安全管理器與ACS的整合

目錄

簡介

本檔案介紹如何將思科安全管理員與思科安全存取控制伺服器(ACS)整合。

Cisco Secure ACS為使用管理應用程式（如思科安全管理器）來配置受管網路裝置的使用者提供命令授權。唯一命令授權集型別（在思科安全管理器中稱為角色）支援命令授權，這些型別包含一組許可權。這些許可權（也稱為許可權）決定了具有特定角色的使用者可以在思科安全管理器中執行的操作。

Cisco Secure ACS使用TACACS+與管理應用程式通訊。要使思科安全管理器與思科安全ACS通訊，您必須將思科安全ACS中的CiscoWorks伺服器配置為使用TACACS+的AAA客戶端。此外，您必須向CiscoWorks伺服器提供用於登入Cisco Secure ACS的管理員名稱和密碼。當您滿足這些要求時，它將確保思科安全管理器與思科安全ACS之間的通訊的有效性。

思科安全管理器最初與Cisco Secure ACS通訊時，會要求思科ACS建立預設角色，這些角色顯示在Cisco Secure ACS HTML介面的Shared Profile Components部分中。它還規定自定義服務必須由TACACS+授權。此自訂服務會顯示在HTML介面的「介面組態」部分的TACACS+(Cisco IOS®)頁

面上。然後，您可以修改每個思科安全管理器角色中包含的許可權，並將這些角色應用於使用者和使用者組。

注意：無法將CSM與ACS 5.2整合，因為它不受支援。

必要條件

需求

若要使用Cisco Secure ACS，請確保：

- 您可以定義包含所需命令的角色，以便在思科安全管理器中執行必要的功能。
- 如果將NAR應用於配置檔案，則網路訪問限制(NAR)包括要管理的裝置組（或裝置）。
- 在思科安全ACS和思科安全管理器中，受管裝置名稱的拼寫和大寫相同。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全管理員3.0版
- Cisco安全ACS版本3.3

注意：在網路環境中安裝之前，請確保選擇相容的CSM和ACS版本。例如，思科僅使用CSM 3.0測試了ACS 3.3，並在更高版本的CSM中停止了該測試。因此，建議您將CSM 3.0與ACS 3.3配合使用。有關各種軟體版本的更多資訊，請參閱相容性矩陣表。

思科安全管理員版本	已測試的CS ACS版本
3.0.0 3.0.0 SP1	Windows 3.3(3)和4.0(1)
3.0.1 3.0.1 SP1 3.0.1 SP2	解決方案引擎4.0(1)Windows 4.0(1)
3.1.0 3.0.2	解決方案引擎4.0(1)Windows 4.1(1)和4.1(3)
3.1.1 3.0.2 SP1 3.0.2 SP2	解決方案引擎v4.0(1)Windows 4.1(2)、4.1(3)和4.1(4)
3.1.1 SP1	解決方案引擎4.0(1)Windows 4.1(4)
3.1.1 SP2	解決方案引擎4.0(1)Windows 4.1(4)和4.2(0)
3.2.0	解決方案引擎4.1(4)Windows 4.1(4)和4.2(0)
3.2.1	解決方案引擎4.1(4)Windows 4.2(0)

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。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

將思科安全管理器與思科安全ACS整合

本節介紹將思科安全管理器與思科安全ACS整合所需的步驟。有些步驟包含多個子步驟。必須按順序執行這些步驟和子步驟。本節還包含執行每個步驟所使用的具體過程的參考。

請完成以下步驟：

1. **規劃您的管理身份驗證和授權模型。**在使用思科安全管理器之前，必須決定您的管理模式。其中包括計畫使用的管理角色和帳戶的定義。**提示：**定義潛在管理員的角色和許可權時，還要考慮是否啟用工作流。此選擇會影響限制訪問的方式。
2. **安裝Cisco Secure ACS、Cisco Security Manager和CiscoWorks Common Services。**在Windows 2000/2003伺服器上安裝Cisco Secure ACS 3.3版。在其他的Windows 2000/Windows 2003伺服器上安裝CiscoWorks公共服務和思科安全管理器。請參閱以下文件以瞭解更多資訊：思科安全管理器3.0安裝指南Windows 3.3版Cisco Secure ACS安裝指南**註：在選**擇CSM和ACS軟體版本之前，請參閱Compatibility Matrix表以瞭解詳細資訊。
3. **在Cisco Secure ACS中執行整合過程。**將Cisco Security Manager使用者定義為ACS使用者，並根據使用者計畫的角色將其分配給使用者組，新增所有受管裝置（以及CiscoWorks/Security Manager伺服器）作為AAA客戶端，並建立管理控制使用者。如需詳細資訊，請參閱在Cisco Secure ACS中執行的整合程式。
4. **在CiscoWorks公共服務中執行整合過程。**配置與Cisco Secure ACS中定義的管理員匹配的本地使用者，為系統身份設定定義該使用者，並將ACS配置為AAA設定模式。如需詳細資訊，請參閱在CiscoWorks中執行的整合程式。
5. **在Cisco Secure ACS中將角色分配給使用者組。**為Cisco Secure ACS中配置的每個使用者組分配角色。您使用的過程取決於您是否已配置網路裝置組(NDG)。如需詳細資訊，請參閱在Cisco Secure ACS中將角色分配給使用者組。

在Cisco Secure ACS中執行的整合過程

本節介紹在Cisco Secure ACS中必須完成的步驟，以便將其與Cisco Security Manager整合：

1. 在Cisco Secure ACS中定義使用者和使用者組
2. 在Cisco Secure ACS中將受管裝置新增為AAA客戶端
3. 在Cisco Secure ACS中建立管理控制使用者

在Cisco Secure ACS中定義使用者和使用者組

必須在Cisco Secure ACS中定義Cisco Security Manager的所有使用者，並為其分配與其工作職能相應的角色。最簡單的方法是根據ACS中可用的每個預設角色將使用者分為不同的組。例如，將所有系統管理員分配給一個組，將所有網路操作員分配給另一個組，以此類推。有關ACS中的預設角色的詳細資訊，請參閱Cisco Secure ACS預設角色。

此外，您必須建立一個附加使用者，該使用者被指定具有完全許可權的系統管理員角色。以後將在CiscoWorks的「系統身份設定」(System Identity Setup)頁面上使用為此使用者建立的憑證。有關詳細資訊，請參閱定義系統身份使用者。

請注意，在此階段，您只是將使用者分配到不同的組。在CiscoWorks、Cisco Security Manager和任何其他應用程式註冊到Cisco Secure ACS之後，會執行為這些組分配角色的實際操作。

提示：繼續之前，請在一台Windows 2000/2003伺服器上安裝CiscoWorks公共服務和思科安全管理器。在其他的Windows 2000/2003伺服器上安裝Cisco Secure ACS。

1. 登入到Cisco Secure ACS。
2. 配置具有完全許可權的使用者：按一下導航欄上的**User Setup**。在「使用者設定」頁面上，輸入新使用者的名稱，然後按一下**新增/編輯**。從User Setup下的Password Authentication清單中選擇一種身份驗證方法。輸入並確認新使用者的密碼。選擇**組1**作為將使用者分配到的組。按一下「**Submit**」以建立使用者帳號。
3. 對每個思科安全管理器使用者重複步驟2。思科建議您根據為每個使用者分配的角色將使用者分為多個組：組1 — 系統管理員組2 — 安全管理員組3 — 安全批准者組4 — 網路管理員組5 — 批准者組6 — 網路運營商組7 — 幫助台有關與每個角色關聯的預設許可權的詳細資訊，請參閱表。有關自定義使用者角色的詳細資訊，請參閱自定義Cisco Secure ACS角色。**注意**：在此階段，組本身是沒有任何角色定義的使用者集合。完成整合過程後，您可以為每個組分配角色。如需詳細資訊，請參閱在Cisco Secure ACS中將角色分配給使用者組。
4. 建立一個附加使用者並將該使用者分配給系統管理員組。以後將在CiscoWorks的「系統身份設定」(System Identity Setup)頁面上使用為此使用者建立的憑證。有關詳細資訊，請參閱定義系統身份使用者。
5. 繼續在Cisco Secure ACS中將受管裝置新增為AAA客戶端。

在Cisco Secure ACS中將受管裝置新增為AAA客戶端

開始將裝置匯入思科安全管理器之前，必須先將每台裝置配置為思科安全ACS中的AAA客戶端。此外，您必須將CiscoWorks/安全管理器伺服器配置為AAA客戶端。

如果思科安全管理器管理在防火牆裝置上配置的安全情景（包括在FWSM上為Catalyst 6500/7600裝置配置的安全情景），則必須將每個情景單獨新增到Cisco Secure ACS。

新增受管裝置所使用的方法取決於您是否要限制使用者使用網路裝置組(NDG)管理一組特定裝置。請參閱以下部分之一：

- 如果您希望使用者能夠訪問所有裝置，請按照新增裝置作為AAA客戶端而不使用NDG中所述新增裝置。
- 如果您希望使用者僅能訪問某些NDG，請按照配置網路裝置組以便在安全管理器中使用中所述新增裝置。

將裝置新增為沒有NDG的AAA客戶端

以下過程介紹如何將裝置新增為Cisco Secure ACS的AAA客戶端。請參閱網路組態的*AAA使用者端組態*區段，以瞭解所有可用選項的完整資訊。

注意：請記住將CiscoWorks/安全管理器伺服器新增為AAA客戶端。

1. 按一下Cisco Secure ACS導航欄上的**Network Configuration**。
2. 按一下AAA Clients表下的**Add Entry**。
3. 在「新增AAA客戶端」頁中輸入AAA客戶端主機名（最多32個字元）。AAA客戶端的主機名必須與您計畫用於思科安全管理器中的裝置的顯示名稱相匹配。例如，如果您打算在思科安全管理器中將域名附加到裝置名稱，則ACS中的AAA客戶端主機名必須是**<device_name>.<domain_name>**。命名CiscoWorks伺服器時，建議使用完全限定主機名。請務必正確拼寫主機名。主機名不區分大小寫。命名安全上下文時，請將上下文名稱

(_<context_name>)附加到裝置名稱。對於FWSM，這是命名約定：FWSM刀片- **<機箱名稱>_FW_<插槽編號>**安全情景- **<chassis_name>_FW_<slot_number>_<context_name>**
4. 在AAA Client IP Address欄位中輸入網路裝置的IP地址。
5. 在「金鑰」欄位中輸入共用金鑰。
6. 從Authenticate Using清單中選擇**TACACS+(Cisco IOS)**。
7. 按一下「**Submit**」以儲存變更內容。新增的裝置將顯示在AAA客戶端表中。
8. 重複步驟1至7以新增其他裝置。
9. 新增所有裝置後，按一下**Submit + Restart**。
10. 繼續執行在Cisco Secure ACS中建立管理控制使用者。

配置網路裝置組以在安全管理器中使用

Cisco Secure ACS允許您配置包含要管理的特定裝置的網路裝置組(NDG)。例如，您可以為每個地理區域建立NDG或與您的組織結構匹配的NDG。當與思科安全管理器配合使用時，NDG允許您根據使用者需要管理的裝置為使用者提供不同級別的許可權。例如，通過NDG，您可以為位於歐洲的裝置分配使用者A系統管理員許可權，為位於亞洲的裝置分配幫助台許可權。然後，可以將相反的許可權分配給使用者B。

NDG不會直接分配給使用者。而是將NDG分配給為每個使用者組定義的角色。每個NDG只能分配給單個角色，但每個角色可以包含多個NDG。這些定義將儲存為選定使用者組的配置的一部分。

以下主題概述配置NDG所需的基本步驟：

- 啟用NDG功能
- 建立NDG
- 將NDG和角色與使用者組關聯

啟用NDG功能

必須先啟用NDG功能，然後才能建立NDG並用裝置填充它們。

1. 按一下Cisco Secure ACS導航欄上的**Interface Configuration**。
2. 按一下「**Advanced Options**」。
3. 向下滾動，然後選中**Network Device Groups**覈取方塊。
4. 按一下「**Submit**」。
5. 繼續建立NDG。

建立NDG

此過程介紹如何建立NDG並用裝置填充它們。每台裝置只能屬於一個NDG。

注意：思科建議您建立一個包含CiscoWorks/安全管理器伺服器的特殊NDG。

1. 按一下導航欄上的**Network Configuration**。所有裝置最初都放置在Not Assigned下，該選項儲存未放置在NDG中的所有裝置。請記住，「未分配」不是NDG。
2. 建立NDG:按一下「**Add Entry**」。在New Network Device Group頁面上輸入NDG的名稱。最大長度為24個字元。允許使用空格。**使用版本4.0或更高版本時可選**：輸入要供NDG中的所有裝置使用的金鑰。如果為NDG定義金鑰，它將覆蓋NDG中為單個裝置定義的任何金鑰。按一下「**Submit**」以儲存NDG。重複步驟a到d以建立更多NDG。

3. 用裝置填充NDG:在Network Device Groups區域中按一下NDG的名稱。在AAA Clients區域中按一下**Add Entry**。定義要新增到NDG的裝置的詳細資訊，然後按一下**Submit**。如需詳細資訊，請參閱將裝置新增為沒有NDG的AAA使用者端。重複步驟b和c，將剩餘裝置新增到NDG。唯一可以保留在Not Assigned類別中的裝置是預設AAA伺服器。配置最後一個裝置後，按一下**Submit + Restart**。
4. 繼續執行在Cisco Secure ACS中建立管理控制使用者。

在Cisco Secure ACS中建立管理控制使用者

使用Cisco Secure ACS中的Administration Control頁定義在CiscoWorks公共服務中定義AAA設定模式時使用的管理員帳戶。如需詳細資訊，請參閱在CiscoWorks中設定AAA設定模式。

1. 按一下Cisco Secure ACS導航欄上的**Administration Control**。
2. 按一下**Add Administrator**。
3. 在「新增管理員」頁上，輸入管理員的名稱和密碼。
4. 在「管理員許可權」區域中按一下**Grant All**，以便為此管理員提供完全管理許可權。
5. 按一下「**Submit**」以建立管理員。

註：有關配置管理員時可用的選項的詳細資訊，請參閱管理員和管理策略。

在CiscoWorks中執行的整合過程

本節介紹要在CiscoWorks公共服務中完成的步驟，以便將其與思科安全管理器整合：

- 在CiscoWorks中建立本地使用者
- 定義系統身份使用者
- 在CiscoWorks中配置AAA設定模式

完成在Cisco Secure ACS中執行的整合過程後，請完成以下步驟。Common Services會執行任何已安裝應用（例如Cisco Security Manager、自動更新伺服器和IPS管理器）到Cisco Secure ACS的實際註冊。

在CiscoWorks中建立本地使用者

使用CiscoWorks公共服務中的「本地使用者設定」(Local User Setup)頁面，建立與先前在Cisco Secure ACS中建立的管理員重複的本地使用者帳戶。此本地使用者帳戶稍後將用於系統身份設定。有關詳細資訊，請參閱。

注意：繼續之前，請在Cisco Secure ACS中建立管理員。有關說明，請參閱在Cisco Secure ACS中定義使用者和使用者組。

1. 使用預設管理員使用者**帳**戶登入CiscoWorks。
2. 從Common Services中選擇**Server > Security**，然後從TOC中選擇**Local User Setup**。
3. 按一下「**Add**」。
4. 輸入您在Cisco Secure ACS中建立管理員時輸入的相同名稱和密碼。請參閱在Cisco Secure ACS中定義使用者和使用者組中的步驟4。
5. 選中Roles except Export Data下的所有覈取方塊。
6. 按一下**OK**以建立使用者。

定義系統身份使用者

使用CiscoWorks公共服務中的「系統身份設定」頁可建立信任使用者（稱為「系統身份使用者」），該使用者可在屬於同一域的伺服器和位於同一伺服器上的應用程式進程之間進行通訊。應用程式使用系統身份使用者驗證本地或遠端CiscoWorks伺服器上的進程。當應用程式必須在任何使用者登入之前同步時，這一點尤其有用。

此外，通常使用System Identity使用者，以便在已登入使用者已經授權主要任務時執行子任務。例如，要在思科安全管理器中編輯裝置，需要在思科安全管理器與公共服務DCR之間進行應用程式間通訊。在使用者被授權執行編輯任務後，系統身份使用者用於呼叫DCR。

此處配置的系統身份使用者必須與在ACS中配置的具有管理（完全）許可權的使用者相同。否則可能會導致無法檢視思科安全管理器中配置的所有裝置和策略。

注意：繼續之前，請在CiscoWorks公共服務中建立與管理員具有相同名稱和密碼的本地使用者。有關說明，請參閱在CiscoWorks中建立本地使用者。

1. 選擇**Server > Security**，然後從TOC中選擇**Multi-Server Trust Management > System Identity Setup**。
2. 輸入您為Cisco Secure ACS建立的管理員的名稱。請參閱在Cisco Secure ACS中定義使用者和使用者組中的步驟4。
3. 輸入並驗證此使用者的密碼。
4. 按一下「**Apply**」。

在CiscoWorks中配置AAA設定模式

使用CiscoWorks公共服務中的AAA設定模式頁面，將您的Cisco Secure ACS定義為AAA伺服器，其中包括所需的埠和共用金鑰。此外，最多可以定義兩個備份伺服器。

這些步驟執行CiscoWorks、思科安全管理器、IPS管理器（以及自動更新伺服器）到Cisco Secure ACS的實際註冊。

1. 選擇**Server > Security**，然後從TOC中選擇**AAA Mode Setup**。
2. 選中Available Login Modules下的**TACACS+**覈取方塊。
3. 選擇**ACS**作為AAA型別。
4. 在Server Details（伺服器詳細資訊）區域中輸入最多三個Cisco Secure ACS伺服器的IP地址。輔助伺服器和第三級伺服器作為備份，以防主伺服器發生故障。**注意：**如果所有已配置的TACACS+伺服器均無法響應，您必須使用管理員CiscoWorks本地帳戶登入，然後將AAA模式更改回非ACS/CiscoWorks本地。將TACACS+伺服器還原為服務後，必須將AAA模式重新更改為ACS。
5. 在Login區域中，輸入您在Cisco Secure ACS的Administration Control頁面上定義的管理員名稱。如需詳細資訊，請參閱在Cisco Secure ACS中建立管理控制使用者。
6. 輸入並驗證此管理員的密碼。
7. 輸入並驗證在將安全管理器伺服器新增為Cisco Secure ACS的AAA客戶端時輸入的共用金鑰。請參閱將裝置新增為不帶NDG的AAA客戶端中的步驟5。
8. 勾選「**Register all installed applications with ACS**」覈取方塊以向Cisco Secure ACS註冊思科安全管理器和其他任何已安裝的應用程式。
9. 按一下「**Apply**」以儲存設定。進度條顯示註冊進度。註冊完成後，系統會顯示一條消息。
10. 如果將思科安全管理器與任何ACS版本整合，請重新啟動思科安全管理器守護程式管理器服務。有關說明，請參閱重新啟動守護程式管理器。**註：**在CSM 3.0.0之後，思科不再使用ACS 3.3(x)進行測試，因為已經對其進行了大量修補並且宣佈其壽命終止(EOL)。因此，您需要為CSM 3.0.1版及更高版本使用適當的ACS版本。有關詳細資訊，請參閱相容性矩陣表。

11. 重新登入到Cisco Secure ACS，以便為每個使用者組分配角色。有關說明，請參閱在Cisco Secure ACS中為使用者組分配角色。**注意：如**果解除安裝CiscoWorks公共服務或思科安全管理器，則不會保留在此處配置的AAA設定。此外，重新安裝後無法備份和還原此配置。因此，如果您升級到任一應用程式的新版本，則必須重新配置AAA設定模式並重新註冊使用ACS的思科安全管理器。增量更新不需要此過程。如果您在CiscoWorks之上安裝其他應用（例如AUS），則必須重新註冊新應用和思科安全管理器。

重新啟動守護程式管理器

以下過程介紹了如何重新啟動思科安全管理器伺服器的守護程式管理器。您必須執行此操作，才能使配置的AAA設定生效。然後，您可以使用在Cisco Secure ACS中定義的憑證重新登入到CiscoWorks。

1. 登入到安裝思科安全管理器伺服器的電腦。
2. 選擇**開始>程式>管理工具>服務**以開啟「服務」視窗。
3. 從右窗格中顯示的服務清單中，選擇**思科安全管理器守護程式管理器**。
4. 按一下工具欄上的**Restart Service**按鈕。
5. 繼續執行在Cisco Secure ACS中為使用者組分配角色。

在Cisco Secure ACS中將角色分配給使用者組

將CiscoWorks、思科安全管理器和其他已安裝應用程式註冊到Cisco Secure ACS後，您可以為您之前在Cisco Secure ACS中配置的每個使用者組分配角色。這些角色確定允許每個組中的使用者在思科安全管理器中執行的操作。

用於將角色分配給使用者組的過程取決於是否使用NDG:

- 向沒有NDG的使用者組分配角色
- 將NDG和角色與使用者組關聯

向沒有NDG的使用者組分配角色

此過程介紹在未定義NDG時如何將預設角色分配給使用者組。有關詳細資訊，請參閱Cisco Secure ACS預設角色。

注意：繼續之前：

- 為每個預設角色建立使用者組。有關說明，請參閱在Cisco Secure ACS中定義使用者和使用者組。
- 完成在Cisco Secure ACS中執行的整合過程和在CiscoWorks中執行的整合過程中介紹的步驟。

請完成以下步驟：

1. 登入到Cisco Secure ACS。
2. 按一下導航欄上的**Group Setup**。
3. 從清單中選擇系統管理員的使用者組。請參閱在Cisco Secure ACS中定義使用者和使用者組的步驟2，然後按一下**Edit Settings**。

將NDG和角色與使用者組關聯

將NDG與用於思科安全管理器中的角色關聯時，必須在「組設定」(Group Setup)頁面上的兩個位置建立定義：

- CiscoWorks區域
- 思科安全管理器區域

每個區域中的定義必須儘可能地匹配。關聯自定義角色或CiscoWorks公共服務中不存在的ACS角色時，請嘗試根據分配給該角色的許可權定義儘可能關閉等效角色。

您必須為每個使用者組建立關聯才能與思科安全管理器一起使用。例如，如果您有一個包含Western區域支援人員的使用者組，則可以選擇該使用者組，然後將包含該區域中的裝置的NDG與Help Desk角色相關聯。

注意：繼續操作之前，請啟用NDG功能並建立NDG。有關詳細資訊，請參閱配置網路裝置組以便在安全管理器中使用。

1. 按一下導航欄上的**Group Setup**。
2. 從「組」清單中選擇一個使用者組，然後按一下**「編輯設定」**。
3. 對映要在CiscoWorks中使用的NDG和角色：在「Group Setup（組設定）」頁面上，向下滾動到「TACACS+ Settings（TACACS+設定）」下的CiscoWorks區域。選擇**Assign a CiscoWorks on a Per Network Device Group**。從Device Group清單中選擇NDG。從第二個清單中選擇此NDG將關聯到的角色。按一下**Add Association**。關聯將顯示在「裝置組」框中。重複步驟c到e以建立其他關聯。**注意：**要刪除關聯，請從裝置組中選擇該關聯，然後按一下刪除關聯。
4. 向下滾動到「思科安全管理器」(Cisco Security Manager)區域，建立儘可能與步驟3中定義的關聯匹配的關聯。**注意：**在Cisco Secure ACS中選擇安全審批者或安全管理員角色時，建議您選擇「網路管理員」作為最接近的對等CiscoWorks角色。
5. 按一下「**Submit**」以儲存設定。
6. 重複步驟2至5，以便為其餘使用者組定義NDG。
7. 將NDG和角色與每個使用者組關聯後，按一下**Submit + Restart**。

疑難排解

1. 開始將裝置匯入思科安全管理器之前，必須先將每台裝置配置為思科安全ACS中的AAA客戶端。此外，您必須將CiscoWorks/安全管理器伺服器配置為AAA客戶端。
2. 如果收到失敗的嘗試日誌，作者將失敗，在Cisco Secure ACS中出現錯誤。
   ```
   "service=Athena cmd=OGS authorize-deviceGroup*(Not Assigned) authorize-deviceGroup*Test
   Devices authorize-deviceGroup*HQ Routers authorize-deviceGroup*HQ Switches
   authorize-deviceGroup*HQ Security Devices authorize-deviceGroup*Agent Routers authoriz"
   ```
   為了解決此問題，請確保ACS中的裝置名稱必須是完全限定域名。

相關資訊

- Cisco Security Access Control Server for Windows支援頁
- 思科安全管理員支援頁面
- 思科安全存取控制伺服器（Windows專用）
- 思科安全ACS 4.1配置指南
- 思科安全ACS線上故障排除指南4.1
- 安全產品現場通知（包括適用於Windows的CiscoSecure ACS）

- 技術支援與文件 - Cisco Systems