

# Cisco ACS 5.X Integration with RSA SecurID Token Server



Document ID: 117038

Contributed by Anubhav Gupta, Cisco TAC Engineer.  
Jan 16, 2014

## Contents

### Introduction

### Background Information

### Prerequisites

- Requirements

- Components Used

### Configurations

- RSA Server

- ACS Version 5.X Server

### Verify

- ACS Version 5.X Server

- RSA Server

### Troubleshoot

- Create an Agent Record (sdconf.rec)

- Reset the Node Secret (securid)

- Override Automatic Load Balancing

- Manually Intervene to Remove a Down RSA SecurID Server

## Introduction

This document describes how to integrate a Cisco Access Control System (ACS) Version 5.x with RSA SecurID authentication technology.

## Background Information

The Cisco Secure ACS supports the RSA SecurID server as an external database.

RSA SecurID two-factor authentication consists of the user's personal identification number (PIN) and an individually registered RSA SecurID token that generates single-use token codes based on a time code algorithm.

A different token code is generated at fixed intervals, usually every 30 or 60 seconds. The RSA SecurID server validates this dynamic authentication code. Each RSA SecurID token is unique, and it is not possible to predict the value of a future token based on past tokens.

Thus, when a correct token code is supplied together with a PIN, there is a high degree of certainty that the person is a valid user. Therefore, RSA SecurID servers provide a more reliable authentication mechanism than conventional reusable passwords.

You can integrate a Cisco ACS 5.x with RSA SecurID authentication technology in these ways:

- RSA SecurID agent – Users are authenticated with username and passcode through the native RSA protocol.
- RADIUS protocol – Users are authenticated with username and passcode through the RADIUS protocol.

## Prerequisites

## Requirements

Cisco recommends that you have basic knowledge of these topics:

- RSA security
- Cisco Secure Access Control System (ACS)

## Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Access Control System (ACS) Version 5.x
- RSA SecurID Token Server

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

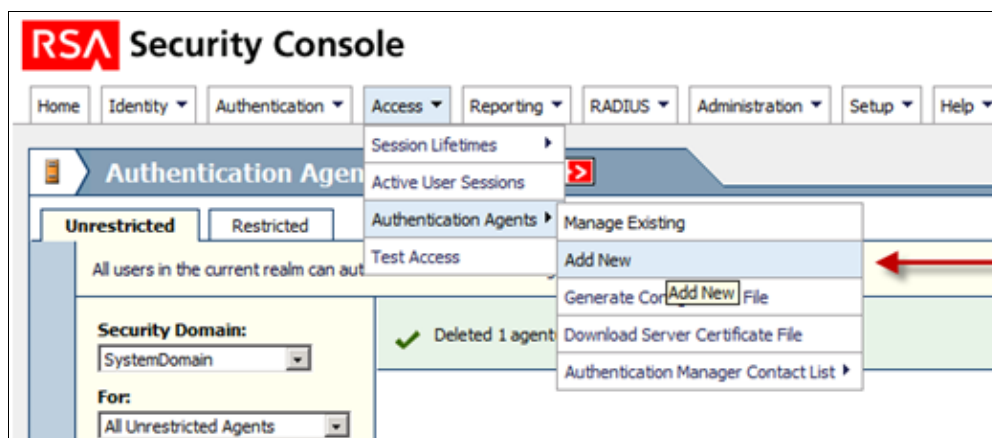
## Configurations

### RSA Server

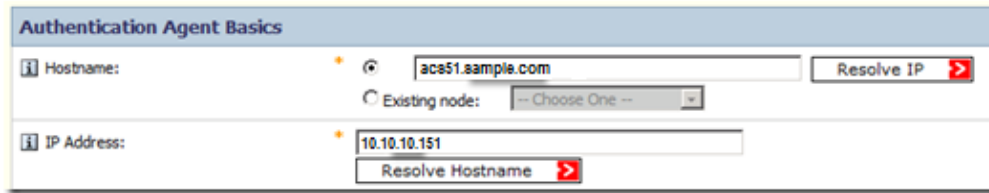
This procedure describes how the RSA SecurID server administrator creates authentication agents and a configuration file. An authentication agent is basically a Domain Name Server (DNS) name and an IP address of a device, software, or service that has rights to access the RSA database. The configuration file basically describes RSA topology and communication.

In this example, the RSA administrator must create two agents for the two ACS instances.

1. In the RSA Security Console, navigate to *Access > Authentication Agents > Add New*:

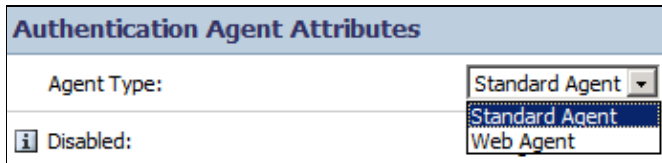


2. In the Add New Authentication Agent window, define a Hostname and IP Address for each of the two agents:

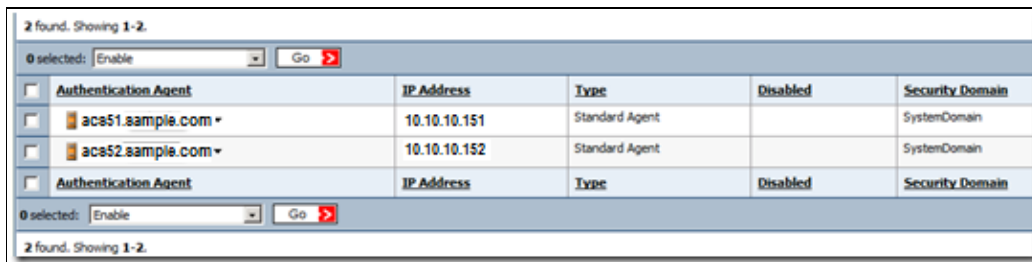


Both DNS forward and reverse lookups for ACS agents should work.

3. Define the Agent Type as Standard Agent:

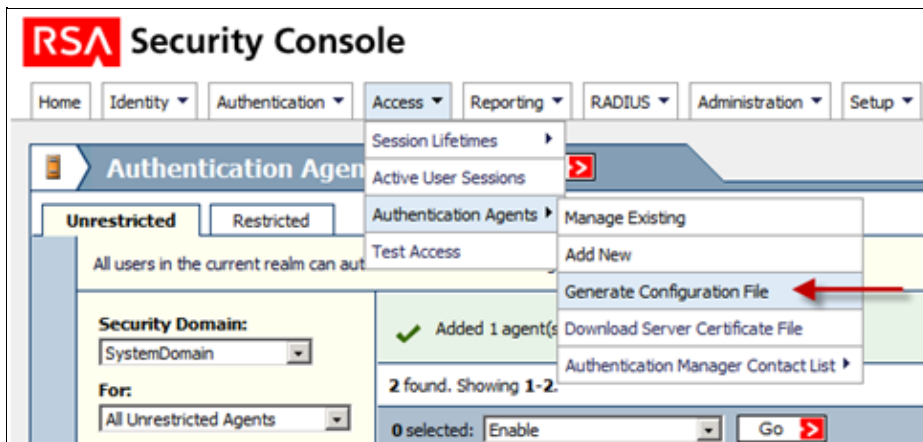


This is an example of the information you see once the agents are added:







Authentication Agent	IP Address	Type	Disabled	Security Domain
acs51.sample.com	10.10.10.151	Standard Agent		SystemDomain
acs52.sample.com	10.10.10.152	Standard Agent		SystemDomain

4. In the RSA Security Console, navigate to *Access > Authentication Agents > Generate Configuration File* in order to generate the sdconf.rec configuration file:





5. Use the default values for Maximum Retries and Maximum Time Between Each Retry:

Cancel  Reset  Generate Config File  

---

**Agent Timeout and Retries**




 Maximum Retries: Allow  attempts before timing out

 Maximum Time Between Each Retry: Allow  seconds between each attempt

---

**Communication Services**

The agents will communicate with the Authentication Manager server using the following service r



 Authentication Service:	Name: securid Port: 5500 Protocol: udp
 Agent Auto-Registration Service:	Name: rsaadmin Port: 5550 Protocol: tcp
 Offline Authentication Download Service:	Name: rsaoad Port: 5580 Protocol: tcp

6. Download the configuration file:

**Download File**

The file is ready to download. When prompted, select **Save it to disk** to save the ZIP file to your local machine.

Filename: AM\_Config.zip

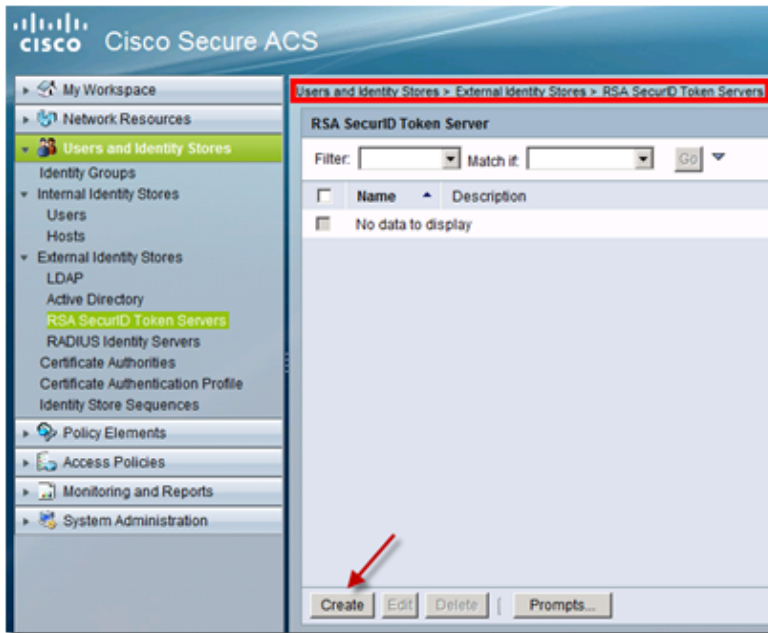
Download: [Download Now](#)  

The .zip file contains the actual configuration sdconf.rec file, which the ACS administrator needs in order to complete configuration tasks.

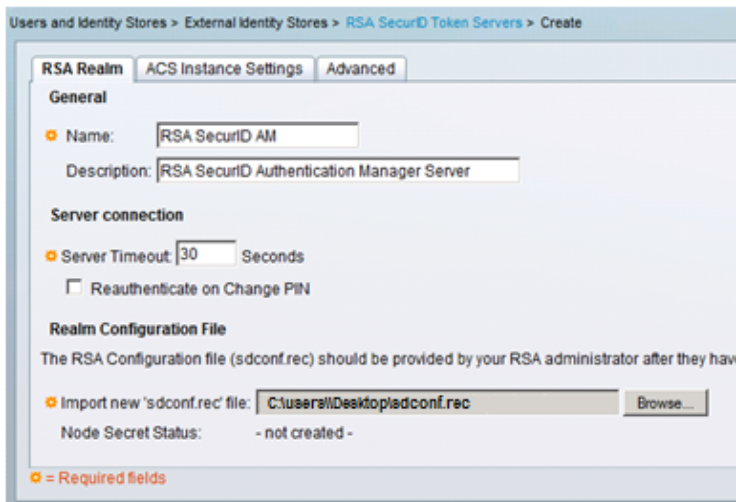
## ACS Version 5.X Server

This procedure describes how the ACS administrator retrieves and submits the configuration file.

1. In the Cisco Secure ACS Version 5.x console, navigate to *Users and Identity Stores > External Identity Stores > RSA SecurID Token Servers*, and click *Create*:



2. Enter the name of the RSA server, and browse to the `sdconf.rec` file that was downloaded from the RSA server:



3. Select the file, and click **Submit**.

**Note:** The first time the ACS contacts the token server, another file, called the node secret file, is created for the ACS agent on the RSA Authentication Manager and is downloaded to the ACS. This file is used for encrypted communication.

## Verify

Use this section in order to confirm that your configuration works properly.

### ACS Version 5.X Server

In order to verify a successful login, go to the ACS console, and review the Hit Count:

Access Policies > Access Services > Service Selection Rules

Single result selection  Rule based result selection

**Service Selection Policy**

Filter: Status Match if: Equals  Clear Filter Go

	Status	Name	Protocol	Conditions	Results	Hit Count
				NDG.Device Type	Service	
1	<input checked="" type="checkbox"/>	Rule-4	-ANY-	In All Device Types:SWITCHES	RSA Device Admin	2

You can also review the Authentication Details from the ACS logs:

Authentication Details	
Status:	Passed
Failure Reason:	
Logged At:	Feb 16, 2013 12:24 PM
ACS Time:	Feb 16, 2013 12:24 PM
ACS Instance:	acs51
Authentication Method:	PAP_ASCII
Authentication Type:	ASCII
Privilege Level:	1
<b>User</b>	
Username:	TEST1
Remote Address:	
<b>Network Device</b>	
Network Device:	SwitchBNNZ231
Network Device IP Address:	
Network Device Groups:	Device Type:All Device Types:SWITCHES:SWITCHES_SSH, Location:All Locations:DATACENTER_BN
<b>Access Policy</b>	
Access Service:	RSA Device Admin
Identity Store:	RSA SecurID AM
Selected Shell Profile:	PRIVILEGE_15
Active Directory Domain:	
Identity Group:	
Access Service Selection Matched Rule :	Rule-4

## RSA Server

In order to verify successful authentication, go to the RSA console, and review the logs:

Time	Activity Key	Description	Reason	User ID	Agent	Server Node IP	Client IP
2013-02-16 12:35:28.764	Principal authentication	User attempted to authenticate using authenticator "SecurID_Native". The user belongs to security domain "MediumSecurityDomain"	Authentication method success	TEST1	acs51.sample.com	10.10.10.211	10.10.10.151

## Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

### Create an Agent Record (sdconf.rec)

In order to configure an RSA SecurID token server in ACS Version 5.3, the ACS administrator must have the sdconf.rec file. The sdconf.rec file is a configuration record file that specifies how the RSA agent

communicates with the RSA SecurID server realm.

In order to create the `sdconf.rec` file, the RSA administrator should add the ACS host as an agent host on the RSA SecurID server and generate a configuration file for this agent host.

## Reset the Node Secret (securid)

After the agent initially communicates with the RSA SecurID server, the server provides the agent with a node secret file called `securid`. Subsequent communication between the server and the agent relies on the exchange of the node secret in order to verify the other's authenticity.

At times, the administrators might have to reset the node secret:

1. The RSA 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 the ACS.

## Override Automatic Load Balancing

The RSA SecurID agent automatically balances the requested loads on the RSA SecurID servers in the realm. However, you have the option to manually balance the load. You can specify the server used by each of the agent hosts. You can assign a priority to each server so that the agent host directs authentication requests to some servers more frequently than others.

You must specify the priority settings in a text file, save it as `sdopts.rec`, and upload it to the ACS.

## Manually Intervene to Remove a Down RSA SecurID Server

When an RSA SecurID server is down, the automatic exclusion mechanism does not always work quickly. Remove the `sdstatus.12` file from the ACS in order to speed up this process.