CSM 3.x:設定使用者許可權和角色

目錄

簡介

本檔案介紹如何在思科安全管理員(CSM)中為使用者設定許可權和角色。

必要條件

需求

本檔案假設CSM已安裝且工作正常。

採用元件

本檔案中的資訊是根據CSM 3.1。

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

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

設定使用者許可權

思科安全管理器會在您登入之前驗證您的使用者名稱和密碼。經過身份驗證後，安全管理器將在應用程式中建立您的角色。此角色定義您的許可權（也稱為許可權），這些許可權是授權您執行的一組任務或操作。如果您沒有授權執行某些任務或裝置，則相關的選單項、目錄項和按鈕將被隱藏或禁用。此外，系統還會顯示一則消息，告訴您您沒有檢視所選資訊或執行所選操作的許可權。

Security Manager的身份驗證和授權由CiscoWorks伺服器或Cisco Secure Access Control Server(ACS)管理。 預設情況下，CiscoWorks管理身份驗證和授權，但您可以使用CiscoWorks公共服務中的AAA模式設定頁面更改到Cisco Secure ACS。

使用Cisco Secure ACS的主要優勢是能夠使用專用許可權集建立高度精細的使用者角色（例如，允許使用者配置某些策略型別，但不允許配置其他型別），以及通過配置網路裝置組(NDG)將使用者限制到某些裝置。

以下主題介紹使用者許可權：

- 安全管理器許可權
- 瞭解CiscoWorks角色
- 瞭解Cisco Secure ACS角色
- 安全管理器中許可權和角色之間的預設關聯

安全管理器許可權

安全管理器將許可權分為以下類別：

1. **View** — 允許您檢視當前設定。有關詳細資訊，請參閱檢視許可權。
2. **Modify** — 允許您更改當前設定。有關詳細資訊，請參閱修改許可權。
3. **Assign** — 允許您將策略分配給裝置和VPN拓撲。有關詳細資訊，請參閱分配許可權
4. **Approve** — 允許您批准策略更改和部署作業。有關詳細資訊，請參閱批准許可權。
5. **Import** — 用於將已在裝置上部署的配置匯入到安全管理器中。
6. **Deploy** — 允許您將配置更改部署到網路中的裝置，並執行回滾以返回到先前部署的配置。
7. **Control** — 允許向裝置發出命令，如ping。
8. **Submit** — 允許您提交配置更改以供審批。

- 當您選擇修改、分配、批准、匯入、控制或部署許可權時，還必須選擇相應的檢視許可權；否則，安全管理器將無法正常工作。
- 當您選擇「修改策略許可權」時，還必須選擇相應的分配和檢視策略許可權。
- 當您允許將策略對象用作其定義的一部分的策略時，還必須向這些對象型別授予檢視許可權。例如，如果您選擇修改路由策略的許可權，還必須選擇檢視網路對象和介面角色的許可權，這些是路由策略所需的對象型別。
- 當允許對象將其他對象用作其定義的一部分時，情況也是如此。例如，如果您選擇修改使用者組的許可權，還必須選擇檢視網路對象、ACL對象和AAA伺服器組的許可權。

檢視許可權

安全管理器中的檢視（只讀）許可權分為以下類別：

- 檢視策略許可權
- 檢視對象許可權
- 其他檢視許可權

檢視策略許可權

安全管理器包括以下策略檢視許可權：

1. **檢視>策略>防火牆。**允許您檢視PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置上的防火牆服務策略（位於防火牆下的策略選擇器中）。防火牆服務策略的示例包括訪問規則、AAA規則和檢查規則。
2. **檢視>策略>入侵防禦系統。**允許您檢視IPS策略（位於IPS下的策略選擇器中），包括在IOS路由器上運行的IPS的策略。
3. **檢視>策略>影象。**允許您在「應用IPS更新」嚮導（位於「工具」>「應用IPS更新」下）中選擇特徵碼更新軟體包，但是不允許將該軟體包分配給特定裝置，除非您還具有「修改」>「策略」>「映像」許可權。
4. **View > Policies > NAT。**允許您檢視PIX/ASA/FWSM裝置和IOS路由器上的網路地址轉換策略。NAT策略的示例包括靜態規則和動態規則。
5. **View > Policies > Site-to-Site VPN。**允許您檢視PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置上的站點到站點VPN策略。站點到站點VPN策略的示例包括IKE提議、IPsec提議和預共用金鑰。
6. **View > Policies > Remote Access VPN。**允許您檢視PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置上的遠端訪問VPN策略。遠端訪問VPN策略的示例包括IKE提議、IPsec提議和PKI策略。
7. **View > Policies > SSL VPN。**允許您檢視PIX/ASA/FWSM裝置和IOS路由器上的SSL VPN策略，如SSL VPN嚮導。
8. **View > Policies > Interfaces。**允許您檢視PIX/ASA/FWSM裝置、IOS路由器、IPS感測器和Catalyst 6500/7600裝置上的介面策略（位於介面下的策略選擇器中）。在PIX/ASA/FWSM裝置上，此許可權涵蓋硬體埠和介面設定。在IOS路由器上，此許可權涵蓋基本和高級介面設定，以及其他與介面相關的策略，如DSL、PVC、PPP和撥號器策略。在IPS感測器上，此許可權涵蓋物理介面和摘要對映。在Catalyst 6500/7600裝置上，此許可權涵蓋介面和VLAN設定。
9. **檢視>策略>橋接。**允許您在PIX/ASA/FWSM裝置上檢視ARP表策略（位於Platform > Bridging下的Policy selector中）。
10. **View > Policies > Device Administration。**允許您檢視PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置上的裝置管理策略（位於Platform > Device Admin下的Policy selector中）：在PIX/ASA/FWSM裝置上，示例包括裝置訪問策略、伺服器訪問策略和故障切換策略。在IOS路由器上，示例包括裝置訪問（包括線路訪問）策略、伺服器訪問策略、AAA和安全裝置調配。在IPS感測器上，此許可權涵蓋裝置訪問策略和伺服器訪問策略。在Catalyst 6500/7600裝置上，此許可權涵蓋IDSM設定和VLAN存取清單。
11. **檢視>策略>身份。**允許您在Cisco IOS路由器上檢視身份策略（位於Platform > Identity下的策略選擇器中），包括802.1x和網路准入控制(NAC)策略。
12. **檢視>策略>日誌記錄。**允許您檢視PIX/ASA/FWSM裝置、IOS路由器和IPS感測器上的日誌記錄策略（位於Platform > Logging下的Policy selector中）。日誌策略示例包括日誌設定、伺服器設定和系統日誌伺服器策略。
13. **View > Policies > Multicast。**允許您在PIX/ASA/FWSM裝置上檢視組播策略（位於Platform > Multicast下的Policy selector中）。組播策略的示例包括組播路由和IGMP策略。

14. **View > Policies > QoS**。允許您在Cisco IOS路由器上檢視QoS策略（位於平台>服務品質下的策略選擇器中）。
15. **檢視>策略>路由**。允許您在PIX/ASA/FWSM裝置和IOS路由器上檢視路由策略（位於Platform > Routing下的Policy selector中）。路由策略的示例包括OSPF、RIP和靜態路由策略。
16. **檢視>策略>安全性**。允許您檢視PIX/ASA/FWSM裝置和IPS感測器上的安全策略（位於Platform > Security下的Policy selector中）：在PIX/ASA/FWSM裝置上，安全策略包括反欺騙、分片和超時設定。在IPS感測器上，安全策略包括阻止設定。
17. **檢視>策略>服務策略規則**。允許您在PIX 7.x/ASA裝置上檢視服務策略規則策略（位於Platform > Service Policy Rules下的Policy選擇器中）。示例包括優先順序隊列和IPS、QoS以及連線規則。
18. **檢視>策略>使用者首選項**。允許您在PIX/ASA/FWSM裝置上檢視部署策略（位於Platform > User Preferences下的Policy selector中）。此策略包含用於清除部署中的所有NAT轉換的選項。
19. **檢視>策略>虛擬裝置**。允許您檢視IPS裝置上的虛擬感測器策略。此策略用於建立虛擬感測器。
20. **View > Policies > FlexConfig**。允許您檢視FlexConfigs，這是可以部署到PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置的附加CLI命令和說明。

檢視對象許可權

安全管理器包括以下對象檢視許可權：

1. **檢視>對象> AAA伺服器組**。允許您檢視AAA伺服器組對象。這些對象用於需要AAA服務（身份驗證、授權和記帳）的策略中。
2. **View > Objects > AAA Servers**。允許您檢視AAA伺服器對象。這些對象表示定義為AAA伺服器組一部分的單個AAA伺服器。
3. **檢視>對象>訪問控制清單 — 標準/擴展**。允許您檢視標準和擴展ACL對象。擴展ACL對象用於各種策略（例如NAT和NAC）和建立VPN訪問。標準ACL對象用於OSPF和SNMP等策略以及建立VPN訪問。
4. **View > Objects > Access Control Lists** - Web。允許您檢視Web ACL對象。Web ACL對象用於在SSL VPN策略中執行內容過濾。
5. **檢視>對象> ASA使用者組**。允許您檢視ASA使用者組對象。這些對象在ASA安全裝置上配置為Easy VPN、遠端訪問VPN和SSL VPN配置。
6. **檢視>對象>類別**。允許您檢視類別對象。這些對象有助於通過使用顏色輕鬆地識別規則表中的規則和對象。
7. **檢視>對象>身份證明**。允許您檢視憑據對象。這些對象在IKE擴展身份驗證(Xauth)期間用於Easy VPN配置。
8. **檢視>對象> FlexConfigs**。允許您檢視FlexConfig對象。這些對象包含帶有其他指令碼語言說明的配置命令，可用於配置安全管理器使用者介面不支援的命令。
9. **「檢視」>「對象」>「IKE提議」**。允許您檢視IKE建議對象。這些對象包含遠端訪問VPN策略中的IKE建議所需的引數。
10. **View > Objects > Inspect - Class Maps** - DNS。允許您檢視DNS類對映對象。這些對象匹配具有特定條件的DNS流量，以便可以對該流量執行操作。
11. **View > Objects > Inspect - Class Maps - FTP**。允許您檢視FTP類對映對象。這些對象匹配具有特定條件的FTP流量，以便可以對該流量執行操作。
12. **檢視>對象>檢查 — 類對映 — HTTP**。允許您檢視HTTP類對映對象。這些對象匹配具有特定條件的HTTP流量，以便可以對該流量執行操作。

13. **檢視>對象>檢查 — 類對映 — IM**。允許您檢視IM類對映對象。這些對象與具有特定條件的IM流量匹配，以便可以對該流量執行操作。
14. **View > Objects > Inspect - Class Maps - SIP**。允許您檢視SIP類對映對象。這些對象匹配具有特定條件的SIP流量，以便可以對該流量執行操作。
15. **檢視>對象>檢查 — 策略對映 — DNS。**允許您檢視DNS策略對映對象。這些對象用於為DNS流量建立檢測對映。
16. **View > Objects > Inspect - Policy Maps - FTP。**允許您檢視FTP策略對映對象。這些對象用於為FTP流量建立檢測對映。
17. **View > Objects > Inspect - Policy Maps - GTP**。允許您檢視GTP策略對映對象。這些對象用於為GTP流量建立檢測對映。
18. **View > Objects > Inspect - Policy Maps - HTTP(ASA7.1.x/PIX7.1.x/IOS)**。 允許您檢視為ASA/PIX 7.1.x裝置和IOS路由器建立的HTTP策略對映對象。這些對象用於為HTTP流量建立檢測對映。
19. **View > Objects > Inspect - Policy Maps - HTTP(ASA7.2/PIX7.2)**。 允許您檢視為ASA 7.2/PIX 7.2裝置建立的HTTP策略對映對象。這些對象用於為HTTP流量建立檢測對映。
20. **View > Objects > Inspect - Policy Maps - IM(ASA7.2/PIX7.2)**。 允許您檢視為ASA 7.2/PIX 7.2裝置建立的IM策略對映對象。這些對象用於為IM流量建立檢測對映。
21. **View > Objects > Inspect - Policy Maps - IM(IOS)**。 允許您檢視為IOS裝置建立的IM策略對映對象。這些對象用於為IM流量建立檢測對映。
22. **View > Objects > Inspect - Policy Maps - SIP**。允許您檢視SIP策略對映對象。這些對象用於為SIP流量建立檢測對映。
23. **檢視>對象>檢查 — 正規表示式**。允許您檢視正規表示式對象。這些對象代表被定義為正規表示式組一部分的各個正規表示式。
24. **檢視>對象>檢查 — 正規表示式組**。用於檢視正規表示式組對象。某些類對映和檢查對映使用這些對象來匹配資料包內的文本。
25. **View > Objects > Inspect - TCP Maps**。允許您檢視TCP對映對象。這些對象在兩個方向上自定義對TCP流的檢查。
26. **檢視>對象>介面角色**。允許您檢視介面角色對象。這些對象定義可表示不同型別裝置上的多個介面的命名模式。介面角色使您能夠將策略應用到多個裝置上的特定介面，而不必手動定義每個介面的名稱。
27. **檢視>對象> IPsec轉換集**。允許您檢視IPsec轉換集對象。這些對象包括安全協定、演算法和其他設定的組合，這些設定具體指定IPsec隧道中的資料將如何加密和身份驗證。
28. **「檢視」>「對象」>「LDAP屬性對映」**。允許您檢視LDAP屬性對映對象。這些對象用於將自定義（使用者定義的）屬性名稱對映到思科LDAP屬性名稱。
29. **檢視>對象>網路/主機**。允許您檢視網路/主機對象。這些對象是代表網路、主機或兩者的IP地址的邏輯集合。網路/主機對象使您能夠定義策略，而無需單獨指定每個網路或主機。
30. **檢視>對象> PKI註冊**。允許您檢視PKI註冊對象。這些對象定義在公共金鑰基礎結構中運行的證書頒發機構(CA)伺服器。
31. **View > Objects > Port Forwarding Lists**。允許您檢視埠轉發清單對象。這些對象定義遠端客戶端上的埠號到應用IP地址和SSL VPN網關後埠的對映。
32. **檢視>對象>安全案頭配置**。允許您檢視安全案頭配置對象。這些對象是可重用的命名元件，SSL VPN策略可以引用這些對象，從而提供一種可靠的方法來消除在SSL VPN會話期間共用的所有敏感資料跟蹤。
33. **檢視>對象>服務 — 埠清單**。允許您檢視埠清單對象。這些對象包含一個或多個埠號範圍，用於簡化建立服務對象的過程。
34. **View > Objects > Services/Service Groups**允許您檢視服務和服務組對象。這些對象是描述策略使用的網路服務（如Kerberos、SSH和POP3）的協定和埠定義的對映定義。
35. **「檢視」>「對象」>「一次登入伺服器」**。允許您檢視一次登入伺服器對象。單點登入

(SSO)允許SSL VPN使用者輸入一次使用者名稱和密碼，並能夠訪問多個受保護服務和Web伺服器。

36. **檢視>對象> SLA監控器**。允許您檢視SLA監控器對象。運行7.2版或更高版本的PIX/ASA安全裝置使用這些對象來執行路由跟蹤。此功能提供了一種跟蹤主路由的可用性並在主路由失敗時安裝備用路由的方法。
37. **View > Objects > SSL VPN Customizations**。允許您檢視SSL VPN自定義對象。這些對象定義如何更改向使用者顯示的SSL VPN頁面的外觀，如登入/註銷和首頁。
38. **View > Objects > SSL VPN Gateways**。允許您檢視SSL VPN網關對象。這些對象定義使網關能夠用作連線到SSL VPN中受保護資源的代理的引數。
39. **「檢視」>「對象」>「樣式對象」**。允許您檢視樣式對象。通過這些對象，您可以配置樣式元素（如字型特徵和顏色），以自定義SSL VPN使用者在連線到安全裝置時顯示的SSL VPN頁面的外觀。
40. **「檢視」>「對象」>「文本對象」**。允許您檢視自由格式文本對象。這些對象包括名稱和值對，其中值可以是單個字串、字串清單或字串表。
41. **檢視>對象>時間範圍。**允許您檢視時間範圍對象。這些對象用於建立基於時間的ACL和檢查規則。在定義ASA使用者組時，也使用它們來將VPN訪問限制在一週內的特定時間。
42. **檢視>對象>通訊流**。允許您檢視流量對象。這些對象定義特定資料流供PIX 7.x/ASA 7.x裝置使用。
43. **「檢視」>「對象」>「URL清單」**。允許您檢視URL清單對象。這些對象定義成功登入後在門戶頁面上顯示的URL。這樣，使用者在無客戶端訪問模式下操作時就可以訪問SSL VPN網站上的可用資源。
44. **檢視>對象>使用者組**。可用於檢視使用者組對象。這些對象定義在Easy VPN拓撲、遠端訪問VPN和SSL VPN中使用的遠端客戶端組。
45. **檢視>對象> WINS伺服器清單**。允許您檢視WINS伺服器清單對象。這些對象表示WINS伺服器，SSL VPN使用這些伺服器來訪問或共用遠端系統上的檔案。
46. **檢視>對象>內部 — DN規則**。允許您檢視DN策略使用的DN規則。這是由安全管理器使用的內部對象，不會顯示在策略對象管理器中。
47. **檢視>對象>內部 — 客戶端更新**。這是未顯示在策略對象管理器中的使用者組對象所需的內部對象。
48. **檢視>對象>內部 — 標準ACE**。這是ACL對象使用的標準訪問控制條目的內部對象。
49. **檢視>對象>內部 — 擴展ACE。**這是ACL對象使用的擴展訪問控制條目的內部對象。

其他檢視許可權

安全管理器包括以下附加檢視許可權：

1. **View > Admin**。允許您檢視安全管理器管理設定。
2. **View > CLI**。允許您檢視在裝置上配置的CLI命令，並預覽將要部署的命令。
3. **View > Config Archive**。允許您檢視配置歸檔檔案中包含的配置清單。您無法檢視裝置配置或任何CLI命令。
4. **View > Devices**。允許您在「裝置」檢視中檢視裝置和所有相關資訊，包括其裝置設定、屬性、分配等。
5. **檢視>裝置管理器**。允許您為單個裝置啟動裝置管理器的只讀版本，例如用於Cisco IOS路由器的Cisco路由器和安全裝置管理器(SDM)。
6. **檢視>拓撲**。允許您檢視在對映檢視中配置的對映。

修改許可權

在安全管理器中修改（讀取/寫入）許可權分為以下類別：

- 修改策略許可權
- 修改對象許可權
- 其他修改許可權

修改策略許可權

注意：指定修改策略許可權時，請確保也選擇了相應的分配和檢視策略許可權。

安全管理器包括以下策略修改許可權：

1. **修改>策略>防火牆。**允許您修改PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置上的防火牆服務策略（位於防火牆下的策略選擇器中）。防火牆服務策略的示例包括訪問規則、AAA規則和檢查規則。
2. **Modify > Policies > Intrusion Prevention System。**允許您修改IPS策略（位於IPS下的策略選擇器中），包括在IOS路由器上運行的IPS的策略。此許可權還允許您在「特徵碼更新」嚮導（位於「工具」>「應用IPS更新」下）中調整特徵碼。
3. **修改>策略>影象。**允許您在「應用IPS更新」嚮導（位於「工具」>「應用IPS更新」下）中將特徵碼更新軟體包分配給裝置。 此許可權還允許您為特定裝置分配自動更新設定（位於「工具」>「安全管理器管理」>「IPS更新」下）。
4. **Modify > Policies > NAT。**允許您修改PIX/ASA/FWSM裝置和IOS路由器上的網路地址轉換策略。NAT策略的示例包括靜態規則和動態規則。
5. **Modify > Policies > Site-to-Site VPN。**允許您在PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置上修改站點到站點VPN策略。站點到站點VPN策略的示例包括IKE提議、IPsec提議和預共用金鑰。
6. **Modify > Policies > Remote Access VPN。**允許您在PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置上修改遠端訪問VPN策略。遠端訪問VPN策略的示例包括IKE提議、IPsec提議和PKI策略。
7. **Modify > Policies > SSL VPN。**允許您修改PIX/ASA/FWSM裝置和IOS路由器上的SSL VPN策略，如SSL VPN嚮導。
8. **Modify > Policies > Interfaces。**允許您修改PIX/ASA/FWSM裝置、IOS路由器、IPS感測器和Catalyst 6500/7600裝置上的介面策略（位於介面下的策略選擇器中）：在PIX/ASA/FWSM裝置上，此許可權涵蓋硬體埠和介面設定。在IOS路由器上，此許可權涵蓋基本和高級介面設定，以及其他與介面相關的策略，如DSL、PVC、PPP和撥號器策略。在IPS感測器上，此許可權涵蓋物理介面和摘要對映。在Catalyst 6500/7600裝置上，此許可權涵蓋介面和VLAN設定。
9. **修改>策略>橋接。**允許您修改PIX/ASA/FWSM裝置上的ARP表策略（位於Platform > Bridging下的Policy selector中）。
10. **修改>策略>裝置管理。**允許您在PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置上修改裝置管理策略（位於Platform > Device Admin下的Policy選擇器中）：在PIX/ASA/FWSM裝置上，示例包括裝置訪問策略、伺服器訪問策略和故障切換策略。在IOS路由器上，示例包括裝置訪問（包括線路訪問）策略、伺服器訪問策略、AAA和安全裝置調配。在IPS感測器上，此許可權涵蓋裝置訪問策略和伺服器訪問策略。在Catalyst 6500/7600裝置上，此許可權涵蓋IDSM設定和VLAN訪問清單。
11. **修改>策略>身份。**允許您在Cisco IOS路由器上修改身份策略（位於Platform > Identity下的策略選擇器中），包括802.1x和網路准入控制(NAC)策略。
12. **修改>策略>日誌記錄。**允許您在PIX/ASA/FWSM裝置、IOS路由器和IPS感測器上修改日誌記錄策略（位於Platform > Logging下的Policy selector中）。日誌策略示例包括日誌設定、

伺服器設定和系統日誌伺服器策略。

13. **Modify > Policies > Multicast**。允許您在PIX/ASA/FWSM裝置上修改組播策略（位於Platform > Multicast下的Policy selector中）。組播策略的示例包括組播路由和IGMP策略。
14. **修改>策略> QoS**。允許您在Cisco IOS路由器上修改QoS策略（位於Platform > Quality of Service下的Policy選擇器中）。
15. **修改>策略>路由**。允許您在PIX/ASA/FWSM裝置和IOS路由器上修改路由策略（位於Platform > Routing下的Policy selector中）。路由策略的示例包括OSPF、RIP和靜態路由策略。
16. **修改>策略>安全性**。允許您在PIX/ASA/FWSM裝置和IPS感測器上修改安全策略（位於Platform > Security下的Policy selector中）：在PIX/ASA/FWSM裝置上，安全策略包括反欺騙、分片和超時設定。在IPS感測器上，安全策略包括阻止設定。
17. **修改>策略>服務策略規則**。允許您在PIX 7.x/ASA裝置上修改服務策略規則策略（位於平台>服務策略規則下的策略選擇器中）。示例包括優先順序隊列和IPS、QoS以及連線規則。
18. **修改>策略>使用者首選項**。允許您在PIX/ASA/FWSM裝置上修改部署策略（位於Platform > User Preferences下的Policy selector）。此策略包含用於清除部署中的所有NAT轉換的選項。
19. **修改>策略>虛擬裝置**。允許您修改IPS裝置上的虛擬感測器策略。使用此策略建立虛擬感測器。
20. **修改>策略> FlexConfig**。允許您修改FlexConfigs，這是可以部署到PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置的附加CLI命令和指令。

修改對象許可權

安全管理器包括以下對象檢視許可權：

1. **Modify > Objects > AAA Server Groups**。允許您檢視AAA伺服器組對象。這些對象用於需要AAA服務（身份驗證、授權和記帳）的策略中。
2. **Modify > Objects > AAA Servers**。允許您檢視AAA伺服器對象。這些對象表示定義為AAA伺服器組一部分的單個AAA伺服器。
3. **修改>對象>訪問控制清單 — 標準/擴展**。允許您檢視標準和擴展ACL對象。擴展ACL對象用於各種策略（例如NAT和NAC）和建立VPN訪問。標準ACL對象用於OSPF和SNMP等策略以及建立VPN訪問。
4. **修改>對象>訪問控制清單 — Web**。允許您檢視Web ACL對象。Web ACL對象用於在SSL VPN策略中執行內容過濾。
5. **Modify > Objects > ASA** User Groups。允許您檢視ASA使用者組對象。這些對象在ASA安全裝置上配置為Easy VPN、遠端訪問VPN和SSL VPN配置。
6. **修改>對象>類別**。允許您檢視類別對象。這些對象有助於通過使用顏色輕鬆地識別規則表中的規則和對象。
7. **修改>對象>身份證明**。允許您檢視憑據對象。這些對象在IKE擴展身份驗證(Xauth)期間用於Easy VPN配置。
8. **修改>對象> FlexConfigs**。允許您檢視FlexConfig對象。這些對象包含帶有其他指令碼語言說明的配置命令，可用於配置安全管理器使用者介面不支援的命令。
9. **修改>對象> IKE提議**。允許您檢視IKE建議對象。這些對象包含遠端訪問VPN策略中的IKE建議所需的引數。
10. **修改>對象>檢查 — 類對映 — DNS**。允許您檢視DNS類對映對象。這些對象匹配具有特定條件的DNS流量，以便可以對該流量執行操作。
11. **修改>對象>檢查 — 類對映 — FTP**。允許您檢視FTP類對映對象。這些對象匹配具有特定條件的FTP流量，以便可以對該流量執行操作。

12. **修改>對象>檢查 — 類對映 — HTTP**。允許您檢視HTTP類對映對象。這些對象匹配具有特定條件的HTTP流量，以便可以對該流量執行操作。
13. **修改>對象>檢查 — 類對映 — IM**。允許您檢視IM類對映對象。這些對象與具有特定條件的IM流量匹配，以便可以對該流量執行操作。
14. **修改>對象>檢查 — 類對映 — SIP**。允許您檢視SIP類對映對象。這些對象匹配具有特定條件的SIP流量，以便可以對該流量執行操作。
15. **修改>對象>檢查 — 策略對映 — DNS**。允許您檢視DNS策略對映對象。這些對象用於為DNS流量建立檢測對映。
16. **Modify > Objects > Inspect - Policy Maps - FTP**。允許您檢視FTP策略對映對象。這些對象用於為FTP流量建立檢測對映。
17. **Modify > Objects > Inspect - Policy Maps - HTTP(ASA7.1.x/PIX7.1.x/IOS)**。 允許您檢視為ASA/PIX 7.x裝置和IOS路由器建立的HTTP策略對映對象。這些對象用於為HTTP流量建立檢測對映。
18. **Modify > Objects > Inspect - Policy Maps - HTTP(ASA7.2/PIX7.2)**。 允許您檢視為ASA 7.2/PIX 7.2裝置建立的HTTP策略對映對象。這些對象用於為HTTP流量建立檢測對映。
19. **Modify > Objects > Inspect - Policy Maps - IM(ASA7.2/PIX7.2)**。 允許您檢視為ASA 7.2/PIX 7.2裝置建立的IM策略對映對象。這些對象用於為IM流量建立檢測對映。
20. **Modify > Objects > Inspect - Policy Maps - IM(IOS)**。 允許您檢視為IOS裝置建立的IM策略對映對象。這些對象用於為IM流量建立檢測對映。
21. **修改>對象>檢查 — 策略對映 — SIP**。允許您檢視SIP策略對映對象。這些對象用於為SIP流量建立檢測對映。
22. **修改>對象>檢查 — 正規表示式**。允許您檢視正規表示式對象。這些對象代表被定義為正規表示式組一部分的各個正規表示式。
23. **修改>對象>檢查 — 正規表示式組**。用於檢視正規表示式組對象。某些類對映和檢查對映使用這些對象來匹配資料包內的文本。
24. **修改>對象>檢查 — TCP對映**。允許您檢視TCP對映對象。這些對象在兩個方向上自定義對TCP流的檢查。
25. **修改>對象>介面角色**。允許您檢視介面角色對象。這些對象定義可表示不同型別裝置上的多個介面的命名模式。介面角色使您能夠將策略應用到多個裝置上的特定介面，而不必手動定義每個介面的名稱。
26. **修改>對象> IPsec轉換集**。允許您檢視IPsec轉換集對象。這些對象包括安全協定、演算法和其他設定的組合，這些設定具體指定IPsec隧道中的資料將如何加密和身份驗證。
27. **修改>對象> LDAP屬性對映**。允許您檢視LDAP屬性對映對象。這些對象用於將自定義（使用者定義的）屬性名稱對映到思科LDAP屬性名稱。
28. **修改>對象>網路/主機**。允許您檢視網路/主機對象。這些對象是代表網路、主機或兩者的IP地址的邏輯集合。網路/主機對象使您能夠定義策略，而無需單獨指定每個網路或主機。
29. **修改>對象> PKI註冊**。允許您檢視PKI註冊對象。這些對象定義在公共金鑰基礎結構中運行的證書頒發機構(CA)伺服器。
30. **修改>對象>埠轉發清單**。允許您檢視埠轉發清單對象。這些對象定義遠端客戶端上的埠號到應用IP地址和SSL VPN網關後埠的對映。
31. **修改>對象>安全案頭配置**。允許您檢視安全案頭配置對象。這些對象是可重用的命名元件，SSL VPN策略可以引用這些對象，從而提供一種可靠的方法來消除在SSL VPN會話期間共用的所有敏感資料跟蹤。
32. **修改>對象>服務 — 埠清單**。允許您檢視埠清單對象。這些對象包含一個或多個埠號範圍，用於簡化建立服務對象的過程。
33. **修改>對象>服務/服務組。**允許您檢視服務和服務組對象。這些對象是描述策略使用的網路服務（如Kerberos、SSH和POP3）的協定和埠定義的對映定義。
34. **修改>對象>單點登入伺服器。**允許您檢視一次登入伺服器對象。單點登入(SSO)允許SSL

VPN使用者輸入一次使用者名稱和密碼，並能夠訪問多個受保護服務和Web伺服器。

35. **修改>對象> SLA監控器**。允許您檢視SLA監控器對象。運行7.2版或更高版本的PIX/ASA安全裝置使用這些對象來執行路由跟蹤。此功能提供了一種跟蹤主路由的可用性並在主路由失敗時安裝備用路由的方法。
36. **Modify > Objects > SSL VPN Customizations**。允許您檢視SSL VPN自定義對象。這些對象定義如何更改向使用者顯示的SSL VPN頁面的外觀，如登入/註銷和首頁。
37. **Modify > Objects > SSL VPN Gateways**。允許您檢視SSL VPN網關對象。這些對象定義使網關能夠用作連線到SSL VPN中受保護資源的代理的引數。
38. **「修改」>「對象」>「樣式對象」**。允許您檢視樣式對象。通過這些對象，您可以配置樣式元素（如字型特徵和顏色），以自定義SSL VPN使用者在連線到安全裝置時顯示的SSL VPN頁面的外觀。
39. **修改>對象>文本對象**。允許您檢視自由格式文本對象。這些對象包括名稱和值對，其中值可以是單個字串、字串清單或字串表。
40. **修改>對象>時間範圍。**允許您檢視時間範圍對象。這些對象用於建立基於時間的ACL和檢查規則。在定義ASA使用者組時，也使用它們來將VPN訪問限制在一週內的特定時間。
41. **修改>對象>流量**。允許您檢視流量對象。這些對象定義特定資料流供PIX 7.x/ASA 7.x裝置使用。
42. **修改>對象> URL清單**。允許您檢視URL清單對象。這些對象定義成功登入後在門戶頁面上顯示的URL。這樣，使用者在無客戶端訪問模式下操作時就可以訪問SSL VPN網站上的可用資源。
43. **修改>對象>使用者組**。可用於檢視使用者組對象。這些對象定義在Easy VPN拓撲、遠端訪問VPN和SSL VPN中使用的遠端客戶端組
44. **修改>對象> WINS伺服器清單**。允許您檢視WINS伺服器清單對象。這些對象表示WINS伺服器，SSL VPN使用這些伺服器來訪問或共用遠端系統上的檔案。
45. **修改>對象>內部 — DN規則。**允許您檢視DN策略使用的DN規則。這是由安全管理器使用的內部對象，不會顯示在策略對象管理器中。
46. **修改>對象>內部 — 客戶端更新**。這是未顯示在策略對象管理器中的使用者組對象所需的內部對象。
47. **修改>對象>內部 — 標準ACE**。這是ACL對象使用的標準訪問控制條目的內部對象。
48. **Modify > Objects > Internal - Extended ACE**。這是ACL對象使用的擴展訪問控制條目的內部對象。

其他修改許可權

安全管理器包括其他修改許可權，如下所示：

1. **Modify > Admin**。允許您修改安全管理器管理設定。
2. **Modify > Config Archive**。允許您在配置歸檔檔案中修改裝置配置。此外，它還允許您向歸檔檔案新增配置並自定義配置歸檔工具。
3. **Modify > Devices**。允許您新增和刪除裝置，以及修改裝置屬性和屬性。要發現要新增的裝置上的策略，還必須啟用「匯入」許可權。此外，如果啟用Modify > Devices許可權，請確保還啟用了Assign > Policies > Interfaces許可權。
4. **修改>層次結構**。允許您修改裝置組。
5. **修改>拓撲**。允許您在「對映」檢視中修改對映。

分配許可權

安全管理器包括策略分配許可權，如下所示：

1. **Assign > Policies > Firewall**。允許您將防火牆服務策略（位於防火牆下的策略選擇器中）分配給PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置。防火牆服務策略的示例包括訪問規則、AAA規則和檢查規則。
2. **Assign > Policies > Intrusion Prevention System**。允許您分配IPS策略（位於IPS下的策略選擇器中），包括在IOS路由器上運行的IPS的策略。
3. **Assign > Policies > Image**。安全管理器當前未使用此許可權。
4. **Assign > Policies > NAT**。允許您為PIX/ASA/FWSM裝置和IOS路由器分配網路地址轉換策略。NAT策略的示例包括靜態規則和動態規則。
5. **Assign > Policies > Site-to-Site VPN**。允許將站點到站點VPN策略分配給PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置。站點到站點VPN策略的示例包括IKE提議、IPsec提議和預共用金鑰。
6. **Assign > Policies > Remote Access VPN**。允許將遠端訪問VPN策略分配給PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置。遠端訪問VPN策略的示例包括IKE提議、IPsec提議和PKI策略。
7. **Assign > Policies > SSL VPN**。允許您將SSL VPN策略分配給PIX/ASA/FWSM裝置和IOS路由器，如SSL VPN嚮導。
8. **Assign > Policies > Interfaces**。允許您將介面策略（位於Interfaces下的Policy selector中）分配給PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置：在PIX/ASA/FWSM裝置上，此許可權涵蓋硬體埠和介面設定。在IOS路由器上，此許可權涵蓋基本和高級介面設定，以及其他與介面相關的策略，如DSL、PVC、PPP和撥號器策略。在Catalyst 6500/7600裝置上，此許可權涵蓋介面和VLAN設定。
9. **Assign > Policies > Bridging**。允許您將ARP表策略（位於Platform > Bridging下的Policy selector）分配給PIX/ASA/FWSM裝置。
10. **Assign > Policies > Device Administration**。允許您將裝置管理策略（位於Platform > Device Admin下的Policy selector中）分配給PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置：在PIX/ASA/FWSM裝置上，示例包括裝置訪問策略、伺服器訪問策略和故障切換策略。在IOS路由器上，示例包括裝置訪問（包括線路訪問）策略、伺服器訪問策略、AAA和安全裝置調配。在IPS感測器上，此許可權涵蓋裝置訪問策略和伺服器訪問策略。在Catalyst 6500/7600裝置上，此許可權涵蓋IDSM設定和VLAN存取清單。
11. **Assign > Policies > Identity**。允許您將身份策略（位於Platform > Identity下的策略選擇器中）分配給Cisco IOS路由器，包括802.1x和網路准入控制(NAC)策略。
12. **Assign > Policies > Logging**。允許您將日誌記錄策略（位於Platform > Logging下的Policy selector中）分配給PIX/ASA/FWSM裝置和IOS路由器。日誌策略示例包括日誌設定、伺服器設定和系統日誌伺服器策略。
13. **Assign > Policies > Multicast**。允許您將組播策略（位於Platform > Multicast下的Policy selector中）分配給PIX/ASA/FWSM裝置。組播策略的示例包括組播路由和IGMP策略。
14. **Assign > Policies > QoS**。允許您將QoS策略（位於Platform > Quality of Service下的Policy選擇器中）分配給Cisco IOS路由器。
15. **Assign > Policies > Routing**。允許您將路由策略（位於Platform > Routing下的Policy selector中）分配給PIX/ASA/FWSM裝置和IOS路由器。路由策略的示例包括OSPF、RIP和靜態路由策略。
16. **Assign > Policies > Security**。允許您將安全策略（位於Platform > Security下的Policy selector中）分配給PIX/ASA/FWSM裝置。安全策略包括反欺騙、分片和超時設定。
17. **Assign > Policies > Service Policy Rules**。允許您將服務策略規則策略（位於Platform > Service Policy Rules下的Policy選擇器中）分配給PIX 7.x/ASA裝置。示例包括優先順序隊列和IPS、QoS以及連線規則。
18. **Assign > Policies > User Preferences**。允許您將部署策略（位於Platform > User Preferences下的Policy selector）分配給PIX/ASA/FWSM裝置。此策略包含用於清除部署中

的所有NAT轉換的選項。

19. **Assign > Policies > Virtual Device**。允許將虛擬感測器策略分配給IPS裝置。使用此策略建立虛擬感測器。
20. **Assign > Policies > FlexConfig**。允許您分配FlexConfigs，這是可以部署到PIX/ASA/FWSM裝置、IOS路由器和Catalyst 6500/7600裝置的附加CLI命令和指令。

注意：指定分配許可權時，請確保也選擇了相應的檢視許可權。

批准許可權

安全管理器提供批准許可權，如下所示：

1. **批准> CLI**。允許您批准部署作業中包含的CLI命令更改。
2. **批准>策略**。允許您批准在工作流活動中配置的策略中包含的配置更改。

瞭解CiscoWorks角色

在CiscoWorks公共服務中建立使用者時，會為其分配一個或多個角色。與每個角色關聯的許可權確定每個使用者有權在安全管理器中執行的操作。

以下主題介紹CiscoWorks角色：

- CiscoWorks常見服務預設角色
- 在CiscoWorks Common Services中為使用者分配角色

CiscoWorks常見服務預設角色

CiscoWorks Common Services包含以下預設角色：

1. **幫助台** — 幫助台使用者可以檢視（但不能修改）裝置、策略、對象和拓撲圖。
2. **網路操作**員 — 除了檢視許可權之外，網路操作員還可以檢視CLI命令和安全管理器管理設定。網路操作員還可以修改配置歸檔檔案，並向裝置發出命令（如ping）。
3. **Approver** — 除檢視許可權外，審批人還可以批准或拒絕部署作業。它們無法執行部署。
4. **網路管理**員 — 網路管理員擁有完整的檢視和修改許可權，修改管理設定除外。它們可以發現裝置以及這些裝置上配置的策略，將策略分配給裝置，並向裝置發出命令。網路管理員無法批准活動或部署作業；但是，他們可以部署其他使用者批准的作業。
5. **系統管理**員 — 系統管理員擁有對所有安全管理器許可權的完整訪問許可權，包括修改、策略分配、活動和作業批准、發現、部署以及向裝置發出命令。

注意：如果在伺服器上安裝了其他應用程式，則其他角色（如匯出資料）可能會顯示在Common Services中。匯出資料角色供第三方開發人員使用，安全管理器不使用此角色。

提示： 雖然無法更改CiscoWorks角色的定義，但您可以定義將哪些角色分配給每個使用者。有關詳細資訊，請參閱在CiscoWorks公共服務中向使用者分配角色。

在CiscoWorks Common Services中為使用者分配角色

CiscoWorks Common Services使您能夠定義將哪些角色分配給每個使用者。通過更改使用者的角色定義，可以更改此使用者有權在安全管理器中執行的操作的型別。例如，如果您指定了「幫助台」角色，則使用者只能檢視操作，並且不能修改任何資料。但是，如果您指定了Network

Operator角色，使用者也可以修改配置存檔。可以為每個使用者分配多個角色。

注意：在對使用者許可權進行更改後，必須重新啟動安全管理器。

過程：

1. 在Common Services中，選擇**Server > Security**，然後從目錄中選擇**Single-Server Trust Management > Local User Setup**。**提示：**要從安全管理器訪問「本地使用者設定」頁，請選擇「工具」>「安全管理器管理」>「伺服器安全」，然後按一下「本地使用者設定」。
2. 選中現有使用者旁邊的覈取方塊，然後按一下**Edit**。
3. 在「使用者資訊」頁面上，通過按一下覈取方塊選擇要分配給此使用者的角色。有關每個角色的詳細資訊，請參閱CiscoWorks常見服務預設角色。
4. 按一下「**OK**」以儲存變更內容。
5. 重新啟動安全管理器。

瞭解Cisco Secure ACS角色

與CiscoWorks相比，Cisco Secure ACS在管理安全管理器許可權方面提供了更大的靈活性，因為它支援您可以配置的特定於應用的角色。每個角色都由確定對安全管理器任務的授權級別的一組許可權組成。在Cisco Secure ACS中，您為每個使用者組分配一個角色（也可以將角色分配給單個使用者），這樣，該組中的每個使用者都可以執行由該角色定義的許可權授權的操作。

此外，您可以將這些角色分配給Cisco Secure ACS裝置組，從而在不同裝置集上區分許可權。

注意：Cisco Secure ACS裝置組獨立於安全管理器裝置組。

以下主題介紹Cisco Secure ACS角色：

- Cisco Secure ACS預設角色
- 自定義Cisco Secure ACS角色

Cisco Secure ACS預設角色

Cisco Secure ACS包含與CiscoWorks相同的角色(請參閱瞭解CiscoWorks角色)，此外還包括以下附加角色：

1. **Security Approver** — 安全審批人可以檢視（但不能修改）裝置、策略、對象、對映、CLI命令和管理設定。此外，安全審批人還可以批准或拒絕活動中包含的配置更改。他們不能批准或拒絕部署作業，也不能執行部署。
2. **安全管**理員 — 除了具有檢視許可權之外，安全管理員還可以修改裝置、裝置組、策略、對象和拓撲圖。他們還可以將策略分配給裝置和VPN拓撲，並執行發現以將新裝置匯入系統。
3. **網路管**理員 — 除了檢視許可權之外，網路管理員還可以修改配置存檔、執行部署並向裝置發出命令。

注意：Cisco Secure ACS網路管理員角色包含的許可權與CiscoWorks網路管理員角色包含的許可權不同。有關詳細資訊，請參閱瞭解CiscoWorks角色。

與CiscoWorks不同，Cisco Secure ACS允許您自定義與每個安全管理器角色關聯的許可權。有關修改預設角色的詳細資訊，請參閱自定義Cisco Secure ACS角色。

注意：必須安裝Cisco Secure ACS 3.3或更高版本才能進行安全管理器授權。

自定義Cisco Secure ACS角色

Cisco Secure ACS允許您修改與每個安全管理器角色關聯的許可權。您還可以通過建立專門的使用者角色來自定義Cisco Secure ACS，這些使用者角色具有針對特定安全管理器任務的許可權。

注意：在對使用者許可權進行更改後，必須重新啟動安全管理器。

過程：

1. 在Cisco Secure ACS中，按一下導航欄上的**Shared Profile Components**。
2. 在「共用元件」頁面上按一下**思科安全管理器**。將顯示為安全管理器配置的角色。
3. 執行下列操作之一：要建立角色，請按一下**Add**。轉至步驟4。要修改現有角色，請按一下該角色。轉至步驟5。
4. 輸入角色名稱以及說明（可選）。
5. 選擇並取消選擇許可權樹中的覈取方塊以定義此角色的許可權選中樹的一個分支的覈取方塊將選擇該分支中的所有許可權。例如，選擇**Assign**將選擇所有分配許可權。有關安全管理器許可權的完整清單，請參閱安全管理器許可權。**注意：**選擇修改、批准、分配、匯入、控制或部署許可權時，還必須選擇相應的檢視許可權；否則，安全管理器將無法正常工作。
6. 按一下**Submit**儲存更改。
7. 重新啟動安全管理器。

安全管理器中許可權和角色之間的預設關聯

此表顯示了安全管理器許可權如何與CiscoWorks Common Services角色和Cisco Secure ACS中的預設角色相關聯。

許可權	角色							
	系統管理員	安全管理員(ACS)	安全審批人(ACS)	網路管理員(CW)	網路管理員(ACS)	審批人	網路運營商	幫助台
檢視許可權								
檢視裝置	是	是	是	是	是	是	是	是
檢視策略	是	是	是	是	是	是	是	是
檢視對象	是	是	是	是	是	是	是	是
檢視拓撲	是	是	是	是	是	是	是	是
檢視CLI	是	是	是	是	是	是	是	否
檢視管理員	是	是	是	是	是	是	是	否
檢視配置存檔	是	是	是	是	是	是	是	是
檢視裝置管理器	是	是	是	是	是	是	是	否

修改許可權								
修改裝置	是	是	否	是	否	否	否	否
修改層次結構	是	是	否	是	否	否	否	否
修改策略	是	是	否	是	否	否	否	否
修改影象	是	是	否	是	否	否	否	否
修改對象	是	是	否	是	否	否	否	否
修改拓撲	是	是	否	是	否	否	否	否
修改管理員	是	否	否	否	否	否	否	否
修改配置存檔	是	是	否	是	是	否	是	否
其他許可權								
分配策略	是	是	否	是	否	否	否	否
批准策略	是	否	是	否	否	否	否	否
批准CLI	是	否	否	否	否	是	否	否
發現（匯入）	是	是	否	是	否	否	否	否
部署	是	否	否	是	是	否	否	否
控制	是	否	否	是	是	否	是	否
提交	是	是	否	是	否	否	否	否

相關資訊

- 思科安全管理員支援頁面
- 技術支援與文件 - Cisco Systems