# Table of Contents

Solution Summary .................................................................................................................. 4  
Use Cases ............................................................................................................................... 4  
Integration Types .................................................................................................................. 4  
Supported Features .............................................................................................................. 5  
  Cisco ASA integration with RSA Cloud Authentication Service ....................................... 5  
  Cisco ASA integration with RSA Authentication Manager .............................................. 5  
Configuration Summary ....................................................................................................... 6  
  Integration Configuration ................................................................................................... 6  
  Use Case Configuration .................................................................................................... 6  
Certification Details ............................................................................................................. 6  
Known Issues ........................................................................................................................ 6  
Integration Configuration ..................................................................................................... 8  
  Authentication Agent ...................................................................................................... 8  
    RSA Authentication Manager ......................................................................................... 8  
    Cisco ASA .................................................................................................................... 8  
    SecurID Agent Integration Details ................................................................................ 11  
  RADIUS with AM ............................................................................................................. 12  
    RSA Authentication Manager ......................................................................................... 12  
    Cisco ASA ................................................................................................................... 12  
  RADIUS with CAS .......................................................................................................... 16  
    RSA Cloud Authentication Service ................................................................................ 16  
    Cisco ASA ................................................................................................................... 16  
  Risk-Based Authentication ............................................................................................... 20  
    RSA Authentication Manager ......................................................................................... 20  
    Cisco ASA ................................................................................................................... 21  
  SSO Agent - SAML ............................................................................................................ 24  
    RSA Cloud Authentication Service ................................................................................ 24  
    Cisco ASA ................................................................................................................... 29  
Use Case Configuration ....................................................................................................... 35  
  AnyConnect ..................................................................................................................... 35  
  Clientless SSL VPN Portal ................................................................................................. 39
Solution Summary

This section shows all of the ways that Cisco ASA can integrate with RSA SecurID Access. Use this information to determine which use case and integration type your deployment will employ.

Use Cases

- **AnyConnect** - When integrated, users must authenticate with RSA SecurID Access in order to establish VPN connection. AnyConnect can be integrated with RSA SecurID Access using RADIUS, SSO Agent and Authentication Agent.

- **Clientless SSL VPN Portal** - When integrated, users must authenticate with RSA SecurID Access in order to access the clientless SSL VPN Portal. Clientless SSL VPN Portal can be integrated with RSA SecurID Access using RADIUS, SSO Agent, Authentication Agent and Risk Based Authentication.

- **Admin Access** - When integrated, users must authenticate with RSA SecurID Access in order to gain access to Cisco ASA’s administrative interfaces (ASDM, Telnet, SSH). Admin Access can be integrated with RSA SecurID Access using RADIUS and Authentication Agent.

- **AAA Firewall Rule** - When integrated, users must authenticate with RSA SecurID Access in order to be permitted network access as defined in the AAA Firewall rule. AAA Firewall Rule can be integrated with RSA SecurID Access using RADIUS and Authentication Agent.

Integration Types

- **RADIUS** integrations provide a text driven interface for RSA SecurID Access within the partner application. RADIUS provides support for most RSA SecurID Access authentication methods and flows.

- **SSO Agent** integrations use SAML 2.0 or HFED technologies to direct users’ web browsers to RSA SecurID Access for authentication. SSO Agents also provide Single Sign-On to other applications configured in the RSA Application Portal.

- **Authentication agent** integrations use an embedded RSA agent to provide RSA SecurID and Authenticate Tokencode authentication methods within the partner’s application.

- **Risk Based Authentication** integrations use customized scripts to direct users’ browsers to RSA SecurID Access for authentication. Risk-Based Authentication leverages an Authentication Agent or RADIUS integration to sign in to the partner application.
**Supported Features**

This section shows all of the supported features by integration type and by RSA SecurID Access component. Use this information to determine which integration type and which RSA SecurID Access component your deployment will use. The next section in this guide contains the instruction steps for how to integrate RSA SecurID Access with Cisco ASA using each integration type.

### Cisco ASA integration with RSA Cloud Authentication Service

<table>
<thead>
<tr>
<th>Authentication Methods</th>
<th>Authentication API</th>
<th>RADIUS</th>
<th>Relying Party</th>
<th>SSO Agent SAML</th>
<th>SSO Agent HFED</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA SecurID</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>LDAP Password</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Authenticate Approve</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Authenticate Tokencode</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Device Biometrics</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>SMS Tokencode</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Voice Tokencode</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>FIDO Token</td>
<td>n/a</td>
<td>n/a</td>
<td>-</td>
<td>✓</td>
<td>-</td>
</tr>
</tbody>
</table>

### Cisco ASA integration with RSA Authentication Manager

<table>
<thead>
<tr>
<th>Authentication Methods</th>
<th>Authentication API</th>
<th>RADIUS</th>
<th>Authentication Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA SecurID</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>On Demand Authentication</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Risk-Based Authentication</td>
<td>n/a</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- Supported
- Not supported
n/t Not yet tested or documented, but may be possible.
n/a Not applicable
Configuration Summary

This section contains links to the sections that contain instruction steps that show how to integrate Cisco ASA with RSA SecurID Access using all of the integration types and also how to apply them to each supported use case. First configure the integration type (e.g. RADIUS) then configure the use case (e.g. AnyConnect).

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 RSA SecurID Access and Cisco ASA components must be installed and working prior to the integration.

Integration Configuration

RADIUS with Authentication Manager
RADIUS with Cloud Authentication Service
SSO Agent - SAML
Authentication Agent
Risk-Based Authentication

Use Case Configuration

AnyConnect
Clientless SSL VPN Portal
Admin Access
AAA Firewall Rule

Certification Details

Date of testing: November 7th, 2018
RSA Cloud Authentication Service
RSA Authentication Manager 8.2 SP1, Virtual Appliance
Cisco ASA9.10(1)
Cisco AnyConnect 4.6.03049, Windows 10 64 bit
Cisco AnyConnect 4.6.03049, Mac OS 10

Known Issues

Clientless SSL VPN - "Wrong URL." After successful RBA Login

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 \texttt{am\_integration.js} file before uploading it to the Web Contents section in ASA:

Change line \#41 of the \texttt{am\_integration.js} file from:

\begin{verbatim}
origActionURL.setAttribute('value', toAbsolutePath(logonForm.action));
\end{verbatim}

To:

\begin{verbatim}
origActionURL.setAttribute('value', 'https://$ASA\_HOSTNAME$/%2Bwebvpn%2B/index.html');
\end{verbatim}

Change \texttt{$ASA\_HOSTNAME$} to your ASA's IP or hostname.

\textbf{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.
Integration Configuration

Authentication Agent

This section contains instructions on how to integrate Cisco ASA with RSA Authentication Manager as an authentication agent.

Architecture Diagram

RSA Authentication Manager

To configure your RSA Authentication Manager for use with an authentication 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.

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

Cisco ASA

Follow the steps in this section to integrate Cisco ASA with RSA SecurID Access as an authentication agent.
Procedure

1. Login to Cisco ASDM and browse to Configuration > Device Management > Users/AAA > AAA Server Groups and click Add.

2. Enter a name for the AAA Server Group, choose SDI from the Protocol drop-down menu and click OK.

3. Highlight your SDI AAA Server Group and click to Add a server to the group.
4. Configure the SDI AAA Server and click **OK**.

- **Interface Name**: Select the interface that will be used to communicate with RSA Authentication Manager.
- **Server Name or IP Address**: Enter the Server Name or IP address of your primary RSA Authentication Manager.

**Important!** **ONLY ADD THE PRIMARY RSA AUTHENTICATION MANAGER. DO NOT ADD REPLICAS.** The Cisco ASA will learn about any RSA Authentication Manager replica servers at the time of the first authentication.

5. Click **Apply**.
SecurID Agent Integration Details

| RSA Authentication Agent API             | Custom build        |
| RSA SecurID Authentication API (REST)   | N/A                  |
| RSA SecurID User Specification          | All users            |
| Display RSA Server Info                 | No                   |
| Perform Test Authentication             | Yes                  |
| Agent Tracing                          | Yes                  |

RSA Authentication Agent Files (C and Java Agents)

<table>
<thead>
<tr>
<th>Agent Files</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>sdconf.rec</td>
<td>None</td>
</tr>
<tr>
<td>sdopts.rec</td>
<td>None</td>
</tr>
<tr>
<td>Node secret</td>
<td>In memory</td>
</tr>
<tr>
<td>sdstatus.12 / jastatus.12</td>
<td>In memory</td>
</tr>
<tr>
<td>rsa_api.properties</td>
<td>None</td>
</tr>
</tbody>
</table>

API Details: (C and Java Agents only)

Cisco ASA implements a modified version of the RSA Authentication Agent. 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: (C and Java Agents only)

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

sdstatus.12: (C and Java Agents only)

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

Next Step: Proceed to the Use Case Configuration Summary section for information on how to apply the Authentication Agent configuration to your use case.
RADIUS with AM

This section contains instructions on how to integrate Cisco ASA with RSA Authentication Manager using RADIUS.

Architecture Diagram

RSA Authentication Manager

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 listens on ports UDP 1645 and UDP 1812.

Cisco ASA

Follow the steps in this section to integrate Cisco ASA with RSA SecurID Access as a RADIUS client.

Procedure

1. Login to Cisco ASDM and browse to Configuration > Device Management > Users/AAA > AAA Server Groups and click Add.
2. Enter a name for the **AAA Server Group**, choose **RADIUS** from the **Protocol** drop-down menu and click **OK**.

3. Highlight your RADIUS AAA Server Group and click to **Add** a server to the group.
4. Configure the RADIUS **AAA server** settings. If you are planning to integrate with AnyConnect using RADIUS, and intend to use software token automation, click to open SDI Messages **Message Table**. If not, click **OK** to continue.

- **Interface Name**: Select the interface that will be used to communicate with RSA SecurID Access.
- **Server Name or IP Address**: Enter the Server Name or IP address of your RSA Authentication Manager server.
- **Timeout**: Set to **10** seconds.
- **Server Authentication Port**: Set to **1645** or **1812**.
- **Server Secret Key**: Enter the RADIUS shared secret. It must match the secret as entered in the RSA RADIUS server.

5. If integrating AnyConnect with RADIUS, and you intend to use software token automation, enter the values exactly as shown below into the **SDI Messages Message Table** and then click **OK**.
<table>
<thead>
<tr>
<th>Message Name</th>
<th>Message Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>ready-for-sys-pin</td>
<td>ARE YOU PREPARED</td>
</tr>
<tr>
<td>new-pin-reenter</td>
<td>re-enter</td>
</tr>
<tr>
<td>new-pin-meth</td>
<td>Do you want</td>
</tr>
<tr>
<td>next-ccode-and-reauth</td>
<td>PIN Accepted</td>
</tr>
<tr>
<td>next-code</td>
<td>Wait for token to change</td>
</tr>
<tr>
<td>new-pin-sys-ok</td>
<td>New PIN Accepted</td>
</tr>
<tr>
<td>new-pin-sup</td>
<td>Are you satisfied with</td>
</tr>
<tr>
<td>new-pin-req</td>
<td>Enter a new PIN</td>
</tr>
</tbody>
</table>

Repeat steps 3 through 5 for replica RSA Authentication Manager servers.

6. Click **Apply**.

**Next Step:** Proceed to the **Use Case Configuration Summary** section for information on how to apply the RADIUS configuration to your use case.
**RADIUS with CAS**

This section contains instructions on how to integrate Cisco ASA with RSA Cloud Authentication Service using RADIUS.

**Architecture Diagrams**

![Architecture Diagram](image)

**RSA Cloud Authentication Service**

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 Cloud Administrative Console** and browse to **Authentication Clients > RADIUS > Add RADIUS Client** and enter the **Name, IP Address** and **Shared Secret**.

Click **Publish**.

**Cisco ASA**

Follow the steps in this section to integrate Cisco ASA with RSA SecurID Access as a RADIUS client.

**Procedure**

1. Login to Cisco ASDM and browse to **Configuration > Device Management > Users/AAA > AAA Server Groups** and click **Add**.
2. Enter a name for the **AAA Server Group**, choose **RADIUS** from the **Protocol** drop-down menu and click **OK**.

3. Highlight your **RADIUS AAA Server Group** and click to **Add** a server to the group.
4. Configure the RADIUS **AAA server** settings and click **OK**.

- **Interface Name**: Select the interface that will be used to communicate with RSA SecurID Access.
- **Server Name or IP Address**: Enter the Server Name or IP address of your RSA Identity Router.
- **Timeout**: Set to **60** seconds.
- **Server Authentication Port**: Set to **1812**.
- **Server Secret Key**: Enter the RADIUS shared secret. It must match the secret as entered in the RSA Cloud Administration Console.

Repeat steps 3 and 4 for replica RSA Identity Routers.

6. Click **Apply**.
Next Step: Proceed to the Use Case Configuration Summary section for information on how to apply the RADIUS configuration to your use case.
Risk-Based Authentication

This section contains instructions on how to integrate Cisco ASA with RSA Authentication Manager using Risk Based Authentication.

Architecture Diagram

---

RSA Authentication Manager

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.


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

/opt rsa/am/utils/rba-agents

Refer to RSA Authentication Manager Administrator’s Guide for more information on RBA integration scripts.
Cisco ASA

Follow the steps in this section to integrate Cisco ASA with RSA SecurID Access using risk-based authentication.

Before you begin

Complete RADIUS or Authentication Agent configuration and apply it to Clientless SSL VPN Portal use case.

Procedure


2. Browse to the am_integration.js integration script, select No to not require authentication for access to content and click Import Now.

4. Enter a **Customization Object Name**, mark the **Use** checkbox for your Connection Profile and then open the **Logon Page > Informational Panel** page.

5. Mark the checkbox to **Display informational panel**, copy the following text into the **Text** field and click **OK**.

```html
<script src='/+CSCOU+/am_integration.js' type='text/javascript'></script>
<script>window.onload=redirectToIdP;</script>
```
6. Click **Apply**.

![Configuration changes saved successfully.](image)

**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.

**Next Step**: Head back to the **main page** for more certification related information.
SSO Agent - SAML

This section contains instructions on how to integrate Cisco ASA RSA Cloud Authentication Service using a SAML SSO Agent.

Architecture Diagram

RSA Cloud Authentication Service

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Cisco ASA in the RSA Cloud Administration Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

Procedure

1. Logon to the RSA Cloud Administration Console and browse to Applications > Application Catalog, search for Cisco ASA and click +Add to add the connector.
2. Enter a **Name** for your application and click **Next Step**.

3. Configure the Initiate SAML Workflow section and then scroll down to the **SAML Identity Provider (Issuer)** section.
4. Configure the Identity Provider section and scroll down to the **Service Provider** section.

- **Identity Provider URL**: The default value will work. If you choose to change the Issuer Entity ID, make sure that the change is reflected in this URL (after `?idp_id=`).
- **Issuer Entity ID**: The default value will work, but you may want to change it to something more friendly since this value will be an identifier for this IdP in the Cisco ASA configuration.
- **SAML Response Signature**: Upload the private key and certificate that SecurID Access will use to sign the SAML response.

5. Configure the Service Provider settings and scroll down to the **User Identity** section.

![](service_provider.png)

- **Assertion Consumer Service (ACS) URL**: Enter the URL `https://$base-url$/+CSCOE+/saml/sp/acs?tname=$connection-profile$` where `$base-url$` matches the Base URL specified in the Cisco ASA SAML SP configuration and `$connection-profile$` matches the name of your AnyConnect or Clientless SSL VPN connection profile.

- **Audience (Service Provider Entity ID)**: Enter the URL `https://$base-url$/saml/sp/metadata/$connection-profile$` where `$base-url$` matches the Base URL specified in the Cisco ASA SAML SP configuration and `$connection-profile$` matches the name of your AnyConnect or Clientless SSL VPN connection profile.

**Note**: If you are unsure of these values, set place holder values so you can continue with the configuration. When you're done with the Cisco ASA configuration, you can return to this page and fill in the correct values.

6. Configure the User Identity section and click **Next Step**.

![](user_identity.png)

7. Configure the Access Policy and click **Next Step**.

![](access_policy.png)
8. Configure the Portal Display settings and click **Save and Finish**.
Important! Unmark the checkbox to Display in Portal if you are enabling this connection for use with AnyConnect or if you want to prevent IdP-initiated workflows to the Clientless SSL VPN Portal.

9. Click Publish Changes.

Cisco ASA

Follow the steps in this section to integrate Cisco ASA with RSA SecurID Access as a SAML SSO Agent.

Procedure
1. Create a trustpoint to associate with your RSA SAML IdP signing certificate. CA certificates and Identity Certificates are both valid for this purpose.

Example: Login to Cisco ASDM and browse to Configuration > Remote Access VPN > Certificate Management > Identity Certificates and click Add.

2. Add the certificate info and click Add Certificate.

3. Click Apply.
Open the SAML IdP management pane. This can be reached inside the AnyConnect Connection Profile or inside the Clientless SSL VPN Connection Profile. Whichever you decide, the IdP configuration can be applied to AnyConnect and/or Clientless SSL VPN.

4. Browse to Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles and then click to Edit a profile.

5. On the Basic tab, under the SAML Identity Provider heading, click Manage...
6. Click **Add**.

7. Configure the SSO Server settings and click **OK**.
- **IDP Entity ID**: Enter the Issuer *Entity ID* from the RSA Cloud Administration Console.
- **Sign In URL**: Enter the *Identity Provider URL* from the RSA Cloud Administration Console.
- **Base URL**: Enter a URL which will be the basis for ACS URL and SP Entity ID.
- **Identity Provider Certificate**: Select the trustpoint which contains the IdP signing certificate.

8. Set the **SAML Server** back to *None* and click **OK**.

Click **Apply**.
**Next Step:** Proceed to the **Use Case Configuration Summary** section for information on how to apply the SAML SSO Agent configuration to your use case.
Use Case Configuration

AnyConnect

Follow the instruction steps in this section to apply your RADIUS, SSO Agent or Authentication Agent configuration to Cisco ASA AnyConnect.

Before you begin: Configure the integration type that your use case will employ. Refer to the Integration Configuration Summary section for more information.

Procedure

1. Login to Cisco ASDM and browse to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles and edit your profile.

2a. If integrating using RADIUS or Authentication Agent (SDI), select AAA from the method drop-down menu, your AAA Server Group from the drop-down menu and click OK.
2b. If integrating using SSO Agent select SAML from the method drop-down, your SAML Server from the drop-down menu and click OK.

**Note:** SSO Agent integrations require at least AnyConnect version 4.6.

3. Click Apply.

If you are integrating AnyConnect with RSA Cloud Authentication Service using RADIUS, complete the rest of the steps in this section; otherwise you are done.

4. Browse to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile and click to Edit the appropriate profile.
5. Open the **Preferences (Part 2)** tab, set the **Authenticate Timeout** to 60 and then open the **Server List** tab.

6. There must be at least one entry in the **Server List**. Verify that there is an entry or add one to the list and click **OK**.
7. Click **Apply**.

Configuration is complete.

**User Experience**

**Video Link** - AnyConnect RADIUS integration with RSA Authentication Manager and Cloud Authentication Service.

Refer to the RSA Ready SecurID Access Implementation Guide for Cisco AnyConnect for information on how to configure Cisco AnyConnect; including software token automation.

Return to the main page for more certification related information.
Clientless SSL VPN Portal

Follow the instruction steps in this section to apply your RADIUS, SSO Agent or Authentication Agent configuration to Cisco ASA Clientless SSL VPN Portal.

Before you begin: Configure the integration type that your use case will employ. Refer to the Integration Configuration Summary section for more information.

Procedure

1. Login to Cisco ASDM and browse to Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles and edit your profile.

2a. If integrating using RADIUS or Authentication Agent (SDI), select AAA from the method drop-down menu, your AAA Server Group from the drop-down menu and click OK.
2b. If integrating using SSO Agent select **SAML** from the method drop-down, your **SAML Server** from the drop-down menu and click **OK**.

3. Click **Apply**.

Configuration is complete.

**User Experience**

Authentication Agent Login Screen:
Return to the main page for more certification related information.
Admin Access

Follow the instruction steps in this section to apply your Authentication Agent or RADIUS configuration to Cisco ASA Admin Access.

Before you begin: Configure the integration type that your use case will employ. Refer to the Integration Configuration Summary section for more information.

Procedure

Login to Cisco ASDM and browse to Configuration > Device Management > Users / AAA > AAA Access, configure the settings and click Apply.

User Experience

ASDM - Authentication Agent
Return to the main page for more certification related information.
AAA Firewall Rule

Follow the instruction steps in this section to apply your RADIUS or Authentication Agent configuration to Cisco ASA AAA Firewall Rule.

Before you begin: Configure the integration type that your use case will employ. Refer to the Integration Configuration Summary section for more information.

Procedure

1. Login to Cisco ASDM and browse to Configuration > Firewall > AAA Rules and click Add > Add Authentication Rule...

2. Select an Authentication Agent or RADIUS AAA Server Group, configure the rest of your rule settings and click OK.
**Note:** When securing traffic other than HTTP, Telnet or SSH the user will have to authenticate with ASA using one of these protocols in order to satisfy the AAA rule. See the Known Issues section for more information.

3. Click **Apply**.

Configuration is complete.

**User Experience**

Authentication Agent - In this case an AAA Firewall Rule triggers authentication using HTTP.
Return to the main page for more certification related information.