RSA SECURID® ACCESS
Standard Agent Implementation Guide

Cisco Adaptive Security Appliance 9.5(2)

Peter Waranowski, RSA Partner Engineering
Last Modified: April 13th, 2017

RSA READY

Solution Summary

Cisco Adaptive Security Appliance (ASA) supports RSA SecurID Access through the use of AAA Server Groups. AAA Server Groups can be configured to communicate with RSA Cloud Authentication Service via RADIUS and with Authentication Manager via either RADIUS or native RSA SecurID protocol. Services able to integrate with RSA SecurID-configured AAA Server Groups include: IPsec VPN, SSL VPN, Firewall AAA Rules and ASDM access.

The clientless SSL VPN portal can be configured for use with Risk-Based Authentication. When configured, a user accessing the SSL VPN portal will be directed to the Authentication Manager Secure Logon page. The user logs in to the system using their username and password. If Authentication Manager determines this to be a low risk logon, the user will be logged in to the SSL VPN portal and the connection will be established. If Authentication Manager determines this to be a high risk logon, the user can be challenged with life questions or ODA to further authenticate the user.

RSA SecurID Access Features	
Cisco ASA 9.5(2)	
Authentication Manager Methods	
RSA SecurID	Yes
On Demand Authentication	Yes
Risk-Based Authentication	Yes
Cloud Authentication Service Methods	
Authenticate App	Yes
FIDO Token	No

Identity Assurance	
Collect Device Assurance and User Behavior	No

Configuration Summary

All of the supported use cases of RSA SecurID Access with Cisco ASA require both server-side and Cisco ASA-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA SecurID and/or **On Demand Authentication** – Cisco ASA can be configured with RSA SecurID Authentication in the following ways:

UDP Agent to RSA Authentication Manager

Authentication Manager UDP Agent Configuration
Cisco ASA UDP Agent Configuration

RADIUS Client to RSA Authentication Manager

Authentication Manager RADIUS Configuration
Cisco ASA RADIUS Configuration

RADIUS Client to Cloud Authentication Service (via RSA Identity Router) – When configuring RSA SecurID authentication via RADIUS, Cisco ASA will always challenge for LDAP Username and Password first.

Cloud Authentication Service RADIUS Configuration
Cisco ASA RADIUS Configuration

LDAP Password – Cisco ASA can be configured with LDAP Password Authentication in the following way:

RADIUS Client to Cloud Authentication Service (via Identity Router) – When configuring LDAP Password authentication via RADIUS, you can configure an Access Policy for additional authentication to Authenticate Approve, Authenticate Tokencode or RSA SecurID methods.

Cloud Authentication Service RADIUS Configuration
Cisco ASA RADIUS Configuration

RSA Risk-Based Authentication – Cisco ASA can be configured with RSA Risk-Based Authentication in the following way(s):

UDP Agent + Risk-Based Authentication to RSA Authentication Manager

Authentication Manager UDP Agent Configuration
Authentication Manager Risk-Based Configuration
Cisco ASA UDP Agent Configuration
Cisco ASA Risk-Based Authentication Configuration

RADIUS Client + Risk-Based Authentication to RSA Authentication Manager

Authentication Manager RADIUS Configuration
Authentication Manager Risk-Based Configuration
Cisco ASA RADIUS Configuration
Cisco ASA Risk-Based Authentication Configuration

Authenticate Approve – Cisco ASA can be configured with Authenticate Approve authentication in the following way:

RADIUS Client to RSA Cloud Authentication Service (via RSA Identity Router) – When configuring Authenticate Approve authentication via RADIUS, Cisco ASA will always challenge for LDAP Username and Password first.

Cloud Authentication Service RADIUS Configuration
Cisco ASA RADIUS Configuration

Authenticate Tokencode – Cisco ASA can be configured with Authenticate Tokencode authentication in the following way(s):

RADIUS Client to RSA Cloud Authentication Service (via Identity Router) – When configuring Authenticate Tokencode authentication via RADIUS, Cisco ASA will always challenge for LDAP Username and Password first.

Cloud Authentication RADIUS Configuration
Cisco ASA RADIUS Configuration

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

RADIUS

To configure RADIUS for Cloud Authentication Service for use with a RADIUS client, you must first configure a RADIUS client in the RSA SecurID Access Console.

Logon to the RSA SecurID Access console and browse to **Authentication Clients** > **RADIUS** > **Add RADIUS Client** and enter the **Name**, **IP Address** and **Shared Secret**. Click **Publish** to push your configuration change to the RADIUS server.

RSA Cloud Authentication Service RADIUS server listens on port UDP 1812.

RSA Authentication Manager Configuration

RSA Authentication Manager can be configured to communicate with 4 distinct types of authentication clients (agents). Each type of agent requires different configuration on the server side.

UDP Agent

To configure your RSA Authentication Manager for use with a UDP-based agent, you must create an agent host record in the Security console of your Authentication Manager and download its configuration file (sdconf.rec).

- Hostname: Configure the agent host record name to match the hostname of the agent.
- IP Address: Configure the agent host record to match the IP address of the agent.

! Important: Authentication Manager must be able to resolve the IP address from the hostname.

RADIUS

To configure your RSA Authentication Manager for use with a RADIUS Agent, you must configure a RADIUS client and a corresponding agent host record in the Authentication Manager Security Console.

The relationship of agent host record to RADIUS client in the Authentication Manager can 1 to 1, 1 to many or 1 to all (global).

RSA Authentication Manager RADIUS server listens on ports UDP 1645 and UDP 1812.

Risk-Based Authentication

To configure your RSA Authentication Manager for risk-based authentication with Cisco ASA, you must create an agent host record and enable it for risk-based authentication in the RSA Authentication Manager Security Console. You will need to download the sdconf.rec and the risk-based authentication integration script for the appropriate device type to configure the agent. RSA Authentication Manager can integrate risk-based authentication with UDP-based or RADIUS agents only.

The latest risk-based authentication script template is at the following link.

https://sftp.rsa.com/human.aspx?Username=partner&password=RSAS3cur3d!&arg01=688653577&arg12=downloaddirect&transaction=signon&quiet=true

Download this file and copy it to the following directory in your primary RSA Authentication Manager server.

```
/opt/rsa/am/utils/rba-agents
```

Please refer to RSA documentation for more information on RBA integration scripts.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Cisco ASA with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Cisco ASA components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Overview

Configure AAA Server Group for RSA SecurID Access

Native UDP Agent integration

Create an AAA Server Group to integrate with RSA Authentication Manager via Native RSA SecurID protocol.

RADIUS integration

Create an AAA Server Group to integrate with RSA Cloud Authentication Service or RSA Authentication Manager.

Integrate Cisco ASA with RSA SecurID Access AAA Server Group

Network (Client) Access using IPsec (IKEv1)

Configure remote access IPsec VPN with RSA SecurID Access for use with Cisco VPN Client.

Network (Client) Access using AnyConnect

Configure remote access SSL or IKEv2 VPN with RSA SecurID Access for use with Cisco AnyConnect Secure Mobility Client.

Firewall

Configure a firewall AAA rule to challenge users accessing protected network services with RSA SecurID Access.

ASDM

Configure ASA with RSA SecurID Access for administrative access to ASDM.

Clientless SSL VPN

Configure clientless SSL VPN with RSA SecurID Authentication.

Configure Cisco ASA for Risk-Based Authentication

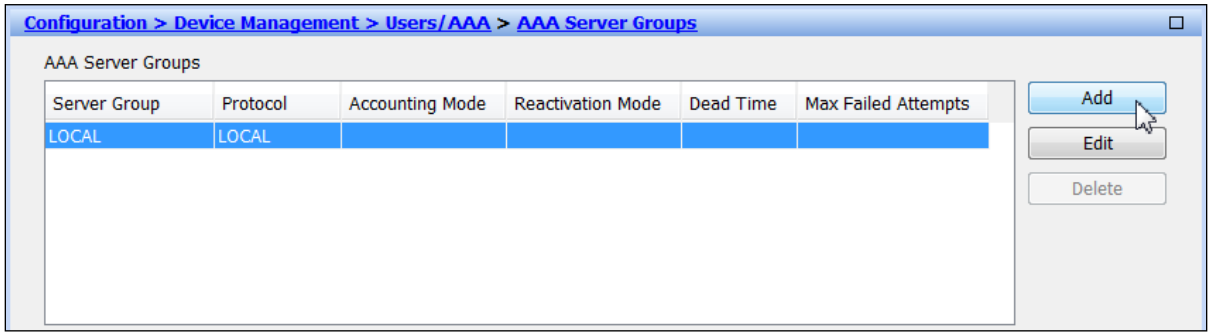
Clientless SSL VPN

Configure clientless SSL VPN with Risk-Based Authentication.

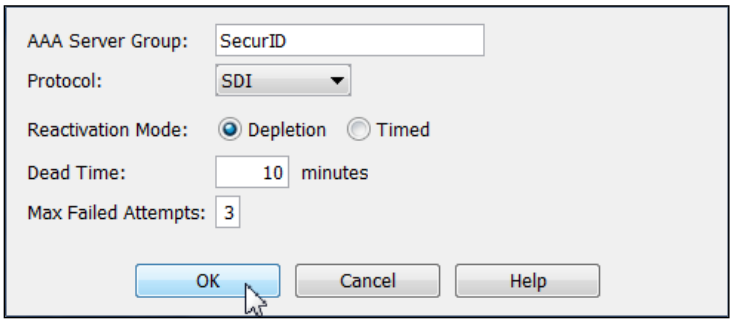
Cisco ASA UDP Agent Configuration

Complete the steps in this section to integrate Cisco ASA with RSA SecurID Access using UDP-based agent protocol.

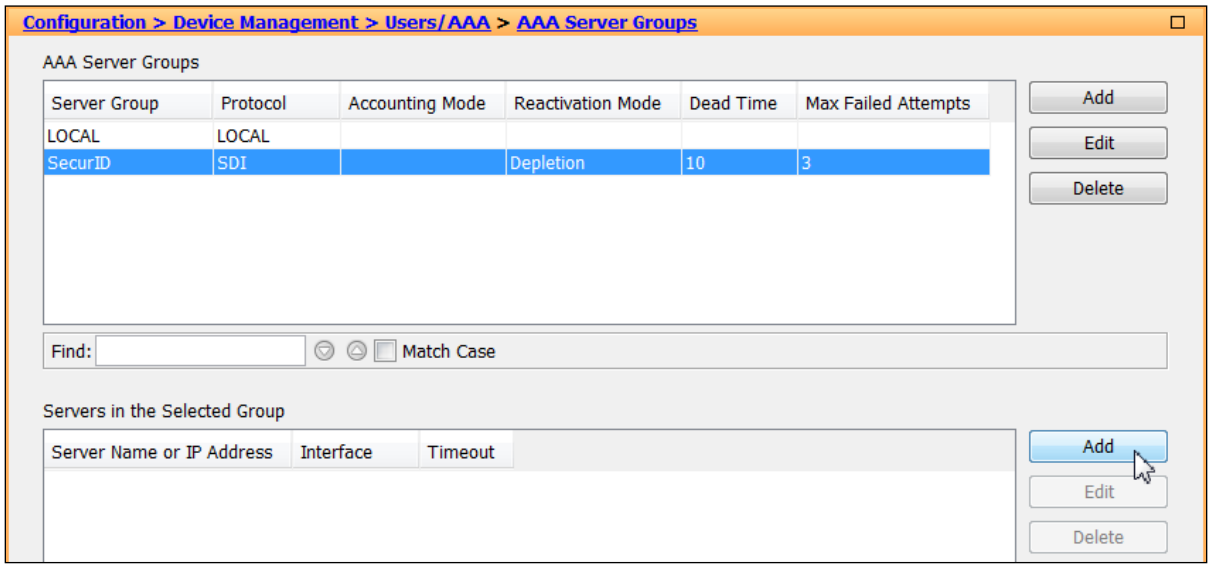
1. Browse to **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups** and click **Add**.



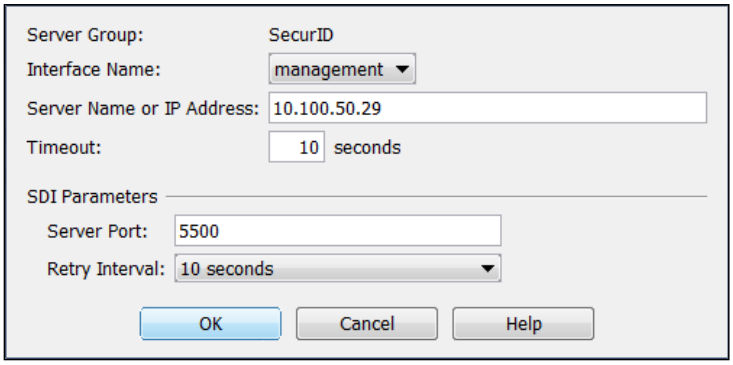
2. Enter **Server Group** name, select **SDI** from the **Protocol** drop-down menu and click **OK**.



3. Select the **AAA Server Group** and click **Add** to add a server to the group.



4. Select the appropriate interface from the **Interface Name** drop-down menu, enter the **Server Name or IP Address** of the primary RSA Authentication Manager server and click **OK**.



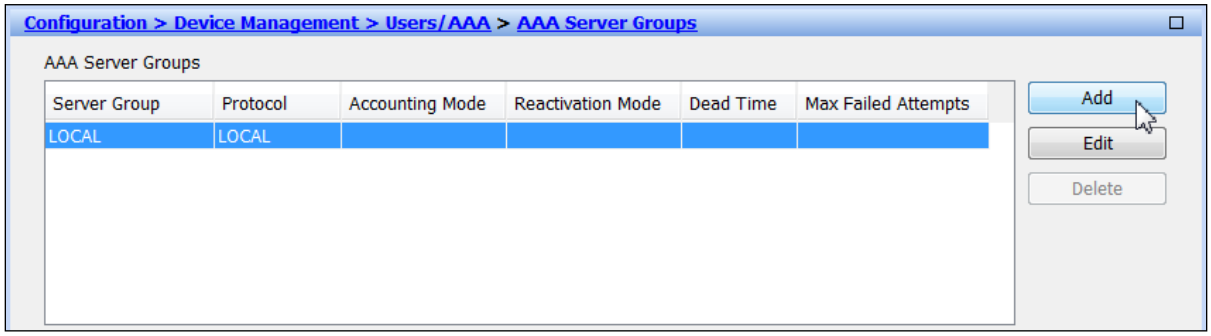
! Important: ONLY ADD THE PRIMARY RSA AUTHENTICATION MANAGER. DO NOT ADD REPLICAS. The Cisco ASA will learn about any RSA Authentication Manager replica servers, and prioritize them at the time of the first authentication. This SDI server list is in memory, and lost when the ASA is shut down. If the primary RSA Authentication Manager server is not available for authentication after the system boots, the ASA will not have knowledge of the RSA Authentication Manager replica servers.

5. Click **Apply** to complete the configuration.

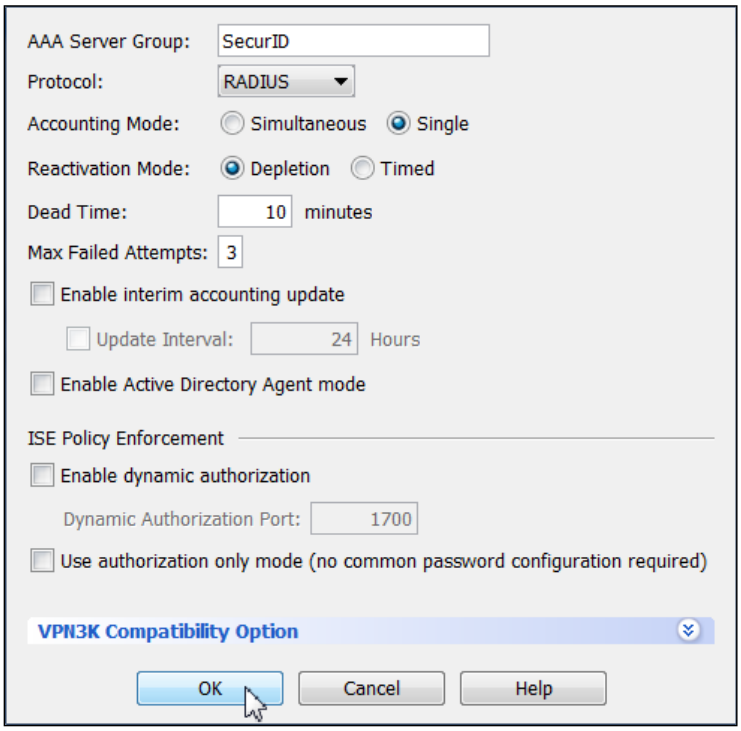
Cisco ASA RADIUS Configuration

Complete the steps in this section to integrate Cisco ASA with RSA SecurID Access using RADIUS authentication protocol.

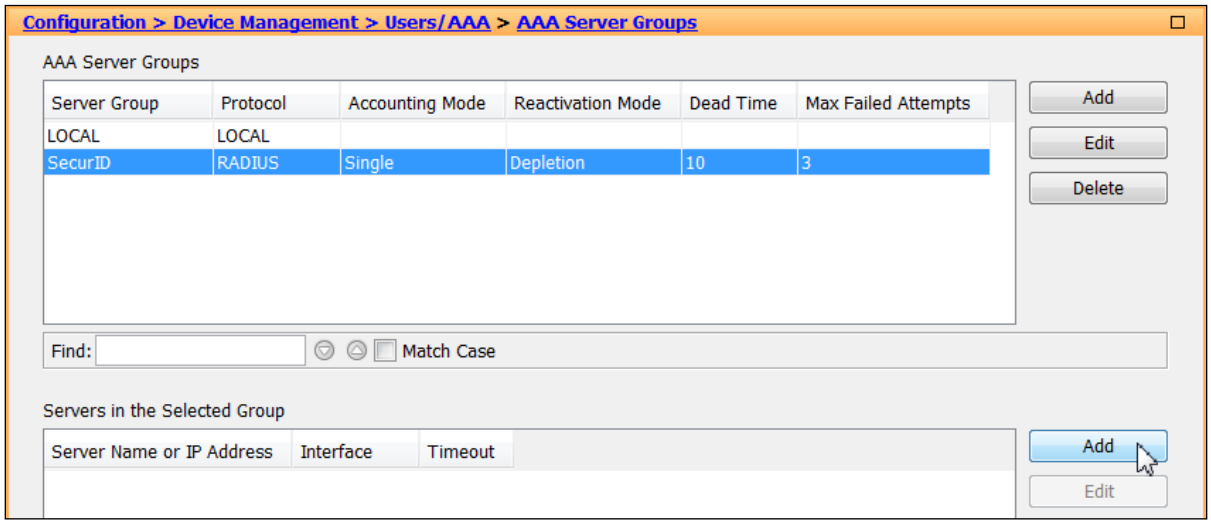
1. Browse to **Configuration** > **Device Management** > **Users/AAA > AAA Server Groups** and click **Add**.



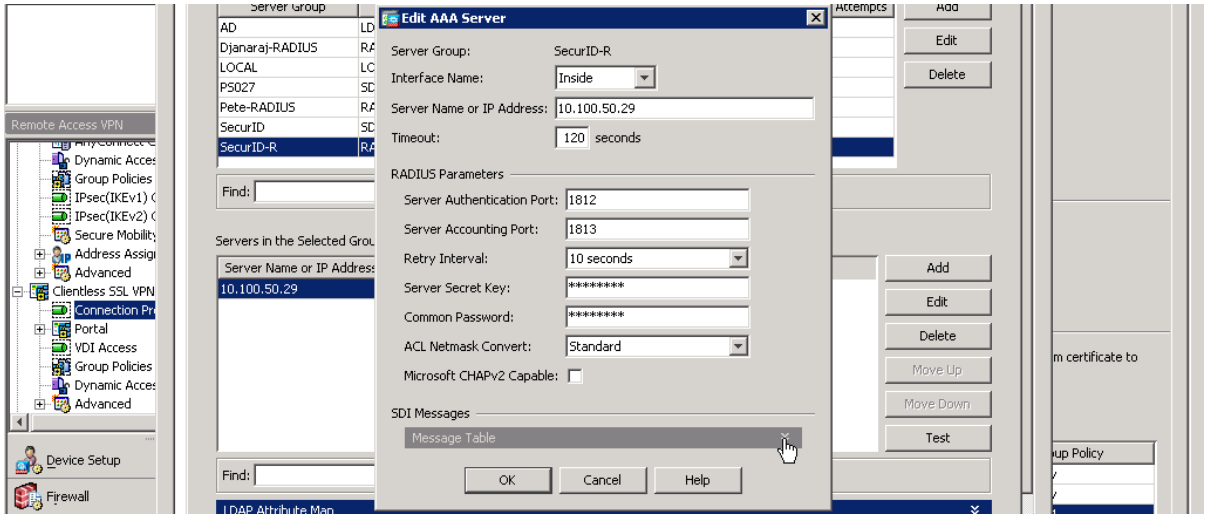
2. Enter **Server Group** name, select **RADIUS** from the **Protocol** drop-down menu and click **OK**.



3. Select the **AAA Server Group** and click **Add** to add a server to the group.



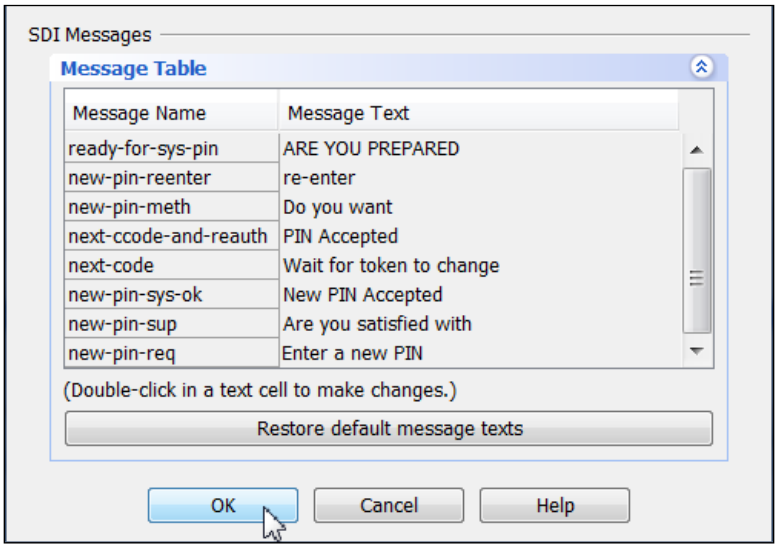
4. Configure the AAA Server and click **Message Table** under **SDI Messages**.



- Select the appropriate interface from the **Interface Name** drop-down menu.
- Enter the **Server Name or IP Address** of the RSA Authentication Manager server.
- Set the **Timeout** value to **120** seconds if you are integrating with RSA Cloud Authentication Service.
- Set the **Server Authentication Port**. Authentication Manager listens on UDP 1645 and 1812 by default. RSA Cloud Authentication Service listens on UDP 1812 by default.
- Enter the **Server Secret Key**.

! Important: Set the Server Authentication Port to 1812 and Timeout value to 120 seconds if you are integrating with RSA Cloud Authentication Service.

5. Set the **Message Text** in the **Message table** as shown in the following image and click **OK**.

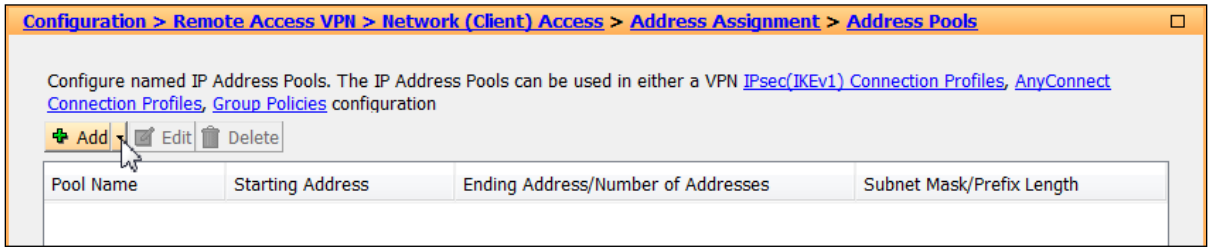


Note: Repeat steps 3-5 to add RSA Authentication Manager replica servers.

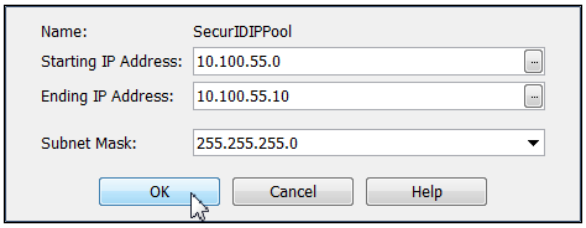
6. Click **Apply** to complete the configuration.

Integrate Network (Client) Access using IPsec (IKEv1) with RSA SecurID Access

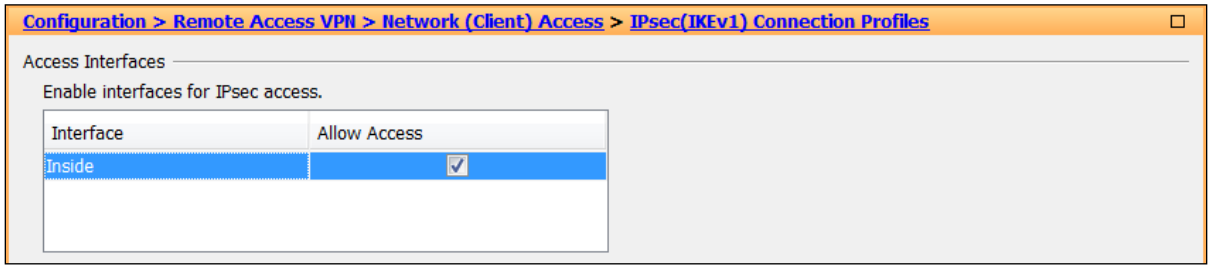
1. Browse to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Address Assignment** > **Address Pools** and click **Add**.



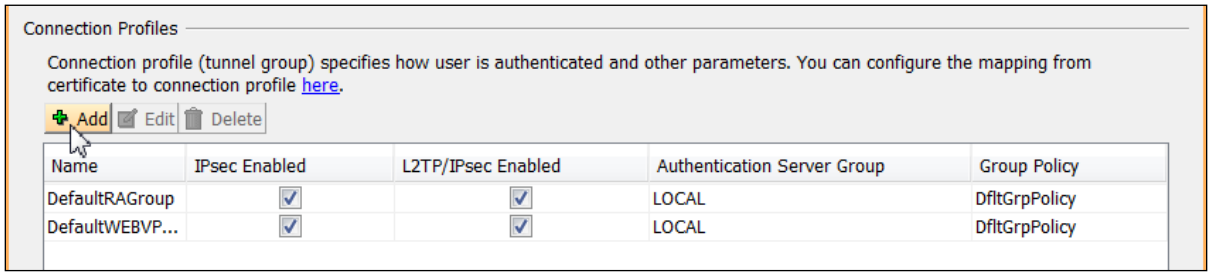
2. Enter the **Name**, **Starting IP Address**, **Ending IP Address** and **Subnet Mask** for your IP Pool and click **OK**.



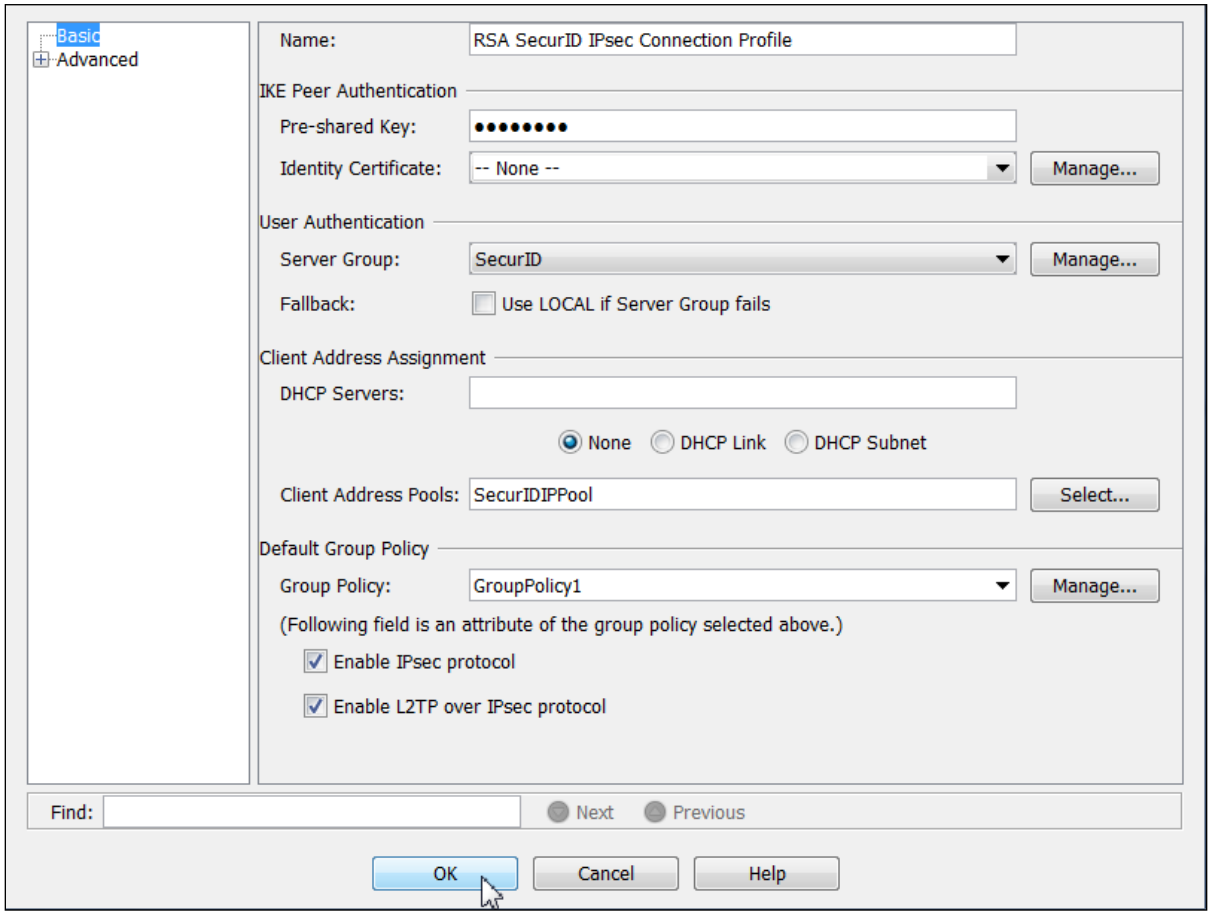
3. Browse to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **IPsec(IKEv1) Connection Profiles** and mark the **Allow Access** checkboxes for the interfaces on which you are enabling IPSec VPN access.



4. Browse to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **IPsec(IKEV1) Connection Profiles** and click **Add** under **Connection Profiles**.



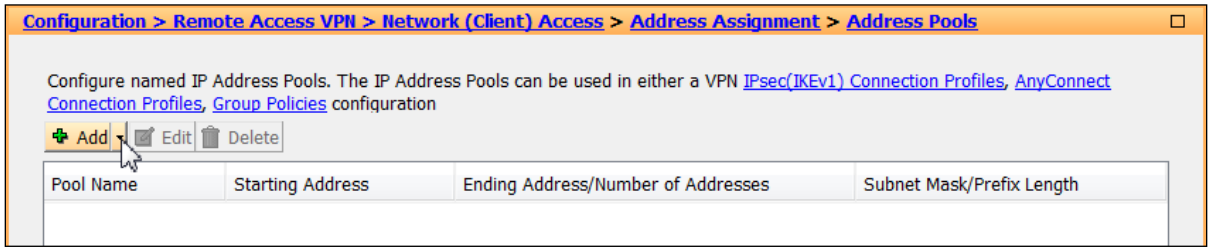
5. Choose a **Name**, **Pre-shared Key**, **User Authentication - Server Group**, **Client Address Pool** and **Group Policy** for this connection profile. Click **OK**.



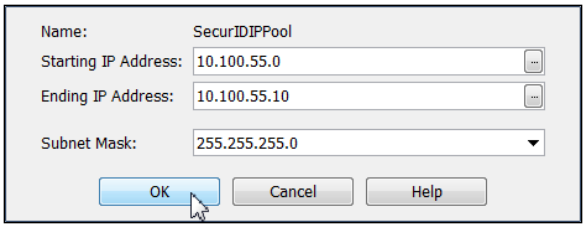
6. Click **Apply** to complete the configuration.

Integrate Network (Client) Access using AnyConnect with RSA SecurID Access

1. Browse to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Address Assignment** > **Address Pools** and click **Add**.

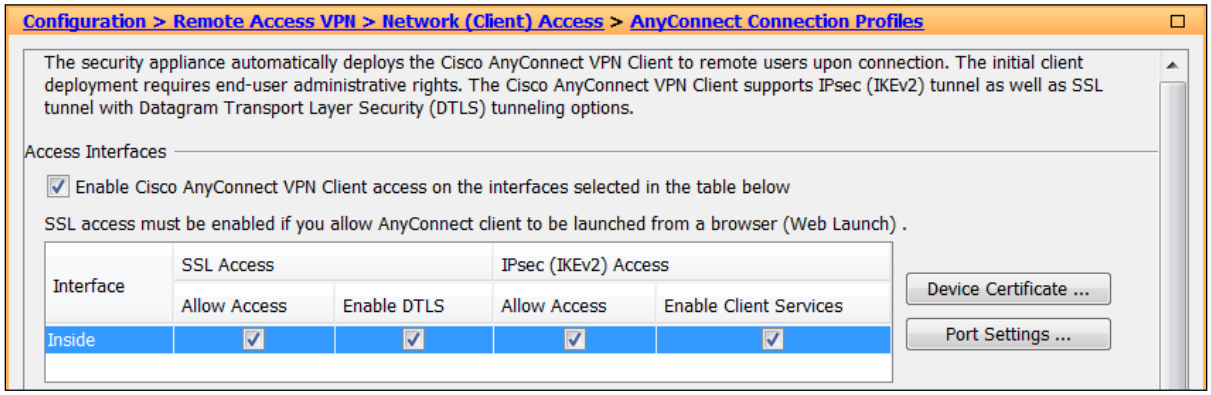


2. Enter the **Name**, **Starting IP Address**, **Ending IP Address** and **Subnet Mask** for your IP Pool and click **OK**.

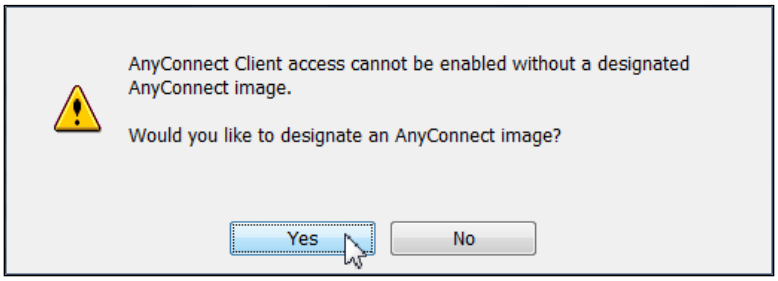


3. Browse to **Configuration** > **Remote Access VPN > Network (Client) Access** > **AnyConnect Connection Profiles**. Mark the checkboxes for the following items:

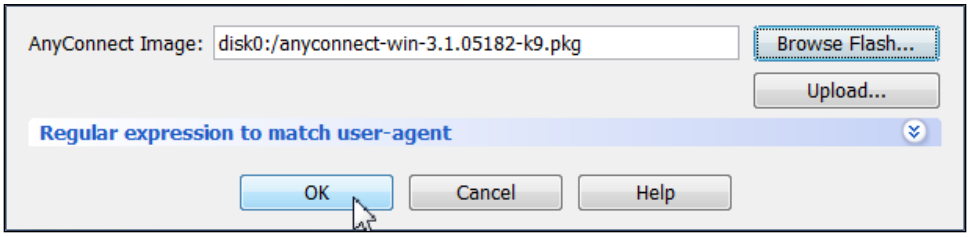
   - Enable Cisco AnyConnect VPN Client access to the interfaces selected in the table below
   - Interface(s) on which you are enabling AnyConnect VPN Client access.



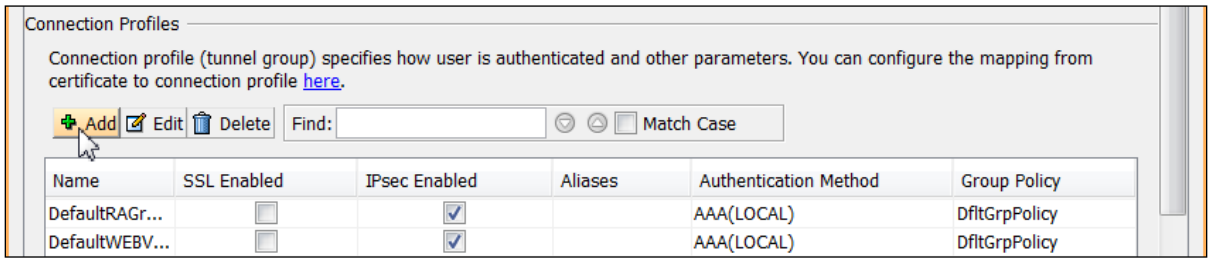
4. Click **Yes** to designate an AnyConnect image.



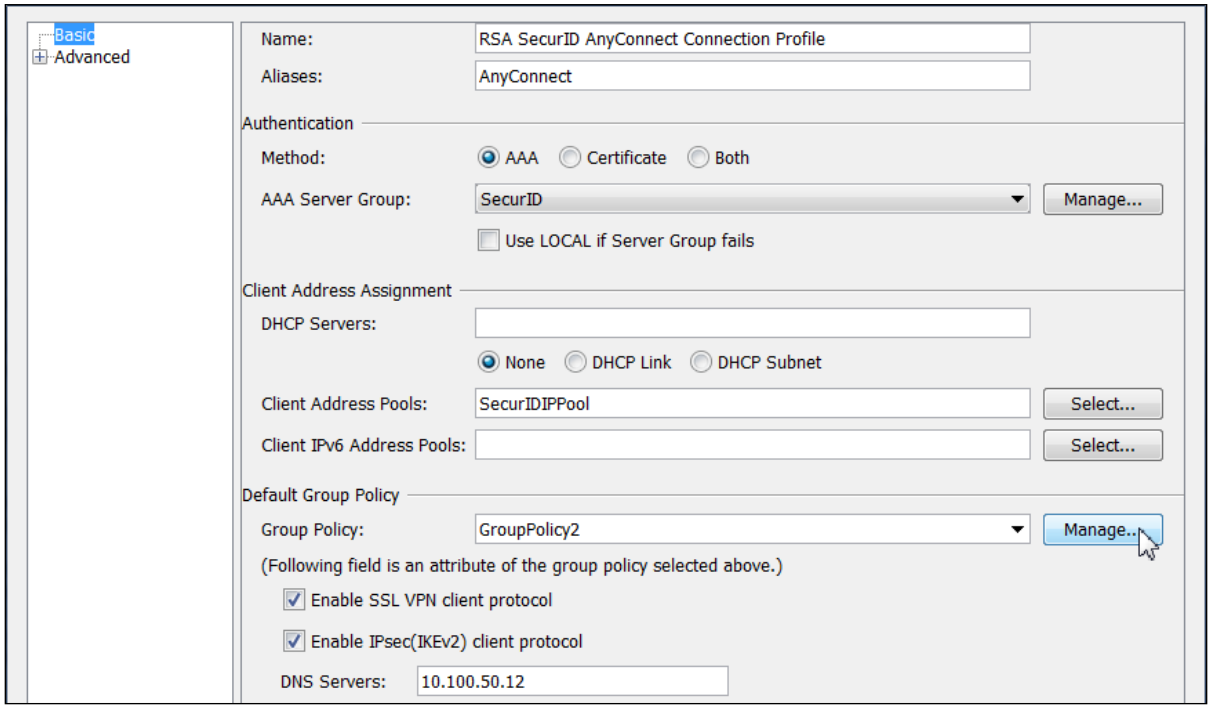
5. **Browse Flash** or **Upload** the AnyConnect image and click **OK**.



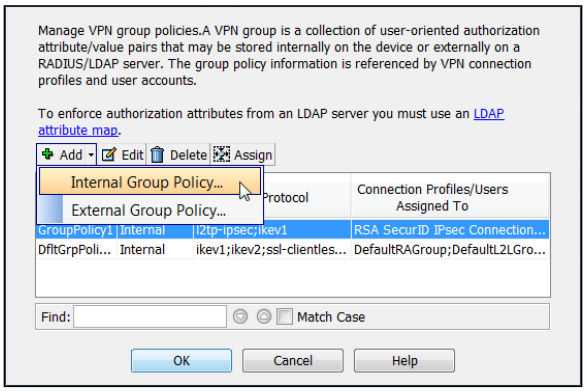
6. Browse to **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **AnyConnect Connection Profiles** and click **Add** under **Connection Profiles**.



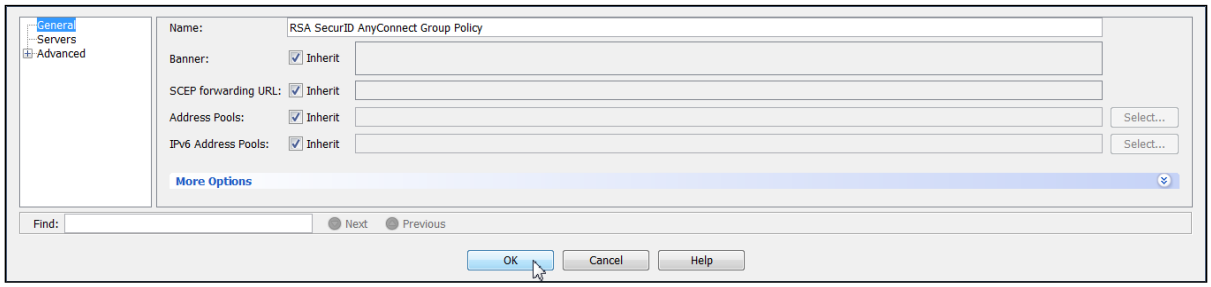
7. Enter **Name**, **Alias**, **AAA Server Group**, **Client Address Pool**, **DNS Servers** and click **Manage** next to **Group Policy**.



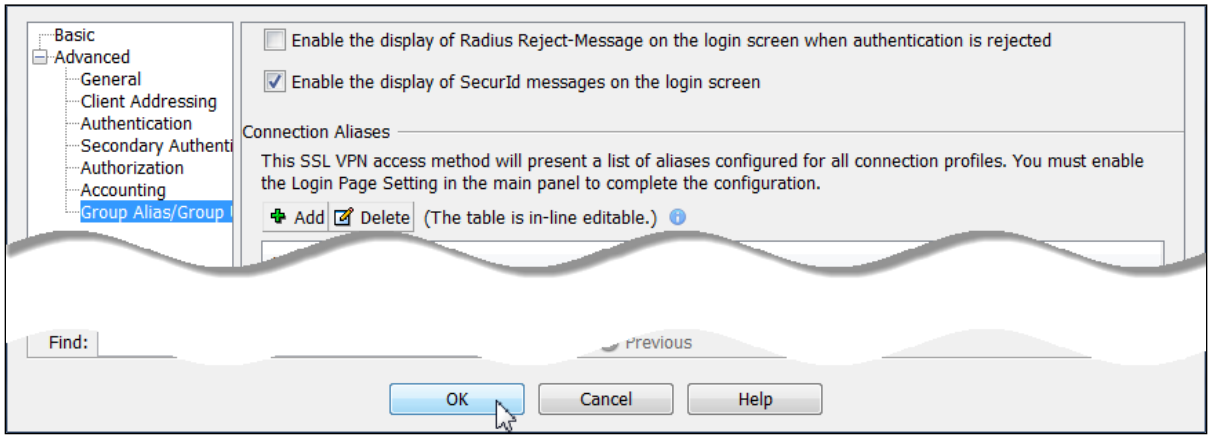
8. Click **Add** > **Internal Group Policy...** to add a group policy.



9. Enter a **Name** for the Group Policy and click **OK**.



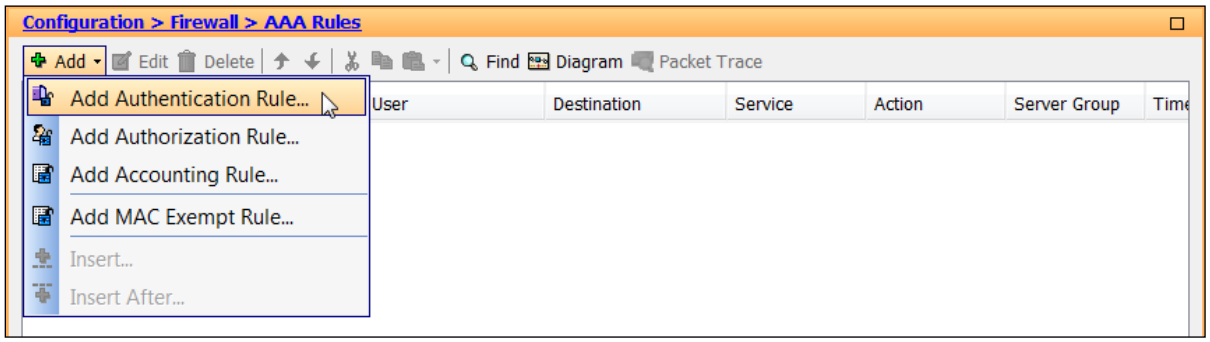
10. If enabling SecurID Authentication via RADIUS, browse to **Advanced** > **Group Alias/Group URL**, mark the checkbox next to **Enable the display of SecurId messages on the login screen** and click **OK**.



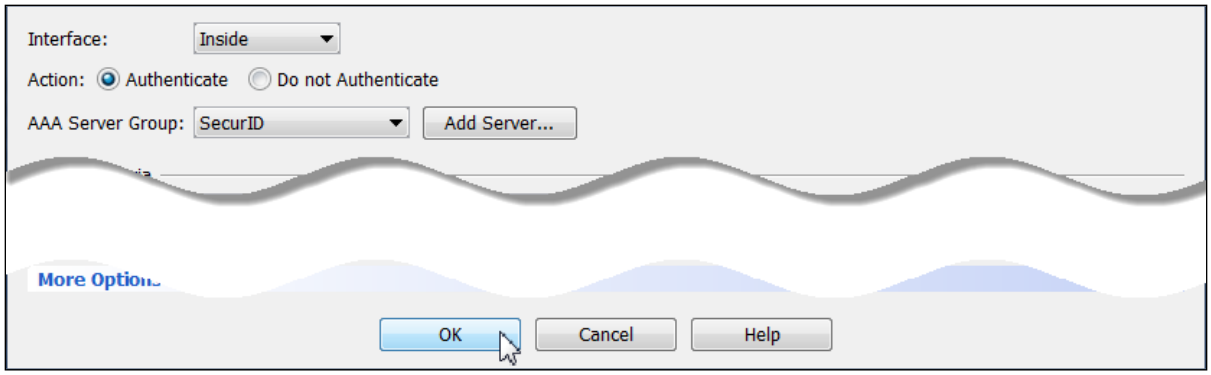
11. Click **Apply** to complete the configuration.

Integrate Firewall with RSA SecurID Access

1. Browse to **Configuration** > **Firewall** > **AAA Rules** and click **Add** > **Add Authentication Rule...**



2. Make the appropriate selections and click **OK**.

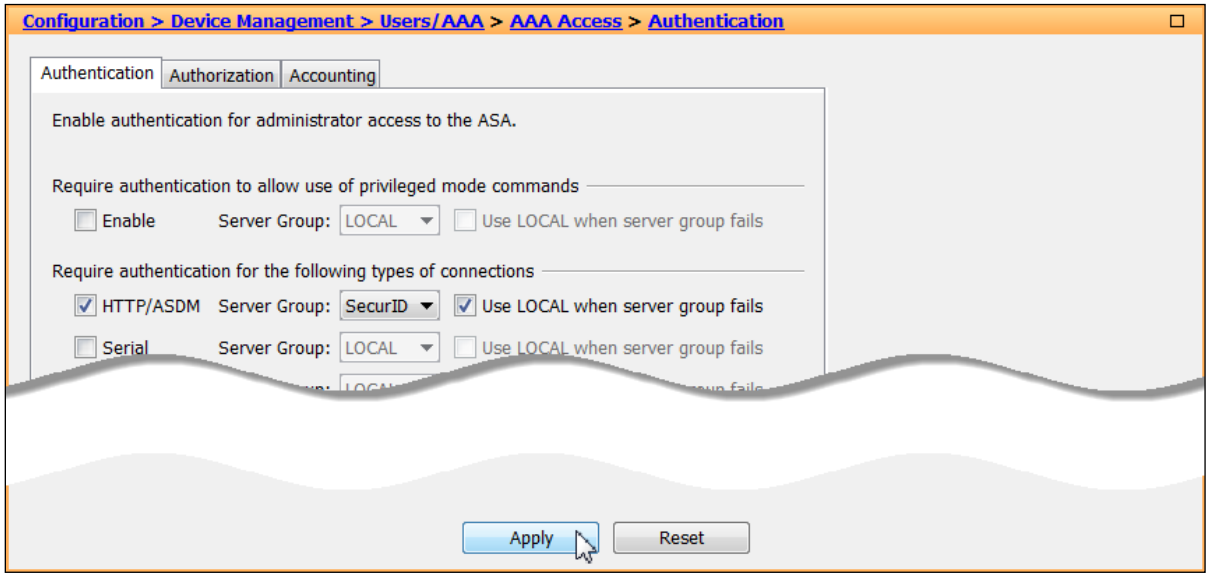


3. Click **Apply** to complete the configuration.

! Important: Although the ASA can be configured to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the ASA allows other traffic requiring authentication. Telnet is the only service in which new PIN and Next Tokencode functions are supported.

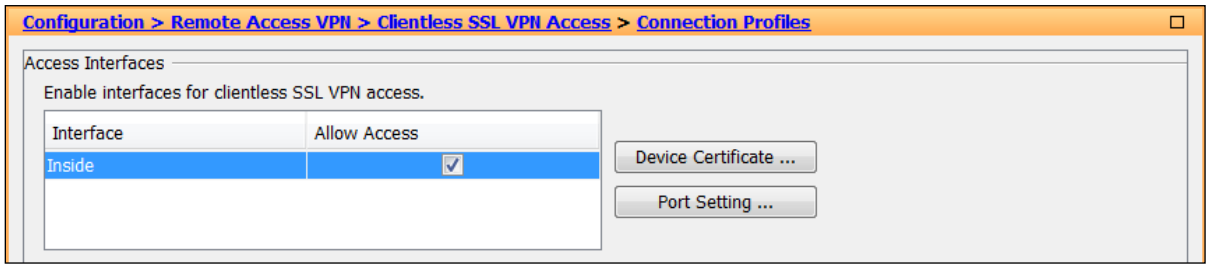
Integrate ASDM with RSA SecurID Access

1. Browse to **Device Management** > **Users/AAA** > **AAA Access**.
2. Mark the checkbox next to **HTTP/ASDM** and select the **AAA Server Group** from the drop-down menu and click **Apply**.

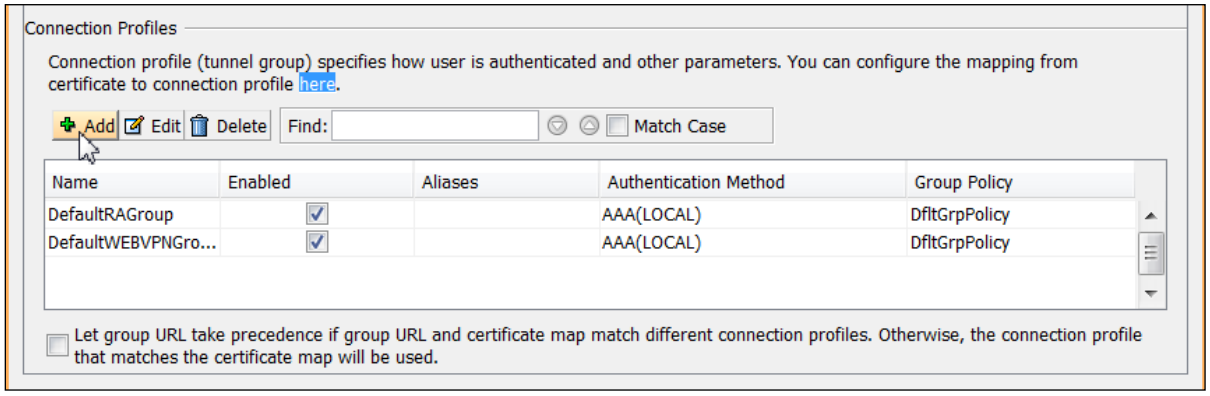


Integrate Clientless SSL VPN Portal with RSA SecurID Access

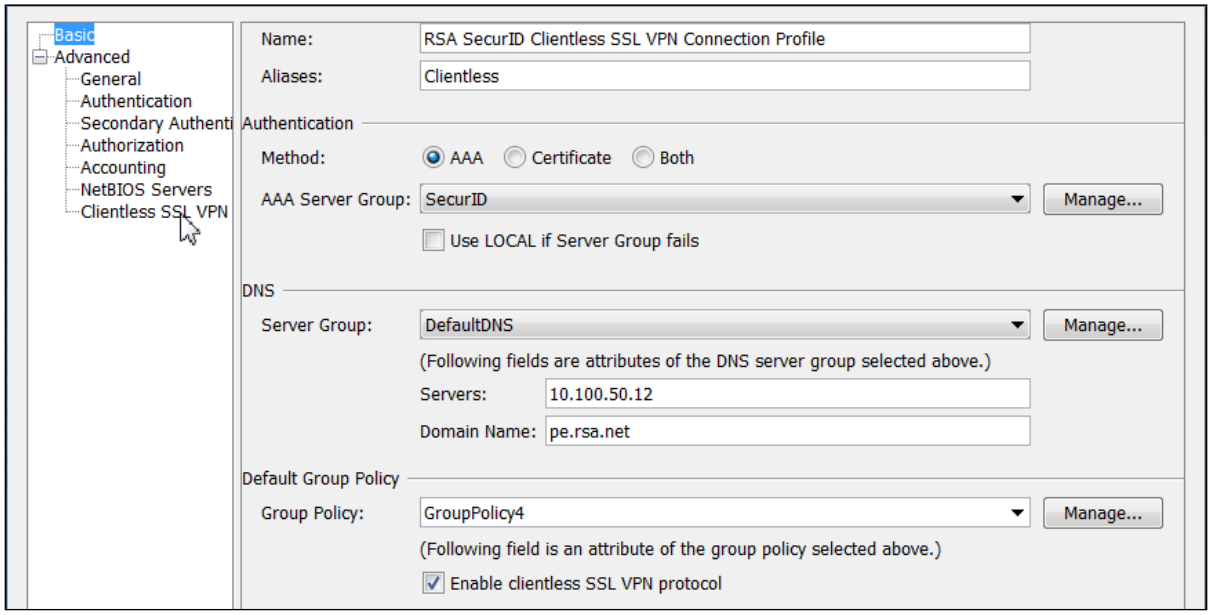
1. Browse to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles** and mark the **Allow Access** checkboxes for the interfaces on which you are enabling Clientless SSL VPN access.



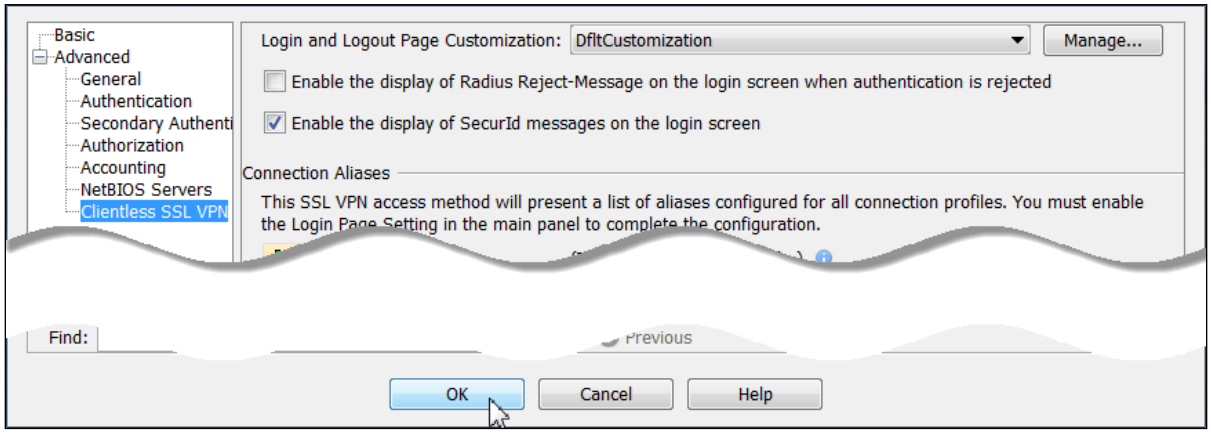
2. Browse to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles** and click **Add** under **Connection Profiles**.



3. Choose a **Name**, **Alias**, **AAA Server Group**, **Group Policy,** mark the checkbox for **Enable clientless SSL VPN protocol** and then browse to **Advanced** > **Clientless SSL VPN**.



4. Mark the checkbox for **Enable the display of SecurID messages on the login screen** and click **OK**.



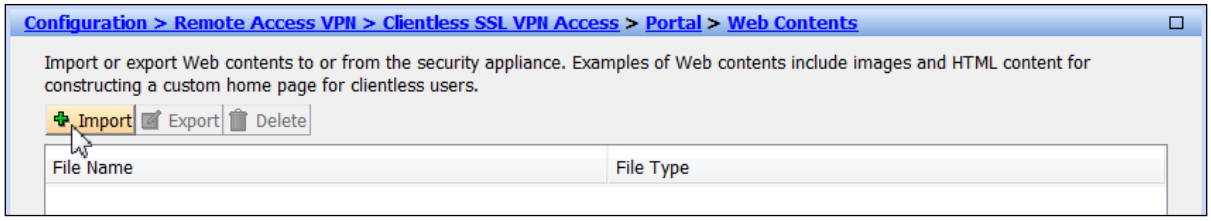
5. Click **Apply** to complete the configuration.

Cisco ASA Risk Based Authentication Configuration

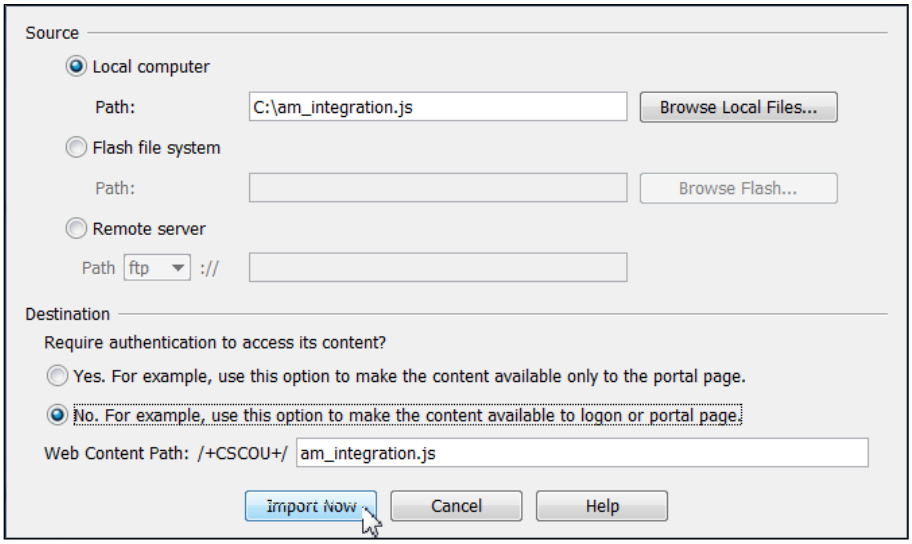
An AA Server Group and Clientless SSL VPN must be configured for SecurID authentication prior to configuring Risk-Based authentication. Refer to the following sections in this guide for information on configuring the AAA Server Group and Clientless SSL VPN for SecurID authentication:

- Configure AAA Server Groups: Server Group for RSA SecurID Authentication
- Integrate Clientless SSL VPN Portal with RSA SecurID Access

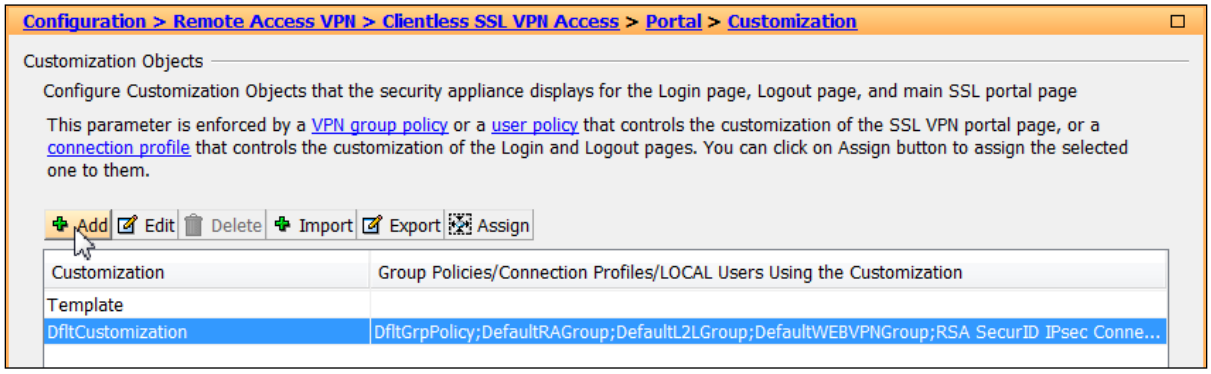
1. Browse to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Portal** > **Web Contents** and click **Import**.



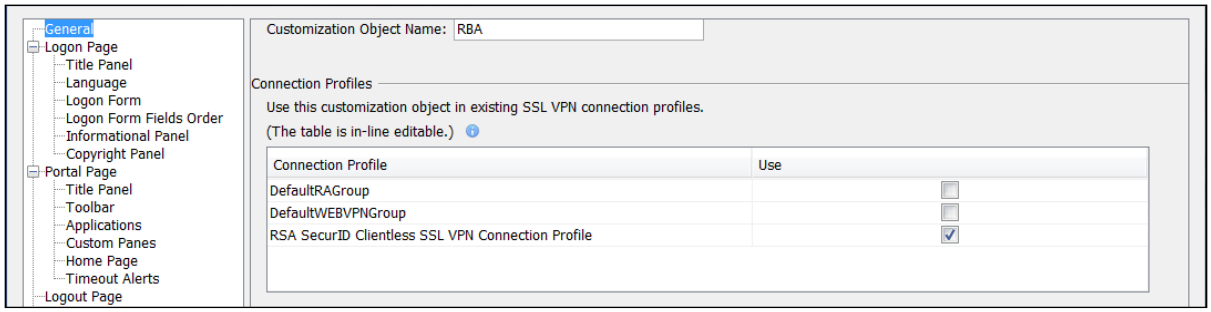
2. **Browse Local Files** to the location of the RBA integration script, for **Require authentication to access its contents** select **No** and click **Import Now**.



3. Browse to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Portal** > **Customization** and click **Add**.

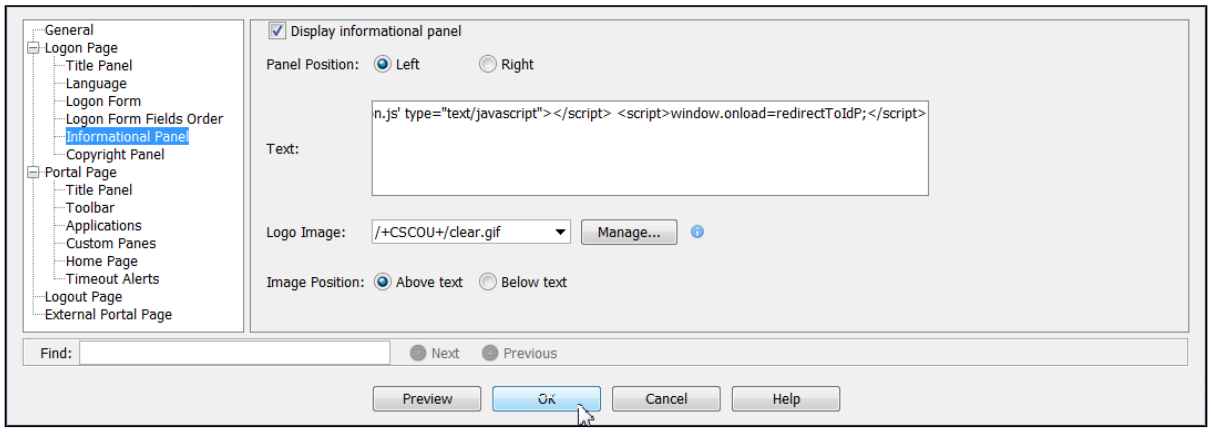


4. Enter a **Customization Object Name** and mark the **Use** checkbox for your **Connection Profile**.

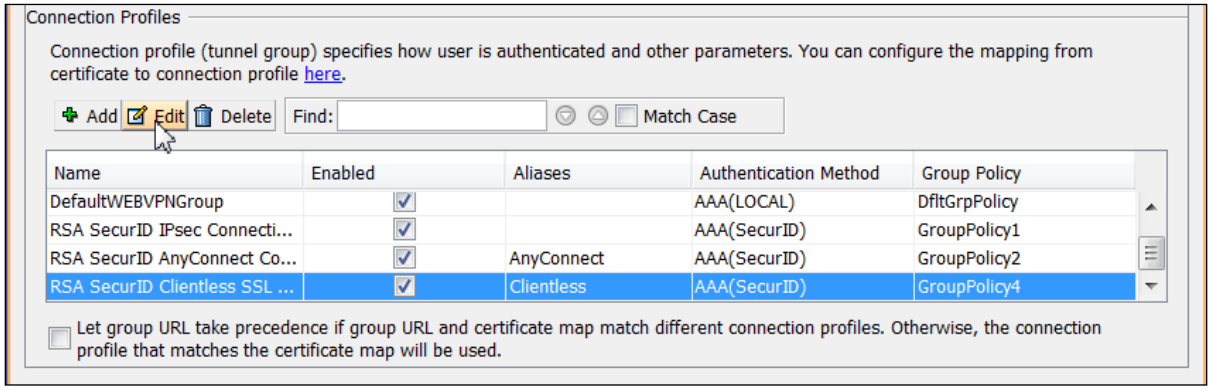


5. From the **Add Customization Object** window browse to **Logon Page** > **Information Panel**. Mark the **Display informational panel** checkbox, and then copy/paste the following line into the **Text:** field and click **OK**.

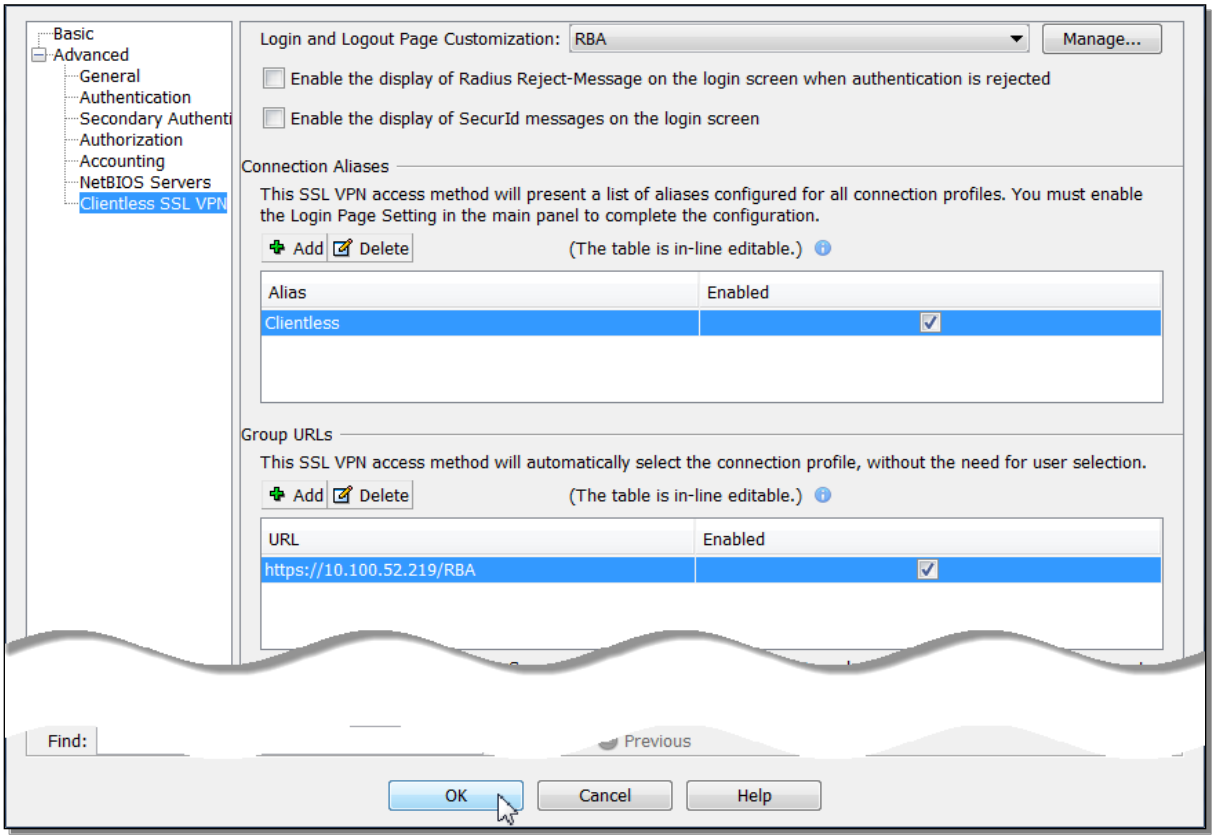
```
<script src='/+CSCOU+/am_integration.js' type="text/javascript"></script>
<script>window.onload=redirectToIdP;</script>
```



6. Browse to **Configuration** > **Remote Access VPN** > **Clientless SSL VPN Access** > **Connection Profiles**, select the connection profile for which you are enabling Risk-Based Authentication and click **Edit**.



7. Expand the **Advanced** menu tree and select **Clientless SSL VPN**. Select the Customization Object you created earlier in this section from the **Login and Logout Page Customization** drop-down menu, enter a **Group URL** to automatically select your connection profile and click **OK**.

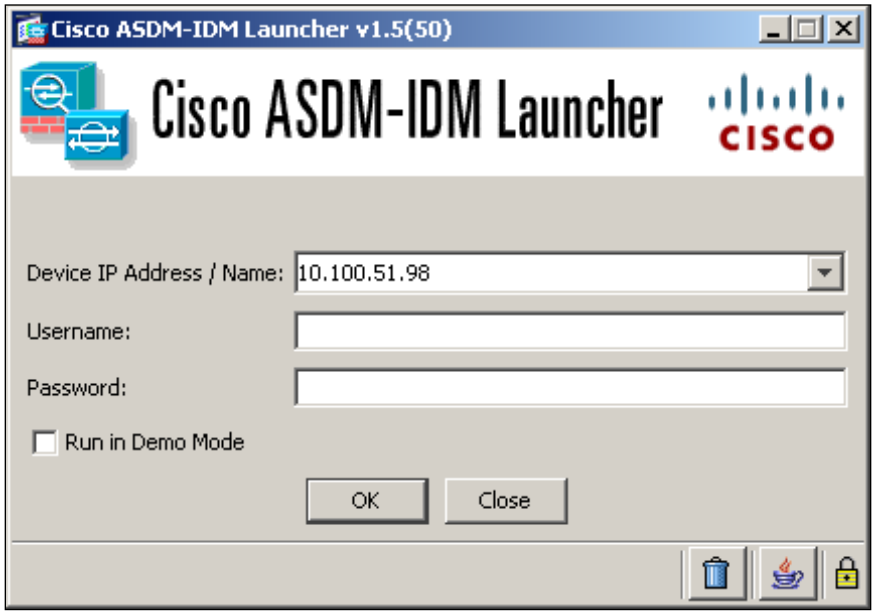


8. Click **Apply** to complete the configuration.

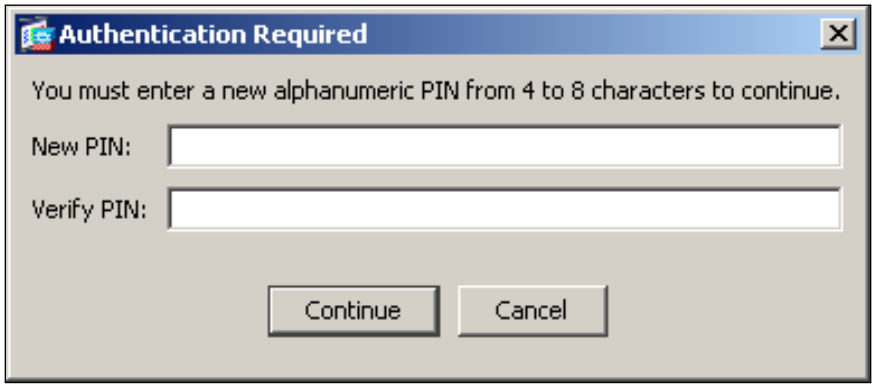
! Important: Depending on which versions of AM and ASA you are integrating, you may get the error "Wrong URL" after RBA logon. See the Known Issues section of this guide for more information and a work-around.

RSA SecurID Login Screens

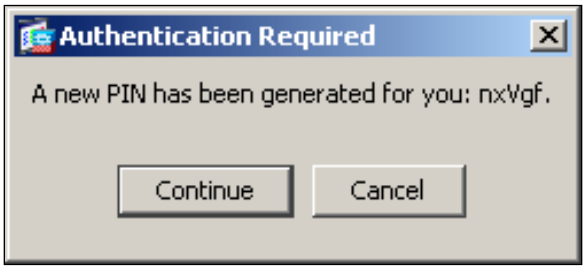
Login screen:



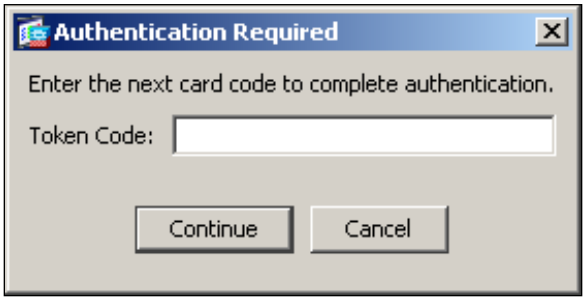
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA SecurID Access

AnyConnect for Windows

Certification Environment Details:

RSA Authentication Manager 8.0, Virtual Appliance

RSA Software Token 5.0 (32bit) Windows 7 Enterprise 64bit

RSA Remote Authentication Client 3.6Windows 7 Enterprise 64bit

Cisco ASA 9.5(2) Proprietary

Cisco AnyConnect 4.2.04.39, Windows 7 Enterprise 64bit

RSA Cloud Authentication Service

Date Tested: April 4th, 2017

Authentication Method	REST Client	RADIUS Client
RSA SecurID	N/A	✓
LDAP Password	N/A	✓
Authenticate Approve	N/A	✓
Authenticate Eyeprint ID	N/A	
Authenticate Fingerprint	N/A	
Authenticate Tokencode	N/A	✓
FIDO Token	N/A	

✓ = Pass ✗ = Fail N/A = Non-Available Function

RSA Authentication Manager

Date Tested: October 20th, 2016

Authentication Method	REST Client	UDP Agent	TCP Agent	RADIUS Client
RSA SecurID	N/A	✓	N/A	✓
RSA SecurID Software Token Automation	N/A	✓	N/A	✓
On Demand Authentication	N/A	✓	N/A	✓
Risk-Based Authentication		N/A		N/A

✓ = Pass ✗ = Fail N/A = Non-Available Function

Certification Checklist for RSA SecurID Access

Clientless SSL VPN Portal

Certification Environment Details:

RSA Authentication Manager 8.2, Virtual Appliance

Cisco ASA 9.5(2), Virtual Appliance

RSA Cloud Authentication Service

Date Tested: April 4th, 2017

Authentication Method	REST Client	RADIUS Client
RSA SecurID	N/A	✓
LDAP Password	N/A	✓
Authenticate Approve	N/A	✓
Authenticate Eyeprint ID	N/A	
Authenticate Fingerprint	N/A	
Authenticate Tokencode	N/A	✓
FIDO Token	N/A	

✓ = Pass ✗ = Fail N/A = Non-Available Function

RSA Authentication Manager

Date Tested: October 13th, 2016

Authentication Method	REST Client	UDP Agent	TCP Agent	RADIUS Client
RSA SecurID	N/A	✓	N/A	✓
RSA SecurID Software Token Automation	N/A	N/A	N/A	N/A
On Demand Authentication	N/A	✓	N/A	✓
Risk-Based Authentication		✓		✓

✓ = Pass ✗ = Fail N/A = Non-Available Function

Certification Checklist for RSA SecurID Access

Firewall

Certification Environment Details:

RSA Authentication Manager 8.2, Virtual Appliance

Cisco ASA 9.5(2), Virtual Appliance

RSA Cloud Authentication Service

Date Tested: April 6th, 2017

Authentication Method	REST Client	RADIUS Client
RSA SecurID	N/A	✓
LDAP Password	N/A	✓
Authenticate Approve	N/A	✓
Authenticate Eyeprint ID	N/A	
Authenticate Fingerprint	N/A	
Authenticate Tokencode	N/A	✓
FIDO Token	N/A	

✓ = Pass ✗ = Fail N/A = Non-Available Function

RSA Authentication Manager

Date Tested: October 13th, 2016

Authentication Method	REST Client	UDP Agent	TCP Agent	RADIUS Client
RSA SecurID	N/A	✓	N/A	✓
RSA SecurID Software Token Automation	N/A	✓	N/A	✓
On Demand Authentication	N/A	✓	N/A	✓
Risk-Based Authentication		N/A		N/A

✓ = Pass ✗ = Fail N/A = Non-Available Function

Certification Checklist for RSA SecurID Access

ASDM

Certification Environment Details:

RSA Authentication Manager 8.2, Virtual Appliance

Cisco ASA 9.5(2) Proprietary

RSA Cloud Authentication Service

Date Tested: April 6th, 2017

Authentication Method	REST Client	RADIUS Client
RSA SecurID	N/A	✓
LDAP Password	N/A	✓
Authenticate Approve	N/A	✓
Authenticate Eyeprint ID	N/A	
Authenticate Fingerprint	N/A	
Authenticate Tokencode	N/A	✓
FIDO Token	N/A	

✓ = Pass ✗ = Fail N/A = Non-Available Function

RSA Authentication Manager

Date Tested: February 5th, 2013

Authentication Method	REST Client	UDP Agent	TCP Agent	RADIUS Client
RSA SecurID	N/A	✓*	N/A	✓
RSA SecurID Software Token Automation	N/A	✓	N/A	✓
On Demand Authentication	N/A	✓	N/A	✓
Risk-Based Authentication		N/A		N/A

✓ = Pass ✗ = Fail N/A = Non-Available Function

*see Known Issues for more information

Known Issues

"Wrong URL." After RBA Logon

Depending on which versions of AM and ASA you are using, you may receive the error "Wrong URL" when you logon with RBA. To work-around the issue, make the following change to the am_integration.js file before uploading it to the Web Contents section in ASA:

Change line #41 of the am_integration.js file from:

origActionURL.setAttribute('value', toAbsolutePath(logonForm.action));

To:

origActionURL.setAttribute('value', 'https://<ASA_HOSTNAME>/%2Bwebvpn%2B/index.html');

Change <ASA_HOSTNAME> to your ASA's IP or hostname.

Potential Replica issue when using Native SecurID Authentication

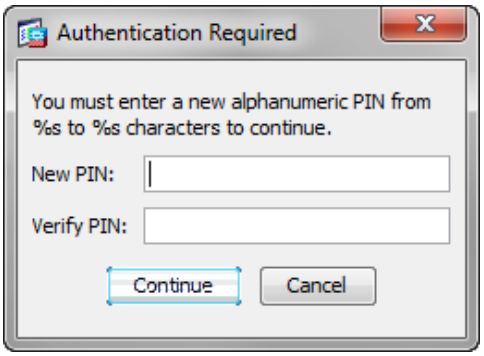
The Cisco ASA 5500 will learn about any RSA Authentication Manager replica servers, and prioritize them at the time of the first authentication. This SDI server list is stored in memory, and lost when the ASA is shut down. If the primary RSA Authentication Manager server is not available for authentication after the system boots, the ASA will not have knowledge of the RSA Authentication Manager replica servers.

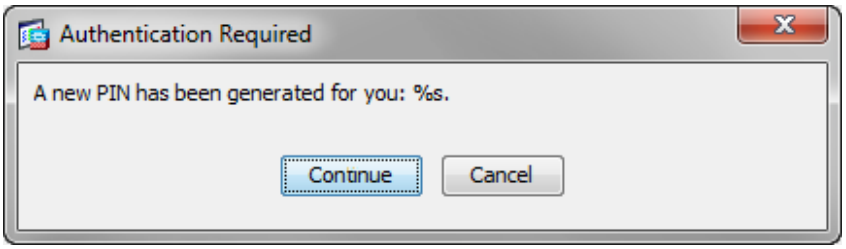
Firewall AAA rule

Although you can configure the ASA to require authentication for network access to any protocol or service, users can authenticate directly with HTTP, HTTPS, Telnet, or FTP only. A user must first authenticate with one of these services before the ASA allows other traffic requiring authentication. Telnet is the only service in which new PIN and Next Tokencode functions are supported.

RSA SecurID Protection of ASDM

ASDM 7.x when configured with SecurID via native SDI variable names for new PIN data are displayed rather than their values. This may cause some difficulty with setting a user-defined PIN, but will make system-generated PINs unusable.





Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	In Memory
sdopts.rec	Not Implemented
Node secret	In Memory
sdstatus.12 / jastatus.12	In Memory
TCP Agent Files	**Location**
rsa_api.properties	N/A
sdconf.rec	N/A
sdopts.rec	N/A
Node secret	N/A

RSA SecurID Integration Details

Partner Integration Details	
RSA SecurID UDP API	Custom build
RSA SecurID TCP API	N/A
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	All Users
Display RSA Server Info	No
Perform Test Authentication	Yes
Agent Tracing	Yes

API Details:

Cisco ASA 5500 implements a modified version of the RSA Authentication API. Important modifications include:

- sdconf.rec not utilized
- sdopts.rec not utilized
- server list stored in memory rather than file system

Refer to Cisco documentation for additional information.

Node Secret:

The Node Secret file is stored in flash memory on the Cisco ASA. The node secret file has its name based on the hexadecimal value of the Authentication Manager server IP address with .sdi appended. (e.g. 10-10-10-2.sdi.) Delete this file to remove the node secret.

sdconf.rec:

Not implemented.

sdopts.rec:

Not implemented.

sdstatus.12:

Not implemented. The SDI Server List can be viewed by entering the following command from the console:

```
# show aaa-server
```

Agent Tracing:

Agent Tracing info can be enabled by entering the following command from the console:

```
# debug sdi
```