RSA Ready Implementation Guide for RSA SecurID

Cisco Secure ACS 5.8

Peter Waranowski, RSA Partner Engineering
Last Modified: October 14th, 2016

RSA READY

Solution Summary

Cisco Secure Access Control Server (ACS) is an access control server that provides an identity-based networking solution to enterprise customers for network access (wired, wireless, remote access) and device administration.

Cisco Secure ACS can be configured to communicate with RSA Authentication Manager via both RADIUS and RSA native SecurID protocols. This integration enables RSA's two factor authentication for users accessing Cisco Secure ACS protected network resources.

RSA Authentication Manager supported features	
Cisco Secure ACS 5.8	
RSA SecurID Authentication via Native RSA SecurID UDP Protocol	Yes
RSA SecurID Authentication via Native RSA SecurID TCP Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
RSA SecurID Authentication via IPv6	No
On-Demand Authentication via Native SecurID UDP Protocol	Yes
On-Demand Authentication via Native SecurID TCP Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	No
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No

RSA Authentication Manager Configuration

Agent Host Configuration

To facilitate communication between Cisco Secure ACS and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies Cisco Secure ACS and contains information about communication and encryption.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

> **Important: The UDP-based authentication agent's hostname must resolve to the IP address specified.**

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with Cisco Secure ACS will occur.

If Cisco Secure ACS will be communicating with RSA Authentication Manager via RADIUS, then a RADIUS client that corresponds to the agent host record must be created in the RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

> **Important: The RADIUS client's hostname must resolve to the IP address specified.**

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Cisco Secure ACS 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.

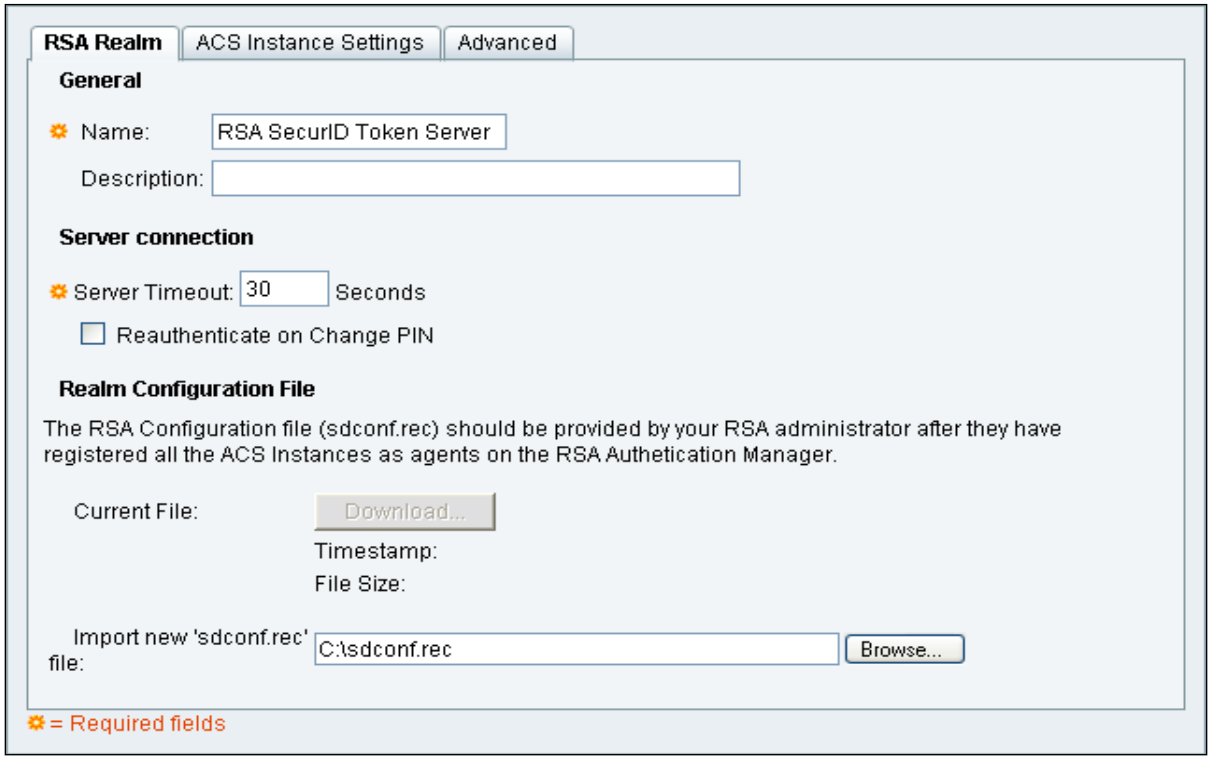
All Cisco Secure ACS components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuring the Cisco ACS for SecurID Authentication

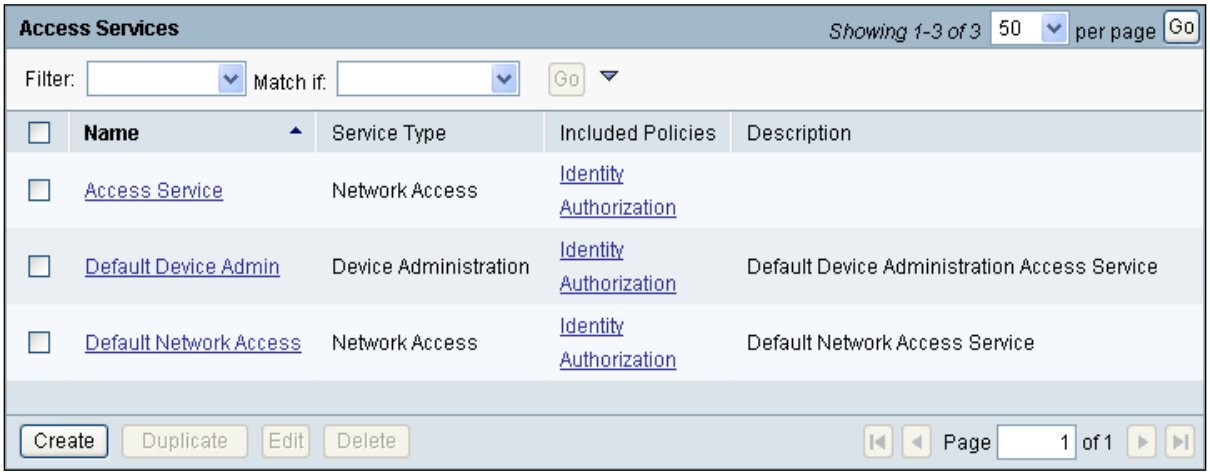
Cisco Secure ACS supports RSA SecurID authentication using both RADIUS and RSA's native SecurID protocol.

Configure SecurID Authentication using native SecurID protocol

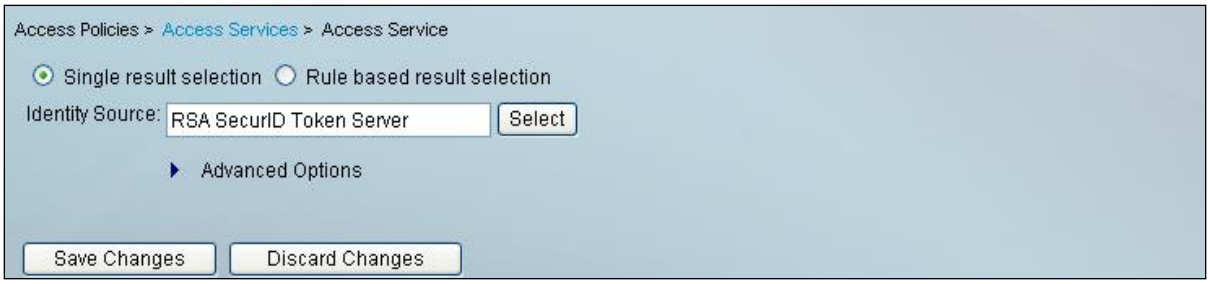
1. Browse to **Users and Identity Stores** > **External Identity Stores** > **RSA SecurID Token Servers** and click **Create**.
2. Specify a name for your RSA SecurID Token Server, the path to sdconf.rec configuration file and click **Submit**.



3. Browse to **Access Policies** > **Access Services**. Edit the **Identity Policy** within the **Access Service** for which you are implementing SecurID authentication.



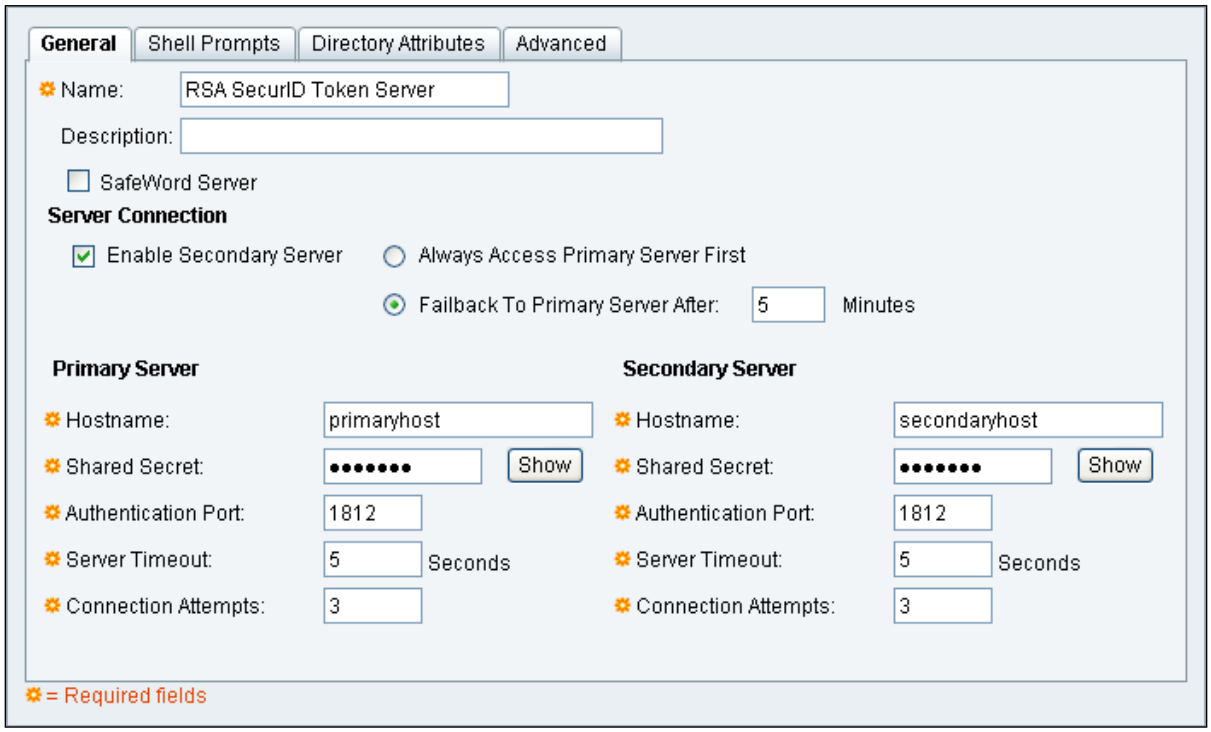
4. Set the **Identity Source** to the RSA SecurID Token Server created in Step 1, and click **Save Changes**.



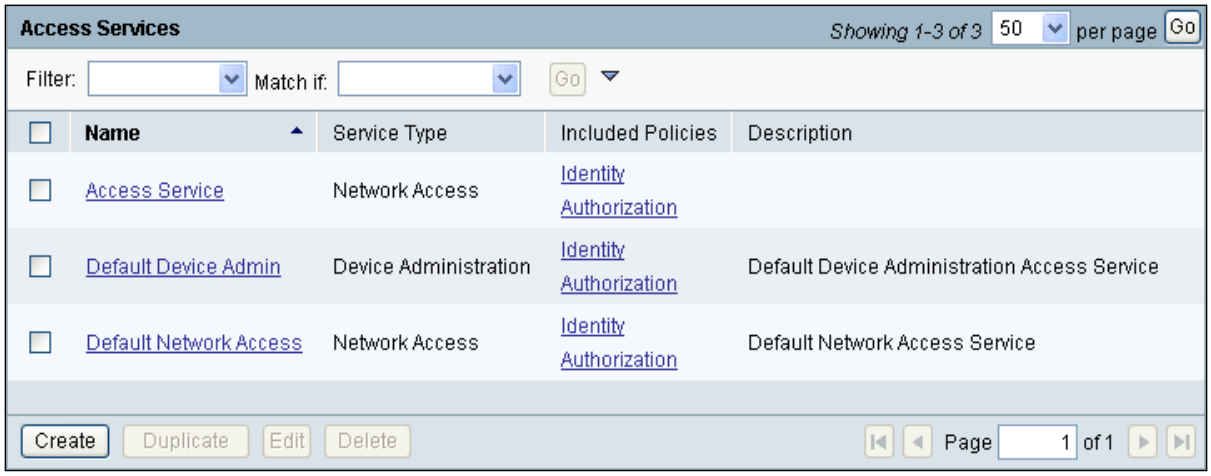
Cisco Secure ACS is now configured for authentication with the RSA SecurID Token Server over the RSA native SecurID protocol.

Configure SecurID Authentication using RADIUS protocol

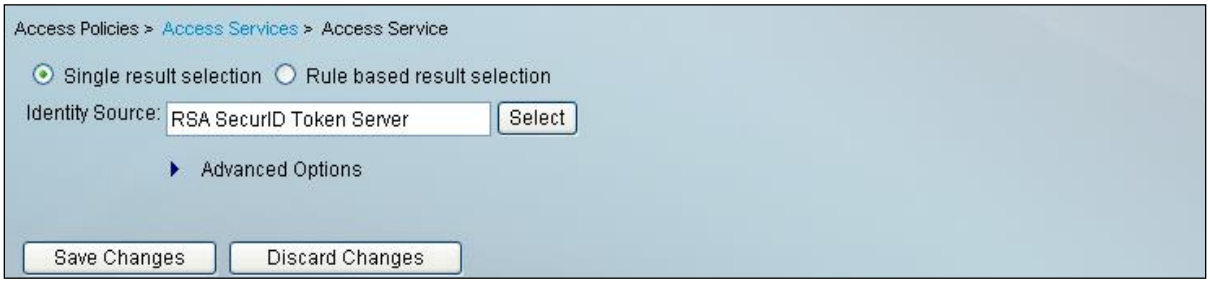
1. Browse to **Users and Identity Stores** > **External Identity Stores** > **RADIUS Identity Servers** and click **Create.**
2. Specify a **Name** for the SecurID Authentication Server. Enter the **Hostname** and **Shared Secret** for the primary server. Enter **Hostname** and **Shared Secret** for the Secondary Server if applicable. Click **Submit**.



3. Browse to **Access Policies** > **Access Services**. Edit the **Identity Policy** within the **Access Service** for which you are implementing SecurID authentication.



4. Set the **Identity Source** to the RSA SecurID Token Server created in Step 1 and click **Save Changes**.



Cisco Secure ACS is now configured for authentication with the RSA SecurID Token Server over the RADIUS protcol.

Certification Checklist for RSA Authentication Manager

Date Tested: October 14th, 2016

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.2	Virtual Appliance
Cisco Secure ACS	5.8.032	Virtual Appliance

RSA SecurID Authentication

Date Tested: October 14th, 2016

Mandatory Functionality	Native UDP	Native TCP	RADIUS Client
New PIN Mode			
Force Authentication After New PIN	✓	N/A	✓
System Generated PIN	✓	N/A	✓
User Defined (4-8 Alphanumeric)	✓	N/A	✓
User Defined (5-7 Numeric)	✓	N/A	✓
Deny 4 and 8 Digit PIN	✓	N/A	✓
Deny Alphanumeric PIN	✓	N/A	✓
Deny PIN Reuse	✓	N/A	✓
Passcode			
16 Digit Passcode	✓	N/A	✓
4 Digit Fixed Passcode	✓	N/A	✓
Next Tokencode Mode			
Next Tokencode Mode	✓	N/A	✓
On-Demand Authentication			
On-Demand Authentication	✓	N/A	✓
On-Demand New PIN	✓	N/A	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	✓	N/A	✓
No RSA Authentication Manager	✓	N/A	✓

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

Appendix

RSA SecurID Authentication Files

RSA SecurID Authentication Files	
UDP Agent Files	**Location**
sdconf.rec	In Memory
sdopts.rec	In Memory
Node secret	In Memory
sdstatus.12 / jastatus.12	In Memory
TCP Agent Files	**Location**
rsa_api.properties	N/A
sdconf.rec	N/A
sdopts.rec	N/A
Node secret	N/A

Partner Integration Details

Partner Integration Details	
RSA SecurID UDP API	6.1; 8.1.1 starting in 5.3 Patch 1
RSA SecurID TCP API	N/A
RSA Authentication Agent Type	Standard Agent
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

API Details:

Cisco Secure ACS 5.3 includes RSA Authentication API 6.1 to perform Native RSA SecurID Authentication. Cisco Secure ACS 5.3 Patch 1 includes the RSA Authentication API 8.1.1. The node secret format is updated to work with the new API as part of the patch installation without user interaction. This process should be completely seamless to the user, but should it fail, it will necessary to clear and create a new node secret using the new libraries. Cisco Secure ACS 5.4 and newer include the RSA Authentication API 8.1.1 as part of the base install.

! Important: The RSA authentication libraries are updated during the installation of ACS 5.3 Patch 1.

Node Secret:

After the agent initially communicates with the RSA SecurID server, the server provides the agent with a node secret file called securid. The Node Secret is used for encrypting traffic between the RSA server and the authentication agent. At times, you might have to reset the node secret. To reset the node secret:

1. The RSA SecurID server administrator must uncheck the Node Secret Created check box on the Agent Host record in the RSA SecurID server.
2. The ACS administrator must remove the securid file from ACS. To remove the secured file from ACS:

   Browse to **User and Identity Stores** > **External Identity Stores** > **RSA SecurID Token Servers**

   1. **Edit** your specified RSA SecurID Token Server.
   2. Open the **ACS Instance Settings** tab, and **Edit** the ACS Instance.
   3. Open the **Reset Agent Files** tab.

Mark the checkbox next to **Remove securid file on submit**, and click **Submit**.

sdopts.rec:

You can enable the RSA options file (*sdopts.rec*) on each ACS instance to control routing priorities for connections between the RSA agent and the RSA servers in the realm. To enable RSA options:

Browse to **User and Identity Stores** > **External Identity Stores** > **RSA SecurID Token Servers**

1. **Edit** your specified RSA SecurID Token Server.
2. Open the **ACS Instance Settings** tab, and **Edit** the ACS Instance
3. From the **RSA Options File** tab, browse to the location of the sdopts.rec file, and click **OK**.

sdstatus.12:

When an RSA SecurID server is down, the automatic exclusion mechanism does not always work quickly. To speed up this process, you can remove the *sdstatus.12* file from ACS. To remove the sdstatus.12 file:

Browse to **User and Identity Stores** > **External Identity Stores** > **RSA SecurID Token Servers**

1. **Edit** your specified RSA SecurID Token Server.
2. Open the **ACS Instance Settings** tab, and **Edit** the ACS Instance.
3. Open the **Reset Agent Files** tab.
4. Mark the checkbox next to **Remove sdstatus.12 file on submit**, and click **Submit**.