RSA SecurID Access Implementation Guide

Cisco Systems, Inc.

Firepower Threat Defense (FTD) 6.3

Pete Waranowski, RSA Partner Engineering

Last modified: January 25th, 2019

Table of Contents

Solution Summary

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

Use Case

Remote Access VPN (AnyConnect) - When integrated, users must authenticate with RSA SecurID Access in order to establish a VPN connection to Cisco FTD using Cisco AnyConnect VPN client. Remote Access VPN can be integrated with RSA SecurID Access using **RADIUS**.

Integration Type

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.

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 CiscoFTD using each integration type.

Cisco FTD integration with RSA Cloud Authentication Service

Authentication Methods	Authentication API	RADIUS	Relying Party	SSO Agent
RSA SecurID	-	✔	-	-
LDAP Password	-	✔	-	-
Authenticate Approve	-	✔	-	-
Authenticate Tokencode	-	✔	-	-
Device Biometrics	-	✔	-	-
SMS Tokencode	-	✔	-	-
Voice Tokencode	-	✔	-	-
FIDO Token	n/a	n/a	-	-

Cisco FTD integration with RSA Authentication Manager

Authentication Methods	Authentiaction API	RADIUS	Authentication Agent
RSA SecurID	-	✔	-
On Demand Authentication	-	✔	-
Risk-Based Authentication	n/a	-	-

✔ Supported

- Not supported

n/t Not yet tested or documented, but may be possible.

Configuration Summary

This section contains links to the sections that contain instruction steps that show how to integrate Cisco FTD 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. Remote Access VPN).

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 FTD components must be installed and working prior to the integration.

Integration Configuration

RADIUS with AM

RADIUS with CAS

Use Case Configuration

Remote Access VPN

Certification Details

Date of testing: January 24th, 2019

RSA Cloud Authentication Service

RSA Authentication Manager 8.3, Virtual Appliance

Cisco FTD 6.3, Operating System

Known Issues

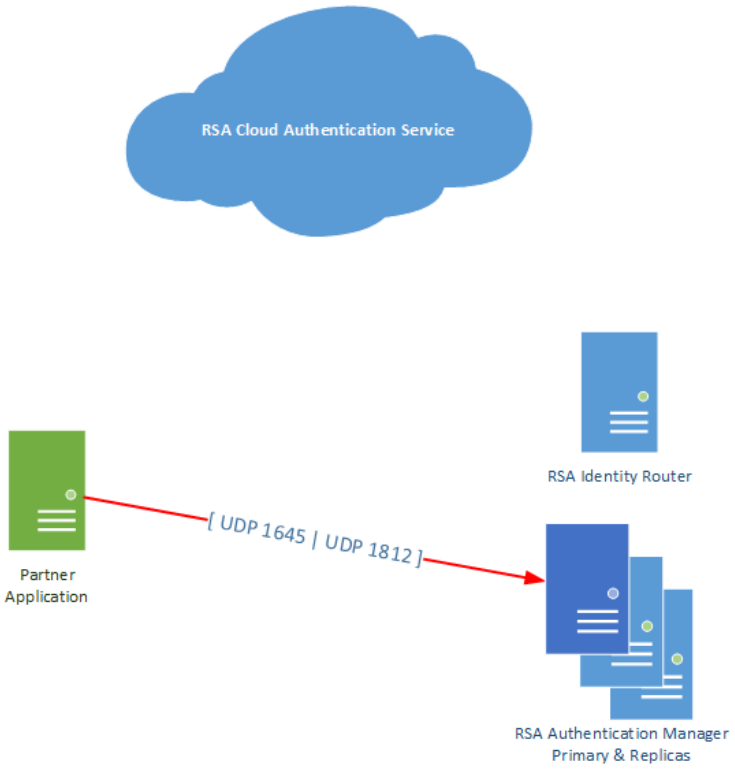
None.

Integration Configuration

RADIUS with AM

This section contains instructions on how to integrate Cisco FTD 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).

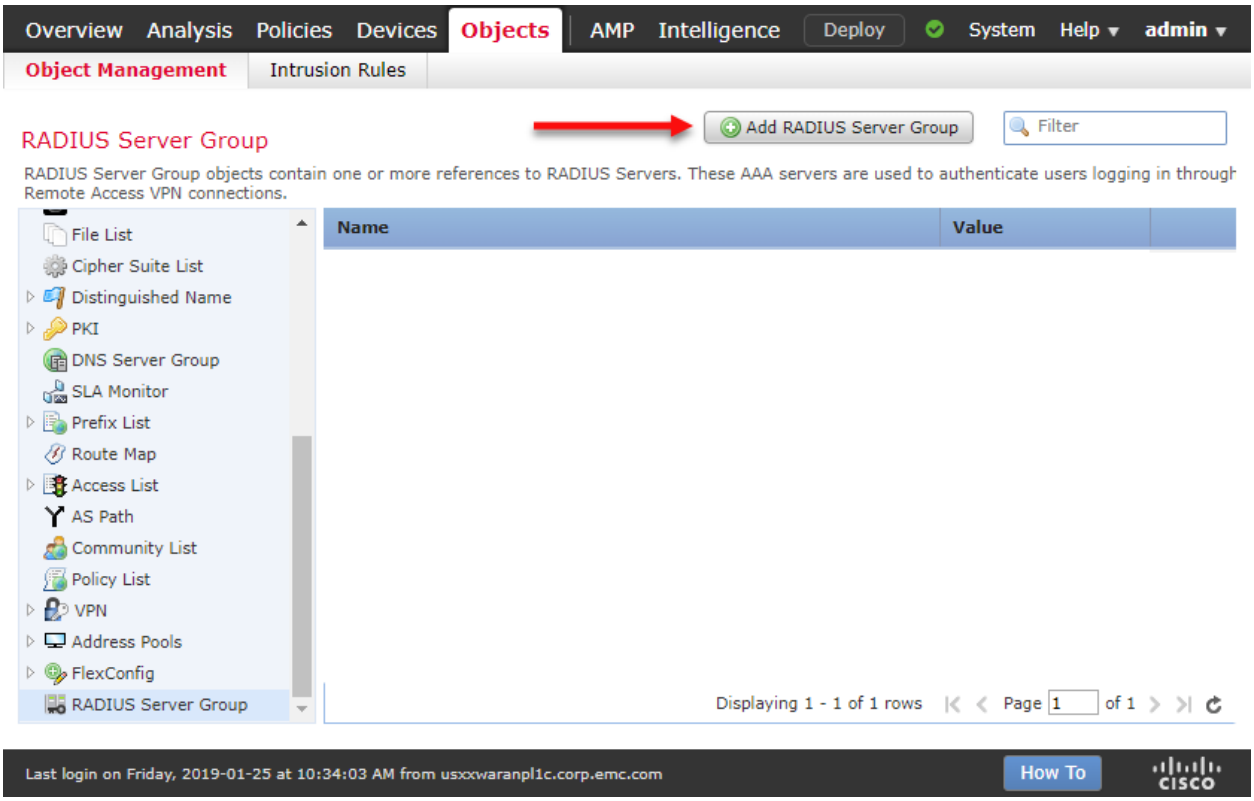
RSA Authentication Manager listens on ports UDP 1645 and UDP 1812.

Cisco FTD

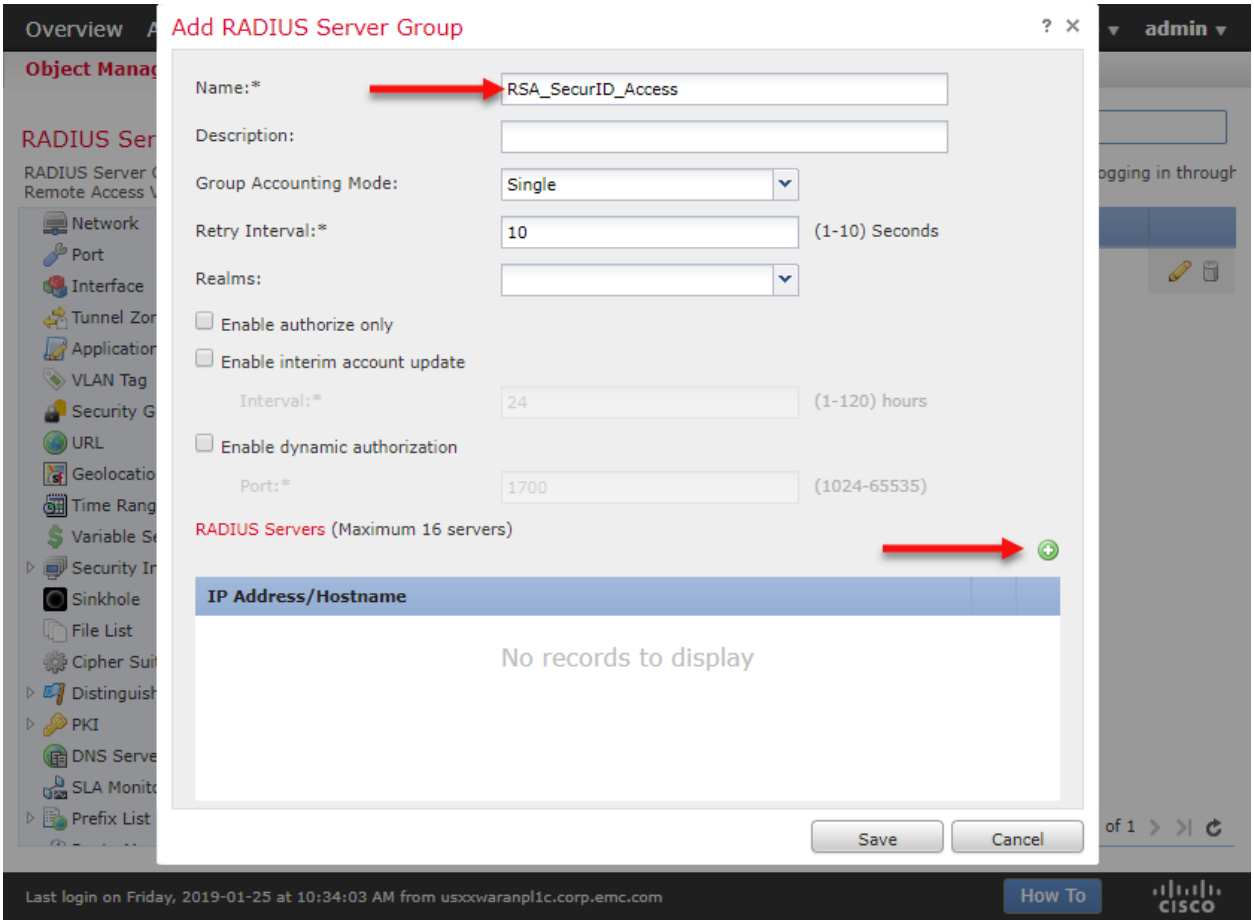
Follow the steps in this section to configure Cisco FTD as a RADIUS client to RSA Authentication Manager.

Procedure

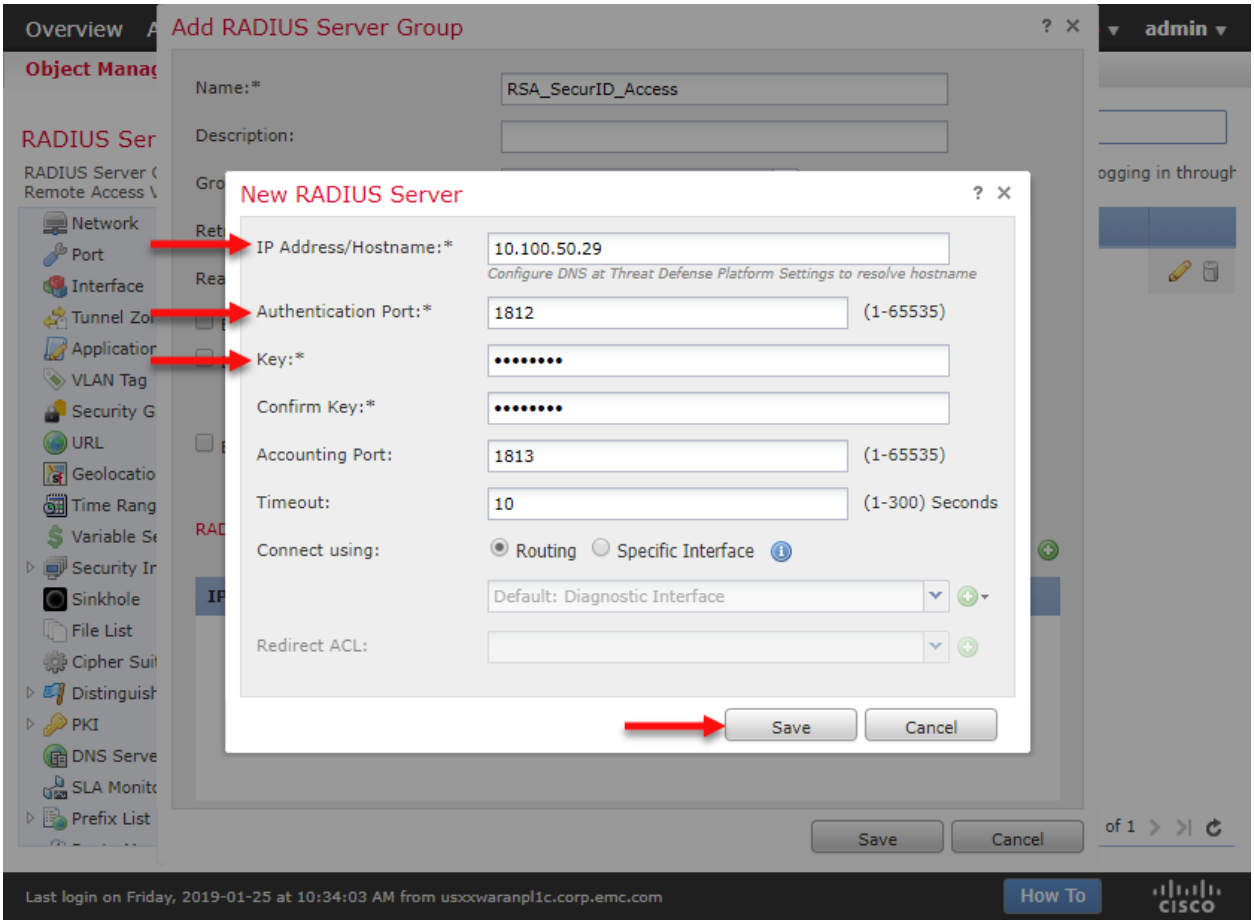
1. Logon to Cisco Firepower Management Center and browse to **Objects** > **Object Management** > **RADIUS Server Group** and click **Add RADIUS Server Group**.



2. Enter a **Name** for the server group and click **+** to add a RADIUS server.

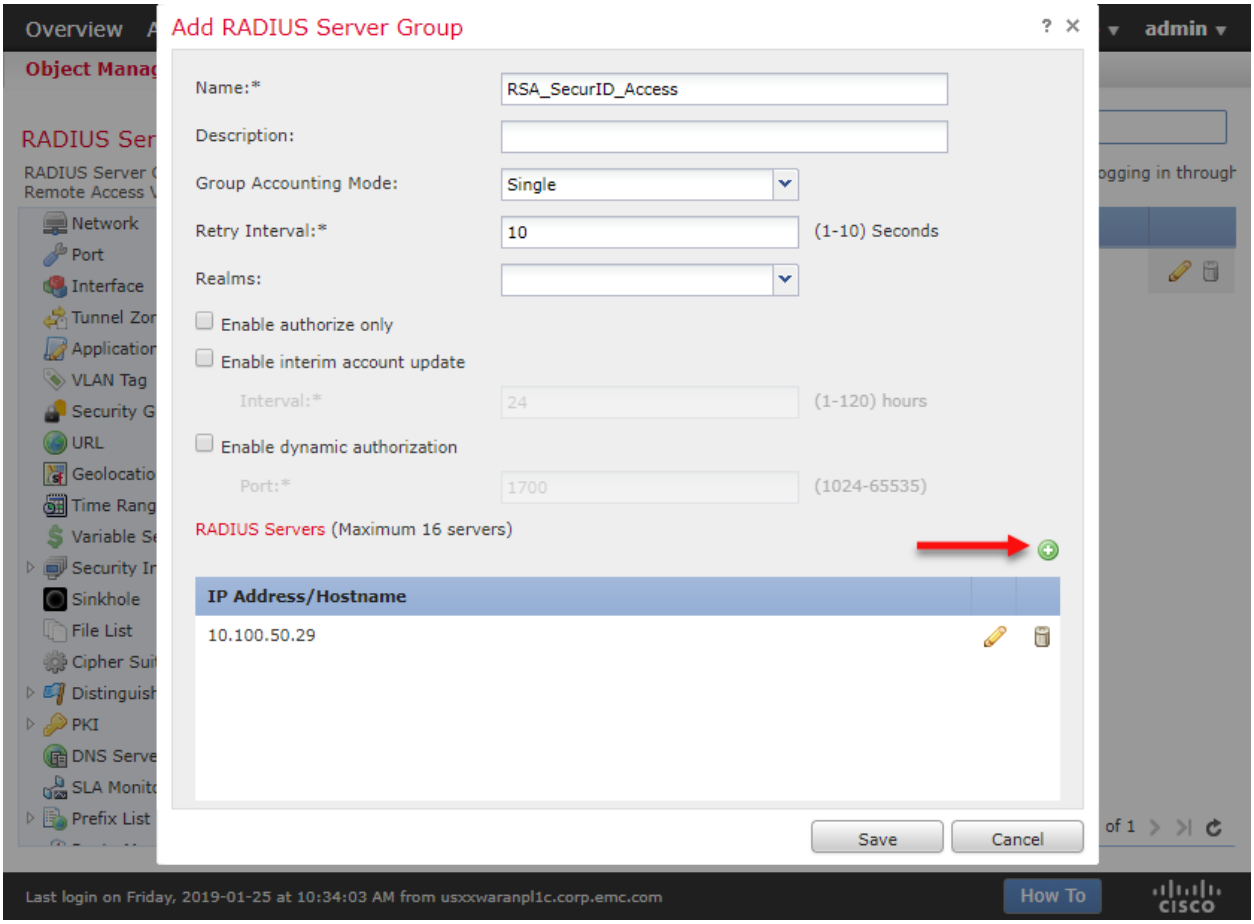


3. Configure the RADIUS server settings and click **Save**.

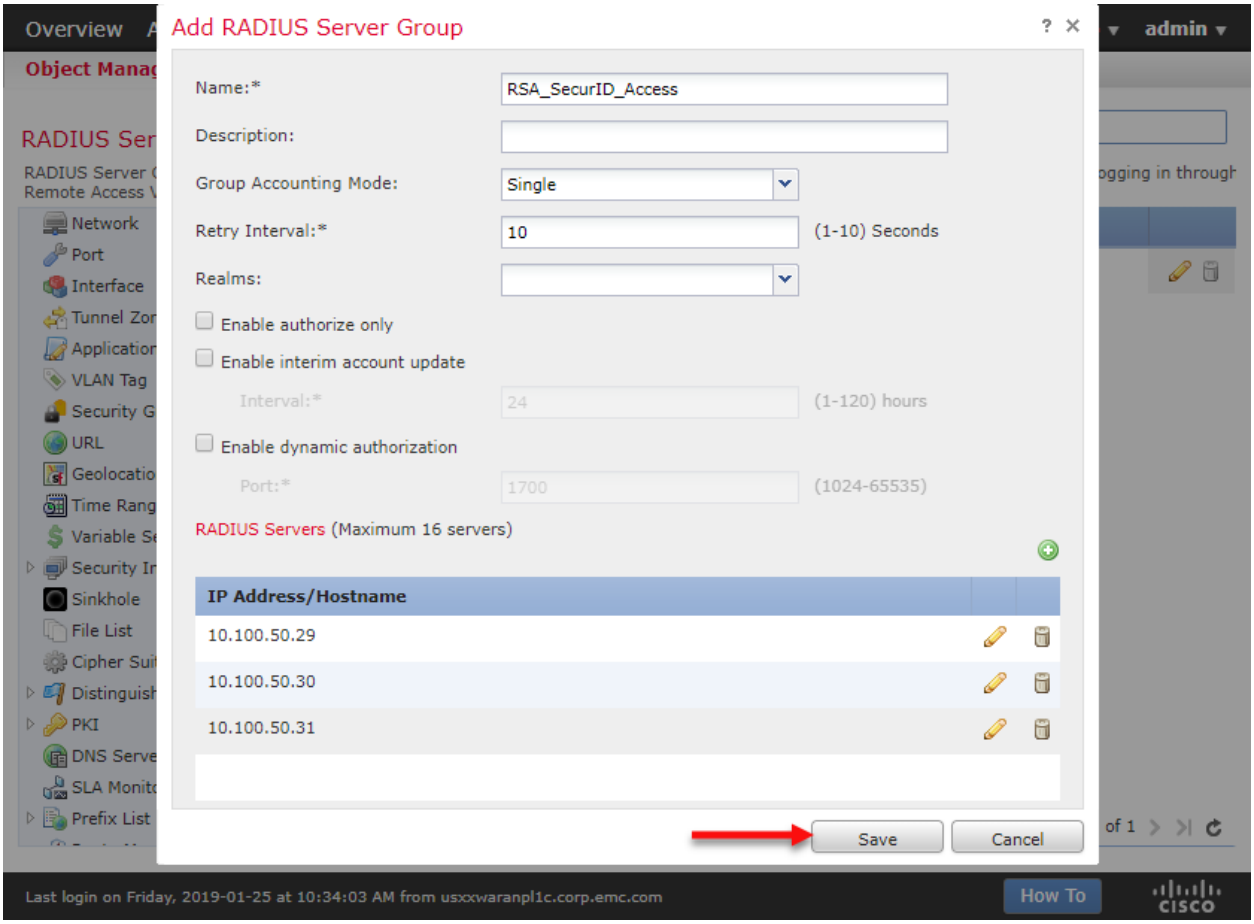


- **IP Address/Hostname** - Enter the hostname or IP address of your RSA Authentication Manager server.
- **Authentication Port** - Enter either 1645 or 1812.
- **Key** - Enter the RADIUS shared secret to match as entered in the RADIUS client in RSA Authentication Manager Security Console.

4. (Optional) click **+** to add RADIUS servers for any RSA Authentication Manager replica servers.



5. Click to **Save** the RADIUS Server Group.

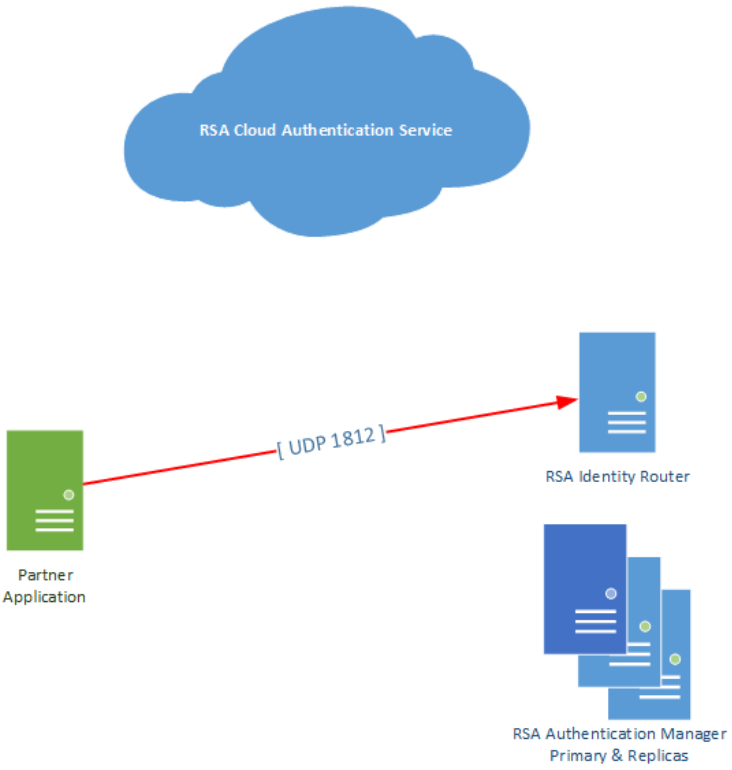


Next Step: Proceed to the Use Case Configuration Summary section for information on how to apply the RADIUS configuration to your use case.

RADIUS with CAS

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

Architecture Diagram



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**.

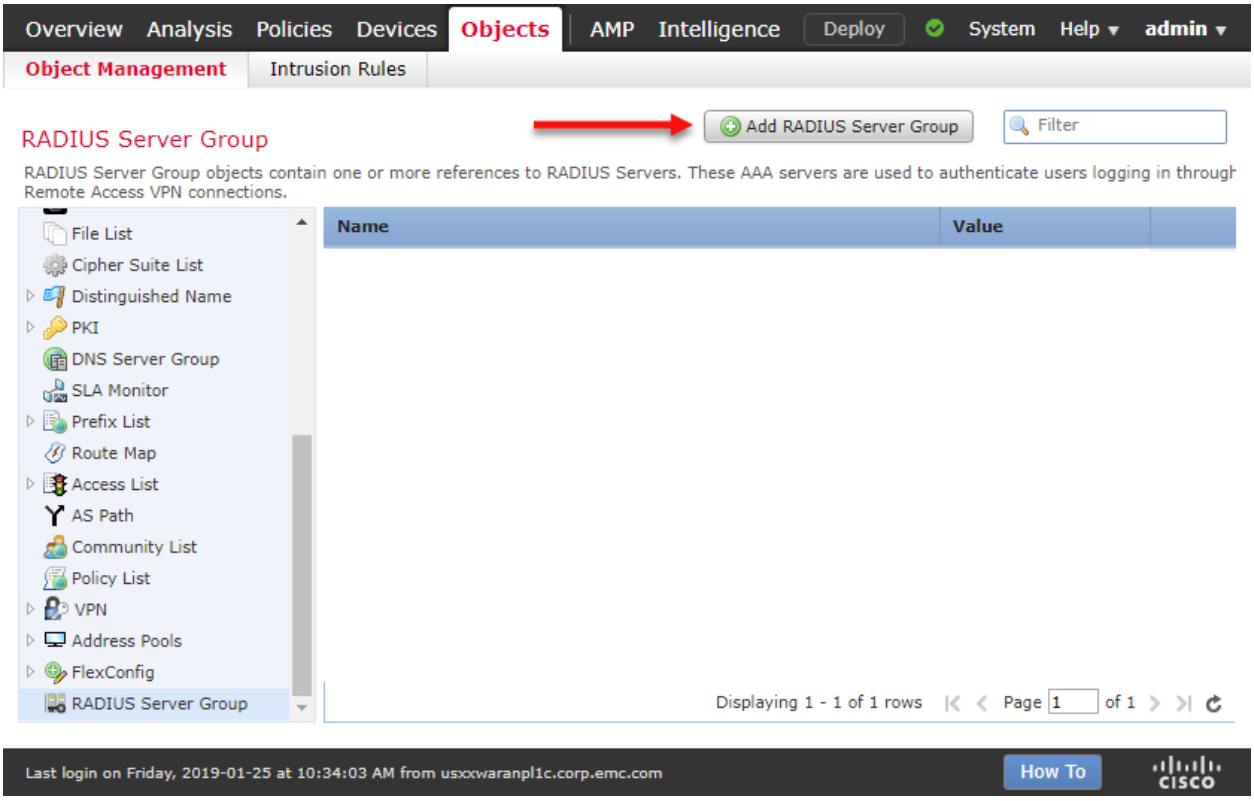
Click **Publish**.

Cisco FTD

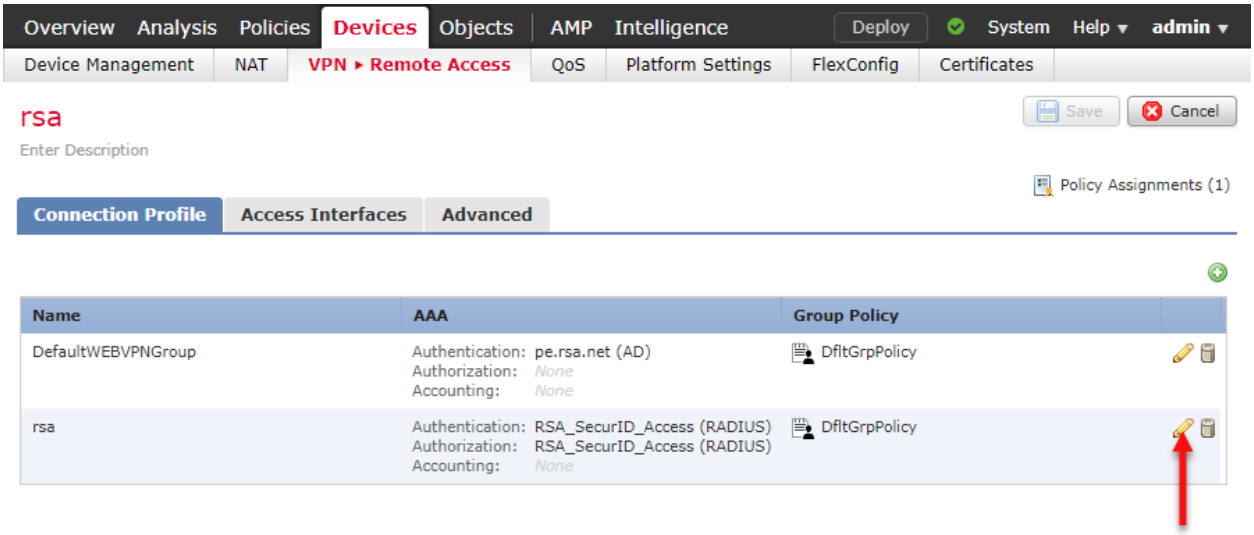
Follow the steps in this section to configure Cisco FTD as a RADIUS client to RSA Cloud Authentication Service.

Procedure

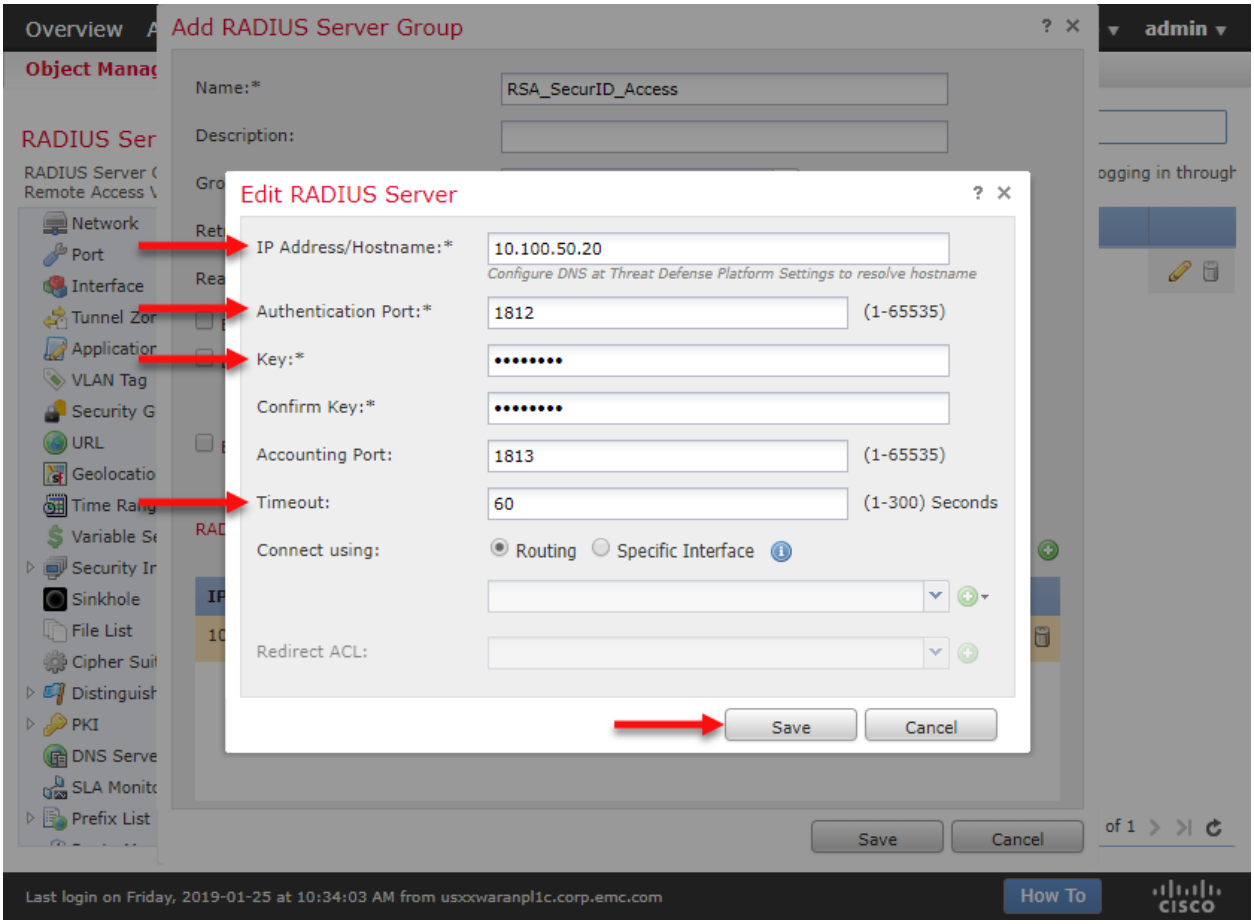
1. Logon to Cisco Firepower Management Center and browse to **Objects** > **Object Management** > **RADIUS Server Group** and click **Add RADIUS Server Group**.



2. Enter a **Name** for the server group and click **+** to add a RADIUS server.

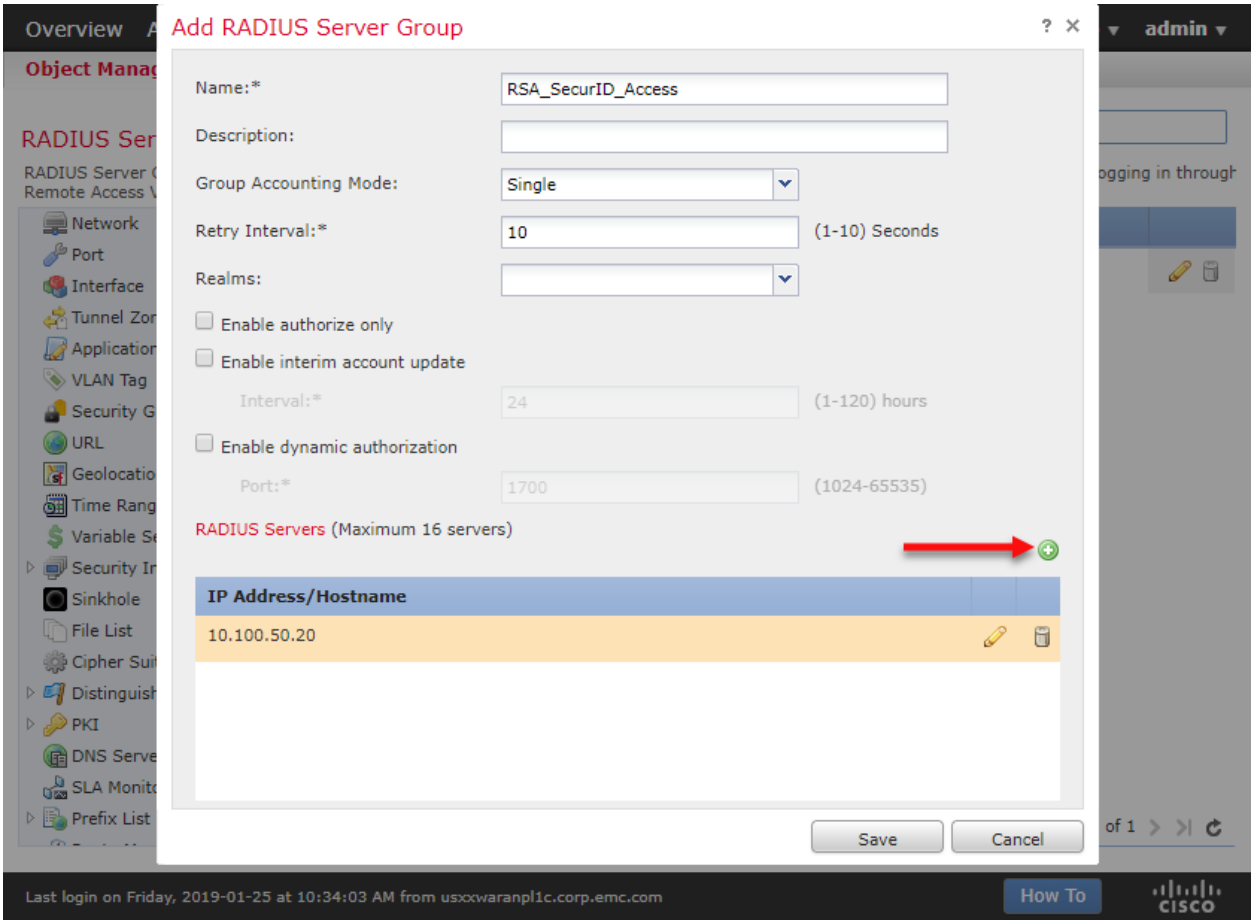


3. Configure the RADIUS server settings and click **Save**.

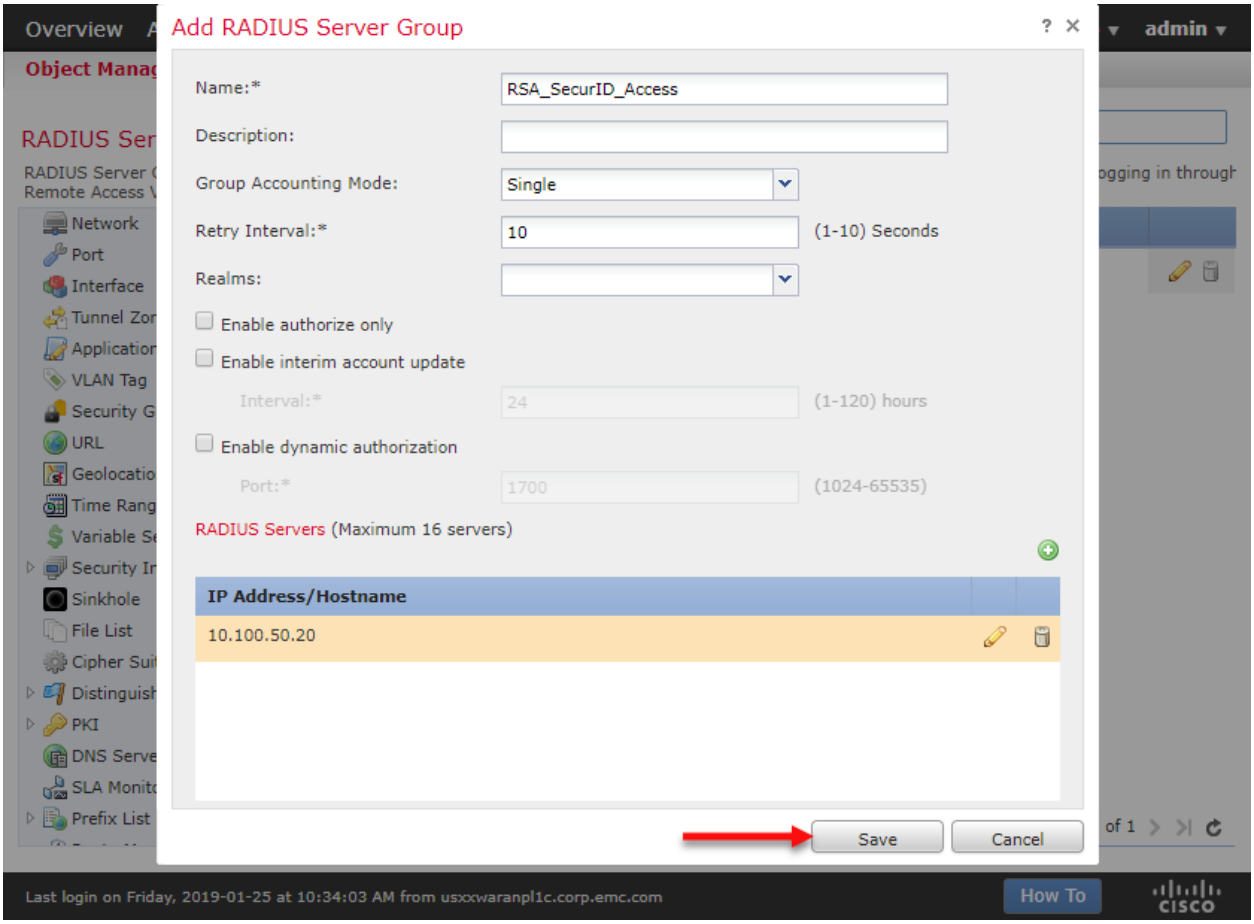


- **IP Address/Hostname** - Enter the hostname or IP address of your RSA Identity Router.
- **Authentication Port** - Enter 1812.
- **Key** - Enter the RADIUS shared secret to match as entered in the RADIUS client in RSA Cloud Administation Console.

4. (Optional) click **+** to add RADIUS servers for any RSA Authentication Manager replica servers.



5. Click to **Save** the RADIUS Server Group.



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

Use Case Configuration

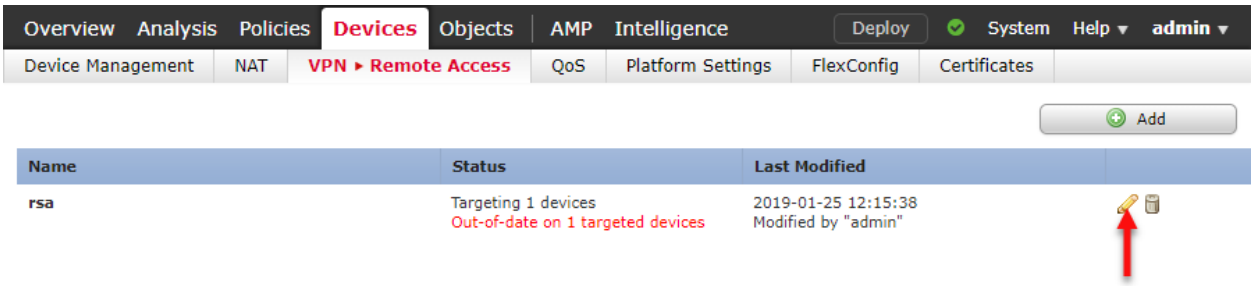
Remote Access VPN

Follow the instruction steps in this section to apply your **RADIUS** configuration to Cisco FTD Remote Access VPN.

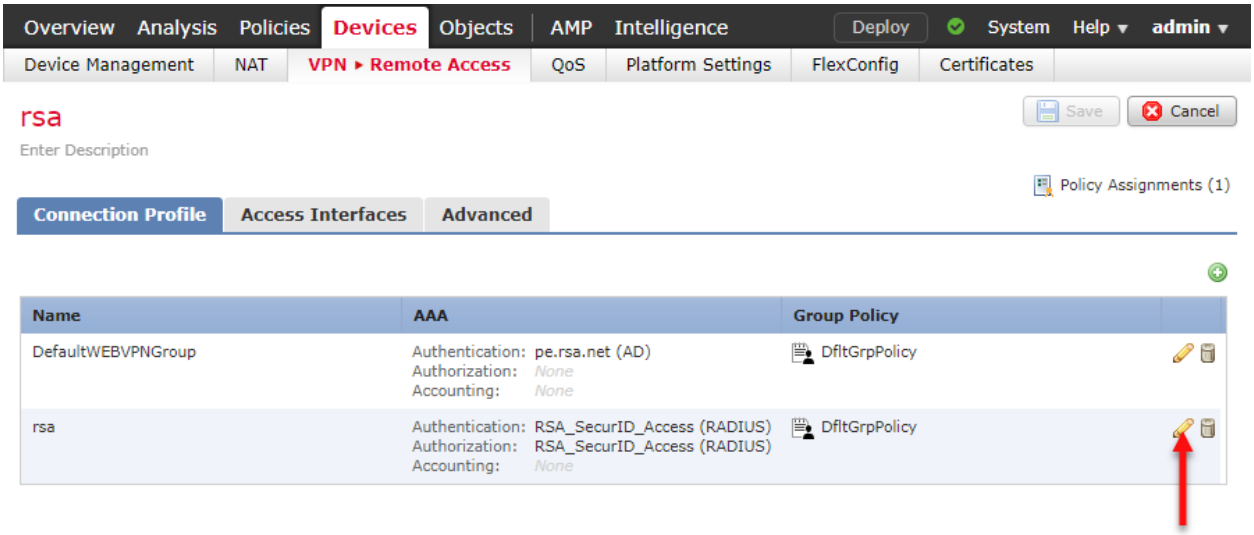
Before you begin: Configure the integration type that your use case will employ. Refer to the Integration Configuration Summary section for more information.

Procedure

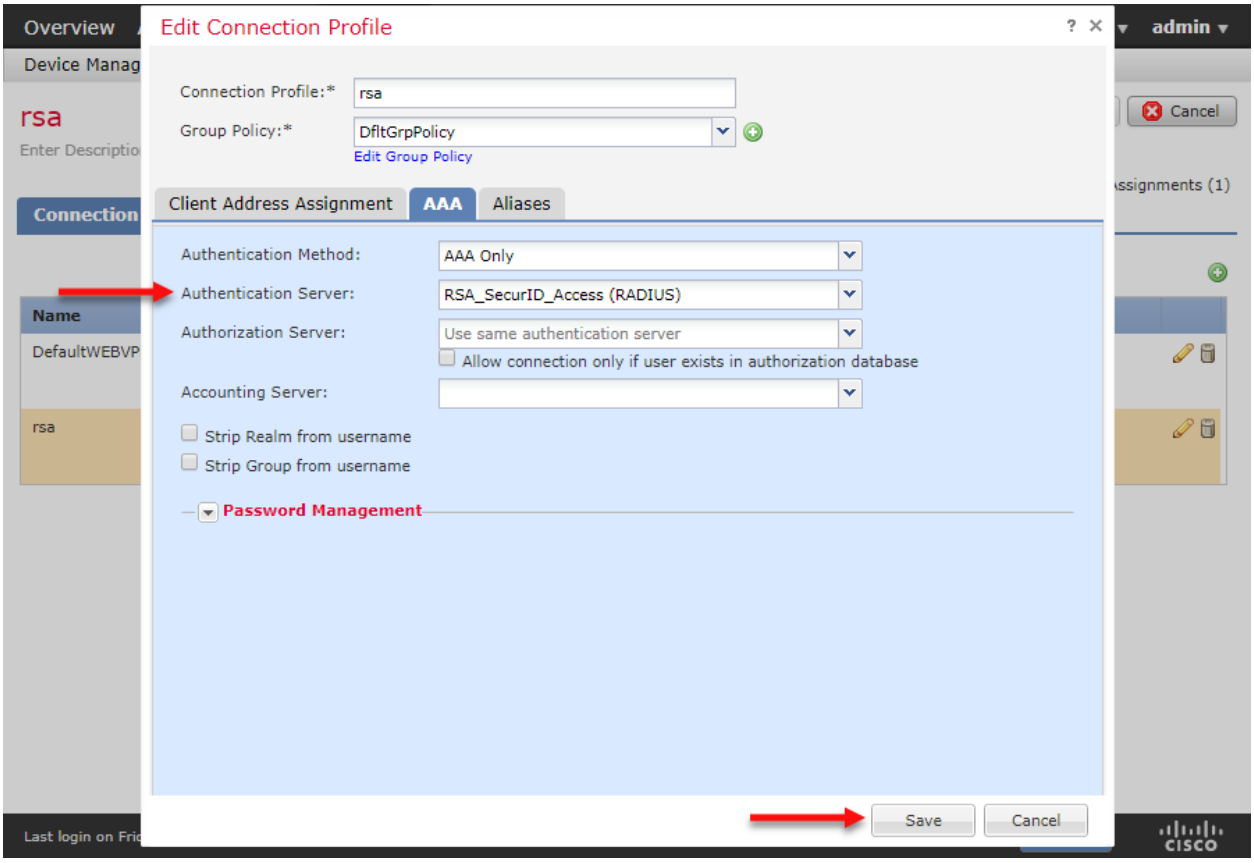
1. Browse to **Devices** > **VPN** > **Remote Access** and click to edit your Remote Access VPN policy.



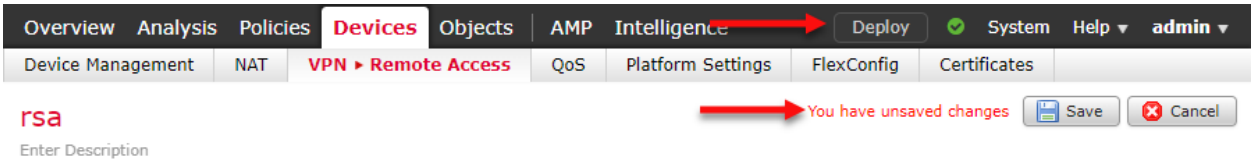
2. Click to Edit the Remote Access VPN Connection profile.



3. Open the **AAA** tab, set the **Authentication Server** to the RADIUS AAA server group you configured in the last section and click **Save**.



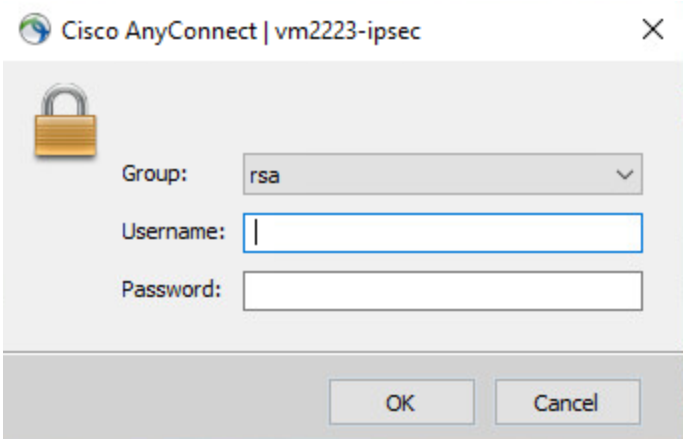
4. Click to **Save** your changes and then click to **Deploy** the updated configuration to the FTD appliance.



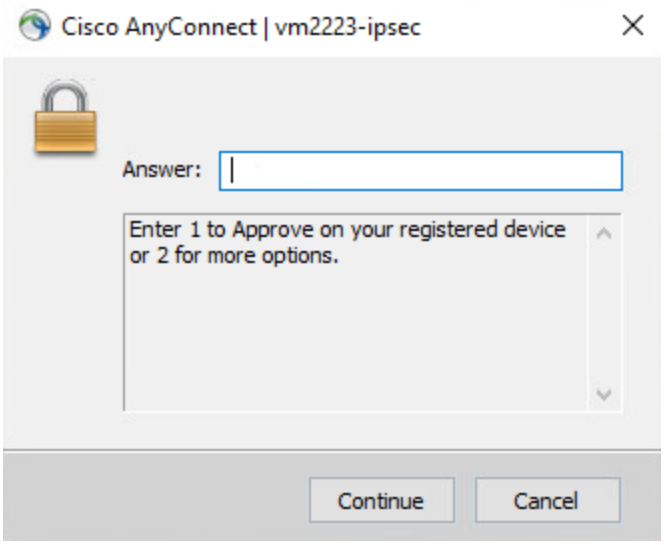
Configuration is complete.

User Experience - RSA Cloud Authentication Service

RADIUS - Login Page



RADIUS - method selection



Head back to the main page for more certification related information.