RSA SecurID Access Implementation Guide

Forescout Technologies Inc.

Forescout 8.0

Certified: August 22, 2019

Table of Contents

Solution Summary

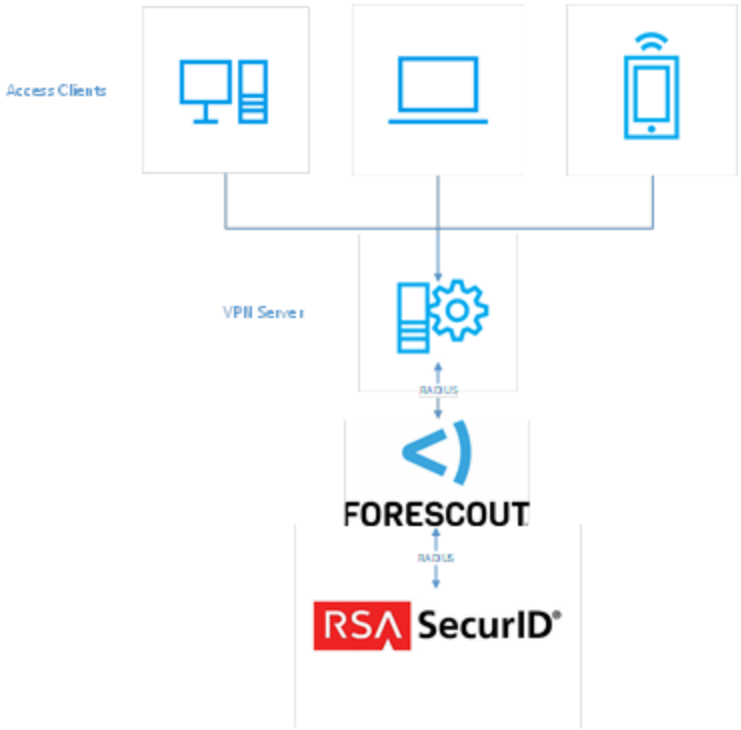
This section describes the ways in which Forescout can integrate with RSA SecurID Access.

Use Cases

RADIUS proxy - Forescout acts a RADIUS proxy between a Cisco ASA and RSA SecurID Access. Should an endpoint or user match a Forescout control policy, Forescout rejects any additional authentication attempts from the user.

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.



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 contains the steps to integrate RSA SecurID Access with Forescout for each integration type.

Forescout 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	-	-

Forescout Integration with RSA Authentication Manager

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

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

Configuration Summary

The following links provide instructions on how to integrate Forescout with RSA SecurID Access.

This document is not intended to suggest optimum installations or configurations. It assumes 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 Forescout components must be installed and working prior to the integration.

Integration Configuration

- RADIUS with AM
- RADIUS with CAS

Certification Details

Date of testing: August 7, 2019

RSA Cloud Authentication Service

RSA Authentication Manager 8.3, Virtual Appliance

Forescout 8.0

Known Issues

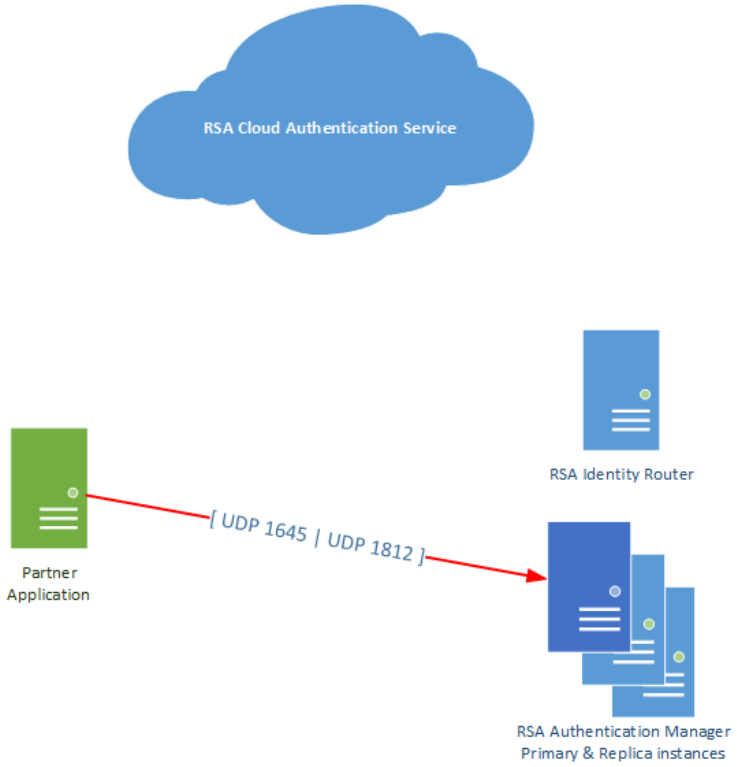
No known issues.

Integration Configuration

RADIUS with AM

This section describes how to integrate Forescout with RSA Authentication Manager using RADIUS.

Architecture Diagram



Configure 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.

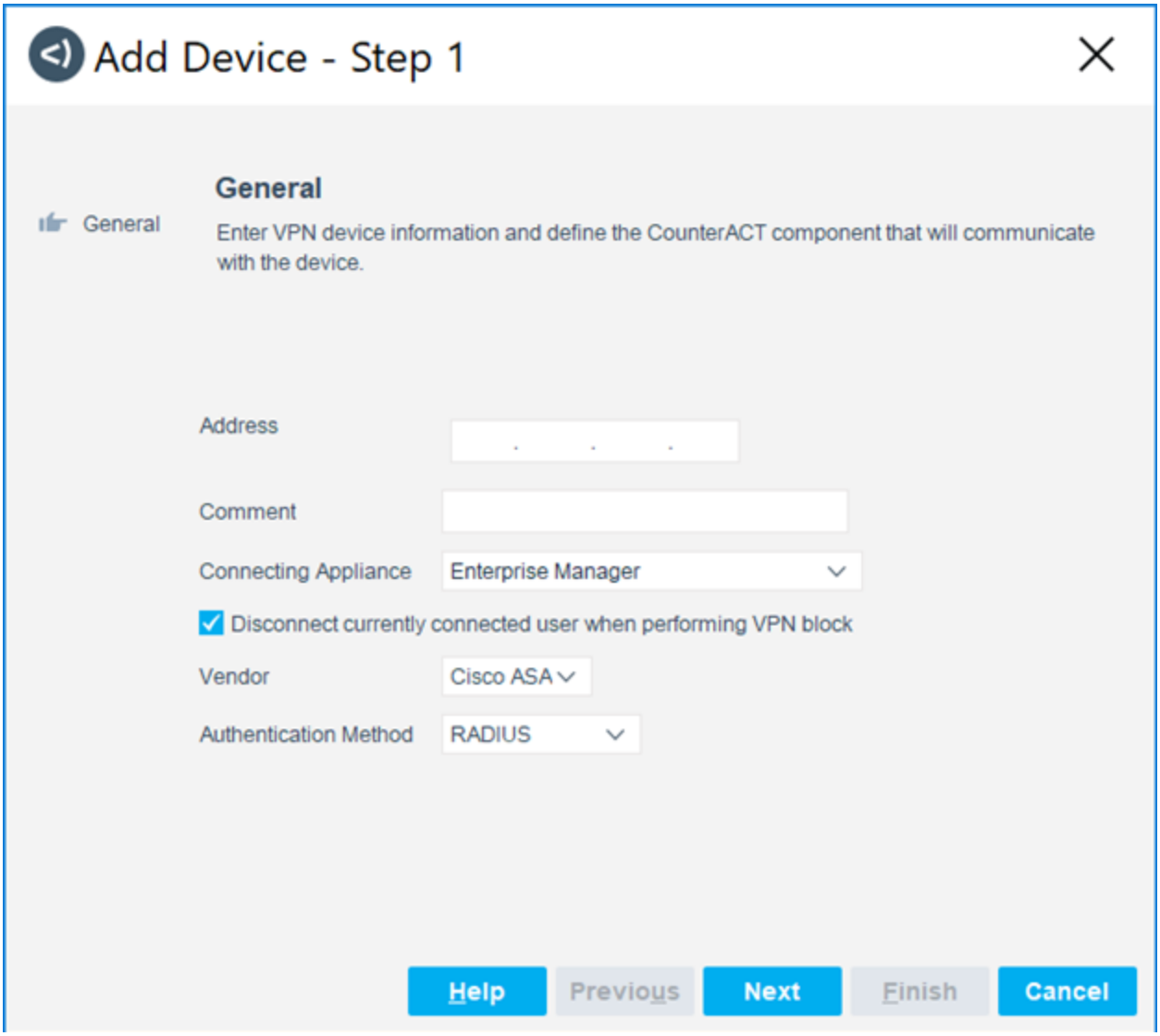
Configure Forescout

Perform these steps to configure Forescout as a RADIUS client to RSA Authentication Manager.

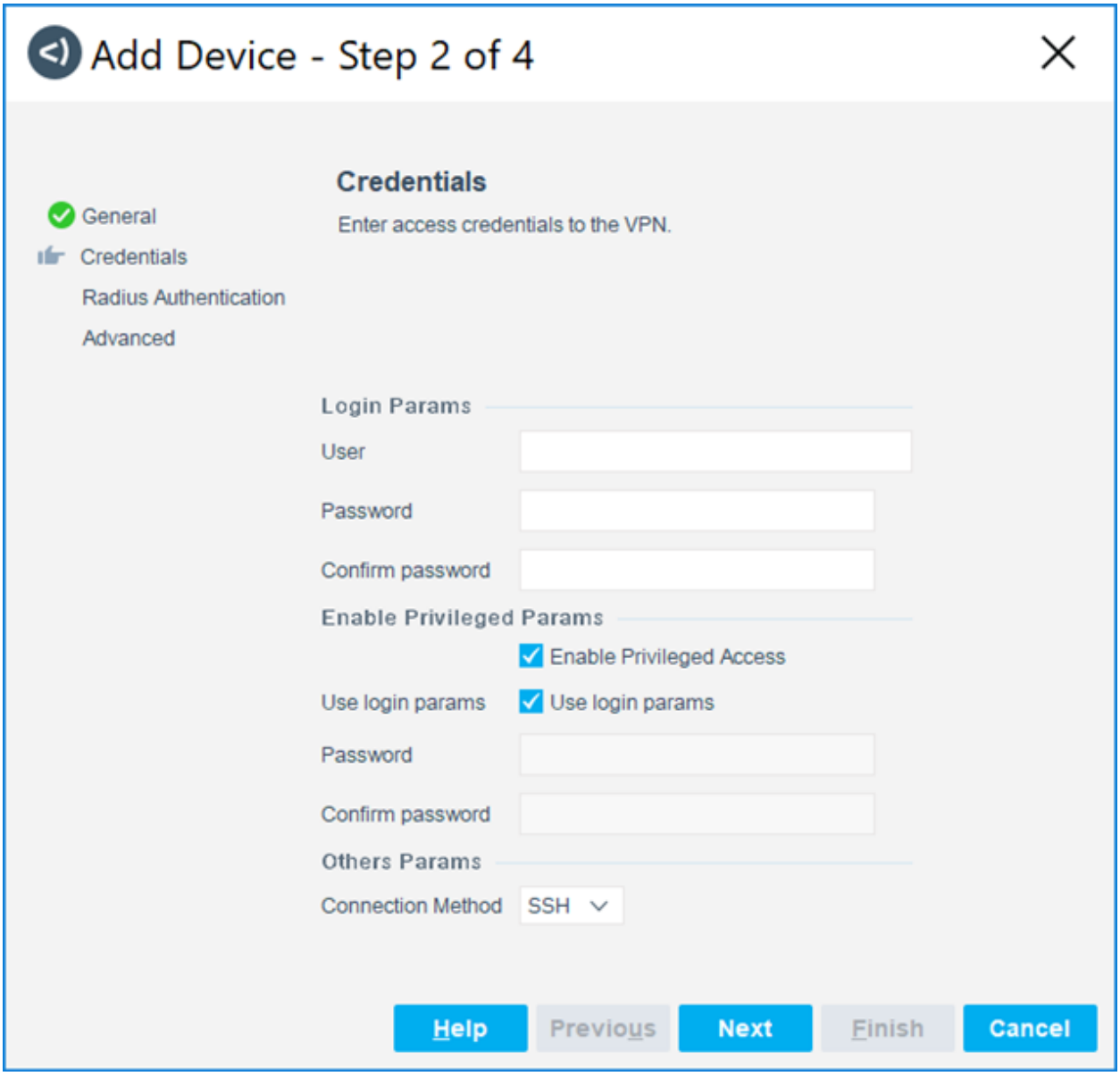
Procedure

1. Sign in to Forescout admin console and click **Options**> **Tools** > **VPN** and click **Add**.

2. Add the Cisco ASA device information and click **Next**.



3. Configure the access credentials for the Cisco ASA and click **Next**.



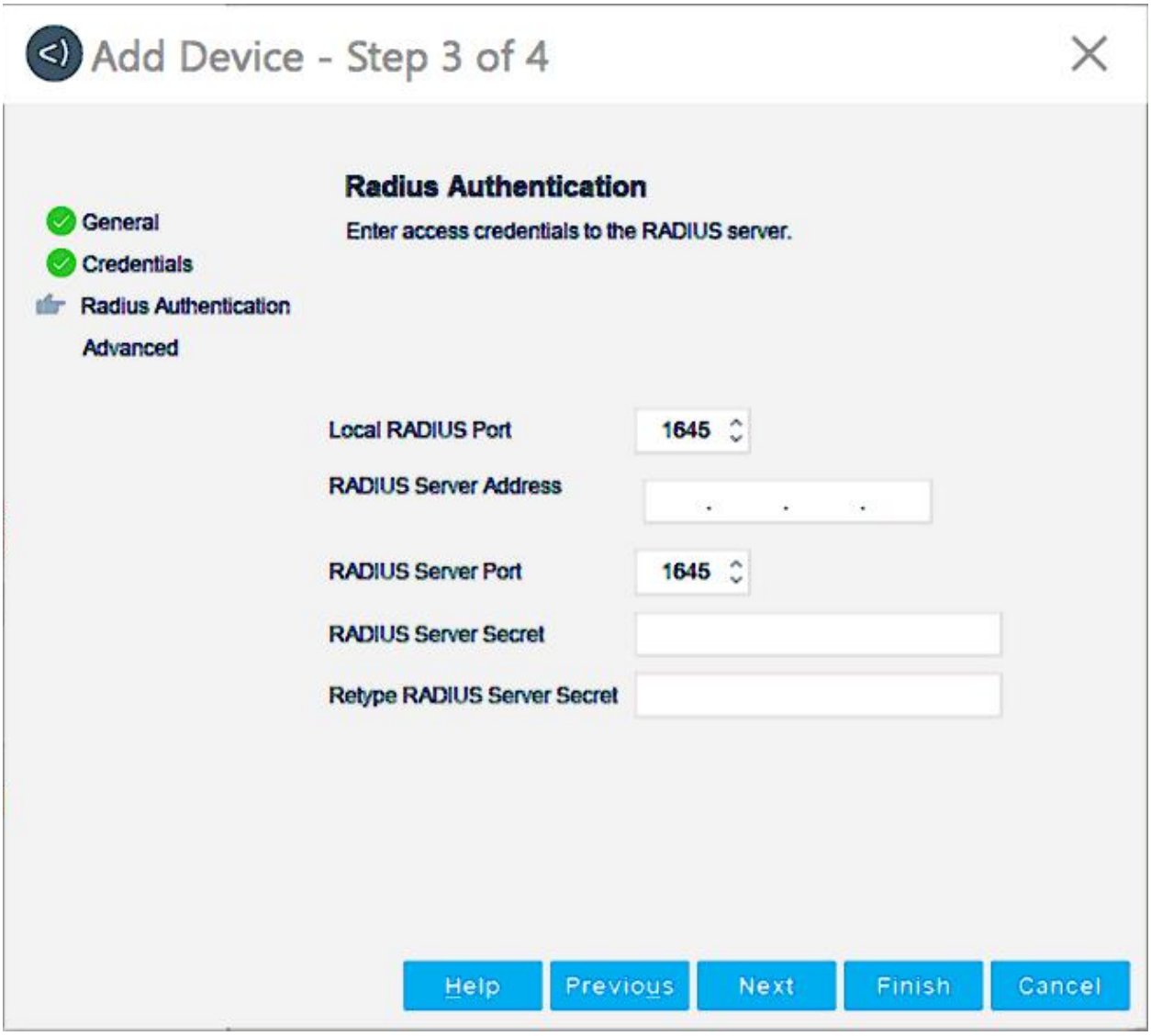
4. Configure the RSA Authentication Manager RADIUS settings and click **Finish**.

   a. **Local RADIUS Port**: This should match the RADIUS port as configured on Cisco ASA.

   b. **RADIUS Server Address**: Enter the IP address of the RSA Authentication Manager server.

   c. **RADIUS Server Port**: Enter 1812 or 1645.

   d. **RADIUS Shared Secret**: Enter the RADIUS shared secret as specified in the RADIUS client in RSA Authentication Manager Security Console.



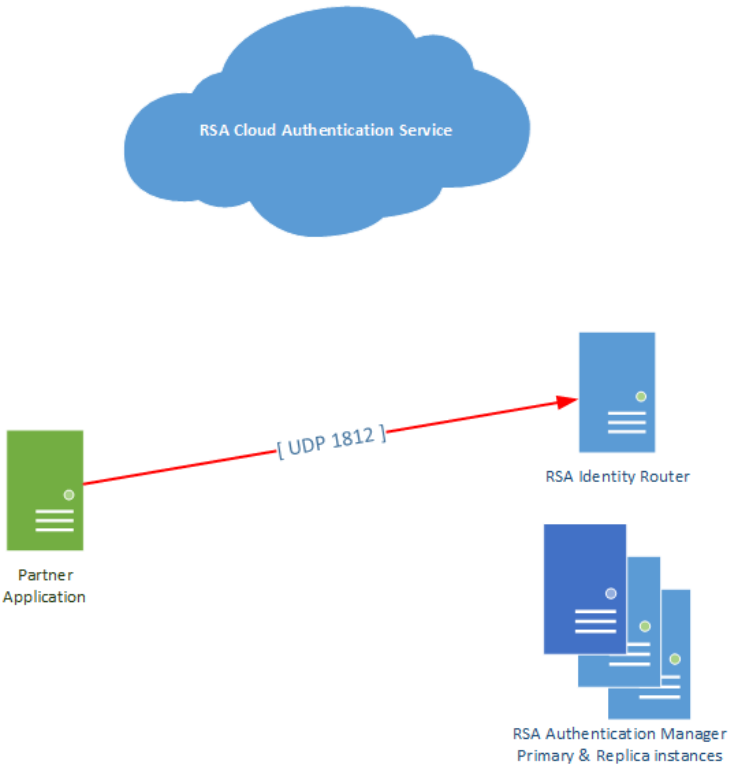
Configuration is complete

Return to the main page for more certification related information.

RADIUS with CAS

This section describes how to integrate Forescout with RSA Cloud Authentication Service using RADIUS.

Architecture Diagram



Configure 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.

Sin into 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**.

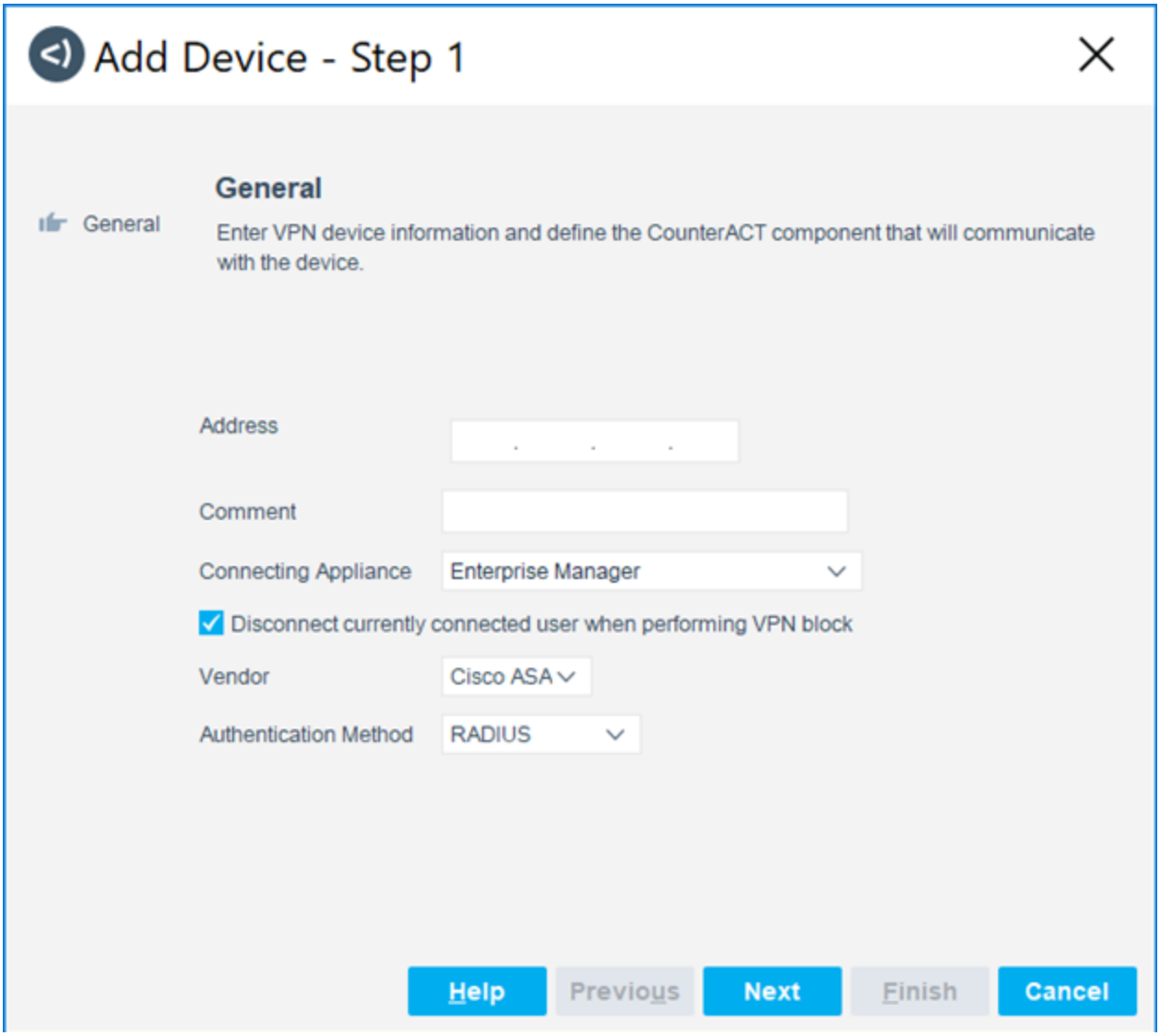
Configure Forescout

Perform these steps to configure Forescout Forescout as a RADIUS client to RSA Cloud Authentication Service.

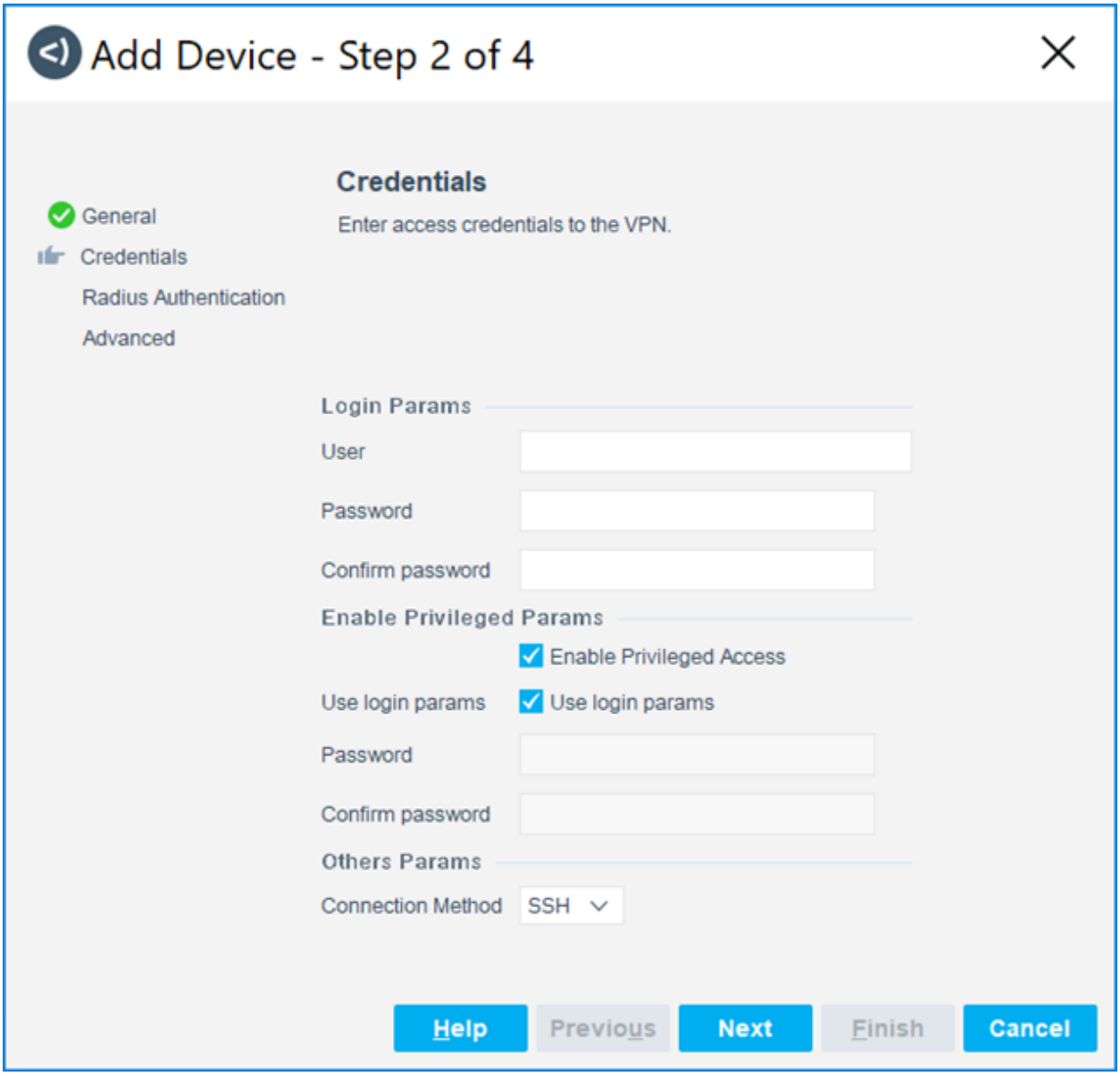
Procedure

Sign in to Forescout admin console and click **Options**> **Tools** > **VPN** and click **Add**.

2. Add the Cisco ASA device information and click **Next**.



3. Configure the access credentials for the Cisco ASA and click **Next**.



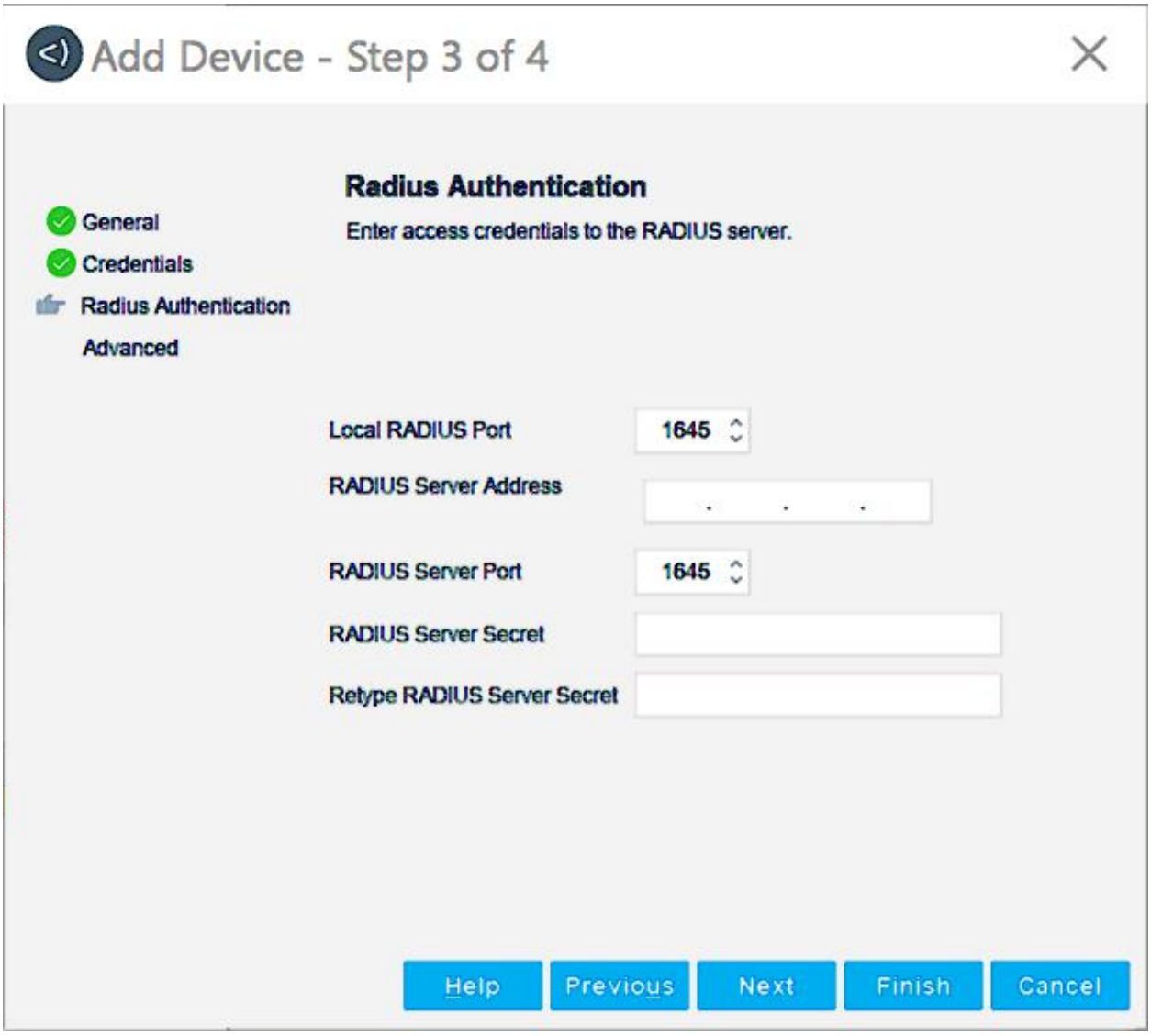
4. Configure the RSA Authentication Manager RADIUS settings and click **Finish**.

   a. **Local RADIUS Port**: This should match the RADIUS port as configured on Cisco ASA.

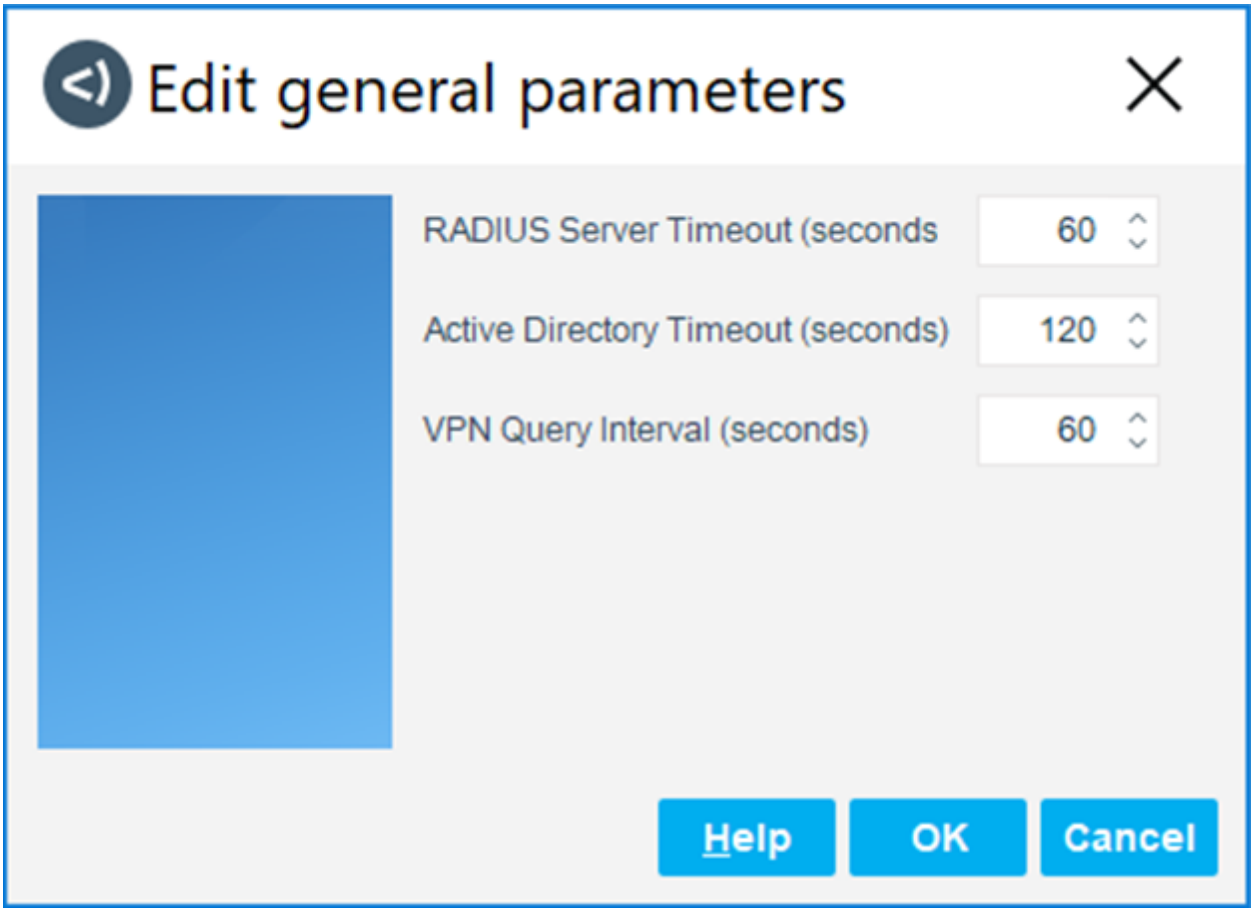
   b. **RADIUS Server Address**: Enter the IP address of the RSA Identity Router.

   c. **RADIUS Server Port**: Enter 1812.

   d. **RADIUS Shared Secret**: Enter the RADIUS shared secret as specified in the RADIUS client in RSA Cloud Administration Console.



5. Click **Options** from the VPN pane, change **RADIUS Server Timeout** to 60 and click **OK**.



Configuration is complete

Return to the main page for more certification related information.