

Integración de Cisco ACS 5.X con el servidor de token RSA SecurID

Contenido

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuraciones](#)

[Servidor RSA](#)

[Servidor ACS versión 5.X](#)

[Verificación](#)

[Servidor ACS versión 5.X](#)

[Servidor RSA](#)

[Troubleshoot](#)

[Crear un registro de agente \(sdconf.rec\)](#)

[Restablecer el secreto de nodo \(securid\)](#)

[Anular equilibrio de carga automático](#)

[Intervenir manualmente para eliminar un servidor RSA SecurID caído](#)

Introducción

Este documento describe cómo integrar un Cisco Access Control System (ACS) versión 5.x con la tecnología de autenticación RSA SecurID.

Antecedentes

Cisco Secure ACS admite el servidor RSA SecurID como base de datos externa.

La autenticación de dos factores RSA SecurID consiste en el número de identificación personal (PIN) del usuario y un token RSA SecurID registrado individualmente que genera códigos de token de un solo uso basados en un algoritmo de código de tiempo.

Se genera un código de token diferente a intervalos fijos, normalmente cada 30 o 60 segundos. El servidor RSA SecurID valida este código de autenticación dinámica. Cada token RSA SecurID es único y no es posible predecir el valor de un token futuro basado en tokens anteriores.

Por lo tanto, cuando se proporciona un código de token correcto junto con un PIN, hay un alto grado de certeza de que la persona es un usuario válido. Por lo tanto, los servidores RSA SecurID proporcionan un mecanismo de autenticación más fiable que las contraseñas reutilizables

convencionales.

Puede integrar un Cisco ACS 5.x con la tecnología de autenticación RSA SecurID de las siguientes maneras:

- Agente RSA SecurID: los usuarios se autentican con nombre de usuario y código de acceso a través del protocolo RSA nativo.
- Protocolo RADIUS: los usuarios se autentican con el nombre de usuario y el código de acceso a través del protocolo RADIUS.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Access Control System (ACS) versión 5.x
- Servidor Token SecurID RSA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

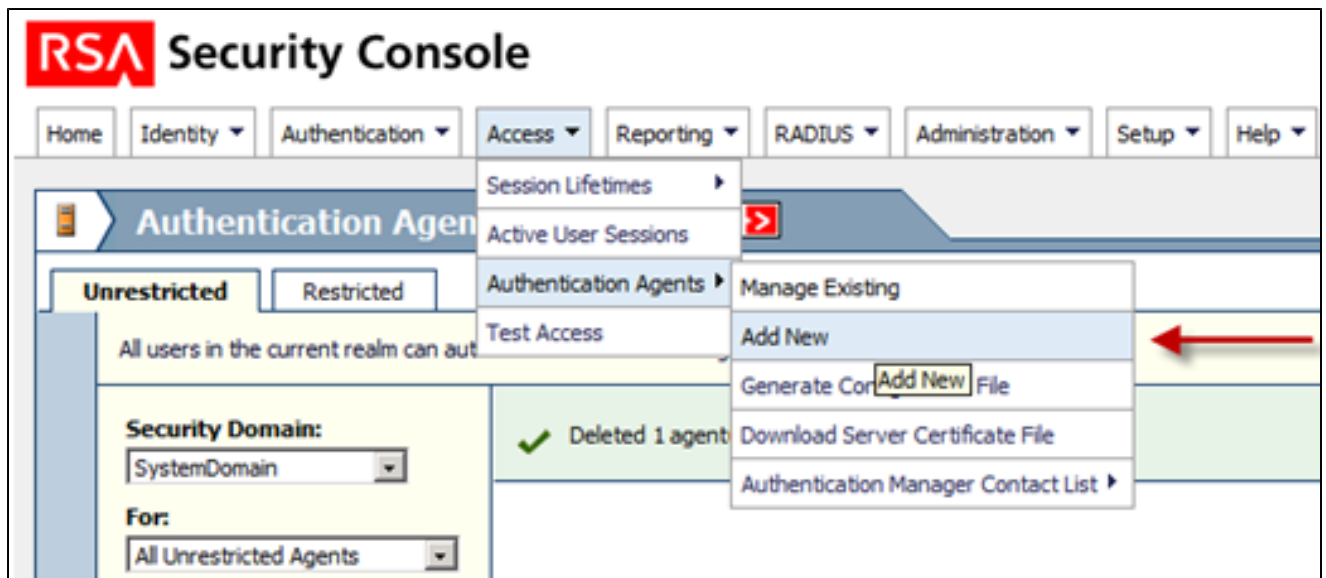
Configuraciones

Servidor RSA

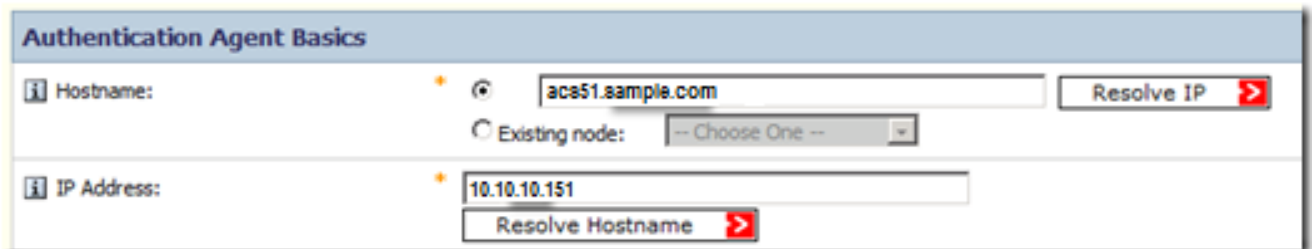
Este procedimiento describe cómo el administrador del servidor RSA SecurID crea agentes de autenticación y un archivo de configuración. Un agente de autenticación es básicamente un nombre de servidor de nombres de dominio (DNS) y una dirección IP de un dispositivo, software o servicio que tiene derechos de acceso a la base de datos RSA. El archivo de configuración describe básicamente la topología y la comunicación RSA.

En este ejemplo, el administrador RSA debe crear dos agentes para las dos instancias de ACS.

1. En la Consola de Seguridad RSA, navegue hasta Access > Authentication Agents > Add New:

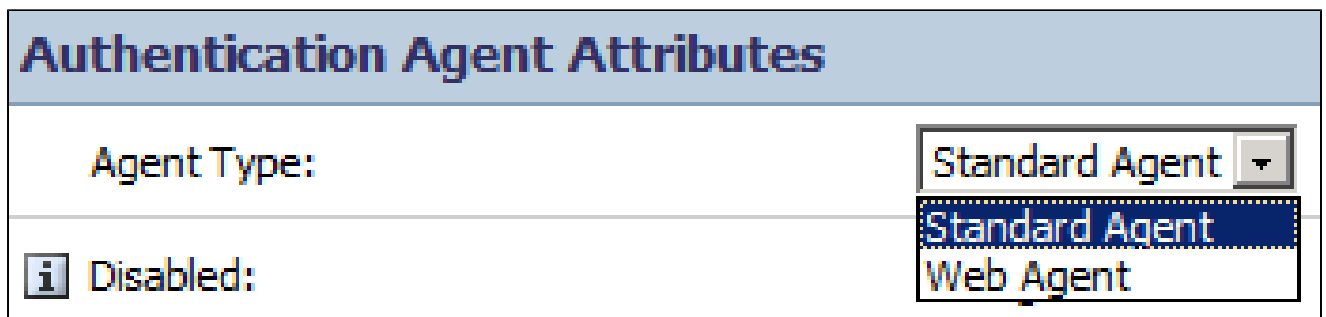


2. En la ventana Add New Authentication Agent , defina un nombre de host y una dirección IP para cada uno de los dos agentes:



Las búsquedas directas e inversas de DNS para agentes ACS deberían funcionar.

3. Defina el tipo de agente como agente estándar:



Este es un ejemplo de la información que se ve una vez que se agregan los agentes:

2 found. Showing 1-2.

0 selected: Enable

<input type="checkbox"/>	Authentication Agent	IP Address	Type	Disabled	Security Domain
<input type="checkbox"/>	acs51.sample.com	10.10.10.151	Standard Agent		SystemDomain
<input type="checkbox"/>	acs52.sample.com	10.10.10.152	Standard Agent		SystemDomain
<input type="checkbox"/>	Authentication Agent	IP Address	Type	Disabled	Security Domain

0 selected: Enable

2 found. Showing 1-2.

4. En la Consola de Seguridad RSA, navegue hasta Access > Authentication Agents > Generate Configuration File para generar el archivo de configuración sdconf.rec:

RSA Security Console

Home Identity Authentication Access Reporting RADIUS Administration Setup

Authentication Agents

Unrestricted Restricted

All users in the current realm can aut

Security Domain: SystemDomain

For: All Unrestricted Agents

0 selected: Enable

Session Lifetimes

Active User Sessions

Authentication Agents

Test Access

Manage Existing

Add New

Generate Configuration File





Download Server Certificate File

Authentication Manager Contact List


Added 1 agent(s)


2 found. Showing 1-2.

5. Utilice los valores predeterminados de Máximo de reintentos y Tiempo máximo entre cada reintento:

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: rsaadmind Port: 5550 Protocol: tcp
 Offline Authentication Download Service:	Name: rsaoad Port: 5580 Protocol: tcp

6. Descargue el archivo de configuración:

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

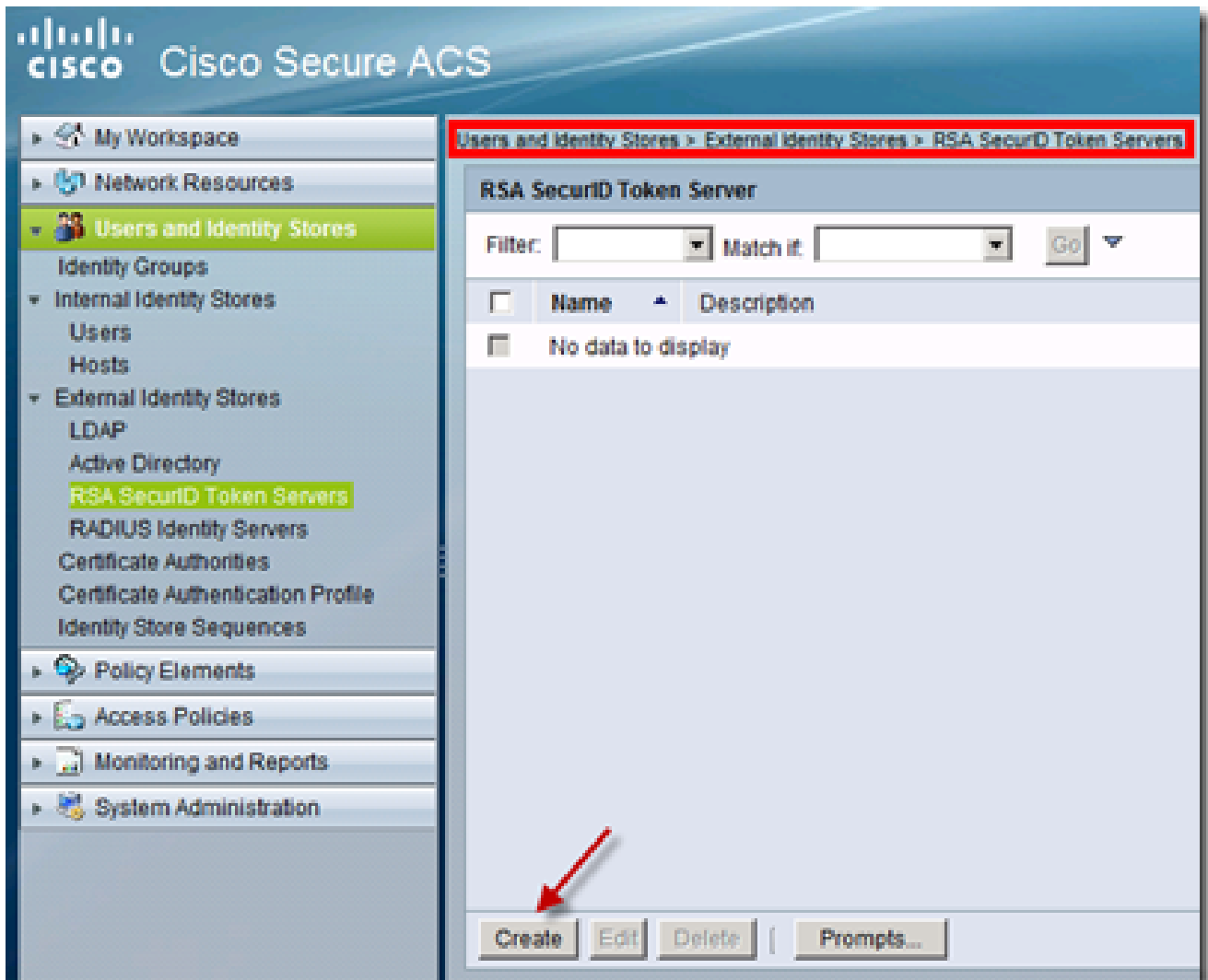
Download: [Download Now](#)  

El archivo .zip contiene el archivo sdconf.rec de configuración real, que el administrador ACS necesita para completar las tareas de configuración.

Servidor ACS versión 5.X

Este procedimiento describe cómo el administrador ACS recupera y envía el archivo de configuración.

1. En la consola de Cisco Secure ACS Version 5.x, navegue hasta Users and Identity Stores > External Identity Stores > RSA SecurID Token Servers, y haga clic en Create:



2. Introduzca el nombre del servidor RSA y busque el archivo sdconf.rec que se descargó del servidor RSA:

Users and Identity Stores > External Identity Stores > RSA SecurID Token Servers > Create

RSA Realm ACS Instance Settings Advanced

General

Name:

Description:

Server connection

Server Timeout: Seconds

Reauthenticate on Change PIN

Realm Configuration File

The RSA Configuration file (sdconf.rec) should be provided by your RSA administrator after they have

Import new 'sdconf.rec' file:

Node Secret Status: - not created -

= Required fields

3. Seleccione el archivo y haga clic en Enviar.

Nota: La primera vez que ACS se pone en contacto con el servidor de token, se crea otro archivo, llamado archivo node secret, para el agente ACS en el Administrador de autenticación RSA y se descarga en el ACS. Este archivo se utiliza para la comunicación cifrada.

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Servidor ACS versión 5.X

Para verificar un login exitoso, vaya a la consola ACS y revise el Hit Count:

Access Policies > Access Services > Service Selection Rules

Single result selection Rule based result selection

Service Selection Policy

Filter: Match if:


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

También puede revisar los detalles de autenticación de los registros ACS:

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

Servidor RSA

Para verificar la autenticación exitosa, vaya a la consola RSA y revise los registros:

Clear Monitor 							
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 <u>success</u>	TEST1	acs51.sample.com	10.10.10.211	10.10.10.151

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Crear un registro de agente (sdconf.rec)

Para configurar un servidor de token RSA SecurID en ACS Version 5.3, el administrador ACS debe tener el archivo sdconf.rec. El archivo sdconf.rec es un archivo de registro de configuración que especifica cómo se comunica el agente RSA con el rango del servidor RSA SecurID.

Para crear el archivo sdconf.rec, el administrador RSA debe agregar el host ACS como un host de agente en el servidor RSA SecurID y generar un archivo de configuración para este host de agente.

Restablecer el secreto de nodo (securid)

Después de que el agente se comunique inicialmente con el servidor RSA SecurID, el servidor proporciona al agente un archivo secreto de nodo denominado securid. La comunicación posterior entre el servidor y el agente se basa en el intercambio del secreto de nodo para verificar la autenticidad del otro.

En ocasiones, es posible que los administradores tengan que restablecer el secreto de nodo:

1. El administrador RSA debe desmarcar la casilla de verificación Node Secret Created en el registro Host de agente en el servidor RSA SecurID.
2. El administrador ACS debe quitar el archivo securid del ACS.

Anular equilibrio de carga automático

El agente RSA SecurID equilibra automáticamente las cargas solicitadas en los servidores RSA SecurID del dominio. Sin embargo, tiene la opción de equilibrar manualmente la carga. Puede especificar el servidor utilizado por cada uno de los hosts del agente. Puede asignar una prioridad a cada servidor para que el host del agente dirija las solicitudes de autenticación a algunos servidores con más frecuencia que a otros.

Debe especificar la configuración de prioridad en un archivo de texto, guardarlo como `sdopts.rec` y cargarlo en ACS.

Intervenir manualmente para eliminar un servidor RSA SecurID caído

Cuando un servidor RSA SecurID está inactivo, el mecanismo de exclusión automática no siempre funciona rápidamente. Quite el archivo `sdstatus.12` del ACS para acelerar este proceso.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).