

Cisco IQ虛擬裝置操作指南v1.2.0

簡介

Cisco IQ™為您提供各種增強功能和特性，旨在改善資產可視性、跨環境提供更智慧的洞察力，並簡化案例管理。此外，Cisco IQ AI Assistant等AI功能通過提供情景理解來最佳化運營成果和Cisco IQ使用者體驗，從而讓您能夠做出主動、明智的決策，並簡化客戶參與和成功的流程。

Cisco IQ On-Prem Air-Gapped是Cisco IQ的部署模式之一，專為具有嚴格合規性、資料主權和安全要求的嚴格監管行業的客戶設計。在此模式下，思科IQ作為獨立虛擬機器(VM)提供，稱為思科IQ虛擬裝置(VA)。VA完全在客戶的設施中運行，與外部網路完全隔離。為了維護這種隔離，可從Cisco IQ SaaS獲取軟體更新和維護包，並通過經批准的手動流程將其傳輸到VA。

Cisco IQ On-Prem Air-Gapped將Cisco IQ SaaS的關鍵功能擴展到空口環境，使任務關鍵型團隊能夠以與雲連線企業相當的速度和診斷智慧進行運營。

要訪問Cisco IQ VA，請開啟支援的瀏覽器，然後導航至<https://<fqdn-of-the-appliance>>。使用在安裝過程中設定的管理使用者名稱和密碼登入。

 附註：Cisco IQ VA目前僅限註冊參加受控可用性計畫的客戶。從Cisco IQ門戶下載訪問VA系統軟體和其他操作包（模組、規則和授權）的許可權專門提供給選定客戶。有關詳細資訊，請與您的客戶代表聯絡。

連線管理（資料收集）

思科IQ VA是一種用於網路資料收集的本地解決方案，可提供對您的基礎設施的深入可視性。它通過Catalyst Center和Direct Connection收集資料。它簡化了您管理網路身份驗證和裝置發現的方式。配置資料收集包括：

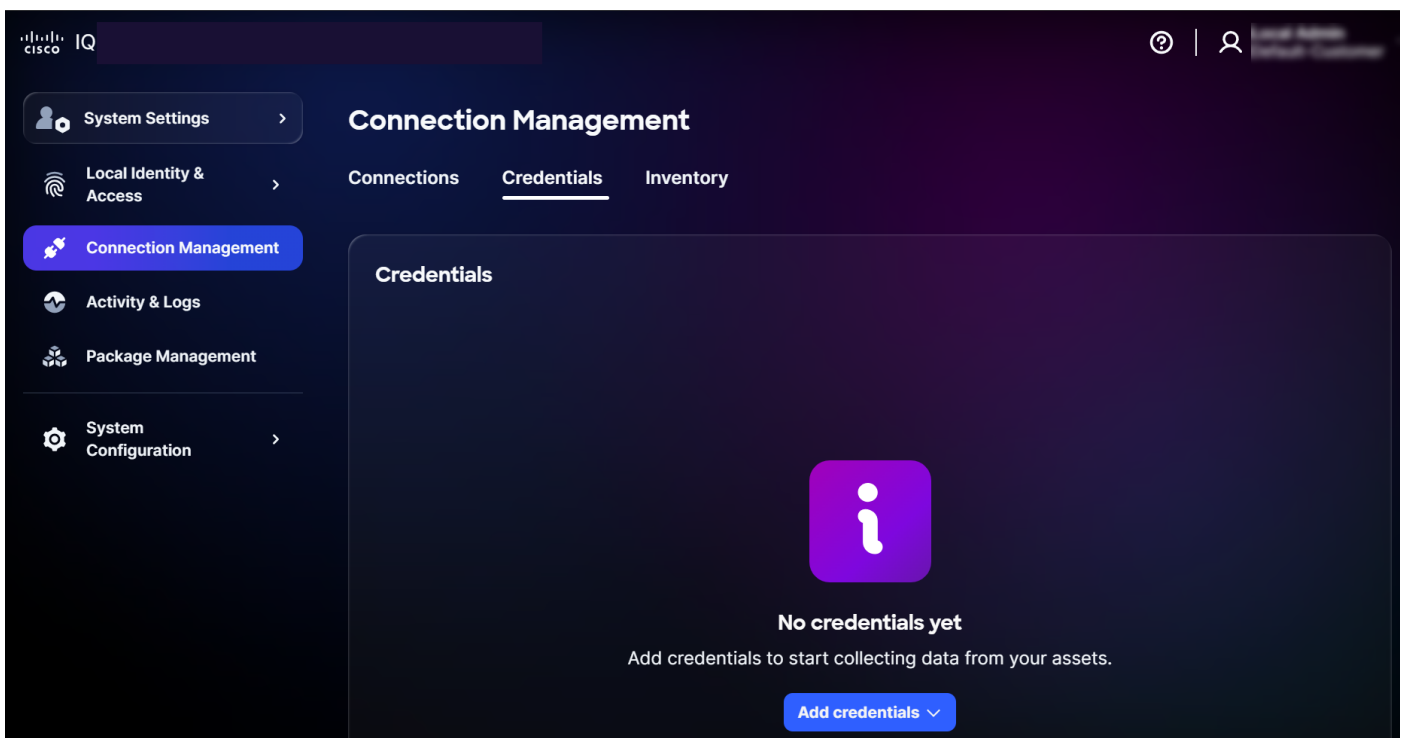
- 正在建立憑據集:建立驗證通訊協定(例如簡易網路管理通訊協定(SNMP)v1/v2c/v3)以與網路裝置通訊。通過按安全區域或位置集中憑據（例如，「SanJose-SNMPv3」），您可以在一個位置更新密碼，更改會自動傳播到所有關聯裝置。
- 將憑證對映到庫存:將憑證集與清單資產進行對映以自動執行身份驗證過程。通過建立將特定IP範圍連結到已定義的憑據集的規則，系統在資料收集期間自動應用正確的身份驗證。這消除了手動輸入錯誤，並確保隨著網路的增長您的配置保持準確。

 附註：裝置發現需要SNMPv2c/SNMPv3和SSH，並且在配置Catalyst Center之前必須提供HTTP/HTTPS憑證。

新增憑據

必須先新增憑據才能執行資料收集。要新增憑據，請執行以下操作：

1. 在System Settings中選擇Connection Management。系統隨即會顯示Connection Management頁面。
2. 按一下Credentials頁籤。



Credentials頁籤

3. 按一下Add credentials。

The screenshot shows the Cisco IQ interface with the 'Add Credentials' wizard. The left sidebar contains navigation links: System Settings, Local Identity & Access, Connection Management (highlighted), Activity & Logs, Package Management, and System Configuration. The main area has a breadcrumb '← Connection Management' and the title 'Add Credentials'. A progress bar shows three steps: 1. Credential Name and Protocols (active), 2. Enter Login Details, and 3. Specify IP Addresses. The active step contains a 'Name' input field, a 'Select at least one protocol' section with checkboxes for SNMPv3, SNMPv2, SSHv2, Telnet, and HTTP/HTTPS, and 'Cancel' and 'Next' buttons at the bottom.

新增憑據

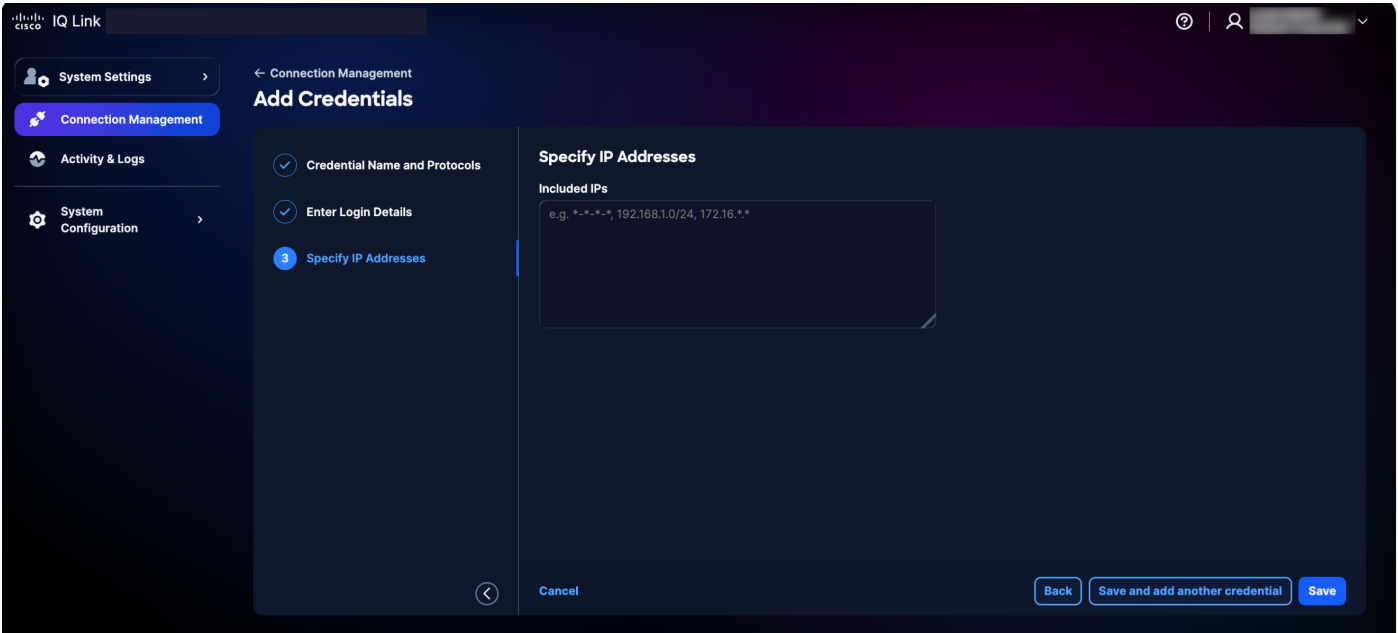
4. 輸入Name。
5. 選中所有適用的協定覈取方塊。
6. 按「Next」(下一步)。

The screenshot shows the 'Add Credentials' wizard at Step 2: Enter Login Details. The progress bar now shows Step 1 as completed with a checkmark, and Step 2 as active. The active step contains a section for 'SNMPv3' with fields for 'Username', 'Engine ID (optional)', 'Authorization algorithm' (a dropdown menu), 'Authorization password' (with a 'Show' button), 'Privacy algorithm' (a dropdown menu), and 'Privacy password (optional)' (with a 'Show' button). 'Cancel', 'Back', and 'Next' buttons are at the bottom.

新增憑據詳細資訊

 附註：對於上圖，說明在上一步中選擇了所有協定時的檢視。您的介面僅顯示您選擇的協定。

- 7. 輸入每個選定協定的登入詳細資訊。
- 8. 按「Next」(下一步)。

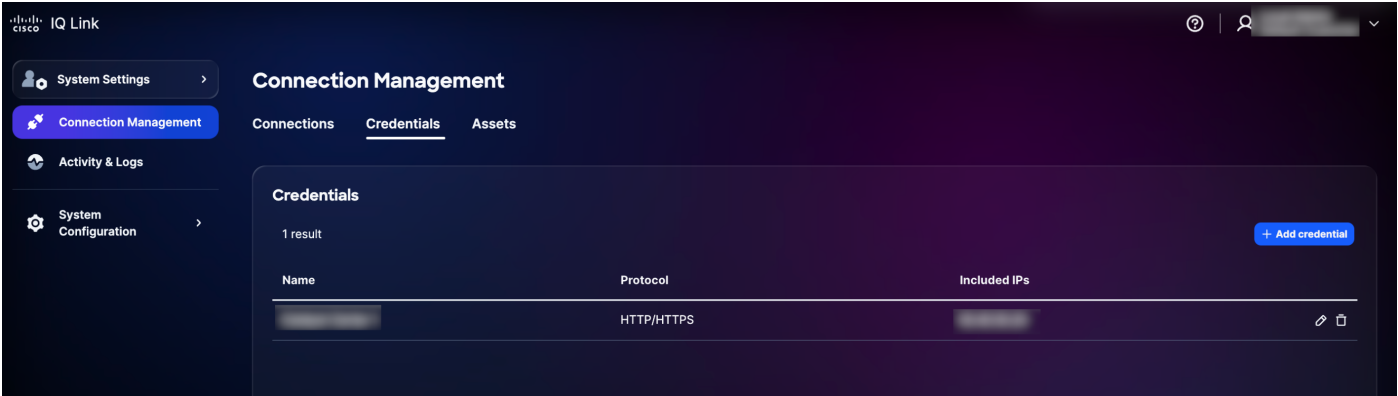


指定IP地址

- 9. 輸入Included IP。

 附註：此欄位定義可用於建立連線的IP地址或IP範圍。它支援IP和IP掩碼的組合 (使用萬用字元表示法)。有關支援的格式的詳細資訊，請參閱[憑據選擇和匹配邏輯](#)。

- 10. 按一下「Save」。系統將顯示一條確認消息，您將被重定向到Credentials頁籤。



憑據已新增

您可以通過按一下Edit圖示編輯憑證，然後按一下Delete圖示刪除憑證。

憑據選擇和匹配邏輯

遙測引擎使用基於優先順序的匹配邏輯來確定在發現和收集期間應用哪些憑證。瞭解此層次結構可確保為目標裝置使用正確的憑證。

- 優先順序排名：當多個憑證集應用於一台裝置時，Cisco IQ會根據它們與裝置的具體匹配程度來評估這些憑證集；系統將應用以下優先順序，並且優先使用更具體的匹配項：
 - 完全符合IP:最高優先順序
 - 尾隨萬用字元匹配:優先順序取決於尾隨星數；星星越少，表示更具體的匹配，因此優先順序越高
- 萬用字元格式規則:萬用字元(*)僅支援作為IP地址中的尾部字元；必須從右到左應用它們。
 - 支援的格式：
 - 1.2.3.* (最高優先順序)
 - 1.2.*.*
 - 1.*.*.*
 - *.*.*.* (最低優先順序)
 - 不支援的格式：
 - 前導萬用字元 (例如*.1.2.3)
 - 八位元之間的萬用字元 (例如10.10.*.20)
 - 使用短劃線或其他非標準分隔符

憑據選擇示例:

下表說明了當裝置匹配多個定義的模式時，遙測引擎如何選擇最合適的憑證集。

表 1：憑據選擇示例

裝置IP	可用的憑據集	所選憑據集
10.10.1.5	10.10.1.5、10.10.1、10.10..*	10.10.1.5 (完全匹配)
10.10.2.15	10.10.2.,10.10..*	10.10.2.* (更詳細)
10.10.5.50	10.10...	10.10.. (更具體一些)

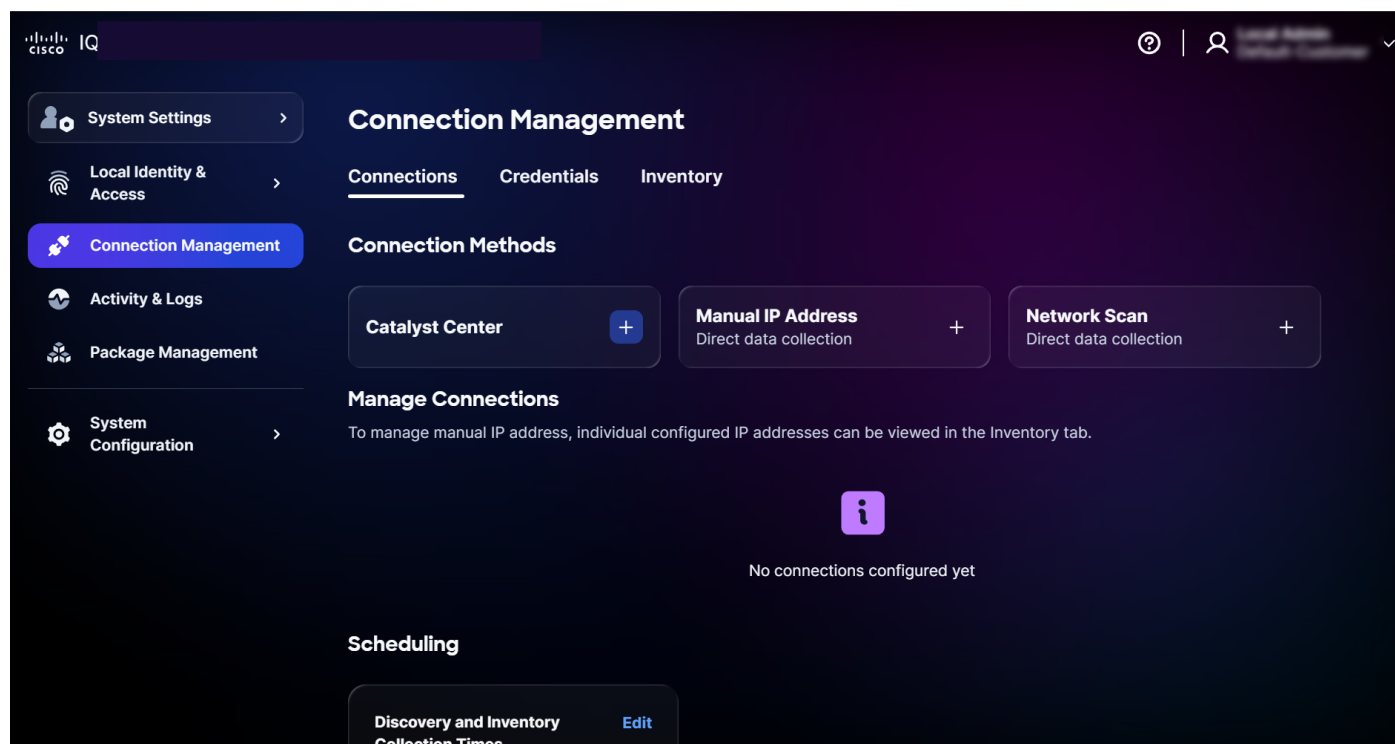
 附註：如果裝置屬於多個重疊類別，系統總是選擇具有最高特異性的憑證集（換句話說，尾隨萬用字元最少）。

使用Catalyst Center進行資料收集

每個Cisco IQ VA例項最多可連線20個Catalyst Center（非群集）。

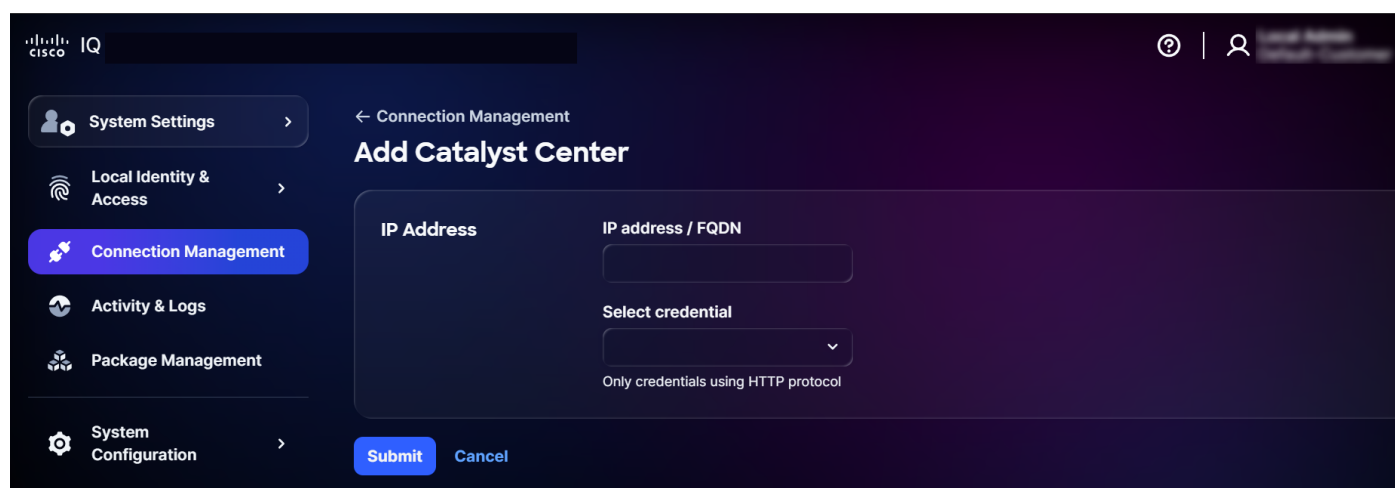
對於使用Catalyst Center進行資料收集：

1. 在System Settings中選擇Connection Management。系統隨即會顯示Connection Management頁面。



連線管理

2. 按一下Catalyst Center選項。



新增Catalyst Center

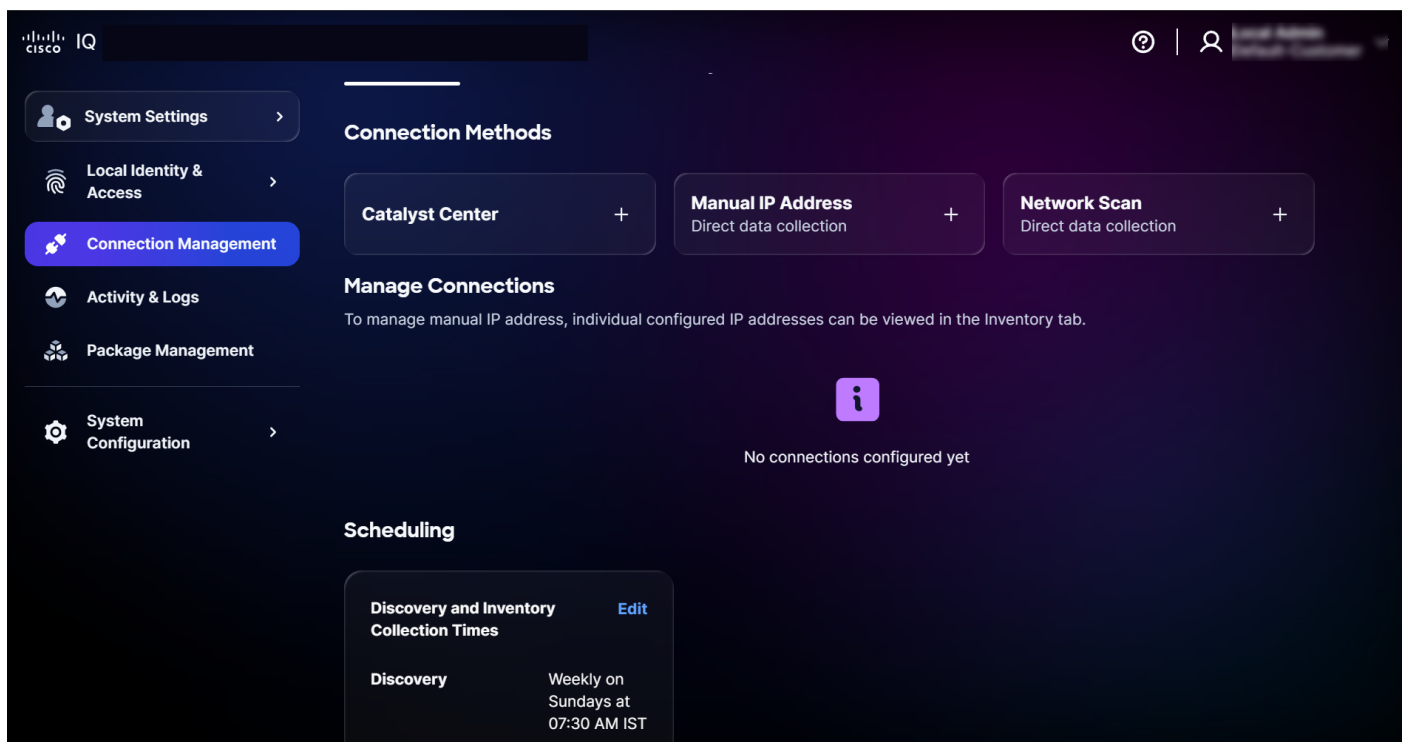
3. 輸入IP Address或FQDN。
4. 從Select credential下拉選單中選擇配置的HTTP/HTTPS憑據。
5. 按一下Submit (提交)。系統會顯示確認消息 (最多需要75分鐘)。您可以在Configured Connections下檢視新增的Catalyst Center。
6. 計畫收藏。有關詳細資訊，請參閱[計畫](#)。

 附註：思科IQ VA預配置了自動計畫設定，系統啟動預設自動收集計畫。強烈建議您編輯計畫以符合組織的要求和維護視窗。

手動資料收集

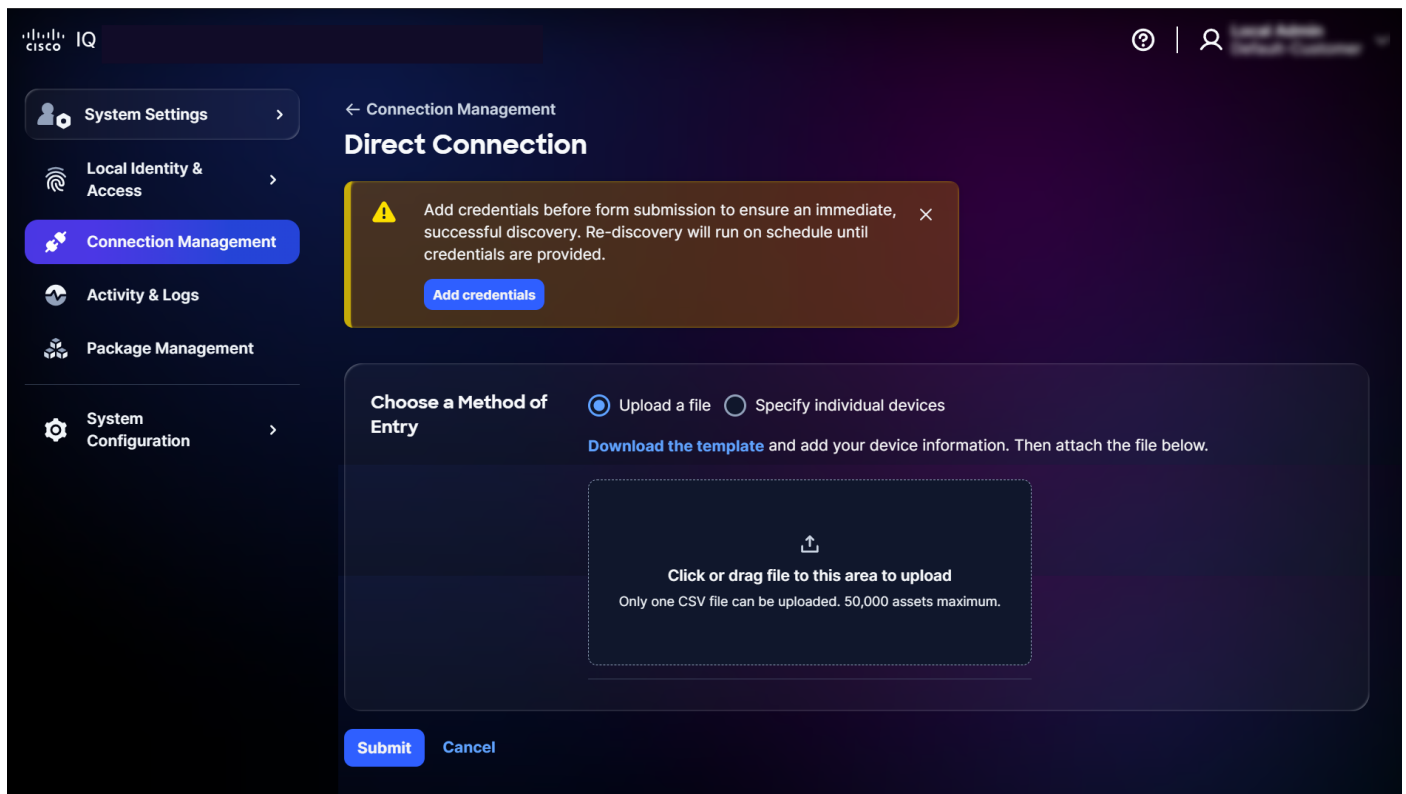
要新增直接資料連線的裝置，請執行以下操作：

1. 在System Settings中選擇Connection Management。系統隨即會顯示Connection Management頁面。



連線管理

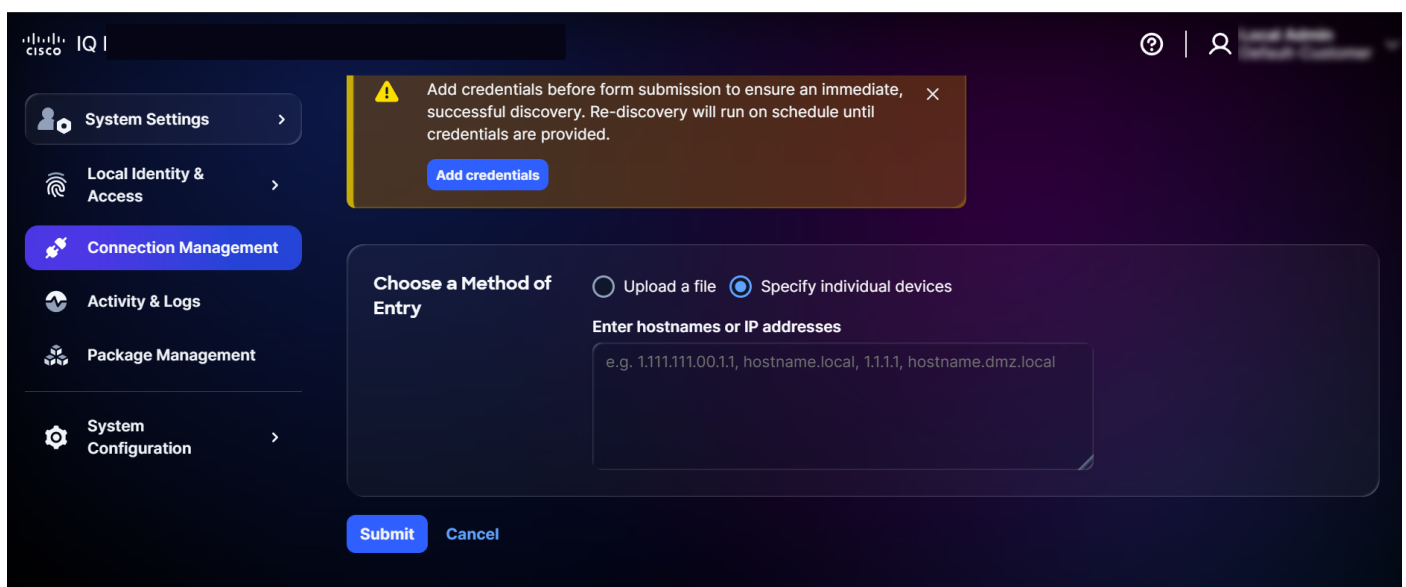
2. 按一下「Manual IP Address」。將顯示Direct Connection頁，其中包含兩(2)個用於收集資料的選項。



上傳檔案

3. 按一下Choose a Method of Entry中的首選選項，然後使用以下方法之一提供裝置資訊：

- 上傳檔案:按一下或拖放檔案



指定單個裝置

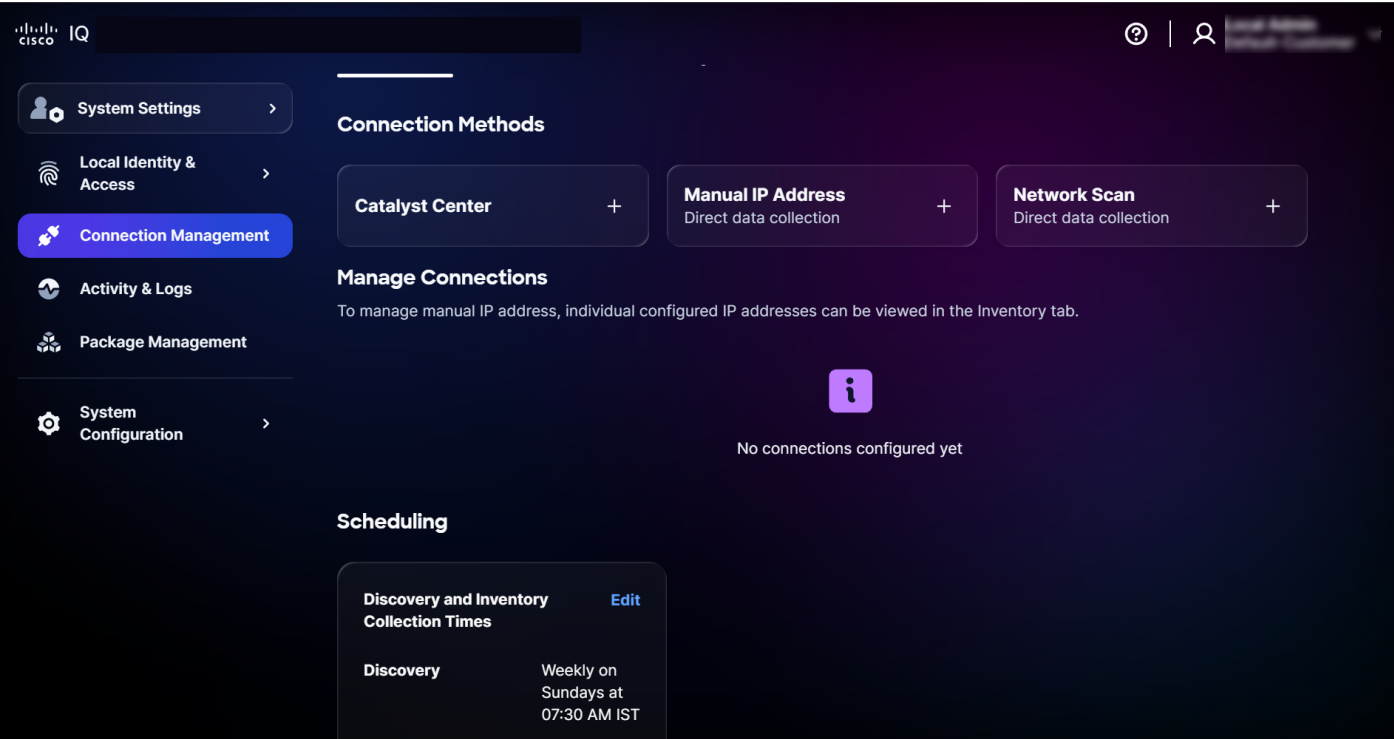
- 指定單個裝置:輸入單個主機名、IP地址或逗號分隔的主機名和/或IP地址清單

4. 按一下「Submit」。成功提交後，系統會將您重新導向到Assets索引標籤。
5. 計畫收藏。有關詳細資訊，請參閱[計畫](#)。

 附註：思科IQ VA預配置了自動計畫設定，系統啟動預設自動收集計畫。強烈建議您編輯計畫，使其符合組織的要求和維護視窗。

網路掃描

1. 在System Settings中選擇Connection Management。系統隨即會顯示Connection Management頁面。



網路掃描

2. 按一下「Network Scan (網路掃描)」。將顯示Connect Assets by Network Scan頁面，其中包含三(3)個選項。

The screenshot shows the Cisco IQ web interface. On the left is a navigation sidebar with options: System Settings, Local Identity & Access, Connection Management (highlighted), Activity & Logs, Package Management, and System Configuration. The main content area is titled 'Connection Management' and 'Connect Assets by Network Scan'. It contains a 'Scan Method' section with three radio buttons: 'Specify IP Range' (selected), 'Specify Discovery Protocol (CDP/LLDP)', and 'File Upload'. Below this is a 'Name' text field. Further down are 'IP Start' and 'IP End' text fields. A 'Schedule Scan' section follows, with a 'Frequency' dropdown menu and a 'Time' field showing 'hh:mm' and a clock icon, with 'IST' as the time zone. At the bottom are 'Connect assets' and 'Cancel' buttons.

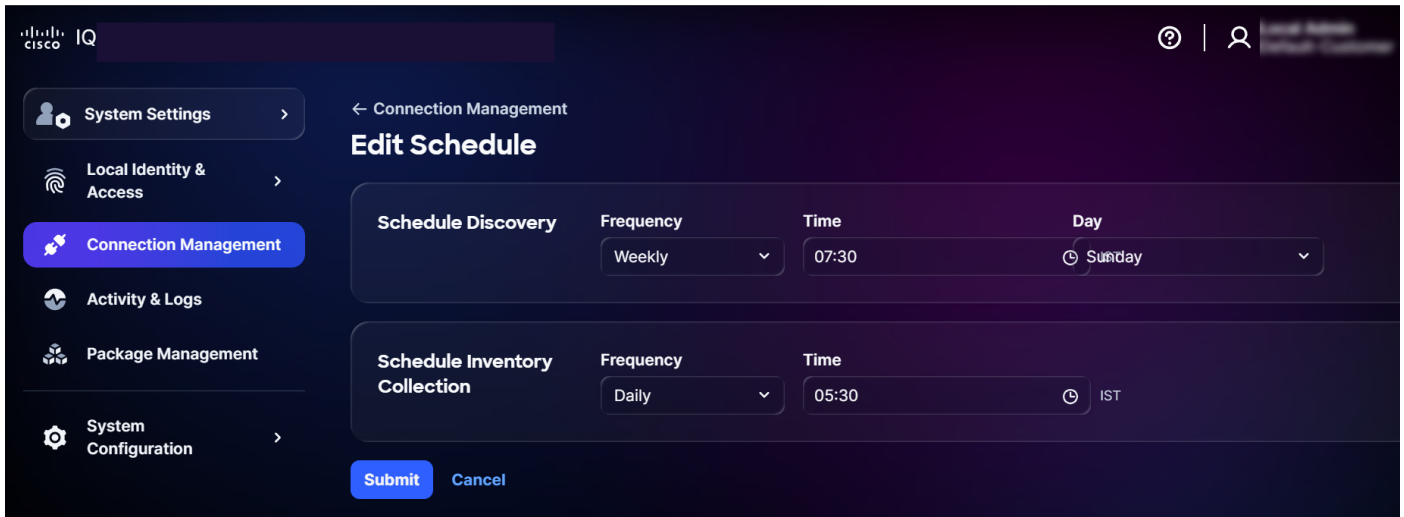
- 指定IP範圍:為網路發現或管理任務定義該範圍內的目標裝置的IP地址範圍
- 指定發現協定(CDP/LLDP):選擇要使用的網路發現協定
- 檔案上傳:上傳檔案，例如配置檔案或資料

3. 輸入Name。
4. 輸入IP Start和IP End。
5. 在Schedule Scan下，選擇Frequency and Time。
6. 按一下Connect assets。

日程安排

計畫允許您定義Cisco IQ VA何時執行自動資料收集。要計畫收集，請執行以下操作：

1. 在Connection Management頁面的Scheduling部分中，為要修改的計畫按一下Edit。系統隨即會顯示「編輯計畫」頁面。



編輯計畫

2. 在Schedule Discovery部分，從下拉選單中選擇首選Frequency和Day，然後輸入所需的開始時間。
3. 在Schedule Inventory Collection部分，從下拉選單中選擇您首選的Frequency，並輸入所需的開始時間。
4. 按一下「Submit」。

 附註：對發現或收集計畫所做的任何更改留出5到10分鐘的時間，以便在Virtual Appliance中同步和準確地反映這些更改。

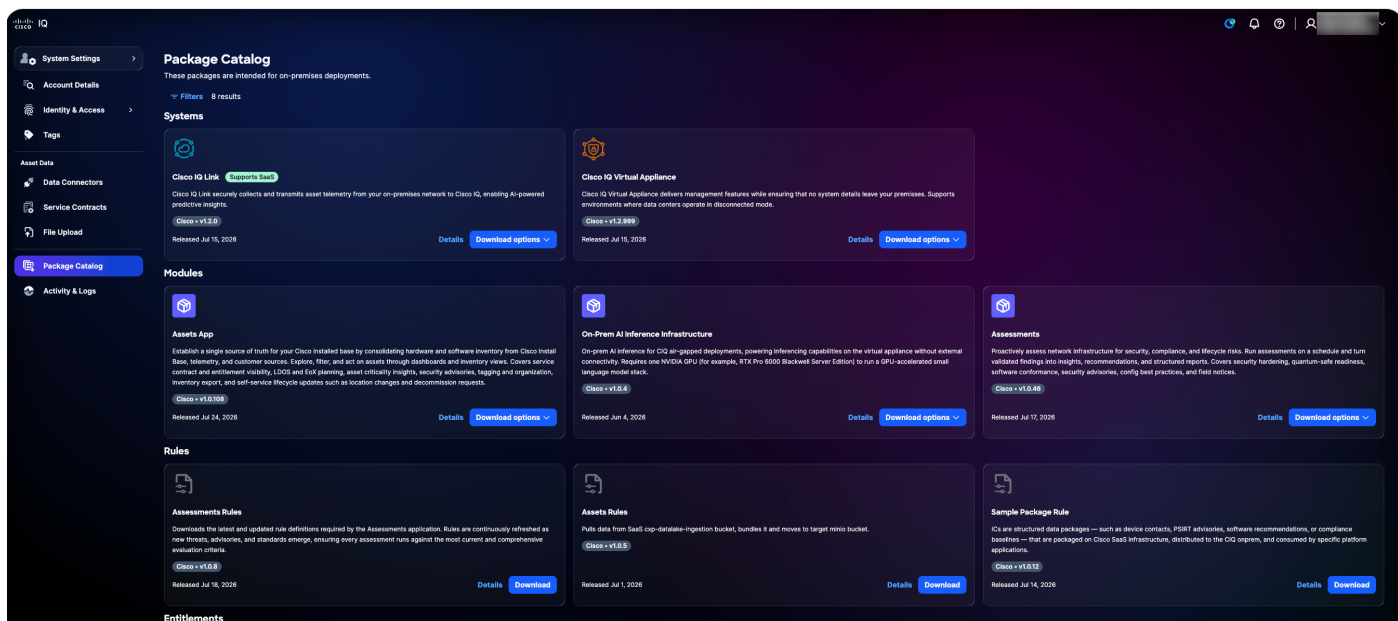
安裝包（模組、規則和授權）

您可以管理VA內運行模組、規則、權利和專用人工智慧驅動功能的軟體生命週期（即安裝和配置）。您可以通過導航至軟體包目錄，從Cisco IQ(SaaS)下載最新版本來安裝它們。包目錄顯示可供您使用的軟體例項。它使您能夠無縫地監控和管理更新，確保高效地跟蹤和管理您的系統例項。

新增模組

模組是獨立軟體包，在VA內提供核心功能。它是一種獨立的服務，具有自己的生命週期，允許進行安裝、維護和調整大小。資源消耗(包括CPU、圖形處理單元(GPU)和RAM)是根據初始安裝期間選擇的部署大小（小、中或大）動態分配的。

1. 登入到[Cisco IQ](#)。
2. 導航到系統設定 > 程式包目錄。

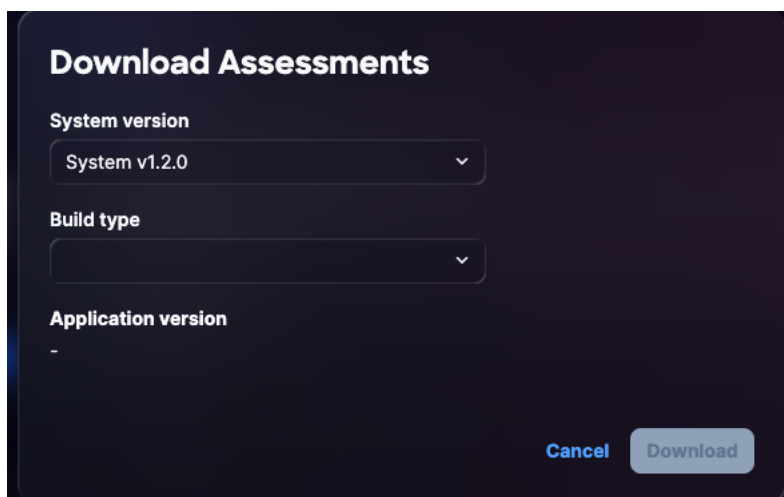


包目錄

3. 從所需的模組卡中，按一下Download options > Installation packages。Download視窗隨即開啟。



附註：「評估」模組用於示例影象。



下載

4. 從下拉選單中選擇System Version。
5. 從下拉選單中選擇Build type。
6. 按一下「Download」，將檔案儲存在本地。

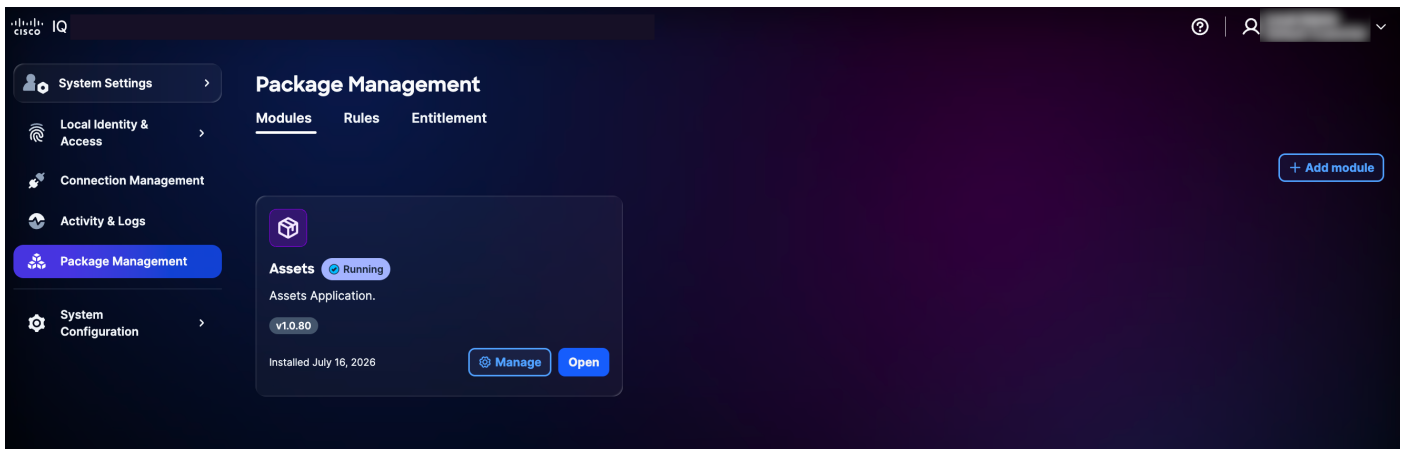


附註：安裝檔案較大(10-25 GB);下載前確保有足夠的磁碟空間。

7. 導航至VA。

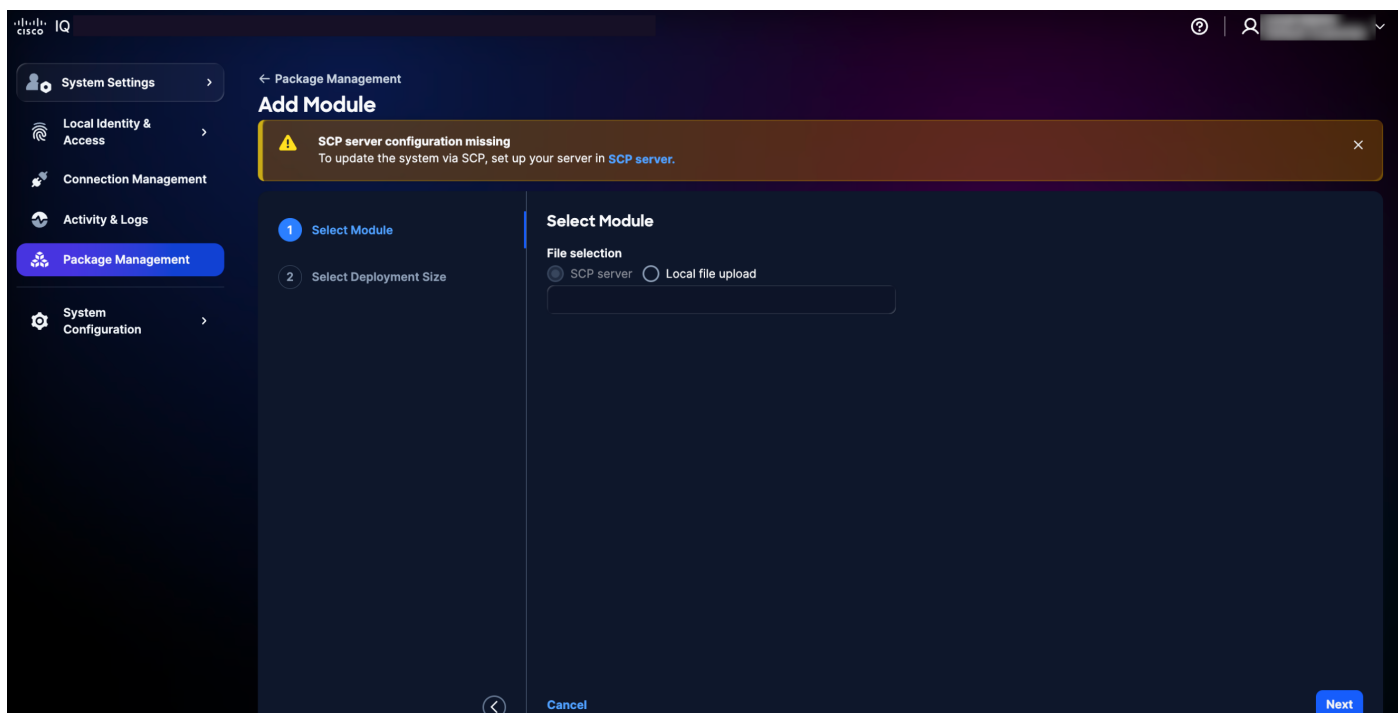
8. 導覽至Home > System Settings > Package Management。系統隨即會顯示「Package Management」頁面，其中包含以下頁籤：

- 模組
- 規則
- 權利



模組

9. 按一下Add module。

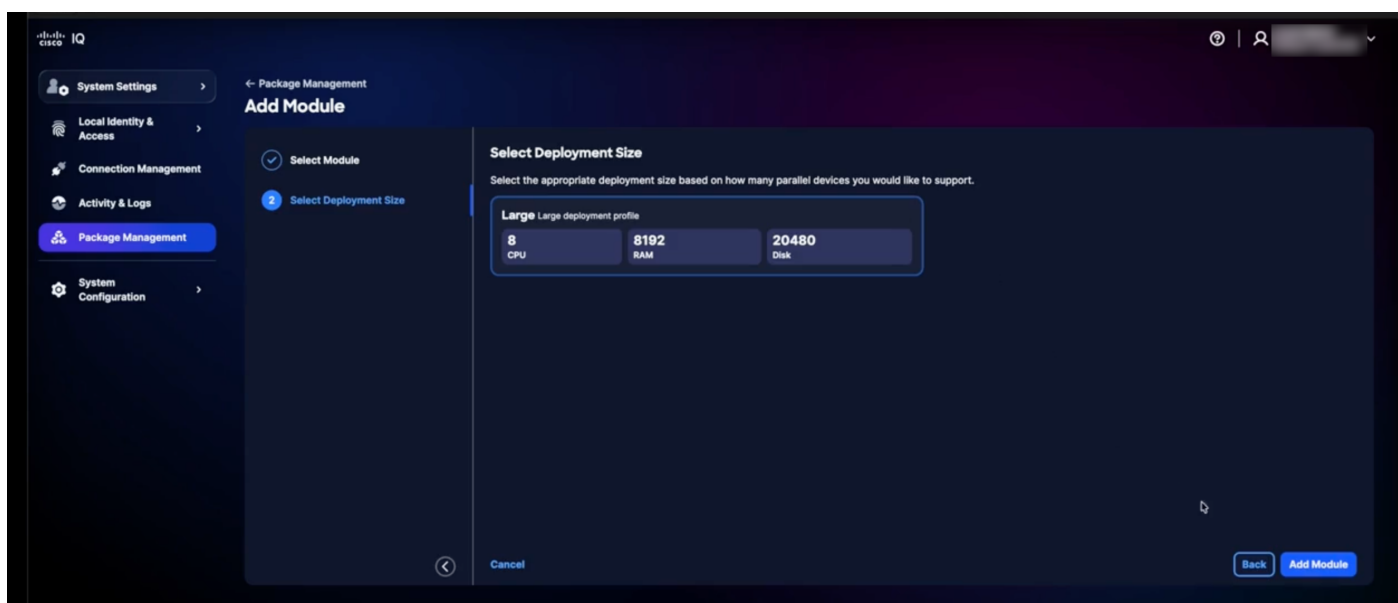


新增模組

10. 選擇首選的File selection選項：

- SCP伺服器:輸入安裝軟體包的確切檔名 (建議用於大檔案)
- 本地檔案上傳:拖放下載的安裝檔案 (由於上傳時間的原因，不建議對30 GB或更大的檔案使用)

11. 按「Next」(下一步)。

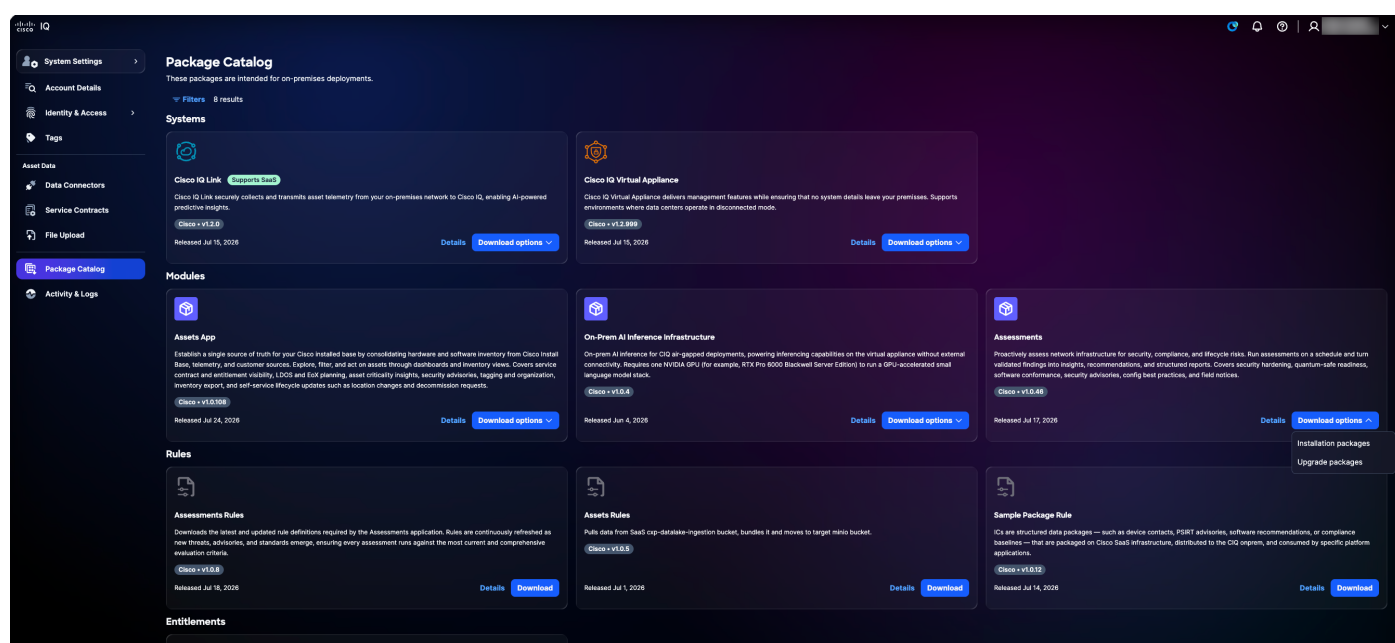


部署大小

- 選擇Deployment Size (例如 , Small、Medium或Large) 。 這些大小是預定義的並規定了資源需求。
- 按一下「Add Module」。新安裝的模組顯示在軟體包管理中的模組頁籤上。完成後，模組狀態更改為「Running」，Open按鈕變為可用。

升級模組

最新的模組在軟體包目錄 (Cisco IQ中) 中不斷更新。 要升級到最新版本：



通過網路掃描連線資產

- 從所需的模組卡中，按一下Download options > Upgrade packages。Download視窗隨即開啟。



附註：「評估」模組用作影象的示例。

Upgrade Assessments

System version

System v1.2.0



Current app version



Build type



Application version

-

Cancel

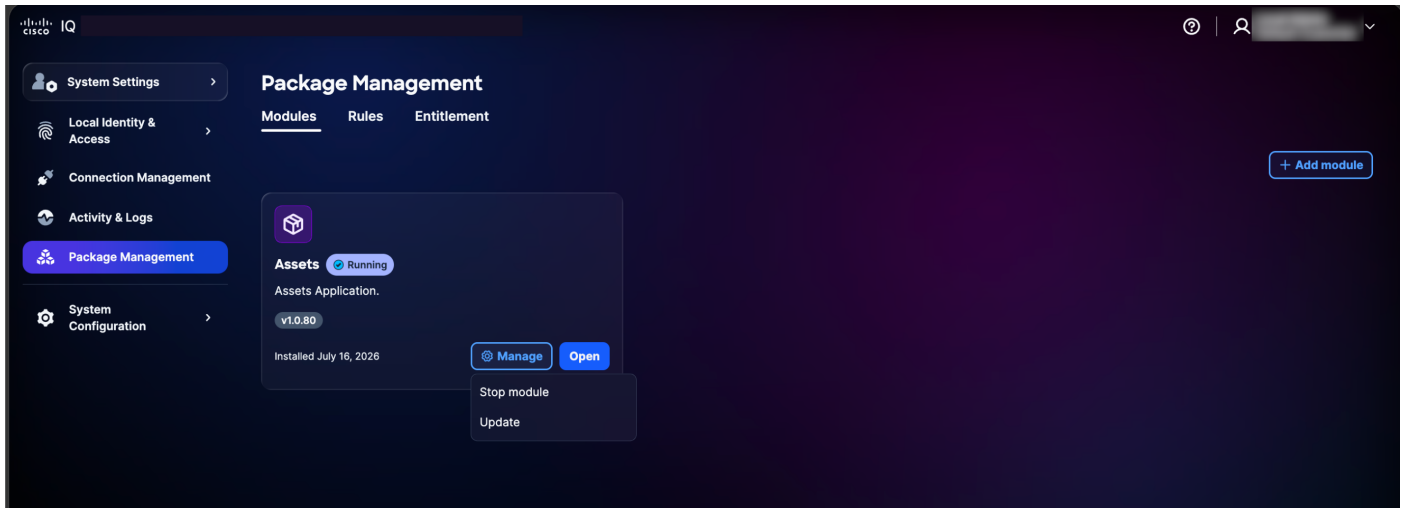
Download

下載

2. 從下拉選單中選擇System version。
3. 從下拉選單中選擇Current app version。
4. 從下拉選單中選擇Build type。
5. 按一下「Download」，將檔案儲存在本地。
6. 導航到VA並完成下載檔案的安裝。

管理模組

新增模組後，您可以通過按一下管理從包管理頁面對其進行修改。可用的修改選項包括調整大小和升級到更高版本。管理模組：



更新型別

1. 在Package Management頁面中，按一下所需模組的Manage > Update。
2. 選擇Update type:
 - 僅更改部署大小
 - 更新版本
3. 如果選擇了更改部署大小，請按一下下一步，然後在下一頁上選擇新的部署大小。

或

如果選擇Update Version，將顯示File selection選項。選擇SCP Server並輸入安裝軟體包的確切檔名，或選擇Local file upload，然後拖放下載的安裝檔案。

4. 按「Next」（下一步）。系統隨即會顯示「選擇更新計畫」頁。
5. 從以下單選按鈕選項中進行選擇，以更新計畫：
 - 立即更新
 - 稍後更新



附註：某些模組支援更新而不出現任何停機。如果需要停機，則標語會顯示詳細資訊。

6. 如果選擇Update later，請輸入Date和Time。
7. 按「Next」（下一步）。系統隨即會顯示更新摘要。

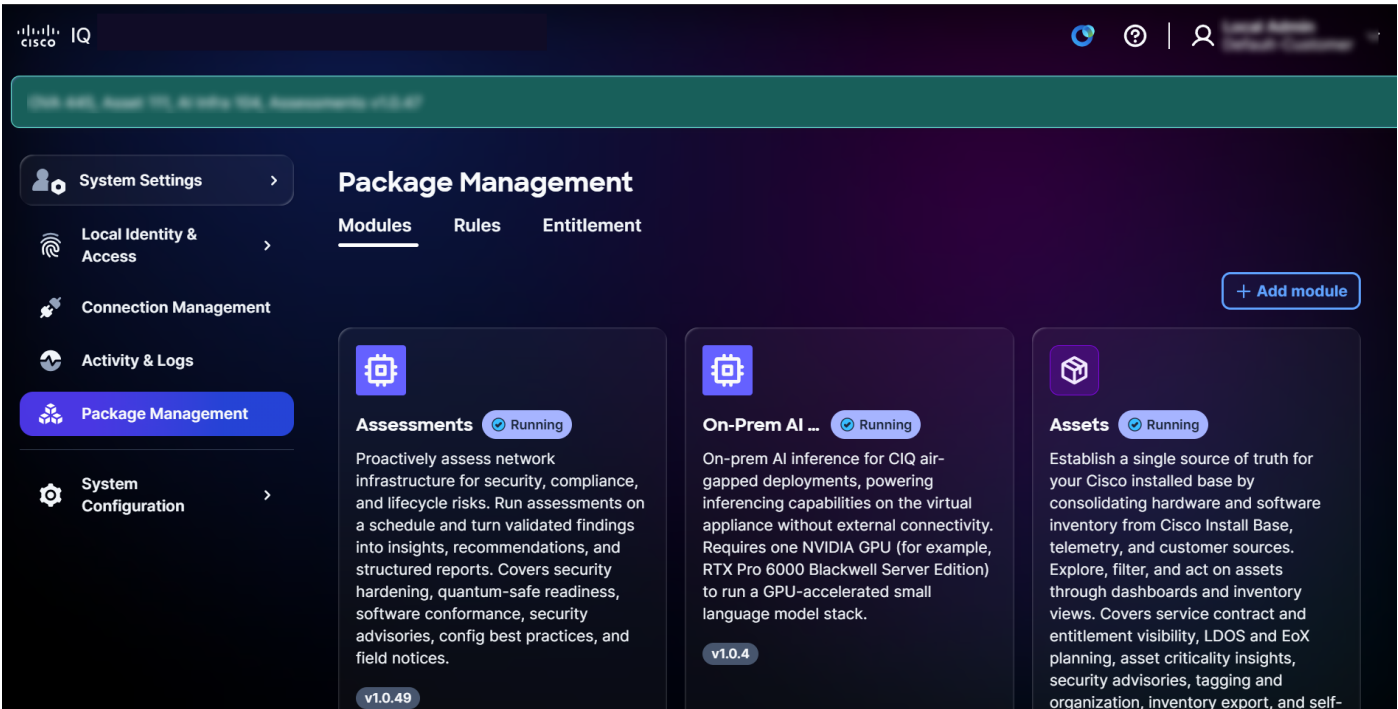


附註：您可以從更新摘要訪問發行說明。

8. 按一下Update Module，然後導航到Module頁籤。模組顯示「更新已計畫」狀態。

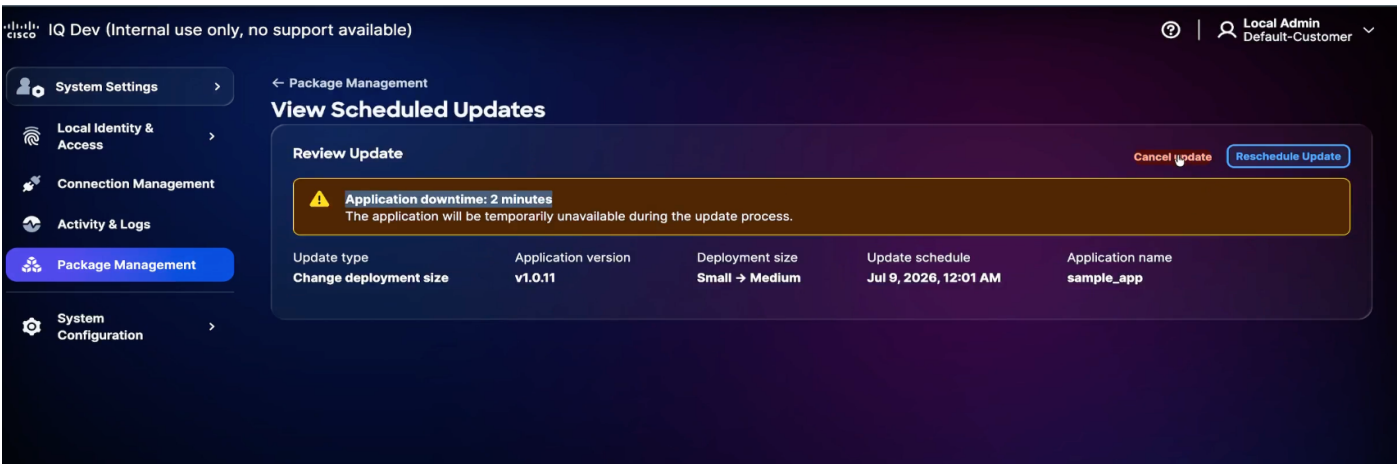
編輯計畫

您還可以檢視、編輯或取消計畫的更新。要編輯或取消計畫的更新，請執行以下操作：



編輯計畫

- 1. 在Package Management頁面中，按一下所需模組的Manage > View Scheduled update。將顯示檢視計畫更新視窗。



計畫更新

- 2. 根據需要按一下Cancel Update或Reschedule Update。

3. 按照螢幕上的說明完成操作。

 附註：如果模組操作（例如，安裝、升級或調整大小）失敗，請選擇以下選項之一：

重試:UI顯示「重試」按鈕，允許您再次嘗試該操作。 **日誌:**如果錯誤仍然存在，請按一下「日誌」檢視詳細的診斷資訊。這是確定安裝或運行時失敗原因的主要方法。

安裝規則

規則是擴展或修改現有模組功能的專用元件或「外掛」。規則不是作為獨立的程式運行的；它們「插入」模組以提供特定的規則、邏輯或功能。規則繫結到特定模組。安裝規則後，該規則會連結到其支援的模組。規則允許更新或自定義系統，而無需對核心模組進行完全升級。如果需要一組新的規則或功能，您只需向現有模組新增一個新規則即可。

要下載規則，請執行以下操作：

1. 登入到[Cisco IQ](#)。
2. 導航到System Settings > Package Catalog。
3. 從所需的規則卡中，按一下Download。

 附註：以下示例影像用於Assets規則。

Download Assets Rules

Target app version

assets v1.0.0



Cancel

Download

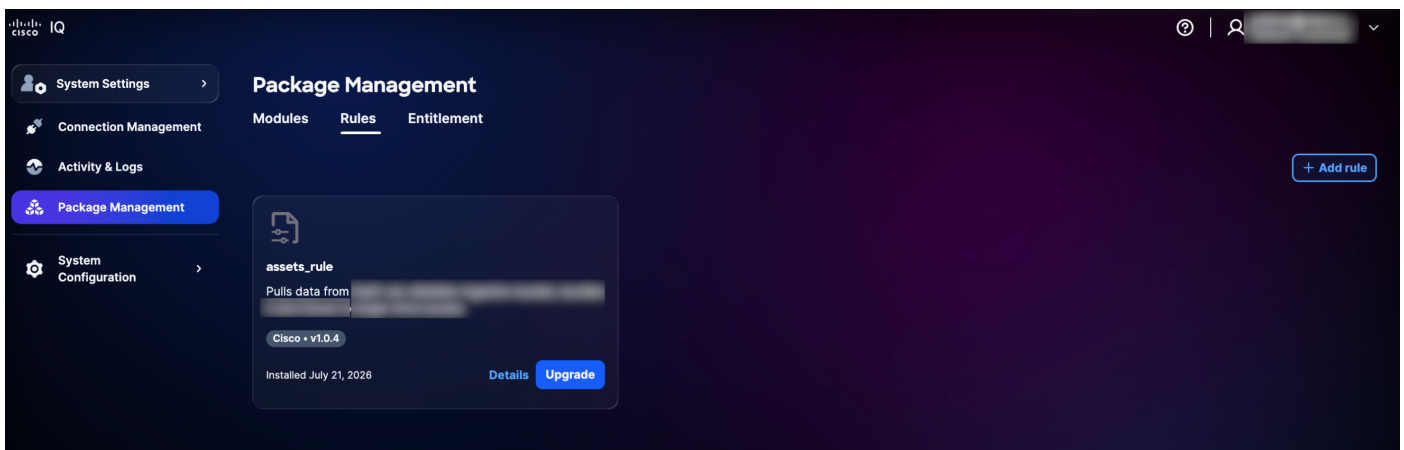
下載

4. 從下拉選單中選擇目標應用程式版本。
5. 按一下「Download」，將檔案儲存在本地。



附註：安裝檔案很大(10-25 GB);下載前確保有足夠的磁碟空間。

6. 導航至VA。
7. 導覽至Home > System Settings > Package Management。系統隨即會顯示「Package Management」頁面，其中包含以下頁籤。
 - 模組
 - 規則
 - 權利
8. 按一下Rules頁籤。



封包管理

9. 按一下Add rule。

Add rule



SCP server configuration missing



To update the system via SCP, set up your server in [SCP server](#).

File selection



SCP server



Local file upload

Cancel

Add

新增規則

10. 選擇首選的File selection選項：

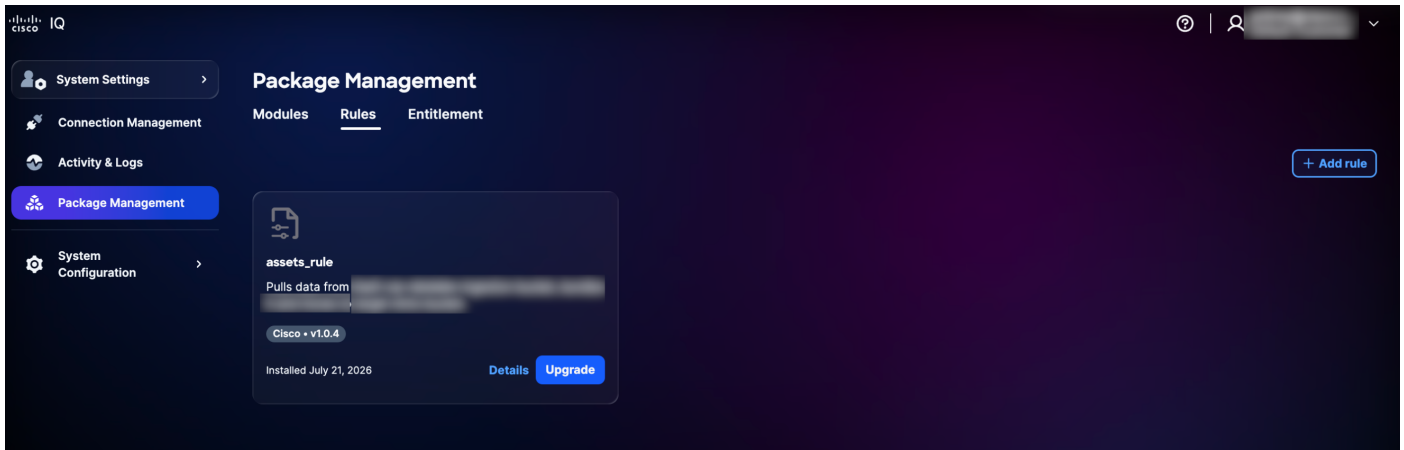
- 安全複製協定(SCP)伺服器:輸入安裝軟體包的確切檔名。對於大型檔案，建議使用此方法。
- 本地檔案上傳:拖放下載的安裝檔案。

11. 按一下「新增」。新增的規則顯示在包管理中。

升級規則

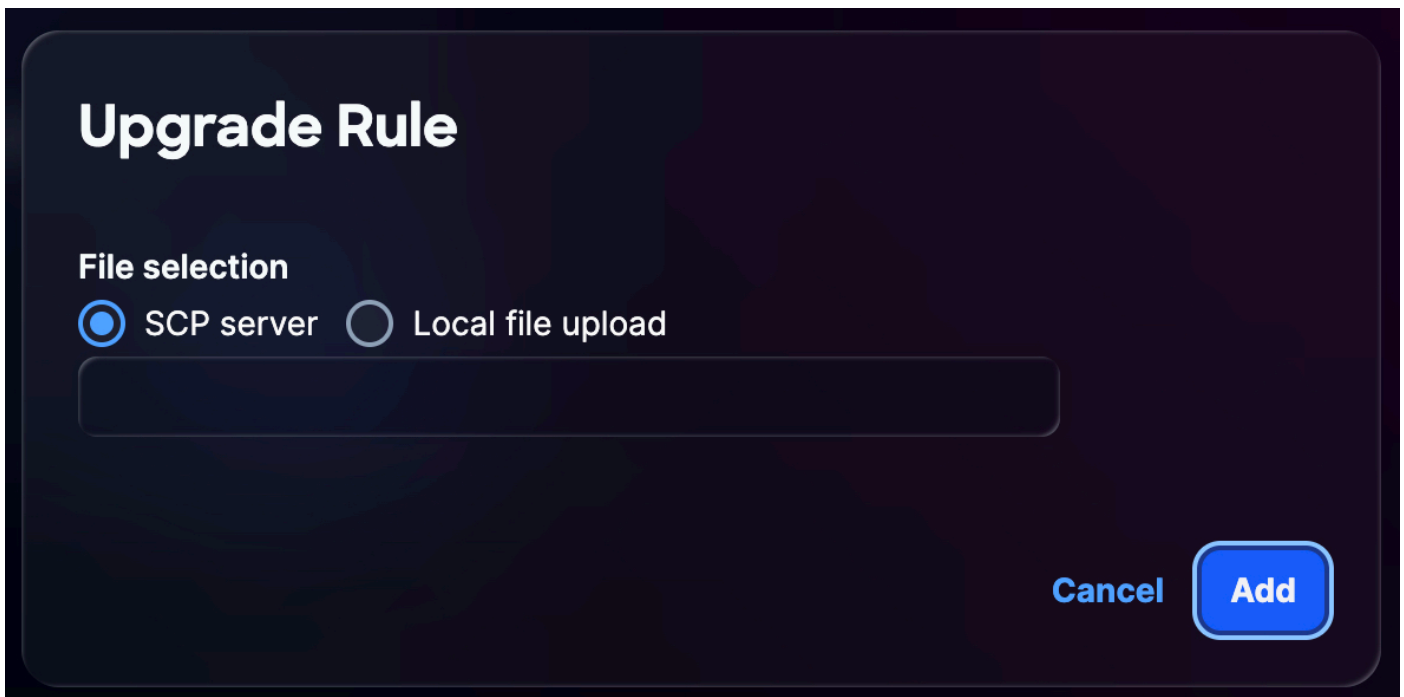
要升級規則，請執行以下操作：

1. 導航到VA中的System Settings > Package Management。



升級

2. 在所需的規則中，按一下Upgrade。Upgrade Rule視窗開啟。



升級規則

3. 選擇首選的File selection選項：

- 安全複製協定(SCP)伺服器:輸入安裝軟體包的確切檔名。對於大型檔案，建議使用此方法。
- 本地檔案上傳:拖放下載的安裝檔案。

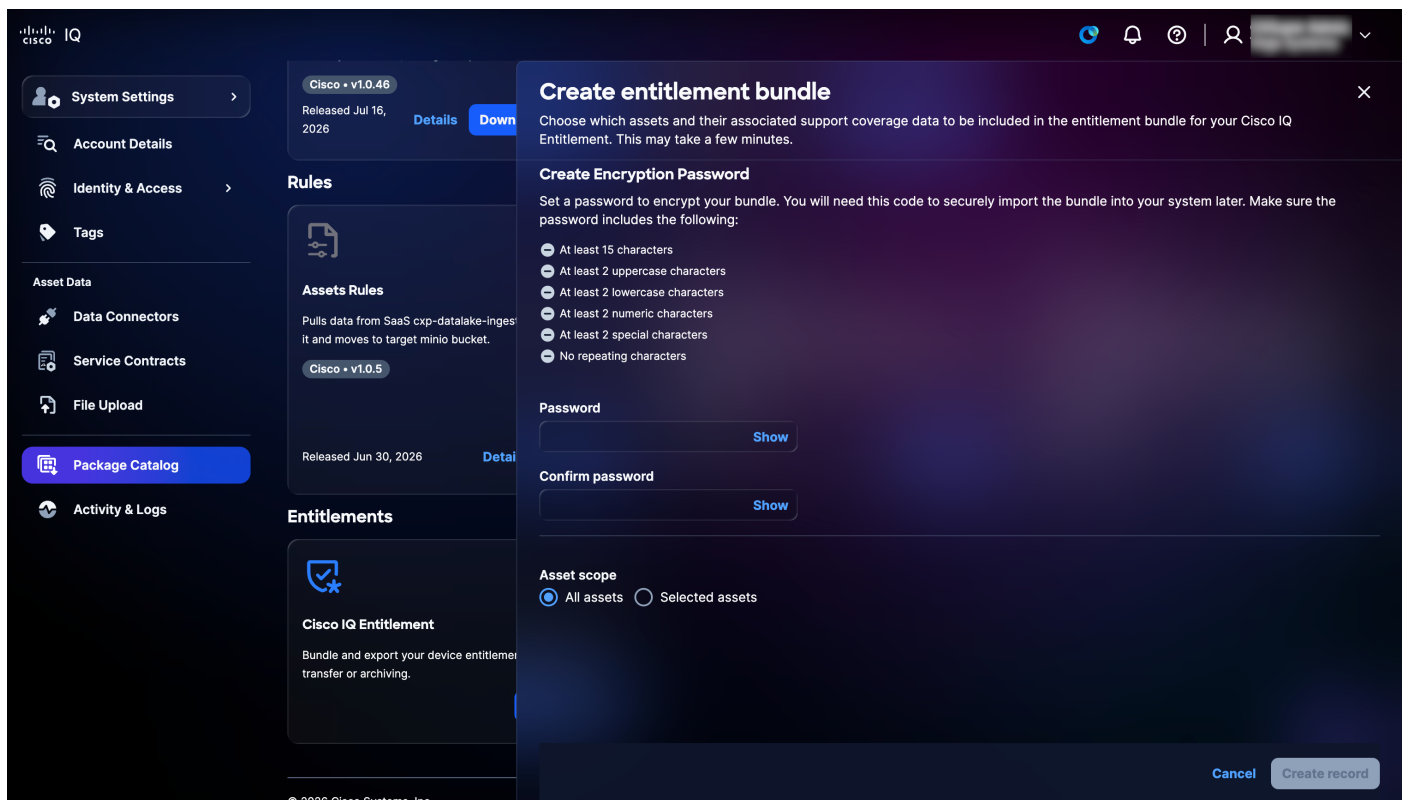
4. 按一下「新增」。

 附註：這些規則應用於週期性計畫裝置遙測收集。對於立即應用，您可以手動啟動裝置遙測收集。

安裝權利

權利檔案驗證貴組織使用特定軟體功能、模組或服務的權利。要安裝權利，請執行以下操作：

1. 登入到[Cisco IQ](#)。
2. 導覽至System Settings > Package Catalog。
3. 在權利卡中，按一下建立記錄。將開啟建立權利包視窗。



建立權利捆綁包

4. 輸入密碼。請參閱螢幕上顯示的密碼建立規則。
5. 在Confirm Password中再次輸入相同的密碼。
6. 選擇首選「資產範圍」單選按鈕。
 - 所有資產:包括連結至您的所有資產
 - 所選資產:允許您選擇與您的環境一致的特定裝置；如果選中此選項，則選中所有適用資

產的覈取方塊

7. 按一下Create record以本地儲存檔案。

 附註：建立權利套件組合後，請勿離開當前螢幕。如果您導航到另一個頁面，套件組合將失效，您必須重新產生套件組合才能啟用下載選項。

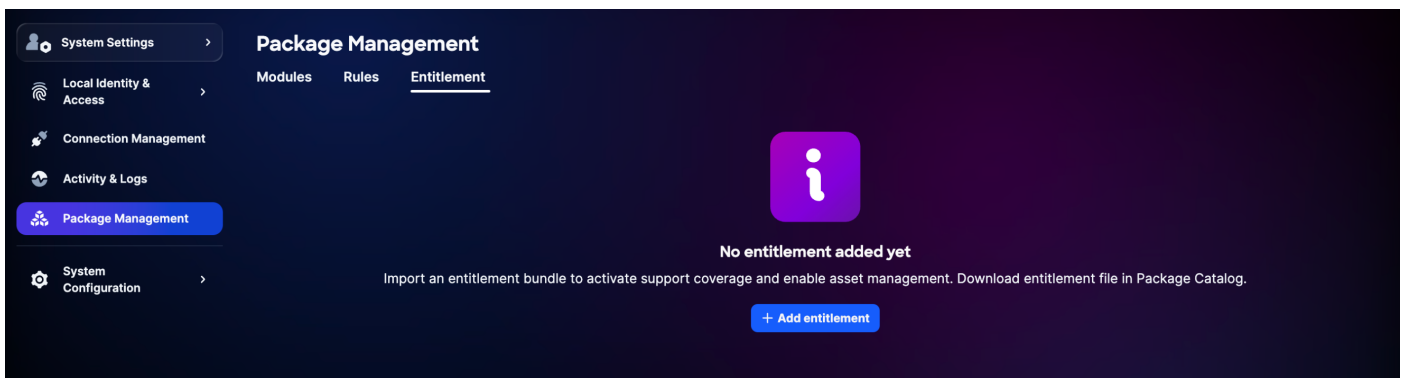
 附註：安裝檔案很大(10-25 GB);下載前確保有足夠的磁碟空間。

8. 登入到VA。

9. 導覽至Home > System Settings > Package Management。Package Management頁面包含以下頁籤：

- 模組
- 規則
- 權利

10. 按一下Entitlements頁籤。



Entitlement頁籤

11. 按一下Add Entitlement。

Add Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

[Show](#)[Cancel](#)[Add](#)

新增權利

12. 選擇首選的File selection選項。

- 安全複製協定(SCP)伺服器:輸入安裝軟體包的確切檔名；對於大型檔案，建議使用此方法
- 本地檔案上傳:拖放下載的安裝檔案

13. 輸入密碼。

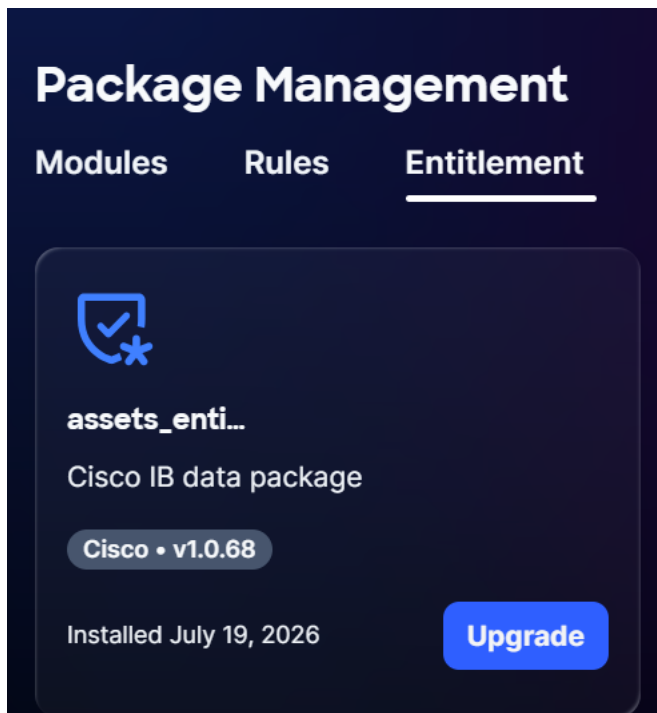
14. 按一下「新增」。新安裝的權利會顯示在軟體包管理的權利頁籤上。

15. 要啟用權利，請在新增權利之後等待5到10分鐘，然後啟動裝置遙測收集。

 附註：在權利流程中新增服務合約會將連結到該合約的所有裝置新增到本地裝置資產清單。您可以選擇按序列號篩選裝置、使用多個帳戶ID或選擇特定裝置來管理授權。

升級權利

要升級權利：



權利升級

1. 在所需的Entitlement中，按一下Upgrade。

Upgrade Entitlement

File selection

☒ SCP server ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

[Show](#)[Cancel](#)[Add](#)

升級權利

2. 選擇首選的File selection選項：

- 安全複製協定(SCP)伺服器:輸入安裝軟體包的確切檔名；對於大型檔案，建議使用此方法
- 本地檔案上傳:拖放下載的安裝檔案

3. 輸入密碼。

4. 按一下「新增」。

AI支援的功能

本地AI推理基礎設施模組在VA中啟用本地AI驅動功能。它在本地運行一個小型語言模型(SLM)，允許系統對AI驅動的提示做出響應。安裝之後，您就可以直接在VA介面中與其互動。

支援以下查詢型別：

- 資產:識別由於生命週期結束狀態、軟體貨幣或不合規、安全漏洞和合約覆蓋差距而處於風險中的資產
- 庫存:請求對庫存中的資產進行AI驅動分析

本地AI推理基礎設施安裝軟體包可從Cisco IQ軟體包目錄獲得，其分發方式與其他模組（如資產）相同。

 附註：每個GPU一次只能運行一(1)個本地AI推理基礎架構。完成安裝大約需要40-45分鐘。安裝檔案很大（大約30 GB）；下載前確保有足夠的磁碟空間。

本地AI推理基礎架構的前提條件

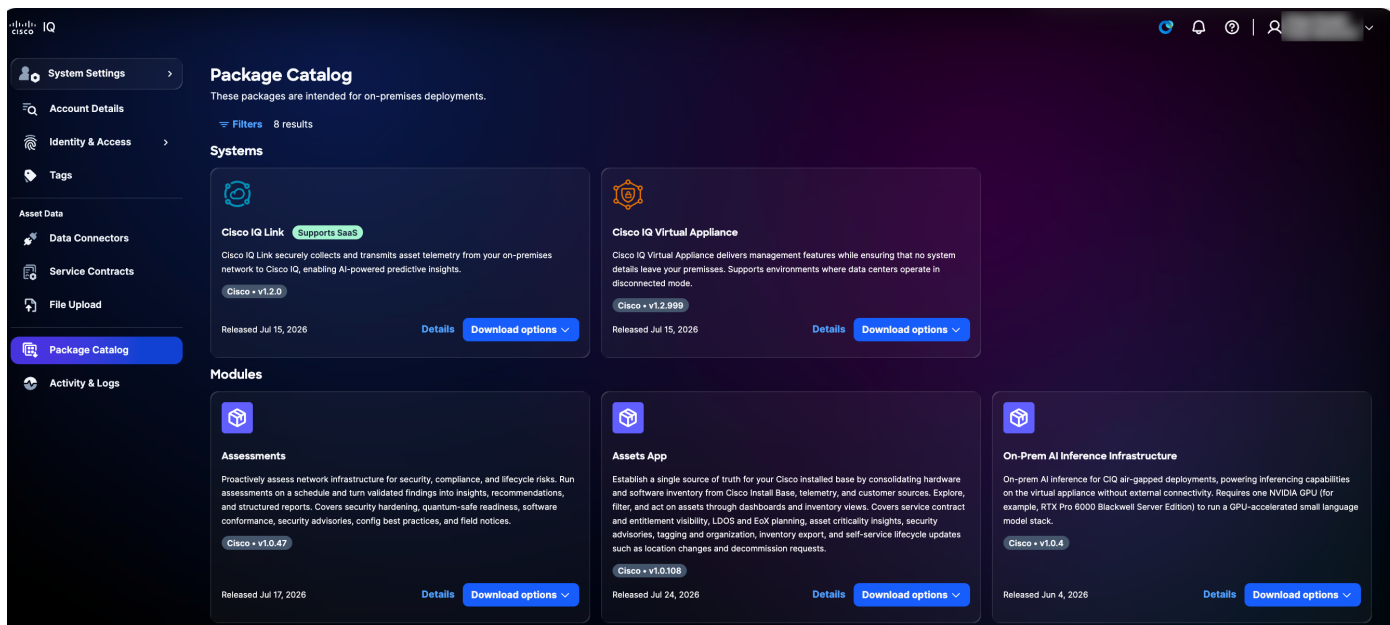
在安裝本地AI推理基礎結構之前，必須滿足以下條件：

- VA必須包括具有GPU訪問許可權的VM;slm需要一個GPU，如果沒有一個GPU，則無法運行
- GPU虛擬機器必須有80GB或更多的GPU VRAM可用

安裝本地AI推理基礎結構

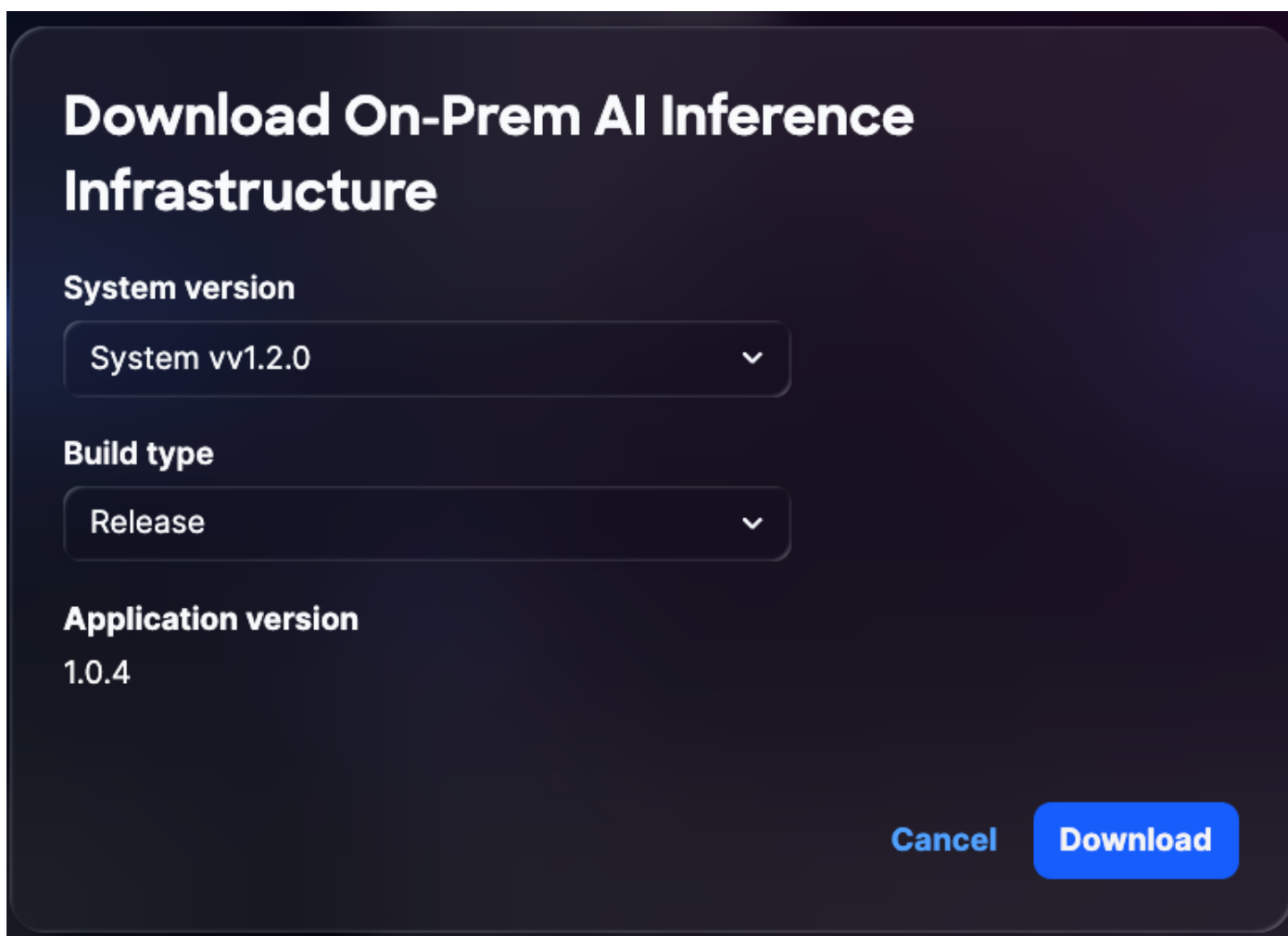
要在VA上安裝內部AI推理基礎設施，請從Cisco IQ SaaS下載內部AI推理基礎設施模組：

1. 登入到[Cisco IQ](#)。
2. 導覽至System Settings > Package Catalog。



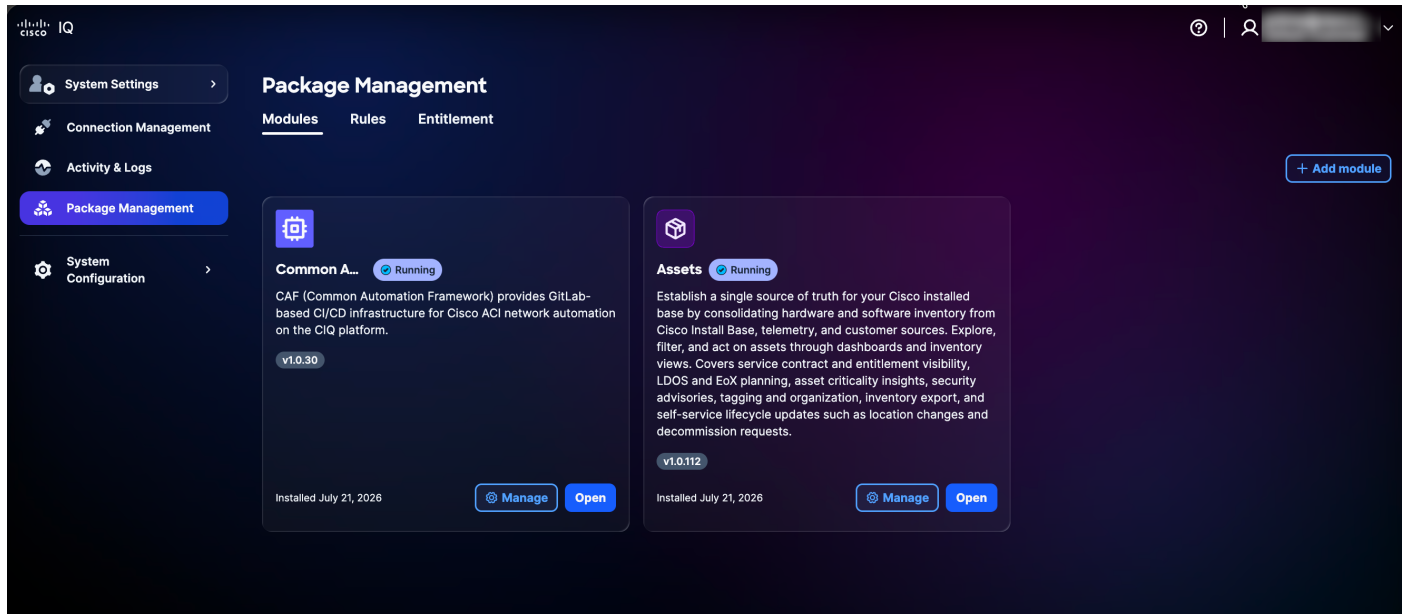
安裝程式包

- 從本地AI推理基礎結構卡中，按一下Download options > Installation packages。將開啟Download Application視窗。



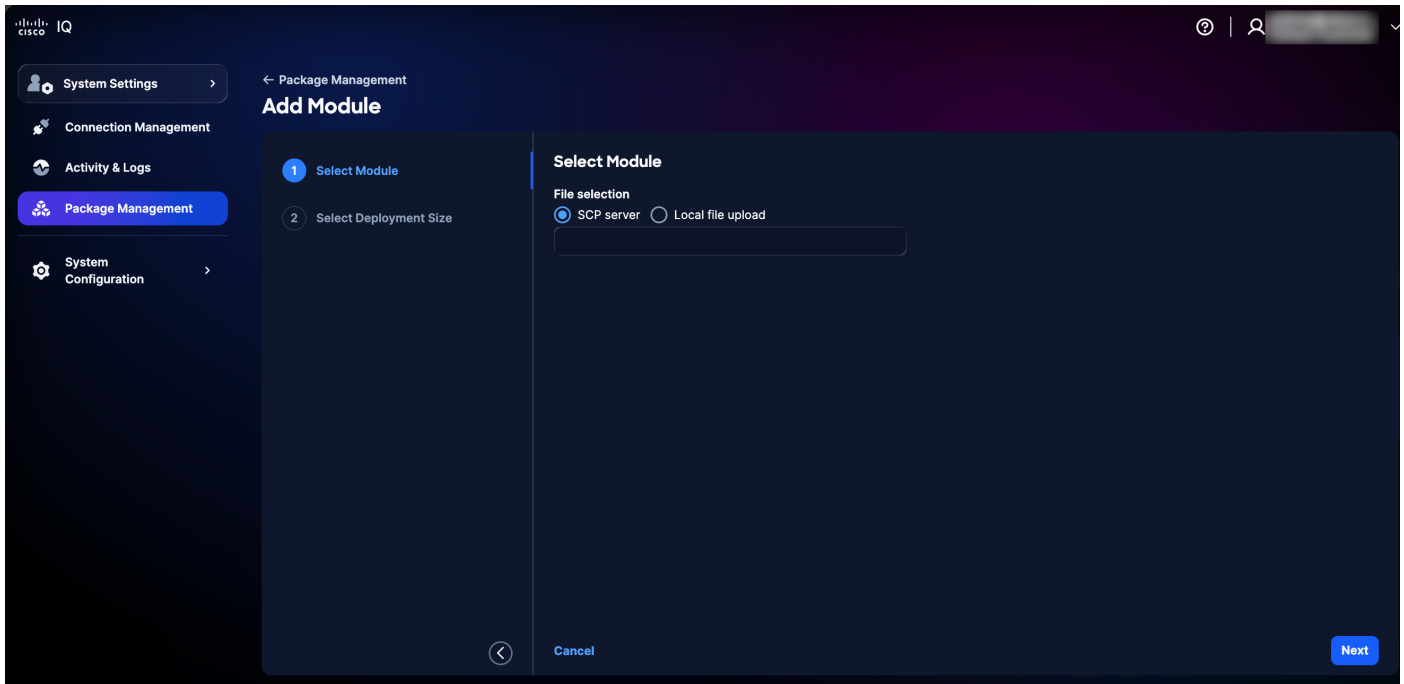
下載AI推理基礎架構

4. 從下拉選單中選擇System version。
5. 從下拉選單中選擇Build type。
6. 按一下「Download」。
7. 導航至VA。



封包管理

8. 導覽至Home > System Settings > Package Management。系統隨即會顯示「Package Management」頁面，其中包含以下頁籤：
 - 模組
 - 規則
 - 權利
9. 在「Modules」頁籤中，按一下Add modules。



選擇模組

10. 選擇首選的File selection選項：

- SCP伺服器:輸入安裝軟體包的確切檔名（建議用於大檔案）。
- 本地檔案上傳:拖放下載的安裝檔案（由於上傳時間的原因，不建議對30 GB或更大的檔案使用）。附註：本地檔案上傳方法具有20分鐘閾值。如果上傳過程超過此持續時間，安裝將失敗。使用SCP伺服器是確保成功而穩定的安裝的首選方法。

11. 按「Next」（下一步）。系統開始上傳檔案。

12. 選擇Deployment Size（例如Small、Medium或Large）。

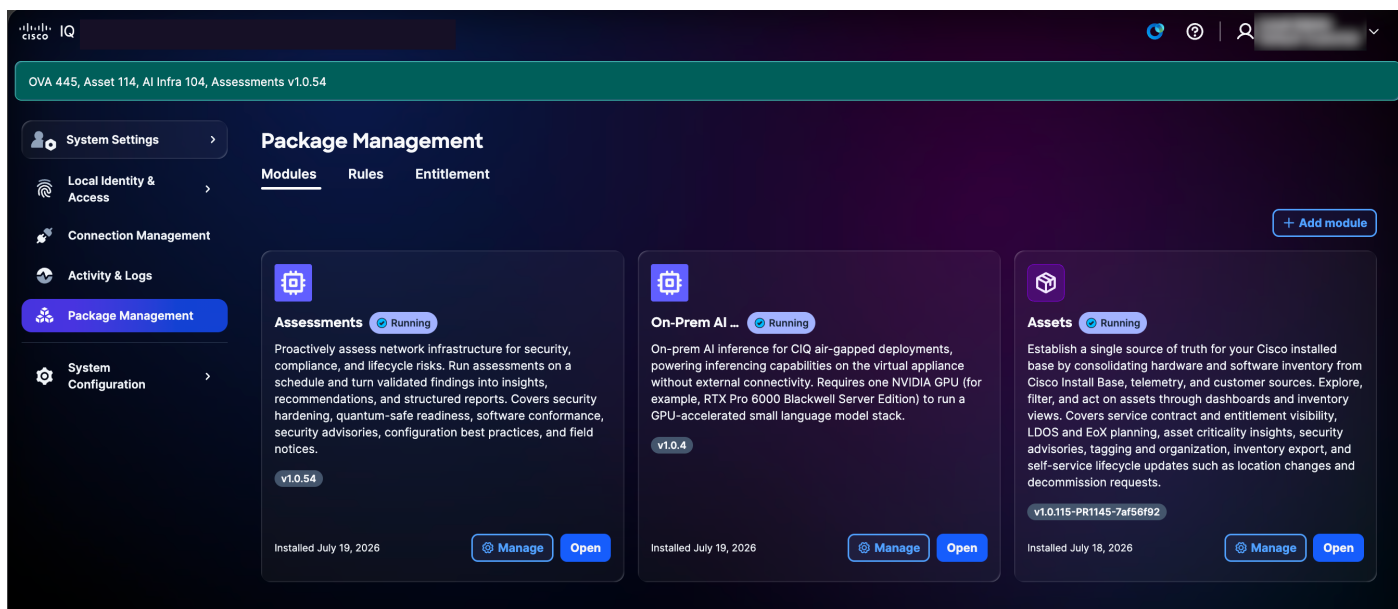
13. 按一下「Add Module」。安裝開始，大約需要40-45分鐘才能完成。

安裝完成後，本地AI推理基礎結構將顯示在軟體包管理的模組頁籤上。

 附註：每個GPU只能運行一個本地AI推理基礎設施模組。該模組使用約90%的GPU VRAM。不支援嘗試在同一GPU上安裝其他例項。

管理本地AI推理基礎結構模組

安裝後，可在Package Management的Applications頁籤中管理本地AI推理基礎結構模組。



編輯AI推理基礎結構

要管理該模組，請點選On-Prem AI Inference Infrastructure模組旁邊的Manage。如需詳細資訊，請參閱[管理模組](#)。

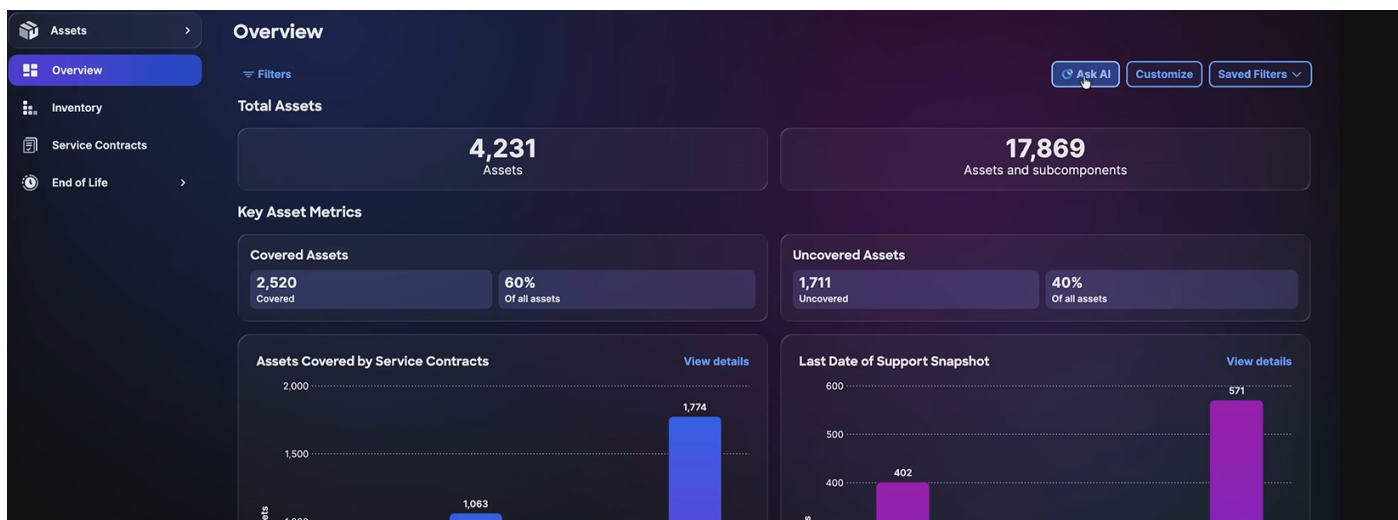
使用AI支援的功能

成功安裝本地AI推理基礎設施模組後，VA介面中會出現Ask AI按鈕。

詢問資產中的AI

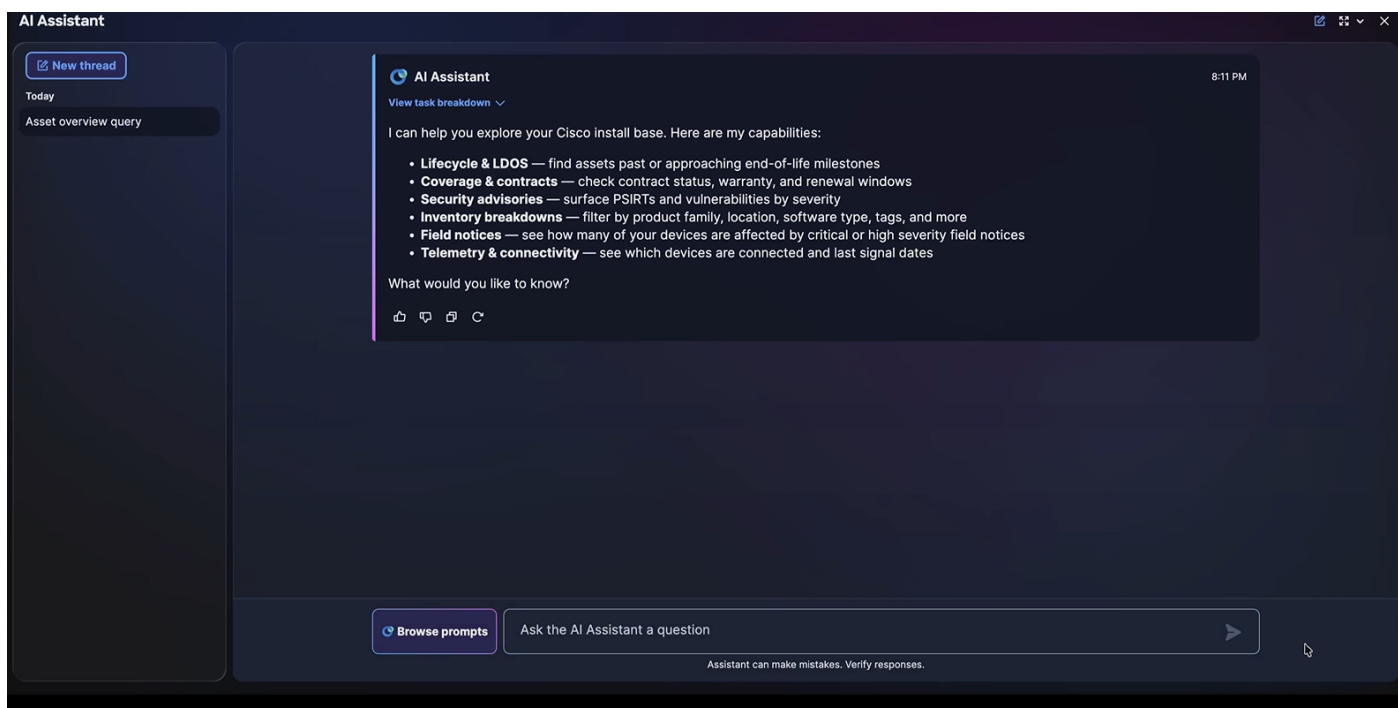
要在資產中使用Ask AI，請執行以下操作：

1. 選擇Home選單> Assets。系統隨即會顯示「Assets」頁面。



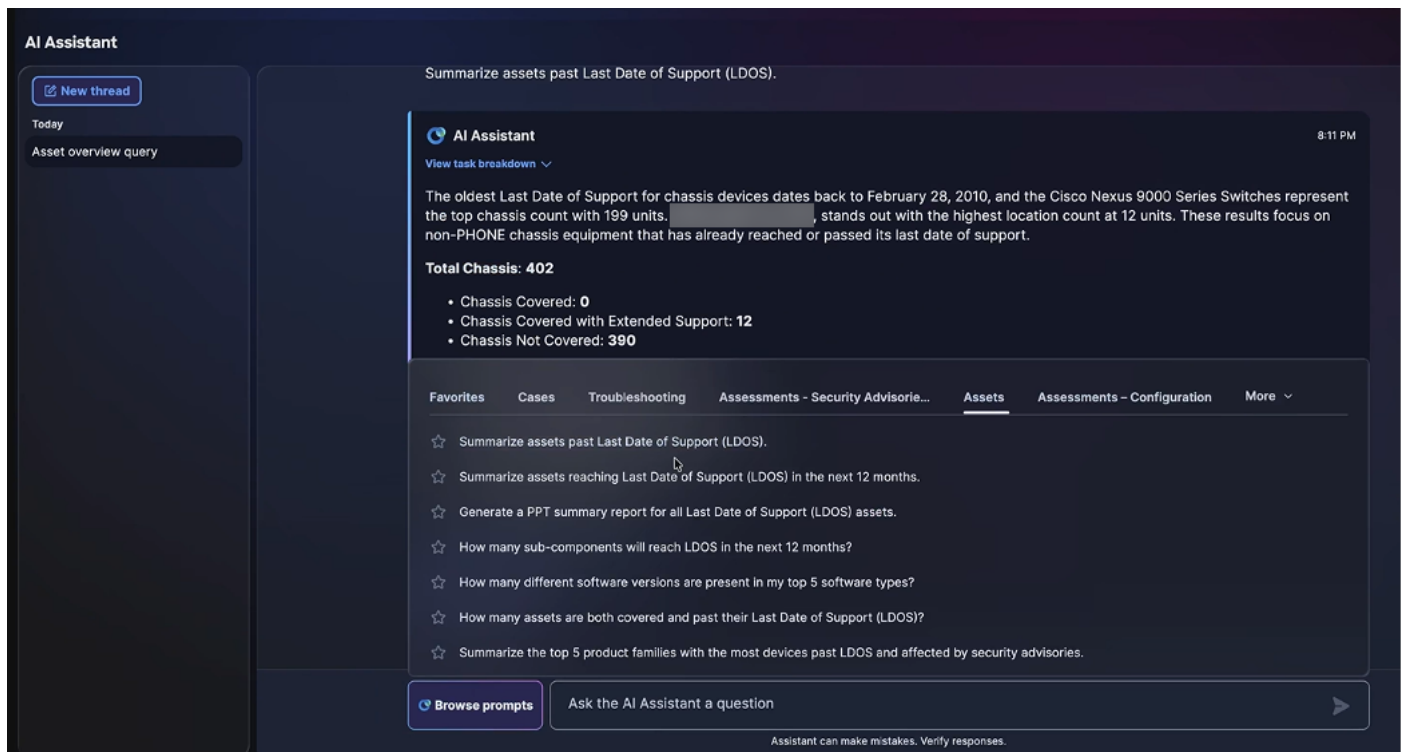
「資源」頁

2. 按一下Ask AI。內部的AI推理基礎設施啟動。



瀏覽提示

3. 按一下Browse prompts以檢視可用的提示，或在Ask the AI Assistant a question欄位中輸入自定義問題。



提示集

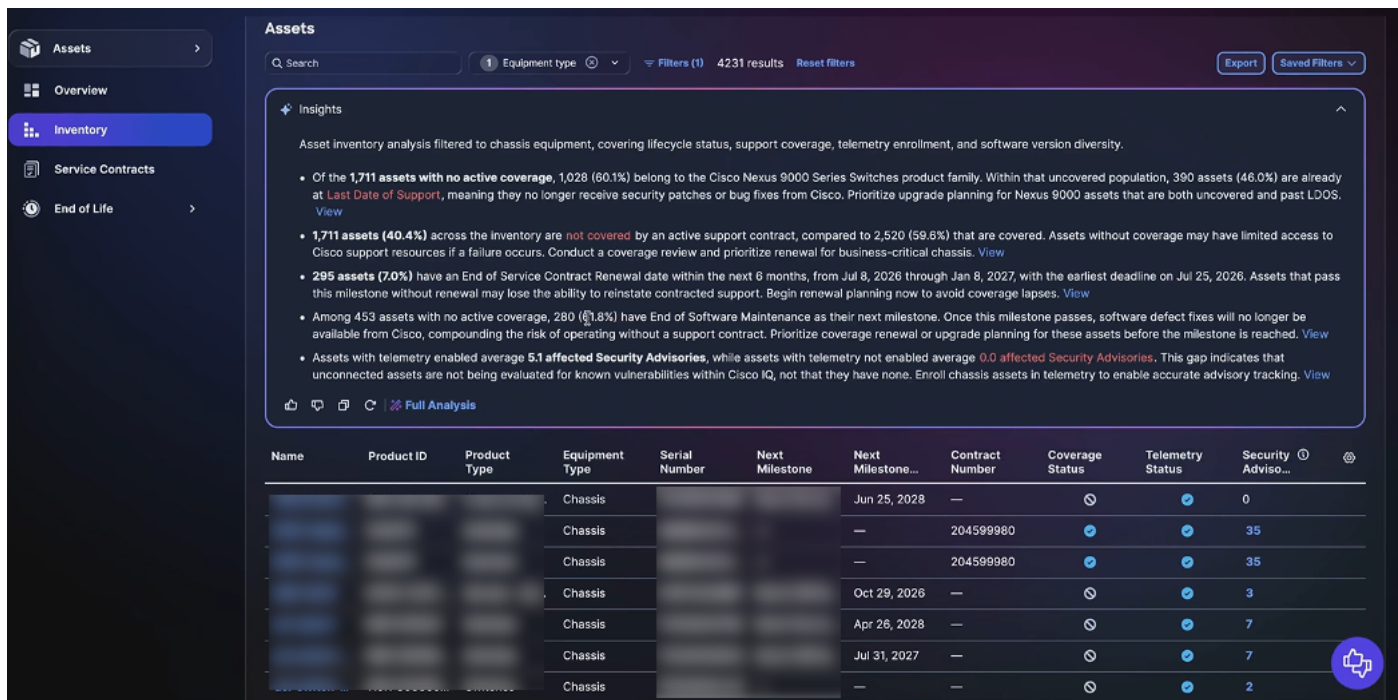
4. 按一下所需的提示或按Enter鍵。本地SLM生成響應。

庫存中的人工智慧分析

本地AI推理基礎架構模組在「清單」部分提供自動AI驅動分析。一旦填寫庫存資料，分析結果將自動顯示。

要在Oracle Inventory中檢視AI分析：

1. 選擇Home選單> Inventory。系統隨即會顯示Inventory頁面。



庫存

2. 檢視AI生成的分析。資料可用後，結果將顯示在庫存檢視中。

 附註：按一下Full Analysis可檢視圖形、儀表板和圖表等視覺化圖形，這些圖形可提供更多見解。

模組的常見功能

本節詳細介紹在所有模組間共用的核心功能。這些功能提供一致的使用者體驗、最佳化系統效能並簡化管理工作流程

分析資料

Insights面板提供該頁面上資料的AI驅動分析，提供切實可行的見解，以提高網路環境的安全性和健康狀況。

 附註：「分析」(Analysis)功能僅在選定頁面上可用。

Assets

Overview

Inventory

Service Contracts

End of Life

Inventory

Ask AI

Assets

Search

Product family

Product ID

Location

Tags

Filters (1)

1716 results

Reset filters

Export

Insights

- 69 assets that are **not covered** by any support contract have already reached **Last Date of Support**, leaving them without security patches or bug fixes. Prioritize upgrades or replacements for these assets to mitigate operational risks. [View](#)
- 175 Cisco Catalyst 9300 Series Switches (49.7% of **not covered** assets) lack active support contracts, which may limit access to Cisco support resources. Align renewal planning with the channel partner for these business-critical switches. [View](#)
- 73 assets with **telemetry not enabled** are at **End of Software Maintenance**, reducing visibility within Cisco IQ for proactive alerts and lifecycle planning. Enable telemetry for these assets to restore full monitoring capabilities. [View](#)
- 75 assets (4.4%) have **coverage expiring** between **Apr 24, 2026** and **Oct 24, 2026**, with the earliest deadline on **Apr 30, 2026**. Review these contracts to avoid lapses in vendor support and potential cost increases. [View](#)
- 75 assets (4.4%) have **End of Service Contract Renewal** dates between **May 1, 2026** and **Oct 24, 2026**, starting with a deadline on **May 1, 2026**. Coordinate with the selling partner to renew these contracts before expiry. [View](#)

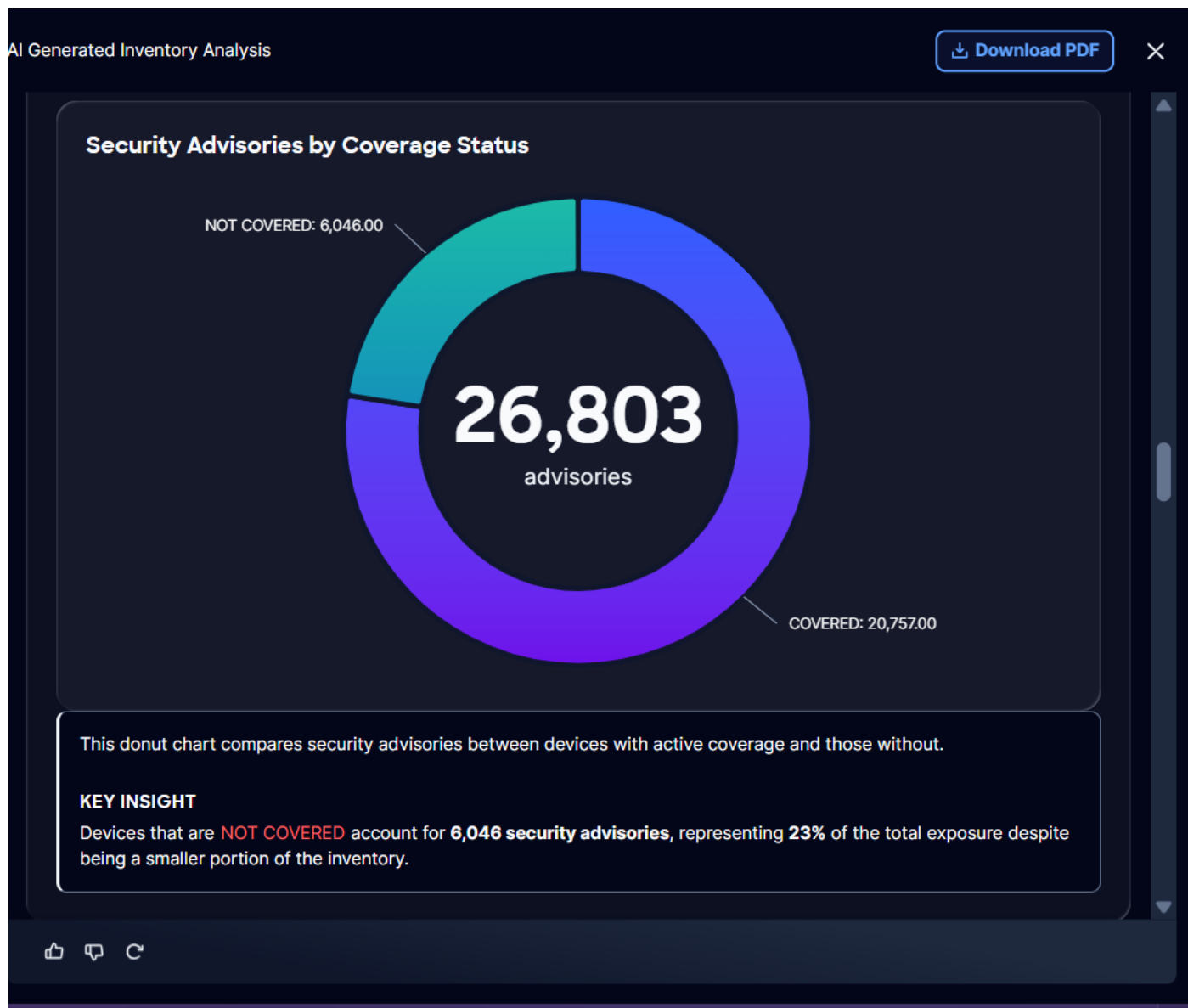
Full Analysis

☐	Name	Product ID	Product Type	Serial Number	Next Milestone	Next Milesto...	Contract Number	Coverage Status	Telemetry Status	Security...	
☐			Cloud and ...		End of Ser...	Jun 25, 2028	—	🔒	🟢	0	
☐			Switches		End of Ser...	Jan 29, 2027	—	🔒	🟢	4	
☐			Switches		—	—		🟢	🟢	23	
☐			Switches		—	—		🟢	🟢	23	
☐			Switches		—	—		🟢	🟢	23	

深入分析面板

「見解」面板中提供了以下選項：

- 按一下Expand圖示可展開面板並顯示其他見解
- 按一下Thumbs Up或Thumbs Down圖示提供有關AI生成的資訊的反饋
- 按一下Full Analysis以顯示附加資訊、更深入的分析以及圖形、儀表板和圖表等視覺化效果



全面分析

完全分析中提供了以下選項：

- 按一下下載PDF，為您的記錄或合作儲存分析的離線副本

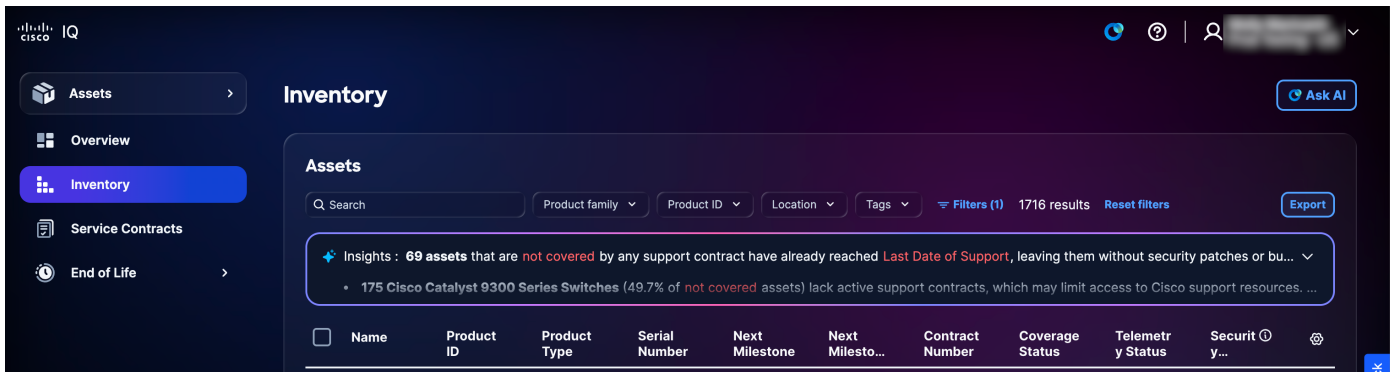
匯出資訊

匯出功能允許您以.xls或.csv格式匯出資產和安全資訊的自定義檢視。

 附註：匯出功能僅適用於選定頁面。

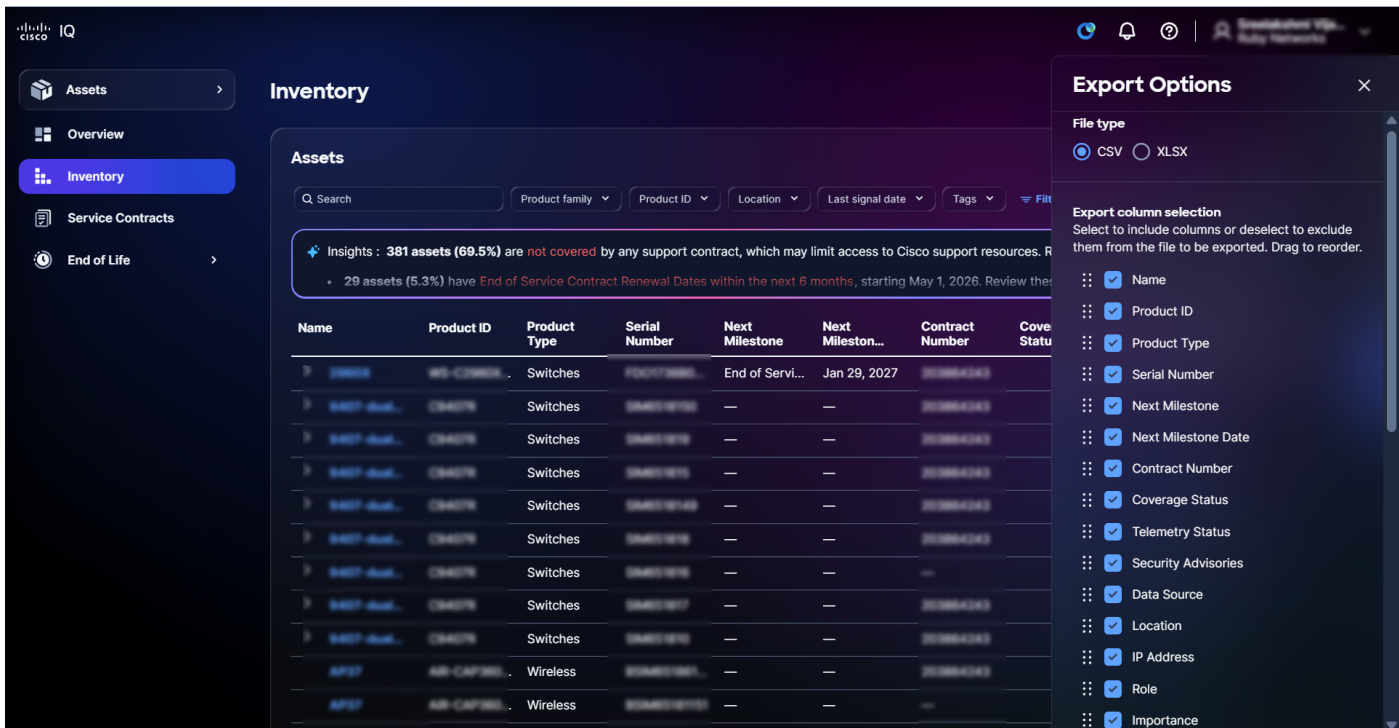
從頁面匯出資訊：

1. 導航到該頁面。



在資產模組中匯出庫存

2. 按一下「Export」。系統隨即會顯示「匯出選項」。



匯出選項

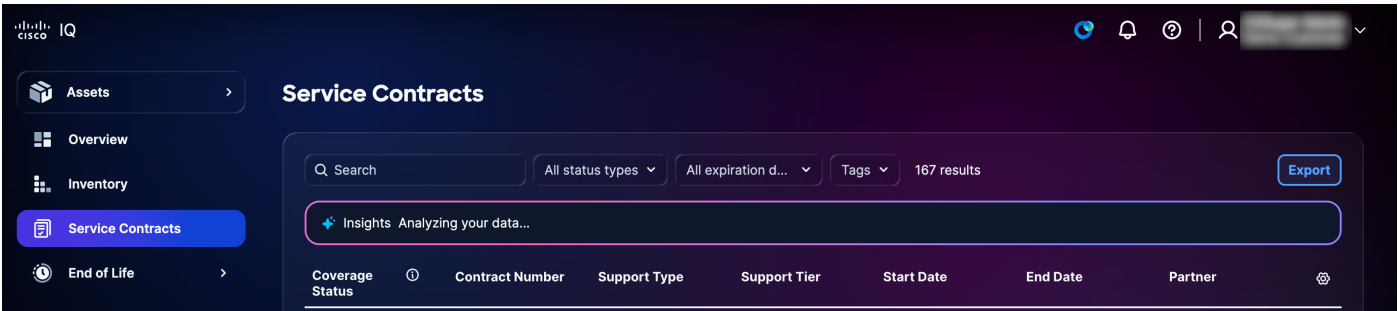
3. 選擇文件型別。

4. 選中所需列中的覈取方塊。

5. 按一下「Export」。檔案下載到瀏覽器的本地下載資料夾。

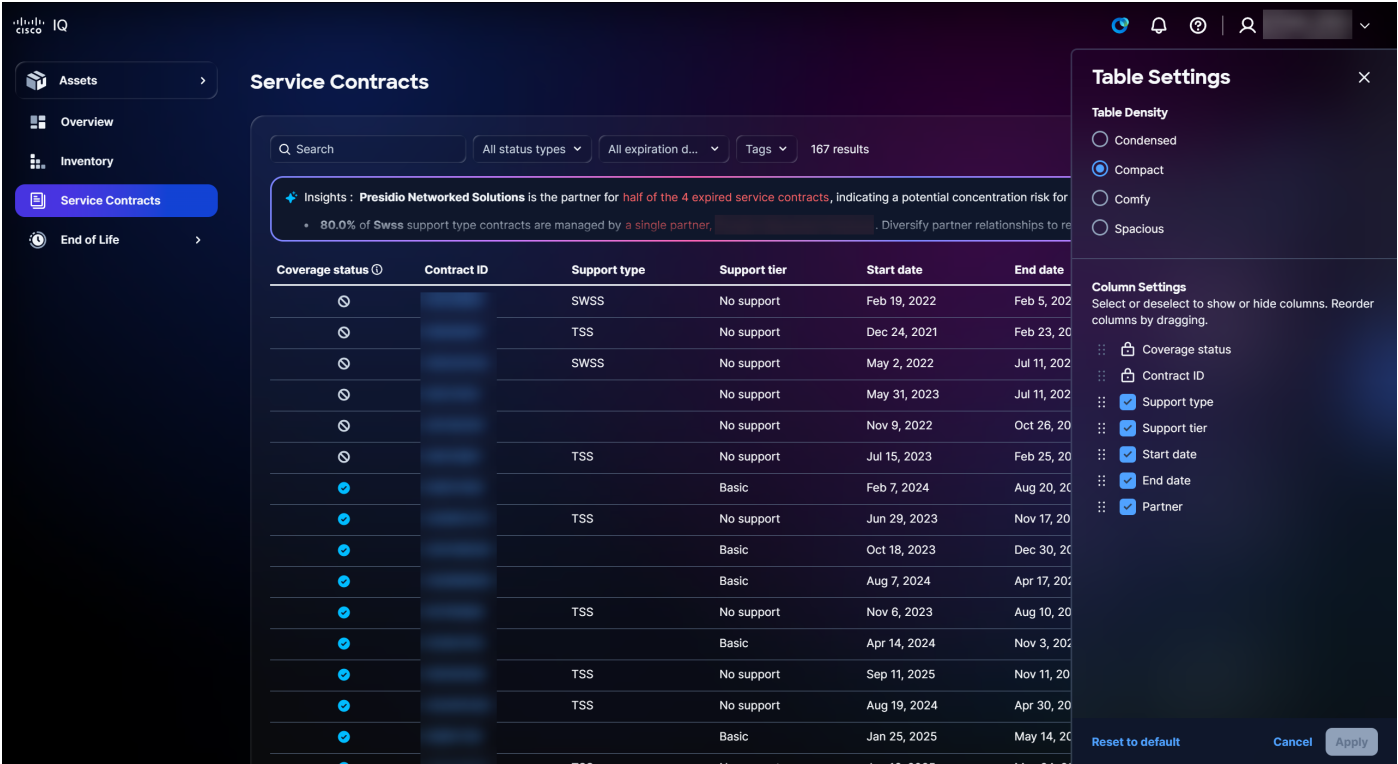
表設定

您可以配置表設定，為不同的模組功能建立自定義檢視和細化檢視。



表設定

要更改在選定頁面上顯示的列，請按一下表設定圖示。Table settings隨即顯示。



表設定選項

更改表檢視

要更改表檢視，請執行下列操作：

- 1. 選擇下清單密度選項之一：

- 精簡:最小化可視元素和間距以顯示更多資訊
- 精簡:減少UI元素之間的空白並縮小間距
- 舒適:利用更多的空白和更大的元素間距
- 寬敞:強調豐富的空白和更大的UI元素

2. 按一下「Apply」。

新增和刪除列

要新增或刪除列，請執行以下操作：

1. 選中或清除列設置覈取方塊。
2. 按一下「Apply」。



附註：無法從表檢視中刪除Name列。

更改列順序

要更改列順序：

1. 拖放列名以按所需順序排列專案。
2. 按一下「Apply」。

自定義儀表板

自定義控制面板功能使您能夠通過一系列直觀的自定義選項來個人化標準控制面板：

- 使用拖放功能重新排列儀表板小部件或面板
- 刪除與工作流程無關的任何元件
- 您的個人化控制面板佈局會安全地儲存到您的使用者配置檔案中，並自動應用於所有會話和裝置
- 使用簡單的重置選項恢復原始儀表板佈局

要自定義儀表板，請執行以下操作：

1. 導航到儀表板。



自訂

2. 按一下「Customize」。



編輯儀表板

3. 根據需要更改控制面板：

- 重新排列：將小部件拖放到所需的佈局中
- 刪除:按一下Delete圖示可刪除構件
- 重設:按一下重置為預設，將儀表板重置為其原始佈局

4. 按一下「Save」。將顯示Dashboard Saved消息。

儀表板佈局會自動應用於所有會話和裝置。

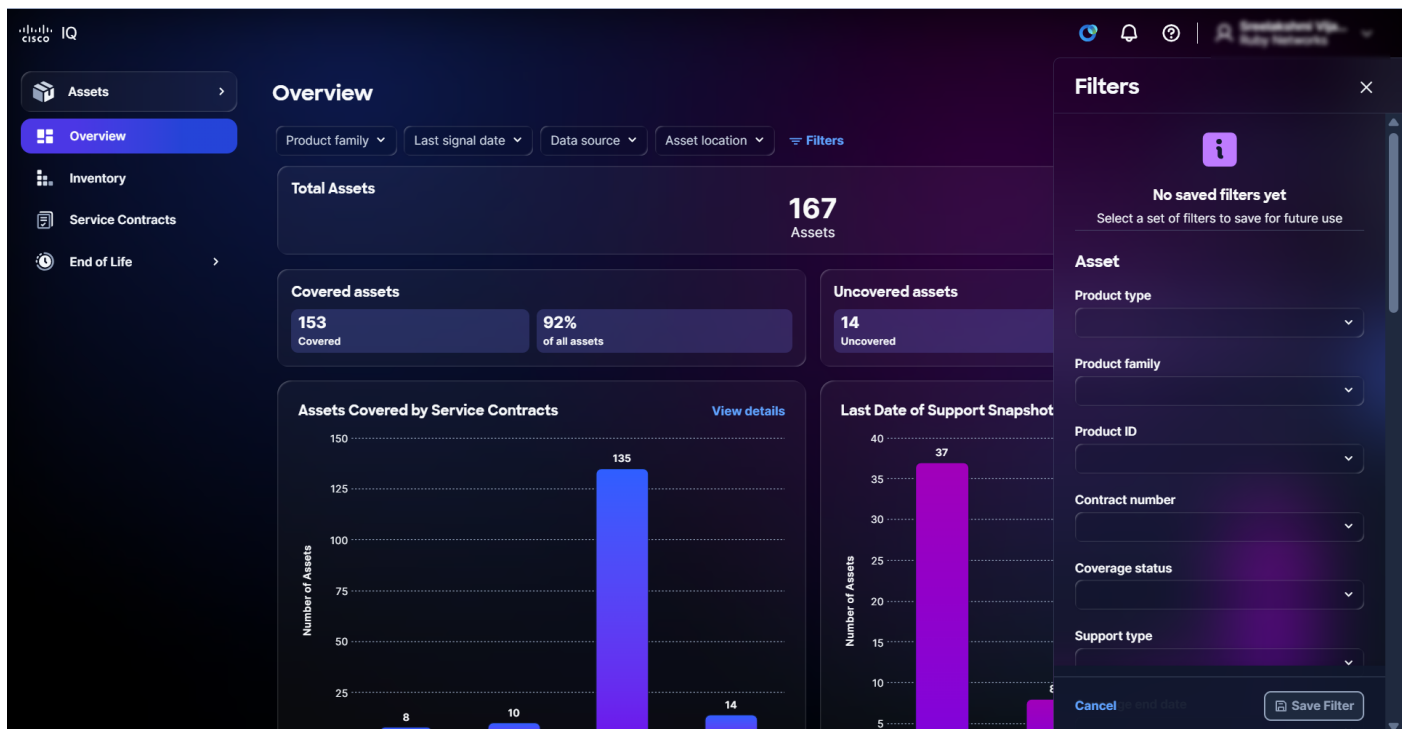
自定義篩選器

您可以為任何儀表板檢視儲存自定義篩選器配置，從而根據需要輕鬆返回首選設定。所有篩選器首選項都以每個使用者、每個帳戶的方式安全地儲存，確保您每次訪問Cisco IQ時都能獲得個人化和一致的體驗。

建立篩選器

要建立自定義篩選器：

1. 導航到儀表板。
2. 按一下「Filters」。



篩選條件

3. 從下拉選單中選擇所需的過濾器。
4. 按一下「Save Filter」。將開啟「名稱儲存的過濾器」(Name Saved Filter)視窗。

Name saved Filter

Filter name *

Custom Filter |

Cancel

Save Filter

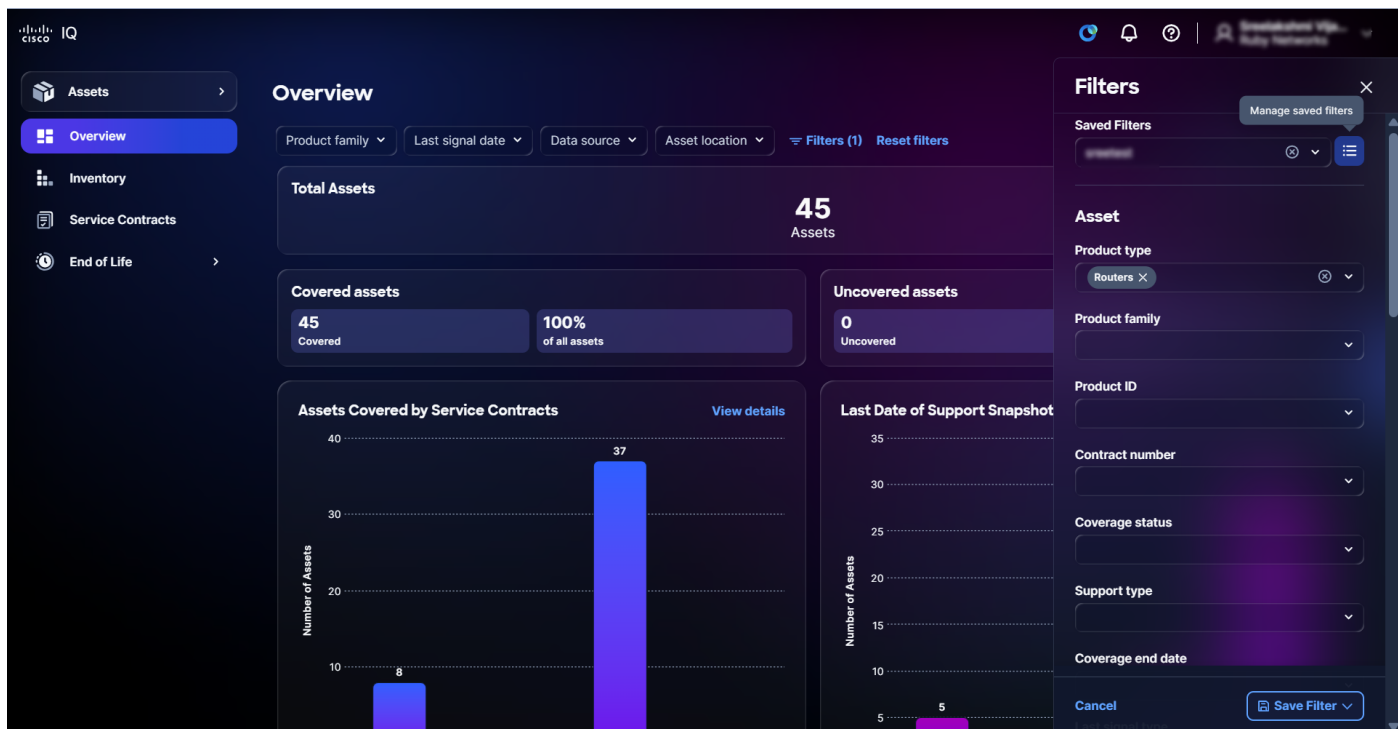
篩選器名稱

5. 輸入過濾器名稱。
6. 按一下Save Filter進行確認。

編輯過濾器名稱

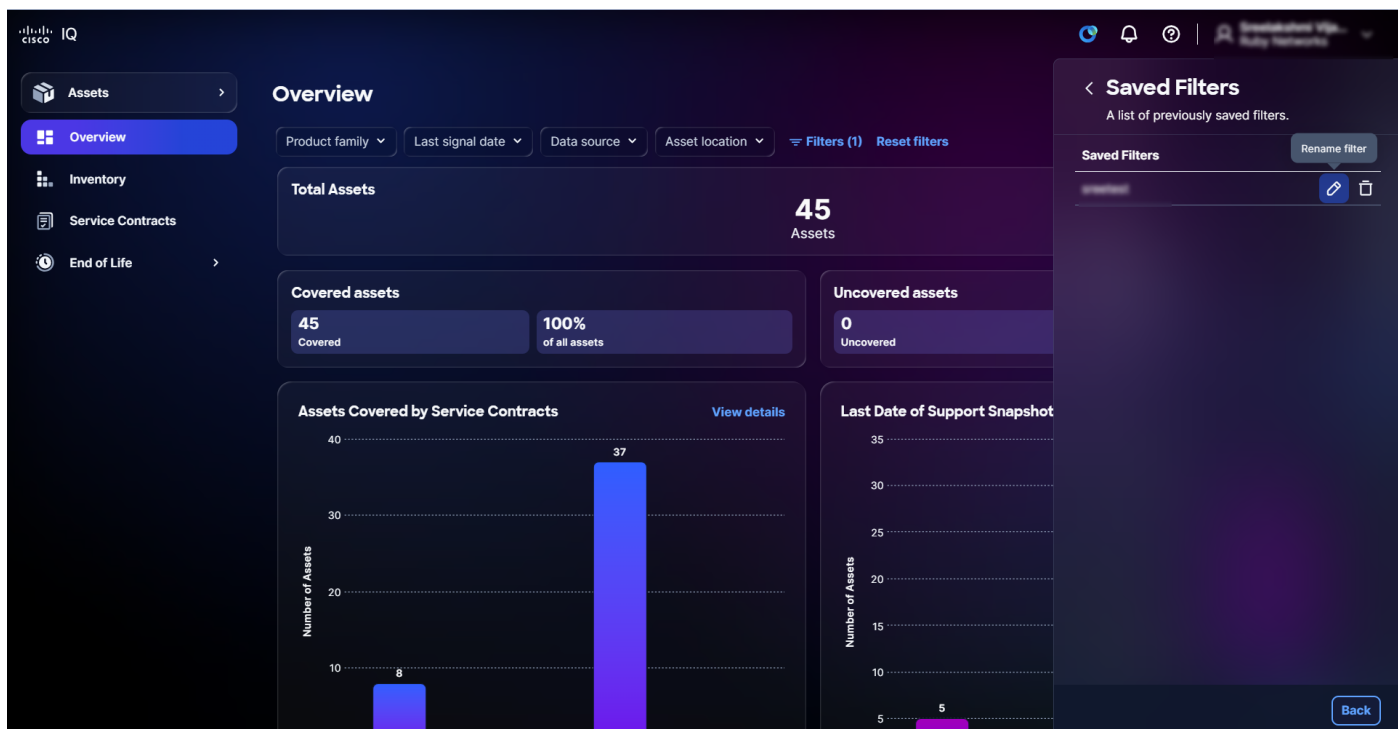
要編輯自定義篩選器，請執行以下操作：

1. 按一下「Filters」。



管理已儲存的篩選器

- 點選管理儲存的過濾器圖示。
- 導航到篩選器。



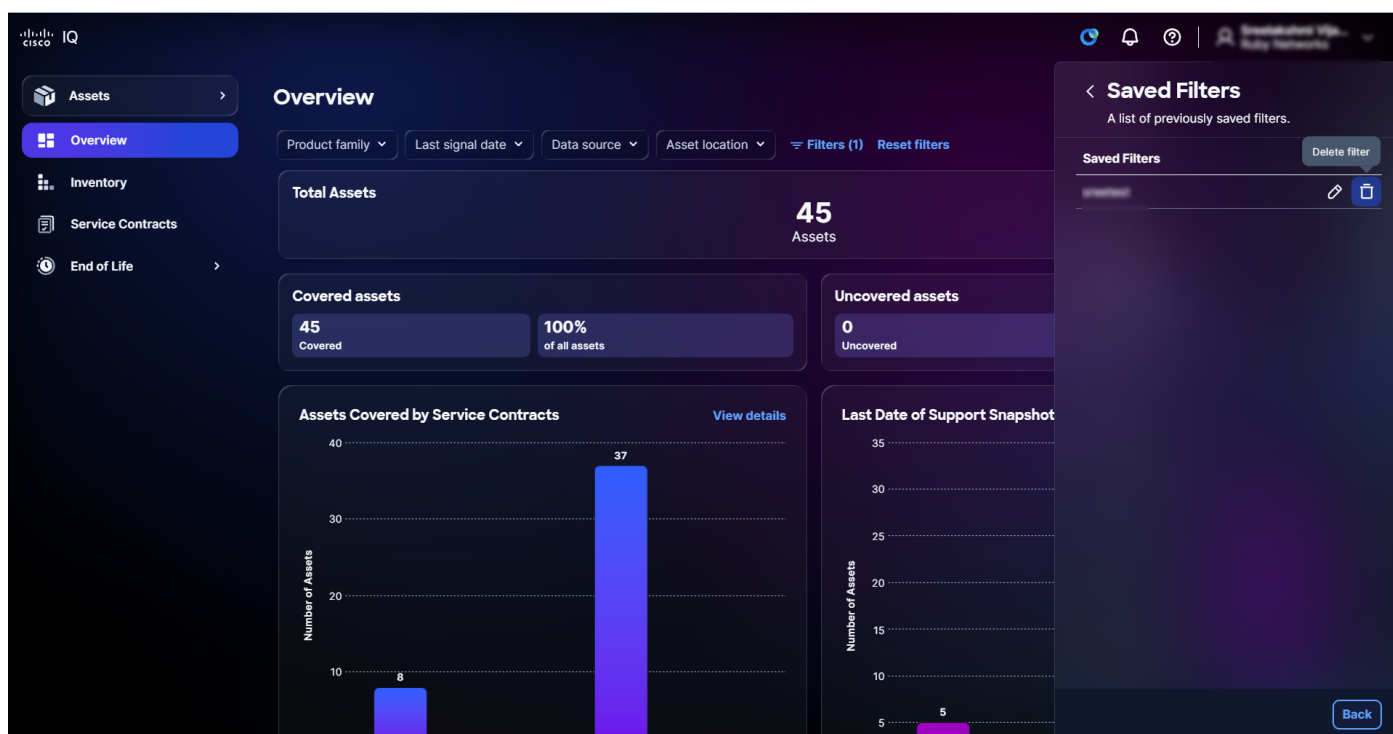
編輯篩選器

4. 按一下Edit圖示。將開啟名稱儲存的篩選器視窗。
5. 編輯過濾器名稱。
6. 按一下Save Filter進行確認。

刪除篩選器

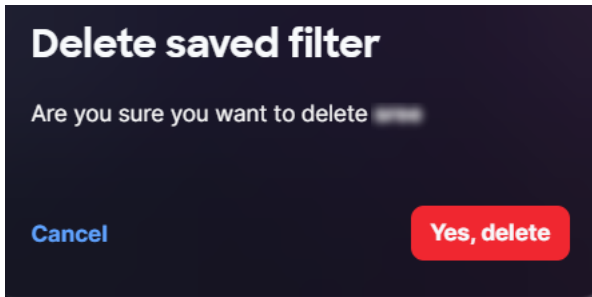
要刪除自定義過濾器，請執行以下操作：

1. 按一下「Filters」。
2. 按一下託管儲存的過濾器圖示
3. 導航到篩選器。



刪除儲存的篩選器

4. 按一下Delete圖示。將開啟刪除儲存的篩選視窗。



刪除儲存的過濾器確認

5. 按一下Yes，delete進行確認。

資產模組

資產模組為思科資產提供全面的可視性和管理功能，是思科IQ的基礎，提供組織內所有裝置的集中清單。通過從多個來源收集資訊，它可以作為裝置清單的單一資料來源。維護完整而準確的資產清單至關重要，因為Cisco IQ中的其他模組（如「評估」模組）會依賴此資料來評估裝置的健康和安全性。

核心概念

Assets模組基於以下核心概念：

- 資產:作為思科服務交付的一部分進行清點和管理的任何物理裝置、硬體或軟體，並詳細跟蹤其身份、功能、服務覆蓋範圍和生命週期
- 源自合約之資產:資產直接從連結的服務合約資料進入庫存，而不是通過遙測方式。Cisco IQ從合約資料接收以下裝置型別：機箱、模組、電源和風扇。即使不存在遙測連線，這些資產在清單中也是可見的
- 最後支援日期(LDOS):思科產品的生命週期結束和支援結束里程碑跟蹤
- 服務範圍:與特定硬體或軟體相關聯的有效支援合約、保修和權利級別
- 資產標籤:分配給資產的用於組織、篩選和操作工作流程的使用者定義標籤
- 裝置訊號:是指思科上次根據裝置遙測、支援案例和合約續訂來觀察裝置（按序列號）的時間；通過多層資料管道攝入和豐富資產遙測資料

訪問資產模組

要訪問Cisco IQ中的資產管理功能，請選擇Home menu > Assets，或者從Home page > Launchpad頁籤的Application部分按一下Assets。系統隨即會顯示Overview頁面。

資產概述

Overview頁面顯示一個控制面板，您可以通過該控制面板快速評估裝置的運行狀況和狀態。

100% Assets, Asset ID, At-risk Assets, Asset Inventory, v1.0.0



Assets



Overview



Inventory



Service Contracts



End of Life



Overview

Filters

Ask AI

Customize

Saved Filters

Total Assets

199

Assets

928

Assets and subcomponents

Key Asset Metrics

Covered Assets

186

Covered

93%

Of all assets

Uncovered Assets

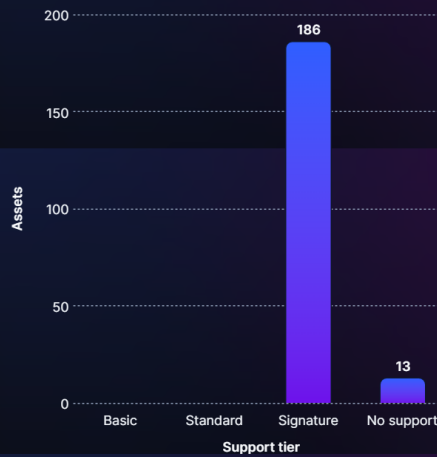
13

Uncovered

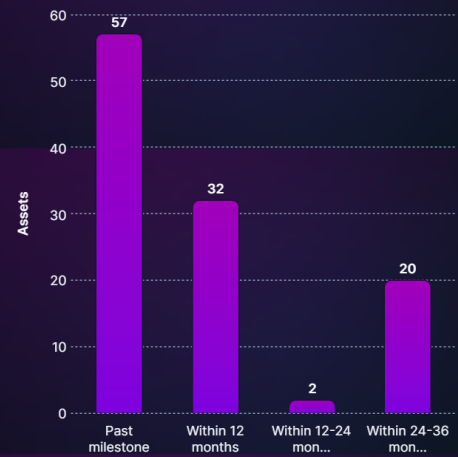
7%

Of all assets

Assets Covered by Service Contracts [View details](#)



Last Date of Support Snapshot [View details](#)



Assets With Telemetry Enabled

186

With telemetry

93%

Of all assets

Assets Without Telemetry Enabled

13

Without telemetry

7%

Of all assets

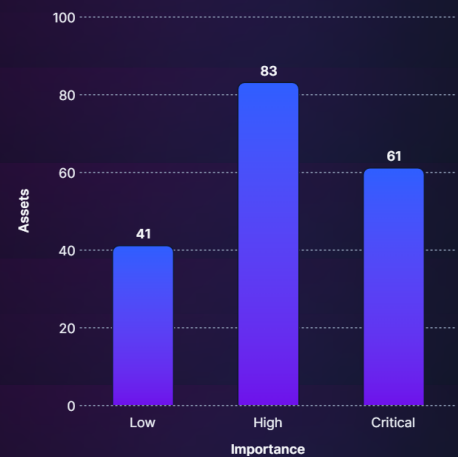
Assets With Critical or High Security Advisories [View details](#)



Of the 186 assets with telemetry enabled, 170 have critical or high Security Advisories

Assets by Importance [View details](#)

Importance can be evaluated for 185 assets.

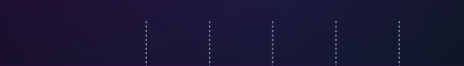


Asset Breakdown

Top 5 Product Families [View details](#)



Top 5 Install-At Locations [View details](#)



資產概述

控制面板顯示以下資訊：

- 總資產: Cisco IQ帳戶內的資產總數
- 關鍵資產指標: 其他關鍵指標，如遙測狀態、關鍵安全建議和LDOS資訊
- 覆蓋資產: 服務合約覆蓋的資產總數和百分比
- 未覆蓋資產: 服務合約未覆蓋的資產總數和百分比
- 服務合約涵蓋的資產: 服務合約涵蓋的資產（硬體或軟體）數量的細分，按權利級別分類
- 最後支援日期快照: 超過LDOS或達到LDOS的資產數量細分
- 啟用遙測的資產: 啟用遙測的資產總數和百分比
- 未啟用遙測的資產：未啟用遙測的資產總數和百分比
- 具有關鍵或高級安全建議的資產：已啟用遙測且具有關鍵或高級安全建議的總資產百分比
- 按重要性列出的資產：相對於網路中的其他裝置而言，分配給裝置的優先順序的細分。
- 資產細分: 資產資訊的詳細顯示，例如產品系列、安裝位置、軟體版本和資產角色

篩選資源的檢視

您可以從下拉選單中選擇一個過濾器，或按一下過濾器並從可用過濾器清單中選擇一個選項，從而對儀表板檢視進行篩選。

 附註：根據螢幕縮放設定，可能會隱藏某些濾鏡。根據您的角色和許可權，可使用不同的過濾器。

檢視資產的詳細資訊

按一下View Details時，該頁面將重定向到Inventory頁面。有關更多資訊，請參閱[清單](#)。

資產重要度洞察

思科IQ包括Asset Criticality Insights，這是Assets模組中的一項新功能，用於預測網路裝置的功能角色和業務重要性。通過分析裝置配置和啟用的功能，資產重要性洞察可幫助您確定哪些資產對網路的影響最大，以便您可以根據安全補救、軟體升級、生命週期終止(EOL)規劃和覆蓋決策確定這些資產的優先順序。

 附註：資產重要程度洞察僅適用於具有活動遙測連線的標準或簽名級別的資產。請確保您的資產滿足配置要求，以便在控制面板中填充這些見解。

資產重要度分析可在資產應用中以下區域獲得：

- 資產概述:按資產重要度分析屬性篩選和檢視摘要細分
- 資產庫存:按角色和重要性顯示、搜尋、篩選和排序裝置
- 資產詳細資訊:檢視單個裝置的角色和重要性，並提供說明每個值的資訊工具提示

覆蓋角色和重要性分類

思科IQ根據遙測資料自動預測每項資產的角色和重要性。當自動預測不能準確反映資產在網路中的功能或重要性時，帳戶管理員可以手動更正這些分類。

 附註：覆蓋控制僅適用於帳戶管理員。對於所有其他使用者角色，「角色」和「重要性」值均為只讀。

改寫庫存表中的分類

要改寫一個或多個資產的職責或重要性，請執行以下操作：

1. 定位至資產 > 庫存。
2. 按一下所需資產行的覈取方塊。要同時更新多個資產，請選中多個覈取方塊。

Assets Overview Inventory Service Contracts End of Life

Inventory

Assets

Search Filters (2) 20 results Reset filters Export Saved Filters

Insights: Of the 1 assets where Coverage Status is not covered, 1 (100.0%) have Product Description NCS 560 Route...
For 1 assets with Support Tier No Support, Product Family NCS 500 Modules leads at 1 instances (100.0%). Assets la...

4 items selected Cancel Manage Tags

Name	Product ID	Product...	Equipment...	Serial Nu...	Next Mile...	Next Mile...	Contract...	Coverage...	Telemetry...	
		Modules	Module		—	—		✓	✓	0
		Modules	Module		—	—		○	✓	0
✓		Unified ...	Chassis		—	—		✓	✓	1
		Storage...	Chassis		—	—		✓	✓	0

角色和重要性

- 在Role或Importance列中，從資產行下拉選單中選擇正確的值。
- 按一下Apply以確認覆蓋。

具有手動覆蓋值的資產在「角色」或「重要性」列中顯示一個可視指示器。

附註：要刪除先前配置的覆蓋並返回自動預測，請從角色或重要性下拉選單中選擇短劃線(—)選項。

改寫資產明細中的分類

要從資產詳細資訊檢視改寫職責或重要性，請執行以下操作：

- 定位至資產 > 庫存，然後按一下資產。
- 在資產詳細資訊面板中，找到Role和Importance欄位。
- 點選要更新的欄位下拉框並選擇正確的值。
- 按一下「Apply」以確認。

資產的詳細資訊檢視還顯示用於通知原始自動預測的遙測屬性的說明，以幫助確定覆蓋是否合適。

檢視改寫跟蹤線索

所有角色和重要性覆蓋都記錄在帳戶級別的審計線索中。要訪問審計追蹤，請執行以下操作：

- 1. 選擇Home > System Settings > Activity & Logs。
- 2. 選擇Filters > Action Type > override以僅顯示覆蓋事件。

跟蹤線索顯示資產名稱、以前值和新值、進行更改的使用者以及更改的日期和時間。可以使用Export選項匯出審計追蹤。

 附註：可以按日期範圍、使用者和資產名稱過濾審計追蹤。

庫存

Inventory頁面提供Cisco IQ帳戶中所有思科資產的清單。

 IQ

Assets

Overview

Inventory

Service Contracts

End of Life

Inventory

Ask AI

Assets

Search

1 Equipment type

Filters (1)

Reset filters

Export

Saved Filters

Insights: Among the 13 assets with Telemetry Status **Not Connected**, Support Tier **NO SUPPORT** is the most frequen...

With a Partition Key of " (empty)", 10 of the 13 assets have the Next Milestone as End Of Sale (40.0%). As these produc...

☐	Name	Produ ct ID	Produ ct...	Equip men...	Serial Nu...	Next Mile...	Next Mile...	Contr act...	Cover age...	Telem etry...	
☐			Cloud a...	Chassis		End of ...	Jun 25, ...	204107...			0
☐			Wireless	Chassis		—	—	204107...			0
☐			Wireless	Chassis		—	—	204107...			0
☐			Routers	Chassis		—	—	204107...			8
☐			Routers	Chassis		End of ...	Feb 19, ...	204107...			0
☐			Switches	Chassis		—	—	204107...			10

庫存

搜尋和篩選資產清單檢視

您可以從下拉式清單中選擇篩選條件，或按一下Filters，然後從可用篩選條件清單中選擇一個選項，藉此篩選清單檢視。您也可以通過在搜尋欄位中輸入資產名稱來搜尋資產。



附註：

- 根據螢幕縮放設定，某些濾鏡可能被隱藏。
- 根據您的角色和許可權，可使用不同的過濾器。

庫存分析

Inventory頁面上的Insights面板顯示AI驅動分析，該分析提供資產摘要，重點關注支援範圍、連線和里程碑。按一下Full Analysis可檢視圖形、儀表板和圖表等視覺化圖形，這些圖形可提供更多見解。如需詳細資訊，請參閱[分析](#)通用模組功能中的資料。

匯出庫存

按一下Export,以.xls或.csv格式儲存已過濾的資產清單。如需詳細資訊，請參閱[在](#)通用模組功能中匯出資訊。

檢視資產詳細資訊

按一下資產以檢視資產詳細資訊。顯示資產的詳細資訊檢視，其中包含以下頁籤：

- 詳情:顯示資產詳細資訊，如產品、訊號資料、身份、位置、保修和覆蓋範圍資訊

Assets

Overview

Inventory

Service Contracts

End of Life

Inventory

10.197.238.131

Cisco Catalyst Center Appliance (Gen 2) - 44 Core

DetailsProduct AlertsHardwareSoftware

Product

Product ID

Product type

Product family

Last Date of Support

Identity

Serial number

IP address

Hostname

Software version

Role

Importance

Tags

Sold by

Location

Install-at

Signals

Last signal

Last signal type

Telemetry

Telemetry status

Last data collection

Data connector

Warranty

Warranty type

Warranty end date

Coverage

Coverage status

Contract number

Support tier

Coverage end date

Ask AI

資產詳細資訊

- 產品警報：顯示相關產品提示，如安全建議和現場通知

- 硬體:提供硬體EOL詳細的時間表檢視(例如銷售結束、最後發貨和最後支援日期)
- 軟體:提供軟體EOL詳細的時間表檢視

資產標籤

資產標籤是您分配給Cisco IQ中資產清單的自定義標籤。標籤是您定義的key:value對，例如Environment:Prod或Label:Campus。您可以一次為單個資產或許多資產分配標籤，而且您可以按標籤篩選庫存，以快速找到您關心的資產。

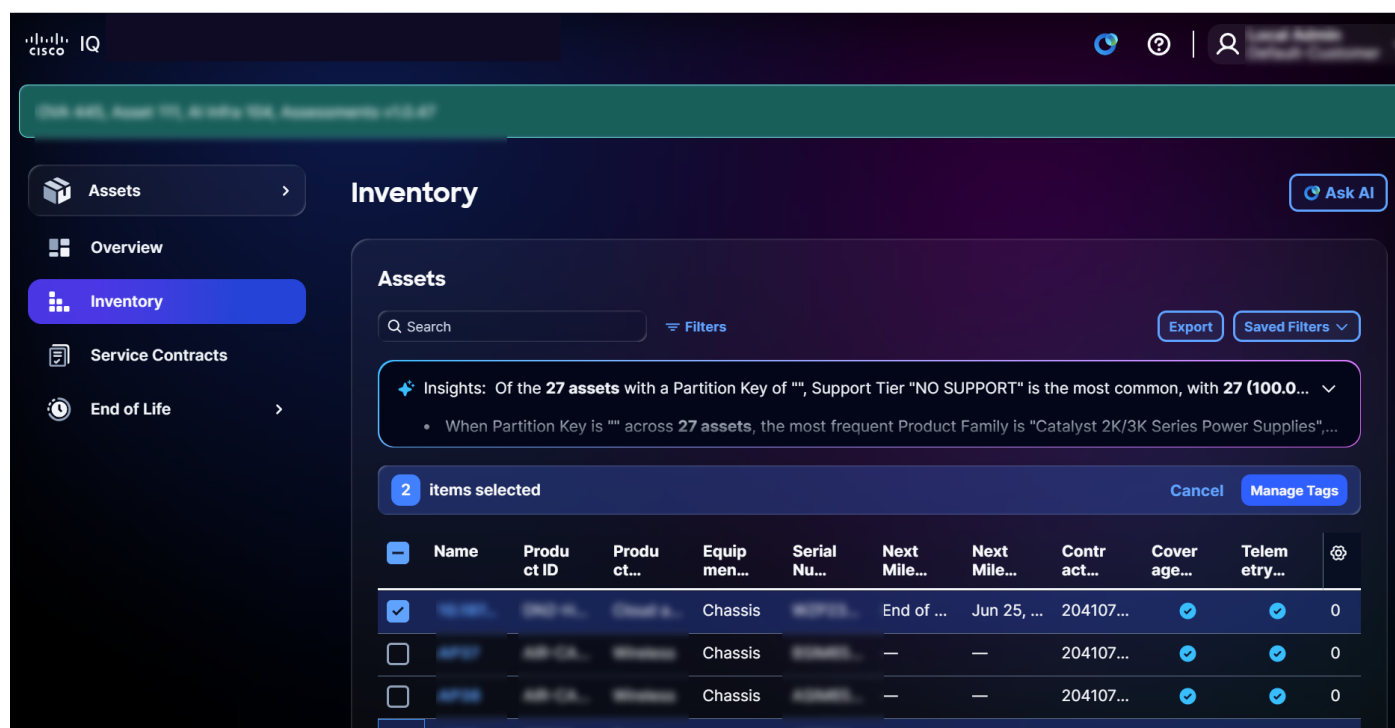
 附註：在帳戶管理員建立標籤後，使用者可以將標籤分配給資產。

分配標籤

在Inventory檢視中向選定資產分配標籤，可以組織和分類資產，從而增強篩選、報告和管理能力。

要將標籤分配給資產，請執行以下操作：

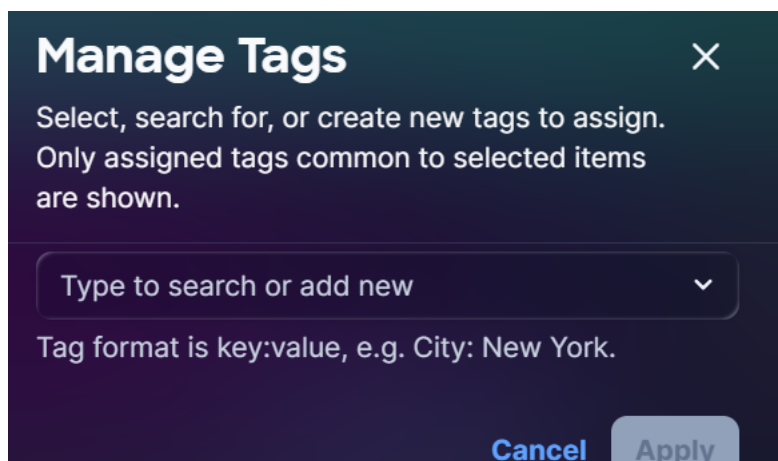
1. 定位至資產 > 庫存。



The screenshot shows the Cisco IQ Inventory page. The left sidebar contains navigation links: Assets, Overview, Inventory (selected), Service Contracts, and End of Life. The main content area is titled 'Inventory' and shows a table of assets. The table has columns: Name, Product ID, Product Name, Equipment Name, Serial Number, Next Mile, Next Mile Date, Contract, Coverage, and Telemetry. A status bar above the table indicates '2 items selected' and provides 'Cancel' and 'Manage Tags' buttons. An 'Insights' section above the table shows that 27 assets have a Partition Key of '' and that the most common Support Tier is 'NO SUPPORT'.

標籤資產

2. 選中所需資源的覈取方塊。
3. 按一下Manage Tags。Manage Tags視窗開啟。



分配標籤

4. 在文本欄位中，輸入或從現有選項中選擇標籤名稱，然後按Enter鍵。



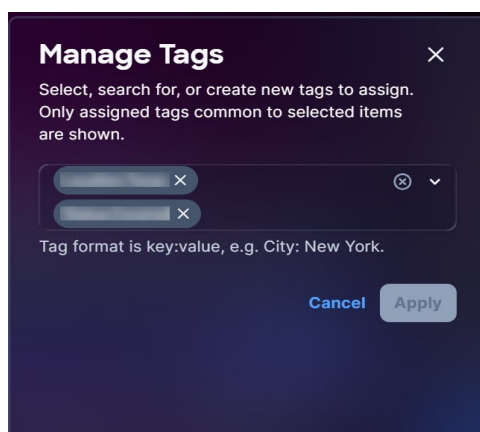
附註：標籤採用key:value格式（例如，City:NYC）。

5. 按一下「Apply」。

刪除資產標籤

要從一個或多個資源中刪除標籤：

1. 定位至資產 > 庫存。
2. 選中一個或多個資產旁邊的覈取方塊。
3. 按一下Manage tags。Manage tags視窗開啟。



刪除標籤

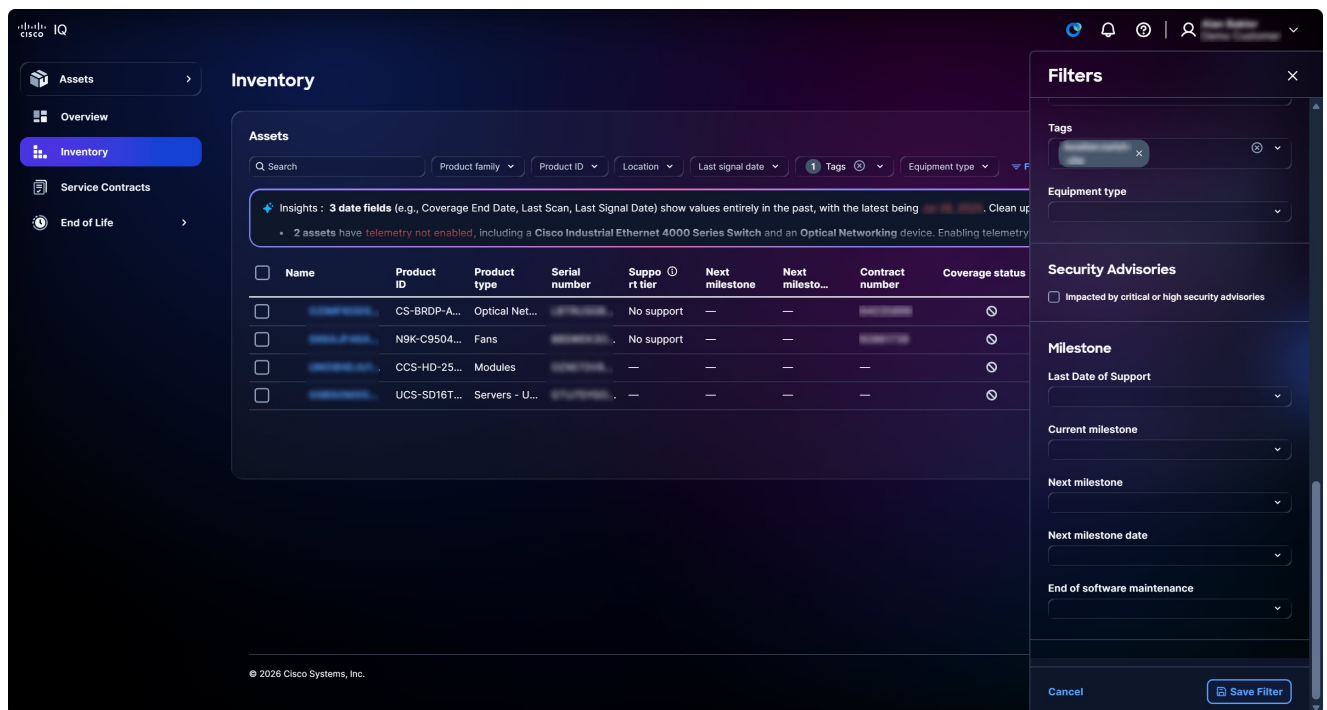
4. 按一下任何標籤上的X將其從選擇內容中刪除。
5. 按一下「Apply」。

使用資產標籤作為過濾器

建立標籤後，可以使用該標籤作為過濾器。

要將標籤用作過濾器，請執行以下操作：

1. 定位至「資產」頁。
2. 按一下「Filters」。Filters視窗開啟。



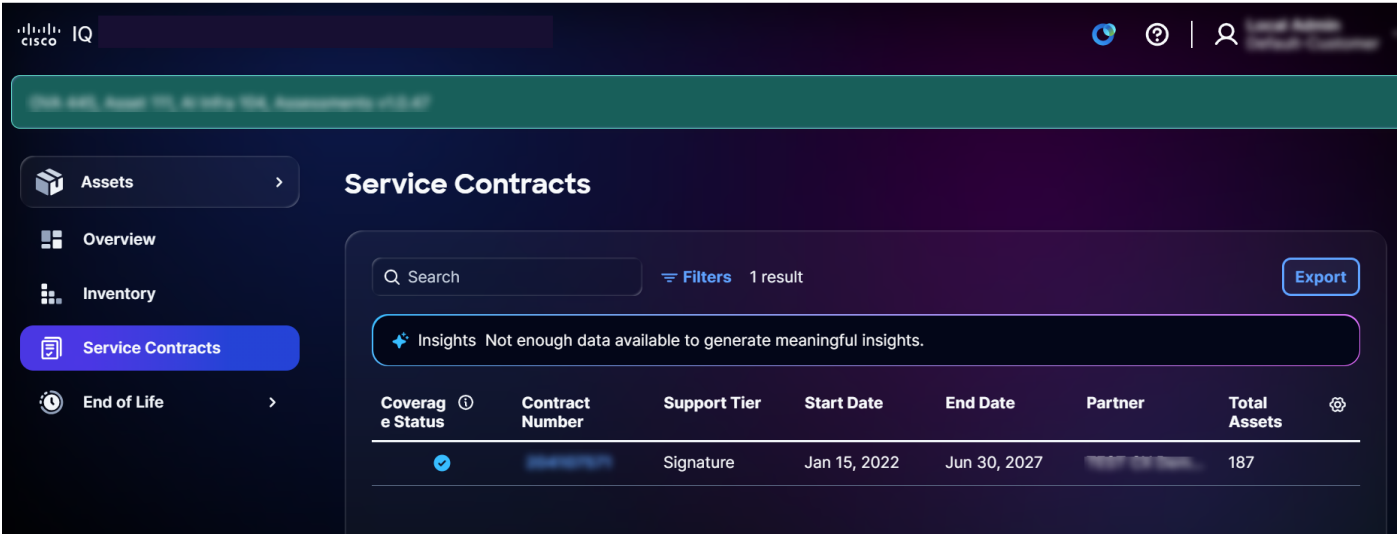
使用標籤作為過濾器

3. 在Tags下拉選單中，選中所需標籤的覈取方塊。選擇標籤後，Inventory頁面上的檢視將更新為篩選檢視。

服務合約

服務合約頁面通過提供摘要和詳細的合約資訊、支援有效的續約規劃和覆蓋範圍戰略，簡化了支援

合約監督工作。



服務合約

搜尋和篩選服務合約檢視

您可以從下拉選單中選擇篩選器，從而篩選清單檢視。您還可以通過在搜尋欄位中輸入合約編號來搜尋服務合約。

匯出服務合約

按一下「Export」，以.xls或.csv格式儲存已篩選的合約清單。如需詳細資訊，請參閱在通用模組功能中匯出資訊。

服務EA摘要

Services Enterprise Agreement(EA)Summary頁提供了整個資產組合中Install Base增長的整合檢視。資料直接來自思科的Install Base記錄，為您和客戶團隊提供了產品組合隨時間變化的統一檢視。

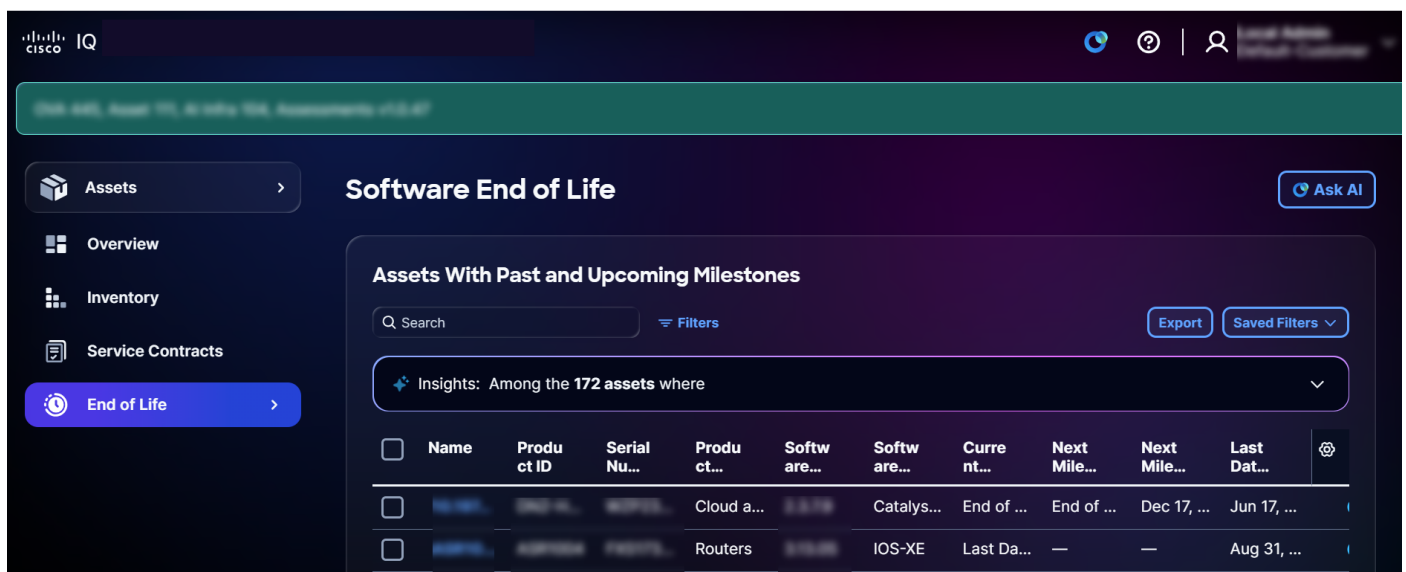
服務EA彙總頁顯示以下資訊：

- 新增的資產：在報告期間向Install Base中新增的新資產
- 淨變化:報告期間安裝資訊庫大小的總體變化

 附註：訪問「服務EA摘要」頁面可能需要遵守角色和許可權要求。如果此頁面在您的導航中不可見，請與您的帳戶管理員聯絡。

壽命終止

硬體壽命終止和軟體壽命終止頁提供詳細的EOL資訊，使使用者能夠獲得主動管理產品更新週期和支援覆蓋範圍所需的支援。按一下「壽命終止」頁上的資產，會將您重定向至「庫存」頁上的相關資產。



☐	Name	Product ID	Serial Nu...	Product...	Software...	Software...	Current...	Next Mile...	Next Mile...	Last Dat...
☐	Cloud a...			Cloud a...	2.2.18	Catalys...	End of ...	End of ...	Dec 17, ...	Jun 17, ...
☐	Routers			Routers	2.2.18	IOS-XE	Last Da...	—	—	Aug 31, ...

軟體壽命終止

壽命終止分析

End of Life頁面上的Insights面板顯示了由人工智慧驅動的資產概述，其中定義了支援的最後一天。按一下Full Analysis可檢視圖形、儀表板和圖表等視覺化圖形，這些圖形可提供更多見解。如需詳細資訊，請參閱[分析](#)通用模組功能中的資料。

匯出壽命終止

按一下Export,以.xls或.csv格式儲存已過濾的EOL資產清單。如需詳細資訊，請參閱[在](#)通用模組功能中匯出資訊。

評估模組

「評估」模組提供了一個評估框架，使您能夠主動調查並緩解與安全性、穩定性、容量、合規性和老化相關的風險，從而保持網路的安全、穩定和可靠。

核心概念

「評估」模組基於以下核心概念：

- 評估:根據預定義的標準對基礎設施實體進行系統評估，以衡量效能、合規性、安全性或運營能力；評估按需求、按時間表或由事件觸發
- 評估執行:評估的例項或單個運行；每次執行都會建立一個新的執行記錄，用於跟蹤評估生成的範圍、觸發機制、時間戳和結果資料
- 查詢結果：可操作的有效的觀察，可識別差距、風險、問題或值得注意的狀態。評價結果表示評價期間的地面資料
- 深入分析:從多個調查結果的模式或趨勢中得出的更高級的分析結論。洞察力解釋在更廣泛的業務或運營環境中發現結果的意義
- 建議：與發現或洞察力相聯絡的具體可行處方；建議就解決已發現問題或把握機遇的必要步驟提供明確指導
- 報告:針對目標受眾彙總調查結果、見解和建議的結構化文檔；報告是將評估結果傳達給客戶、執行官和技術團隊的主要交付內容

訪問評估模組

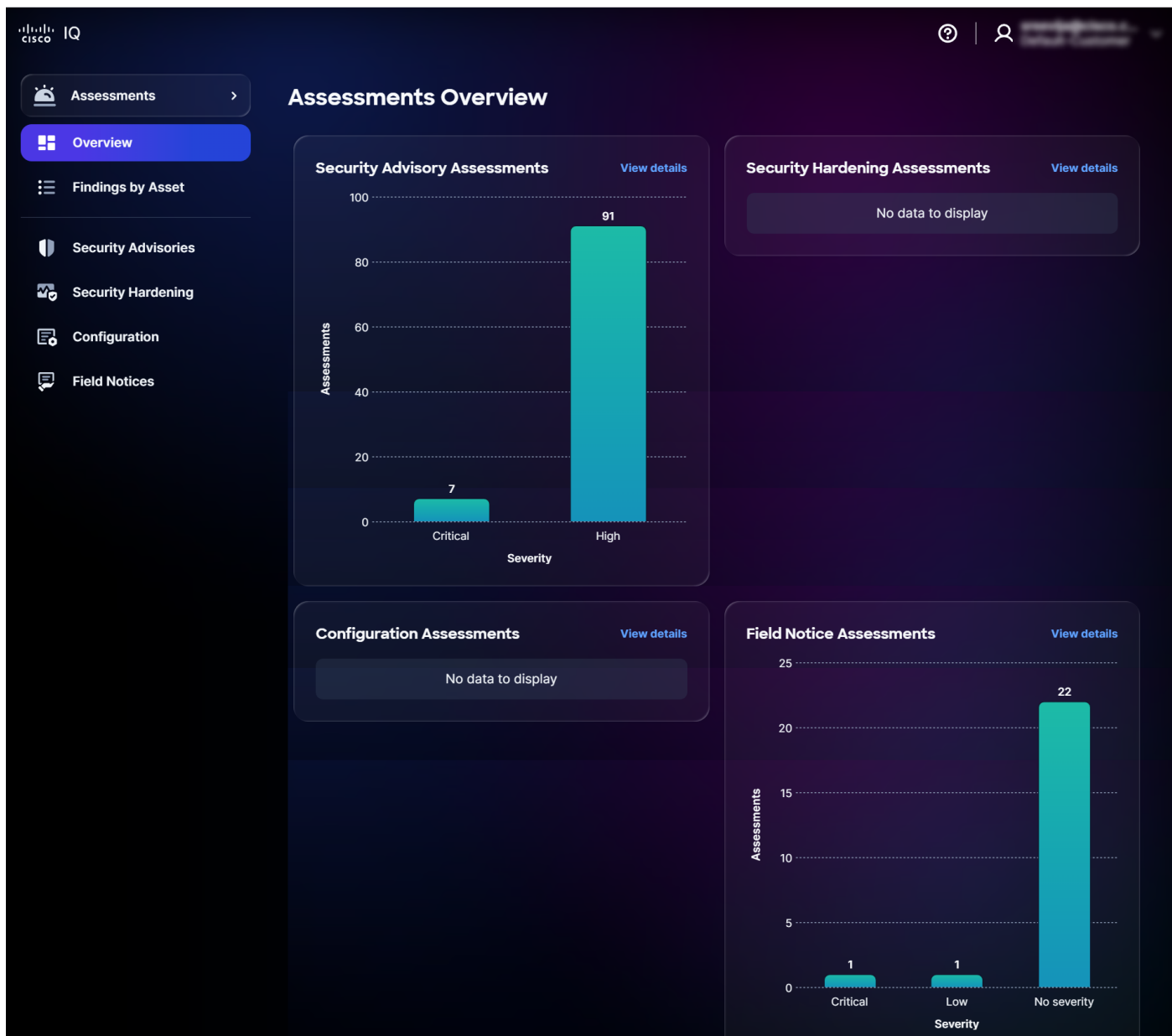
要訪問Virtual Appliance中的安全和評估功能，請選擇「首頁」(Home)菜單>「評估」(Assessments)，或者從「首頁」(Home)頁面>「啟動板」(Launchpad)頁籤的「應用程式」(Application)部分按一下「評估」(Assessments)。系統隨即會顯示「Assessments Overview」頁面。



附註：也可以從系統配置 > 軟體包管理啟動評估模組。

評估概述

Assessments Overview頁顯示以下控制面板：



評估概述

控制面板顯示以下資訊：

- 安全諮詢評估:顯示安全諮詢評估，按「嚴重」和「高」嚴重性分類
- 安全強化評估:顯示未通過安全強化規則的資產，按「高」、「中」、「低」和「資訊」嚴重性分類
- 配置評估:顯示配置合規性規則失敗的資產，按「嚴重」、「高」、「中」、「低」和「資訊」嚴重性分類
- 現場通知評估:顯示現場通知評估，按「嚴重」、「高」和「不適用」嚴重性進行分類



附註：您只能檢視您有權訪問的資產。

按資產顯示的結果

按資產列出的結果頁提供了已使用以下評估中的至少一個評估的資產清單：資安諮詢、資安加固、組態和現場通知。

The screenshot shows the 'Findings by Asset' page in the Cisco IQ interface. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset (selected), Security Advisories, Security Hardening, Configuration, and Field Notices. The main content area displays a table of findings. The table has the following columns: Name, Importance (with a help icon), IP Address, Serial Number, Security Advisory, Security Hardening, Configuration, Field Notice, and Signature (with a help icon). The table contains 5 rows of data, all with 'Low' importance and 'Signature' links. Above the table, there is a search bar, a 'Filters' button, and a '208 results' indicator. To the right of the table, there are 'Export' and 'Saved Filters' buttons.

Name	Importance	IP Address	Serial Number	Security Advisory	Security Hardening	Configuration	Field Notice	Signature
Device A	Low	10.10.1.1	123456789	5	11	32	1	Signature
Device B	Low	10.10.1.2	123456789	5	11	32	1	Signature
Device C	Low	10.10.1.3	123456789	5	11	32	1	Signature
Device D	Low	10.10.1.4	123456789	5	11	32	1	Signature
Device E	Low	10.10.1.5	123456789	5	11	32	1	Signature

按資產顯示的結果

按資產搜尋和篩選查詢結果的檢視

您可以從下拉式清單中選擇篩選條件，或按一下Filters，然後從可用篩選條件清單中選擇一個選項，藉此篩選清單檢視。您還可以在「搜尋」(Search)欄位中按資產搜尋查詢結果。



附註：

- 根據螢幕縮放設定，某些濾鏡可能被隱藏。
- 根據您的角色和許可權，可使用不同的過濾器。

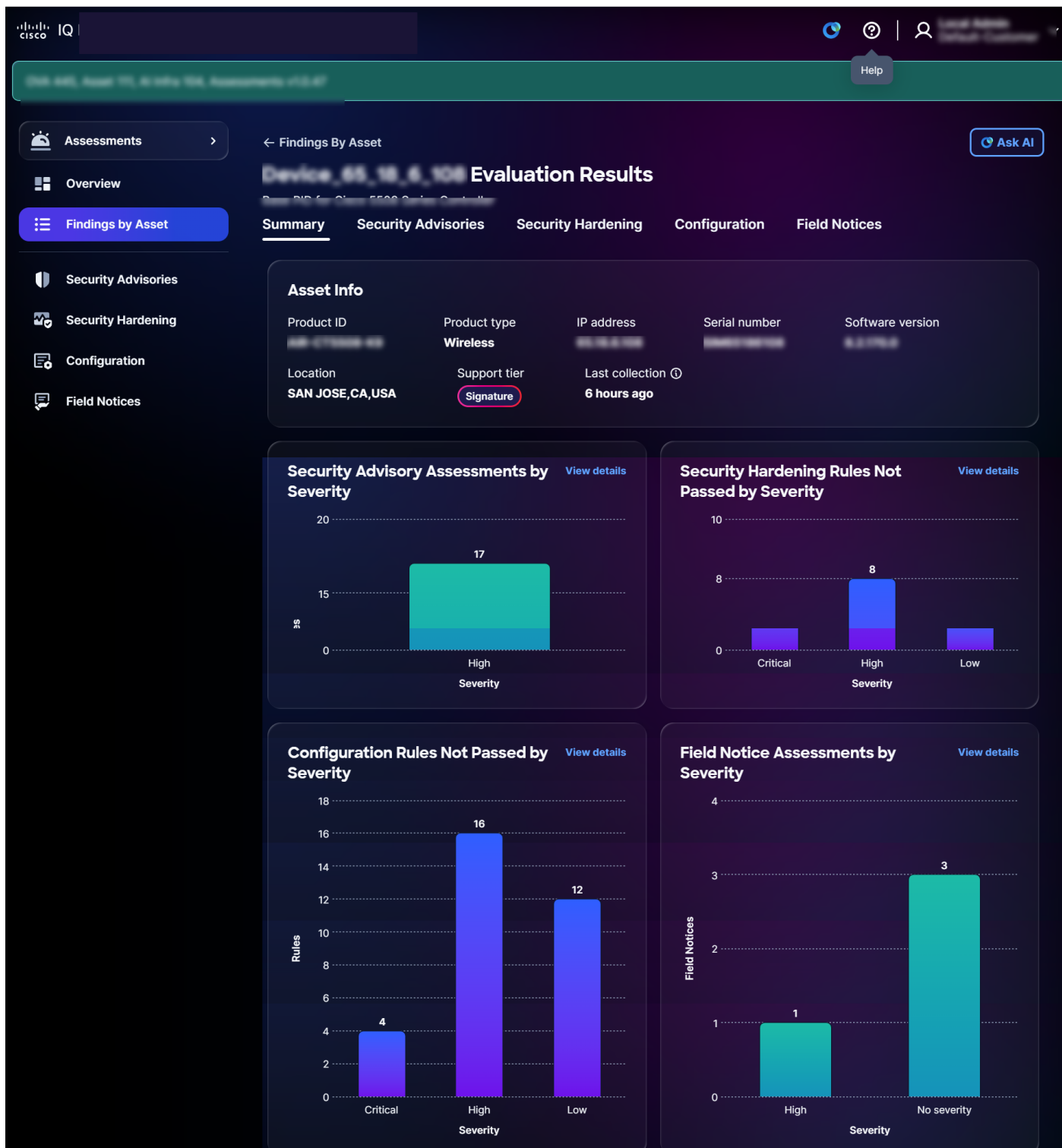
按資產匯出結果

要按資產匯出查詢結果清單檢視，請按一下匯出。如需詳細資訊，請參閱[匯出資訊](#)。

按資產詳細資訊檢視查詢結果

要按資產詳細資訊檢視查詢結果，請單擊資產。以下頁籤顯示所選資產的詳細資訊：

- 摘要:提供詳細的資產資訊，包括Security Advisories、Security Hardening、Configuration和Field Notices的數量
- 參考指南:提供相關安全諮詢評估清單
- 安全強化:提供不符合安全強化規則的資產的清單
- 組態:提供未通過配置最佳實踐規則的資產清單
- 社群與培訓:提供相關的Field Notice評估清單



按資產詳細資訊列出的結果

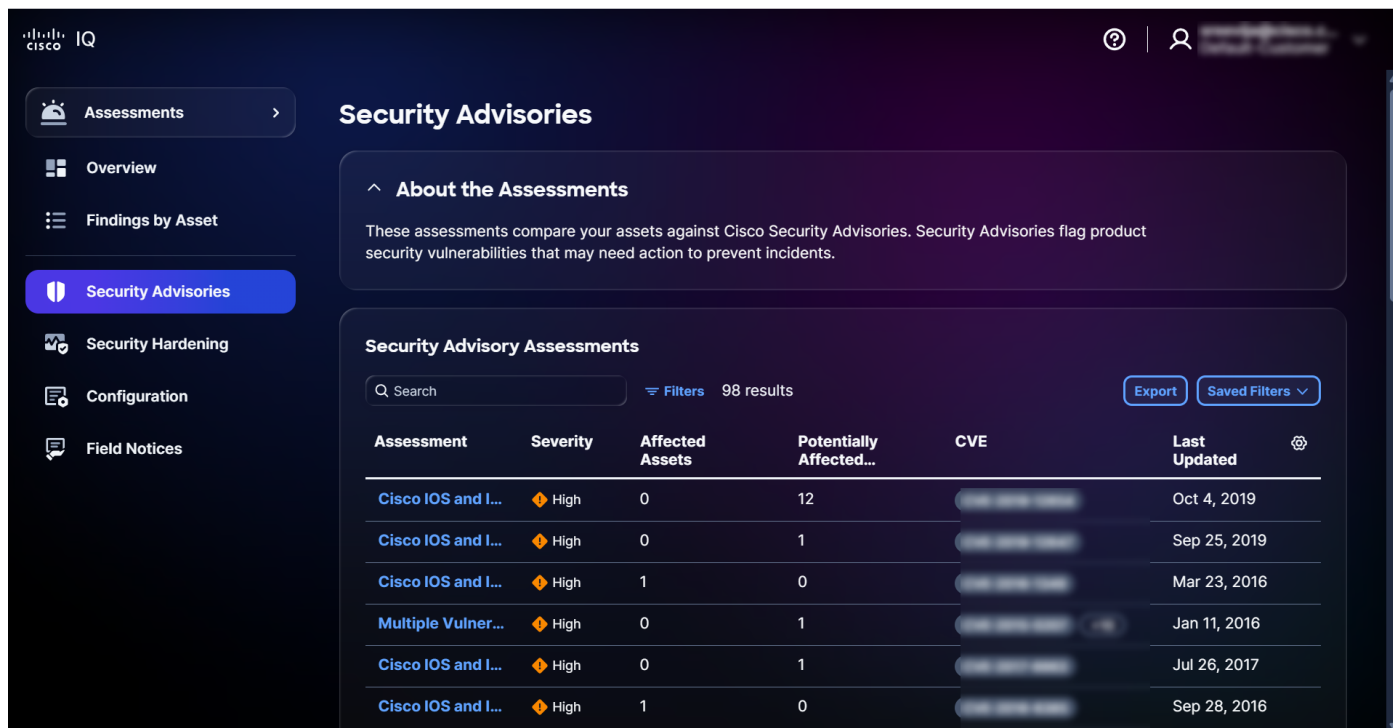
在磁貼上按一下View Details時，頁面將重定向到模組中的相關頁面。

按一下檢視全部資產詳細資訊時，將顯示「資產詳細資訊」檢視頁。

參考指南

安全諮詢評估可識別漏洞，並根據漏洞的風險、嚴重性和重要性確定優先順序，從而增強組織的風險管理能力。安全諮詢可提供關於漏洞的精細洞察，幫助加快關鍵威脅的緩解，並確保與合規性和業務目標保持一致。這增強了安全狀況，最佳化了資源分配，並促進了針對整個企業中不斷演變的威脅的恢復能力。Cisco IQ中發佈的安全建議一經發佈即自動更新。

Security Advisories頁面提供在組織中檢測到漏洞的所有安全諮詢的清單。按一下「安全建議評估」清單中的建議可以導航到相應的詳細檢視。



Assessment	Severity	Affected Assets	Potentially Affected...	CVE	Last Updated
Cisco IOS and I...	High	0	12		Oct 4, 2019
Cisco IOS and I...	High	0	1		Sep 25, 2019
Cisco IOS and I...	High	1	0		Mar 23, 2016
Multiple Vulner...	High	0	1		Jan 11, 2016
Cisco IOS and I...	High	0	1		Jul 26, 2017
Cisco IOS and I...	High	1	0		Sep 28, 2016

參考指南

搜尋和篩選檢視以查詢安全建議

您可以通過從下拉選單中選擇篩選器來篩選清單檢視。您也可以通過在搜尋欄位中輸入評估名稱來搜尋安全建議評估。

 注意：根據螢幕縮放設定，一些濾鏡可能被隱藏。根據螢幕縮放設定，一些濾鏡可能被隱藏。根據您的角色和許可權，可使用不同的過濾器。缺少的嚴重性值顯示為「—」，帶有描述性工具提示。

匯出安全建議

要匯出安全諮詢評估，請按一下匯出。如需詳細資訊，請參閱[匯出資訊](#)。

檢視安全建議評估詳細資訊

按一下Assessment可檢視有關它的其他詳細資訊。詳細資訊頁面提供例如通用漏洞評分系統(CVSS)評分、通用漏洞和洩露(CVE)、Severity等資訊，以及指向所參考思科安全顧問的連結。

您可以在「測評結果」(Assessment outcome)表格中查看以下結果：

- **影響**:表示該資產或元件具有已被確認的漏洞，攻擊者可以利用該漏洞進行攻擊，從而需要進行補救
- **可能受到影響**：表示該資產或元件顯示可能導致漏洞的跡象，但並未得到最終確認；可能還需要做進一步調查

The screenshot displays the Cisco IQ interface for a security advisory. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories (selected), Security Hardening, Configuration, and Field Notices. The main content area is titled 'Cisco IOS and IOS XE Software Session Initiation Protocol Denial of Service Vulnerability'. It includes an 'About the Assessment' section with a description of the vulnerability, a 'Severity' of High, a 'CVE' identifier, a 'CVSS score', 'Version' 1.1, 'First published' date of Sep 25, 2019, and 'Last updated' date of Oct 4, 2019. Below this is the 'Asset Results' section, which shows a table of 12 results. The table has columns for Asset, Result, Product ID, IP Address, Serial Number, and Support Tier. All results are marked as 'Potentially Affected'.

Asset	Result	Product ID	IP Address	Serial Number	Support Tier
ISR44...	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature
Isr4431	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR44...	Potentially Affected				Signature
ISR43...	Potentially Affected				Signature

參考指南

搜尋和篩選資產評估結果的檢視

您可以從下拉式清單中選擇篩選條件，或按一下Filters，然後從可用篩選條件清單中選擇一個

選項，藉此篩選清單檢視。您也可以通過在搜尋欄位中輸入資產名稱來搜尋資產。

 附註：根據螢幕縮放設定，一些篩選器可能會被隱藏。根據您的角色和許可權，不同的篩選器可用。

檢視資產評估結果

要檢視測評結果的詳細資訊，請按一下「測評結果」(Assessment Outcome)表格中的資產。系統將顯示資產的評估結果詳細資訊頁面。

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Security Advisories > Cisco Secure Boot Hardware Tampering Vulnerability

Device_66_10_4_106 **Result**

Assessment: Cisco Secure Boot Hardware Tampering Vulnerability

Result Details

Potentially affected

Evidence

Matched on software type

Matched on chassis product ID

Matched on module product ID

Additional Verification Needed

1) Software Releases are not checked for the automation of this Security Advisory. You must manually check your software release against the information in the advisory. 2) Module/Chassis PID level Automation is not done for the following product families. Please refer to the Security Advisory for the impacted PIDs and determine the Vulnerability of the device Cisco 4000 Series Integrated Services Routers Cisco Catalyst 6800 Series Switches Cisco Network Convergence System 5500 Series Routers

About the Assessment

A vulnerability in the logic that handles access control to one of the hardware components in Cisco's proprietary Secure Boot implementation could allow an authenticated, local attacker to write a modified firmware image to the component. This vulnerability affects multiple Cisco products that support hardware...

Show more

Severity

High

CVE

CVSS score

6.7

First published

May 13, 2019

Last updated

Nov 20, 2019

References

Security Advisory

About the Asset

View evaluated asset

Product ID

Product type

Switches

IP Address

Serial Number

Software version

Location

SAN JOSE,CA,USA

Support tier

Signature

結果詳細資訊

匯出資產結果以進行安全諮詢

要匯出資產結果，請按一下匯出。如需詳細資訊，請參閱[匯出資訊](#)。

安全強化

安全加固功能可針對行業標準基準持續評估路由器、交換機和防火牆，從而近乎即時地自動瞭解網路基礎設施的安全狀態。它可識別配置差距並提供切實可行的補救指導，使客戶管理員能夠有效地減少攻擊面，並保持與思科嚴格的安全最佳實踐的一致性一致。通過集中合規性監控和簡化強化過程，該模組將安全管理從被動任務轉變為主動的、資料驅動的戰略，從而確保恢復力和安全的企業網路。



附註：安全強化評估僅適用於具有標準支持層的資產。

檢視安全強化評估

Security Hardening Assessment頁面顯示以下資訊：

Security Hardening Assessment

This assessment only applies to assets with Standard or Signature support. Learn about your coverage details in [Cisco Support Tiers](#).

About the Assessment

This assessment evaluates your assets against Cisco OS Hardening Guides. It detects configuration deviations across your infrastructure that may affect security posture, or risk exposure. Each security hardening rule is evaluated across your covered assets, with findings prioritized by severity to help you... [Show more](#)

Execution Outcome for Jul 20, 2026, 5:40 AM

Summary

Rule evaluations	Assets included
179	146

Rule evaluations

The number of assets evaluated by a rule may differ based on its pre-checks.

Q Search Filters 179 results Export Saved Filters

Rule	Severity	Assets Evaluated	Did Not Pass	Passed	Inconclusive	Not Appli...	Soft war...
Console M...	Medium	6	0	0	6	0	IOS
IGP MD5 A...	High	6	0	0	6	0	IOS
Minimum P...	High	31	31	0	0	0	AireOS

安全強化

- 關於評估:通過總結評估的目的提供其他詳細資訊
- 執行結果:提供資產評估結果的摘要，包括規則評估和所包含資產的總數
- 規則評估:提供有關規則的詳細資訊，包括嚴重性、評估的資產、未通過、通過、不確定

、不適用和軟體型別

- 嚴重性:提供規則評估的重要性或影響級別
- 評估資產:提供根據規則條件評估的資產總數
- 未通過:提供評估期間不符合規則條件的資產
- 通過:提供評估期間符合規則標準的資產
- 無結論:提供評估無法確定失敗的資產
- 不適用:指示規則不適用或不相關的資產或方案
- 軟體型別:提供軟體資產型別

搜尋和篩選規則檢視

您可以從下拉式清單中選擇篩選條件，或按一下Filters，然後從可用篩選條件清單中選擇一個選項，藉此篩選清單檢視。也可以通過在搜尋欄位中輸入規則名稱來搜尋規則。



注意：根據螢幕縮放設定，一些濾鏡可能會隱藏。根據您的角色和許可權，可使用不同的過濾器。

檢視規則評估詳細資訊

要檢視有關規則評估的其他詳細資訊，請按一下規則。將顯示規則的評估詳細資訊頁面，其中包含以下資訊：

The screenshot shows the Cisco IQ Security Hardening Assessment interface. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening (highlighted), Configuration, and Field Notices. The main content area is titled 'Security Hardening Assessment' and 'Minimum Password Length Policy', evaluated on Jul 20, 2026, at 5:39 AM. It includes an 'Ask AI' button. The 'About the Rule' section explains the policy: 'Check 'Min. Password length' in show switch config, and warn if it is lower than 8. Proper security configuration protects the wireless infrastructure from unauthorized access, data interception, and compliance violations.' It shows a severity of 'High', software type of 'AireOS', and 31 assets evaluated. The 'Results Summary' for 31 assets shows: 0 Passed, 31 Didn't pass, 0 Inconclusive, and 0 Not applicable. The 'Asset Results' table lists 31 results, all marked 'Didn't pass'. The table columns are Asset, Result, Product ID, Serial Number, IP Address, and Support Tier. Each row shows a device name, a 'Didn't pass' status, and a 'Signature' link.

規則檢視

- 關於規則:提供規則的詳細資訊，例如Severity、Software type、Version和Assets evaluated，並包括說明性標籤的連結至相關來原始檔
- 結果摘要:提供與規則相關的資產結果摘要，例如Passed、Not pass、Inconsistinal和 Not applicable
- 資產業績:提供資產清單，其中包含資產、結果、產品ID、序列號、IP地址和支援層等詳細資訊



附註：當評估發現為「無結論」時，思科IQ可提供明確的指導，說明原因（例如，缺少遙測或不支援作業系統）並建議驗證資料收集、更新憑證或刷新資料等步驟。此外，還提供相關文檔的標籤連結以幫助解決問題。

搜尋和篩選資產規則的檢視

您可以從下拉式清單中選擇篩選條件，或按一下Filters，然後從可用篩選條件清單中選擇一個選項，藉此篩選清單檢視。您也可以通過在搜尋欄位中輸入資產名稱來搜尋資產評估結果。

 注意：根據螢幕縮放設定，一些濾鏡可能會隱藏。根據您的角色和許可權，可使用不同的過濾器。

匯出資產結果

要匯出規則的評估結果，請按一下匯出。如需詳細資訊，請參閱[匯出資訊](#)。

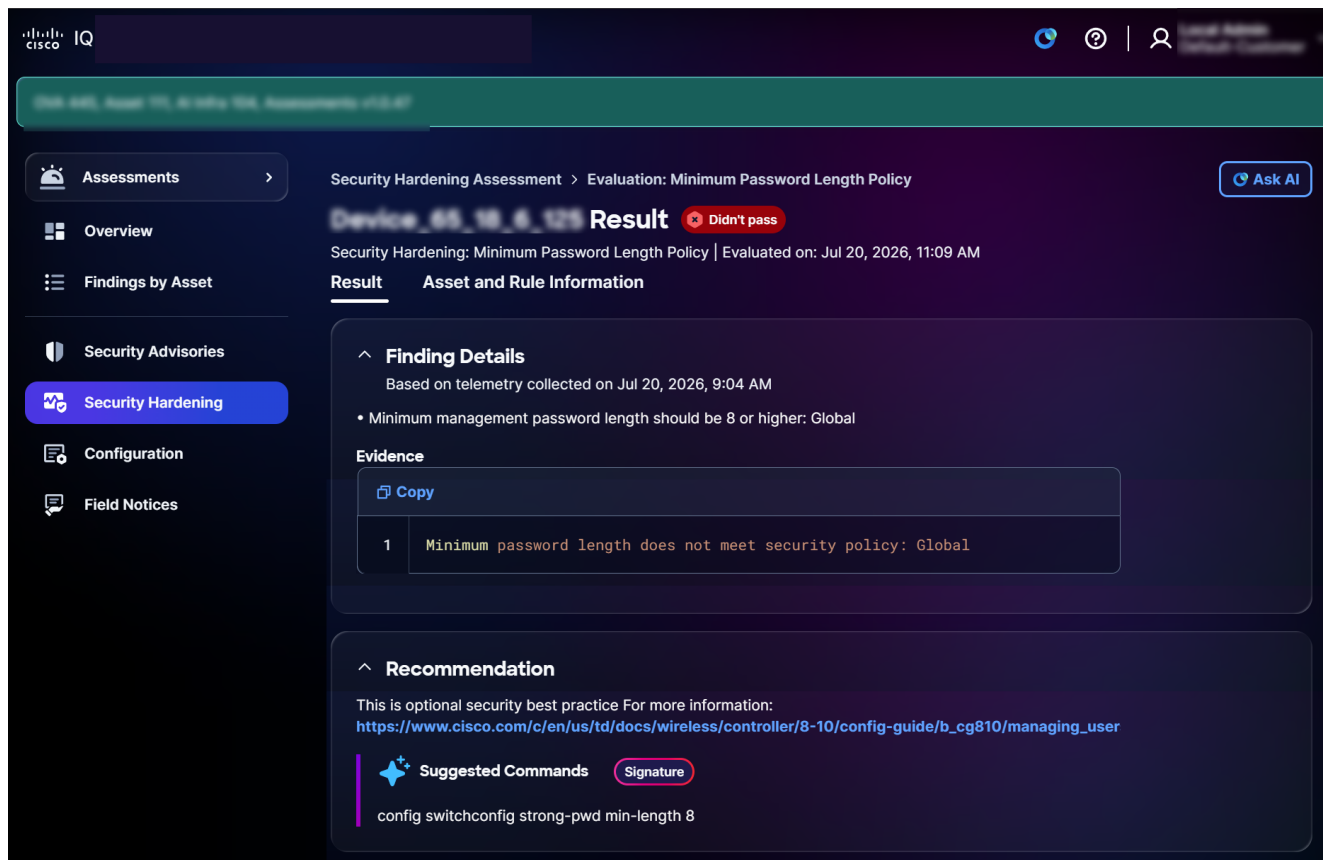
搜尋和篩選資源結果檢視

您可以從下拉式清單中選擇篩選條件，或按一下Filters，然後從可用篩選條件清單中選擇一個選項，藉此篩選清單檢視。您也可以通過在搜尋欄位中輸入資產名稱來搜尋資產結果。

 附註：根據螢幕縮放設定，某些濾鏡可能被隱藏。根據您的角色和許可權，可使用不同的過濾器。

檢視用於加強安全性的資產結果

從「資產結果」中按一下一項資產，以檢視其詳細資訊。資產的結果詳細資訊頁面根據您的權利級別或層顯示資訊。



The screenshot shows the Cisco IQ interface for a Security Hardening Assessment. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening (highlighted), Configuration, and Field Notices. The main panel displays the assessment results for 'Device_65_10_6_125' under the 'Minimum Password Length Policy'. The result is 'Didn't pass'. The findings section shows a single finding: 'Minimum management password length should be 8 or higher: Global'. The evidence section shows a single piece of evidence: 'Minimum password length does not meet security policy: Global'. The recommendation section provides a link to Cisco documentation and suggests the command 'config switchconfig strong-pwd min-length 8'.

安全強化標準層

- 標準層

- 查詢詳細資訊:提供有關評估期間確定的配置偏差以及證據日誌的資訊
- 建議:提供指導，以解決發現的問題並確保配置一致性

檢視資產和規則資訊以強化安全性

要檢視資產及其規則的詳細資訊，請點選Asset and Rule Info選項卡。系統隨即會顯示Asset and Rule Info頁面。

關於資產:提供資產的詳細資訊，如產品ID、產品型別、IP地址、序列號、軟體版本、位置和支援層

- 關於規則:提供規則詳細資訊(包括嚴重性和軟體型別)以及特定強化檢查的重要性

組態

配置評估根據思科成熟的专业知識，根據建議的最佳實踐來評估您的資產，以檢測可能會影響整個基礎設施的可用性、安全性或效能的配置偏差。每個最佳實踐規則都會在您覆蓋的資產中進行評估，並將結果按照嚴重性排定優先順序，以確保配置一致性、增強可復原性並降低運營風險。



附註：配置評估僅適用於具有標準支援層的資產。

檢視配置評估

Configuration Assessment頁面顯示以下資訊：

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Configuration Assessment

This assessment only applies to assets with Standard and Signature support. Learn about your coverage details in [Cisco Support Tiers](#).

About the Assessment

This assessment evaluates your assets against recommended best practices based on Cisco's proven expertise. It detects configuration deviations across your infrastructure that may affect availability, security, or performance. Each best practice rule is evaluated across your covered assets, with findings prioritized b...
[Show more](#)

Execution Outcome for Jul 20, 2026, 05:40 AM

Summary

Rule evaluations

729

Assets included

146

Rule Evaluations

The number of assets evaluated by a rule may differ based on its pre-checks.

Q Search

Filters

729 results

Export

Saved Filters

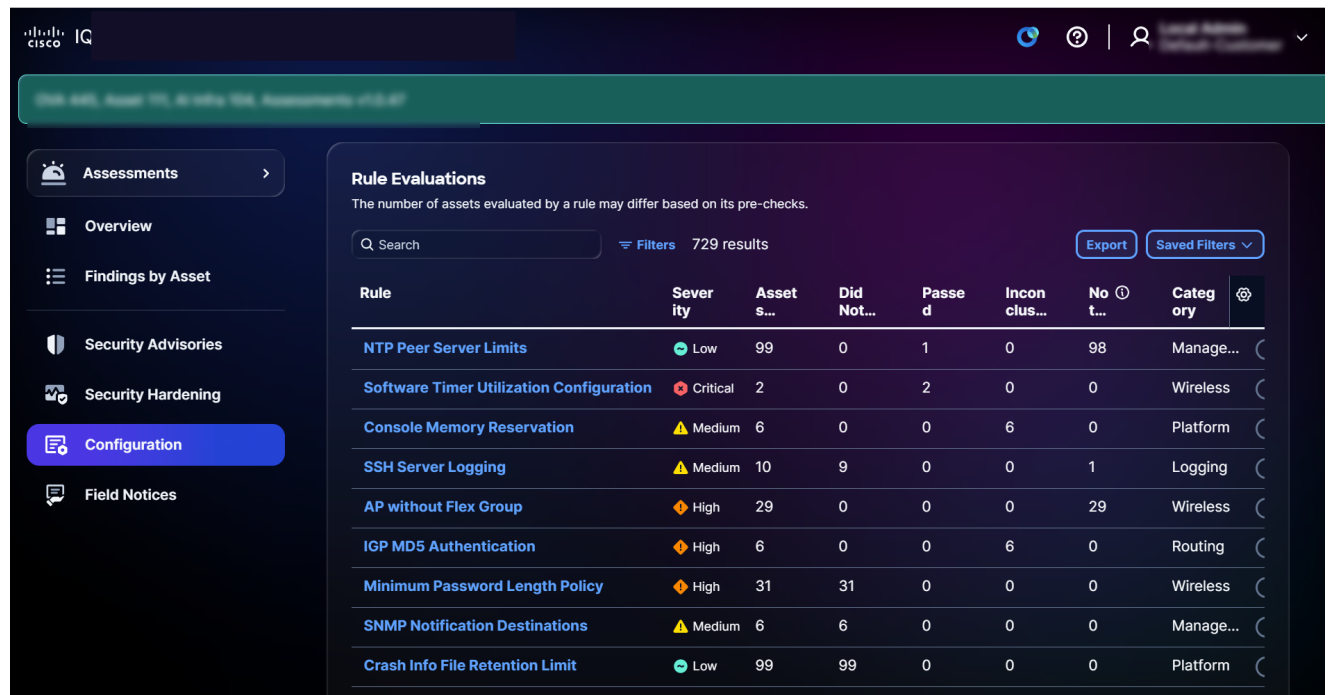
Rule	Severity	Assets	Did Not...	Passed	Inconclus...	Not...	Category
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging

配置評估

- 關於評估:通過總結評估的目的提供其他詳細資訊
- 摘要:提供配置執行摘要，如Rules evaluated和Assets evaluated
- Insights:深入瞭解通過模式分析和結果關聯產生的已識別配置差距；它們顯示為智慧分組的金鑰卡，以突出顯示需要注意的最關鍵領域
- 規則評估:提供有關規則的詳細資訊，包括嚴重性、評估的資產、未通過、通過、不確定、不適用、Category和軟體型別
- 嚴重性:提供規則評估的重要性或影響級別
- 評估資產:提供根據規則條件評估的資產總數
- 未通過:提供評估期間不符合規則條件的資產總數
- 無結論:提供無法運行評估的資產總數
- 通過:提供評估期間符合規則標準的資產
- 不適用:指示規則不適用或不相關的資產或方案
- 類別：提供規則所屬的域區域

- 軟體型別：指示應用規則的軟體資產的型別

搜尋和篩選規則檢視



Rule	Severity	Asset s...	Did Not...	Passed	Inconclus...	No t...	Category	
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...	
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless	
Console Memory Reservation	Medium	6	0	0	6	0	Platform	
SSH Server Logging	Medium	10	9	0	0	1	Logging	
AP without Flex Group	High	29	0	0	0	29	Wireless	
IGP MD5 Authentication	High	6	0	0	6	0	Routing	
Minimum Password Length Policy	High	31	31	0	0	0	Wireless	
SNMP Notification Destinations	Medium	6	6	0	0	0	Manage...	
Crash Info File Retention Limit	Low	99	99	0	0	0	Platform	

規則評估

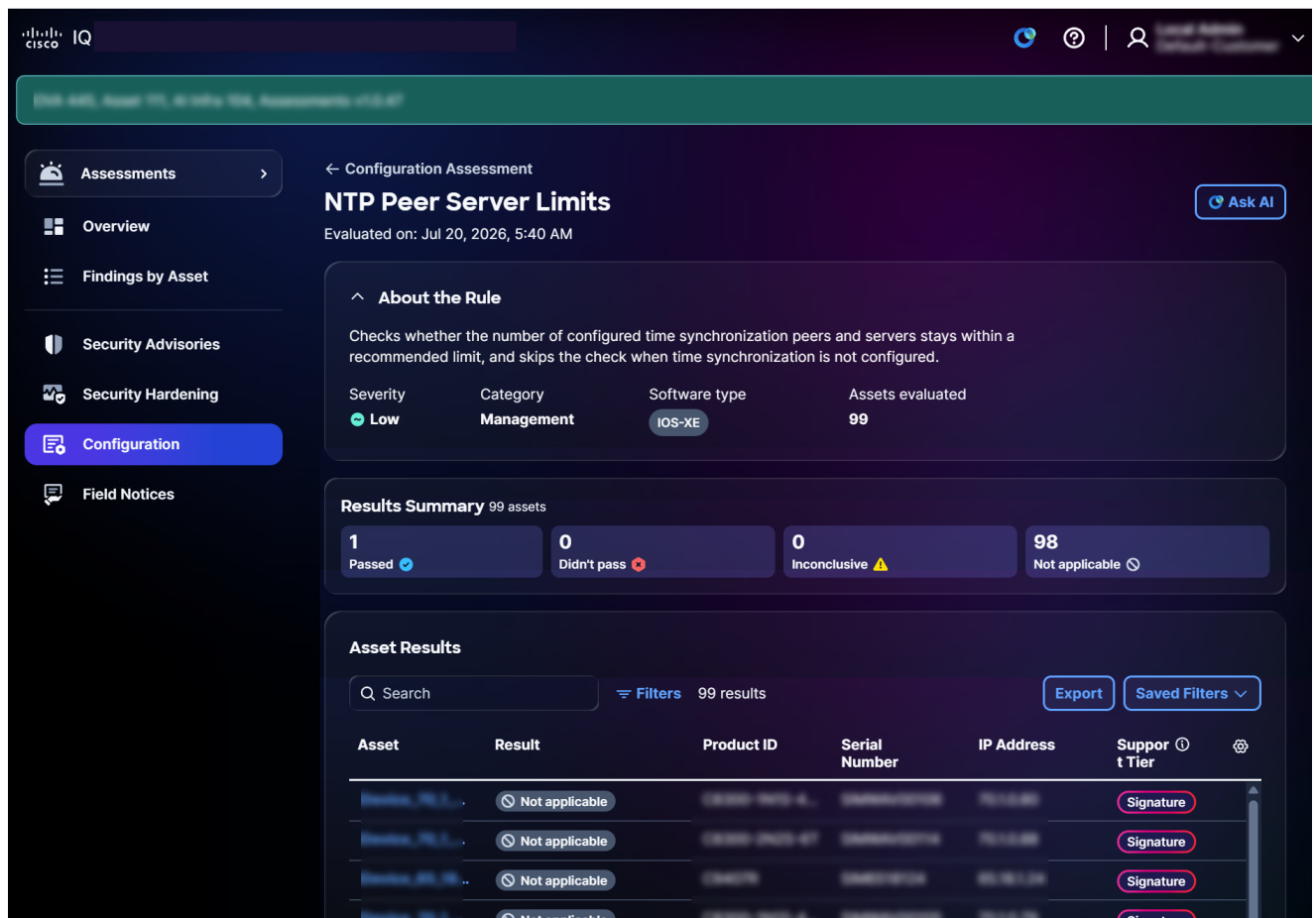
您可以從下拉式清單中選擇篩選條件，或按一下Filters，然後從可用篩選條件清單中選擇一個選項，藉此篩選清單檢視。也可以通過在搜尋欄位中輸入規則名稱來搜尋規則。



附註：根據螢幕縮放設定，某些濾鏡可能被隱藏。根據您的角色和許可權，可使用不同的過濾器。

檢視規則評估詳細資訊

要檢視有關規則評估的其他詳細資訊，請按一下任何規則。將顯示規則的評估詳細資訊頁面，其中包含以下資訊：



評估

- 關於規則:提供諸如Severity、Category、Software type和Assets evaluated等規則的詳細資訊，並包括說明性標籤的連結至相關來原始檔
- 結果摘要:通過顯示通過、未通過、不確定和不適用狀態的資產數，提供整體資產結果
- 資產結果:提供受所選規則影響的具有結果狀態的資產的清單

 附註：當評估發現為「無結論」時，思科IQ可提供明確的指導，說明原因（例如，缺少遙測或不支援作業系統）並建議驗證資料收集、更新憑證或刷新資料等步驟。此外，還提供相關文檔的標籤連結以幫助解決問題。評估模組支援對規則進行多類別選擇，支援同時處理多個規則類別並進行評估。

匯出資產結果

要匯出規則的資產結果，請按一下匯出。如需詳細資訊，請參閱[匯出資訊](#)。

搜尋和篩選資源結果檢視

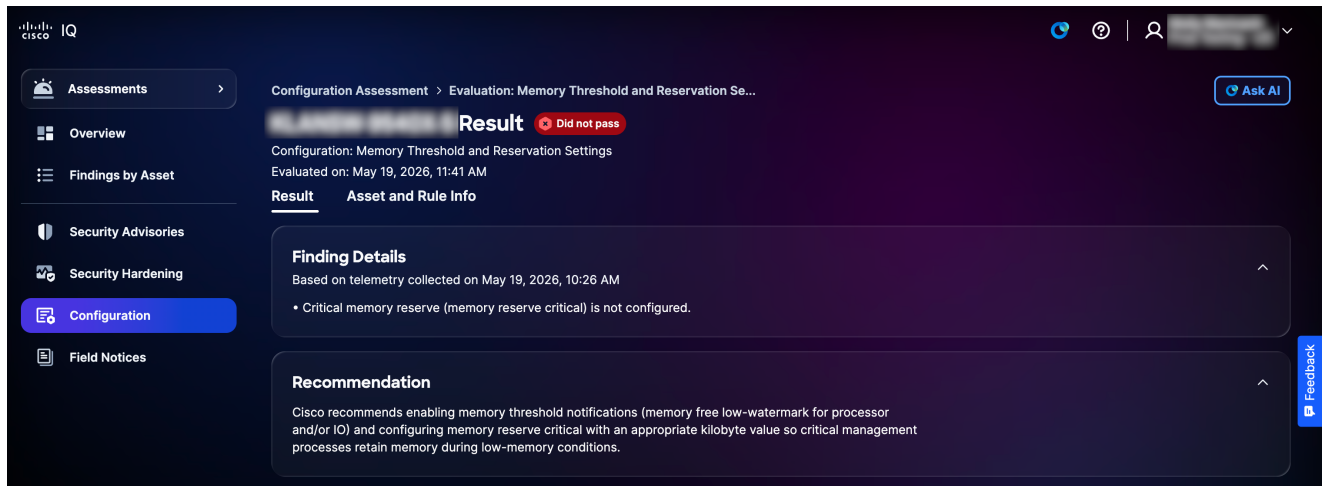
您可以從下拉式清單中選擇篩選條件，或按一下Filters，然後從可用篩選條件清單中選擇一個選項，藉此篩選清單檢視。您也可以通過在搜尋欄位中輸入資產名稱來搜尋資產結果。

 附註：根據螢幕縮放設定，某些濾鏡可能被隱藏。根據您的角色和許可權，可使用不同的過濾器。

檢視配置評估的資產結果

要檢視資產結果的詳細資訊，請從「資產」結果中按一下資產。

資產的結果詳細資訊頁面根據您的權利級別或層顯示資訊。

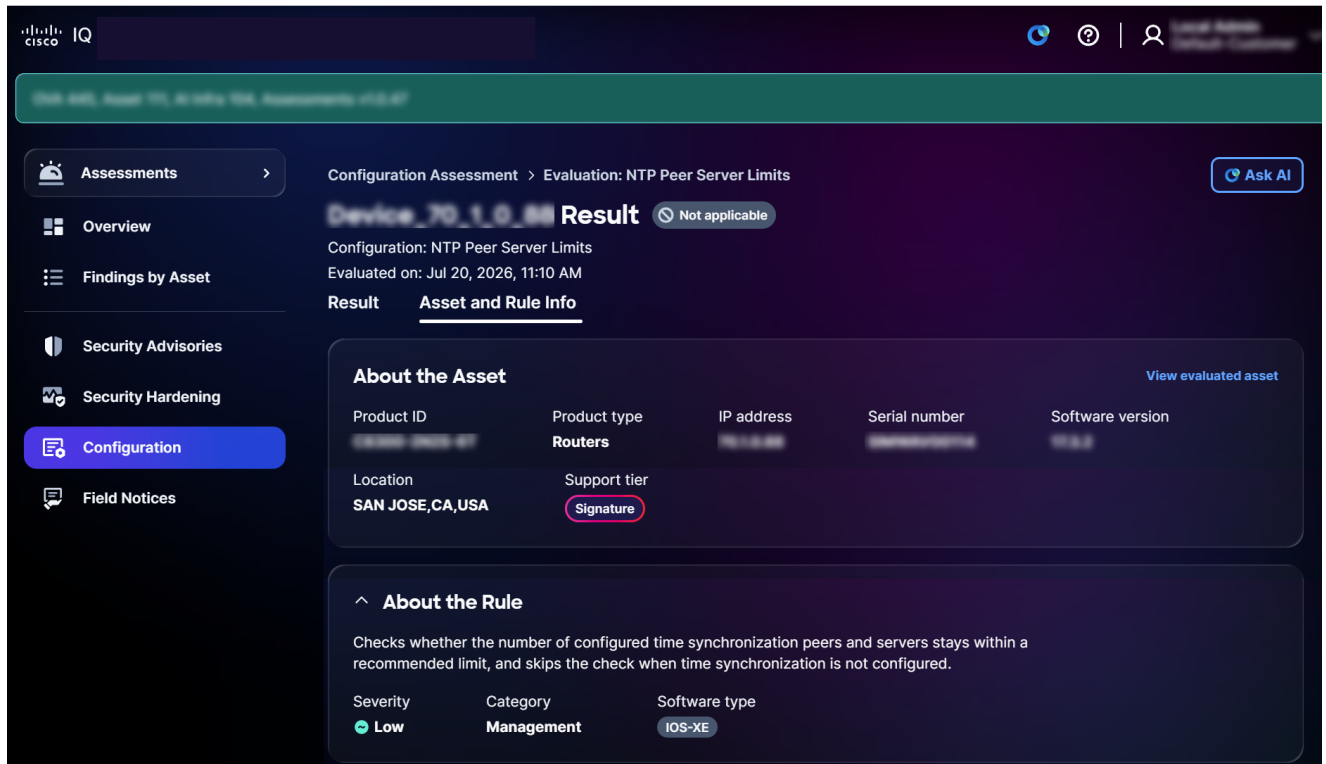


配置標準層

- 標準層
- 查詢詳細資訊:提供有關評估期間確定的配置偏差以及證據日誌的資訊
- 建議:提供指導，以解決發現的問題並確保配置一致性

檢視配置評估的資產和規則資訊

要檢視資產和規則資訊詳細資訊，請點選資產和規則資訊選項卡。



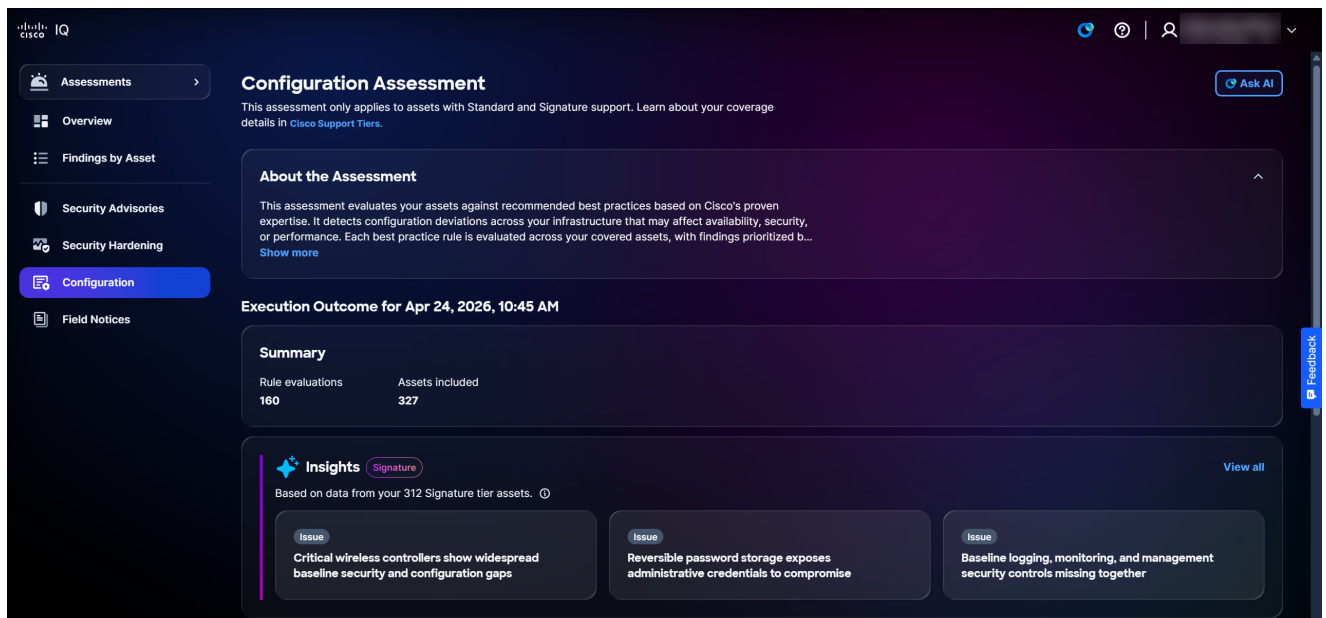
資產和規則資訊

此時會顯示「Asset and Rule Info」頁面，其中包含以下資訊：

- 關於資產:提供資產的詳細資訊，例如產品ID、產品型別、IP地址、序列號、軟體版本、位置和支援層
- 關於規則:提供規則的詳細資訊，例如Severity、Category和Software type

檢視見解

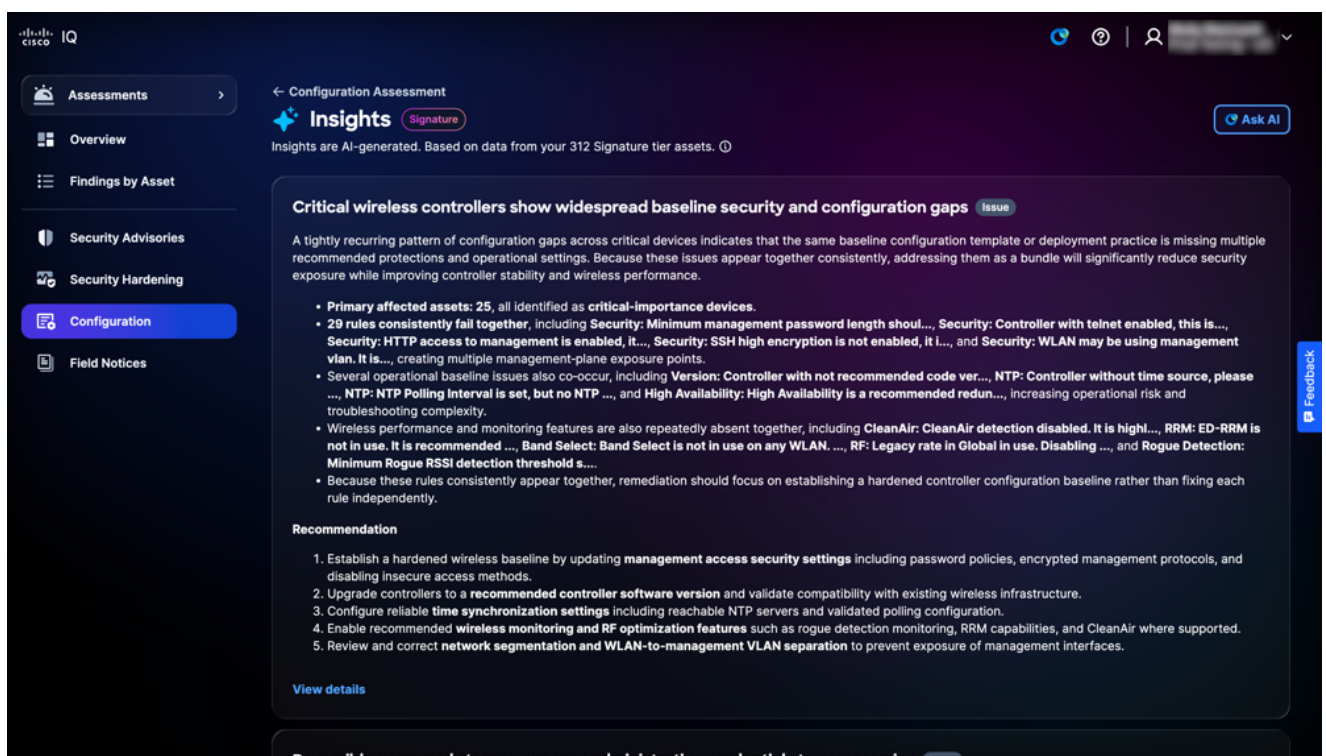
見解由AI生成，用作智慧儀表板，將評估資料合成到按優先順序排列的關鍵卡中，突出顯示了多個結果之間的關鍵配置差異。它使您能夠專注於這些緊急領域，從而高效地解決影響最大的基礎結構風險。它還通過確定您的基礎設施在哪些領域的表現以及根據最佳實踐來突出優勢。



Insights

要檢視見解詳細資訊，請執行以下操作：

1. 在「見解」面板中，按一下檢視全部。Insights頁面顯示所有洞察。



深入分析頁面

2. 按一下View details或按一下任意卡。此時將顯示「Insights detail」（深入分析）頁面，其中包含以下資訊：

Configuration Assessment > Insights

Critical wireless controllers show widespread baseline security and configuration gaps

Insights are AI-generated. Based on data from 312 assets with Signature support. ⓘ

[Signature](#) [Ask AI](#)

Details **Source Findings**

Insight

A tightly recurring pattern of configuration gaps across critical devices indicates that the same baseline configuration template or deployment practice is missing multiple recommended protections and operational settings. Because these issues appear together consistently, addressing them as a bundle will significantly reduce security exposure while improving controller stability and wireless performance.

- **Primary affected assets:** 25, all identified as **critical-importance devices**.
- **29 rules consistently fail together**, including **Security: Minimum management password length should be at least 12 characters**, **Security: Controller with telnet enabled, this is insecure**, **Security: HTTP access to management is enabled, it is insecure**, **Security: SSH high encryption is not enabled, it is insecure**, and **Security: WLAN may be using management vlan. It is insecure**, creating multiple management-plane exposure points.
- Several operational baseline issues also co-occur, including **Version: Controller with not recommended code version**, **NTP: Controller without time source, please use NTP**, **NTP: NTP Polling Interval is set, but no NTP server is configured**, and **High Availability: High Availability is a recommended redundancy feature**, increasing operational risk and troubleshooting complexity.
- Wireless performance and monitoring features are also repeatedly absent together, including **CleanAir: CleanAir detection disabled. It is high priority**, **RRM: ED-RRM is not in use. It is recommended**, **Band Select: Band Select is not in use on any WLAN**, **RF: Legacy rate in Global is in use**, **Disabling Rogue Detection: Minimum Rogue RSSI detection threshold should be set**, and **Rogue Detection: Minimum Rogue RSSI detection threshold should be set**.
- Because these rules consistently appear together, remediation should focus on establishing a hardened controller configuration baseline rather than fixing each rule independently.

Recommendation

1. Establish a hardened wireless baseline by updating **management access security settings** including password policies, encrypted management protocols, and disabling insecure access methods.
2. Upgrade controllers to a **recommended controller software version** and validate compatibility with existing wireless infrastructure.
3. Configure reliable **time synchronization settings** including reachable NTP servers and validated polling configuration.
4. Enable recommended **wireless monitoring and RF optimization features** such as rogue detection monitoring, RRM capabilities, and CleanAir where supported.
5. Review and correct **network segmentation and WLAN-to-management VLAN separation** to prevent exposure of management interfaces.

Affected Assets

Q Search Product type Product family Product ID [Filters](#) 25 results [Export](#)

Name	Product ID	Serial Number	IP Address
ASR9901-01	ASR9901-01	ASR9901-01	10.10.10.1
ASR9901-02	ASR9901-02	ASR9901-02	10.10.10.2
ASR9901-03	ASR9901-03	ASR9901-03	10.10.10.3
ASR9901-04	ASR9901-04	ASR9901-04	10.10.10.4
ASR9901-05	ASR9901-05	ASR9901-05	10.10.10.5

深入分析詳細資訊

- **深入分析:**提供摘要，重點介紹通過跨多個調查結果的全面分析確定的重複出現的配置偏差模式，以及您的基礎設施中與最佳實踐一致的卓越領域
 - **建議：**提供可操作的步驟，以修正已確定的配置差距
 - **受影響的資產：**提供已識別配置偏差的特定裝置的清單，這些偏差在Insight部分中定義
3. 按一下Source Findings。Source Findings頁面顯示支援您的洞察的詳細單個調查結果。

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Configuration Assessment > Insights

Critical wireless controllers show widespread baseline security and configuration gaps

Insights are AI-generated. Based on data from 312 assets with Signature support.

DetailsSource Findings

SearchSeverityResult725 resultsExport

Asset	Rule	Severity	Serial Number	Result
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass
...	High Availability: High Availa...	Low	...	Did not pass

源查詢結果

您可以從Severity和Result下拉選單中選擇篩選器，從而篩選表檢視。

 附註：建議和受影響資產是可選的，具體取決於每項見解輸出。

社群字

現場通知可識別重要的非安全相關產品問題，並根據其影響的嚴重性和重要性對其進行組織，從而增強組織管理產品風險的能力。現場通知提供對產品缺陷的可行性見解，通過推薦的升級或變通方法加速緩解，並確保與運營和業務目標保持一致。這增強了產品的可靠性，最佳化了資源分配，並增強了可復原性，以應對企業中不斷變化的產品挑戰。

Assessments

Overview

Findings by Asset

Security Advisories

Security Hardening

Configuration

Field Notices

Field Notices

Ask AI

About the Assessments

Field Notice Assessments

SearchFilters47 resultsExportSaved Filters

Assessment	Severity	Affected Assets	Potentially Affected Assets
FN74350 - Cisco Unified Border ...	Critical	0	24
FN74223 - Some Cisco NCS 540 ...	Critical	0	3
FN74267 - Cisco NCS-55A2 and ...	Critical	0	1
FN74353 - Cisco Network Conve...	High	0	1

社群字

搜尋和篩選現場通知檢視

您可以從下拉選單中選擇篩選器，從而篩選清單檢視。您也可以通過在搜尋欄位中輸入測評名稱來搜尋現場通知測評。

檢視現場通知的評估

要檢視有關現場通知的其他詳細資訊，請按一下評估。將顯示以下評估詳細資訊：

- 關於評估:通過總結評估的目的提供其他詳細資訊
- 現場通知評估:顯示受所選現場通知影響的資產的清單，包括檢測到漏洞的資產

The screenshot displays the Cisco IQ interface for a field notice. The left sidebar contains navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration, and Field Notices (selected). The main content area shows the field notice titled "FN74223 - Some Cisco NCS 540 Series Medium Density Routers May Become Unresponsive After Upgrade to Cisco IOS XR Software Release 7.11.1 or Later - Workaround Provided". Below the title, there is a section "About the assessment" with details on severity (Critical), last updated date (Dec 11, 2024), and bugs. The "Asset Results" section shows a table with 3 results, filtered by "Potentially affected". The table columns include Asset, Result, Product ID, Serial Number, Product Type, Product Family, and Sup po... (Support point). The table lists three devices, all with a "Potentially affected" result and a "Signature" link.

Asset	Result	Product ID	Serial Number	Product Type	Product Family	Sup po...
Device_70_1_...	Potentially affected			Routers	Cisco Network...	Signature
Device_70_1_...	Potentially affected			Routers	Cisco Network...	Signature
Device_70_1_...	Potentially affected			Routers	Cisco Network...	Signature

檢視現場通知的評估

為現場通知的資產結果搜尋和篩選檢視

您可以從下拉式清單中選擇篩選條件，或按一下Filters，然後從可用篩選條件清單中選擇一個選項，藉此篩選清單檢視。您也可以通過在搜尋欄位中輸入資產名稱來搜尋資產結果。

 附註：根據螢幕縮放設定，某些濾鏡可能被隱藏。根據您的角色和許可權，可使用不同的過濾器。

匯出現場通知的資產結果

要匯出現場通知的評估資產結果，請按一下匯出。如需詳細資訊，請參閱[匯出資訊](#)。

檢視現場通知的資產評估結果

要檢視資產的評估結果詳細資訊，請從「資產評估結果」中按一下資產。此時將顯示資產的評估結果詳細資訊頁面。

您可以檢視以下型別的結果：

- **影響**:表示符合現場通知的所有自動檢查標準且無需其他手動驗證以確認其受到影響的資產
- **可能受到影響**：表示滿足現場通知的所有自動檢查條件，但需要額外手動驗證以確認這些資產是否真正受到影響的資產

Assessments - Security Hardening頁籤下提供以下提示：

- 思科網路裝置的安全強化最佳實踐是什麼？
- 如何強化Cisco IOS XE裝置？
- 列出路由器和交換機的關鍵安全強化步驟。
- 推薦用於思科裝置的基線強化設定是什麼？
- 有多少資產違反了安全強化最佳實踐？

本地身份驗證

帳戶管理員應使用以下憑據成功登入到VA:

- 預設使用者名：admin
- 預設密碼：在VA安裝過程中設定的密碼；有關詳細資訊，請參閱入門指南
- 預設帳戶上下文:Default-Customer

登入後，預設使用者「admin」和帳戶名稱「Default-Customer」將顯示在首頁上。

設定本地管理員安全

您可以通過首頁中的使用者配置檔案選單更改密碼和設定安全問題。

鎖定設定

部署期間可配置以下帳戶鎖定設定：

- 鎖定狀態：啟用或禁用帳戶鎖定功能。
- Maximum Login Attempts：設定帳戶鎖定前允許的最大連續失敗嘗試次數(預設值：3;範圍:0-10)。
- 滾動時間窗口：定義跟蹤失敗嘗試的時間段(預設值：15分鐘；範圍:0-60分鐘)。
- Duration：設定達到最大嘗試次數後帳戶保持鎖定狀態的持續時間(預設值：30分鐘；範圍:0-60分鐘)。

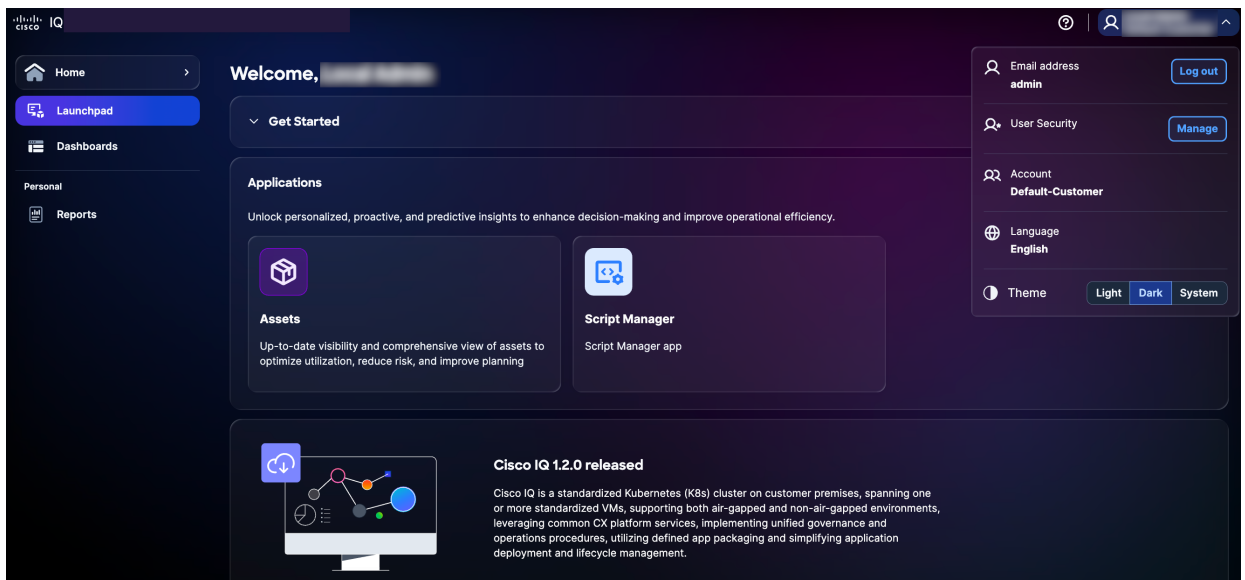
 附註：在15分鐘內，您有三(3)次嘗試輸入正確的密碼。如果所有三(3)次嘗試均失敗，您的帳戶將臨時鎖定30分鐘以保護您的安全。在鎖定期間無法嘗試登入。系統會顯示以下消息：「由於嘗試失敗次數過多，帳戶被鎖定。請稍後再試。」，包括鎖定到期時間。您的帳戶會在30分鐘後自動解鎖，此時您可能會嘗試登入或重置密碼。

設定安全問答

如果您忘記了密碼，安全性問題有助於驗證您的身份。帳戶管理員必須設定五(5)個安全問題的答案才能啟用密碼重置功能。這是一次性設定。

要設定安全問題，請執行以下操作：

1. 在Home頁面中，按一下User Profile圖示。將開啟下拉選單。



使用安全性

2. 按一下「Manage in User security」。系統隨即會顯示User Security頁面。



The screenshot shows the 'User Security' interface in Cisco IQ. The 'Change Password' tab is selected. It includes a list of password requirements: at least 15 characters, at least 2 uppercase characters, at least 2 lowercase characters, at least 2 numeric characters, at least 2 special characters, and no repeating characters. Below these are three input fields for 'Password', 'New password', and 'Confirm password', each with a 'Show' button. A 'Save' button is at the bottom.

User Security

Change Password Security Questions

Change Password
Choose a strong password that contains the following:

- At least 15 characters
- At least 2 uppercase characters
- At least 2 lowercase characters
- At least 2 numeric characters
- At least 2 special characters
- No repeating characters

Password [Show](#)

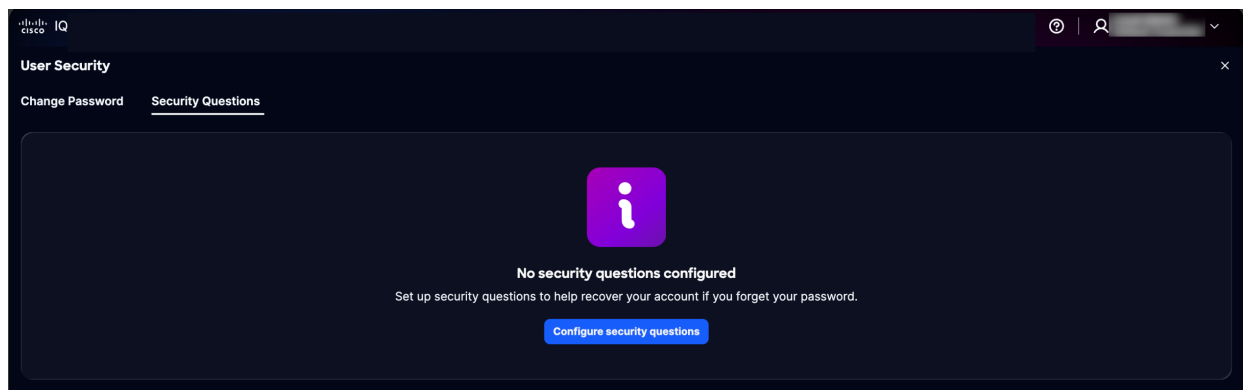
New password [Show](#)

Confirm password [Show](#)

[Save](#)

安全問題

3. 按一下Security Questions以開啟該頁籤。



The screenshot shows the 'User Security' interface in Cisco IQ. The 'Security Questions' tab is selected. It displays a message: 'No security questions configured. Set up security questions to help recover your account if you forget your password.' Below this is a 'Configure security questions' button.

User Security

Change Password **Security Questions**

No security questions configured
Set up security questions to help recover your account if you forget your password.

[Configure security questions](#)

「安全問題」頁籤

4. 按一下配置安全問題。



User Security

[Change Password](#)[Security Questions](#)

Security Questions

Set up security questions to help recover your account if you forget your password. You must answer all questions.

Question 1 *

Select a security question

Answer *

Question 2 *

Select a security question

Answer *

Question 3 *

Select a security question

Answer *

Question 4 *

Select a security question

Answer *

Question 5 *

Select a security question

Answer *

配置安全問題

- 從下拉選單中選擇任意五(5)個安全問題。
- 輸入每個問題的回答。
- 按一下「Save」。



附註：答案不區分大小寫，例如，「SMITH」和「smith」被視為相同。忽略多餘的空格，這意味著「Smith」和「Smith」會得到相同的處理。請記住您輸入答案的方式（例如，全名與暱稱）。使用多年後您會記住的簡單答案。選擇答案不會隨時間而變化的問題。



附註：如果需要，您可以稍後更新您的答案。當您更新答案時，以前的所有答案都將被替換，因此您必須再次提供所有五(5)個問題的答案，而不僅僅是您要更改的問題。

管理密碼

帳戶管理員和本地使用者可以管理Cisco IQ的密碼。

為確保您的帳戶安全，將實施以下密碼策略：

- 重新使用限制：您的新密碼不能與之前五(5)個密碼中的任何一個。此策略適用於「註冊」、「忘記密碼」和「更改密碼」流程。
- 字元變體：在驗證時更改密碼時，新密碼中必須至少有八(8)個字元與當前密碼不同。
- 最小更改間隔：預設情況下，必須等待24小時才能再次更改密碼。如果配置了不同的時間間隔，則在該時間過去之前，您無法更新密碼。
- 密碼過期：密碼每60天過期一次。在到期日期後首次登入時，您需要設定一個新密碼，然後才能訪問系統（如果配置為0，則密碼到期將被禁用）。

必要條件

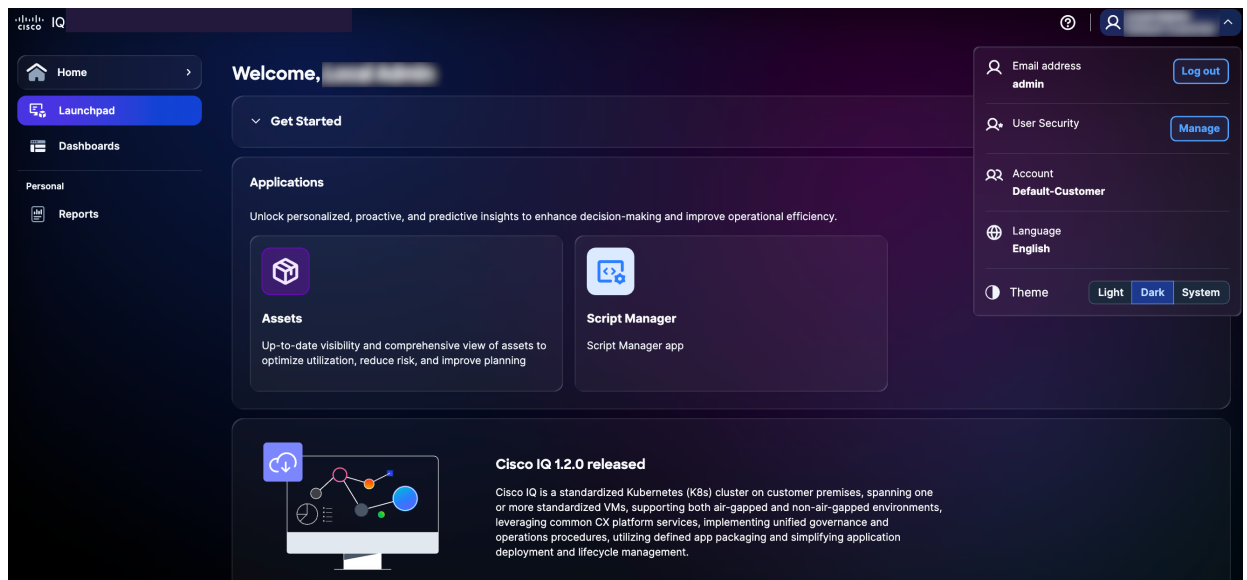
要管理密碼，必須滿足以下條件：

- 您是本地帳戶管理員或使用者
- 您正在使用本地帳戶(不是單一登入(SSO)或外部身份驗證)
- 您已登入Cisco IQ
- 您知道當前密碼

更改密碼

要更改密碼：

1. 在首頁中，按一下您的使用者配置檔案圖示。將開啟下拉選單。



管理使用者安全

2. 按一下「Manage in User security」。系統隨即會顯示User Security頁面。



更改密碼

3. 輸入當前的密碼。
4. 輸入New password。
5. 再次輸入新密碼以確認。
6. 按一下「Save」。

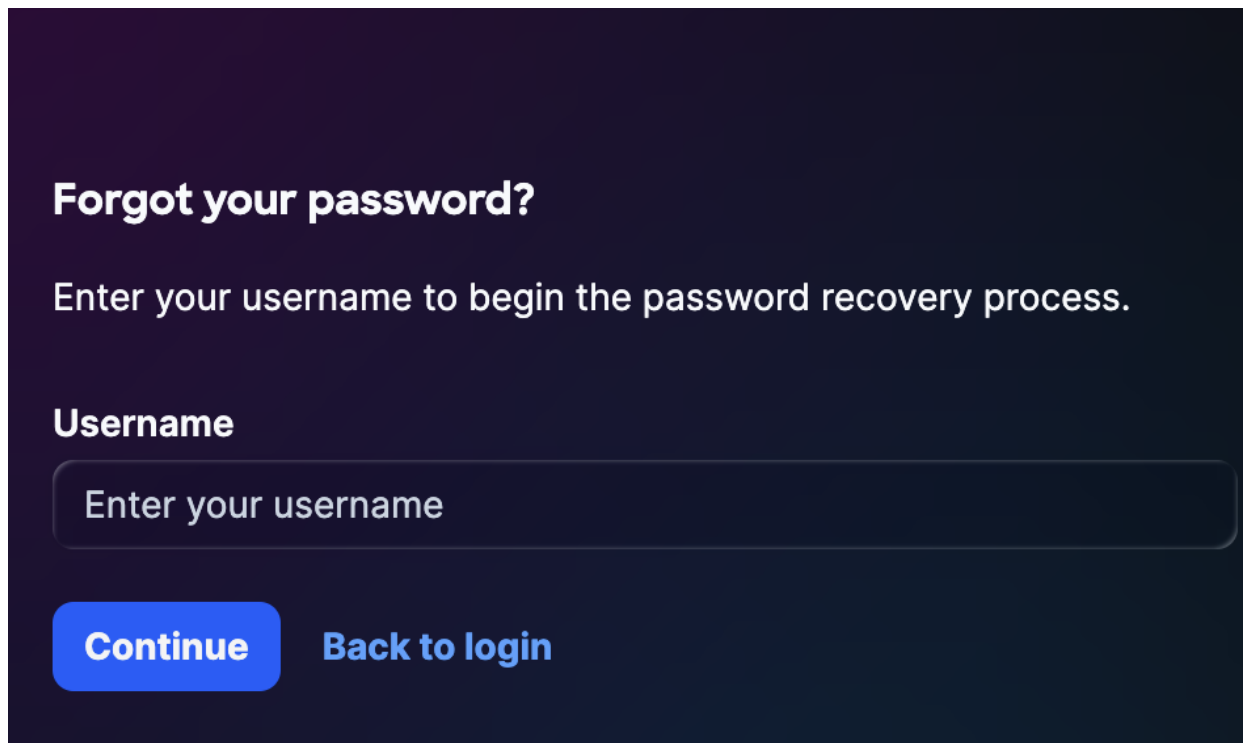
密碼在Cisco IQ系統中更新，包括Cisco IQ VM。

重置忘記的密碼

您可以使用安全問題驗證過程重置密碼。

要重置忘記的密碼：

1. 導航至Cisco IQ VA登入頁面。
2. 按一下「Forgot Password」。



Forgot your password?

Enter your username to begin the password recovery process.

Username

Enter your username

Continue **Back to login**

忘記密碼

3. 輸入Username。
4. 按一下「Continue」（繼續）。Verify Identity頁顯示先前配置的五(5)個問題中的三(3)個隨機安全問題。

Verify Identity

Answer the following security questions to verify your identity.

What city were you born in?

Enter your answer

Show

What is your mother's maiden name?

Enter your answer

Show

What was the name of your elementary school?

Enter your answer

Show

Verify and continue

Back to login

驗證身份

5. 輸入所有三(3)個顯示問題的回答。
6. 按一下「Verify and continue」。如果提交的響應與之前儲存的響應匹配，系統將提示您輸入新密碼。

Set New Password

Choose a strong password that contains the following:

- At least 15 characters
- At least 2 uppercase characters
- At least 2 lowercase characters
- At least 2 numeric characters
- At least 2 special characters
- No repeating characters

New password

Show

Confirm password

Show

Reset password

Back to login

重設密碼

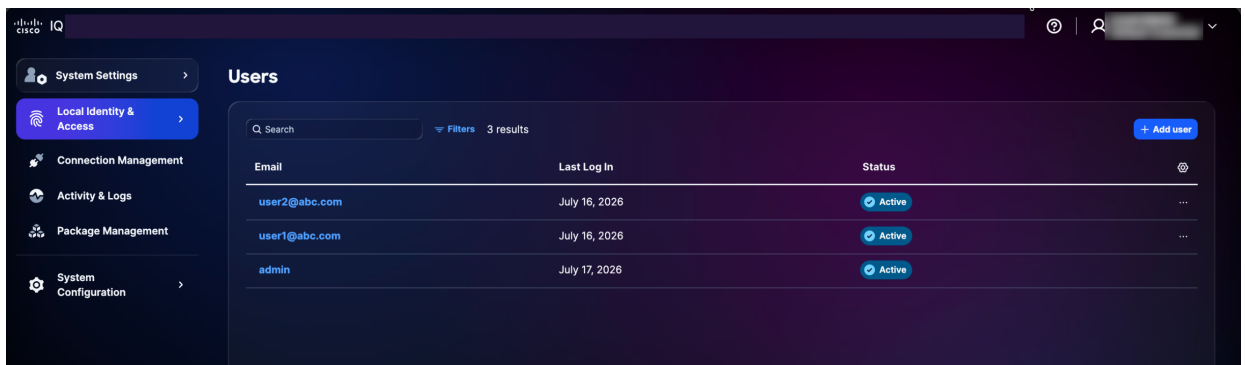
 附註：在15分鐘內，您有三(3)次嘗試輸入正確的密碼。如果所有三(3)次嘗試均失敗，您的帳戶將臨時鎖定30分鐘以保護您的安全。在鎖定期間無法嘗試登入。系統會顯示以下消息：「由於嘗試失敗次數過多，帳戶被鎖定。請稍後再試。」，包括鎖定到期時間。您的帳戶會在30分鐘後自動解鎖，此時您可能會嘗試登入或重置密碼。

- 輸入新密碼。
- 再次輸入密碼以確認。
- 按一下「Submit」。

新增本地使用者

帳戶管理員可以將使用者新增到Cisco IQ帳戶。新增新使用者：

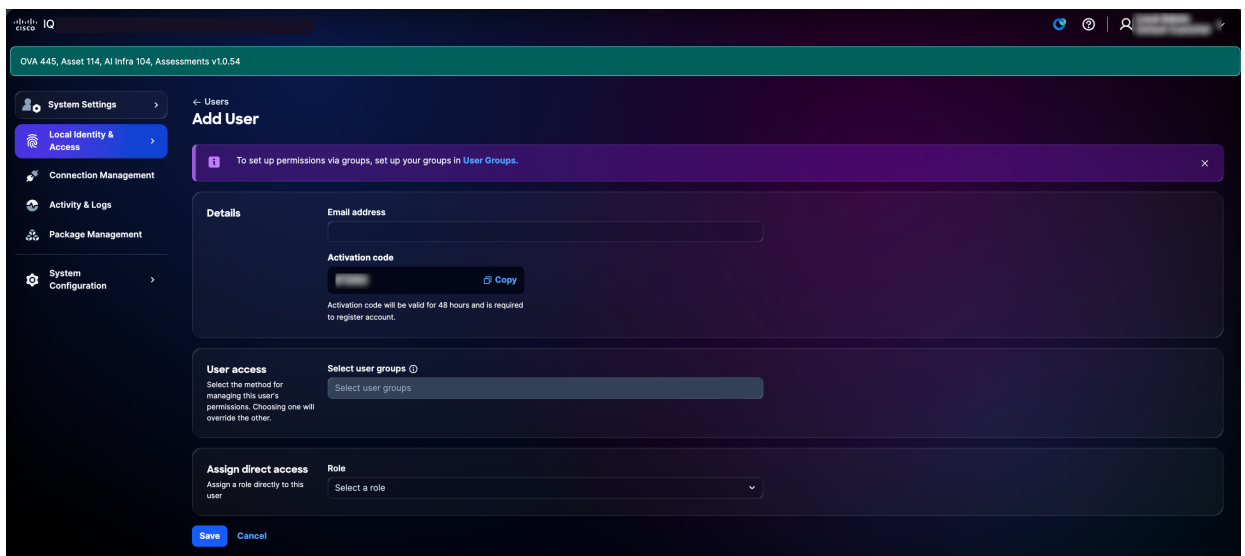
- 導覽至System Settings > Local Identity & Access > Users。系統隨即會顯示Users頁面。它列出所有現有的本地使用者及其狀態。



「使用者」頁

 附註：請勿在不安全的通道上共用啟用代碼。如果代碼丟失或受損，請使用「選單」圖示重新生成新的啟用代碼，這將使上一個啟用代碼失效。啟用碼的有效期為48小時。如果您的代碼過期，請與您的帳戶管理員聯絡以請求新的代碼。

- 按一下「Add users」。系統隨即會顯示Add User頁面。



新增使用者

- 輸入電子郵件地址。
- 輸入啟用代碼。

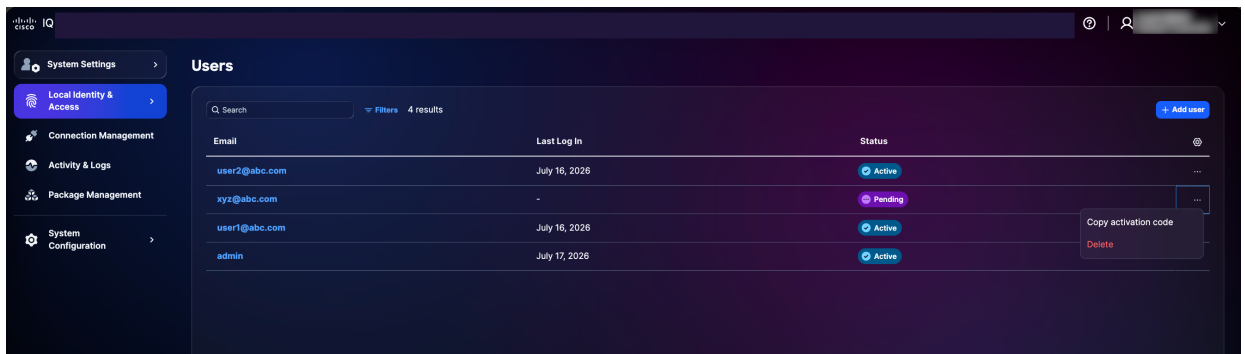
 附註：預設情況下顯示啟用代碼。與使用者共用顯示的啟用碼，因為註冊需要該啟用碼。

- 在User access中，從Select user groups下拉選單中選擇使用者組。

 附註：使用者從選定組繼承訪問許可權。

- 在Assign direct access中，從Role下拉選單中選擇角色。有兩(2)個可用角色：

- 檢視器:檢視和訪問應用程式
 - 帳戶管理員：訪問模組和管理系統設定(系統管理和身份提供程式(IDP)除外)
7. 按一下「Save」。此時將建立新使用者並以待定狀態顯示在使用者清單中。
Pending表示使用者尚未完成自啟用。
 8. 在清單中找到新建立的使用者，並確認Status列顯示Pending。
 9. 按一下新建立的使用者旁邊的More Options圖示。



複製啟用代碼

10. 從下拉選單中選擇Copy activation code。啟用碼將複製到剪貼簿。
11. 安全地與使用者共用此代碼（例如，通過安全的內部管道）。啟用碼僅供一次性使用，需要該啟用碼才能完成註冊。

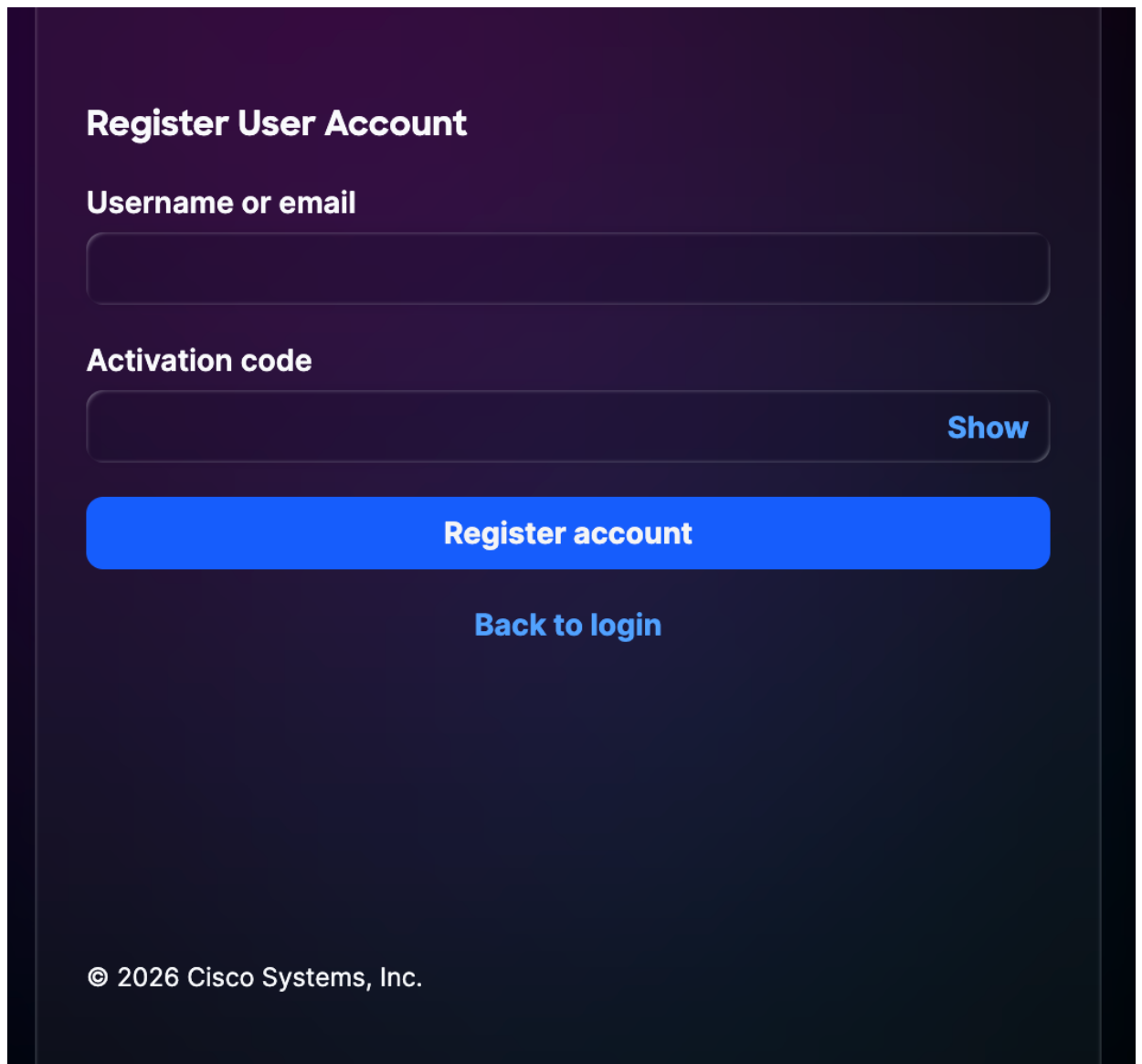
 附註：請勿在不安全的通道上共用啟用代碼。如果代碼丟失或受損，請使用「選單」圖示重新生成新的啟用代碼，這將使上一個啟用代碼失效。啟用碼的有效期為48小時。如果您的代碼過期，請與您的帳戶管理員聯絡以請求新的代碼。

12. 要註銷，請按一下右上角的User Profile圖示，然後選擇Logout。您將返回到Cisco IQ登入頁面。

註冊新使用者帳戶

註冊新使用者帳戶：

1. 在登入頁面上，按一下Register a new user account連結。

A registration form titled "Register User Account" on a dark purple background. It features two input fields: "Username or email" and "Activation code". The "Activation code" field has a "Show" button to its right. Below the fields is a large blue "Register account" button, and below that is a blue "Back to login" link. At the bottom left is the copyright notice "© 2026 Cisco Systems, Inc.".

Register User Account

Username or email

Activation code

Show

Register account

[Back to login](#)

© 2026 Cisco Systems, Inc.

新使用者帳戶

2. 輸入建立使用者時使用的使用者名稱或電子郵件地址(例如user1@abc.com)
3. 輸入由帳戶管理員共用的啟用代碼。
4. 按一下「Register account」。將顯示Set New Password視窗。

Set New Password

Choose a strong password that contains the following:

- At least 15 characters
- At least 2 uppercase characters
- At least 2 lowercase characters
- At least 2 numeric characters
- At least 2 special characters
- No repeating characters

New password

Show

Confirm password

Show

[Reset password](#)

[Back to login](#)

新使用者帳戶密碼

5. 輸入新密碼。
6. 在Confirm password中再次輸入密碼。
7. 首次成功登入時，系統會提示使用者配置五(5)個安全問題。(請參閱[設定安全問題](#))。

管理本地使用者組

使用者組使帳戶管理員可以同時管理多個本地使用者的角色。您可以建立一個組，將角色和使用者組附加到組，並在一個位置更新角色或成員身份，而不是將角色單獨分配給每個使用者。從Local Identity & Access頁面執行所有使用者組管理。

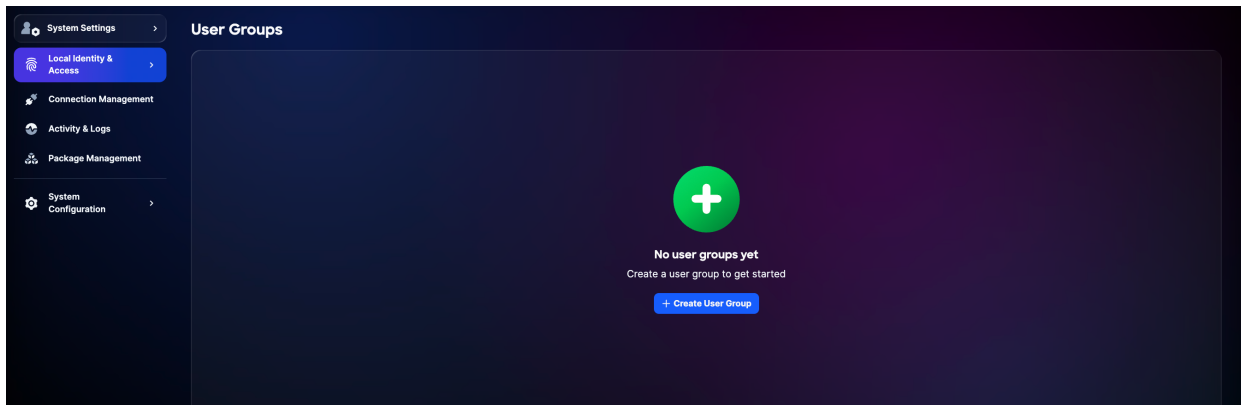
 附註：只有帳戶管理員才能建立、編輯或刪除使用者組。組由現有本地使用者組成；必須先建立使用者，然後才能將其新增到組中。有關詳細資訊，請參閱[新增本地](#)

 [使用者](#)。

建立使用者組

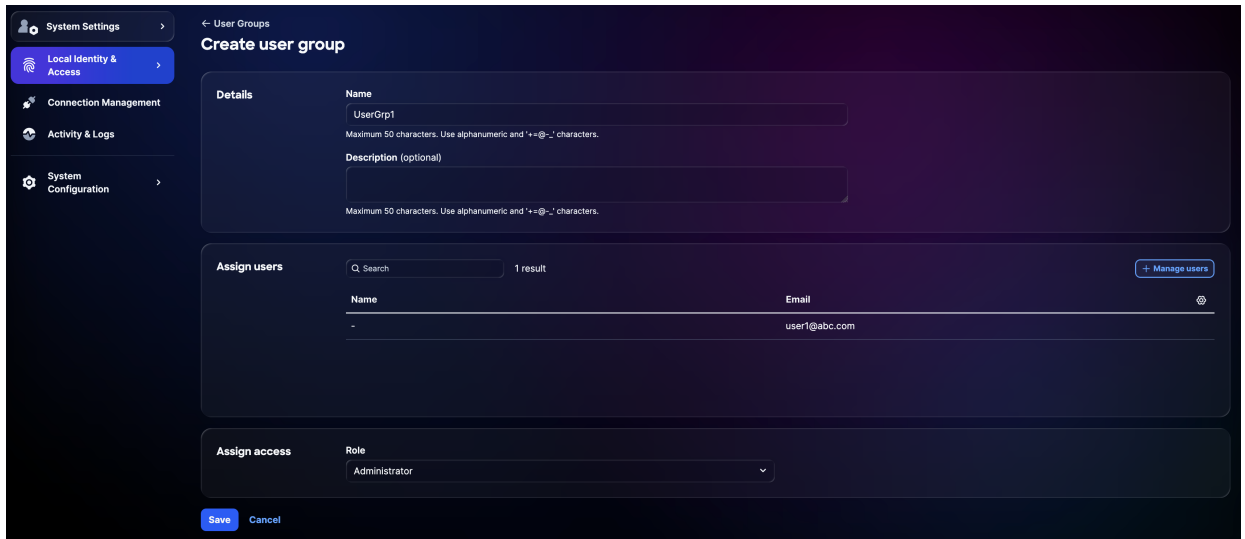
要建立使用者組，請執行以下操作：

1. 在System Settings中選擇Local Identity & Access > User Groups。系統隨即會顯示User Groups頁面。



使用者群組

2. 按一下建立使用者組。將顯示建立使用者組頁。



建立使用者組

3. 完成以下部分：

- 詳細資料
- 名稱:輸入組的唯一名稱 (例如，只讀運算子)
- 說明 (可選):組的簡短說明(最多50個字元；允許使用字母數字和+ = @ - _個字元)

- 分配使用者:搜尋並選擇要新增到組的一個或多個現有本地使用者。附註：要新增尚未列出的使用者，請按一下管理使用者。
- 分配訪問許可權
- 角色:選擇要分配給此組的所有成員的系統角色。以下角色可用：
 - 檢視器:檢視和存取模組（唯讀）
 - 管理員:訪問模組和管理系統設定

4. 按一下「Save」。

新使用者組連同其分配的角色和成員計數一起顯示在User Groups清單中。

編輯使用者組

要編輯使用者組，請執行以下操作：

1. 在User Groups清單中，找到要修改的組。
2. 選擇更多選項圖示> 編輯所需的組。將顯示編輯使用者組頁。

編輯使用者組

3. 進行所需的更改。
4. 按一下「Save」。

更新的組將顯示在「用戶組」清單中。新角色將對組的所有成員生效。

刪除使用者組

要刪除使用者組，請執行以下操作：

1. 在User Groups清單中，找到要刪除的組。
2. 按一下組旁邊的More Options圖示，然後選擇Delete。

Delete user group?

User group will be permanently removed from the platform.

Cancel

Delete user group

刪除使用者組

3. 出現提示時確認刪除。

該組將從User Groups列表中移除。



附註：刪除使用者組將從所有成員中刪除基於組的角色分配。單個使用者帳戶不會被刪除。

配置身份提供程式

登入到VA後，帳戶管理員可以配置各種設定。帳戶管理員可以使用本地管理或IDP配置登入。

SSO的OKTA IDP SAML配置

配置IDP SAML的先決條件

- 本地管理員對Cisco IQ的訪問
- 訪問IDP門戶

SSO的IDP SAML配置

要為SSO配置IDP安全宣告標籤語言(SAML)，請執行以下操作：

1. 導航到您的IDP門戶。

表 2：Cisco IQ屬性

欄位	價值
應用程式名稱	<應用程式名稱>
環境	ESP業務應用程式
應用程式所有者組	IDP設定的所有者
團隊郵件程式	團隊的郵件程式

欄位	價值
對象	非工作人員
入職類別	選擇「New Onboarding」

表 3：SAML配置引數

參數	組態	範例
受眾 (實體ID)	完全限定的域名 (FQDN)	mymanagementhost.mydomain.com
單一登入URL	SAML斷言客戶服務(ACS)終結點	https://mymanagementhost.mydomain.com/saml/acs
名稱ID格式	電子郵件地址	不適用
應用程式使用者名稱	使用者名稱	不適用

5. 配置屬性語句。



附註：IDP屬性更改取決於特定的提供程式和配置。Cisco IDP及其屬性作為示例在下面共用。

- 第一個條目
 - 名稱:使用者名稱
 - 值：user.login
- 第二個條目
 - 名稱:主要電子郵件
 - 值：user.email
- 組屬性語句
 - 名稱:組
 - Filter: (篩選條件：)REGEX
 - 值：.*

6. 配置應用程式中的單一註銷(SLO)設定。

表 4：SLO配置設定

欄位	價值
簽名證書	對於Okta，只有當您選擇啟用SLO時才需要此證書。使用身份提供程式中的下載SP證書來下載簽名證書。將檔案另存為sp-public-key.crt。如需詳細資訊，請參閱 單一註銷組態 。
SP後設資料	僅對於ADFS IDP (而不是Okta)，需要服務提供商(SP)後設資料。
是否要啟用單一註銷	是或否
單一註銷URL	https://mymanagementhost.mydomain.com/saml/logout
SP頒發者 (受眾/實體)	https://mymanagementhost.mydomain.com

欄位

價值

ID或ACS URL)

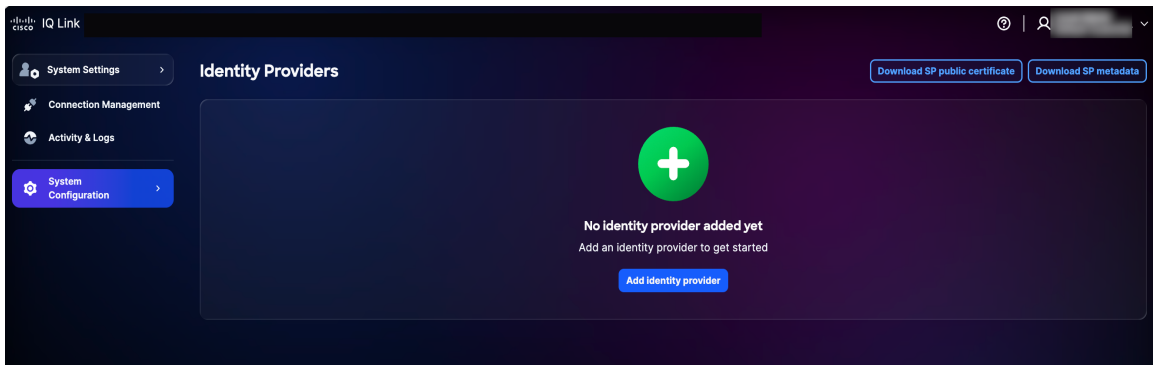
8. 按一下Download圖示下載「IDP Metadata XML」檔案。

9. 根據提供商的要求設定或建立應用程式。

新增Okta IDP

在Cisco IQ中新增IDP:

1. 在System Settings中選擇System Configuration > Identity Providers。系統隨即會顯示Identity Providers頁面。



IDP首頁



 附註：在給定時間只能新增一(1)個IDP。

2. 按一下Add Identity Provider。將顯示Add Identity Provider頁。

System Configuration

← Identity Providers

Add Identity Provider

Identity provider name *

Enter identity provider name

Domains

Enter domain names **Add**

Organization IDP metadata *

Select or drag file to this area to upload

Only one file can be uploaded at 5 MB or less

☐ Enable single log out (SLO)

Save **Cancel**

新增身份提供程式

3. 輸入身份提供程式名稱。
4. 點選Add以將Cisco IQ配置的域名新增到Domain(s)欄位。
5. 在組織IDP後設資料欄位中，拖放或上載從IDP應用程式獲取的SAML後設資料文件。此檔案包含證書詳細資訊和SP實體詳細資訊。
6. (可選) 開啟Enable single logout切換按鈕。您也可以稍後啟用SLO。
7. 按一下「Save」。

角色對映配置

1. 從新增的IDP中，選擇More Options圖示> Map Roles。將顯示對映使用者角色頁。

×

Map identity provider roles to system roles to assign permissions.

Map User Roles

IDP Role	System Role
iq-demo-user	General Account... × ▼
	▼
	▼
	▼
	▼

+ Add identity provider role

Save

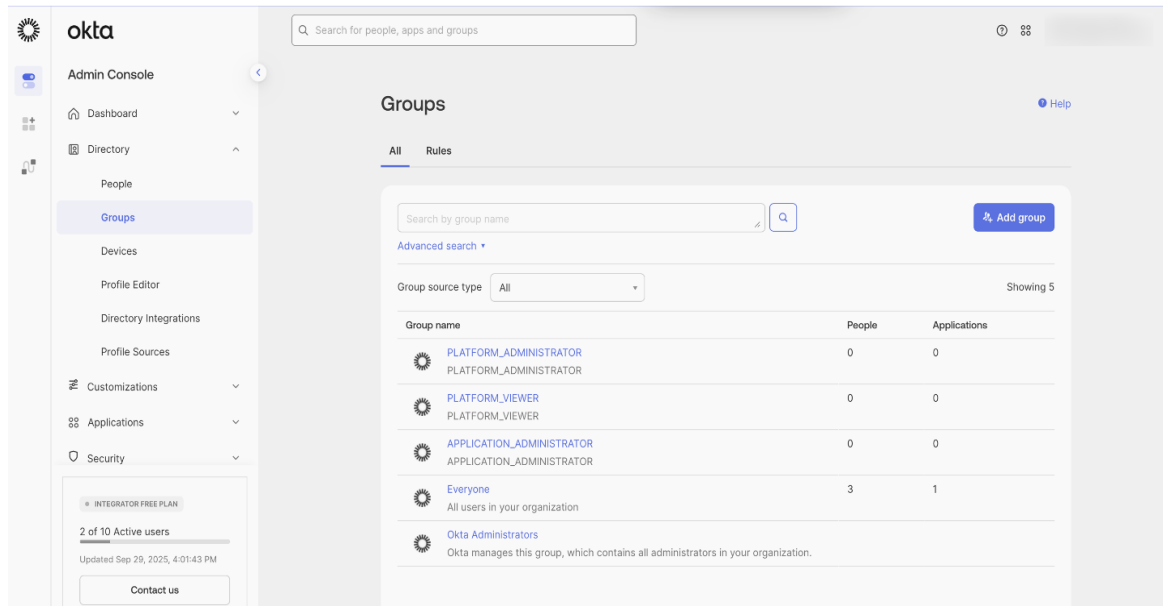
對映使用者角色

2. 為所選系統角色輸入IDP角色。支援以下系統角色：

- 一般帳戶管理員:一般帳戶管理員具有執行產品中所有操作的完全許可權
- 常規帳戶檢視器:常規帳戶檢視器具有只讀訪問許可權



附註：IDP角色是一個開放文本欄位。它必須與組織IDP中配置的組或角色名稱完全匹配。下面共用了一個Okta組的示例。



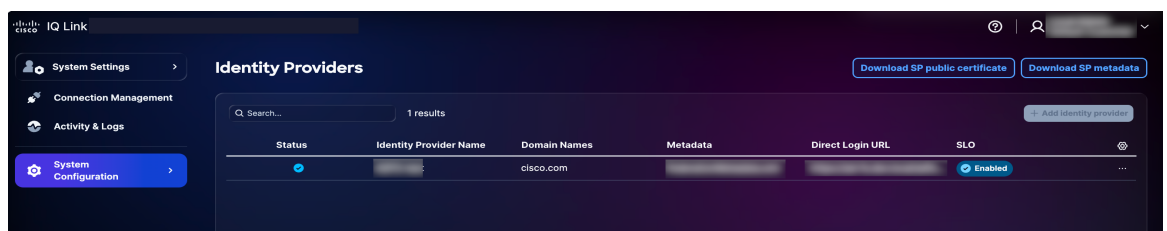
角色對映引用

3. 通過按一下新增身份提供程式角色根據需要對映其他角色。
4. 按一下「Save」。配置後，登入頁面將顯示使用SSO（通過IDP）登入的選項。

單一註銷配置

如果選擇啟用SLO，則必須上傳包含SLO URL的後設資料。您可以通過編輯身份提供程式設定並為啟用單一註銷開啟開關來配置此項。要完成SLO配置，請執行以下操作：

1. 從身份提供程式首頁中，按一下下載SP公共證書。



SP公共證書

2. 將下載的檔案另存為sp-public-key.crt。

3. 導航到您的IDP門戶。
4. 上載在SSO的IDP SAML配置中生成的簽名證書檔案。
5. 輸入SLO URL(例如https://ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com/saml/logout)。
6. 輸入SP頒發者(例如 , ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com)。
7. 按一下「Submit」。
8. 再次下載IDP後設資料檔案。
9. 在「身份提供者」頁面上，選擇新增的IDP的「更多選項」圖示>「編輯」。
10. 開啟Enable single log out(SLO)切換按鈕。
11. 上載新下載的後設資料檔案。
12. 使用以下核對表驗證SSO和SLO功能：

驗證核對表：

- 本地管理員登入成功
- 已配置並調配IDP門戶
- IDP以「成功」狀態新增到思科IQ
- 配置和測試角色對映
- 下載SP後設資料並提取證書
- 如果啟用SLO，則使用實際簽名證書完成SLO配置
- 已成功測試端到端SSO和SLO流

疑難排解IDP問題

下表列出了常見問題和可能的解決方案，以幫助快速識別和解決與IDP狀態、證書錯誤、SSO登入失敗和SLO配置相關的問題：

表 5：疑難排解

問題	解決方案
IDP狀態顯示為「未完成」	驗證角色對映配置
證書錯誤	驗證證書格式和有效性
SSO登入失敗	驗證屬性對映和組分配
SLO未按預期工作	確保正確上傳證書並配置SLO URL

適用於SSO的ADFS IDP SAML配置

本節提供將Microsoft Active Directory(AD)聯合身份驗證服務(FS)配置為Cisco IQ的SAML IDP的指南，支援基於密碼和公鑰基礎設施(PKI)或基於證書的身份驗證。

配置用於SSO的ADFS IDP SAML的先決條件

- 建議使用ADFS 6.0+
- Windows Server 2016 + (推薦2019年)
- 已配置的AD與使用者帳戶整合
- ADFS伺服器上的SSL/TLS證書
- 管理員對Cisco IQ的訪問
- 對ADFS伺服器(Windows Server)的管理訪問
- ADFS伺服器上的PowerShell訪問
- ADFS和Cisco IQ之間的網路連線
- 企業憑證授權單位(CA) (已安裝或可連線)
- 域管理員或企業管理員許可權 (僅適用於PKI)
- ADFS伺服器配置詳細資訊 (如下表中所列)

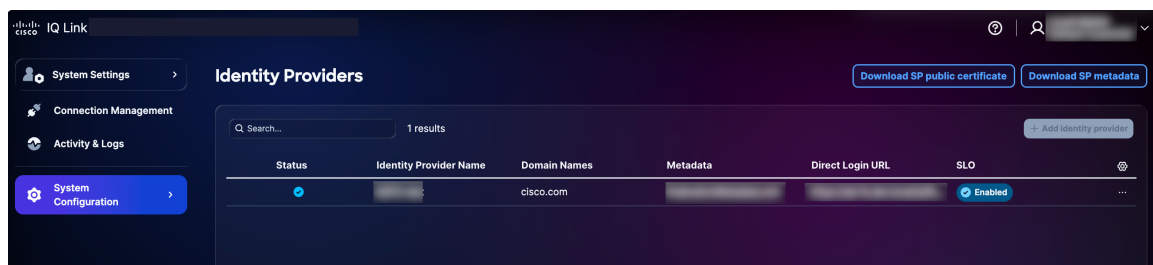
表 6：身份驗證流概述

專案	說明	範例
Cisco IQ FQDN	使用者部署主機名	<Your-CIQ-FQDN>例如 dev35-23.cx-xxx- xxx.cisco.com
ADFS伺服器URL	使用者ADFS伺服器地址	https://<Your-ADFS- HOSTNAME>例如 https://ad-fs.dev.local
公司域	電子郵件域	<您的域>
AD組	Active Directory組域名 (DN)	CN=Role - CXIQ開發人員 OU=Groups , DC=dev , DC=local
CA名稱(PKI)	企業CA名稱	<Your-CA-Name>
憑證驗證連線埠(PKI)	ADFS備用TLS埠	49443
SSL證書指紋	ADFS伺服器SSL證書	<YOUR-SSL-CERT- THUMBPRINT>

配置基本ADFS SAML

要配置ADFS，請執行以下操作：

1. 在System Settings中選擇System Configuration > Identity Providers。系統隨即會顯示Identity Providers頁面。



下載選項

2. 按一下下載SP公共證書和下載SP後設資料以下載這些檔案。
3. 將service-provider-metadata.xml和service-provider-certificate.crt檔案複製並儲存到ADFS伺服器(例如，C:\)。
4. 登入到ADFS伺服器。
5. 在ADFS Management選單中，按一下信賴方信任。
6. 在信賴方信任選單中，按一下新增信賴方信任。將開啟新嚮導。
7. 按一下Claims Aware單選按鈕。
8. 按一下「Start」以繼續設定。
9. 按一下Import data about the relisting party from a file，從作為步驟3一部分儲存的檔案中獲取詳細資訊。
10. 按一下Browse選擇服務提供商後設資料檔案並完成檔案上傳。
11. 按「Next」(下一步)。
12. 輸入顯示名稱 (例如「Cisco IQ」)，新增任何相關註釋，然後點選下一步。
13. 在「Choose Access Control Policy」頁面上，按一下Permit everyone (或您的組織的安全配置所需的策略)。
14. 按一下其餘螢幕中的下一步。
15. 按一下關閉完成信賴方信任配置。



附註：除非您的ADFS伺服器具有註冊的多因素身份驗證(MFA)介面卡(例如

Azure MFA , 已設定時間型一次性密碼(TOTP)。

如果在未配置MFA提供程式的情況下啟用此策略，則ADFS會對使用者進行身份驗證，但最終會拒絕狀態為urn:oasis:names:tc:SAML:2.0:status:RequestDenied的請求。由於SAML響應不包含斷言，因此外掛會失敗並報告「缺少電子郵件」錯誤。

問題：已選擇「Permit Everyone with MFA」。

因應措施：在PowerShell中，通過運行以下命令檢查當前策略。

```
Get-AdfsRelyingPartyTrust -Name  
“
```

```
”).AccessControlPolicyName
```

To set “Permit everyone” (no MFA requirement), run the following command:

```
Set-AdfsRelyingPartyTrust -TargetName “
```

```
”
```

```
-AccessControlPolicyName “Permit everyone”
```

You can also create the trust through PowerShell:

```
-Add-AdfsRelyingPartyTrust `
```

```
=Name “
```

```
” `
```

```
-Identifier “
```

```
” `
```

```
-SamlEndpoint (New-AdfsSamlEndpoint -Binding POST -Protocol
```

```
SAMLAssertionConsumer -Uri “
```

```
” `
```

```
-AccessControlPolicyName “Permit everyone” `
```

```
-IssuanceAuthorizationRules '=> issue(Type =
```

```
“http://schemas.microsoft.com/authorization/claims/permit”, Value =
```

```
“true”);
```

配置ADFS宣告規則

要配置ADFS宣告規則，請執行以下部分中列出的步驟。

所需索賠

請參閱下表瞭解所需索賠。

表 7：所需索賠

領款申請	目的	來源
電子郵件	使用者識別符號	AD郵件
顯示名稱	使用者的全名	AD顯示名稱
UPN	PKI/證書身份驗證	ADFS通過UPN將客戶端證書對映到AD使用者
名稱ID	SAML主題	從電子郵件轉換
組	基於角色的訪問	AD組成員(MemberOf)

應用報銷申請規則

1. 定義信賴方信任的名稱 (例如「Cisco IQ - Production」) 。

```
$relyingPartyName = "Your-RP-Name"
```

2. 定義宣告規則以將使用者資訊和組成員身份傳送到Cisco IQ。

```
$claimRules = @'
@RuleTemplate = "LdapClaims"
@RuleName = "Send Email and Name"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),
@RuleTemplate = "LdapClaims"
@RuleName = "Send UPN"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"),
query = ";userPrincipalName;{0}", param = c.Value);
@RuleName = "Transform Email to NameID"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "mailto:{0}" );
@RuleName = "Send Group Membership"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/group"),
```

```
query = “;memberOf:{0}”, param = c.Value);  
'@
```

3. 通過運行以下命令應用宣告規則：

```
Set-AdfsRelyingPartyTrust -TargetName $relyingPartyName  
-IssuanceTransformRules $claimRules
```

寫主機「宣告規則配置成功！」 — 前景顏色綠色

警告：每個AD使用者帳戶都必須填充郵件屬性。如果缺少此屬性，則SAML斷言不包含電子郵件宣告，從而導致身份驗證被拒絕。

要更新使用者的電子郵件地址，請執行以下PowerShell命令：

```
Set-ADUser -Identity “  
  
” -EmailAddress  
“  
  
”
```

驗證使用者組

1. 通過運行以下命令設定使用者名稱以檢查使用者的組成員身份：

```
$username = “username”
```

2. 運行以下命令以查詢使用者帳戶：

```
$searcher = [adsisearcher]“(samaccountname=$username)”  
$user = $searcher.FindOne()
```

3. 使用以下命令顯示使用者所屬的組：

```
$user.Properties.memberof
```

輸出範例：

CN=Role - CXIQ Developers , OU=Role Groups , DC=dev , DC=local

配置ADFS以信任SP簽名證書

1. 在ADFS伺服器中，將SP證書匯入TrustedPeople儲存區：

```
Import-Certificate -FilePath "C:-provider-certificate.crt"  
-CertStoreLocation "Cert:"
```

2. 選擇以下選項之一：



附註：SP證書由內部CA頒發，ADFS無法通過標準信任鏈進行驗證。

- 為此信賴方全域性禁用鏈驗證

```
Set-AdfsRelyingPartyTrust `   
-TargetIdentifier "  
  
" `   
-SigningCertificateRevocationCheck None `   
-EncryptionCertificateRevocationCheck None
```

- 如果SP證書由CA頒發（非自簽名），請將頒發的CA證書匯入根證書儲存

```
Import-Certificate -FilePath "C:-ca.cer" -CertStoreLocation  
"Cert:"
```

3. 通過重新啟動ADFS服務應用更改。

重新啟動 — 服務adfssrv

設定PKI/證書身份驗證

本節介紹如何在密碼中新增基於證書（即智慧卡或軟體證書）的身份驗證。如果僅密碼身份驗證足夠，則可以跳過此部分。

安裝AD CS CA角色

要安裝AD證書服務(CS)CA角色，請執行以下操作：

1. 通過運行以下命令，驗證域中是否已存在企業CA:

```
certutil -config - -ping
```

如果命令返回有效響應，則可以跳過本節的其餘部分。您的環境已配置。如果命令指示未找到任何CA，請繼續執行步驟2。

2. 通過運行以下命令安裝CA角色：

```
install-WindowsFeature AD-Certificate -IncludeManagementTools
```

3. 通過運行以下命令配置CA角色：

```
install-AdcsCertificationAuthority `
-CAType EnterpriseRootCA `
-CACommonName "
    " `
-KeyLength 2048 `
-HashAlgorithmName SHA256 `
-CryptoProviderName "RSA#Microsoft Software Key Storage Provider" `
-ValidityPeriod Years `
-ValidityPeriodUnits 10 `
-Force
```

4. 通過運行以下命令驗證安裝：

```
certutil -ca
```

5. 通過運行以下命令確認服務處於活動狀態且可以訪問：

```
certutil -config - -ping
```

配置證書模板

要使用客戶端身份驗證增強型金鑰使用(EKU)配置證書模板，請執行以下操作：

1. 開啟certsrv.msc並展開CA節點。
2. 按一下右鍵Certificate Templates > Manage。
3. 複製使用者模板。



附註：僅當從內建使用者模板頒發的證書包含客戶端身份驗證EKU時，該模板才正常工作或有效。

4. 配置以下頁籤上的設定：

- 一般:在Name欄位中輸入「CIQ User Authentication」，有效期為一(1)年
- 請求處理:從Purpose下拉選單中選擇Signature and encryption，並選中Allow private key to be exported覈取方塊
- 使用者名稱:選擇Build from Active Directory Information，並在Subject和SAN欄位中包含電子郵件

警告：Subject和SAN欄位必須包含使用者的使用者主體名稱(UPN)或匹配AD帳戶的電子郵件。ADFS使用這些欄位將證書對映到AD使用者。

- 延伸:確保應用策略包括「客戶端身份驗證(1.3.6.1.5.7.3.2)」
- 資安：新增域使用者並授予其讀取和註冊許可權

5. 使用以下命令發佈模板：

```
Add-CATemplate -Name "CIQUserAuthentication" -Force
```

註冊使用者證書

1. 以目標使用者身份登入。
2. 通過運行以下命令註冊證書：

```
certreq -enroll -user "CIQUserAuthentication"
```

3. 通過運行以下命令驗證證書安裝：

```
Get-ChildItem Cert:| Where-Object {
```

```
$_.EnhancedKeyUsageList.ObjectId -contains "1.3.6.1.5.5.7.3.2"} | Format-Table Subject,
```

從Windows匯出使用者證書並在客戶端(Mac)上安裝

要將使用者證書從Windows匯出到Mac:

1. 通過運行以下命令從Windows將證書匯出為PFX檔案：

```
$cert = Get-ChildItem Cert:| Where-Object { $_.Subject -like "*"
    *"} }
$password = ConvertTo-SecureString -String "
    " -Force -AsPlainText
Export-PfxCertificate -Cert $cert -FilePath "C:-cert.pfx" -Password $password
```

2. 將user-cert.pfx檔案傳輸到Mac裝置。

3. 通過運行以下命令將證書匯入Mac金鑰鏈：

```
security import user-cert.pfx -k ~/Library/Keychains/login.keychain-db -P "
    "
```



附註：匯入證書後，必須關閉瀏覽器並重新開啟才能對其進行識別。

4. 通過運行以下命令信任Mac上的CA:

```
sudo security add-trusted-cert -d -r trustRoot \
-k /Library/Keychains/System.keychain ca-certificate.cer
```

啟用ADFS證書身份驗證終結點

要啟用ADFS證書身份驗證終結點，請執行以下操作：

1. 通過運行以下命令啟用所需的ADFS證書端點：

```
EEnable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificate
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/2005/certificate/transport
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificate
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificate/transport
```

2. 通過運行以下命令驗證是否已啟用所有端點：

```
Get-AdfsEndpoint | Where-Object { $_.AddressPath -like "*cert*" } | Format-Table AddressPath
```

啟用證書身份驗證作為主要

要啟用證書身份驗證作為主要身份驗證，請執行以下操作：

1. 使用以下命令配置Intranet和Extranet訪問的主要身份驗證提供程式：

```
Set-AdfsGlobalAuthenticationPolicy `
-PrimaryIntranetAuthenticationProvider @(“CertificateAuthentication”, “WindowsAuthentication”)
-PrimaryExtranetAuthenticationProvider @(“CertificateAuthentication”, “FormsAuthentication”)
```

2. 使用以下命令驗證兩個清單是否包括CertificateAuthentication和FormsAuthentication:

```
(Get-AdfsGlobalAuthenticationPolicy).PrimaryIntranetAuthenticationProvider
(Get-AdfsGlobalAuthenticationPolicy).PrimaryExtranetAuthenticationProvider
```

3. 使用以下命令檢查當前TLS客戶端埠配置：

```
Get-AdfsProperties | Select-Object HostName, HttpsPort, TlsClientPort
```

4. 如果未啟用TlsClientPort，49443使用以下命令更新埠並重新啟動ADFS服務：

```
Set-AdfsProperties -TlsClientPort 49443
Restart-Service adfssrv
```

SChannel/TLS修復（對於PKI至關重要）

:49443

正在清理證書儲存 (關鍵)

要清理證書儲存，請執行以下操作：

警告：如果受信任的根儲存區中存在非自簽名證書，Windows SChannel將拒絕所有客戶端證書。這是PKI故障的主要根本原因。

1. 通過運行以下命令識別受信任的根儲存中的非自簽名證書：

```
$bad = Get-ChildItem Cert:| Where-Object { $_.Issuer -ne $_.Subject }
$bad | ForEach-Object { Write-Host "PROBLEM: $($_.Subject) | Issuer: $($_.Issuer)" -ForegroundColorRed }
```

2. 通過運行以下命令，將這些證書移動到中間CA儲存：

```
$bad | Move-Item -Destination Cert:\IntermediateCA
Write-Host "Moved $($bad.Count) cert(s) from Root to Intermediate CA store" -ForegroundColorGreen
```

3. 通過運行以下命令，驗證受信任的根儲存中沒有保留任何非自簽名證書：

```
Get-ChildItem Cert:| Where-Object { $_.Issuer -ne $_.Subject }
```

Channel Registry Fixes (關鍵)

配置SChannel登錄檔設定以確保正確的證書身份驗證：

1. 使用以下命令定義登錄檔路徑變數：

```
$regPath = "HKLM:"
```

2. 使用以下命令應用下表中定義的登錄檔設定：

```
Set-ItemProperty -Path $regPath -Name "ClientAuthTrustMode" -Value 2 -Type DWord
Set-ItemProperty -Path $regPath -Name "SendTrustedIssuerList" -Value 0 -Type DWord
```

表 8：通道登錄檔設定

設定	價值	目的
ClientAuthTrustMode	2	啟用專用CA信任以更正預設驗證路徑。

設定	價值	目的
SendTrustedIssuerList	0	防止伺服器在TLS握手期間傳送完全的受信任頒發者清單。

驗證CA證書儲存

驗證CA證書儲存：



附註：頒發使用者證書的CA證書必須位於SystemCertificates儲存中，以確保正確識別該證書。

1. 使用以下命令定義CA證書的指紋：

```
$caThumbprint = "
"
```

2. 使用以下命令驗證LocalMachinestore*中是否已經存在CA證書：

```
$exists = Test-Path "HKLM:\caThumbprint"
```

如果找不到該證書，請將其匯入到LocalMachine儲存區：

```
if (-not $exists) {
    Import-Certificate -FilePath "C:\YOUR-CA-CERT>.cer" `
        -CertStoreLocation "Cert:"
}
```

重新啟動ADFS伺服器 (必填)

使用以下命令重新啟動ADFS伺服器：

```
Restart-Computer -Force
```



附註：ClientAuthTrustMode登錄檔更改僅在伺服器重新啟動後生效。

匯出ADFS後設資料

您可以使用PowerShell或Web瀏覽器下載ADFS後設資料。

PowerShell

要使用PowerShell匯出ADFS後設資料，請執行以下操作：

1. 在ADFS伺服器上開啟PowerShell。
2. 運行以下命令以下載後設資料檔案。

```
$metadataUrl = (Get-AdfsEndpoint | Where-Object {$_.Protocol -eq "Federation Meta  
Invoke-WebRequest -Uri $metadataUrl.AbsoluteUri -OutFile "C:-metadata.xml"  
Write-Host "ADFS metadata exported to C:-metadata.xml" -ForegroundColor Green
```

運行這些命令後，後設資料檔案將儲存到C:-metadata.xml中。

Web瀏覽器

要使用Web瀏覽器匯出ADFS後設資料，請執行以下操作：

1. 導航至<https://<your-adfs-server>/FederationMetadata/2007-06/FederationMetadata.xml>，將「<your-adfs-server>」替換為ADFS伺服器的主機名。
2. 出現提示時，將後設資料XML檔案儲存到電腦。

在Cisco IQ上配置

要在Cisco IQ上配置：

1. 將ads-metadatas.xml傳輸到您的工作站。
2. 在Cisco IQ中，導航到System Settings > System Configuration > Identity Providers。
3. 上傳ADFS後設資料檔案以自動提取IDP證書、實體ID和SSO URL。
4. 儲存組態。



附註：如果ADFS執行自動令牌簽名證書滾動更新，您必須重新匯出後設資料檔案並將其上傳到Cisco IQ以確保繼續身份驗證。

新增ADFS IDP

1. 在「身份提供程式」頁上，按一下新增身份提供程式。
2. 輸入身份提供程式名稱。
3. 輸入域(例如，company.com)。
4. (可選) 如果需要，開啟啟用單一註銷切換按鈕。
5. 在Upload IDP Metadata欄位中拖放或上載從IDP應用程式獲取的SAML後設資料檔案。
6. 按一下「Save」。

 附註：狀態顯示為「未完成」，直到角色對映完成；這是預期行為。

配置角色對映

繼續配置角色對映之前，請確保可以從AD中查詢要用於對映的組。要從AD查詢組，請運行以下PowerShell命令：

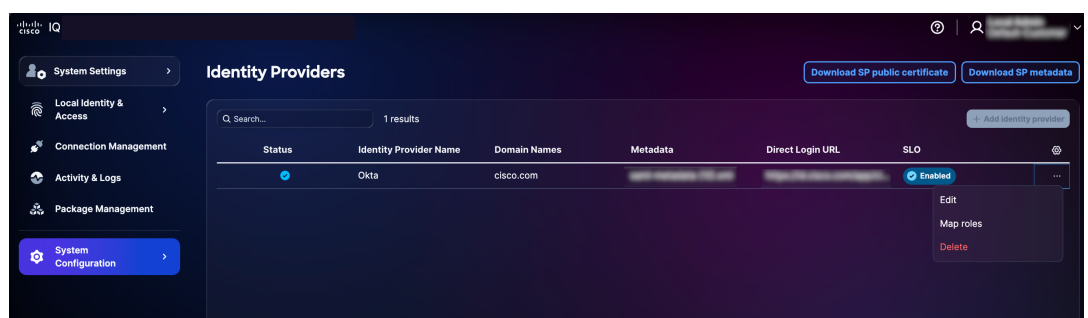
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = "(&(objectClass=group)(cn=Role - CXIQ*))"
$searcher.PropertiesToLoad.Add("distinguishedName") | Out-Null
$searcher.PropertiesToLoad.Add("cn") | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties["distinguishedname"] }
```

系統直接通過輕量級目錄訪問協定(LDAP)查詢AD，無需其他模組。組資訊以完整的可分辨名稱格式返回，例如：

CN=Role - CXIQ Developers，OU=Groups，DC=dev，DC=example，
DC=com CN=Role - CXIQ Viewers，OU=Groups，DC=dev，
DC=example，DC=com

如果未列出所需的組，則必須在帳戶管理員在AD中建立這些組，然後才能完成ADFS角色對映。

要配置角色對映，請執行以下操作：



角色對映

1. 從新增的IDP中，選擇More Options圖示> Map Roles。將顯示對映使用者角色頁。

Cisco IQ Link_IDP ×

Map identity provider roles to system roles to assign permissions.

Map user roles

IDP role	System role
	General Account... × ▼ 🗑️
	General Account... × ▼ 🗑️
	Select option ▼ 🗑️
	Select option ▼ 🗑️
	Select option ▼ 🗑️

[+ Add identity provider role](#)

Save

角色對映

2. 為所選系統角色輸入IDP角色。支援以下系統角色：
 - 一般帳戶管理員:一般帳戶管理員具有執行產品中所有操作的完全許可權。IDP角色 (解析名稱) 是CXIQ管理員。
 - 常規帳戶檢視器:General Account Viewer具有只讀訪問許可權。IDP角色 (解析的名稱) 是CXIQ開發人員和CXIQ檢視器。



附註：使用解析的名稱（例如CXIQ開發人員）而不是完整的DN。

3. 按一下「Save」。狀態更新為Success。

SChannel Client Cert Test

要驗證SChannel是否正確配置為接受客戶端證書，請開啟一個新的PowerShell視窗並執行以下命令：

```
curl.exe -insecure `
-cert "CurrentUser\YOUR-USER-CERT-THUMBPRINT>" `
-v "https://

:49443/adfs/ls/"
```

預期輸出是HTTP響應（例如，重定向或ADFS頁）。如果發生TLS握手錯誤，則連線失敗。

PKI流的端到端瀏覽器測試

在開始對PKI流進行端到端瀏覽器測試之前，請確保使用者證書安裝在MacOS金鑰鏈中(請參閱[在客戶端電腦\(MacOS\)上匯入使用者證書](#))。要測試：

1. 導航到應用程式SAML登入URL。ADFS提供證書和密碼選項。
2. 選擇Certificate Authentication。瀏覽器提示輸入證書。
3. 上傳證書。ADFS對使用者進行身份驗證，使用SAML響應重定向請求，並建立新會話。

對口令流進行端到端瀏覽器測試

開始端到端瀏覽器測試密碼流之前：

1. 導航到應用程式SAML登入URL。ADFS提供證書和密碼選項。
2. 選擇Password/Forms身份驗證。
3. 輸入Username。

4. 輸入Password。
5. 驗證是否成功登入。

 附註：這兩個流必須同時工作。

疑難排解ADFS問題

以下清單概述了常見問題和可能的解決方案，以幫助快速識別和解決與ADFS狀態、證書錯誤、SSO登入失敗和SLO配置相關的問題。

表 9：ADFS問題

問題	症狀/說明	原因/檢查/變通方法和修復程式
未提取的組	登入後沒有角色	◦ 缺少索賠規則:重新運行配置ADFS宣告規則中的說明
解密失敗	在日誌中「無法解密斷言」	檢查ADFS證書配置的配置 ◦ 無效的ACS URL:驗證:https://your-fqdn/saml/acs ◦ Cookie不匹配:檢查瀏覽器Cookie以查詢正確的域
登入回圈	停滯在身份驗證或登入環路中	

用於故障排除的診斷命令

要確保ADFS環境與Cisco IQ之間的成功整合，請使用以下診斷命令。這些命令可幫助驗證後設資料可訪問性、證書配置和端點設定。

- 驗證ADFS後設資料可訪問性:確認ADFS聯合後設資料可訪問且可公開訪問；這是建立初始信任的關鍵步驟

```
curl -k https://
```

```
/FederationMetadata/2007-06/FederationMetadata.xml
```

- 驗證加密憑證:確保正確的加密證書與Cisco IQ信賴方信任相關聯

```
Get-AdfsRelyingPartyTrust -Name "Cisco IQ - Production" |
```


- 檢視SAML終端配置:驗證Cisco IQ信任的SAML端點是否正確配置，以及身份驗證請求和斷言是否路由到預期的URL

```
Get-AdfsRelyingPartyTrust -Name "Cisco IQ - Production" |  
Select-Object SamlEndpoints
```

適用於SSO的Microsoft Entra ID SAML配置

本節提供將Microsoft Entra ID(Entra ID)配置為Cisco IQ的SAML IDP的指南，同時支援基於密碼和PKI或基於證書的身份驗證(CBA)。

配置用於SSO的Entra ID SAML的先決條件

- Entra ID租戶（例如，"ciqtestdev.onmicrosoft.com"）
- 全域性管理員或應用程式管理員角色對Cisco IQ的訪問許可權
- Entra ID（雲）和Cisco IQ之間的連線
- 已安裝或可訪問的企業CA（僅適用於PKI）
- 可從網際網路存取憑證撤銷清單(CRL)發佈點（僅限PKI所需）

表 10：Entra ID伺服器配置

專案	說明	範例
租戶ID	Entra ID租戶識別符號	37352d8f-0ebe-4762-8161-8775ffe897cb
Cisco IQ FQDN	部署主機名	<YOUR-CIQ-FQDN>
IDP實體標識	Entra ID頒發者URL	https://sts.windows.net/<TENANT-ID>/
IDP SSO URL	SAML登入終結點	https://login.microsoftonline.com/<TENANT-ID>/saml2
公司域	使用者的電子郵件域	<您的域>

配置Entra ID SAML應用程式

建立企業應用程式

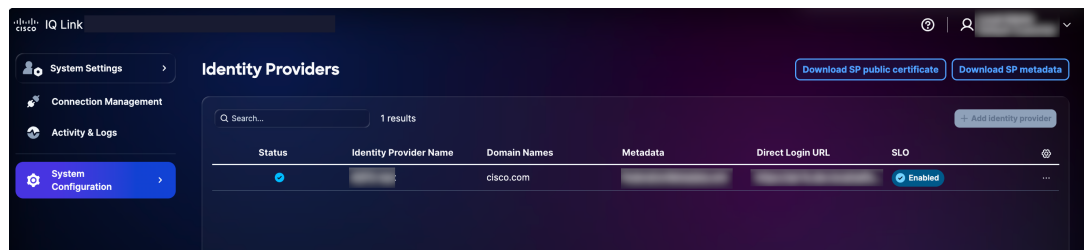
1. 登入到[Microsoft Entra管理中心](#)。

2. 導航到身份 > 應用 > 企業應用。
3. 按一下New application > Create your own application。
4. 輸入名稱 (例如「Cisco IQ」)。
5. 選擇整合您在相簿 (非相簿) 中找不到的所有其他應用程式。
6. 按一下「Create」。

配置SAML單點登入

要配置SAML單點登入，必須上傳SP後設資料檔案。您可以通過從VA執行以下步驟來獲取它：

1. 在System Settings中選擇System Configuration > Identity Providers。系統隨即會顯示Identity Providers頁面。



下載選項

2. 按一下Download SP metadata進行下載。將上載此下載的SP後設資料檔案以完成SAML單點登入配置。
3. 按一下Upload Metadata file按鈕上載SP後設資料檔案。成功上載後，SP後設資料檔案中的資料將自動填充到基於SAML的單一登入螢幕。

您還可以選擇手動輸入這些詳細資訊以配置單點登入設定。要手動配置SAML單點登入，請執行以下操作：

4. 在企業應用程式中，導航到單點登入，然後選擇SAML。
5. 在基本SAML配置部分中，按一下編輯，然後輸入以下內容：
 - 識別符號 (實體ID) :<YOUR-CIQ-FQDN>
 - 回覆URL(ACS URL):https://<YOUR-CIQ-FQDN>/saml/acs
 - 登入URL:https://<YOUR-CIQ-FQDN>/saml/login
 - 註銷URL:https://<YOUR-CIQ-FQDN>/saml/logout
6. 按一下「Save」。



附註：實體ID必須與Cisco IQ用作其SP實體ID的完全匹配。這通常是部署的FQDN。

7. 要配置SAML屬性和宣告，請在屬性和宣告部分按一下編輯。

8. 配置以下宣告：

表 11：所需的SAML宣告

領款申請 唯一使用 者識別符 號 (名稱 ID)	源屬性	名稱空間
電郵地址	user.mail	http://schemas.xmlsoap.org/ws/2005/05/identity/
givenname	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/
姓氏	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/
名稱	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/
組	user.assignedroles	(空 — 清除名稱空間)



附註：對於groups聲明：

- 使用user.assignedroles作為源 — 而不是user.groups
- Namespace欄位必須為空。這可以確保SAML斷言中的屬性名稱只是組，而不是完整的統一資源識別符號(URI)
- 請勿使用user.groups新增重複組宣告，因為這會導致衝突

配置應用程式角色

在App Registration (而不是Enterprise Application) 中配置應用角色；要配置應用程式角色，請執行以下操作：

1. 導航到Identity > Applications > App registrations。
2. 查詢並選擇應用程式。
3. 轉到App roles > Create app role。
4. 對於每個需要的角色，配置以下內容：
 - 顯示名稱:例如，Cisco IQ管理員
 - 允許的成員型別:使用者/組
 - 值：例如，Cisco IQ管理員

- 說明:例如 , Cisco IQ Administrators

5. 按一下「Apply」。



附註：建立符合您的Cisco IQ角色對映要求的角色（例如CXIQ管理員、CXIQ開發人員或CXIQ檢視者）。

使用應用角色而不是組宣告，原因如下：

- 僅雲租戶無法傳送沒有P1或P2許可證的組顯示名稱
- sAMAccountName僅適用於從本地AD同步的組
- 組ID源傳送難以對映的通用唯一識別符號(UUID)
- 應用角色傳送與Cisco IQ角色期望值匹配的精確字串值

將使用者分配給應用程式角色

要將使用者分配給應用程式角色，請執行以下操作：

1. 返回Enterprise Application > Users and groups。
2. 按一下Add user/group。
3. 選擇使用者並分配適當的應用角色。
4. 按一下「Assign」。角色值在SAML宣告組屬性中顯示為可讀字串。

正在下載IDP後設資料和證書

下載IDP後設資料和證書：

1. 從「企業應用程式」中選擇「單一登入」>「SAML簽名證書」。
2. 下載聯合後設資料XML（另存為entra-id-metadata.xml）。

或

下載證書(Base64)以進行手動證書輸入。

3. 注意「設定」(Set)部分中的以下值：

- 登入URL(IDP SSO URL)
- Azure AD識別符號 (IDP實體ID)
- 註銷URL(IDP SLO URL)

 附註：由於Entra ID定期輪換簽名證書，因此必須重新下載後設資料，並在活動證書更改時將其上載到VA，以確保不間斷的SSO服務。

新增內部ID IDP

 附註：在Cisco IQ中新增IDP時，會自動為SAML建立APISIX路由，無需手動配置路由。

新增內部ID IDP:

1. 以帳戶管理員身份登入到VA。
2. 導航到System Settings > System Configuration > Identity Providers。
3. 按一下Add identity provider。
4. 輸入IDP的Name (例如，「Entra ID」)。
5. 輸入域 (例如「ciqtestdev.onmicrosoft.com」或您的公司域)。
6. (可選) 如果需要，開啟啟用單一註銷切換按鈕。
7. 拖放或上載Upload IDP Metadata欄位中的從Entra ID獲取的entra-id-metadata.xml檔案。
8. 按一下「Save」。

 附註：角色對映完成之前，狀態仍為「未完成」；這是預期的行為。

配置角色對映

要配置角色對映，請執行以下操作：

1. 從新增的IDP中，選擇More Options圖示> Map Roles。將顯示對映使用者角色頁。
2. 為每個系統角色輸入IDP角色。支援以下系統角色：

表 12：系統角色

系統角色	IDP角色 (應用角色值)	說明
general_account_administrator	CXIQ管理員	所有操作的完全許可權
general_account_viewer	CXIQ開發人員	只讀訪問
general_account_viewer	CXIQ檢視器	只讀訪問

 附註：完全使用Entra ID中配置的應用程式角色值字串(有關詳細資訊，請參閱[配置應用程式角色](#))

4. 按一下「Save」。狀態更新為Success。

驗證SAML流程 (密碼身份驗證)

要驗證SAML流，請執行以下操作：

1. 在Incognito或Private模式下開啟瀏覽器。
2. 導航至https://<YOUR-CIQ-FQDN>/saml/login。
3. 驗證是否已重新導向至Microsoft登入頁面。
4. 使用您的憑證進行驗證 (如果已設定MFA)。
5. 驗證之後，確認系統是否將您重新導向回/saml/acs並顯示Cisco IQ應用程式。
6. 通過運行以下命令驗證組提取：

```
kubectl -ncxue logs deployment/apisix -since=5m | grep -E "authentication success"
```

預期輸出

已成功對使用者進行SAML 2.0相容身份驗證：user@domain.com全名：
：N/A和1組

提取的組：CXIQ管理員(原始：CXIQ管理員)

提取的組總數：1

配置基於證書的身份驗證

本節介紹如何在密碼旁新增CBA。如果僅密碼身份驗證足夠，則可以跳過此部分。

CBA的必備條件

- 配置了AD CS和企業CA的Windows伺服器 (例如「DEV-ADCS-CA」)
- CA伺服器上的PowerShell管理員訪問許可權
- 證書UPN必須與Entra ID userPrincipalName匹配

- CRL分發點必須可從網際網路訪問

在AD CS上建立證書模板

1. 在CA伺服器上開啟certtmpl.msc。
2. 複製使用者模板並將其命名為「EntraUserCert」。
3. 配置模板：
 - 一般:顯示名稱EntraUserCert，有效期1-2年
 - 請求處理:目的=簽名和加密
 - 使用者名稱:在請求中選擇「供應」
 - 延伸:應用策略必須包括客戶端身份驗證(1.3.6.1.5.5.7.3.2)
 - 資安：向通過身份驗證的使用者授予讀取和註冊許可權
4. 使用以下命令發佈模板：

```
Add-CATemplate -Name "EntraUserCert" -Force
```

請求和頒發使用者證書

1. 使用以下PowerShell指令碼建立證書配置(INF)檔案(例如C:-cert.inf):

```
@”
[Version]
Signature = “`$Windows NT`$”
[NewRequest]
Subject = “CN=

”

KeyLength = 2048
KeySpec = 1
KeyUsage = 0xa0
MachineKeySet = FALSE
ProviderName = “Microsoft RSA SChannel Cryptographic Provider”
RequestType = PKCS10
[RequestAttributes]
CertificateTemplate = EntraUserCert
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.5.5.7.3.2
OID = 1.3.6.1.4.1.311.20.2.2
[Extensions]
2.5.29.17 = “{text}”
_continue_ = “upn=
```

```
        &"
_continue_ = "email=

"
"@ | Out-File -FilePath C:-cert.inf -Encoding ASCII
```

2. 將<USER-UPN>替換為Entra ID UPN(例如
， user@ciqtestdev.onmicrosoft.com)。

3. 要生成證書，請運行以下命令：

```
certreq -new C:-cert.inf C:-cert.csr
```

4. 要向CA提交請求，請運行以下命令：

```
certreq -submit -config "  
  
    \CA-NAME>" C:-cert.csr C:-cert.cer
```

5. 要將證書安裝到CA，請運行以下命令：

```
certreq -accept C:-cert.cer
```

匯出證書

要將使用者證書匯出為PFX檔案（用於客戶端），請運行以下指令碼：

```
$cert = Get-ChildItem Cert: | Where-Object { $_.Subject -like "*"
```



```

        *} }
$password = ConvertTo-SecureString -String “

        ” -Force -AsPlainText
Export-PfxCertificate -Cert $cert -FilePath C:-cert.pfx -Password $password

```

要匯出CA根證書（用於Entra ID），請運行以下指令碼：

```

Get-ChildItem Cert: | Where-Object { $_.Subject -like “*

        *} } |
Select-Object -First 1 | Export-Certificate -FilePath C:-root.cer -Type CERT

```

在客戶端電腦(MacOS)上匯入使用者證書

要匯入使用者證書(PFX)，請運行以下命令：

```

security import /path/to/entra-cert.pfx -k ~/Library/Keychains/login.keychain-db

        ”

```

要匯入CA根證書，請運行以下命令：

```

security import /path/to/ca-root.cer -k ~/Library/Keychains/login.keychain-db

```

在Keychain Access中將CA證書設定為Always Trust:

1. 開啟金鑰鏈訪問。
2. 找到CA證書，然後按一下Get Info。

3. 在Trust下，設定為「Always Trust」。



附註：匯入後，請退出並重新開啟瀏覽器以識別證書。

上傳CA根憑證至Entra ID

1. 登入到[Microsoft Entra管理中心](#)。
2. 導航到Protection > Security > Certificate authorities。
3. 按一下Upload並選擇ca-root.cer檔案。
4. 將其標籤為根CA證書。
5. 輸入CRL分發點URL (必須可公開訪問) 。

在Entra ID身份驗證方法中啟用CBA

1. 導覽至Protection > Authentication methods > Policies。
2. 按一下Certificate-based authentication進行配置。
3. 啟用CBA並新增目標使用者或組。
4. 在「配置」下，將保護級別設定為「單因素身份驗證」。

配置使用者名稱繫結

在CBA配置中，轉到使用者名稱繫結頁籤並設定以下繫結：

- 證書欄位：主體名稱
- 使用者屬性:使用者主體名稱

這會將憑證使用者替代名稱(SAN)中的UPN對應到Entra ID使用者。

檢驗CBA流程

1. 在Incognito或Private模式下開啟瀏覽器。
2. 導航至https://<YOUR-CIQ-FQDN>/saml/login。
3. 在Microsoft登入頁面中，輸入使用者的電子郵件，然後按一下下一步。
4. 選擇Use a certificate or smart card (或者它可以自動提示) 。
5. 當瀏覽器提示選擇證書時，選擇適用的使用者證書。
6. 驗證Entra ID驗證證書、使用SAML響應重定向並建立會話。

 附註：確保選擇正確的客戶端證書。選擇錯誤的證書（例如，其他使用者的證書或過期的證書）會導致身份驗證失敗。

疑難排解Entra ID問題

以下清單概述了常見問題和可能的解決方案，以幫助快速識別和解決與Entra ID SAML配置相關的問題。

表 13：疑難排解

問題	原因	修正
無效的SAML響應 — 缺少電子郵件	SAML斷言沒有NameID或電子郵件屬性	驗證Entra ID宣告配置(有關詳細資訊，請參閱 配置SAML單一登入)。檢查使用者是否已填充郵件屬性。
提取的組總數：0	組宣告未配置或來源錯誤	使用user.assignedroles作為源。確保將該使用者分配給應用角色(有關詳細資訊，請參閱 將使用者分配給應用角色)。
重複組宣告	user.groups和user.assignedroles均處於活動狀態	刪除user.groups宣告。僅保留user.assignedroles。
顯示為UUID的組	源屬性為「組ID」	使用應用程式角色方法(有關詳細資訊，請參閱 配置應用程式角色)。
屬性名稱顯示長URI	名稱空間欄位不為空	清除組宣告設定中的Namespace欄位。
無效的SAML簽名	IdP證書已輪換或不匹配	從Entra ID重新下載後設資料並重新上傳到Cisco IQ。
AADSTS500191	無法從網際網路訪問CRL	將CRL發佈到可公開訪問的URL，或使用自簽名CA方法(有關詳細資訊，請參閱 CRL可達性問題的CRL解決方法)。
未提示證書	證書不在金鑰鏈中、CA不受客戶端信任或未啟用CBA	驗證是否已在MacOS Keychain Access中匯入使用者證書(有關詳細資訊，請參閱 在客戶端電腦上匯入使用者證書 (MacOS))，已使用所需設定在Entra ID中啟用CBA(有關詳細資訊，請參閱 在Entra ID身份驗證方法 中啟用CBA)，並且已重新啟動Chrome以應用更改。
SAML斷言已過期	系統之間的時鐘偏差	增加外掛配置中的

問題	原因	修正
虛擬裝置中的狀態「未完成」	尚未配置角色對映	clock_skew_seconds(預設值為300;使用30000作為實驗)。 完成角色對映(有關詳細資訊，請參閱 配置角色對映)。

可達性問題的CRL解決方法

如果無法從Internet訪問CA的CRL分發點 (在實驗室設定中常見)，請使用無CRL要求的自簽名CA:

```
powershell
# Create self-signed CA
$rootCA = New-SelfSignedCertificate `
-Subject "CN=CIQ-Test-CA" `
-CertStoreLocation "Cert:" `
-KeyUsage CertSign, CRLSign `
-KeyLength 2048 `
-NotAfter (Get-Date).AddYears(5) `
-TextExtension @("2.5.29.19={text}ca=TRUE")
# Create user cert signed by the CA
$userCert = New-SelfSignedCertificate `
-Subject "CN=

", `

-CertStoreLocation "Cert:" `
-Signer $rootCA `
-KeyUsage DigitalSignature `
-KeyLength 2048 `
-NotAfter (Get-Date).AddYears(2) `
-TextExtension @(
"2.5.29.37={text}1.3.6.1.5.5.7.3.2",
"2.5.29.17={text}upn=

&email=

"
)
```

僅將根CA憑證上傳到Entra ID。由於自簽名時未使用思科發現協定

(CDP) , 因此Entra ID不會嘗試CRL驗證。

完成安裝核對表

本節介紹使用Microsoft Entra ID SAML應用程式和可選CBA配置VA的完整設定核對表。

Entra ID SAML應用程式設定

- 在Entra ID中建立企業應用程式 (非庫)
- 通過手動輸入SP後設資料配置基本SAML配置
- 配置屬性和宣告 (包括電子郵件、名稱和使用user.assignedroles的組)
- 在應用程式註冊中建立應用程式角色
- 將使用者分配給應用程式角色
- 下載聯合後設資料XML

Cisco IQ配置

- 通過上載Entra ID後設資料在Cisco IQ中新增IDP
- 配置角色對映以將應用角色值對映到Cisco IQ系統角色
- 驗證基於密碼的登入是否端到端工作
- 驗證是否在日誌中正確提取組

基於證書的身份驗證 (可選)

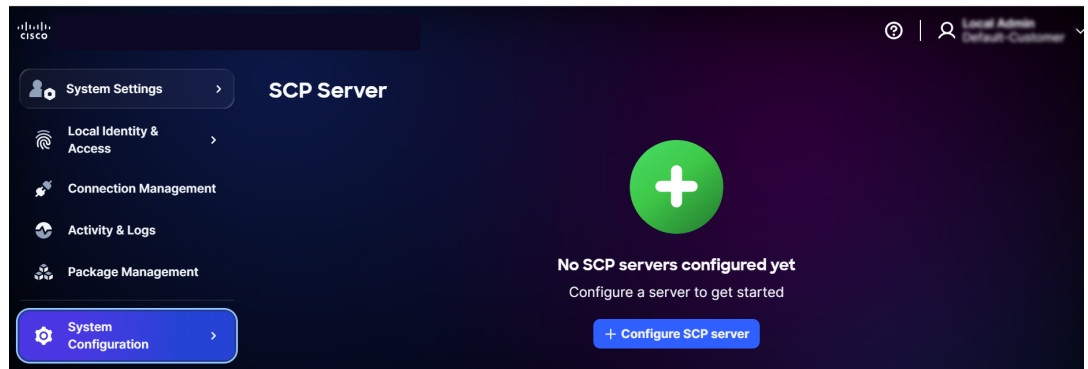
- 使用客戶端身份驗證EKU在AD CS上建立證書模板
- 頒發使用者證書，其中的UPN與Entra ID使用者匹配
- 將使用者證書匯出為PFX檔案並將其安裝在客戶端電腦上
- 信任客戶端電腦上的CA證書
- 將CA根證書上傳到Protection > Certificate authorities下的Entra ID
- 在身份驗證方法中啟用CBA
- 配置使用者名稱繫結 (PrincipalName和userPrincipalName)
- 驗證CBA登入是否端到端工作

新增SCP伺服器

SCP伺服器是匯入對新增、升級或修復Cisco IQ安裝至關重要的升級檔案的先決條件。

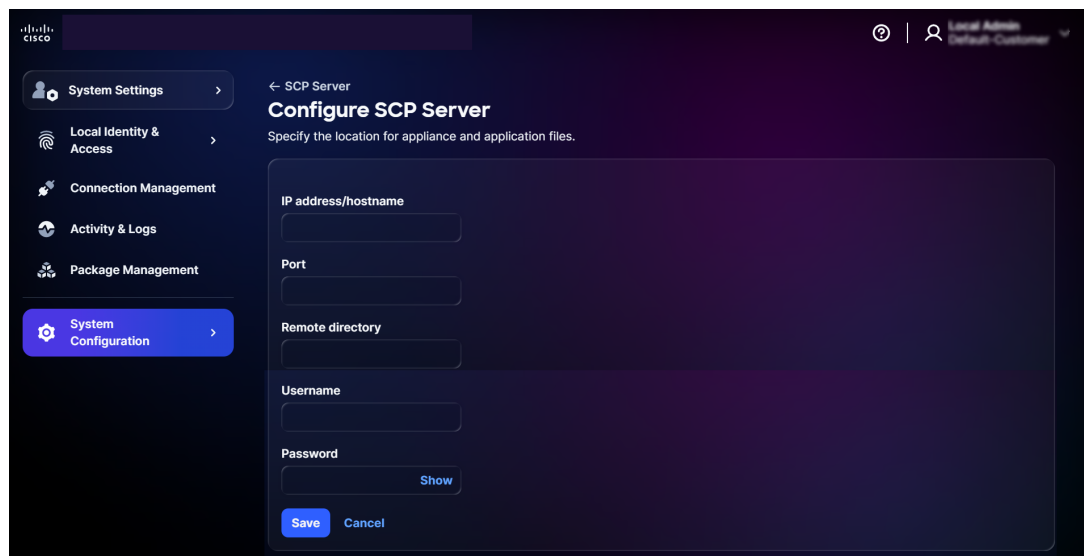
新增SCP伺服器的步驟：

1. 在System Settings中選擇System Configuration > SCP Server。系統隨即會顯示「SCP服務」頁面。



SCP伺服器首頁

2. 按一下Configure SCP server。將顯示配置SCP伺服器頁。



配置SCP伺服器

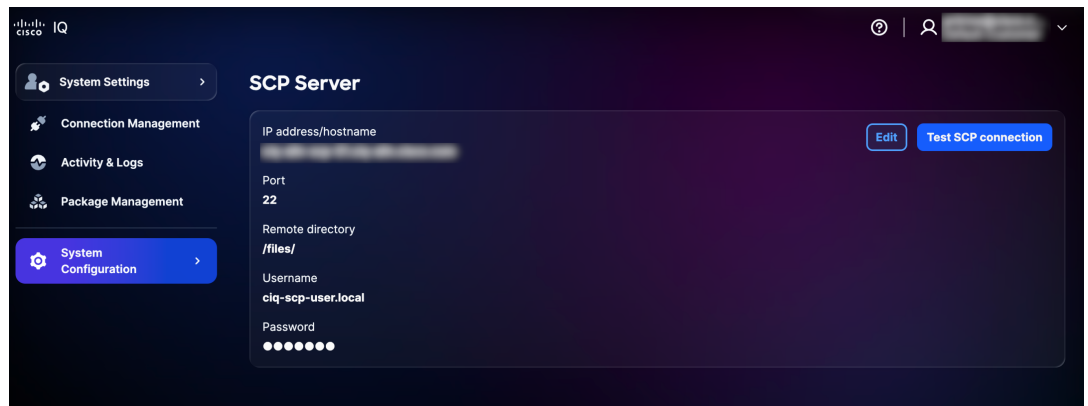
3. 輸入IP地址/主機名。
4. 輸入Port。
5. 輸入遠程目錄。
6. 輸入使用者名。

7. 輸入密碼。
8. 按一下「Save」。系統會顯示確認。

編輯現有SCP伺服器

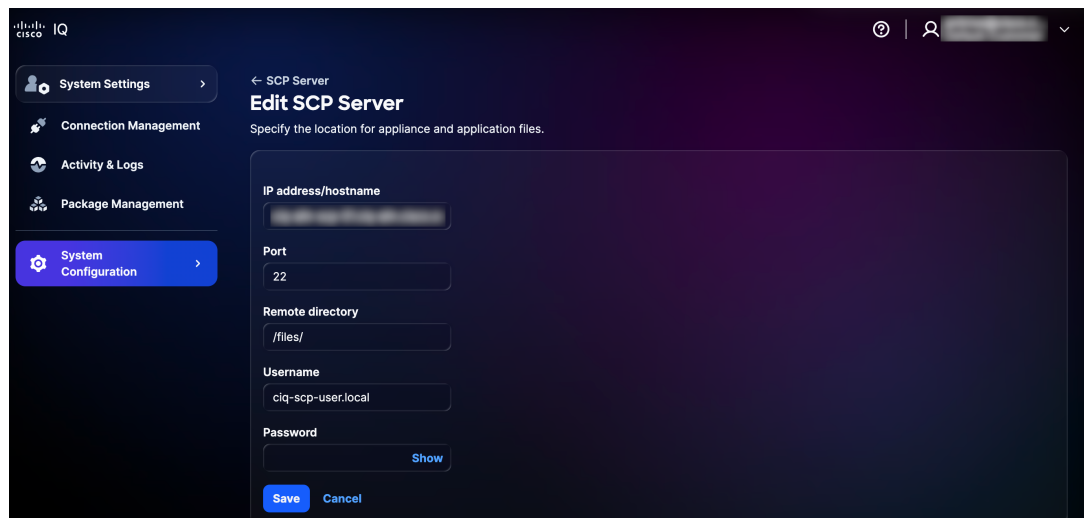
要編輯現有SCP伺服器，請執行以下操作：

1. 導航到SCP Server頁面。



已新增SCP伺服器

2. 按一下Edit所需的現有SCP伺服器。



編輯SCP伺服器

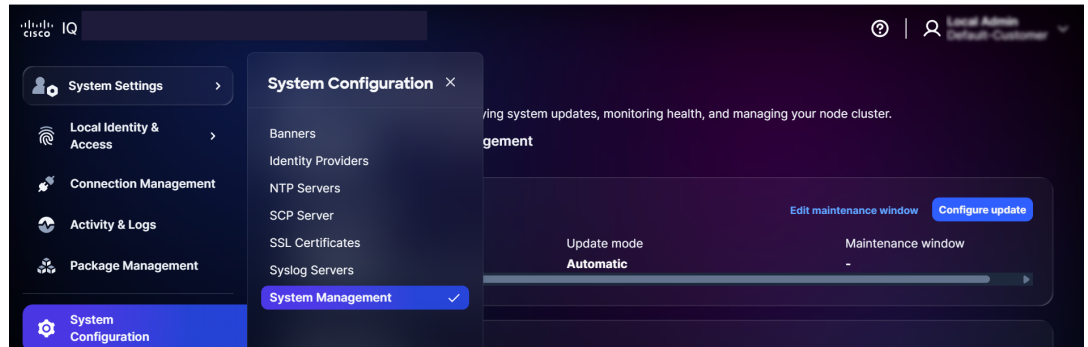
3. 根據需要修改詳細資訊。
4. 按一下「Save」。

系統管理

您可以通過使用者介面升級到最新的Cisco IQ VA版本。您也可以從Cisco IQ Data Connectors頁面進行驗證。

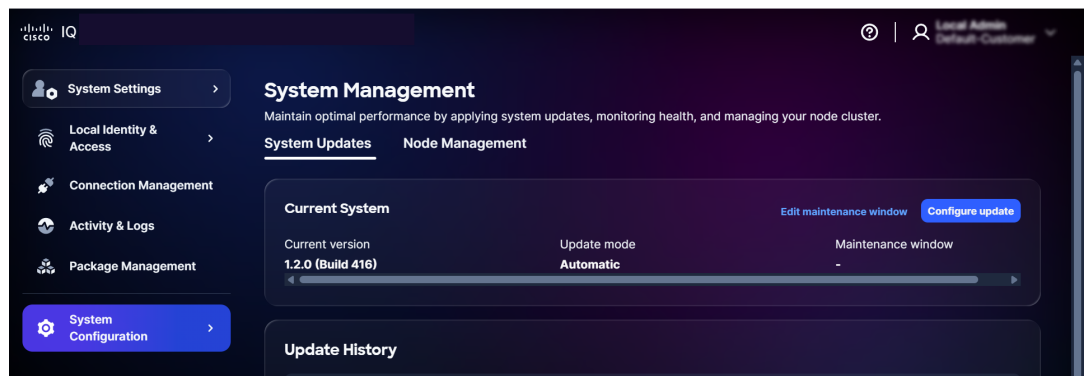
重新計畫系統更新

要重新計畫系統更新，請執行以下操作：



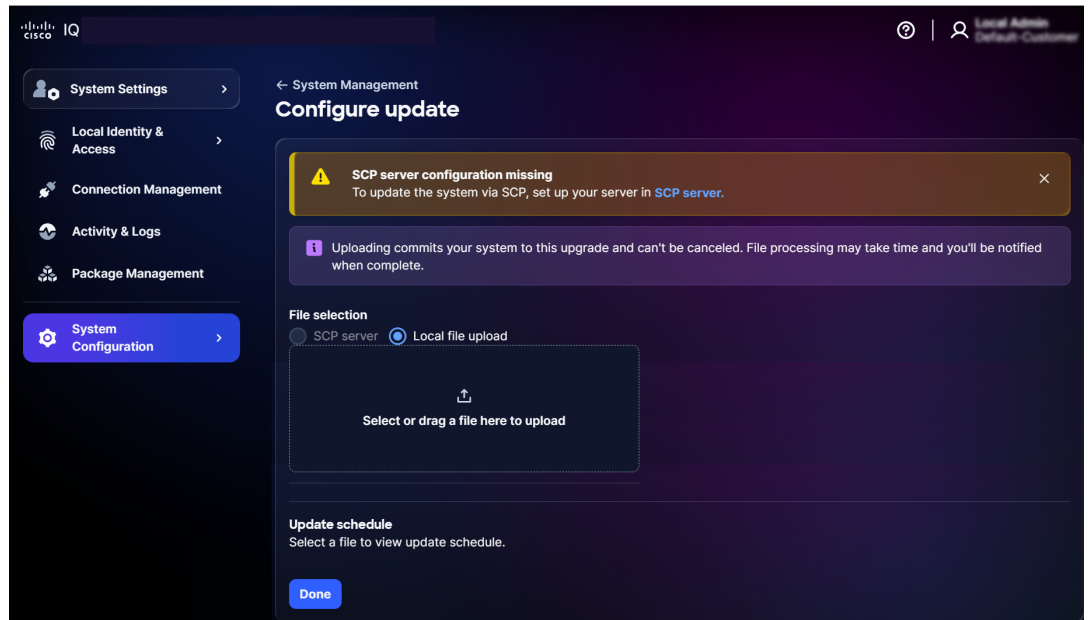
系統管理

1. 在System Settings中選擇System Configuration > System Management。系統隨即會顯示System Management頁面。此頁顯示當前運行的系統版本；如果尚未配置更新，則Update History部分為空。



系統升級

2. 按一下「Configure update」。系統隨即會顯示Configure update頁面。



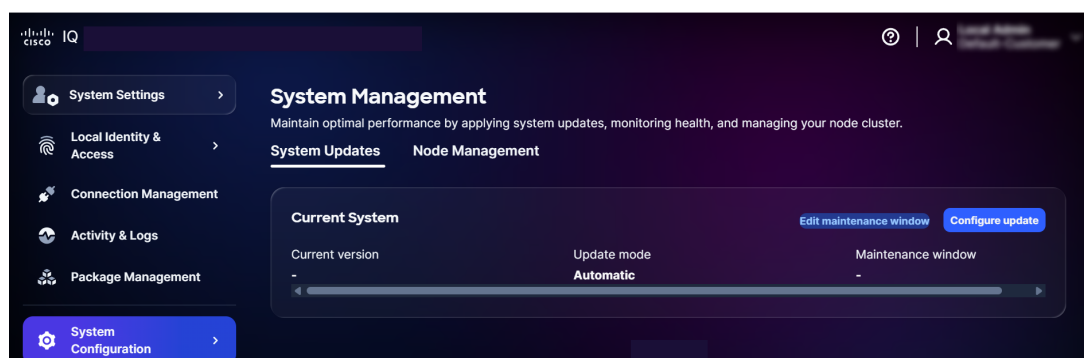
配置升級

3. 選擇Update schedule以計畫其他時間。
4. 等待檔案上傳完成；持續時間取決於捆綁包大小和網路速度。

通過驗證Update Status (更新狀態) 列下顯示的複選標籤圖示來確認更新成功。

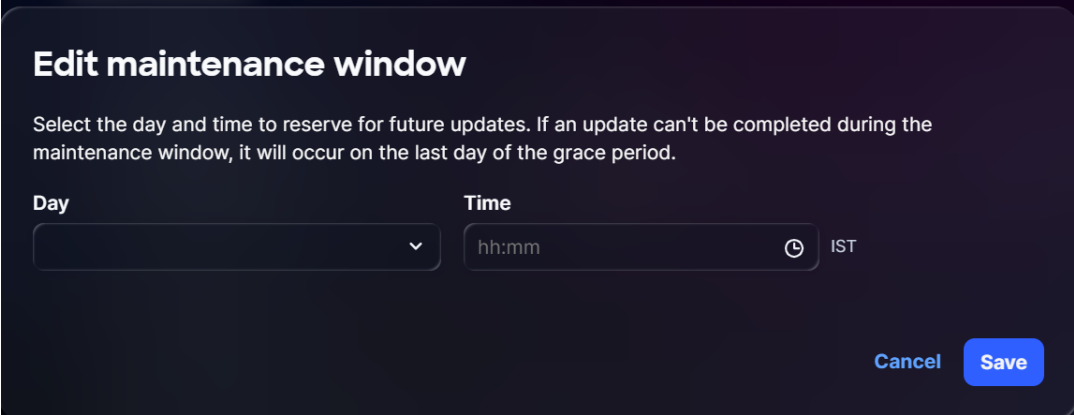
編輯系統升級計畫

您可以為系統升級建立自定義計畫。如果配置了自定義計畫，則升級將在使用者定義的日期進行，前提是升級在最大寬限期內進行。要建立系統升級計畫，請執行以下操作：



編輯維護

1. 在System Management頁面的Current System部分，按一下Edit maintenance。



Edit maintenance window

Select the day and time to reserve for future updates. If an update can't be completed during the maintenance window, it will occur on the last day of the grace period.

Day

Time IST

Cancel Save

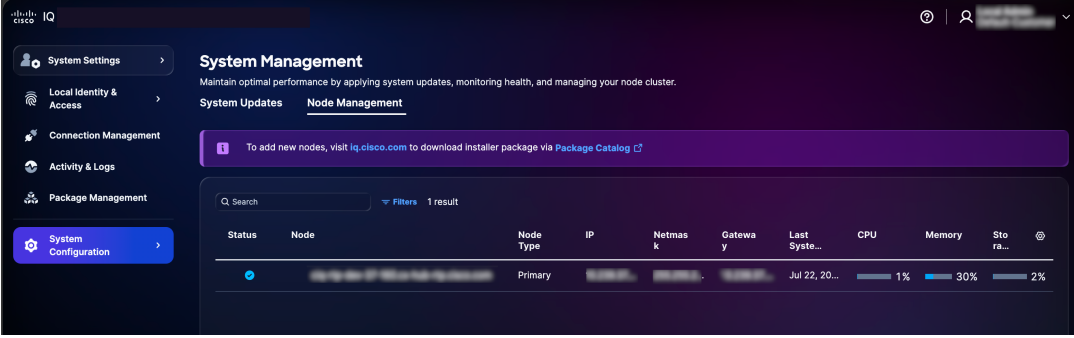
編輯維護視窗

2. 從Day和Time下拉選單中選擇一個選項。
3. 按一下儲存。已成功計畫維護視窗。根據顯示的計畫觸發更新。

 附註：如果未配置升級計畫，對於不重新啟動的升級，系統預設為兩(2)周的寬限期；對於需要重新啟動的升級，系統預設為四(4)周的寬限期。在這些寬限期之後，必須手動執行更新。如果升級失敗，系統將執行最多兩(2)次自動重試。已安排第三次嘗試，但需要手動啟動。

節點管理

1. 導航到System Configuration > System Management > Node Management，以檢視和管理集群中的節點。



Status	Node	Node Type	IP	Netmask	Gateway	Last System...	CPU	Memory	Storage
	10.10.10.10	Primary	10.10.10.10	255.255.255.0	10.10.10.1	Jul 22, 20...	1%	30%	2%

節點管理

2. 節點清單顯示每個節點的狀態、主機名、節點型別、IP地址、網路掩碼、網關和上次同步時間。

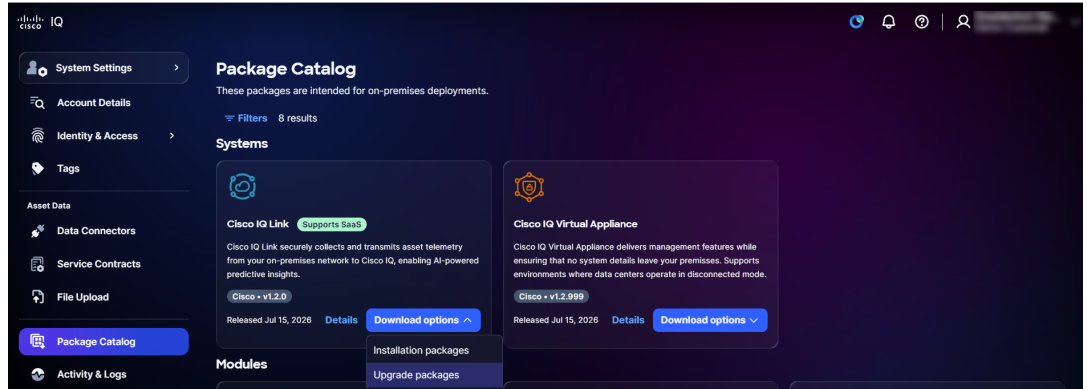
 附註：Status列中的藍色複選標籤表示節點處於活動狀態。

手動升級系統

如果來自Cisco IQ SaaS的自動分發不可用或延遲，您可以直接從Cisco IQ

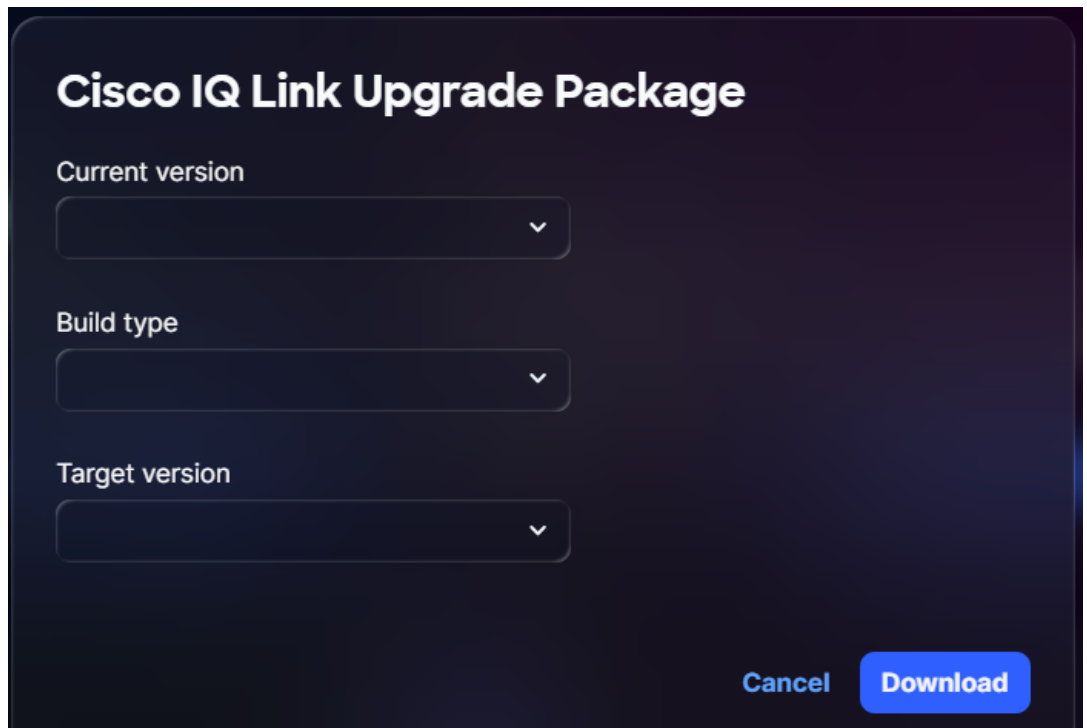
SaaS下載升級捆綁包手動執行系統升級。要手動升級系統，請執行以下操作：

1. 登入到[Cisco IQ SaaS](#)。
2. 導覽至Home > System Settings > Package Catalog。



軟體目錄

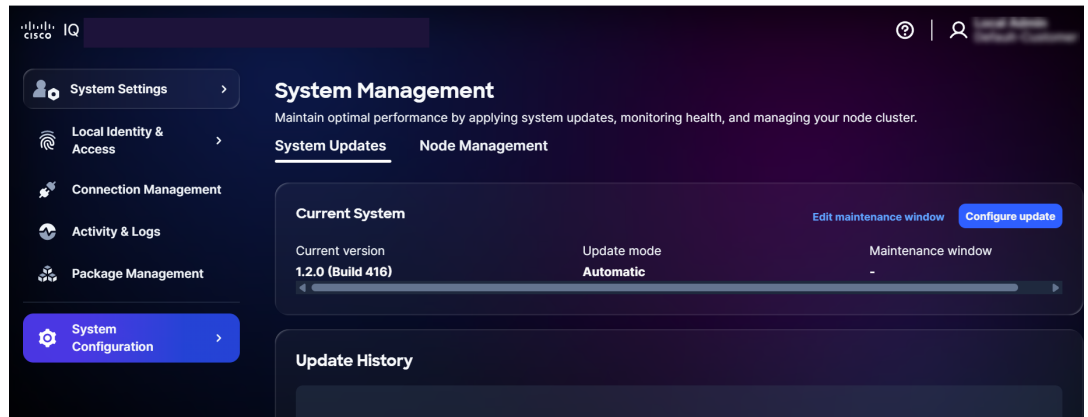
3. 在Cisco IQ Virtual Appliance卡中，按一下Download options > Upgrade packages。



升級包

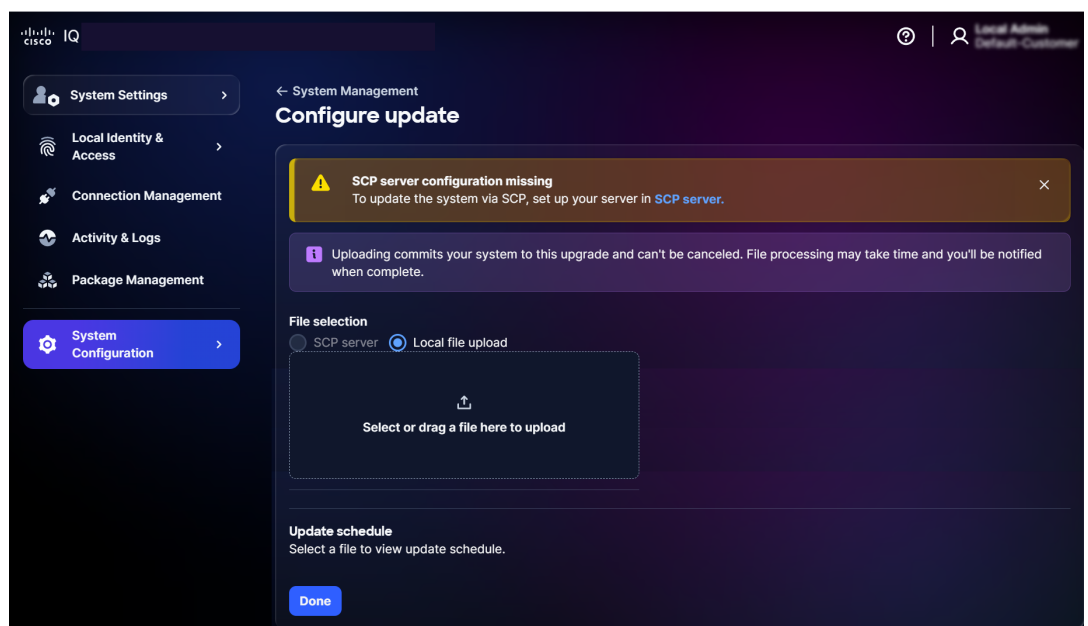
4. 從下拉選單中選擇Current version。
5. 從下拉選單中選擇Build type。
6. 從下拉選單中選擇Target version。

7. 按一下「Download」。下載升級套件組合。
8. 導航至Cisco IQ VA。
9. 在System Settings中選擇System Configuration > System Management。



配置更新

10. 按一下「Configure update」。



本地檔案上傳

11. 按一下「Local file upload」單選按鈕。
12. 選擇下載的升級套件組合檔案或將其拖到上傳欄位中。
13. 等待檔案上傳完成；持續時間取決於捆綁包大小和網路速度。

SSL證書配置

Cisco IQ中預安裝並啟用了預設自簽名證書，但您也可以上傳自定義SSL證

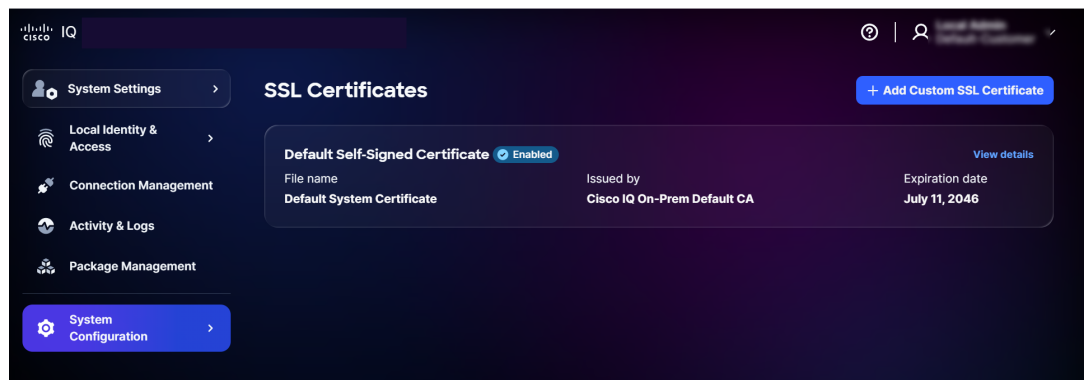
書。啟用自訂SSL憑證時，會將其用於HTTPS連線；如果證書被禁用或刪除，系統會自動恢復為預設證書。無法編輯或刪除預設SSL證書。

 附註：證書的有效期限必須至少為90天。如果證書到到期的剩餘時間少於90天，則將其視為「接近到期」。新增、編輯或刪除SSL證書後，必須按照[完成Okta IDP或ADFS IDP的SLO配置](#)中的說明上傳新的SSL證書。

新增自定義SSL證書

新增自定義SSL證書的步驟：

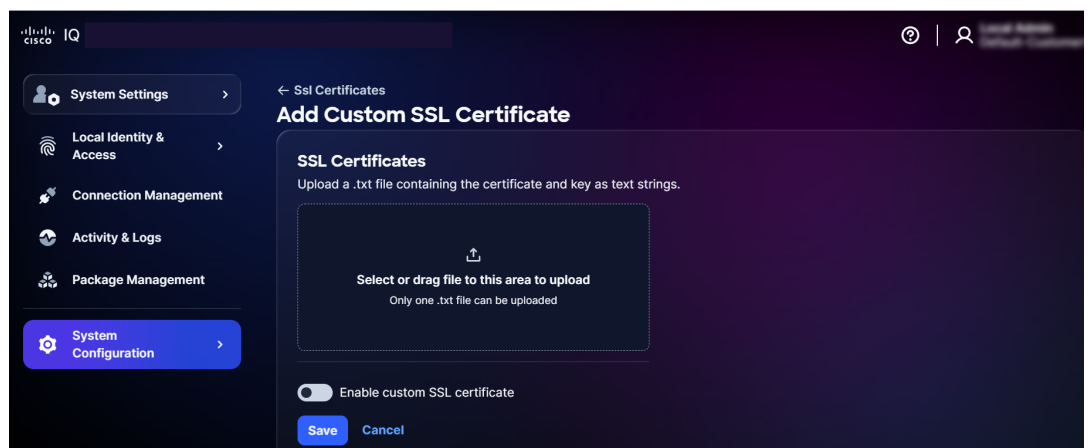
1. 在System Settings中選擇System Configuration > SSL Certificates。將顯示SSL Certificates頁面，其中列出了系統的所有SSL證書。



新增SSL證書

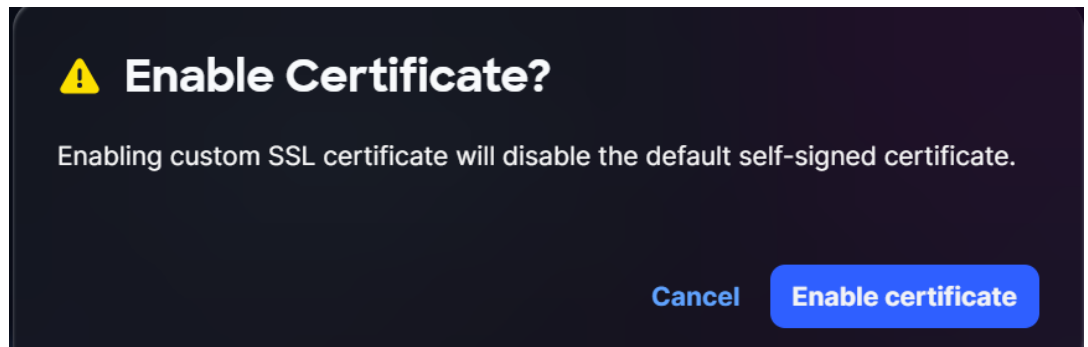
2. 按一下「Add Custom SSL Certificate」。

 附註：上傳包含隱私增強型郵件編碼證書和金鑰作為文本字串的.txt檔案。一次只能上傳一個.txt檔案。檔案必須同時包含證書和私鑰。



上傳SSL憑證

3. 拖放或上傳SSL Certificate部分下的自定義SSL證書。
4. 開啟Enable custom SSL certificate (啟用自定義SSL證書) 切換按鈕。



啟用證書

 附註：如果要上傳證書而不立即啟用證書，請保持關閉狀態。

5. 按一下「Enable certificate」。
6. 按一下「Save」。

自定義SSL證書已啟用且處於活動狀態。預設系統證書將自動停用。

編輯自定義SSL證書

您可以編輯自定義SSL證書以上傳新證書或禁用當前啟用的證書。要編輯：

1. 導航到所需的自定義SSL證書。
2. 選擇更多選項圖示> 編輯。系統隨即會顯示Edit SSL Certificate頁面。
3. 根據需要編輯證書詳細資訊。
4. 按一下「Save」。

刪除自定義SSL證書

警告：可隨時刪除自定義SSL證書，但此操作不可逆；您可以在刪除後隨時上傳新的自定義證書。

刪除：

1. 導航到所需的個人SSL證書。
2. 選擇更多選項圖示> 刪除。
3. 按一下「Delete Certificate」。系統會刪除自訂憑證，並自動重新啟用

預設憑證。

系統日誌伺服器配置

具有帳戶管理員角色的使用者可以配置外部系統日誌伺服器以匯出系統日誌。最多可以配置兩(2)台系統日誌伺服器。

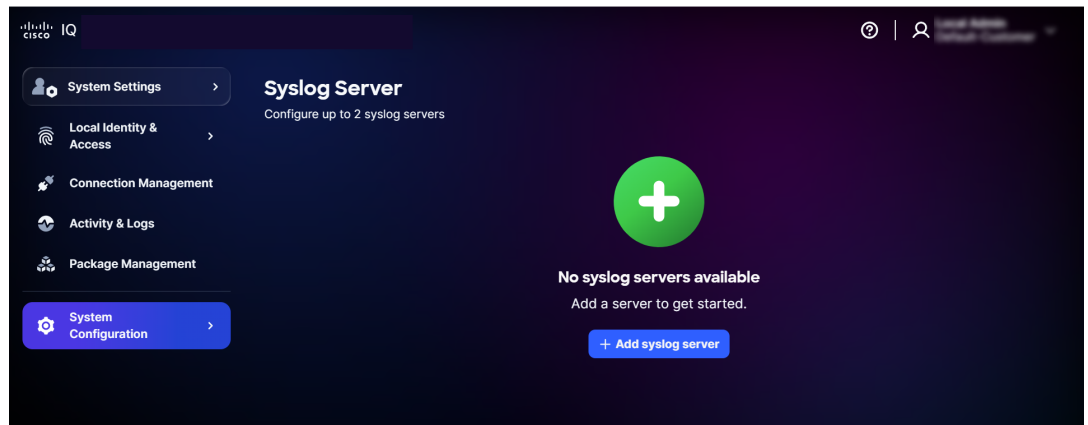


附註：系統日誌伺服器必須指定為IP地址，而不是完全限定的域名(FQDN)。

新增系統日誌伺服器

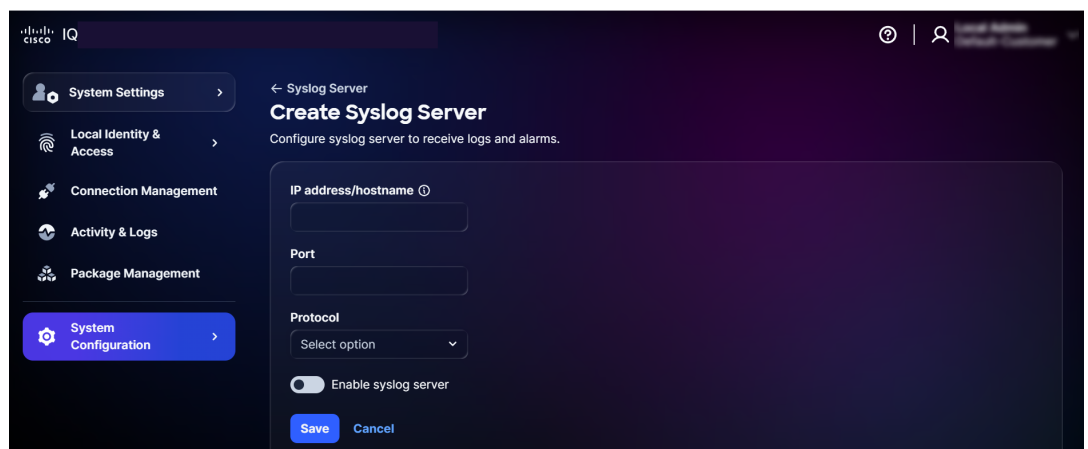
新增系統日誌伺服器：

1. 在System Settings中選擇System Configuration > Syslog Server。將顯示Syslog Server頁。



新增系統日誌伺服器

2. 按一下Add syslog server。將顯示Create Syslog Server頁。



建立系統日誌伺服器

3. 輸入IP地址/主機名。

4. 輸入Port。
5. 從Protocol下拉選單中選擇適用的協定（例如UDP、TCP）。
6. 開啟Enable syslog server切換按鈕。
7. 按一下「Save」。系統將顯示一個確認消息，新新增的系統日誌伺服器將顯示在Syslog伺服器首頁上。

編輯配置的系統日誌伺服器

要編輯已配置的系統日誌伺服器，請執行以下操作：

1. 導航到所需的系統日誌伺服器。
2. 選擇更多選項圖示> 編輯。將顯示Edit Syslog Server頁。
3. 根據需要編輯詳細資訊或關閉Enable syslog server切換。
4. 按一下「Save」。

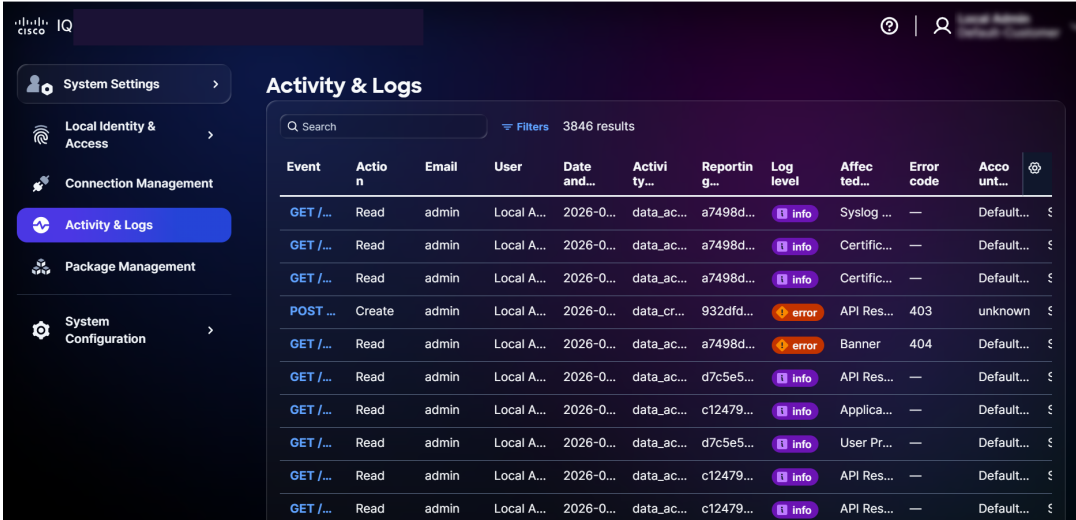
刪除已配置的系統日誌伺服器

要刪除已配置的系統日誌伺服器，請執行以下操作：

1. 導航到所需的系統日誌伺服器。
2. 選擇更多選項圖示> 刪除。系統會顯示確認。
3. 按一下Delete syslog server。

活動和日誌

活動和日誌提供思科IQ中使用者和更改的詳細記錄，允許帳戶管理員跟蹤使用者活動並保持透明度。



Event	Action	Email	User	Date and time	Activity ID	Reporting ID	Log level	Affected resource	Error code	Account	
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Syslog ...	—	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Certific...	—	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	info	Certific...	—	Default...	⋮
POST ...	Create	admin	Local A...	2026-0...	data_cr...	932dfd...	error	API Res...	403	unknown	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	a7498d...	error	Banner	404	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	d7c5e5...	info	API Res...	—	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	Applica...	—	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	d7c5e5...	info	User Pr...	—	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	API Res...	—	Default...	⋮
GET /...	Read	admin	Local A...	2026-0...	data_ac...	c12479...	info	API Res...	—	Default...	⋮

活動和日誌

要檢視活動和日誌，請從System Settings選單中選擇Activity & Logs。

活動和日誌：

- 記錄網關級別的所有API操作
- 支援過濾器、分頁和搜尋功能，幫助您輕鬆查詢和管理資訊

可以使用以下過濾器選項：

- 上次記錄日期:過濾日誌到特定時間範圍
- 日誌級別:按嚴重性過濾日誌（例如，錯誤、警告和資訊）
- 活動型別:按系統活動型別過濾日誌
- 錯誤代碼:特定錯誤代碼的篩選器

橫幅

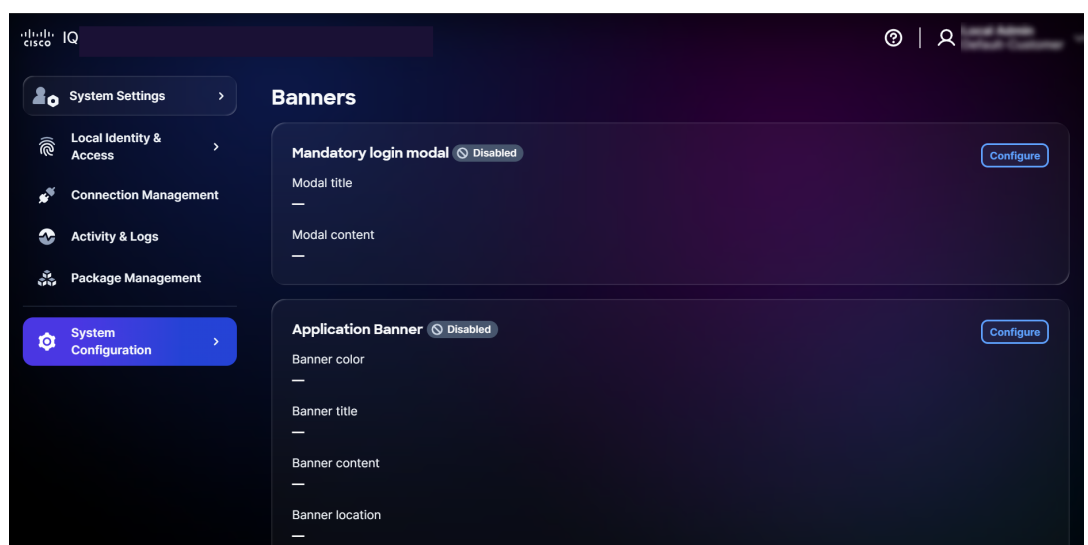
帳戶管理員可以配置系統範圍的橫幅以符合安全和合規標準。

- 強制登入模式:進入登入螢幕之前，必須確認必填標語。
- 應用橫幅:這些是自定義橫幅，在成功身份驗證後橫跨應用程式顯示。

配置強制登入模式橫幅

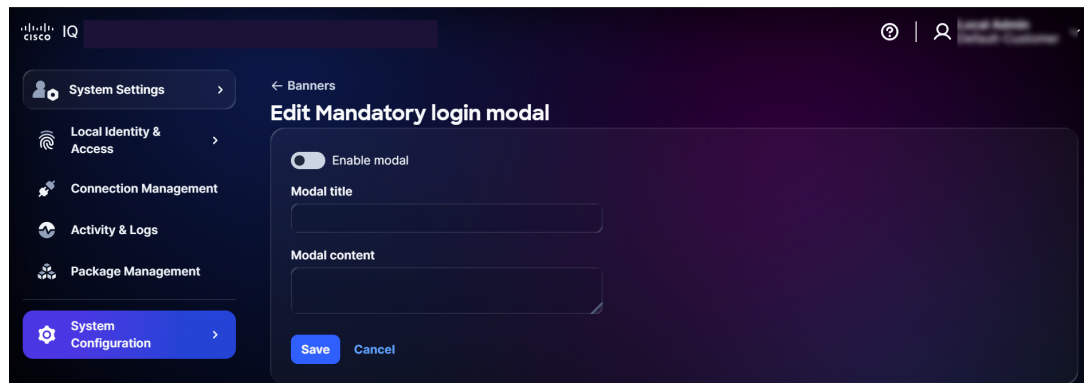
要配置強制性標語，請執行以下操作：

1. 在System Settings中選擇System Configuration > Banners。系統隨即會顯示Banners頁面。



配置強制標語

2. 在Mandatory login modal中按一下Configure。系統隨即會顯示Edit Mandatory login modal頁面。



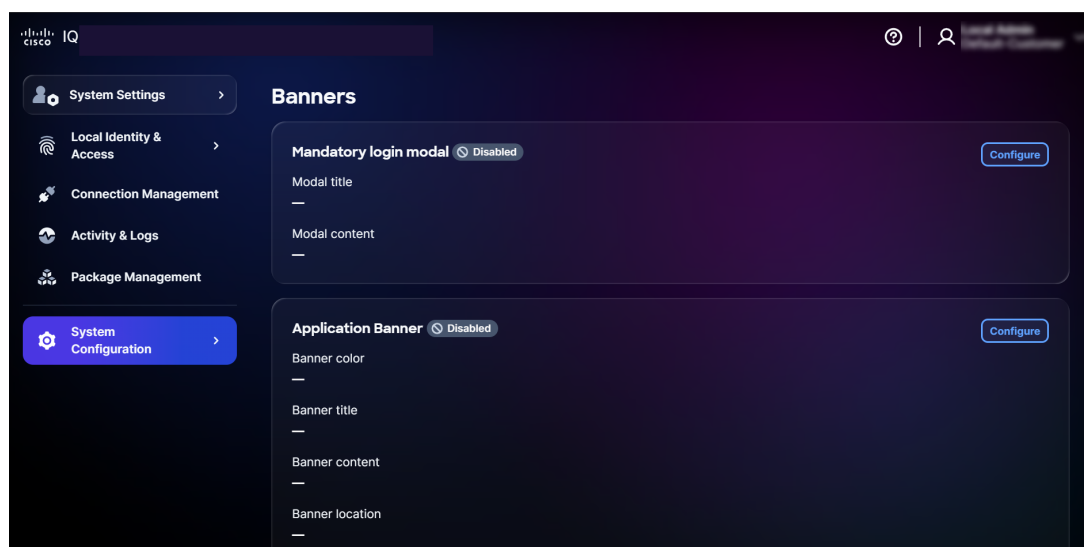
編輯強制登入模式橫幅

3. 按一下切換以啟用或禁用標語。
4. 輸入模式標題。
5. 輸入Modal內容。
6. 按一下「Save」。「必填」登入模式已儲存。

配置應用橫幅

要配置應用程式橫幅，請執行以下操作：

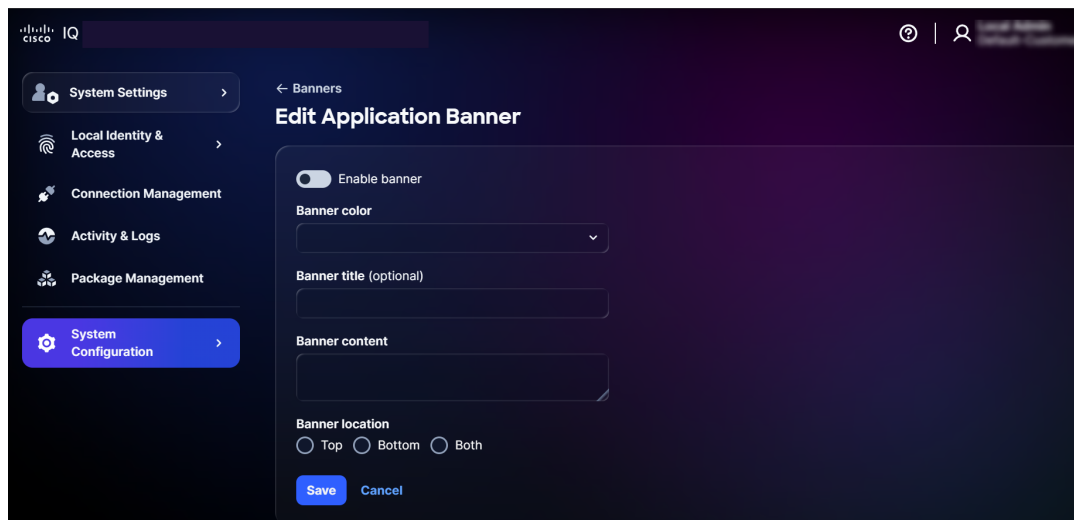
1. 在System Settings中選擇System Configuration > Banners。系統隨即會顯示Banners頁面。



配置標語

2. 按一下Application Banner中的Configure。系統隨即會顯示Edit

Application Banner頁面。



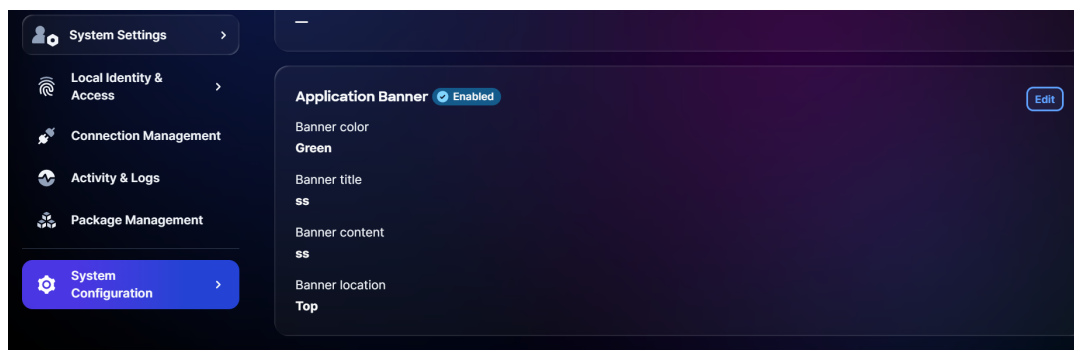
編輯應用程式橫幅

3. 按一下切換以啟用或禁用標語。
4. 選擇標語顏色。
5. 輸入標語標題。
6. 輸入Banner內容。
7. 選擇標語位置。
8. 按一下「Save」。橫幅顯示於整個應用程式中。

編輯橫幅

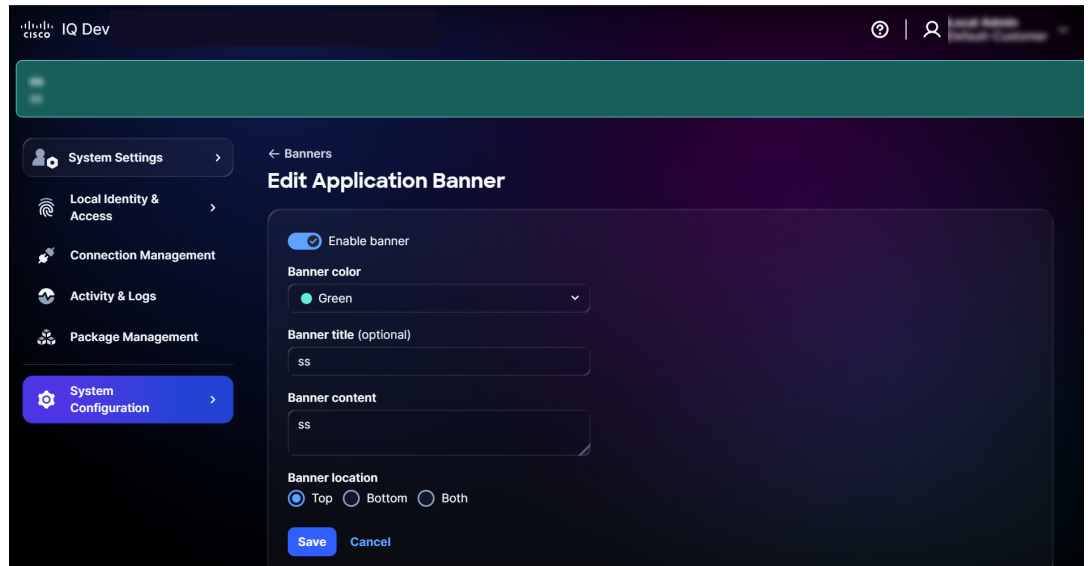
要編輯橫幅，請執行以下操作：

1. 在System Settings中選擇System Configuration > Banners。系統隨即會顯示Banners頁面。



編輯橫幅

2. 按一下「Edit」。系統隨即會顯示Edit Application Banner頁面。



編輯應用程式橫幅

3. 編輯所需的詳細資訊。
4. 按一下切換以啟用或禁用標語。
5. 按一下「Save」。

疑難排解

您可以從Cisco IQ系統收集診斷和日誌檔案，並將其安全地傳輸到SCP伺服器。在報告問題時，可以將這些檔案與支援團隊共用，以提供有價值的上下文並幫助進行故障排除。

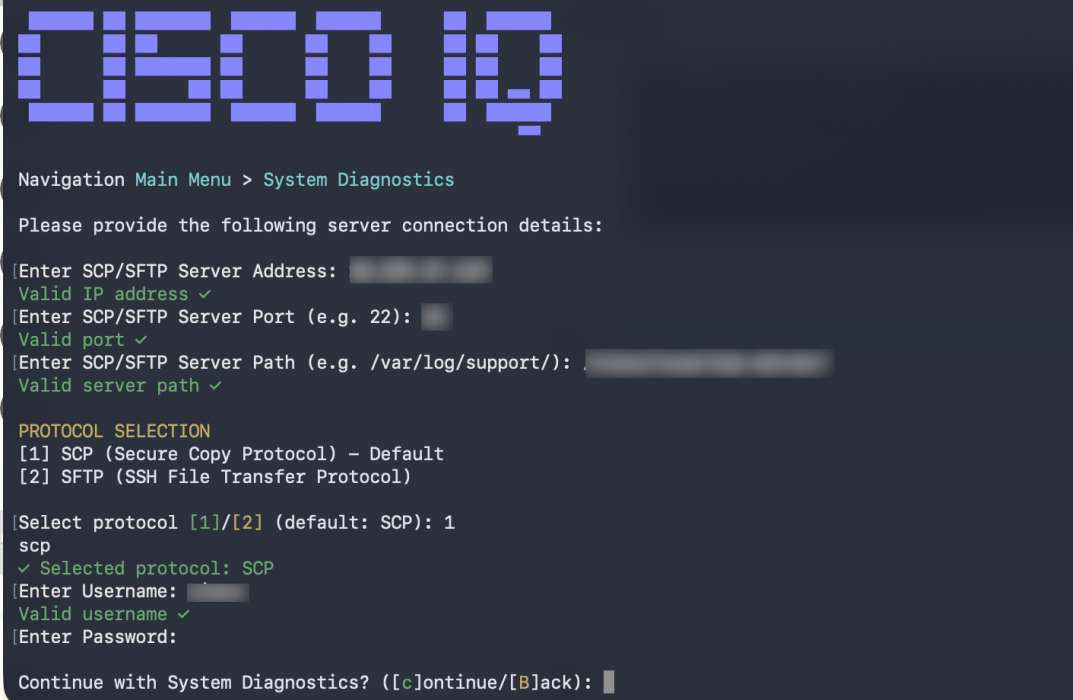
收集診斷和日誌檔案：

1. 登入到Cisco IQ。



主選單

2. 在Cisco IQ主菜單中，輸入「3」並按Enter選擇System Diagnostics。



```
Cisco IQ

Navigation Main Menu > System Diagnostics

Please provide the following server connection details:

[Enter SCP/SFTP Server Address: ]
Valid IP address ✓
[Enter SCP/SFTP Server Port (e.g. 22): ]
Valid port ✓
[Enter SCP/SFTP Server Path (e.g. /var/log/support/): ]
Valid server path ✓

PROTOCOL SELECTION
[1] SCP (Secure Copy Protocol) - Default
[2] SFTP (SSH File Transfer Protocol)

Select protocol [1]/[2] (default: SCP): 1
scp
✓ Selected protocol: SCP
[Enter Username: ]
Valid username ✓
[Enter Password: ]

Continue with System Diagnostics? ([c]ontinue/[B]ack):
```

系統診斷

3. 輸入SCP/SFTP伺服器地址。
4. 輸入SCP/SFTP Server Port。
5. 輸入SCP/SFTP伺服器路徑。
6. 選擇一個協定。
7. 輸入Username。
8. 輸入Password。
9. 輸入「C」並按Enter以繼續系統診斷。



Navigation **Main Menu** > System Diagnostics

```
Checking Reachability ..... ✓
Collecting System Info ..... ✓
Collecting Kubernetes Info ..... ✓
Collecting Logs ..... ✓
Preparing System Diagnostics Bundle ..... ✓
Uploading System Diagnostics Bundle ..... ✓
System Diagnostics Bundle is 'CIQ_Diagnostics_██████████.tar.gz'
System Diagnostics operation completed successfully!

Press Enter to return to main menu...█
```

系統診斷操作完成

系統將開始診斷過程並執行下列操作：

- 檢查可達性
- 收集系統資訊
- 收集Kubernetes資訊
- 收集日誌
- 準備系統診斷捆綁包
- 上傳系統診斷套件組合

完成後，系統會顯示一條確認消息，指示生成的捆綁包名稱。

支援模組

您可以通過Cisco IQ SaaS建立VA和特定於模組的支援案例。思科IQ SaaS中提供了支援模組，該模組提供了支援案例的整合檢視。它允許您篩選、排序和自定義案例清單檢視，讓您能夠檢視您有權訪問的未結和已結案例。有關Cisco IQ SaaS中支援模組的更多詳細資訊，請參閱[Cisco IQ SaaS入門指南](#)。

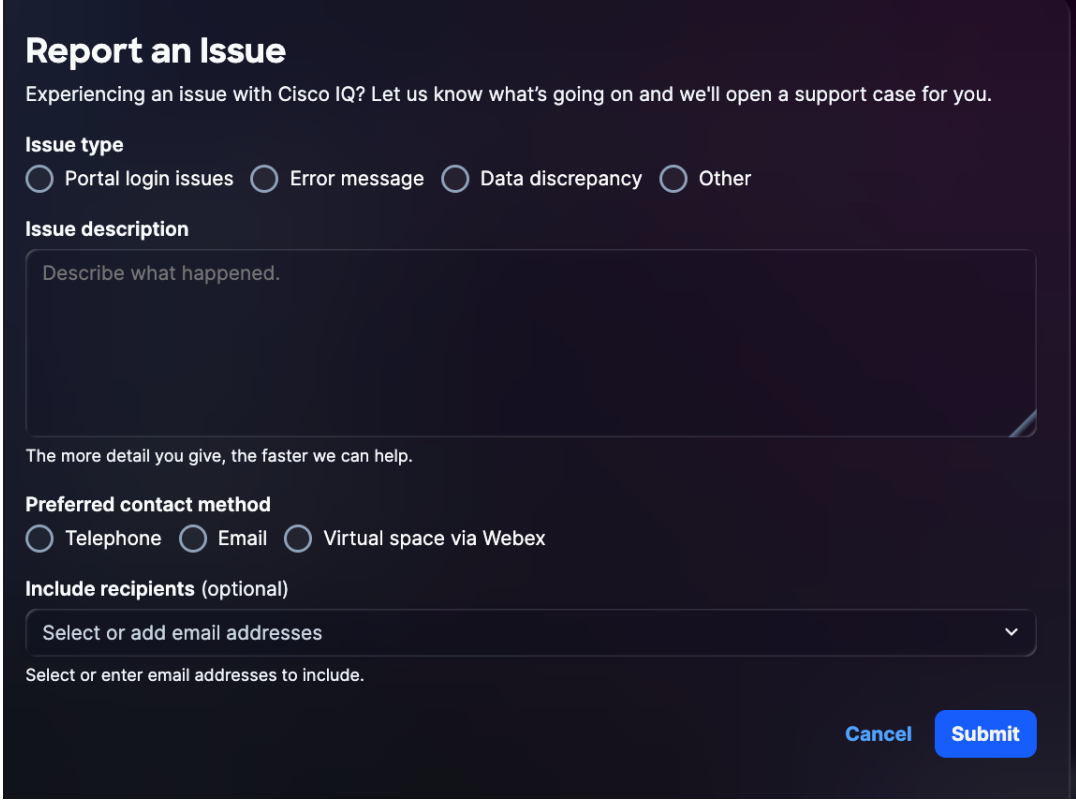


附註：Cisco IQ VA客戶可以訪問大多數Cisco IQ SaaS支援模組功能，包括開啟與Cisco IQ VA及其模組相關的技術支援中心(TAC)案例，以及建立和管理產品案例。

建立支援問題單

您可以在Cisco IQ SaaS中建立VA和模組特定的案例。要建立案例，請執行以下操作：

1. 登入到[Cisco IQ\(SaaS\)](#)。
2. 按一下Help圖示> Report an Issue。將打開「Report an Issue (報告問題)」視窗。



Report an Issue

Experiencing an issue with Cisco IQ? Let us know what's going on and we'll open a support case for you.

Issue type

☐ Portal login issues ☐ Error message ☐ Data discrepancy ☐ Other

Issue description

Describe what happened.

The more detail you give, the faster we can help.

Preferred contact method

☐ Telephone ☐ Email ☐ Virtual space via Webex

Include recipients (optional)

Select or add email addresses

Select or enter email addresses to include.

Cancel Submit

報告問題

3. 提供所需的詳細資訊。
4. 按一下「Submit」。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。