



RSA SecurID Ready Implementation Guide

Last Modified: June 30th, 2009

Partner Information

Product Information	
Partner Name	Cisco Systems
Web Site	www.cisco.com
Product Name	ASA 5500 Series Adaptive Security Appliances
Version & Platform	8.2(1)
Product Description	Cisco® ASA 5500 Series adaptive security appliances are purpose-built solutions that combine best-of-breed security and VPN services with the innovative Cisco Adaptive Identification and Mitigation (AIM) architecture. Designed as a key component of the Cisco Self-Defending Network, the Cisco ASA 5500 Series provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity. The result is a powerful multifunction network security appliance family that provides the security breadth and depth for protecting small and medium-sized business and enterprise networks while reducing the overall deployment and operations costs and complexities associated with providing this new level of security.
Product Category	Perimeter Defense (Firewalls, VPNs & Intrusion Detection)





Solution Summary

Cisco ASA 5500 Series Adaptive Security Appliances are purpose-built solutions that integrate world-class firewall, unified communications security, VPN, intrusion prevention (IPS), and content security services in a unified platform. The series builds upon proven technologies from Cisco PIX® 500 Series Security Appliances, Cisco IPS 4200 Series Sensors, and Cisco VPN 3000 Series Concentrators.

Cisco ASA 5500 Series Adaptive Security Appliances are a key component of the Cisco Self-Defending Network. The Cisco ASA 5500 Series provides intelligent threat defense that stops attacks before they penetrate the network perimeter, controls network and application activity, and delivers secure remote access and site-to-site connectivity.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication and RADIUS
List Library Version Used	5.02
RSA Authentication Manager Replica Support *	Full Replica Support
Secondary RADIUS Server Support	Yes (2)
RSA Authentication Agent Host Type for 6.1	Communication Server
RSA Authentication Agent Host Type for 7.1	Standard Agent
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	Yes
RSA Software Token and RSA SecurID 800 Automation	Yes

Product Requirements

Partner Product Requirements: Cisco ASA 5500	
Firmware Versions	8.2(1)

Additional Software Requirements	
Application	Additional Versions/Patches
Cisco VPN Client	5.0.05.0290
RSA Software Token	4.0.242
RSA Smart Card Middleware	3.0 (install available via RSA Software Token 4.0.242)



Agent Host Configuration

!> Important: “Agent Host” and “Authentication Agent” are synonymous. “Agent Host” is a term used with the RSA Authentication Manager 6.x servers and below. RSA Authentication Manager 7.1 uses the term “Authentication Agent”.

!> Important: All “Authentication Agent” types for 7.1 should be set to “Standard Agent”.

To facilitate communication between the Cisco ASA 5500 and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database and RADIUS Server database if using RADIUS. The Agent Host record identifies the Cisco ASA 5500 within its database and contains information about communication and encryption.

To create the Agent Host record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces

When adding the Agent Host Record, you should configure the Cisco ASA 5500 as a Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with the Cisco ASA 5500 will occur.

To create the RADIUS client record, you will need the following information.

- Hostname
- IP Addresses for all network interfaces
- RADIUS Secret

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA Security documentation for additional information about Creating, Modifying and Managing Agent Host records.

RSA SecurID files

RSA SecurID Authentication Files	
Files	Location
sdconf.rec	None stored
Node Secret	In Memory
sdstatus.12	In Memory
sdopts.rec	“Not implemented”

Note: Go to the appendix of this document to get detailed information regarding these files.



Partner Authentication Agent Configuration

Before You Begin

This section provides instructions for integrating the partners' product with RSA SecurID Authentication. 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 vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Overview

This guide provides configuration information for RSA SecurID Authentication to challenge users in a Cisco ASA environment. The Cisco ASA, Cisco IPSec VPN Client, SSL VPN, Firewall, and ASDM configurations all have independent sections below. The guide is organized as follows:

- **Configuring SecurID Authentication**
 - **Authentication via RSA Native SecurID Protocol**

This section documents configuration steps necessary for RSA SecurID Authentication via RSA's NATIVE protocol when utilizing Cisco ASA 5500 Series Adaptive Security Appliances.
 - **Authentication via RADIUS Protocol**

This section documents configuration steps necessary for RSA SecurID Authentication via the RADIUS protocol when utilizing Cisco ASA 5500 Series Adaptive Security Appliances.
- **IPSec VPN Configuration**

This section documents configuration steps necessary for RSA SecurID Authentication when utilizing Cisco's IPSec VPN Client solution with Cisco ASA 5500 Series Adaptive Security Appliances.

 - Configuring IP Address Pools
 - Configuring IKE Policies
 - Configuring IPSec Connection Policies
- **SSL VPN Configuration**

This section documents configuration steps necessary for RSA SecurID Authentication when utilizing Cisco's SSL VPN solution with Cisco ASA 5500 Series Adaptive Security Appliances.

 - Configuring SSL VPN Connection Policies
- **Firewall Configuration**

This section documents configuration steps necessary for RSA SecurID Authentication when utilizing Cisco's Firewall solution with Cisco ASA 5500 Series Adaptive Security Appliances.

 - Building a Firewall rule that will allow for services to be protected by RSA SecurID Authentication.
- **ASDM – One Time Password Support for ASDM Authentication**

This section documents configuration steps necessary for RSA SecurID Authentication when utilizing Cisco's ASDM management solution with Cisco ASA 5500 Series Adaptive Security Appliances.

 **Note: Configuration via NATIVE RSA and/or RADIUS authentication is required prior to configuring VPN, Firewall, or ASDM components.**



Configuring SecurID Authentication

The ASA 5500 Series Adaptive Security Appliances can authenticate to an RSA Authentication Manager in two ways. One way is via the Native RSA SecurID Authentication Protocol and the other is via RADIUS. The ASA also has three areas where RSA SecurID Authentication can be enabled. They are IPSEC VPN, Web SSL VPN and Firewall. Start the Cisco ASDM manager and go to the appropriate configuration section below for your needs.



Note: Click Apply after your configuration changes when appropriate.

Authentication via RSA Native SecurID Protocol

1. Select **Configuration** from the top menu and then select **AAA/Local Users** from the Features Menu on the left.
2. Select **AAA Server Groups**.
3. Click **Add** located on the right side.

The screenshot shows the Cisco ASDM configuration interface. The left sidebar displays the configuration tree with 'Remote Access VPN' selected. The main window shows the 'AAA Server Groups' configuration page. The table below lists the configured server groups.

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
ACS_EXPRESS	RADIUS	Single	Depletion	10	3
AM6_1_idm	SDI		Depletion	10	3
Access_Manager	HTTP Form		Depletion	10	5
Authenticating	SDI		Depletion	10	3
Authn71	SDI		Depletion	10	3
Ash_AA_Gesinger	HTTP Form		Depletion	10	3
CISCO_ACS_APP	RADIUS	Single	Depletion	10	3
CISCO_ACS_RADIUS	RADIUS	Single	Depletion	10	3
GesingerGregD	HTTP Form		Depletion	10	5
HTTP_FORM_GROUP	HTTP Form		Depletion	10	3
LOCAL	LOCAL				
NH_AM_71	SDI		Depletion	10	3
RADIUS_A_1	RADIUS	Single	Depletion	10	3
RADIUS_A_1	RADIUS	Single	Depletion	10	3
Steel_belted	RADIUS	Single	Depletion	10	3

Below the table, the 'Servers in the Selected Group' section shows a single entry:

Server Name or IP Address	Interface	Timeout
10.100.50.25	inside	10



Add AAA Server Group

Server Group: AuthMan61

Protocol: SDI

Reactivation Mode: RADIUS, TACACS+, NT Domain, SDI, Kerberos, LDAP, HTTP Form

Dead Time: 10

Max Failed Attempts:

OK Cancel Help

4. **Server Group:** Enter name for server group.
5. **Protocol:** Select SDI.

 **Note:** Cisco refers to RSA SecurID authentication as “SDI”.

6. Click **OK**.
7. Click **Add** on the bottom right pane.
8. Select **Interface Name**:
9. Enter **Server Name or IP Address**:
10. **SDI Parameters** are defaults and do NOT need to be changed. (optional)

Edit AAA Server

Server Group: AuthMan61

Interface Name: inside

Server Name or IP Address:

Timeout: 10 seconds

SDI Parameters

Server Port: 5500

Retry Interval: 10 seconds

OK Cancel Help



Authentication via RADIUS Protocol

1. Select **Configuration** from the top menu and then select **AAA/Local Users** from the Features Menu on the left.
2. Select **AAA Server Groups**.

The screenshot shows the Cisco configuration interface for Remote Access VPN. The left sidebar shows the navigation tree with 'AAA Server Groups' selected. The main area displays a table of AAA Server Groups and a section for servers in the selected group.

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
ACS_EXPRESS	RADIUS	Single	Depletion	10	3
APB_L_Spl	SDI		Depletion	10	3
Access_Manager	HTTP Form		Depletion	10	5
AuthMan01	SDI		Depletion	10	5
AuthMan71	SDI		Depletion	10	5
Auth_AA_Gesinger	HTTP Form		Depletion	10	3
CISCO_ACS_APP	RADIUS	Single	Depletion	10	3
CISCO_ACS_RADIUS	RADIUS	Single	Depletion	10	3
GesingerGrepD	HTTP Form		Depletion	10	5
HTTP_FORM_GROUP	HTTP Form		Depletion	10	3
LOCAL	LOCAL		Depletion	10	3
WPA_Auth_71	SDI		Depletion	10	3
RADIUS_6_1	RADIUS	Single	Depletion	10	3
RADIUS_7_1	RADIUS	Single	Depletion	10	3
Steel_belted	RADIUS	Single	Depletion	10	3

Server Name or IP Address	Interface	Timeout
10.100.50.25	inside	10
10.100.50.36	inside	10
10.100.50.37	inside	10

3. Click **Add** located on the right side.

The 'Add AAA Server Group' dialog box contains the following fields and options:

- Server Group:
- Protocol:
- Accounting Mode:
- Reactivation Mode:
- Dead Time:
- Max Failed Attempts:
- Enable interim accounting update
- VPN3K Compatibility Option:

Buttons: OK, Cancel, Help



4. Name the **Server Group**:
5. Select **Interface Name**:
6. Select **AAA Setup – AAA Servers**.
7. Enter **Server Name** or **IP Address**:
8. **Server Ports** and **Retry Intervals** are defaults and do NOT need to be changed. (optional)
9. Enter **Server Secret Key**.

Add AAA Server

Server Group: RADIUS_6.1

Interface Name: outside

Server Name or IP Address:

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645

Server Accounting Port: 1646

Retry Interval: 10 seconds

Server Secret Key:

Common Password:

ACL Netmask Convert: Standard


Microsoft CHAPv2 Capable:

SDI Messages

Message Table

OK Cancel Help

10. Click **OK**.

 **Note:** The **Server Secret Key** needs to match the **Shared Secret Key** created in the **RADIUS** server.



IPSec VPN Configuration

IP Address Pools

1. Select **Configuration** from the top menu and then select **Remote Access VPN** from the Features Menu on the left.
2. Select **Address Management, Address Pools**.
3. Enter **Name**: of address pool.
4. Enter **Starting** and **Ending** IP addresses.
5. Select appropriate **Subnet Mask**.

The screenshot shows the Cisco configuration interface for Remote Access VPN. The left sidebar shows the navigation tree with 'Address Pools' selected under 'Address Assignment'. The main content area displays a table of existing IP address pools:

Pool Name	Starting Address	Ending Address/Number of Addresses	Subnet Mask/Prefix Length
ScottPool2	192.168.78.240	192.168.78.245	255.255.255.0
ScottPool	10.100.48.200	10.100.48.210	255.255.248.0

An 'Add IP Pool' dialog box is open, showing the following configuration:

- Name: VPN_IP_ADDR_POOL
- Starting IP Address: 192.168.1.1
- Ending IP Address: 192.168.1.100
- Subnet Mask: 255.255.255.0

Buttons for OK, Cancel, and Help are visible at the bottom of the dialog box.

6. Click **OK**.



IKE Policies

1. Select **Configuration** from the top menu and then select **Network (Client) Access, IPSec, IKE Policies**.
2. Click **Add** from the right pane.
3. Create your IKE Policy with **pre-shared** selected for Authentication and the appropriate settings for the other parameters. (defaults are pre-configured)

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > IKE Policies

Configure specific Internet Key Exchange (IKE) algorithms and parameters, within the IPsec Internet Security Association Key Management Protocol (ISAKMP) framework, for the AH and ESP IPsec protocols.

Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime (seconds)
20	3des	md5		2 rsa-sig	86400
10	3des	sha		2 rsa-sig	86400
65,535	3des	sha		2 pre-share	86400
50	3des	md5		2 pre-share	86400

Edit IKE Policy

Priority: 55535 Authentication: pre-share

Encryption: 3des D-H Group: 2

Hash: sha Lifetime: Unlimited 86400 seconds

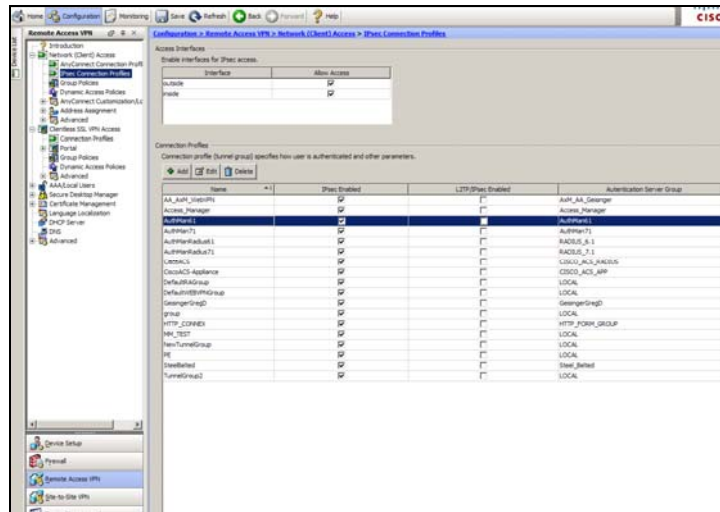
OK Cancel Help

4. Click **OK**.

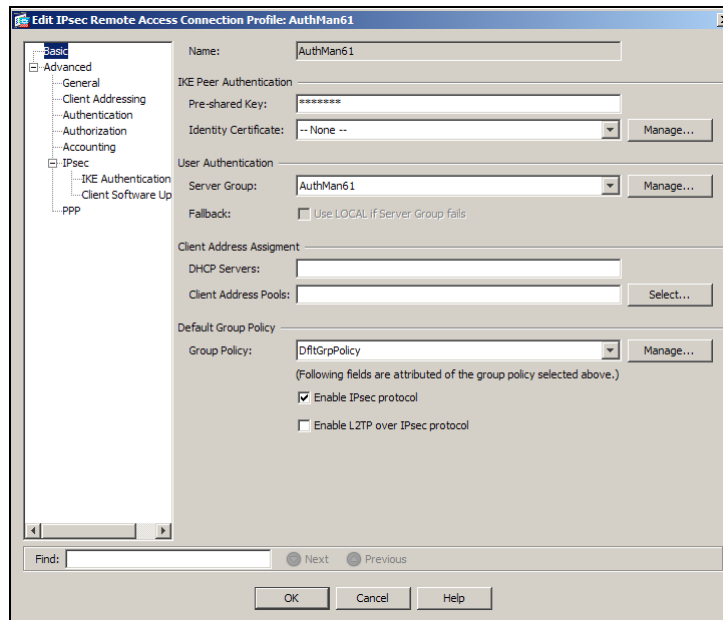


IPsec Connection Profiles

1. Select the **Configuration** tab on the top menu.
2. Select **Network (Client) Access**.
3. Click on **IPsec Connection Profiles**.
4. Click **Add** from the right pane.



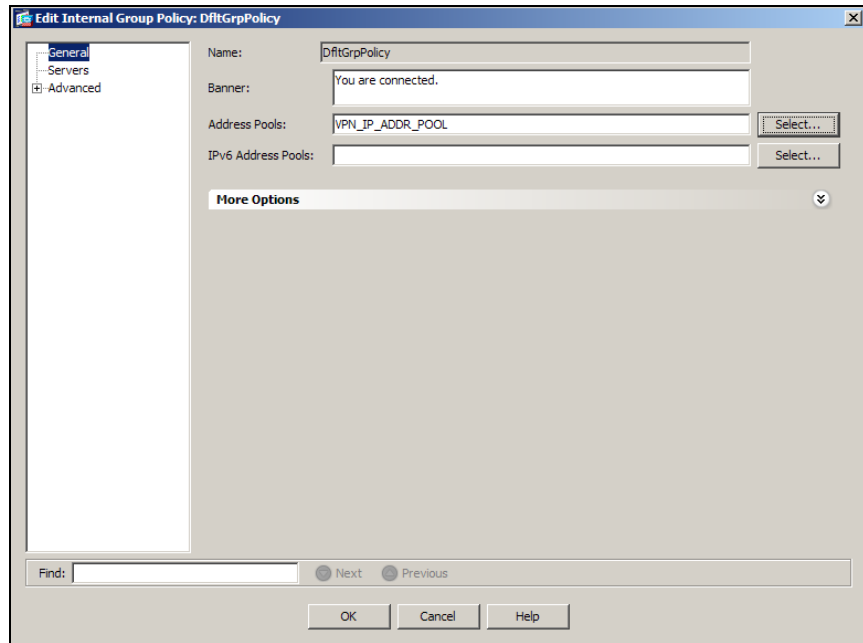
5. Select **Basic**.
6. Enter **Name**:
7. Enter **Pre-Shared Key**:
8. Configure **Server Group**:
9. Configure **Group Policy** under **Default Group Policy**.
10. Check **Enable IPsec protocol**.



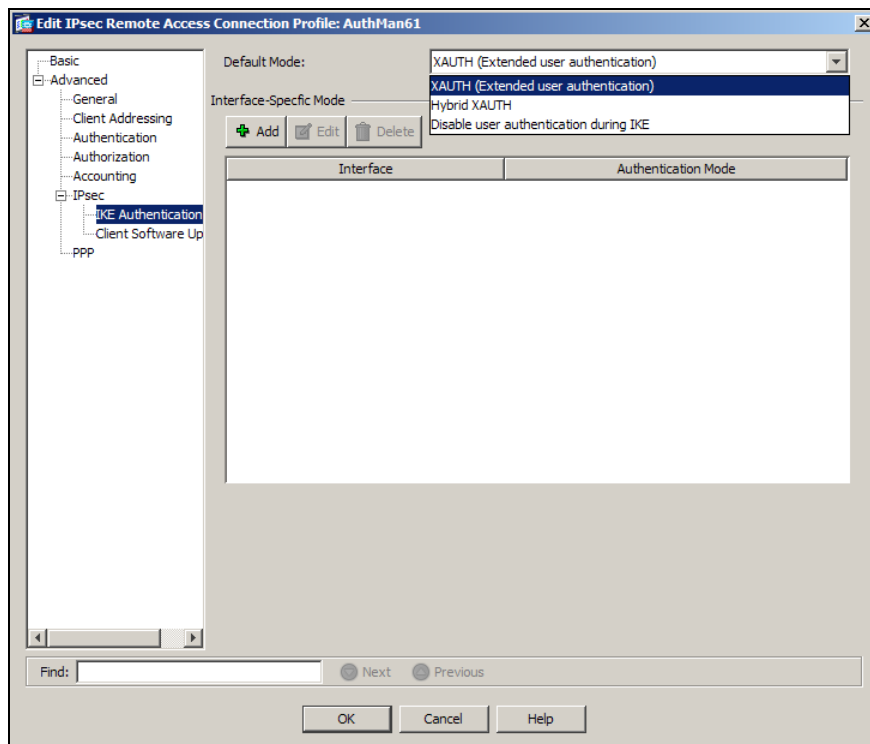
11. Do NOT Click **OK**.
12. Click **Manage** to manage Group Policy:



13. Edit the **Group Policy**, select **General** from the left pane.
14. Click **Select** to configure desired **Address Pool(s)**:



15. Click **OK** twice.
16. Select **Advanced**, **IPsec**, **IKE Authentication** from **Advanced** menu on the left pane.
17. Select **XAUTH (Extended user authentication)** from the **Default Mode:** pull down menu.



18. Click **OK**.



SSL VPN Configuration

SSL VPN Connection Policies

1. Select **Configuration** from the top menu and then select **Remote Access VPN** from the Features Menu on the bottom left.
2. Expand Clientless SSL VPN Access.
3. Select **Connection Profiles**.
4. Click **Add** from the right had pane.

The screenshot shows the Cisco configuration interface for Remote Access VPN. The left sidebar shows the navigation tree with 'Remote Access VPN' selected. The main content area is titled 'Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles'. It includes sections for 'Access Interfaces', 'Login Page Setting', and 'Connection Profiles'. The 'Access Interfaces' section shows a table with columns 'Interface' and 'Allow Access', listing 'outside' and 'inside' both checked. The 'Login Page Setting' section has two checkboxes: 'Allow user to select connection profile...' (checked) and 'Allow user to enter internal password...' (unchecked). The 'Connection Profiles' section contains a table with columns: Name, Enabled, Aliases, Authentication Method, and DNS Servers.

Name	Enabled	Aliases	Authentication Method	DNS Servers
AA_AxM_WebVPN	<input checked="" type="checkbox"/>	AA_AxM_WebVPN	AAA(AxM_AA_Geisinger)	10.100.50.12
Access_Manager	<input checked="" type="checkbox"/>	Access_Manager	AAA(Access_Manager)	10.100.50.12
AuthMan61	<input checked="" type="checkbox"/>	61_NATIVE	AAA(AuthMan61)	10.100.50.12
AuthMan71	<input checked="" type="checkbox"/>	71_NATIVE	AAA(AuthMan71)	10.100.50.12
AuthManRadius61	<input checked="" type="checkbox"/>	61_RADIUS	AAA(RADIUS_6.1)	10.100.50.12
AuthManRadius71	<input checked="" type="checkbox"/>	71_RADIUS	AAA(RADIUS_7.1)	10.100.50.12
CiscoACS	<input checked="" type="checkbox"/>		AAA(CISCO_ACS_RADIUS)	10.100.50.12
CiscoACS-Appliance	<input checked="" type="checkbox"/>		AAA(CISCO_ACS_APP)	10.100.50.12
DefaultRAGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)	10.100.50.12
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>	LOCAL	AAA(LOCAL)	10.100.50.12
GeisingerGregD	<input checked="" type="checkbox"/>	GeisingerGregD	AAA(GeisingerGregD)	10.100.50.12
group	<input checked="" type="checkbox"/>		AAA(LOCAL)	10.100.50.12
HTTP_CONNEX	<input checked="" type="checkbox"/>	HTTP_Form	AAA(HTTP_FORM_GROUP)	10.100.50.12
MM_TEST	<input checked="" type="checkbox"/>	MM_TEST	AAA(LOCAL)	10.100.50.12
NewTunnelGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)	10.100.50.12
PE	<input checked="" type="checkbox"/>		AAA(LOCAL)	10.100.50.12
SteelBelted	<input checked="" type="checkbox"/>		AAA(SteelBelted)	10.100.50.12
TunnelGroup2	<input checked="" type="checkbox"/>		AAA(LOCAL)	10.100.50.12

5. Select **Basic** from the left pane.
6. Enter an **Aliases:** name. (an Alias name is required)
7. Select **AAA Server Group** created in fist configuration section of this document.
8. Enter and configure **DNS**.
9. Select the appropriate **Group Policy**:
10. Check **Enable clientless SSL VPN Protocol**.

Edit Clientless SSL VPN Connection Profile: AuthMan61

Basic
Advanced

Name: AuthMan61

Aliases: 61_NATIVE

Authentication

Method: AAA Certificate Both

AAA Server Group: AuthMan61 Manage...

Use LOCAL if Server Group fails

DNS

Server Group: DefaultDNS Manage...

(Following fields are attributes of the DNS server group selected above.)

Servers: 10.100.50.12

Domain Name: pe.rsa.net

Default Group Policy

Group Policy: DfftGrpPolicy Manage...

(Following field is an attribute of the group policy selected above.)

Enable clientless SSL VPN protocol

Find: Next Previous

OK Cancel Help

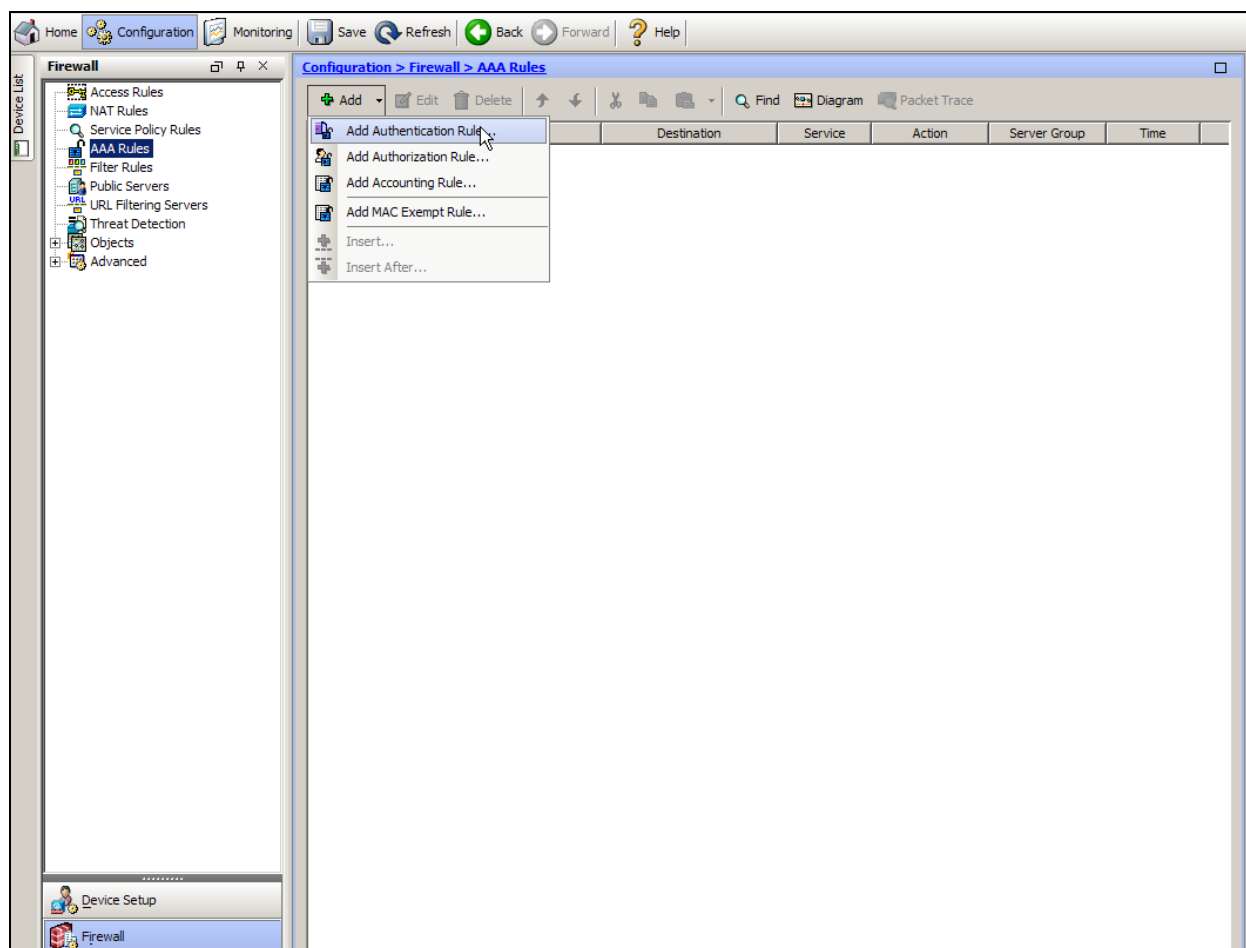
11. Click **OK**.



Firewall Configuration

Building a Firewall rule

1. Select **Configuration** from the top menu and then select **Firewall** from the left bottom left pane.
2. Select **AAA Rules** from the left Pane.
3. Click **Add**, **Add Authentication Rule**.



4. Click **OK**.



5. Click **Edit** or double click on the rule just created.
6. Select the appropriate **AAA Server Group**.

Edit Authentication Rule

Interface: outside

Action: Authenticate Do not Authenticate

AAA Server Group: AuthMan71

Source: AM6.1_jdm

Destination: AuthMan71

Service: CISCO_ACS_APP

Description: MM_AM_71

More Options

7. Select the appropriate **Source, Destination, Service**:

Edit Authentication Rule

Interface: outside

Action: Authenticate Do not Authenticate

AAA Server Group: AuthMan61

Source: any

Destination: any

Service: tcp/telnet

Description:

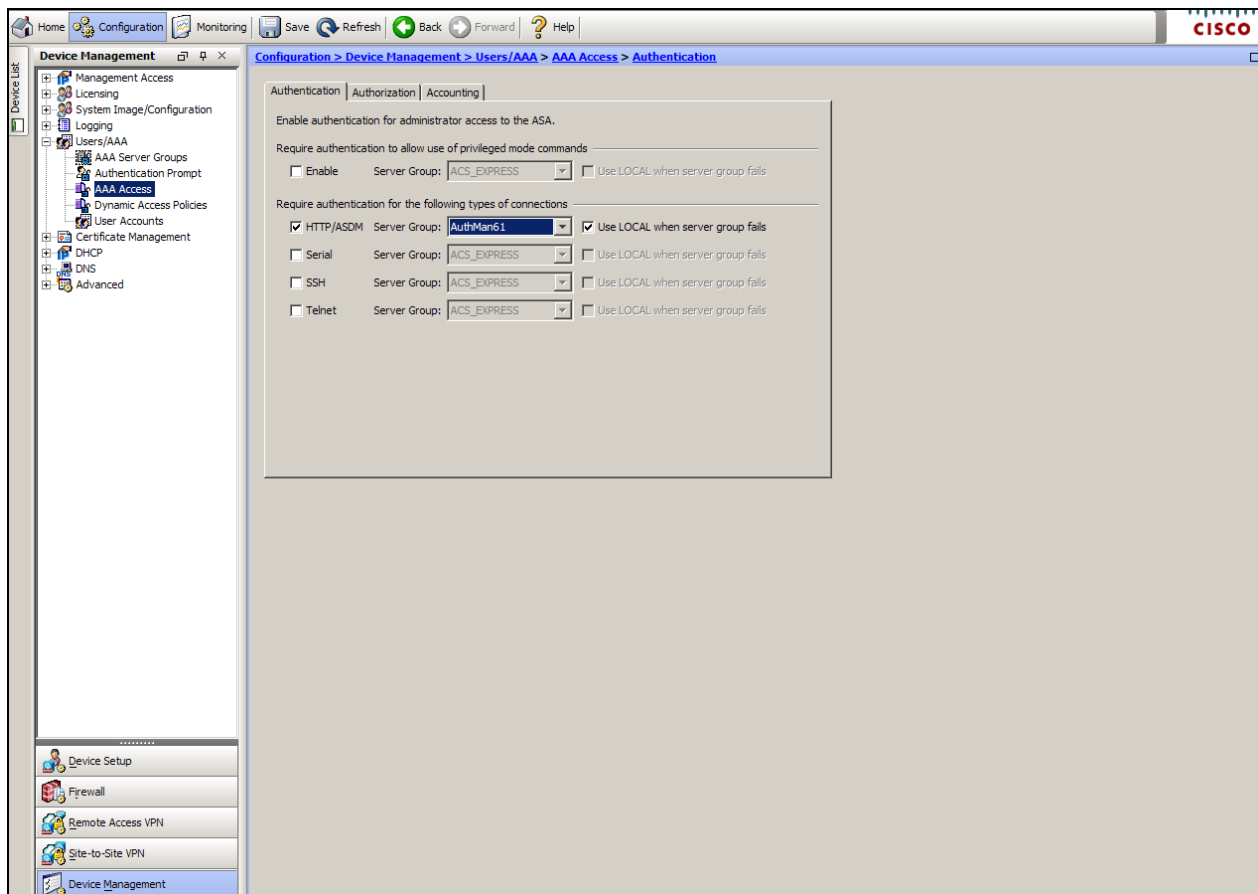
More Options

8. Click **OK**

ASDM – One Time password support for ASDM authentication

ASDM now supports administrator authentication using one time passwords (OTPs) supported by RSA SecurID (SDI). This feature addresses security concerns surrounding administrators authenticating with static passwords.

1. Select **Configuration** from the top menu.
2. Select **Device Management** from the bottom left.
3. Expand **Users/AAA** from the left pane.
4. Select **AAA Access**.
5. On the **Authentication** tab, check **HTTP/ASDM**.
6. Select the appropriate **Server Group**:
7. Check **Use LOCAL when server group fails**.



8. Click **OK**.

! **Important:** Refer to the Cisco Administration documentation to ensure uninterrupted management access to the Cisco ASA device. Changing the authentication method for administration access could temporarily eliminate access to the ASA device. It is highly recommended that a complete backup of the ASA configuration be saved prior to changing the ASDM authentication method.



ASDM Login Prompts

The screenshot shows the Cisco ASDM-IDS Launcher v1.5(41) dialog box. It features the Cisco logo and the text "Cisco ASDM-IDS Launcher". The fields are as follows:

- Device IP Address / Name: 1.2.3.4
- Username: cyork
- Password: (empty)
- Run in Demo Mode

Buttons for "OK" and "Close" are at the bottom. There are also icons for trash, a coffee cup, and a lock.

User Selectable

The screenshot shows the "Authentication Required" dialog box with the following text and options:

You must create a new PIN. Select whether you want to create your own PIN or have the system generate one for you.

- Have the system generate a new pin
- Create your own new PIN

Buttons for "Continue" and "Cancel" are at the bottom.

System Generated

The screenshot shows the "Authentication Required" dialog box with the following text and options:

A new PIN has been generated for you: ofg6.

Buttons for "Continue" and "Cancel" are at the bottom.



Next Token Code Mode

Authentication Required [X]

Enter the next card code to complete authentication.

Token Code:

New PIN via RADIUS

Authentication Required [X]

A new PIN is required.
Do you want system to generate your new PIN? (y/n):

Response:

New PIN accepted

Authentication Required [X]

PIN Accepted.
Wait for the token code to change,
then enter the new passcode:

Response:

Certification Checklist: IPSEC VPN – Authentication Manager 6.1

Date Tested: June 30th, 2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1.2	Windows 2003 SP2
Cisco ASA 5500	8.2 (1)	IOS
Cisco VPN Client	5.0.05.0290	Windows XP SP2

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
PASSCODE			
16 Digit PASSCODE	<input checked="" type="checkbox"/>	16 Digit PASSCODE	<input checked="" type="checkbox"/>
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>

Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>	User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input checked="" type="checkbox"/>
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
RSA SecurID 800 Token Automation			
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>	User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input checked="" type="checkbox"/>
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>

CMY

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

Certification Checklist: IPSEC VPN – Authentication Manager 7.1

Date Tested: June 30th, 2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1.2	Windows 2003 SP2
Cisco ASA 5500	8.2 (1)	IOS
Cisco VPN Client	5.0.05.0290	Windows XP SP2
RSA Software Token	4.0	Windows XP SP2

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input checked="" type="checkbox"/>
PIN Reuse	<input checked="" type="checkbox"/>	PIN Reuse	<input checked="" type="checkbox"/>
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Fixed Passcode	<input checked="" type="checkbox"/>	4 Digit Fixed Passcode	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>	User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
RSA SecurID 800 Token Automation			
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>	User Defined (8 Digit Numeric)	<input checked="" type="checkbox"/>
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>

CMY

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

Certification Checklist: SSL VPN – Authentication Manager 6.1

Date Tested: June 30th, 2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1 (295)	Windows 2003 SP2
Cisco ASA 5500	8.2 (1)	IOS

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
PASSCODE			
16 Digit PASSCODE	<input checked="" type="checkbox"/>	16 Digit PASSCODE	<input checked="" type="checkbox"/>
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input type="checkbox"/> N/A
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

CMY

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

Certification Checklist: SSL VPN – Authentication Manager 7.1

Date Tested: June 30th, 2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1.2	Windows 2003 SP2
Cisco ASA 5500	8.2 (1)	IOS

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input checked="" type="checkbox"/>
PIN Reuse	<input checked="" type="checkbox"/>	PIN Reuse	<input checked="" type="checkbox"/>
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Fixed Passcode	<input checked="" type="checkbox"/>	4 Digit Fixed Passcode	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

CMY

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

Certification Checklist: Firewall – Authentication Manager 6.1

Date Tested: June 30th, 2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1 (295)	Windows 2003 SP2
Cisco ASA 5500	8.2 (1)	IOS

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
PASSCODE			
16 Digit PASSCODE	<input checked="" type="checkbox"/>	16 Digit PASSCODE	<input checked="" type="checkbox"/>
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

CMY

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

Certification Checklist: Firewall – Authentication Manager 7.1

Date Tested: June 30th, 2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows 2003 SP2
Cisco ASA 5500	8.03	IOS

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input checked="" type="checkbox"/>
PIN Reuse	<input checked="" type="checkbox"/>	PIN Reuse	<input checked="" type="checkbox"/>
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Fixed Passcode	<input checked="" type="checkbox"/>	4 Digit Fixed Passcode	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

CMY

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

Certification Checklist: ASDM – Authentication Manager 6.1

Date Tested: June 30th, 2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	6.1.2	Windows 2003 SP2
Cisco ASA 5500	8.2 (1)	IOS
ASDM	1.5(41)	Windows XP SP2

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
User Selectable	<input checked="" type="checkbox"/>	User Selectable	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
PASSCODE			
16 Digit PASSCODE	<input checked="" type="checkbox"/>	16 Digit PASSCODE	<input checked="" type="checkbox"/>
4 Digit Password	<input checked="" type="checkbox"/>	4 Digit Password	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
Name Locking Enabled	<input checked="" type="checkbox"/>	Name Locking Enabled	<input type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
User Selectable	<input type="checkbox"/> N/A	User Selectable	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A

CMY

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

Certification Checklist: ASDM – Authentication Manager 7.1

Date Tested: June 30th, 2009

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	7.1	Windows 2003 SP2
Cisco ASA 5500	8.03	IOS
ASDM	1.5(41)	Windows XP SP2

Mandatory Functionality			
RSA Native Protocol		RADIUS Protocol	
New PIN Mode			
Force Authentication After New PIN	<input checked="" type="checkbox"/>	Force Authentication After New PIN	<input checked="" type="checkbox"/>
System Generated PIN	<input checked="" type="checkbox"/>	System Generated PIN	<input checked="" type="checkbox"/>
User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>	User Defined (4-8 Alphanumeric)	<input checked="" type="checkbox"/>
User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>	User Defined (5-7 Numeric)	<input checked="" type="checkbox"/>
Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>	Deny 4 and 8 Digit PIN	<input checked="" type="checkbox"/>
Deny Alphanumeric PIN	<input checked="" type="checkbox"/>	Deny Alphanumeric PIN	<input checked="" type="checkbox"/>
Deny Numeric PIN	<input checked="" type="checkbox"/>	Deny Numeric PIN	<input checked="" type="checkbox"/>
PIN Reuse	<input checked="" type="checkbox"/>	PIN Reuse	<input checked="" type="checkbox"/>
Passcode			
16 Digit Passcode	<input checked="" type="checkbox"/>	16 Digit Passcode	<input checked="" type="checkbox"/>
4 Digit Fixed Passcode	<input checked="" type="checkbox"/>	4 Digit Fixed Passcode	<input checked="" type="checkbox"/>
Next Tokencode Mode			
Next Tokencode Mode	<input checked="" type="checkbox"/>	Next Tokencode Mode	<input checked="" type="checkbox"/>
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	<input checked="" type="checkbox"/>	Failover	<input checked="" type="checkbox"/>
No RSA Authentication Manager	<input checked="" type="checkbox"/>	No RSA Authentication Manager	<input checked="" type="checkbox"/>
Additional Functionality			
RSA Software Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A
RSA SecurID 800 Token Automation			
System Generated PIN	<input type="checkbox"/> N/A	System Generated PIN	<input type="checkbox"/> N/A
User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A	User Defined (8 Digit Numeric)	<input type="checkbox"/> N/A
Next Tokencode Mode	<input type="checkbox"/> N/A	Next Tokencode Mode	<input type="checkbox"/> N/A


CMY

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



Known Issues

1. **Firewall authentication:** New-PIN and Next-Tokencode does not work via FTP or HTTP. Virtual telnet needs to be configured to enable this functionality. See the Cisco documentation on how to enable this feature.

 **Note:** This issue has been resolved as of version 5.0.04 of the Cisco VPN Client. Refer to Cisco bugs CSCsl66524, CSCsj23555 and CSCsl22039

Appendix

SecurID server Files

Node Secret: The Node Secret file is stored in flash on the Cisco ASA. To see this file run *show flash*. The Node Secret file will be named with the IP Address of the Primary RSA Authentication Server with a .sdi extension. Example 10-10-10-2.sdi. Delete this file to remove the node secret.

sdconf.rec: Not implemented. You configure the RSA Authentication Managers manually.

sdopts.rec: Not implemented

sdstatus.12: Not implemented: You can see the server list by running “*show aaa-server*”

VPN Client information

! Important: If you are configuring the ASA Server to use IPsec you will also need to configure the Cisco VPN client. Information on how to configure the Cisco VPN client can be found in the Cisco VPN client implementation guide located at http://www.rsa.com/rsasecured/guides/imp_pdfs/Cisco_VPN_Client_AuthMan7.1.pdf
