

# Cisco ACS 5.X與RSA SecurID令牌伺服器整合

## 目錄

[簡介](#)

[背景資訊](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[組態](#)

[RSA伺服器](#)

[ACS 5.X版伺服器](#)

[驗證](#)

[ACS 5.X版伺服器](#)

[RSA伺服器](#)

[疑難排解](#)

[建立代理記錄\(sdconf.rec\)](#)

[重置節點金鑰 \(安全ID\)](#)

[覆蓋自動負載平衡](#)

[手動干預以刪除RSA SecurID伺服器](#)

## 簡介

本文檔介紹如何將思科訪問控制系統(ACS)版本5.x與RSA SecurID身份驗證技術整合。

## 背景資訊

Cisco Secure ACS支援RSA SecurID伺服器作為外部資料庫。

RSA SecurID雙因素身份驗證由使用者的個人標識號(PIN)和單獨註冊的RSA SecurID令牌組成，該令牌根據時間碼演算法生成一次性令牌代碼。

以固定間隔生成不同的令牌代碼，通常每30或60秒生成一次。RSA SecurID伺服器驗證此動態身份驗證代碼。每個RSA SecurID令牌都是唯一的，無法根據過去的令牌預測未來令牌的值。

因此，當提供正確的令牌碼和PIN時，該人是有效使用者具有高度確定性。因此，RSA SecurID伺服器提供了一種比傳統可重用密碼更可靠的身份驗證機制。

您可以通過以下方式將Cisco ACS 5.x與RSA SecurID身份驗證技術整合：

- RSA SecurID代理 — 使用者通過本機RSA協定使用使用者名稱和密碼進行身份驗證。

- RADIUS通訊協定 — 使用者是透過RADIUS通訊協定進行使用者名稱和密碼驗證。

## 必要條件

### 需求

思科建議您瞭解以下主題的基本知識：

- RSA安全性
- 思科安全存取控制系統(ACS)

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全存取控制系統(ACS)版本5.x
- RSA SecurID令牌伺服器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

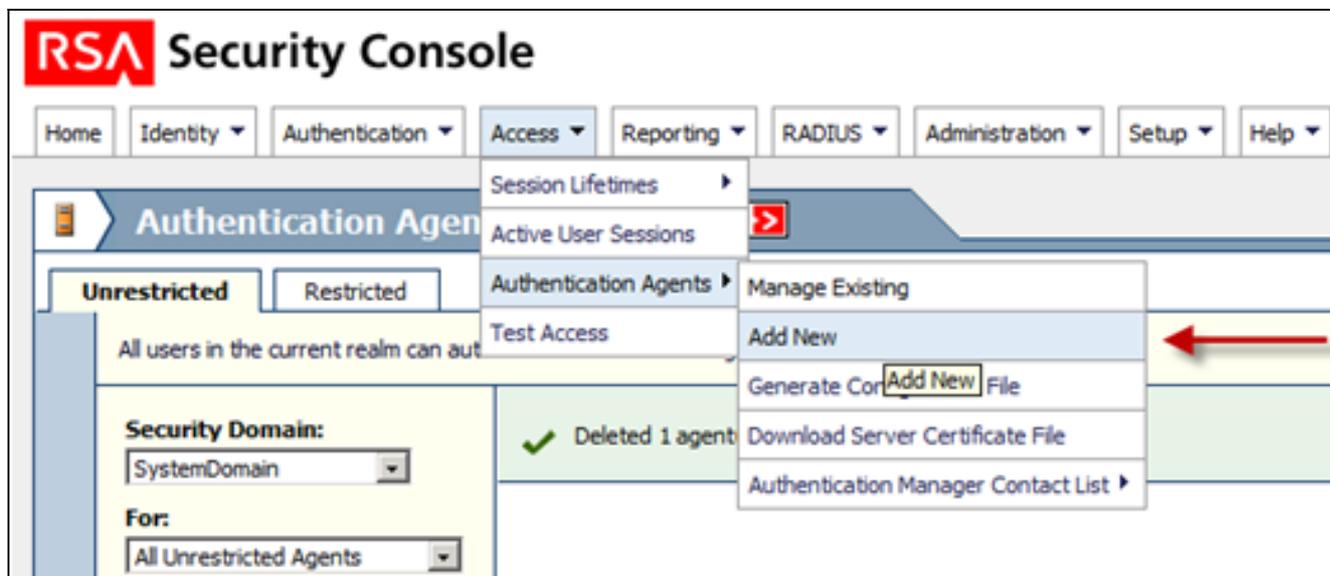
## 組態

### RSA伺服器

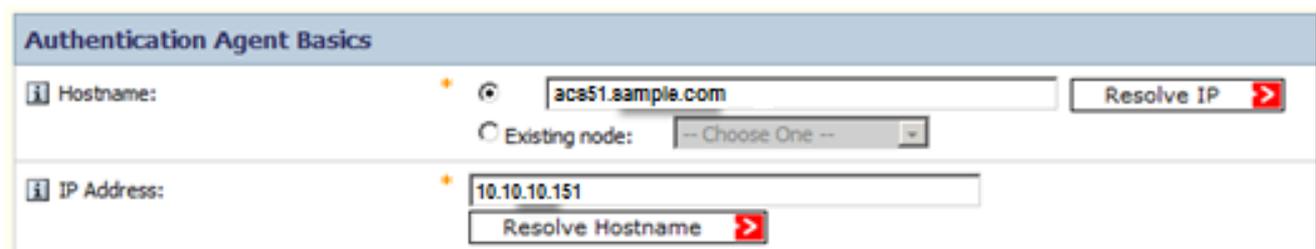
此過程描述RSA SecurID伺服器管理員如何建立身份驗證代理和配置檔案。身份驗證代理基本上是域名伺服器(DNS)名稱以及有權訪問RSA資料庫的裝置、軟體或服務的IP地址。配置檔案主要描述RSA拓撲和通訊。

在本示例中，RSA管理員必須為兩個ACS例項建立兩個代理。

1. 在RSA安全控制檯中，導航到**Access > Authentication Agents > Add New:**

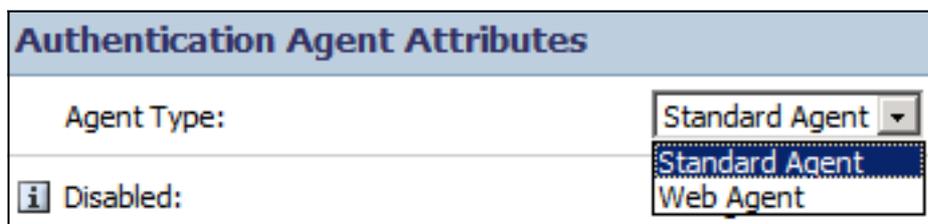


2. 在Add New Authentication Agent ( 新增新身份驗證代理 ) 視窗中，為兩個代理中的每一個定義主機名和IP地址：



ACS代理的DNS正向查詢和反向查詢都應該起作用。

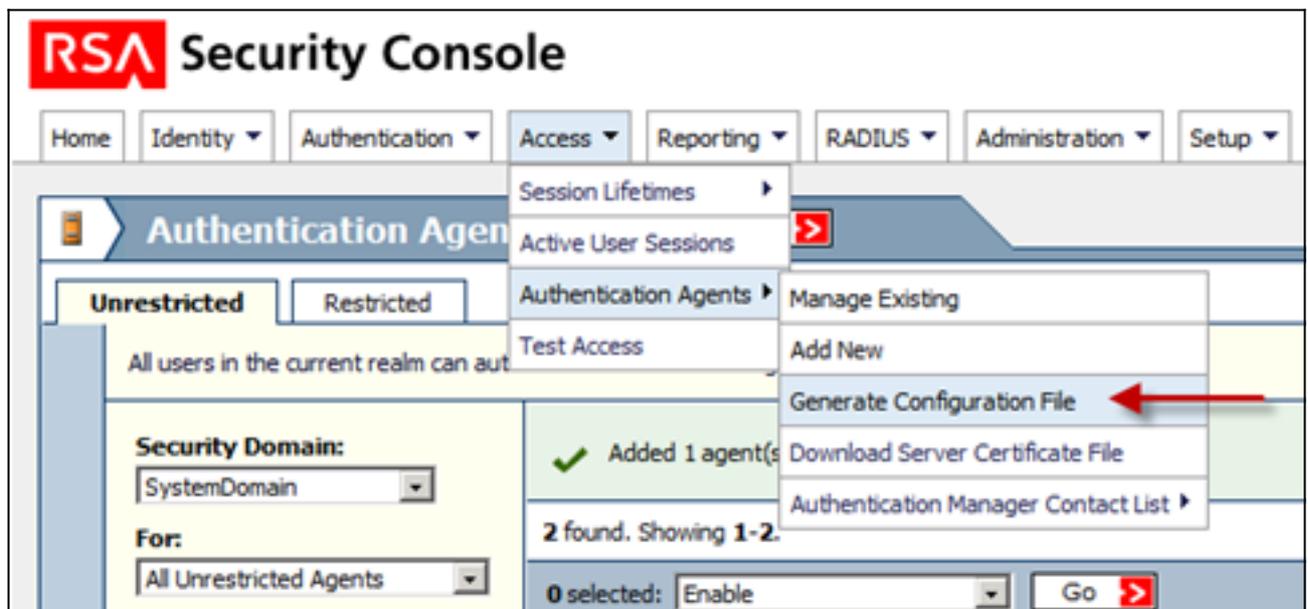
3. 將代理型別定義為標準代理：



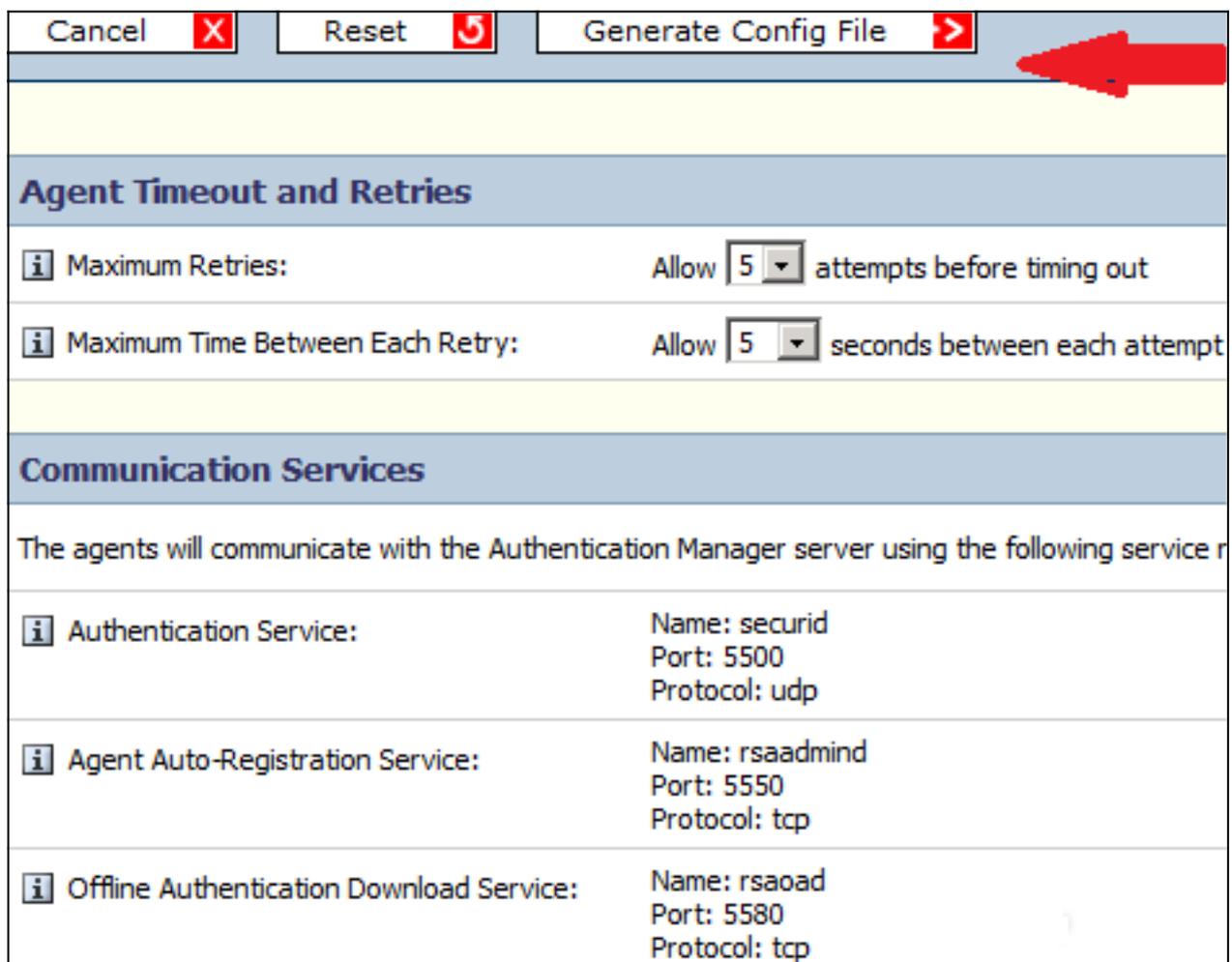
以下是新增座席後所看到的資訊示例：

2 found. Showing 1-2.					
0 selected: Enable [Go]					
<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 [Go]					
2 found. Showing 1-2.					

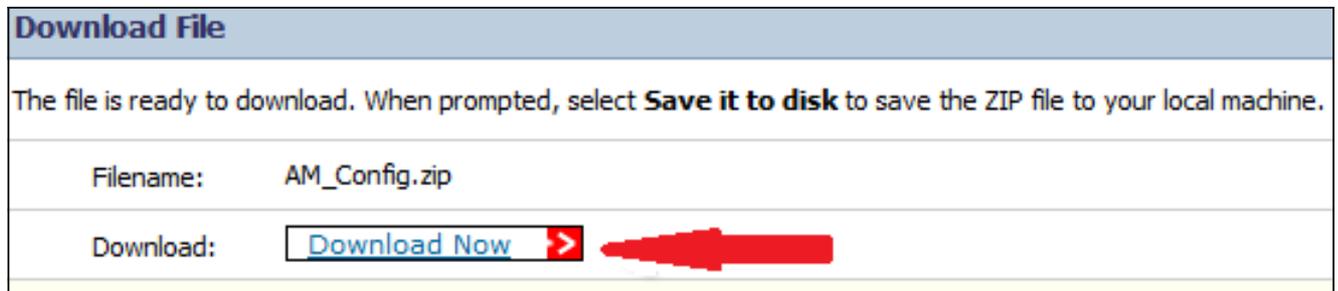
4. 在RSA安全控制檯中，導航到Access > Authentication Agents > Generate Configuration File以生成sdconf.rec配置檔案：



5. 使用每次重試的最大重試次數和最大間隔時間的預設值：



6. 下載組態檔：

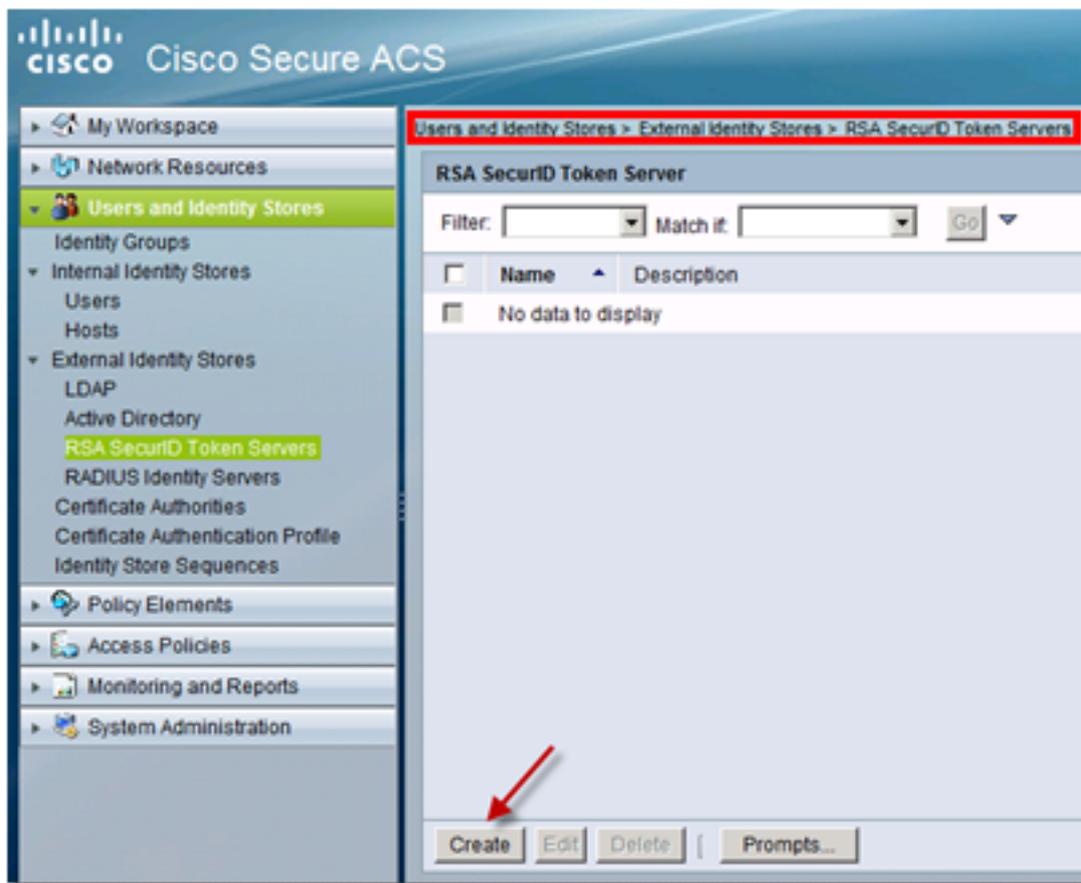


.zip檔案包含實際配置sdconf.rec檔案，ACS管理員需要該檔案來完成配置任務。

## ACS 5.X版伺服器

此過程描述ACS管理員如何檢索並提交配置檔案。

1. 在Cisco Secure ACS 5.x版控制檯中，導航到Users and Identity Stores > External Identity Stores > RSA SecurID Token Servers，然後按一下Create:



2. 輸入RSA伺服器的名稱，並瀏覽到從RSA伺服器下載的sdconf.rec檔案：

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

RSA Realm ACS Instance Settings Advanced

**General**

Name: RSA SecurID AM  
 Description: RSA SecurID Authentication Manager Server

**Server connection**

Server Timeout: 30 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: C:\users\!\Desktop\sdconf.rec

Node Secret Status: - not created -

**= Required fields**

3. 選擇檔案，然後按一下**提交**。

**附註：**ACS首次聯絡令牌伺服器時，會為RSA身份驗證管理器上的ACS代理建立另一個檔案（稱為節點金鑰檔案），並將其下載到ACS。此檔案用於加密通訊。

## 驗證

使用本節內容，確認您的組態是否正常運作。

## ACS 5.X版伺服器

要驗證登入是否成功，請轉到ACS控制檯，並檢視Hit Count:

Access Policies > Access Services > Service Selection Rules

Single result selection  Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals

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

您還可以檢視ACS日誌中的身份驗證詳細資訊：

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:	<u>acs51</u>
Authentication Method:	PAP_ASCII
Authentication Type:	ASCII
Privilege Level:	1
<b>User</b>	
Username:	TEST1
Remote Address:	
<b>Network Device</b>	
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
<b>Access Policy</b>	
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

## RSA伺服器

要驗證身份驗證是否成功，請轉到RSA控制檯並檢視日誌：

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

## 疑難排解

本節提供的資訊可用於對組態進行疑難排解。

### 建立代理記錄(sdconf.rec)

要在ACS版本5.3中配置RSA SecurID令牌伺服器，ACS管理員必須具有sdconf.rec檔案。sdconf.rec檔案是指定RSA代理如何與RSA SecurID伺服器領域通訊的配置記錄檔案。

為了建立sdconf.rec檔案，RSA管理員應將ACS主機新增為RSA SecurID伺服器上的代理主機，並生成此代理主機的配置檔案。

## 重置節點金鑰 (安全ID)

代理最初與RSA SecurID伺服器通訊後，伺服器會向代理提供名為securid的節點機密檔案。伺服器與代理之間的後續通訊依賴於交換節點金鑰以驗證對方的真實性。

有時，管理員可能需要重置節點金鑰：

1. RSA管理員必須取消選中RSA SecurID伺服器中代理主機記錄上的「已建立節點金鑰」覈取方塊。
2. ACS管理員必須從ACS中刪除安全檔案。

## 覆蓋自動負載平衡

RSA SecurID代理自動平衡領域中RSA SecurID伺服器上請求的負載。但是，您可以選擇手動平衡負載。可以指定每個代理主機使用的伺服器。可以為每台伺服器分配優先順序，以便代理主機將身份驗證請求定向到某些伺服器的頻率高於其他伺服器。

您必須在文本檔案中指定優先順序設定，將其另存為sdopts.rec，然後將其上傳到ACS。

## 手動干預以刪除RSA SecurID伺服器

當RSA SecurID伺服器關閉時，自動排除機制並不總是能夠快速運行。從ACS中刪除sdstatus.12檔案以加快此過程。