SafeNet Authentication Service
Integration Guide
Using RADIUS Protocol for Cisco ASA
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: 007-012967-001, Rev. C
Release Date: November 2015
Third-Party Software Acknowledgement ................................................................. 4
Description .................................................................................................................. 4
Applicability .................................................................................................................. 4
Environment ................................................................................................................ 4
Audience ....................................................................................................................... 4
RADIUS-based Authentication using SAS Cloud ......................................................... 5
RADIUS-based Authentication using SAS-SPE and SAS-PCE .................................... 6
RADIUS Authentication Flow using SAS .................................................................... 6
RADIUS Prerequisites ............................................................................................... 7
Configuring SafeNet Authentication Service ........................................................... 7
Creating Users Stores in SAS ....................................................................................... 7
Assigning an Authenticator in SAS .............................................................................. 8
Adding Cisco ASA as an Authentication Node in SAS ............................................... 9
Checking the SAS RADIUS Address ....................................................................... 11
Configuring Cisco ASA ............................................................................................. 12
Creating a RADIUS-enabled AAA Server Group ....................................................... 12
Adding an IP ADDRESS POOL ................................................................................... 15
Adding a Group Policy ............................................................................................... 16
Configuring a Connection Profile for Network (Client) Access .................................. 18
Configuring a Connection Profile for Clientless SSL VPN Access ............................. 22
Configuring a Connection Profile for Clientless SSL VPN Access for GrIDsure ......... 27
Running the Solution .................................................................................................. 33
Using Clientless SSL VPN Access ............................................................................. 34
Using Clientless SSL VPN Access with GrIDsure Authentication ............................... 36
Using the Cisco AnyConnect Secure Mobility Client .................................................. 37
Using the SAS Agent for Cisco AnyConnect ............................................................. 39
Using the Cisco VPN Client (IPsec) .......................................................................... 41
Appendix ....................................................................................................................... 43
Obtaining a Grid URL ................................................................................................. 43
Verifying the Grid URL ............................................................................................... 44
Configuring SafeNet Cisco AnyConnect Agent Registry Key ..................................... 44
Support Contacts ........................................................................................................ 49
Third-Party Software Acknowledgement

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

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

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

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Cisco ASA using SafeNet one-time (OTP) authenticators managed by SafeNet Authentication Service.

- Configure Cisco ASA to work with SafeNet Authentication Service in RADIUS mode.

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

Cisco ASA can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with SafeNet Authentication 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 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 ASA, 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 hosted RADIUS service diagram](image)

- **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 hosted on-premises diagram](image)

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


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 ASA.

1. A user attempts to log on to Cisco ASA using an OTP authenticator.
2. Cisco ASA sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
3. The SAS authentication reply is sent back to the Cisco ASA.
4. The user is granted or denied access to the Cisco ASA based on the OTP value calculation results from SAS.
RADIUS Prerequisites

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

- End users can authenticate from the Cisco ASA environment with a static password before configuring the Cisco ASA to use RADIUS authentication.
- Ports 1812/1813 are open to and from Cisco ASA.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and 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.
- Cisco VPN client is installed on the client machine.
- SafeNet eToken PASS and MP-1 token are already enrolled as an OTP token in SAS.

Configuring SafeNet Authentication Service

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

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding Cisco ASA as an Authentication Node in SAS, page 8
- Checking the SAS RADIUS Address, page 11

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 ASA.

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

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 screenshot](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.</td>
</tr>
<tr>
<td><strong>Agent Description</strong></td>
<td>Enter a host description.</td>
</tr>
</tbody>
</table>

![Add Auth Nodes screenshot](image)

The authentication node is added to the system.
Checking the SAS RADIUS Address

Before adding SAS as a RADIUS server in Cisco ASA, check its IP address. The IP address will then be added to Cisco ASA 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.

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

- Creating a RADIUS-enabled AAA Server Group, page 12
- Adding AN IP ADDRESS POOL, page 15
- Adding a Group Policy, page 16
- Configuring a Connection Profile for Network (Client) Access, page 18
- Configuring a Connection Profile for Clientless SSL VPN Access, page 22
- Configuring a Connection Profile for Clientless SSL VPN Access for GrIDsure, page 27

Creating a RADIUS-enabled AAA Server Group

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

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

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

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

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

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

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

<table>
<thead>
<tr>
<th>AAA Server Group</th>
<th>Enter a name for the AAA Server Group (for example, radiusgroup).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select RADIUS.</td>
</tr>
</tbody>
</table>

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

7. Under **AAA Server Groups**, select the newly created AAA server group.
8. Adjacent to the **Servers in the Selected Group** window, click **Add**.

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

<table>
<thead>
<tr>
<th><strong>Interface Name</strong></th>
<th>Select the interface to use to reach the RADIUS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server Name or IP Address</strong></td>
<td>Enter a server name or IP address to use to reach the RADIUS server.</td>
</tr>
<tr>
<td><strong>Server Authentication Port</strong></td>
<td>Enter the RADIUS server’s authentication port; for example, <strong>1812</strong>.</td>
</tr>
<tr>
<td><strong>Server Secret Key</strong></td>
<td>Enter the shared secret that will be used between Cisco ASA and the RADIUS server.</td>
</tr>
</tbody>
</table>

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

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

1. Launch the Cisco Adaptive Security Device Manager (ASDM).
2. Click the Configuration tab.
3. In the left pane, click Remote Access VPN.
4. Click Network (Client) Access > Address Assignment > Address Pools.

5. Click Add.

6. 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, up to 64 characters (for example, vpnpool).</td>
</tr>
<tr>
<td>Starting IP Address</td>
<td>Enter the first IP address available in the pool (for example, 8.8.8.1).</td>
</tr>
<tr>
<td>Ending IP Address</td>
<td>Enter the last IP address available in the pool (for example, 8.8.8.25).</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the subnet on which this IP pool resides (for example, 255.255.255.0).</td>
</tr>
</tbody>
</table>
7. Click **Apply**.

**Adding a Group Policy**

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

1. Launch the Cisco Adaptive Security Device Manager (ASDM).
2. Click the **Configuration** tab.
3. In the left pane, click **Remote Access VPN**.
4. Click **Network (Client) Access > Group Policies**.

5. Click **Add**.
6. On the **Add Internal Group Policy** window, perform the following steps, and then click **OK**.
   a. In the **Name** field, enter a name for the group policy (for example, **safenetpolicy**).
   b. Click **More Options**.
   c. Adjacent to **Tunneling Protocols**, deselect **Inherit**.
   d. Select the following:
      - Clientless SSL VPN
      - SSL VPN Client
      - IPsec IKEv1
      - IPsec IKEv2 (optional)
      - L2TP/IPsec (optional)

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

A connection profile consists of a set of records that determines tunnel connection policies. These records identify the servers to which the tunnel user is authenticated, as well as the accounting servers (if any), to which connection information is sent.

A connection profile also identifies a default group policy for the connection, which contains protocol-specific connection parameters, including a small number of attributes that pertain to creating the tunnel itself. Connection profiles include a pointer to a group policy that defines user-oriented attributes.

Configuring a Connection Profile for AnyConnect

1. Launch the Cisco Adaptive Security Device Manager (ASDM).
2. Click the **Configuration** tab.
3. In the left pane, click **Remote Access VPN**.
4. Click **Network (Client) Access > AnyConnect Connection Profiles**.

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

5. Under **Access Interfaces**, complete the following steps:
   e. Select **Enable Cisco AnyConnect VPN Client access** on the interfaces selected in the table below.
   f. For each interface (outside and inside), under **SSL Access**, select **Allow Access** and **Enable DTLS**.
   g. For each interface (outside and inside), under **IPsec Access**, select **Allow Access** and **Enable Client Services**.

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
6. Under **Connection Profiles**, click **Add**.

7. On the **Add AnyConnect Connection Profile** window, click **Basic**, and then complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter the name of the connection profile (for example, safenetprofile).</td>
</tr>
<tr>
<td><strong>Aliases</strong></td>
<td>Enter the alias for the connection profile (for example, safenet).</td>
</tr>
<tr>
<td><strong>AAA Server Group</strong></td>
<td>Select an appropriate AAA server group (for example, radiusgroup) for the menu. This will be the authentication method that will be associated with this profile.</td>
</tr>
<tr>
<td><strong>Client Address Pools</strong></td>
<td>Click <strong>Select</strong> and assign an address pool; for example, vpnpool.</td>
</tr>
</tbody>
</table>
| **Group Policy**     | - Select an appropriate group policy (for example, safenetpolicy) from the menu.  
                         - Select Enable SSL VPN client protocol.  
                         - Select Enable IPsec client protocol (optional).  
                         - Fill in the DNS Server detail. |

8. Click **OK**.

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
9. On the **AnyConnect Connection Profiles** window, verify these options are selected:
   - (Optional) Under **Access Interfaces**: Bypass interface access lists for inbound VPN sessions
   - Under **Login Page Setting**: Allow user to select connection profile on the login page

![Configuration window](image)

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

10. Click **Apply**.

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

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

![Configuration window](image)

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

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

![Configuration window](image)

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

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

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

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

1. Launch the Cisco Adaptive Security Device Manager (ASDM).
2. Click the Configuration tab. Then, in the left pane, click Remote Access VPN.
3. Click Clientless SSL VPN Access > Portal > Customization.

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

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

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

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
8. Under **Connection Profiles**, select the profile that you created earlier (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.)*

9. Click **Basic**, complete the following fields:

<table>
<thead>
<tr>
<th>AAA Server Group</th>
<th>Select an appropriate server group (for example, <code>radiusgroup</code>) from the menu.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Group</td>
<td>Select an appropriate DNS server group.</td>
</tr>
<tr>
<td>Group Policy</td>
<td>Select an appropriate group policy (for example, <code>safenetpolicy</code>) from the menu.</td>
</tr>
<tr>
<td>Enable clientless SSL VPN protocol</td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

   ![Edit Clientless SSL VPN Connection Profile](image)

   *(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)*
10. On the **Edit Clientless SSL VPN Connection Profile** window, click **Advanced > Clientless SSL VPN**.

![Edit Clientless SSL VPN Connection Profile](image1)

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

11. Complete the following steps, and then click **OK**:

    h. In the **Login and Logout Page Customization** menu, verify that **DfltCustomization** is selected.

    i. Under **Connection Aliases**, verify the **safenet** alias is set to **Enabled**.

![Login and Logout Page Customization](image2)

*(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)*
12. 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 this configuration, you will create another template with different login page settings.

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

1. Launch the Cisco Adaptive Security Device Manager (ASDM).
2. Click the Configuration tab.
3. In the left pane, click Remote Access VPN.
4. Click Clientless SSL VPN Access > Portal > Customization.

5. Under Customization Objects, select the DfltCustomizationGridsure template, and then click Edit. This template will be used for the Login page and the main SSL portal page.

6. On the Edit Customization Object window, click Logon Page > Logon Form.
7. Under **Username and Password**, deselect **Show internal password**, and then click **OK**.

8. Click **Informational Panel**, and then click **Display Informational Panel**.
9. 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 Appendix.

```html
<script>
//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.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)
{

</script>
```
obj.innerHTML="Password";
}
</script>

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

![Customization Objects screen](image1.png)

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

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

![Assign GUI Customization window](image2.png)

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

13. In the left pane, under **Remote Access VPN**, click **Clientless SSL VPN Access > Connection Profiles**.

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

15. On the **Edit Clientless SSL VPN Connection Profile** window, click **Advanced > Clientless SSL VPN**.

16. In the **Login and Logout Page Customization** menu, verify that **DfltCustomizationGridsure** is selected, and then click **OK**.
Running the Solution

Before running the RADIUS server integration solution, a corresponding RADIUS client must be added in SAS.

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

- Using Clientless SSL VPN Access, page 34
- Using Clientless SSL VPN Access with GrIDsure Authentication, page 36
- Using the Cisco AnyConnect Secure Mobility Client, page 37
- Using the SAS Agent for Cisco AnyConnect, page 39
Using Clientless SSL VPN Access

Clientless SSL VPN creates a secure, remote-access VPN tunnel to Cisco ASA using a web browser without requiring a software or hardware client. It provides secure and easy access to a broad range of web resources, and both web-enabled and legacy applications, from almost any device that can connect to the Internet via HTTP, including:

- Internal websites
- Web-enabled applications
- NT/Active Directory file shares
- Email proxies, including POP3S, IMP4S, and SMTPS
- Microsoft Web App to Exchange Server 2010 in 8.4(2) and later
- Application Access (smart tunnel or port forwarding access to other TCP-based applications)

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

1. Open the following URL in a web browser: https://<Public IP Address of Cisco ASA>.
2. On the SSL VPN Service window, complete the following fields:

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

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

3. Click Login.

If the login credentials provided are authenticated successfully, you are logged in. You can access the service and application configured.
(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
Using Clientless SSL VPN Access 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 appropriate customization page should be selected in the 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 SAS user ID.</td>
</tr>
</tbody>
</table>

3. Click Get Grid.
4. In the Password field, enter the characters from the grid cells that correspond to your PIP (personal identification pattern), and then click Login.

(The screen image above is from Cisco®. Trademarks are the property of their respective owners.)
After successful authentication, you will be logged in, and the **Home** page is displayed.

![Cisco VPN Service](image)

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

**Using the Cisco AnyConnect Secure Mobility Client**

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

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

4. **Start the Cisco AnyConnect Secure Mobility Client application from Start > All Programs > Cisco > Cisco AnyConnect Secure Mobility Client.**

5. **In the VPN field, enter the fully qualified domain name or IP address for Cisco ASA, and then click Connect.**

![Cisco AnyConnect Secure Mobility Client](image)

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

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

<table>
<thead>
<tr>
<th><strong>Group</strong></th>
<th>Select an appropriate group alias; for example, safenet.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username</strong></td>
<td>Enter your SAS user ID.</td>
</tr>
<tr>
<td><strong>Password</strong></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.
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 MP1 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>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>
If authentication is successful, the VPN session will be established.
Using the Cisco VPN Client (IPsec)

The Cisco VPN Client provides remote users with a secure VPN connection to Cisco ASA using IPsec protocol.

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

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

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

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

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

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

Obtaining a Grid URL

To configure a connection profile for Clientless SSL VPN Access for GrIDsure (as described on page 27), you will need to specify the grid URL in the GrIDsure code. Follow the steps below to obtain the grid URL.

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

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

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

8. Replace the ss.safenet-inc.com to grid.safenet-inc.com:
9. Append the following text in the Self Service Unique URL:

?getChallengelmage=true&userName=

Now you will have the grid maker URL as follows:


Verifying the Grid URL

To verify the grid URL from the previous section is operational, add a valid username after `username=` in the URL, and then paste the URL in the browser to verify that the grid will display.

As an example:

1. Enroll a Gridsure token for the user, alice.
2. Append the username, alice, to `username=` in the URL. The URL would now look like this:


3. Browse to the address. If the grid displays, then the URL is correct. If it does not display, verify the self-service unique URL, appended string, and username are 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

![Registry Key Diagram]

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.
NOTE: In this integration (Using RADIUS Protocol for Cisco Secure ASA), **ALL+ALL+1** is used.

### 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]
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;”

For more information please refer to http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/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>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>