

# Cisco ACS 5.X-Integration mit RSA SecurID Token Server

## Inhalt

[Einführung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurationen](#)

[RSA-Server](#)

[ACS 5.X-Server](#)

[Überprüfen](#)

[ACS 5.X-Server](#)

[RSA-Server](#)

[Fehlerbehebung](#)

[Erstellen eines Agent-Datensatzes \(sdconf.rec\)](#)

[Node Secret \(Sicher\) zurücksetzen](#)

[Überschreiben des automatischen Lastenausgleichs](#)

[Manuelles Eingreifen zum Entfernen eines RSA SecurID-Servers nach unten](#)

## Einführung

In diesem Dokument wird beschrieben, wie ein Cisco Access Control System (ACS) Version 5.x mit der RSA SecurID-Authentifizierungstechnologie integriert wird.

## Hintergrundinformationen

Der Cisco Secure ACS unterstützt den RSA SecurID-Server als externe Datenbank.

Die RSA SecurID-Zwei-Faktor-Authentifizierung besteht aus der persönlichen Identifikationsnummer (PIN) des Benutzers und einem einzeln registrierten RSA SecurID-Token, das auf der Grundlage eines Zeitcode-Algorithmus Tokencodes für eine einzelne Verwendung generiert.

Ein anderer Tokencode wird in festen Intervallen generiert, in der Regel alle 30 oder 60 Sekunden. Der RSA SecurID-Server validiert diesen dynamischen Authentifizierungscode. Jedes RSA SecurID-Token ist eindeutig, und es ist nicht möglich, den Wert eines zukünftigen Tokens auf der Grundlage früherer Token vorherzusagen.

Wenn also ein korrekter Tokencode zusammen mit einer PIN bereitgestellt wird, besteht eine hohe Sicherheit, dass die Person ein gültiger Benutzer ist. Aus diesem Grund bieten RSA SecurID-Server einen zuverlässigeren Authentifizierungsmechanismus als herkömmliche wiederverwendbare Passwörter.

Sie können Cisco ACS 5.x mit RSA SecurID-Authentifizierungstechnologien integrieren:

- RSA SecurID-Agent - Benutzer werden mithilfe des nativen RSA-Protokolls mit Benutzername und Passcode authentifiziert.
- RADIUS-Protokoll - Benutzer werden über das RADIUS-Protokoll mit Benutzername und Passcode authentifiziert.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

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

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

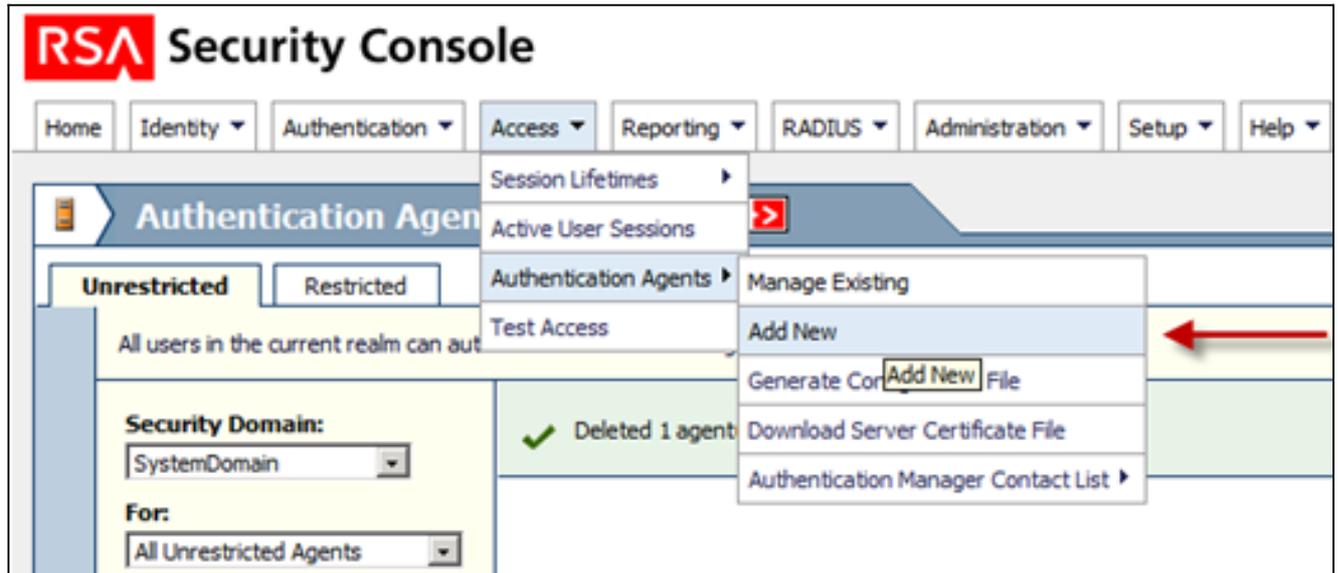
## Konfigurationen

### RSA-Server

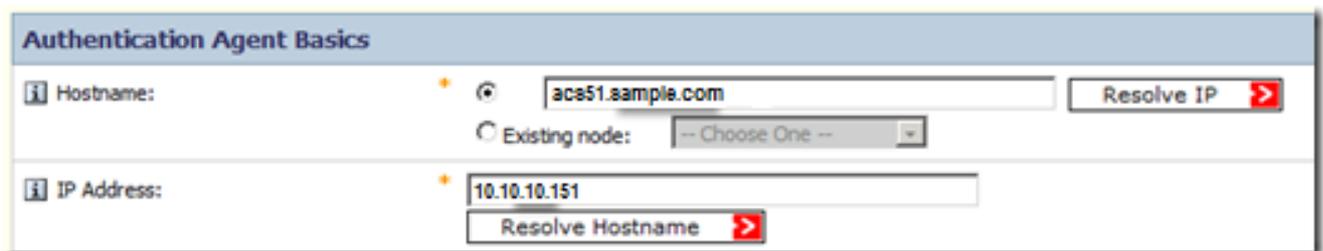
Dieses Verfahren beschreibt, wie der RSA SecurID-Serveradministrator Authentifizierungs-Agenten und eine Konfigurationsdatei erstellt. Ein Authentifizierungs-Agent ist im Prinzip ein Domänenname Server (DNS)-Name und eine IP-Adresse eines Geräts, einer Software oder eines Service, das über Zugriffsrechte für die RSA-Datenbank verfügt. Die Konfigurationsdatei beschreibt im Wesentlichen die RSA-Topologie und -Kommunikation.

In diesem Beispiel muss der RSA-Administrator zwei Agenten für die beiden ACS-Instanzen erstellen.

1. Navigieren Sie in der RSA-Sicherheitskonsole zu **Access > Authentication Agents > Add New**:



2. Definieren Sie im Fenster Add New Authentication Agent (Neuen Authentifizierungs-Agenten hinzufügen) einen Hostnamen und eine IP-Adresse für jeden der beiden Agenten:



Sowohl die DNS-Vorwärts- als auch die umgekehrte Suche nach ACS-Agenten sollte funktionieren.

3. Definieren Sie den Agent-Typ als Standard-Agent:



Dies ist ein Beispiel für die Informationen, die Sie nach dem Hinzufügen der Agenten sehen:

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. Navigieren Sie in der RSA-Sicherheitskonsole zu **Access > Authentication Agents > Generate Configuration File (Konfigurationsdatei generieren)**, um die Konfigurationsdatei sdconf.rec zu generieren:

The screenshot shows the RSA Security Console interface. The top navigation bar includes 'Home', 'Identity', 'Authentication', 'Access', 'Reporting', 'RADIUS', 'Administration', and 'Setup'. The 'Access' menu is expanded, showing options like 'Session Lifetimes', 'Active User Sessions', 'Authentication Agents', and 'Test Access'. The 'Authentication Agents' sub-menu is open, displaying 'Manage Existing', 'Add New', 'Generate Configuration File' (highlighted with a red arrow), 'Download Server Certificate File', and 'Authentication Manager Contact List'. The main content area shows 'Unrestricted' and 'Restricted' tabs, a 'Security Domain' dropdown set to 'SystemDomain', and a 'For:' dropdown set to 'All Unrestricted Agents'. A status message indicates 'Added 1 agent(s)'. At the bottom, there is a search bar with '0 selected: Enable' and a 'Go' button.

5. Verwenden Sie die Standardwerte für die maximale Wiederholungszahl und die maximale Zeitspanne zwischen den einzelnen Wiederholungen:

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. Laden Sie die Konfigurationsdatei herunter:

### 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

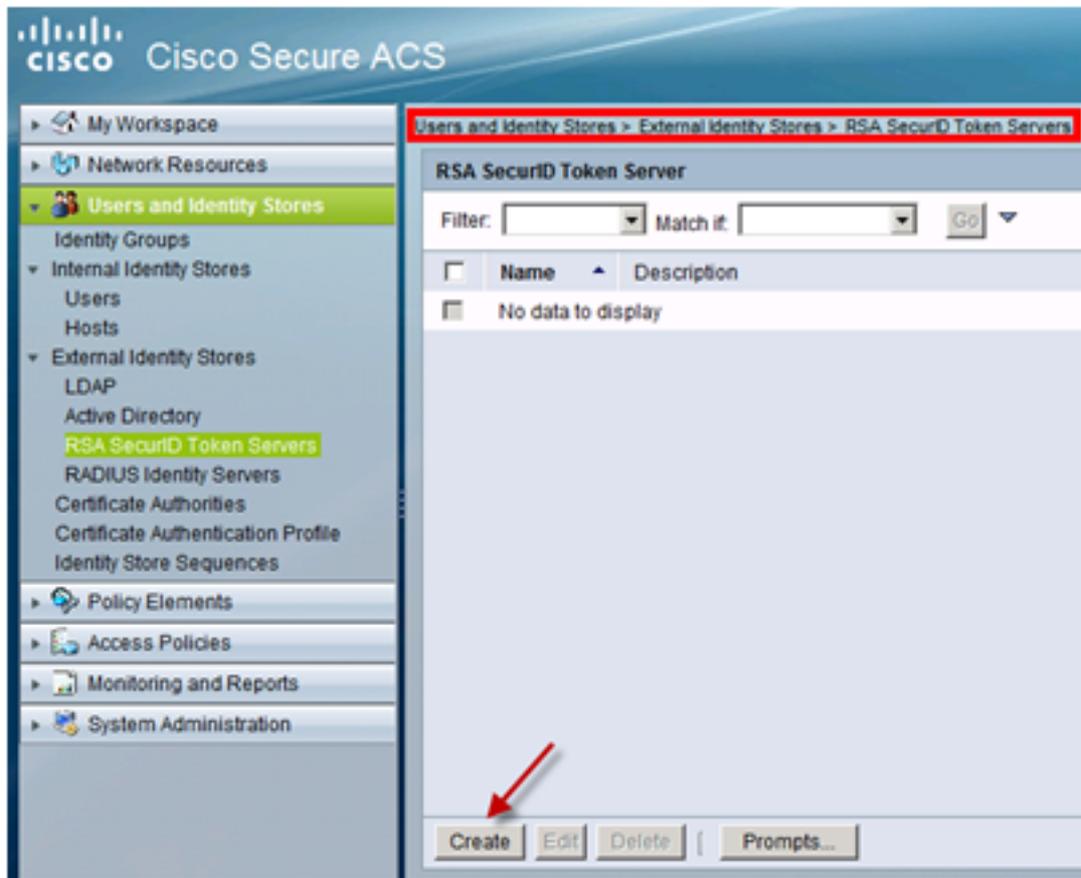
Download:            [Download Now](#)  

Die ZIP-Datei enthält die eigentliche Konfigurationsdatei sdconf.rec, die der ACS-Administrator benötigt, um die Konfigurationsaufgaben durchzuführen.

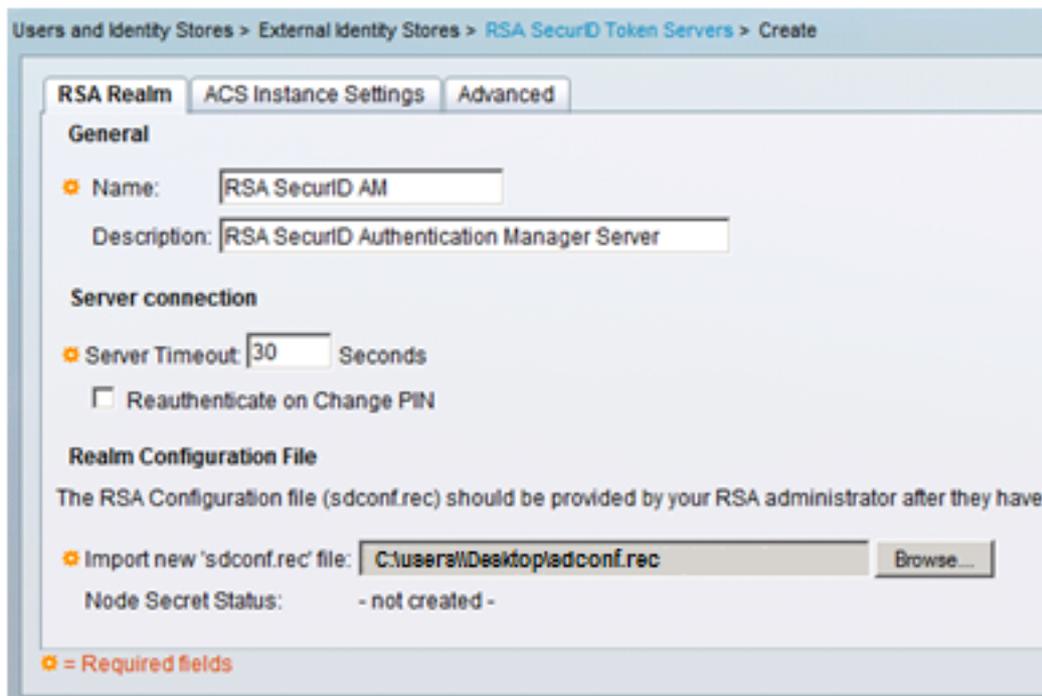
## ACS 5.X-Server

Dieses Verfahren beschreibt, wie der ACS-Administrator die Konfigurationsdatei abrufen und einsendet.

1. Navigieren Sie in der Konsole Cisco Secure ACS 5.x zu **Benutzern und Identitätsdaten > Externe Identitätsspeicher > RSA SecurID Token Servers**, und klicken Sie auf **Erstellen**:



2. Geben Sie den Namen des RSA-Servers ein, und navigieren Sie zur Datei sdconf.rec, die vom RSA-Server heruntergeladen wurde:



3. Wählen Sie die Datei aus, und klicken Sie auf **Senden**.

**Hinweis:** Beim ersten Kontakt des ACS mit dem Tokenserver wird eine weitere Datei, die als geheime Knotendatei bezeichnet wird, für den ACS-Agenten im RSA Authentication Manager erstellt und auf den ACS heruntergeladen. Diese Datei wird für verschlüsselte Kommunikation verwendet.

# Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

## ACS 5.X-Server

Um eine erfolgreiche Anmeldung zu überprüfen, gehen Sie zur ACS-Konsole, und überprüfen Sie die Anzahl der Treffer:

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
1	<input type="checkbox"/>	<a href="#">Rule-4</a>	-ANY-	In All Device Types:SWITCHES	RSA Device Admin	2

Sie können die Authentifizierungsdetails auch aus den ACS-Protokollen überprüfen:

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

## RSA-Server

Um die erfolgreiche Authentifizierung zu überprüfen, rufen Sie die RSA-Konsole auf, und überprüfen Sie die Protokolle:

Time	Activity Key	Description	Reason	User ID	Agent	Server Node IP	Client IP
<a href="#">i</a> <a href="#">2013-02-16 12:35:28.764</a>	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

## Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

### Erstellen eines Agent-Datensatzes (sdconf.rec)

Um einen RSA SecurID-Tokenserver in ACS Version 5.3 zu konfigurieren, muss der ACS-Administrator über die Datei sdconf.rec verfügen. Die Datei sdconf.rec ist eine Konfigurationsdatensatzdatei, die angibt, wie der RSA-Agent mit dem RSA SecurID-Serverbereich kommuniziert.

Um die Datei sdconf.rec zu erstellen, sollte der RSA-Administrator den ACS-Host als Agent-Host auf dem RSA SecurID-Server hinzufügen und eine Konfigurationsdatei für diesen Agent-Host generieren.

### Node Secret (Sicher) zurücksetzen

Nachdem der Agent zunächst mit dem RSA SecurID-Server kommuniziert hat, stellt der Server dem Agenten eine Node-geheime Datei namens securid zur Verfügung. Die nachfolgende Kommunikation zwischen Server und Agent beruht auf dem Austausch des Knotengeheimnisses, um die Authentizität des anderen zu überprüfen.

Manchmal müssen die Administratoren den Knoten möglicherweise geheim zurücksetzen:

1. Der RSA-Administrator muss das Kontrollkästchen "Node Secret Created" (Node-geheim erstellt) auf dem Agent-Host-Datensatz im RSA SecurID-Server deaktivieren.
2. Der ACS-Administrator muss die sichere Datei aus dem ACS entfernen.

### Überschreiben des automatischen Lastenausgleichs

Der RSA SecurID-Agent gleicht automatisch die angeforderten Lasten auf den RSA SecurID-Servern im Bereich aus. Sie haben jedoch die Möglichkeit, die Last manuell auszugleichen. Sie können den Server angeben, der von jedem der Agent-Hosts verwendet wird. Sie können jedem

Server eine Priorität zuweisen, sodass der Agent-Host Authentifizierungsanforderungen häufiger als andere an einige Server weiterleitet.

Sie müssen die Prioritätseinstellungen in einer Textdatei angeben, diese als sdopts.rec speichern und in den ACS hochladen.

## **Manuelles Eingreifen zum Entfernen eines RSA SecurID-Servers nach unten**

Wenn ein RSA SecurID-Server ausgefallen ist, funktioniert der automatische Ausschlussmechanismus nicht immer schnell. Entfernen Sie die Datei sdstatus.12 aus dem ACS, um diesen Prozess zu beschleunigen.