................................................... 51
Using the SAS Agent for Cisco AnyConnect ..................................................................... 52
Appendix ........................................................................................................................... 54
  Obtaining a Grid URL ..................................................................................................... 54
  Verifying the Grid URL ................................................................................................... 55
  Configuring SafeNet Cisco AnyConnect Agent Registry Key .......................................... 55
Support Contacts .............................................................................................................. 59
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Cisco Identity Services Engine.

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 ISE

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

Cisco ASA

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

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Cisco Identity Services Engine using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure Cisco Identity Services Engine to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Cisco Identity Services Engine and Cisco ASA environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Cisco Identity Services Engine 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)**
- **Cisco Identity Services Engine**—Version 1.4.0.253
- **Cisco ASA**—Version 9.2(2)4
- **Cisco Adaptive Security Device Manager (ASDM)**—Version 7.3(1)101
- **Cisco Secure Mobility Client**—Version 3.1.04072
- **SafeNet VPN Client for Cisco AnyConnect**—Version 3.1.04072

Audience

This document is targeted to system administrators who are familiar with Cisco Identity Services Engine, 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.

  ![SAS cloud RADIUS service diagram](image1)

- **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.

  ![Local RADIUS on-premises diagram](image2)

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:

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 Identity Services Engine.

1. A user attempts to log on to Cisco ASA using an Active Directory password and OTP.
2. Cisco ASA sends the LDAP request with the user’s Active Directory credentials to the LDAP server, that is, Microsoft Active Directory.
3. If successfully authenticated, Cisco ASA will send a RADIUS request to Cisco Identity Services Engine. Otherwise, the user will not be granted access.
4. Cisco Identity Services Engine sends a RADIUS request to SafeNet Authentication Service for validation.
5. The SAS authentication reply is sent back to Cisco Identity Services Engine.
6. Cisco Identity Services Engine, in turn, sends the reply back to Cisco ASA.
7. The user is granted or denied access to Cisco ASA based on the OTP value calculation results from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Cisco Identity Services Engine, ensure the following:

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

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Cisco Identity Services Engine using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 9
- Assigning an Authenticator in SAS, Assigning an Authenticator in SAS, page 9
- Adding Cisco Identity Services Engine as an Authentication Node in SAS, page 10
- Checking the SAS RADIUS Server’s IP Address, page 12

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 who 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 further 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 Identity Services Engine.

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 Identity Services Engine 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 Identity Services Engine. You will need the IP address of Cisco Identity Services Engine and the shared secret to be used by both SAS and Cisco Identity Services Engine.

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.
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>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>

The authentication node is added to the system.
Checking the SAS RADIUS Server’s IP Address

Before adding SAS as a RADIUS server in Cisco Identity Services Engine, check the IP address. The IP address will then be added to Cisco Identity Services Engine 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 13
- Adding an IP Address Pool, page 19
- Adding a Group Policy, page 21
- Configuring a Connection Profile for Network (Client) Access, page 23
- Configuring a Connection Profile for Clientless SSL VPN Access, page 27
- Configuring a Connection Profile for Clientless SSL VPN Access for GrIDsure, page 32

Creating AAA Server Groups

To use an external AAA server, you must first create at least one AAA server group per AAA protocol, and add one or more servers to each group. AAA server groups are identified by name. Each server group is associated with only one type of server, such as Kerberos, LDAP, NT, RADIUS, SDI, or TACACS+.

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

You will need to create two server group—for example, adgroup and radiusgroup—and adgroup must be configured with the external LDAP server using LDAP protocol, and radiusgroup must be configured with the external RADIUS server using RADIUS protocol.

Creating the LDAP-enabled AAA Server Group and its Servers

1. Open the Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
2. On the main window, click Configuration.
3. In the left pane, click the Remote Access VPN tab, and then click AAA/Local Users > AAA Server Groups.
4. In the right pane, under the **AAA Server Groups** section, click **Add**.

![Configuration > Remote Access > AAA/Local Users > AAA Server Groups](image)

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

5. On the **Add AAA Server Group** window, complete the following fields, and then click **OK**. 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>

![Add AAA Server Group](image)

*(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*
6. On the main window, in the right pane, under the **AAA Server Groups** section, select the newly created server group (for example **adgroup**).

![Screen Image](https://example.com/image1.png)

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

7. Under the **Servers in the Selected Group** section, click **Add**.

![Screen Image](https://example.com/image2.png)

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

8. On the **Add AAA Server** window, complete the following fields, and then click **OK**. This newly created AAA server 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.</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>
9. Click **Apply**.

**Creating the RADIUS-enabled AAA Server Group and its Servers**

1. Open the Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
2. On the main window, click **Configuration**.
3. In the left pane, click the **Remote Access VPN** tab, and then click **AAA/Local Users > AAA Server Groups**.
4. In the right pane, under the **AAA Server Groups** section, click **Add**.

   ![Add AAA Server Group](image)

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

5. On the **Add AAA Server Group** window, complete the following fields, and then click **OK**. This newly created AAA server group 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, <code>radiusgroup</code>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select <strong>RADIUS</strong>.</td>
</tr>
</tbody>
</table>

   ![Add AAA Server Group Window](image)

   *(The screen image above is from Cisco. Trademarks are the property of their respective owners.)*
6. On the main window, in the right pane, under the **AAA Server Groups** section, select the newly created server group (for example, **radiusgroup**).

![AAA Server Groups](image1)

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

7. Under the **Servers in the Selected Group** section, click **Add**.

![Servers in the Selected Group](image2)

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

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

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Select an appropriate interface that Cisco ASA uses in order to reach Cisco ISE.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name or IP Address</td>
<td>Enter the Cisco ISE IP address.</td>
</tr>
<tr>
<td>Server Authentication Port</td>
<td>Enter <strong>1812</strong>.</td>
</tr>
<tr>
<td>Server Secret Key</td>
<td>Enter the secret key shared between Cisco ASA and Cisco ISE.</td>
</tr>
</tbody>
</table>
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.
3. In the left pane, click the Remote Access VPN tab, and then click Network (Client) Access > Address Assignment > Address Pools.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
4. In the right pane, click **Add**.

![Add IPv4 Pool window](image)

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

5. On the **Add IPv4 Pool** window, complete the following fields, and then click **OK**.

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

![Add IPv4 Pool window](image)

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

6. Click **Apply**.
Adding a Group Policy

A group policy is a set of user-oriented attribute/value pairs for connections that are stored either internally (locally) on the device or externally on a RADIUS server. The connection profile uses a group policy that sets terms for user connections after the tunnel is established. Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user.

1. Open the Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
2. On the main window, click Configuration.
3. In the left pane, click 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, click Add.

(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**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the group policy (for example, safenetpolicy).</th>
</tr>
</thead>
<tbody>
<tr>
<td>More Options</td>
<td>Click to expand the window.</td>
</tr>
<tr>
<td>Tunneling Protocols</td>
<td>- Clear the Inherit check box.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>Clientless SSL VPN</strong>.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>SSL VPN Client</strong>.</td>
</tr>
</tbody>
</table>

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

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

A connection profile consists of a set of records that determines tunnel connection policies. These records identify the servers to which the tunnel user is authenticated, as well as the accounting servers, if any, to which connection information is sent. They also identify a default group policy for the connection, and they contain protocol-specific connection parameters.

1. Open the Cisco Adaptive Security Device Manager (ASDM) for Cisco ASA.
2. On the main window, click Configuration.
3. In the left pane, click the Remote Access VPN tab, and then click Network (Client) Access > AnyConnect Connection Profiles.
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 outside and inside interfaces, under the SSL Access column, select Allow Access and Enable DTLS.
5. In the right pane, under Connection Profiles, click Add.
6. On the **Add AnyConnect Connection Profile** window, in the left pane, click **Basic**. In the right pane, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter the name 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>adgroup</em>). This will</td>
</tr>
<tr>
<td></td>
<td>be the first authentication method associated with the connection profile.</td>
</tr>
<tr>
<td><strong>Client Address Pools</strong></td>
<td>Click <strong>Select</strong>, and then assign an address pool.</td>
</tr>
<tr>
<td><strong>Group Policy</strong></td>
<td>- Select an appropriate group policy (for example, <em>safenetpolicy</em>).</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.)
7. On the **Add AnyConnect Connection Profile** window, in the left pane, click **Advanced > Secondary Authentication**.

![](screenshot.png)

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

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

9. Click **OK**.
10. On the main window, in the right pane, perform the following steps, and then click **Apply**.
   a. Under **Access Interfaces**, select **Bypass interface access lists for inbound VPN sessions**.
   b. Under **Login Page Setting**, select **Allow user to select connection profile on the login page**.
   c. Under **Connection Profiles**, in the connection profile list, select the check box in the **SSL Enabled** column for your connection profile.

![Configuration screen](image)

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

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

4. 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.
5. 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.
6. On the main window, click **Configuration**.
7. 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.)

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

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

10. Complete the following fields:

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

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

12. In the right pane, in the **Server Group** field, select an appropriate server group (for example, **radiusgroup**).
13. In the left pane, click **Advanced > Clientless SSL VPN.**

14. Perform the following steps:
   a. In the right pane, in the **Login and Logout Page Customization** field, select **DfltCustomization.**
   b. Under **Connection Aliases**, select an appropriate alias (for example, **safenet**), and then select the option in the **Enabled** column.

15. Click **OK.**

16. Click **Apply.**

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

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

4. In the right pane, in the Customization objects list, select Dfltcustomizationgridsure, and then click Edit.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
5. 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 the **Show internal password** check box.
   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 “Obtaining a Grid URL” on page 54.

```html
// URL of the BlackShield ID Self Service page
function showGrid()
{
 var obj=document.getElementById('logon_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.getElementsByTagName("Login");
 if(obj)
 {
 obj[0].parentNode.innerHTML += '<INPUT type="button" name="getOTP" value="Get Grid" onclick="showGrid()">';
 }

 obj=document.getElementById("password_field");
```
6. On the main window, in the right pane, in the **Customization objects** list, select **Dfltcustomizationgridsure**, and then click **Assign**.

7. On the **Assign GUI Customization: Dfltcustomizationgridsure** 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.)

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

9. To verify if the **Dfltcustomizationgridsure** 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 Profile**.

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

![Screen Image](image)

(\textit{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 Identity Services Engine

To configure Cisco Identity Services Engine for RADIUS authentication requires the following:

- Configuring Network Devices, page 37
- Configuring External Identity Sources, page 41
- Configuring Policy, page 45

Configuring Network Devices

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

1. Open the following URL in a web browser: https://<Management IP Address of Cisco ISE>/admin
2. On the Identity Services Engine window, enter the appropriate credentials, and then click Login.

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

3. Click **Administration > Network Resources > Network Devices**.

4. From the **Network Devices** navigation pane on the left, click **Network Devices**, and then click **Add**.
5. On the **New Network Device** window, 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 network device (for example <strong>Cisco_ASA</strong>).</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Enter the IP address of the Client (ASA). This field includes the IP address and subnet masks that are associated with the device. A single address or a range, the routable IP address should be one with which the Cisco ISE appliance can communicate.</td>
</tr>
<tr>
<td><strong>Authentication Settings</strong></td>
<td>Enable the check box and expand the window.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the same shared secret that you entered in step 8 in “Creating the RADIUS-enabled AAA Server Group and its Servers” on page 16.</td>
</tr>
</tbody>
</table>

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
6. Click **Submit**. The network device is saved.

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

The Cisco Identity Services Engine (Cisco ISE) integrates with external identity sources to validate credentials in user authentication functions.

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

1. From the Cisco ISE Dashboard, click Administration > Identity Management > External Identity Sources.

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
2. In the left pane, click **RADIUS Token**, and then click **Add**.

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

4. Under the **General** tab, enter the RADIUS server **Name** (for example **FreeRADIUS**).

   (The screen image above is from Cisco. Trademarks are the property of their respective owners.)
3. Click the **Connection** tab, and then complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host IP</strong></td>
<td>Enter the IP address of the primary SAS RADIUS server.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the same shared secret that you entered in step 5 in “Adding Cisco Identity Services Engine as an Authentication Node in SAS” on page 10.</td>
</tr>
<tr>
<td><strong>Authentication Port</strong></td>
<td>Enter the port number on which the SAS RADIUS Server is listening. The default is 1812.</td>
</tr>
</tbody>
</table>

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
4. Click **Submit** to save the RADIUS token identity sources.

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

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

1. From the Cisco ISE Dashboard, click **Policy**. The default Authentication policy is displayed.
2. Select **Default Rule**, and then click **Edit**.

![Image of default policy configuration](image1)

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

3. Click the plus (+) sign in the default policy.

![Image of adding a new policy rule](image2)

(The screen image above is from Cisco. Trademarks are the property of their respective owners.)
4. Click **Identity Source**, and then select the appropriate identity source (for example, **FreeRADIUS**).

![Identity Source Image]

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

5. Click **Done**.

![Done Image]

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

(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 through Cisco ISE:

- Using Clientless SSL VPN, page 47
- Using Clientless SSL VPN with GrIDsure Authentication, page 49
- Using the Cisco AnyConnect Secure Mobility Client, page 51
- Using the SAS Agent for Cisco AnyConnect, page 52

**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.

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><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>2nd Username</strong></td>
<td>Enter your SAS user ID.</td>
</tr>
<tr>
<td><strong>2nd Password</strong></td>
<td>Generate an OTP using SafeNet eToken PASS, and then 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 when 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>GROUP</th>
<th>Select an appropriate group alias (for example, safenet).</th>
</tr>
</thead>
<tbody>
<tr>
<td>USERNAME</td>
<td>Enter your domain user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password associated with your domain user name.</td>
</tr>
<tr>
<td>2nd Username</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.

![Image](image_url)

(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.

![Image](image_url)

(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.

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 the 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 then 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>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 the password associated with your domain user name.</td>
</tr>
<tr>
<td>Token</td>
<td>Select an appropriate MP-1 token.</td>
</tr>
<tr>
<td>Pin</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 the Windows Registry after installing SafeNet Cisco AnyConnect Agent.

For details, refer to “Configuring SafeNet Cisco AnyConnect Agent Registry Key” on page 55.

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.

![Image of SAS console](image1)

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

![Image of Self-service Policy](image2)

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 a grid is displayed, 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 the Windows Registry is located at:

\HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\CiscoAnyClientPlugin

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

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

\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CRYPTOCard\CiscoAnyClientPlugin

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
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**;  
In this example:

- 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.

Refer to the examples below if changing the MP-1 token detection to a different field.

**ALL+ALL+1**

Display MPs in the first username field, and submit the one-time password (OTP) 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 the 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]

![SafeNet VPN Client for Cisco AnyConnect](image)

**NOTE:** In this integration (using RADIUS protocol for Cisco ISE), **ALL+ALL+2** is used.
ALL+ALL+3

Display MPs in the first and second username fields, and submit one-time password (OTP) to the first and second password fields. This setting is used if there needs to be authentication against two SAS servers. Typically, this setting would rarely be used.

Multiple options can be appended to the SoftTokenInclusion key.

Example:

Value of the SoftTokenInclusion Registry key: "ALL+Corporate+1;ALL+safenet+2;ALL+CRYPTOCard+3;"

For additional information, please refer to the SafeNet Authentication Service Cisco AnyConnect Agent Configuration Guide:

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></td>
</tr>
<tr>
<td>United States</td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>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 Gemalto Knowledge Base.