思科IQ鏈路操作指南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、跨您的環境提供更智慧的洞察力，並簡化案例管理。此外，AI功能（如AI Assistant）通過提供情景理解來最佳化運營成果和思科IQ使用者體驗，從而讓您能夠做出主動的、明智的決策，並簡化客戶參與和成功的流程。

Cisco IQ Link安全收集資產遙測資料，並將這些資料從您的內部網路傳輸到Cisco IQ，從而實現AI驅動的預測性洞察，幫助您提高網路可視性、預測問題並提高運營效率。

本地身份驗證

帳戶管理員應使用以下憑證登入到Cisco IQ Link:

- 預設使用者名：admin
- 預設密碼：在Cisco IQ Link安裝過程中設定的密碼；如需詳細資訊，請參閱Cisco IQ Link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User Profile（使用者配置檔案）選單更改密碼並設定安全問題。

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)。

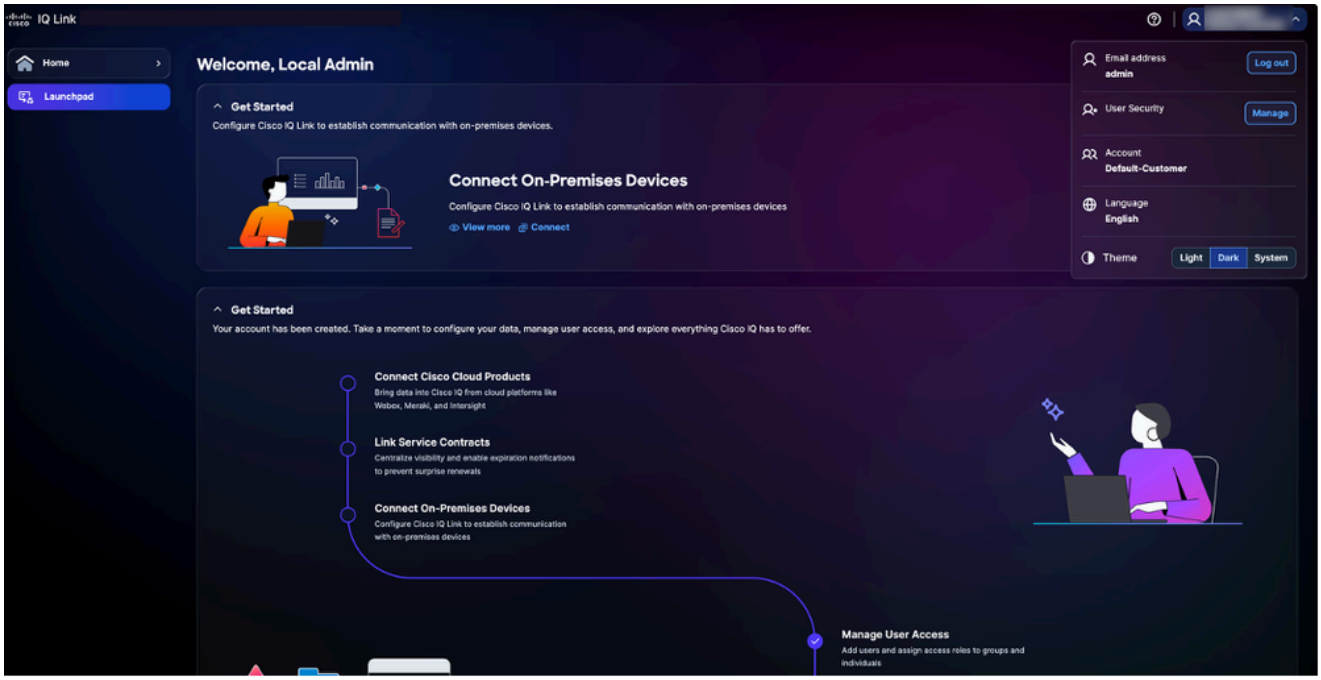
附註：在15分鐘內，您有三(3)次嘗試輸入正確的密碼。如果所有三(3)次嘗試均失敗，您的帳戶將臨時鎖定30分鐘以保護您的安全。
在鎖定期間無法嘗試登入。系統會顯示以下消息：「由於嘗試失敗次數過多，帳戶被鎖定。請稍後再試。」，包括鎖定到期時間。
您的帳戶會在30分鐘後自動解鎖，此時您可能會嘗試登入或重置密碼。

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。

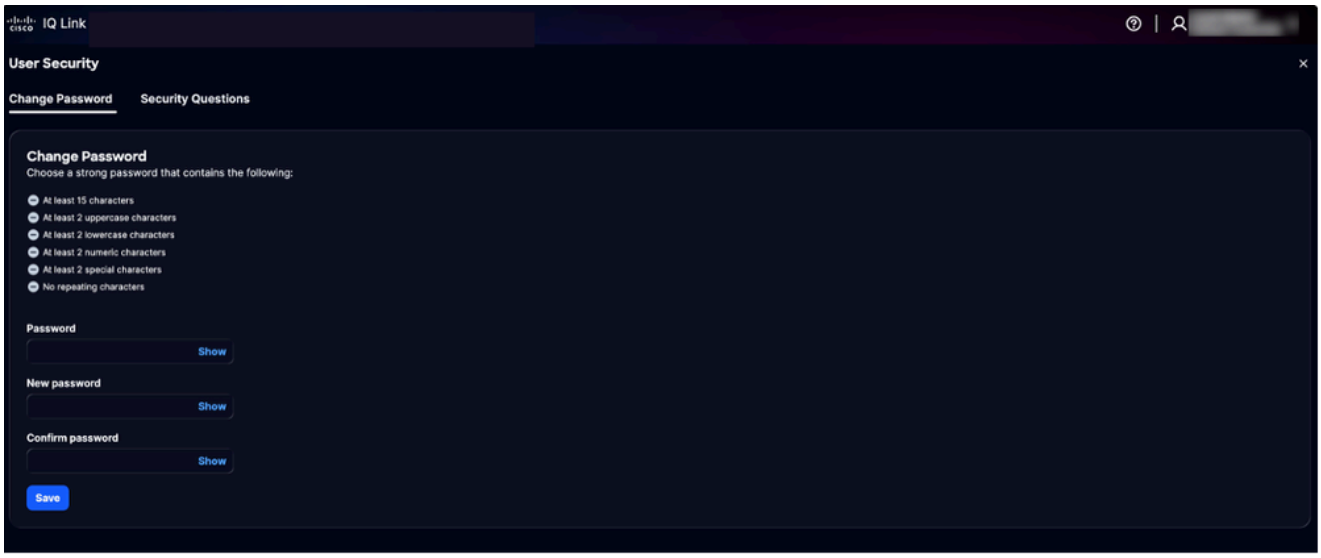
要設定安全問題，請執行以下操作：

1. 在首頁中，按一下您的User Profile圖示。將開啟下拉選單。



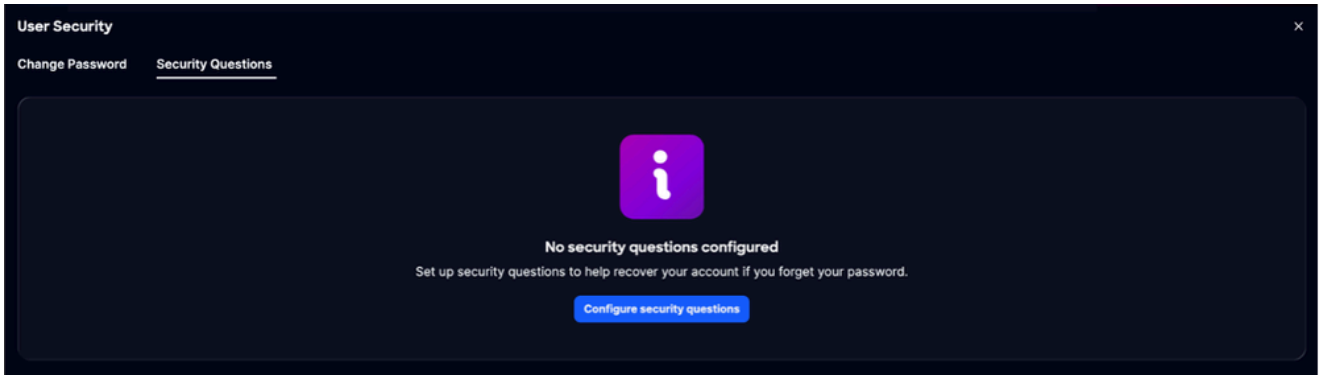
使用者配置檔案選單

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



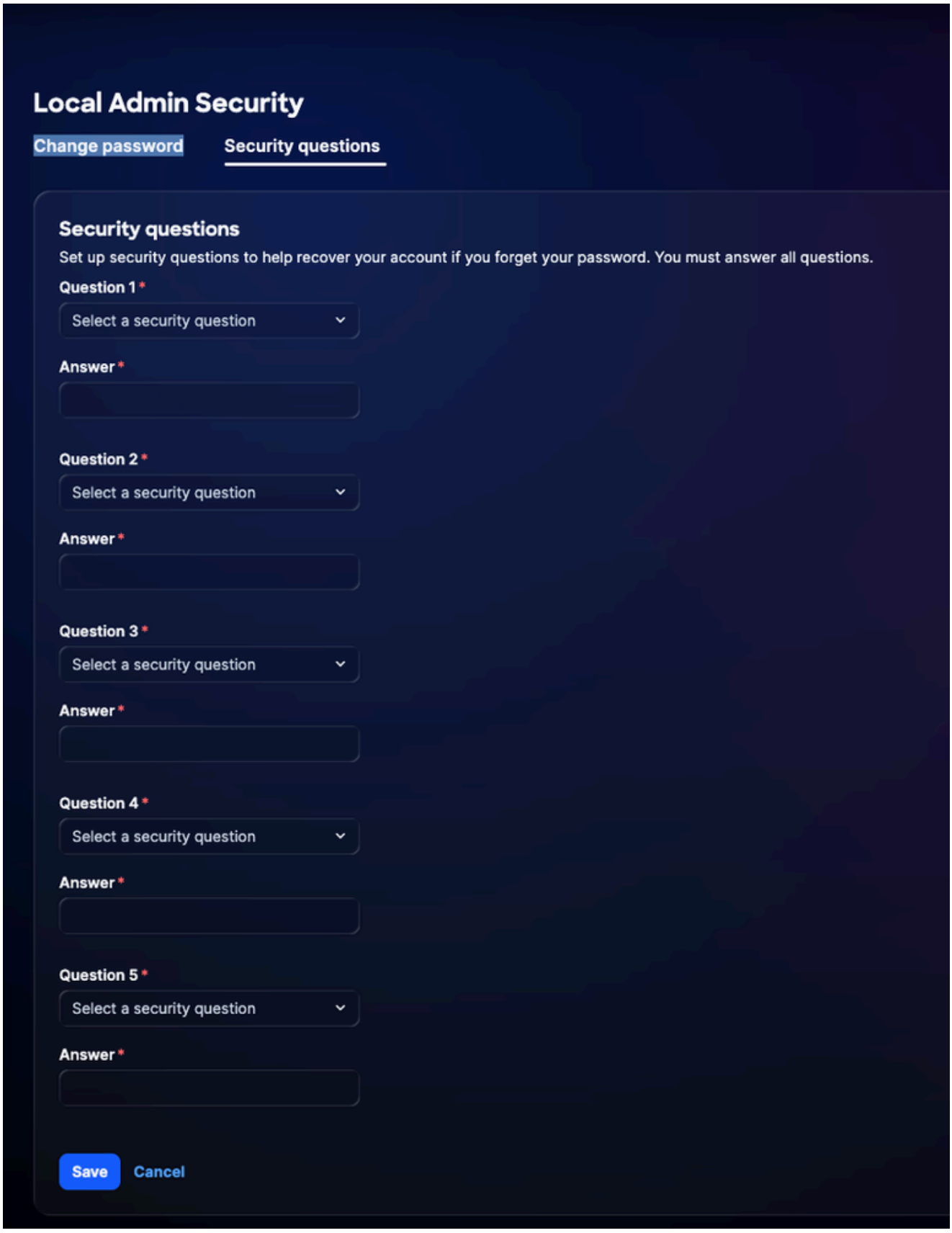
更改密碼

3. 按一下Security Questions以開啟該頁籤。



安全問題

4. 按一下配置安全問題。



安全問題

5. 從下拉選單中選擇任意五(5)個安全問題。
6. 輸入每個問題的回答。

7. 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，例如，「Smith」和「smith」被視為相同。

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，則禁用密碼過期。）

必要條件

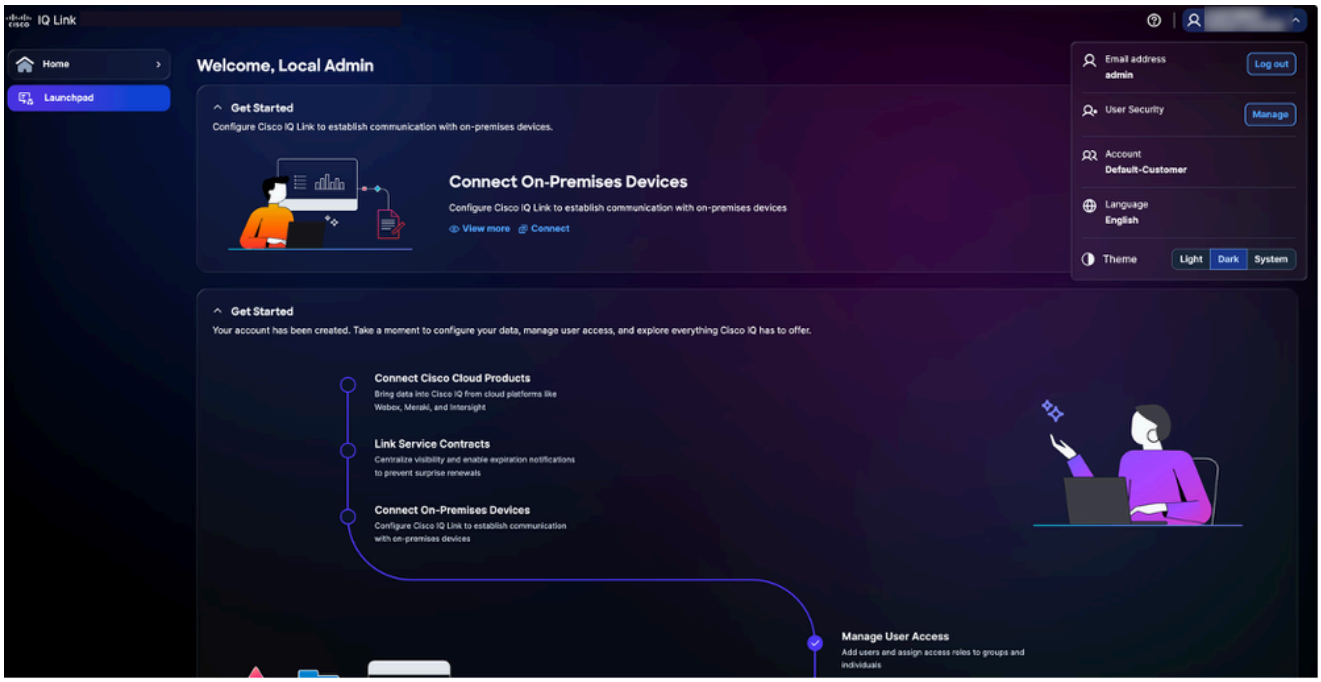
要管理密碼，必須滿足以下條件：

- 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)
- 您已登入到Cisco IQ Link
- 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User Profile圖示。將開啟下拉選單。



使用者配置檔案選單

2. 按一下「User Security」中的「Manage」。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」。

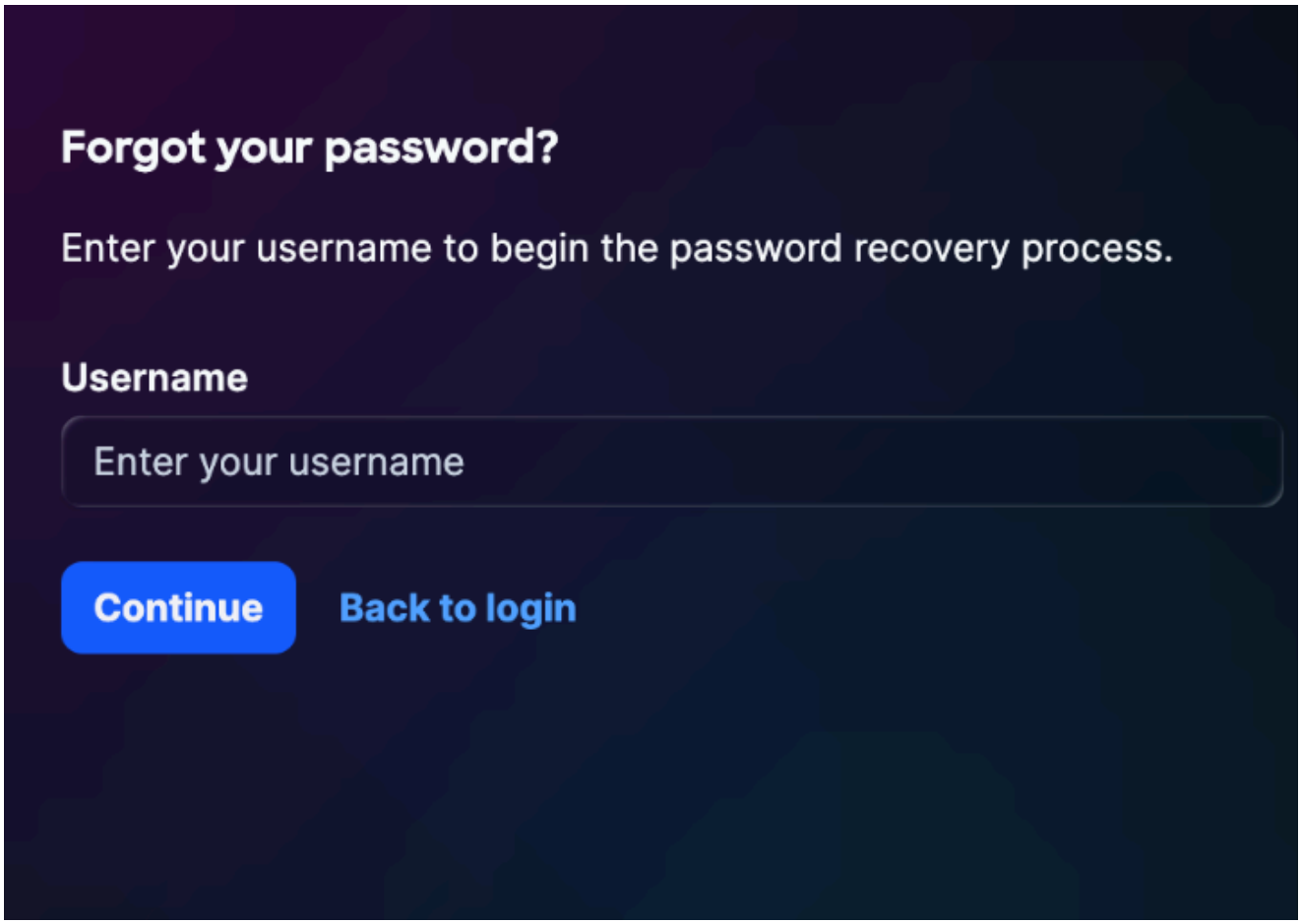
密碼在Cisco IQ系統中更新，包括Cisco IQ虛擬機器(VM)。

重置忘記的密碼

如果您之前設定了安全問題，則可以使用安全問題驗證過程重置忘記的密碼。如需詳細資訊，請參閱設定安全問題和答案。

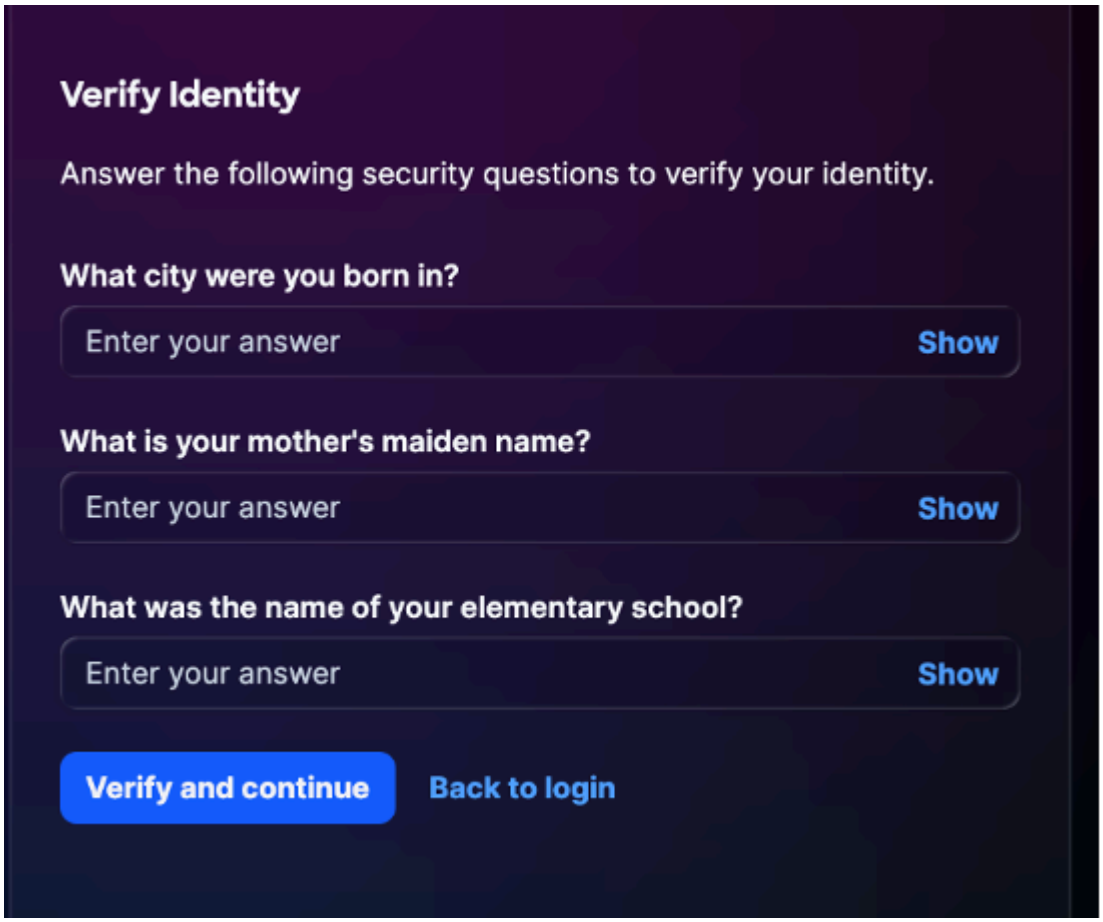
要重置忘記的密碼：

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



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。

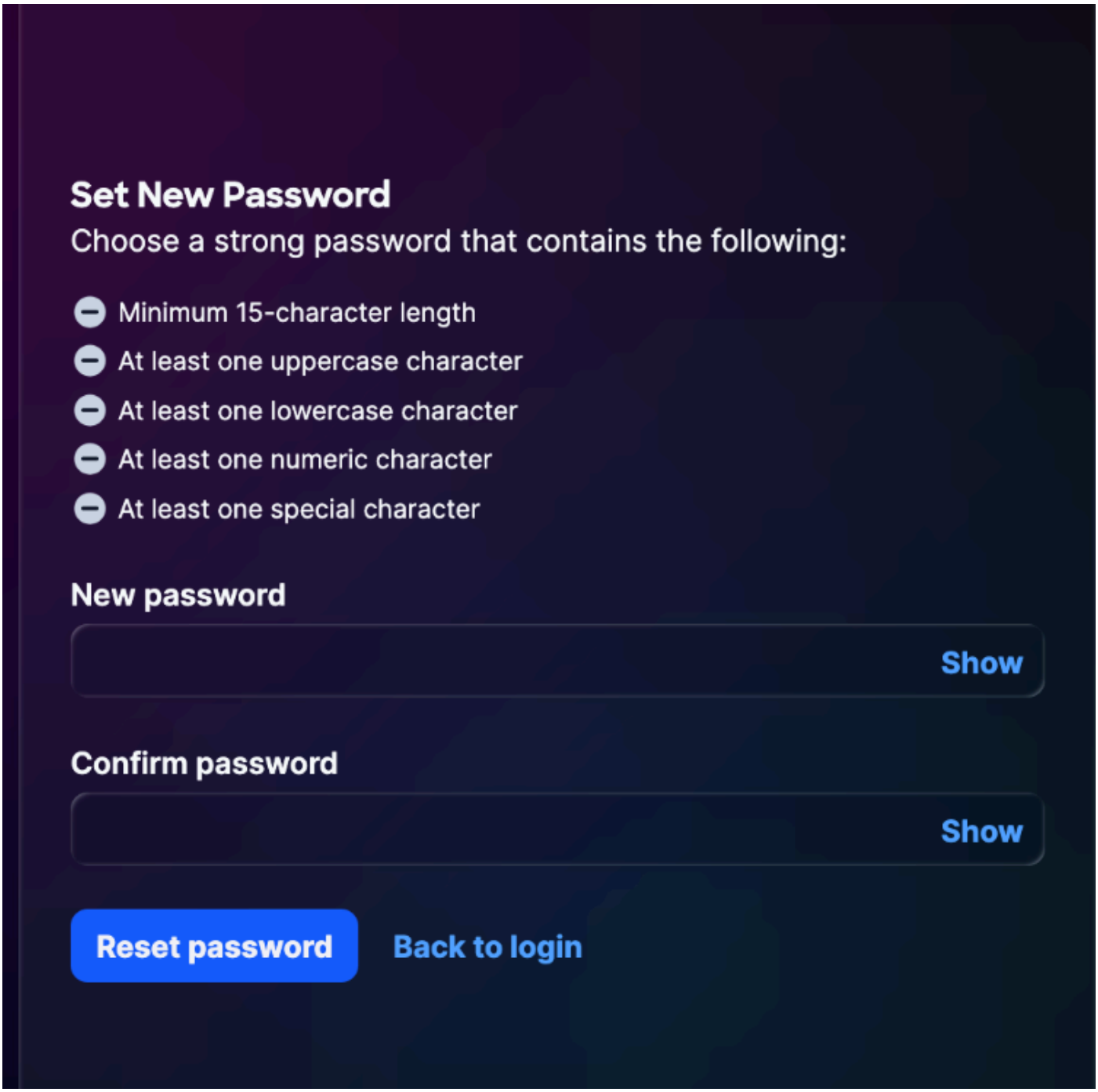


驗證身份

✎ 附註：上面顯示的安全問題是特定於使用者的，因使用者而異。

5.輸入所有三(3)個顯示問題的回答。

6.按一下驗證並繼續。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。



重設密碼

您在15分鐘內三次嘗試正確回答安全問題。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。您無法在鎖定期間重置密碼。
系統會顯示以下消息：「由於驗證嘗試失敗次數過多，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。

7.輸入New password。

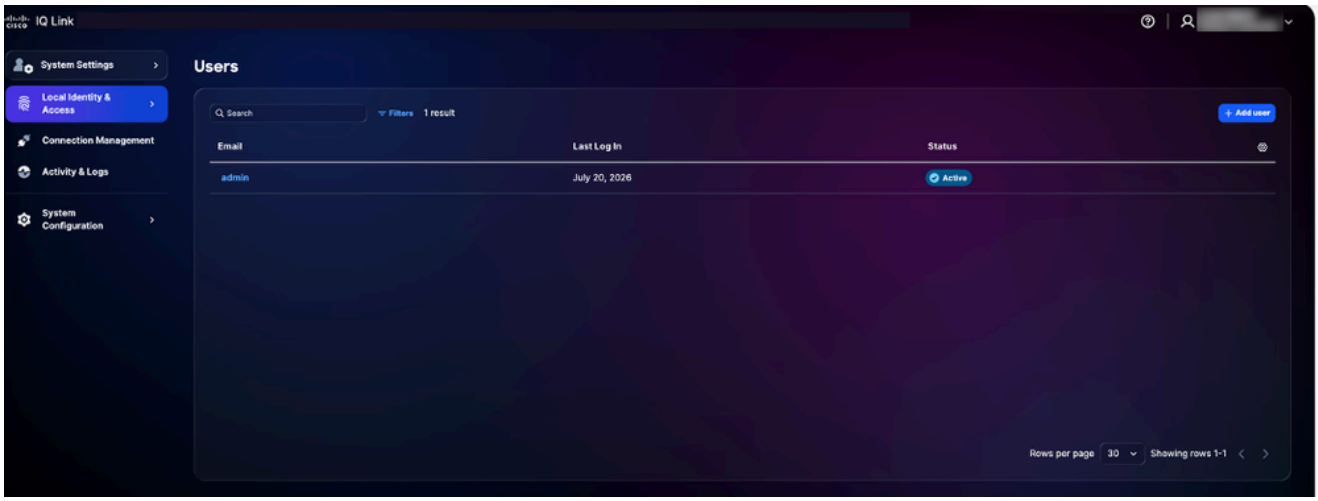
8.再次輸入密碼進行確認。

9.按一下提交。

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：

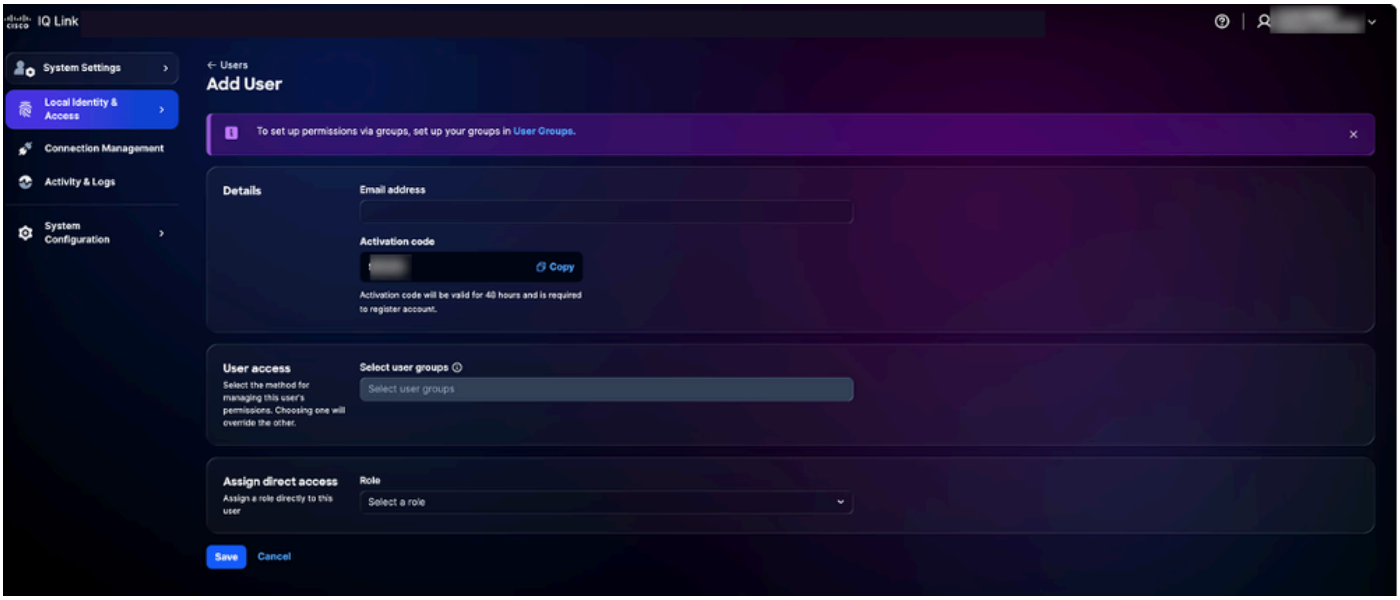
1. 導覽至System Settings > Local Identity & Access > Users。系統隨即會顯示Users頁面。它列出所有現有的本地使用者及其狀態。



「使用者」頁

附註：帳戶管理員不顯示更多選項圖示（如上圖所示）。

2.按一下Add users。系統隨即會顯示Add User頁面。



新增使用者

3.輸入電子郵件地址。

4.輸入激活代碼。

附註：預設情況下顯示啟用代碼。與使用者共用，因為完成註冊需要該共用。

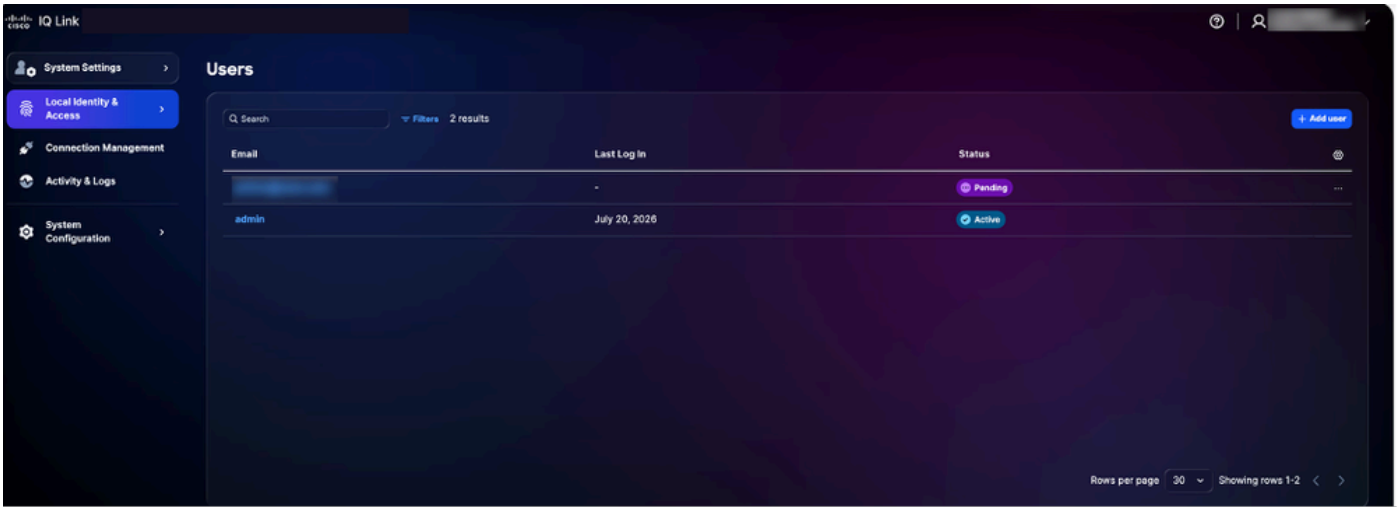
5.在使用者訪問中，從選擇使用者組下拉選單中選擇使用者組。

附註：使用者從選定組繼承訪問許可權。

6.在分配直接訪問中，從角色下拉選單中選擇角色。有兩(2)個可用角色：

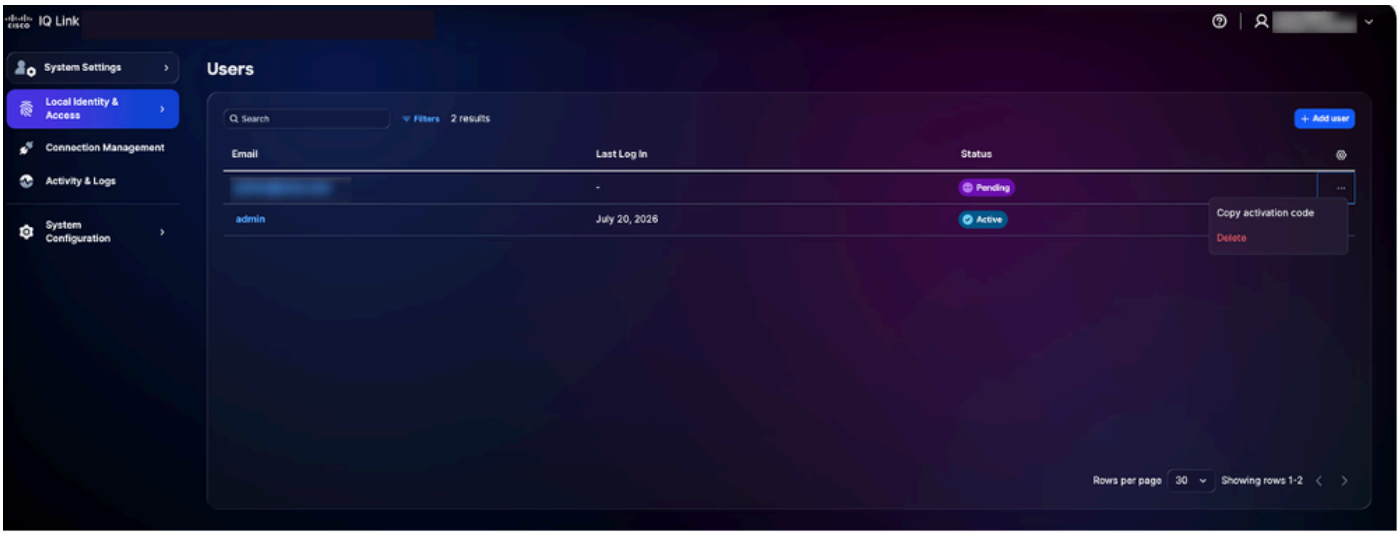
- 檢視器:檢視和訪問應用程式
- 管理員:訪問應用程式和管理系統設定，但系統管理和IDP除外

7.按一下儲存。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。



新新增的使用者

8.在清單中找到新建立的使用者，並確認Status列顯示Pending。



複製啟用代碼

9.按一下新建立使用者旁邊的更多選項圖示> 複製啟用代碼。啟用碼將複製到剪貼簿。

10.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

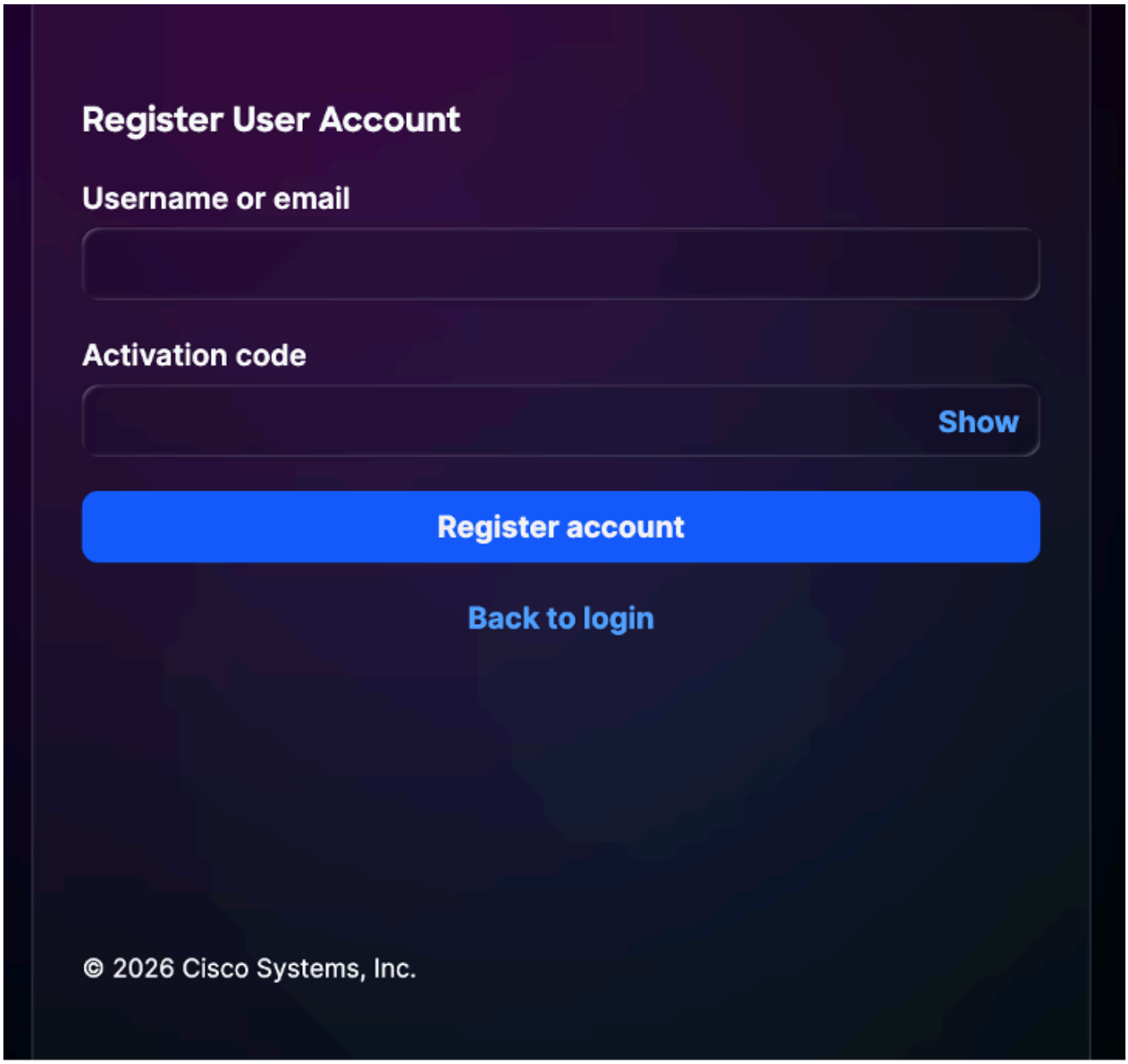
註：啟用碼的有效期為48小時。如果您的代碼過期，請與您的帳戶管理員聯絡以請求新的代碼。

11.要註銷，請按一下右上角的User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。

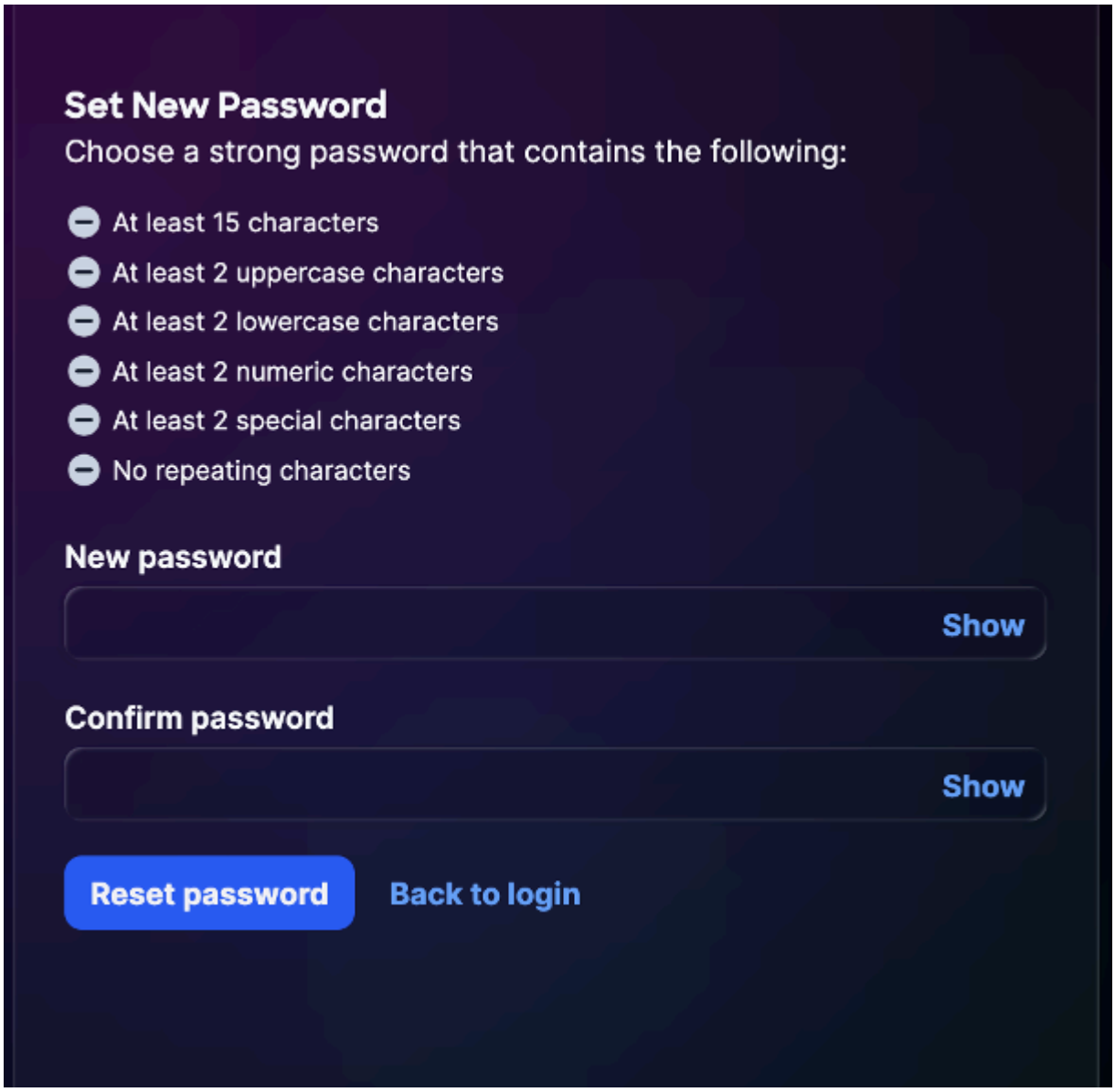


新使用者帳戶

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。



新使用者帳戶密碼

5. 輸入New password。
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(有關詳細資訊，請參閱設定安全問題和答案)。

管理本地使用者組

使用者組使帳戶管理員能夠一起管理多個本地使用者的角色。帳戶管理員可以建立一個組，將一個角色和一組使用者附加到該組，然後在一個位置更新該角色或成員身份，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。

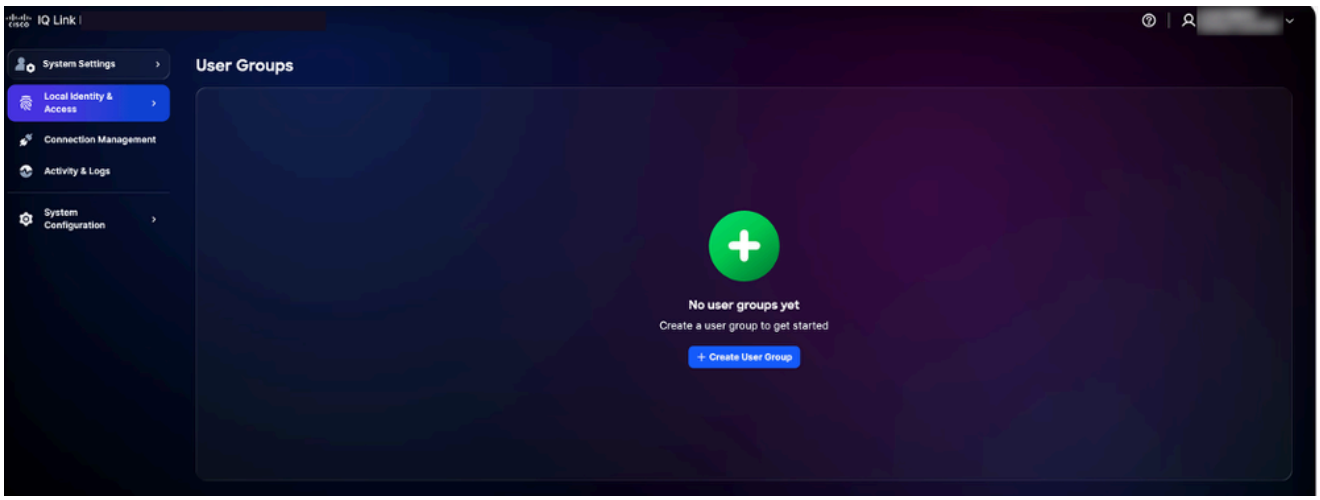
✎ 附註：只有帳戶管理員才能建立、編輯或刪除使用者組。組由現有本地使用者組成；必須先建

立使用者，然後才能將其新增到組中。

建立使用者組

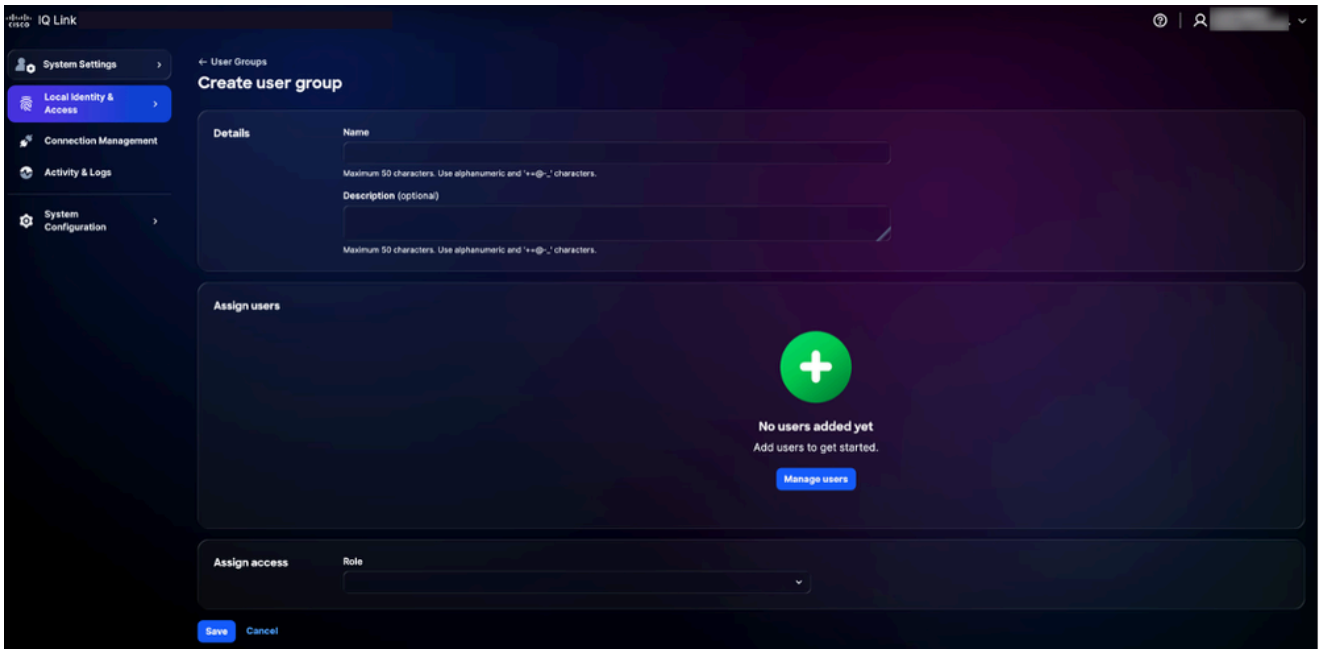
要建立使用者組，請執行以下操作：

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+ = @ - _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:檢視和訪問應用程式（只讀）
    - 管理員:訪問應用程式並管理系統設定

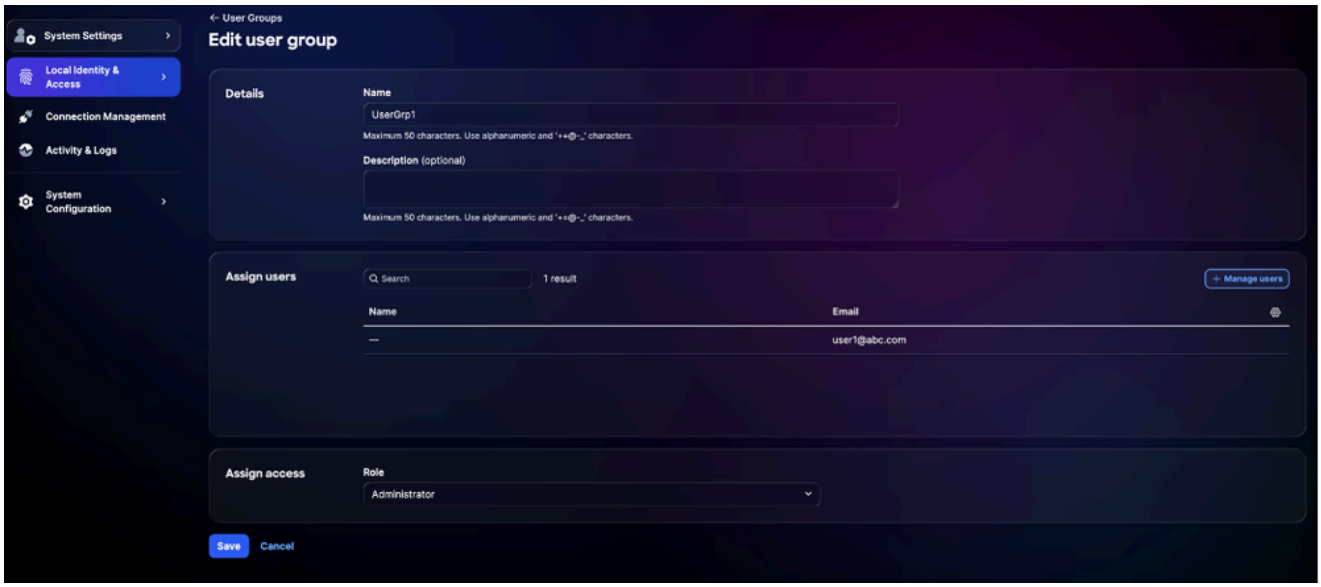
4.按一下Save。

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. 按一下組旁邊的More圖示，然後選擇Edit。將顯示編輯使用者組頁。



編輯使用者組

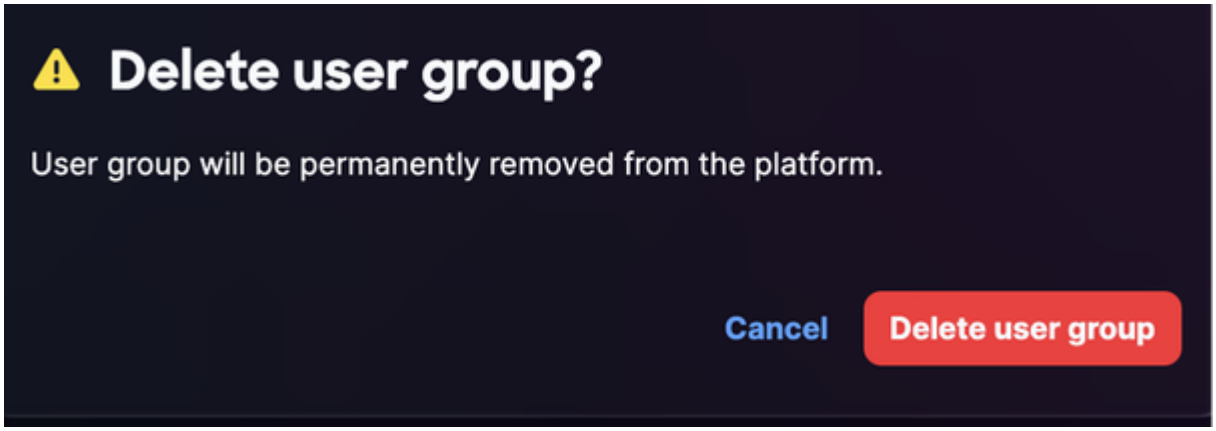
3. 進行所需的更改。
4. 按一下「Save」。

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。



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Cisco IQ Link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身份提供程式(IDP)配置登入到Cisco IQ連結。

SSO的OKTA IDP SAML配置

配置IDP SAML的先決條件

- 本地帳戶管理員對Cisco IQ連結的訪問許可權
- 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。

2.為Cisco IQ Link例項設定以下屬性。
表 1：Cisco IQ連結屬性

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
對象	非員工
入職類別	選擇「New Onboarding」

表 2：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斷言使用者服務(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

3.配置以下強制性屬性語句。

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：.*

4.配置應用程式中的單一註銷(SLO)設定。

表 3：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	SP後設資料僅用於ADFS IDP（而非Okta）。
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ID或ACS URL）	https://mymanagementhost.mydomain.com

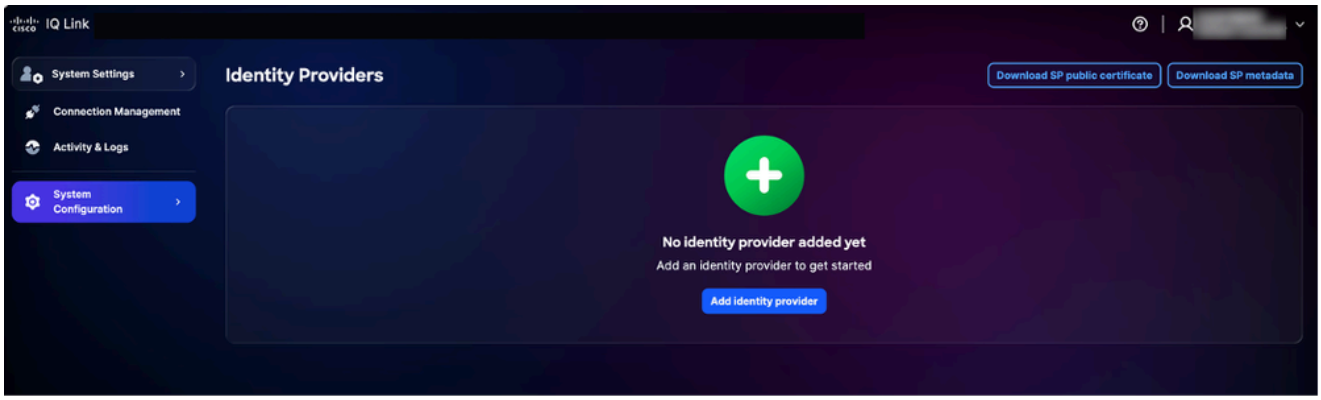
5.按一下下載圖示下載「SP後設資料」檔案。

6.按提供商的要求設定或建立應用程式。

新增Okta IDP

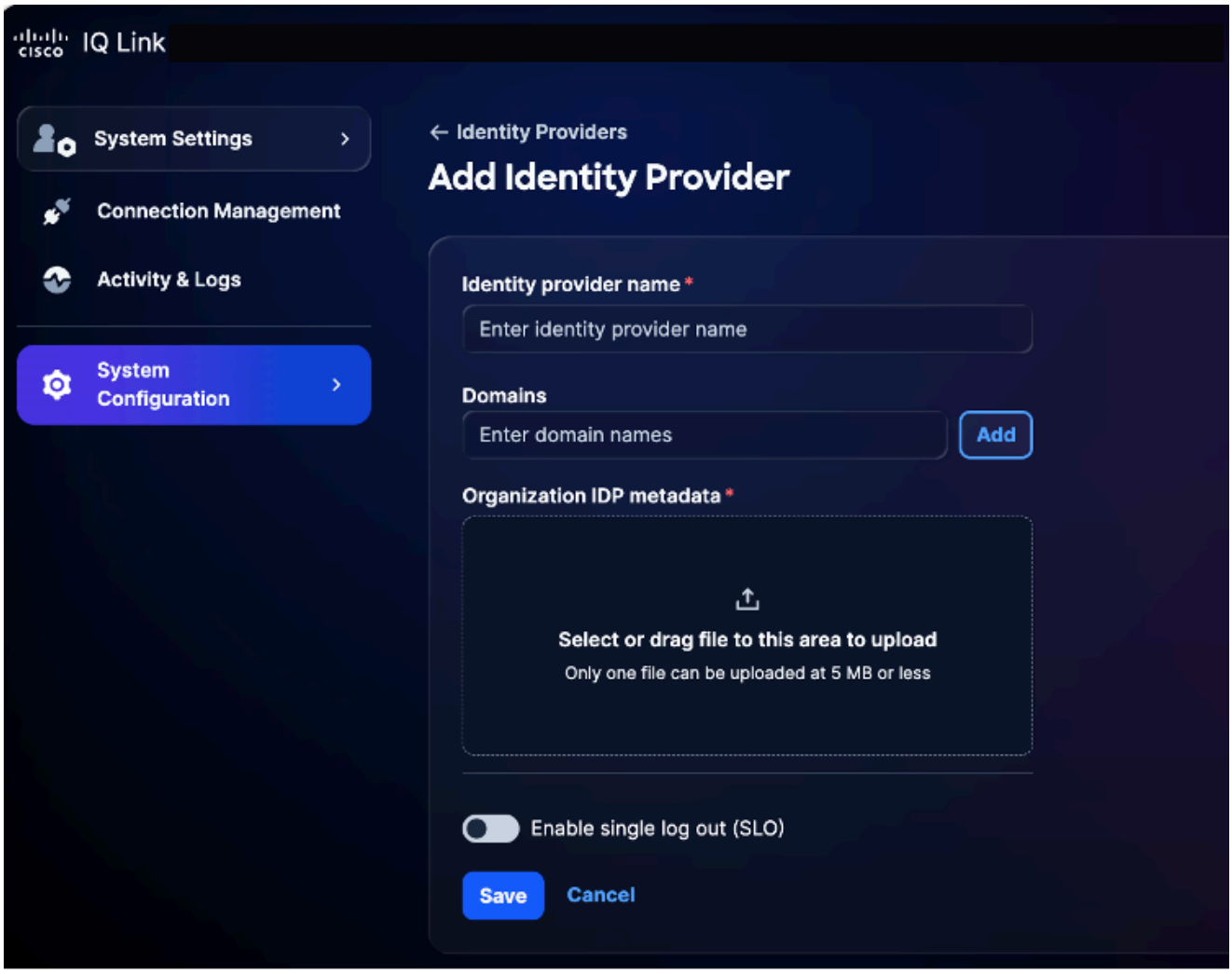
在Cisco IQ Link中新增IDP:

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

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



新增身份提供程式

附註：在給定時間只能新增一(1)個IDP。

3.輸入身份提供程式名稱。

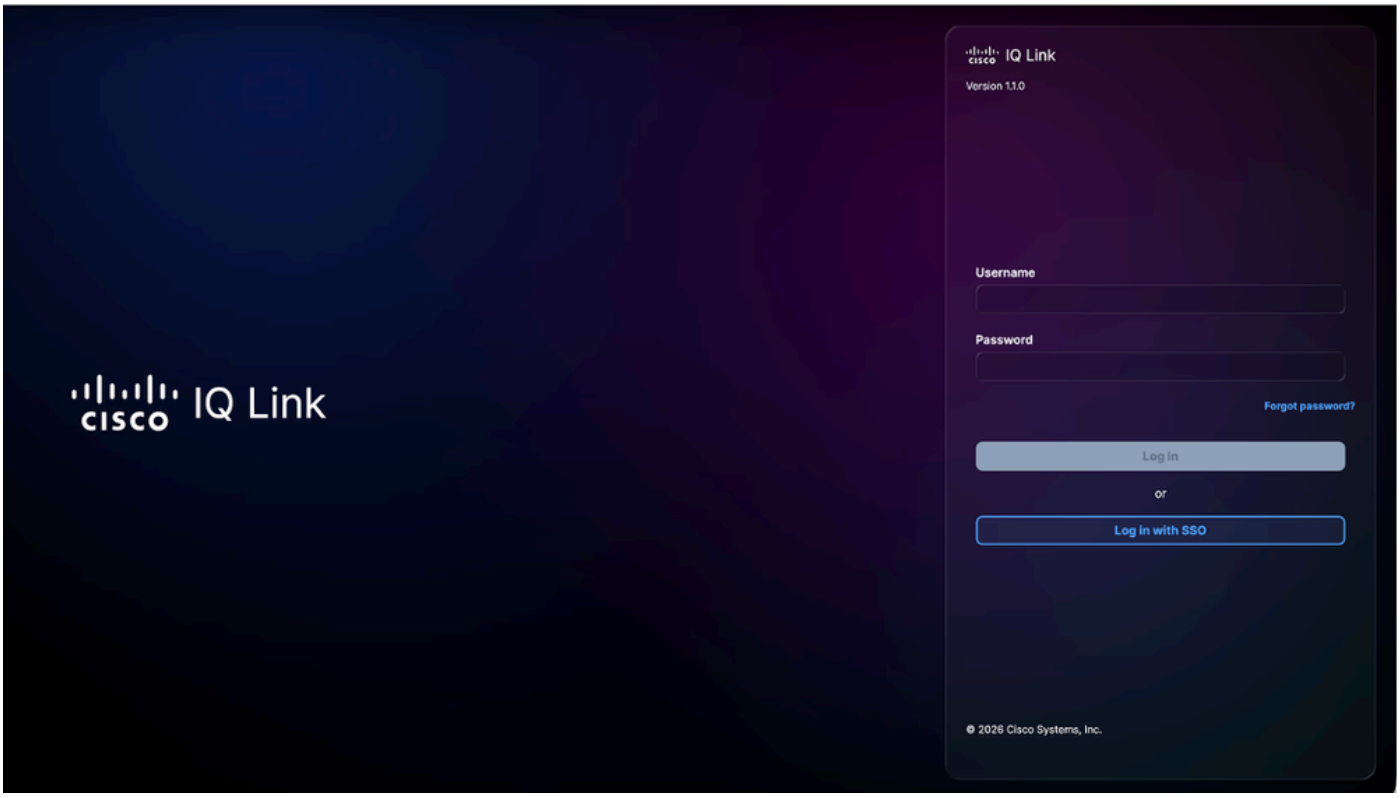
4.按一下Add將已配置Cisco IQ Link的域名新增到Domains欄位。

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服務提供商(SP)實體詳細資訊。

6.（可選）啟用Enable single logout切換按鈕。您也可以稍後啟用SLO。

7.按一下儲存。

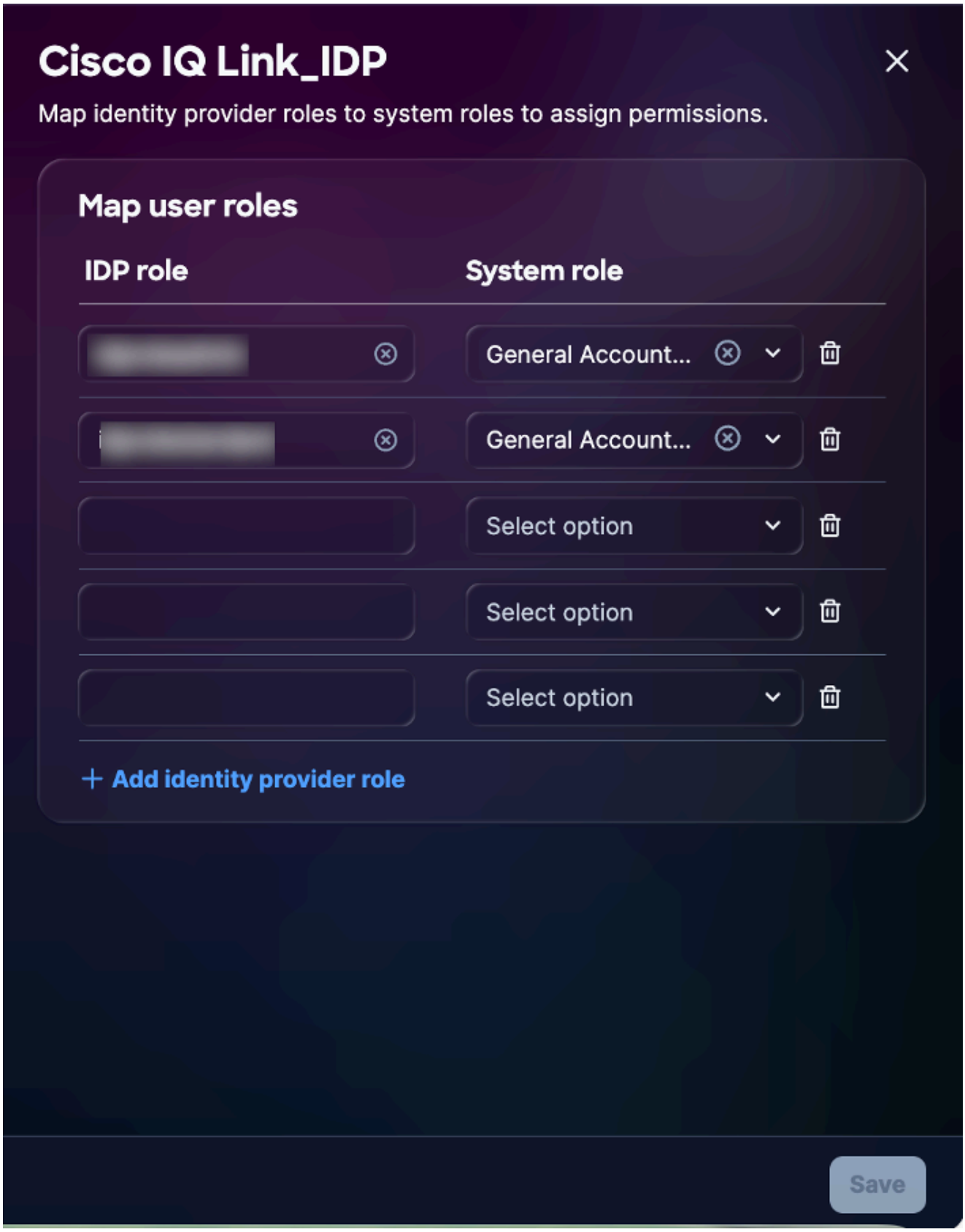
配置後，登入頁面將顯示使用SSO（通過IDP）登入的選項。



Cisco IQ連結登入

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。



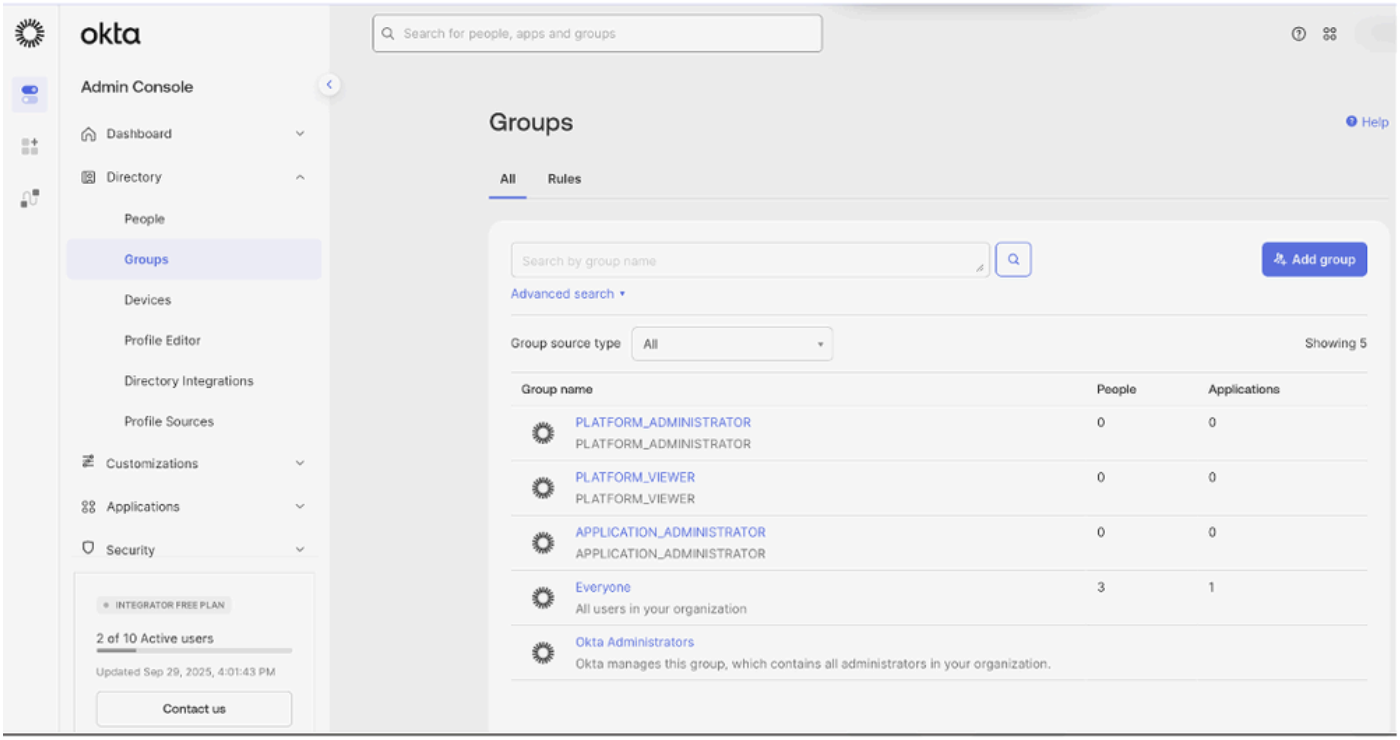
使用者角色對映

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

- 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.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。

單一註銷配置

如果選擇啟用單一註銷配置(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. 在身份提供程式頁面中，按一下下載SP公共證書。

下載公共證書

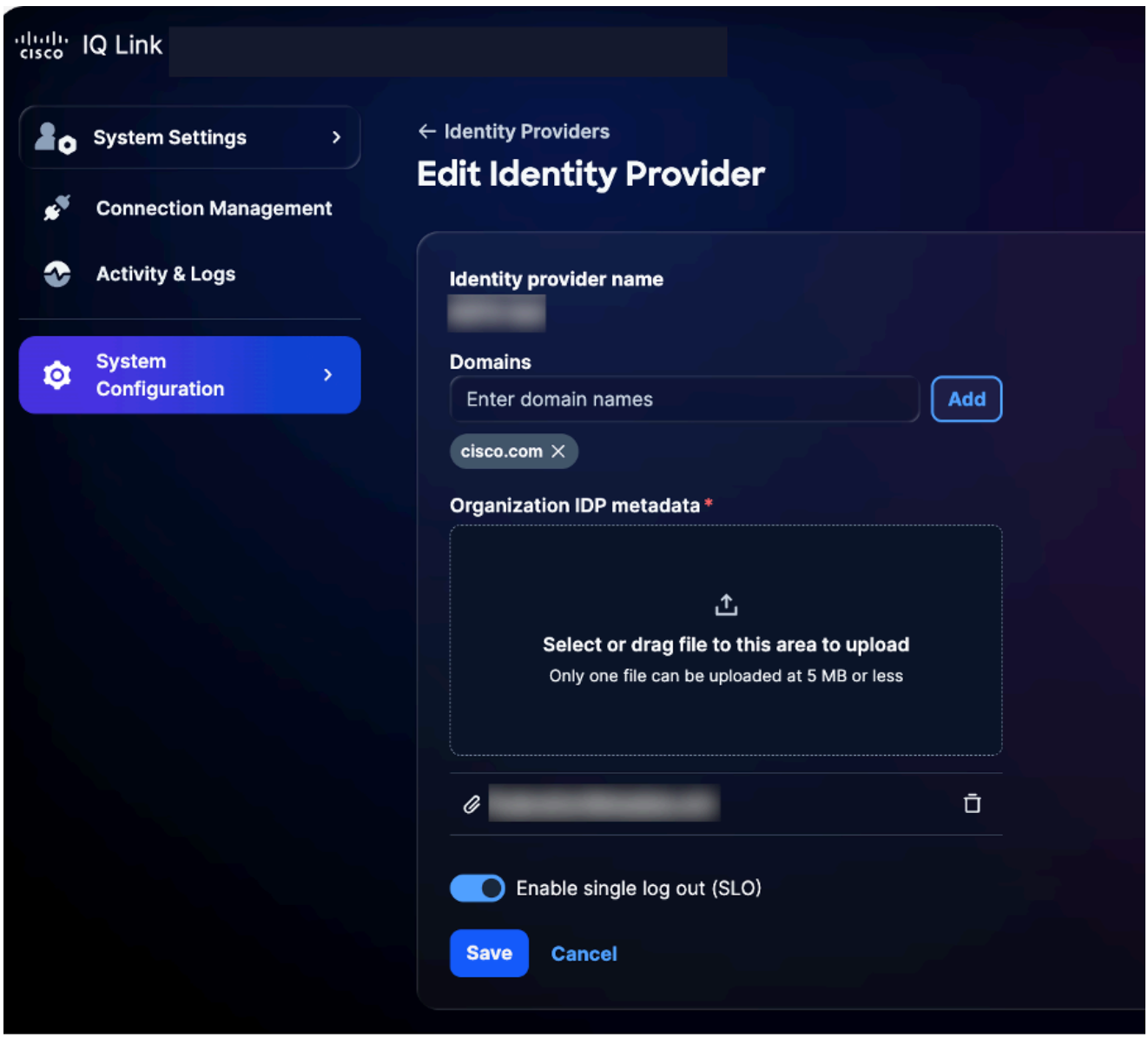
2. 將下載檔案另存為sp-public-key.crt。

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. 再次下載IDP後設資料檔案。

6. 在Identity Providers頁面上，選擇新增的IDP的More Options圖示> Edit。



編輯身份提供程式

7. 開啟Enable single log out(SLO)切換按鈕。
8. 上載新下載的後設資料檔案。
9. 使用以下核對表驗證SSO和SLO功能：

驗證核對表：

- 本地帳戶管理員登入成功
- 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/SLO流

疑難排解IDP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IDP狀態、證書錯誤、SSO登入失敗和SLO配置相關的問題：

表 4：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(ADFS)配置為Cisco IQ的SAML IDP的指南。

配置用於SSO的ADFS IDP SAML的先決條件

- 建議使用ADFS 6.0+
- Windows Server 2012 R2+
- 已配置的AD整合
- ADFS上的SSL/傳輸層安全(TLS)證書
- 帳戶管理員對Cisco IQ的訪問許可權
- 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
- ADFS伺服器配置詳細資訊（如下表中所列）

表 5：ADFS伺服器配置

專案	說明	範例
Cisco IQ FQDN	使用者部署主機名	devxx-23.cx-xxx-xxx.cisco.com
ADFS伺服器URL	使用者ADFS伺服器地址	https://ad-fs.dev.local
公司域	電子郵件域	company.com
AD組	AD組域名(DN)	CN=Role - CXIQ開發人員

配置ADFS伺服器

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Download SP public certificate和Download SP metadata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目錄（例如，C:-certificate.crt）。
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，從檔案中匯入有關信賴方的資料，從作為步驟3的一部分儲存的檔案中獲取詳細資訊。
10. 按一下瀏覽以選擇SP後設資料檔案並完成檔案上載。
11. 按「Next」（下一步）。
12. 輸入顯示名稱（例如「CIQ-Stage」），新增任何相關註釋，然後按一下Next。
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重身份驗證(MFA)介面卡(例如，已配置Azure MFA或*Time-Based One-Time Password(TOTP))，否則不要選擇「允許具有MFA的所有人」。
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
```

要設定「允許所有人」（無MFA要求），請運行以下命令：

```
Set-AdfsRelyingPartyTrust -TargetName “

     ” -AccessControlPolicyName “Permit everyone”
```

您還可以通過PowerShell建立信賴方信任：

```
Add-AdfsRelyingPartyTrust `
    -Name “

     ” `
    -Identifier “

      ” `
-SamlEndpoint (New-AdfsSamlEndpoint -Binding POST -Protocol SAMLAssertionConsumer -Uri “

       ”) `
    -AccessControlPolicyName “Permit everyone” `
    -IssuanceAuthorizationRules ’=> issue(Type = “http://schemas.microsoft.com/authorization/claims/per
```

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 6：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	公開金鑰基礎架構(PKI)/憑證驗證	ADFS通過使用者主體名稱(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 - Stage」）。

```
$relyingPartyName = “Cisco IQ - Stage”
```

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 ”, Issuer == “AD
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/ws/2005/05/identity/claims/em

@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.Iss

@RuleName = “Send Group Membership”
c:[Type == “http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname ”, Issuer == “AD
```

```
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/claims/Group”), query = “;mem
’@@
```

3.通過運行以下命令應用索賠規則：

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

Write-Host “Claim rules configured successfully!” -ForegroundColor Green
```

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. 設定使用者名稱以檢查使用者的組成員身份。

```
$username = “testuser”
```

2.運行以下命令以查詢使用者帳戶：

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

$user = $searcher.FindOne()
```

3.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證書由內部證書頒發機構(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
```

或

- 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區：

```
Import-Certificate -FilePath “C:-iq-onprem-ca.cer” -CertStoreLocation “Cert:”
```

3.通過重新啟動ADFS服務來應用更改。

```
Restart-Service 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.運行以下命令進行安裝：

```
certutil -ca
```

5.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UPN或與AD帳戶匹配的電子郵件。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, Thumbprint, NotAfter -AutoSize
```

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：

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

```
Enable-AdfsEndpoint -TargetAddressPath /adfs/services/trust/13/certificatetransport
```

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, Enabled, Proxy -AutoSize
```

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”, “FormsAu
-PrimaryExtranetAuthenticationProvider @(“CertificateAuthentication”, “FormsAuthentication”, “Microsoft
```

2.使用以下命令驗證兩個清單是否都包括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）

以下各節中的步驟可解決CERT_E_UNTRUSTEDROOT(0x800B0109)錯誤，這些錯誤導致證書身份驗證無法正常工作。

在埠上繫結SSL證49443

要在埠上繫結SSL證書，請執行以49443操作：

1. 使用以下命令刪除連線埠上任何現49443的SSL憑證繫結：

```
netsh http delete sslcert hostnameport=


     :49443
```

2.使用以下命令在啟用客戶端證書協商的情況下建立新繫結：

```
netsh http add sslcert hostnameport=


     :49443 `
    certhash=


       `
    appid="{5d89a20c-beab-4389-9447-324788eb944a}" `
    certstorename=MY `
    clientcertnegotiation=enable `
    verifyclientcertrevocation=disable
```

3.使用以下命令驗證是否已啟用客戶端證書協商：

```
netsh http show sslcert hostnameport=
```

```
: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)” -ForegroundColor Red
```

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:
Write-Host “Moved $($bad.Count) cert(s) from Root to Intermediate CA store” -ForegroundColor Green
```

3.通過運行以下命令，驗證根儲存中是否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 7：Schannel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。
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SystemCertificatesstore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中已經存在CA證書：

```
$exists = Test-Path “HKLM:\caThumbprint”
```

如果未找到證書，請將其匯入到LocalMachinestore:

```
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 Metadata”}).FullUrl
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。
2. 將<your-adfs-server>替換為ADFS伺服器的主機名。
3. 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adfs-metadata.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Identity provider 名稱。
3. 輸入域(例如，company.com)。
4. （可選）如果需要，開啟Enable single logout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。

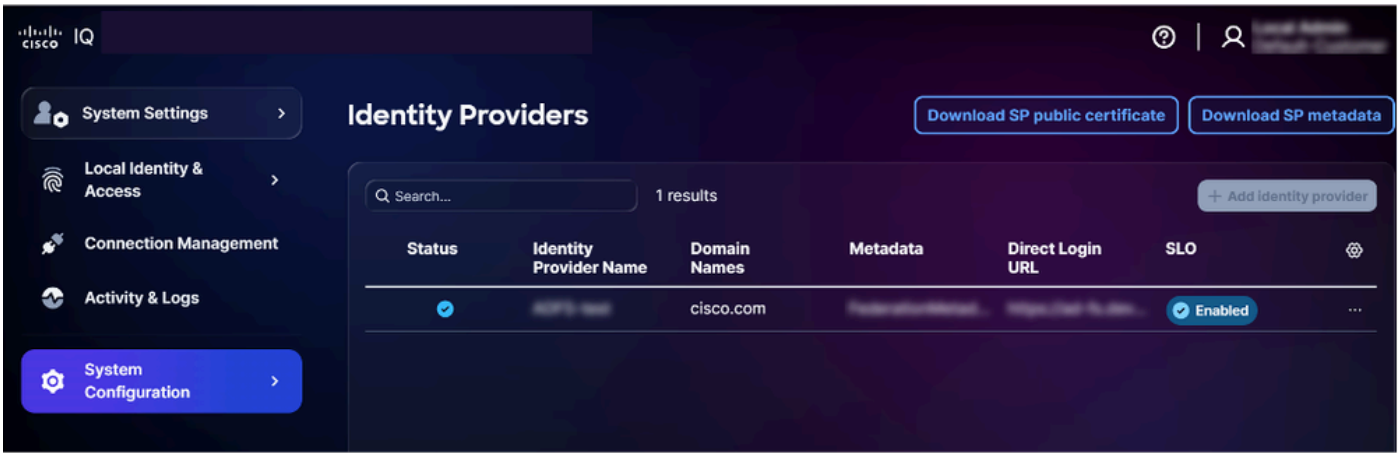
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = “(&(objectClass=group)(cn=Role - CXIQ*))”
$searcher.PropertiesToLoad.Add(“distinguishedName”) | Out-Null
$searcher.PropertiesToLoad.Add(“cn”) | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties[“distinguishedname”]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

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

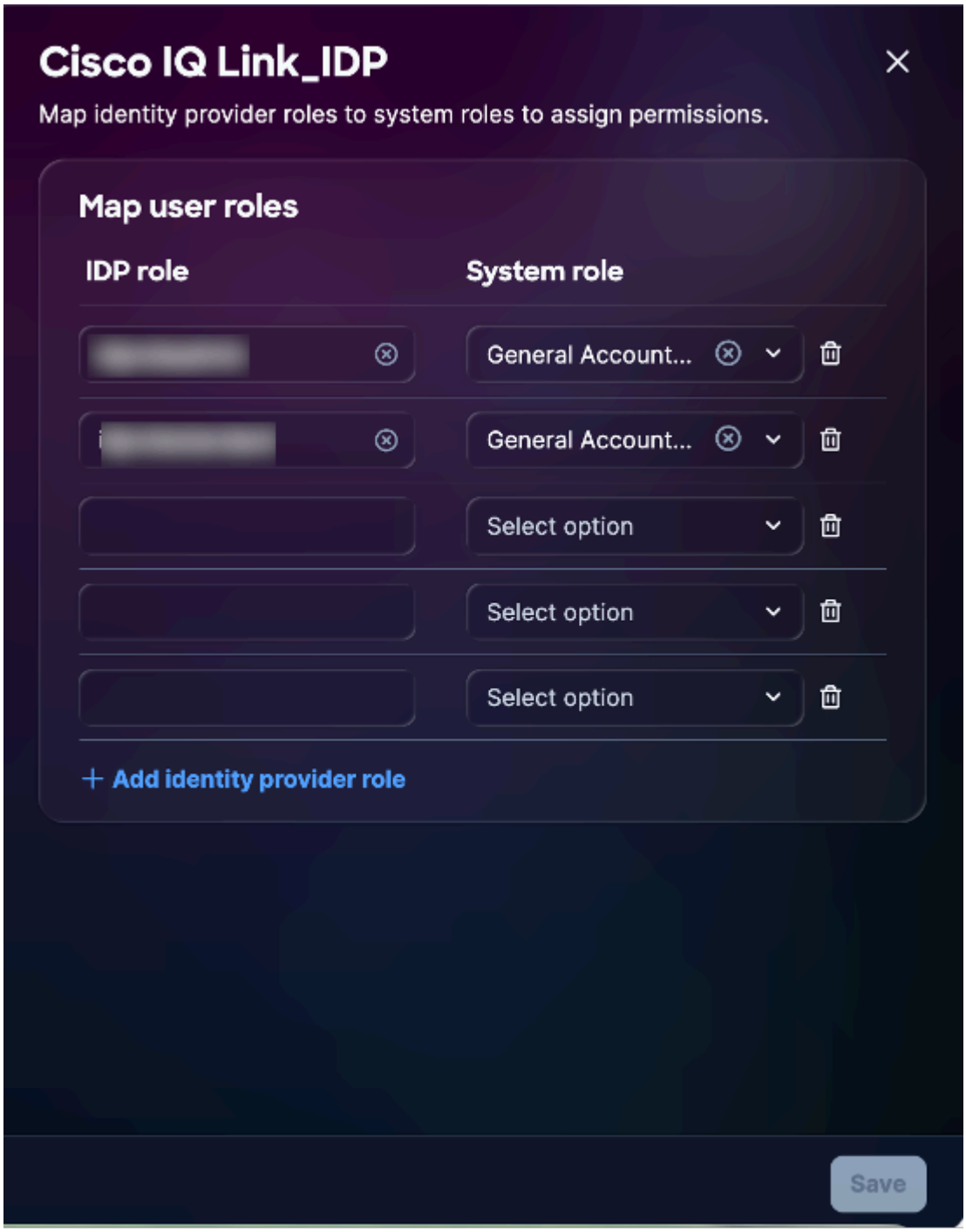
如果未列出所需的組，則必須在帳戶管理員在AD中建立這些組，然後才能完成ADFS角色對映。

要配置角色對映，請執行以下操作：



對映角色

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。



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）而不是完整的域名。

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(有關詳細資訊，請參閱配置基於證書的身份驗證下的「在客戶端電腦(macOS)上匯入使用者證書」(Importing the User Certificate on Client Machine， macOS)。

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。瀏覽器會提示輸入憑證。
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. 驗證登入是否成功。

附註：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 8：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 • 組屬性錯誤:必須是 http://schemas.xmlsoap.org/cla ims/Group • 使用者不在AD組中
解密失敗	在日誌中「無法解密斷言」	檢查ADFS證書配置的配置
登入回圈	停滯在身份驗證或登入環路中	• 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

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 - Stage” | Select-Object EncryptionCertificate | Format-List
```

- 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 - Stage” | 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，同時支援基於密碼的身份驗證和PKI/基於證書的身份驗證(CBA)。

配置用於SSO的Entra ID SAML的先決條件

- Microsoft 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 9：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

專案	說明	範例
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. 選擇整合您在相簿中找不到的任何其他應用程式（非相簿）。
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Virtual Appliance(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的單點登錄螢幕中。

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：

1. 在企業應用程式中，導航到單點登入，然後選擇SAML。

2. 在基本SAML配置部分中，按一下編輯，然後輸入以下內容：

   a. 識別符號（實體ID）:<YOUR-CIQ-FQDN>

   b. 回覆URL(ACS URL):https://<YOUR-CIQ-FQDN>/saml/acs

   c. 登入URL:https://<YOUR-CIQ-FQDN>/saml/login

   d. 註銷URL:https://<YOUR-CIQ-FQDN>/saml/logout

3. 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。

4.要配置SAML屬性和宣告，請在屬性和宣告部分中按一下編輯。

5.配置以下宣告：

表 10：所需的SAML宣告

領款申請	源屬性	名稱空間
唯一使用者識別符號（名稱ID）	user.userprincipalname	(預設)
電郵地址	user.mail	http://schemas.xmlsoap.org/ws/2005/05/identity/claims

領款申請	源屬性	名稱空間
givenname	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
姓氏	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
名稱	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
組	user.assignedroles	（空 — 清除名稱空間）

附註：對於groups聲明：
— 使用user.assignedroles作為源 — 不 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)
— 請勿向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. 導航到身份 > 應用 > 應用註冊。
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、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，轉到單一登入 > SAML簽名證書部分。
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. 在「設定」(Set)部分中記下以下值：

- 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Enable single logout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 11：系統角色

系統角色	IDP角色（應用角色值）	說明
普通帳戶管理員	CXIQ管理員	所有操作的完全許可權
常規帳戶檢視器	CXIQ開發人員	只讀訪問
常規帳戶檢視器	CXIQ檢視器	只讀訪問

附註：使用完全在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Entra ID SAML應用程式下的「配置應用程式角色」)。

3.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. 驗證後，確認系統是否將您重新導向回/saml/acs，以及是否顯示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 successful|Extracted group|To
```

預期輸出

```
SAML 2.0 compliant authentication successful for user: user@domain.com with full name: N/A and 1 groups
Extracted group: CXIQ Admins (original: CXIQ Admins)
Total groups extracted: 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

- Windows Server with AD Certificate Services(CS)with Enterprise CA configured（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 -P "


     "
```

- 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. 查詢CA證書並按一下「獲取資訊」。

3. 在「信任」下，設定為「始終信任」。

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. 導覽至Protection > Security > Certificate authorities。
3. 按一下Upload，然後選擇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Configure下，將保護級別設定為Single-factor authentication。

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

這會將證書的使用者替代名稱中的UPN對映到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登入頁面上，輸入使用者的電子郵件並按一下下一步。

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 12：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Entra ID SAML應用下的配置SAML單點登入)。 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。確保將使用者分配給應用角色(有關更多詳細資訊，請參閱配置Entra ID SAML應用程式下的「將使用者分配給應用角色」(Assigned Users to App Roles)。
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Entra ID SAML應用程式下的配置應用程式角色)。
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，請參閱實驗室環境的CRL解決方法)。
未提示證書	證書不在金鑰鏈中、	驗證是否已在macOS金鑰鏈訪問中匯入使用

問題	原因	修正
	CA不受客戶端信任或未啟用CBA	者證書(有關詳細資訊，請參閱配置基於證書的身份驗證下的匯入客戶端電腦上的使用者證書(macOS))，已使用所需設定在Entra ID中啟用CBA(有關詳細資訊，請參閱配置基於證書的身份驗證下的在Entra ID身份驗證方法中啟用CBA)並重新啟動Chrome以應用更改。
SAML斷言已過期	系統之間的時鐘偏差	在外掛配置中增加clock_skew_seconds(預設值為300，使用30000表示實驗)。
VA中的「未完成」狀態	尚未配置角色對映	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。由於它自簽名時沒有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中新增身份提供程式
- 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，其中包含UPN匹配的Entra ID使用者
- 將使用者證書匯出為PFX並在客戶端電腦上安裝
- 信任客戶端電腦上的CA證書

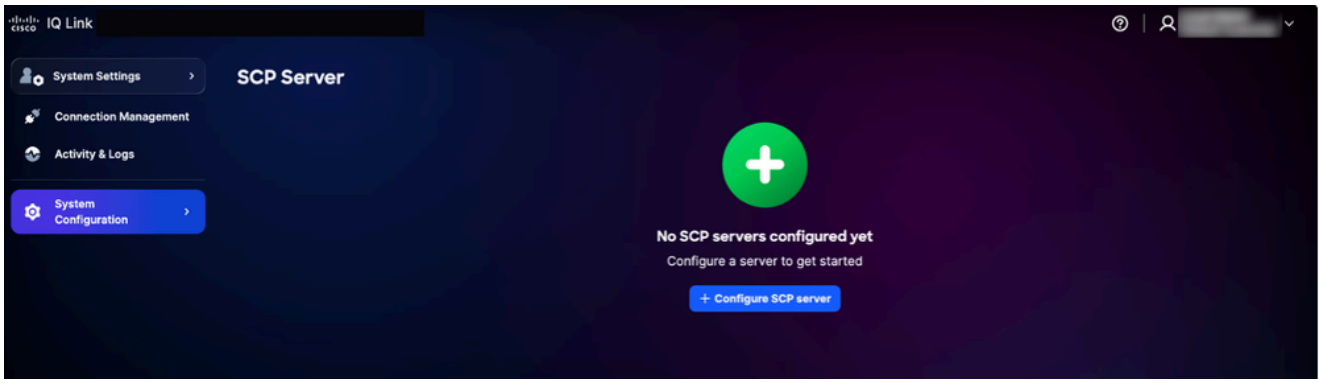
- 在Protection > Certificate authorities下將CA根證書上載到Entra ID
- 在身份驗證方法中啟用CBA
- 配置使用者名稱繫結(PrincipalName和userPrincipalName)
- 驗證CBA登入是否端到端工作

新增SCP伺服器

此安全複製協定(SCP)伺服器是匯入升級檔案的先決條件，這些檔案對於新增、升級或修補思科IQ安裝至關重要。

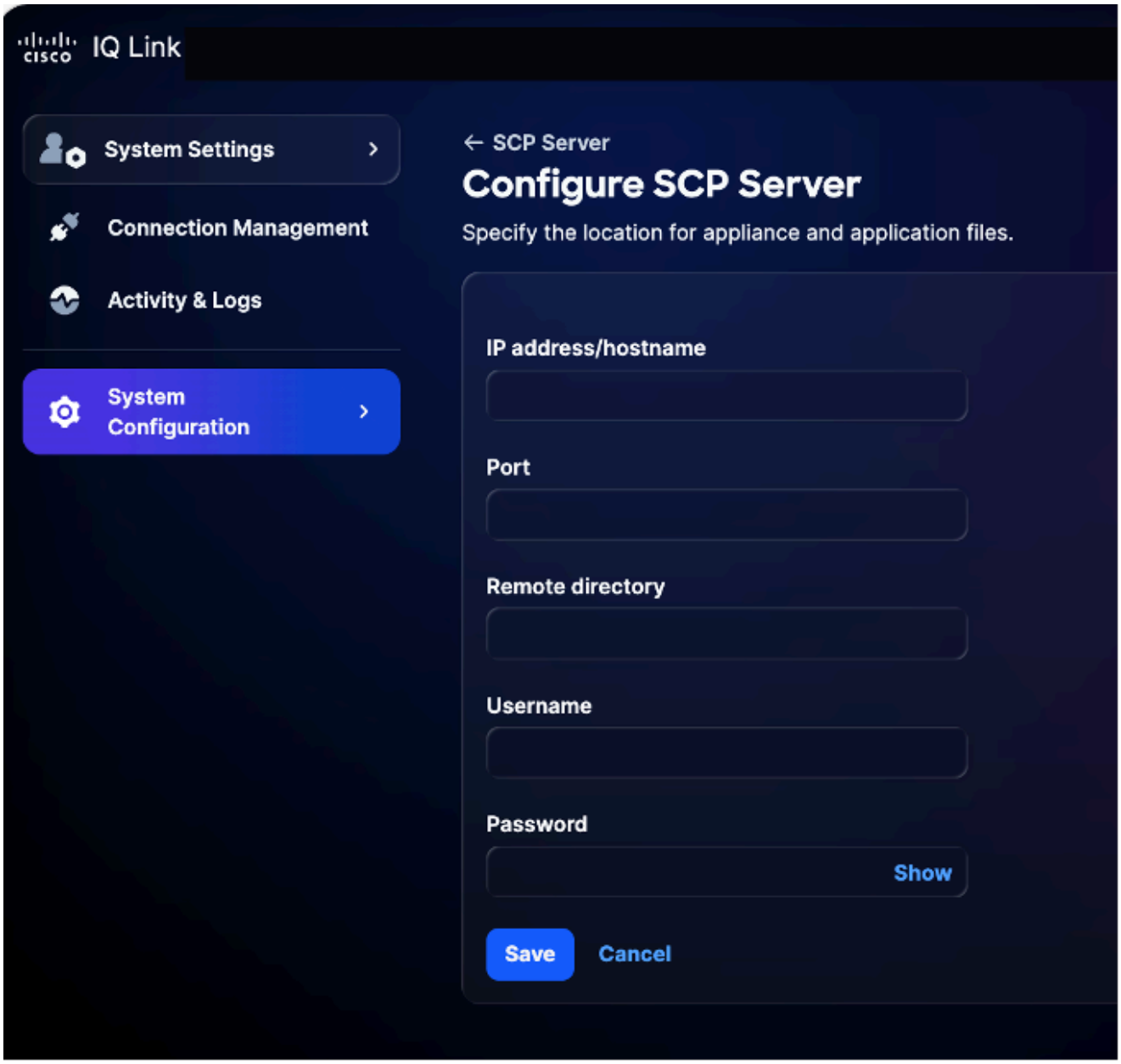
新增SCP伺服器的步驟：

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。



配置SCP伺服器

3. 輸入IP地址/主機名。
4. 輸入埠號。
5. 輸入Remote directory。
6. 輸入Username。
7. 輸入密碼。
8. 按一下「Save」。系統會顯示確認。

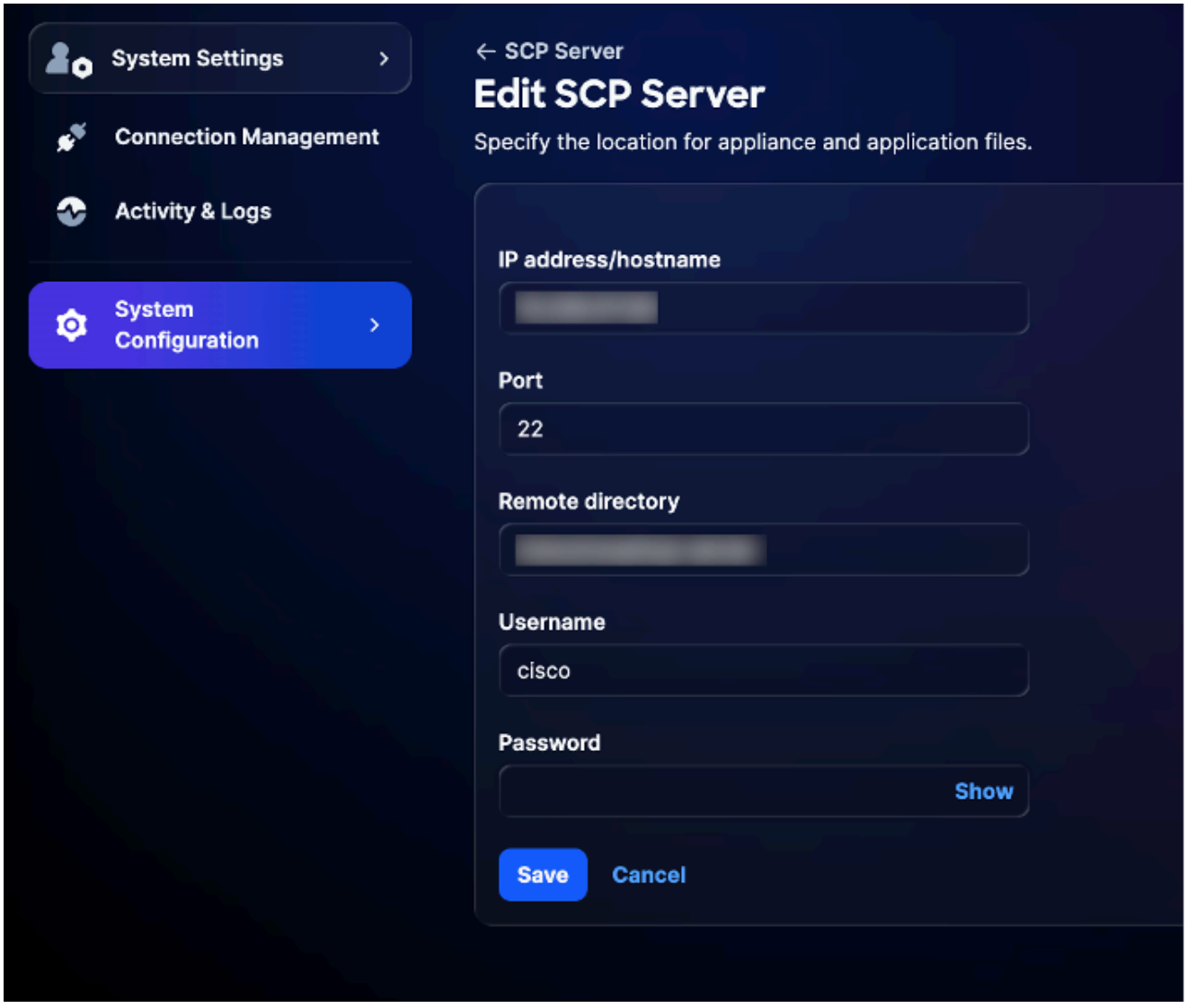
編輯現有SCP伺服器

要編輯現有SCP伺服器，請執行以下操作：

1. 導航到SCP Server頁面。

SCP伺服器

2. 對於所需的現有SCP伺服器，按一下Edit。



編輯SCP伺服器

3. 根據需要修改詳細資訊。

4. 按一下「Save」。

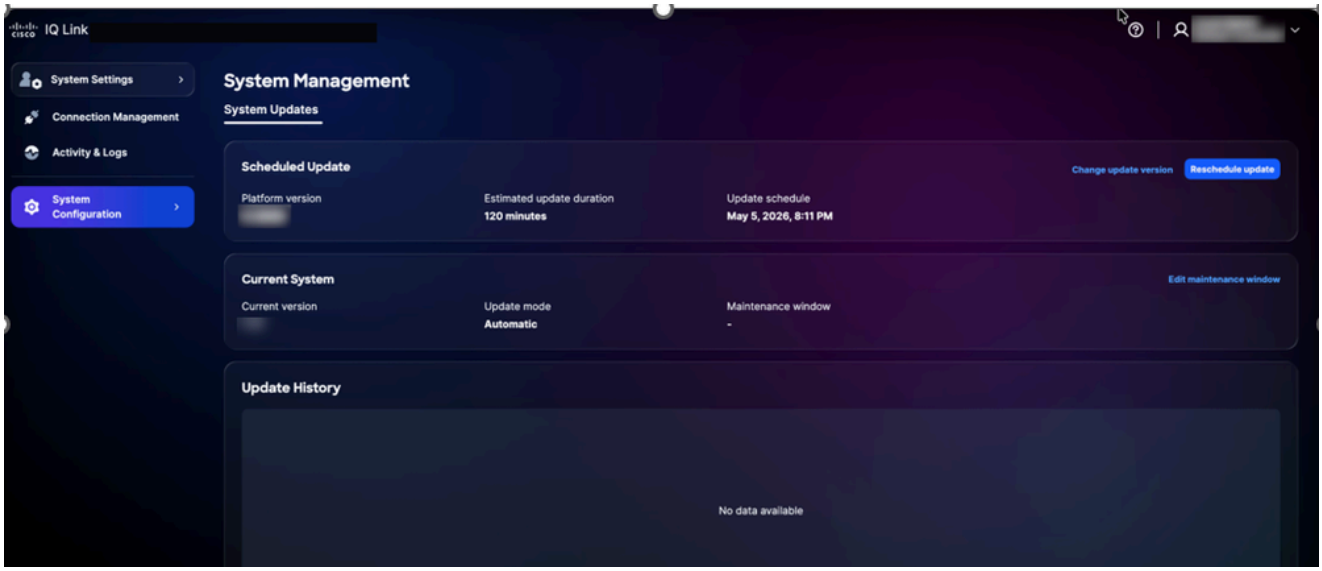
系統管理

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

重新計畫系統更新

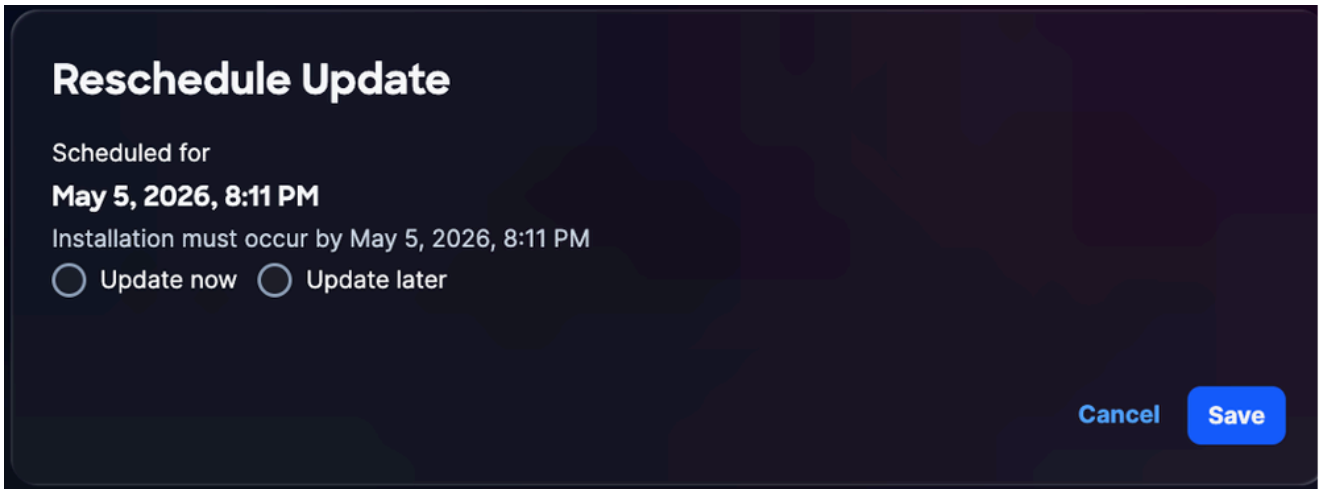
要重新計畫系統更新，請執行以下操作：

1. 在Administration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。



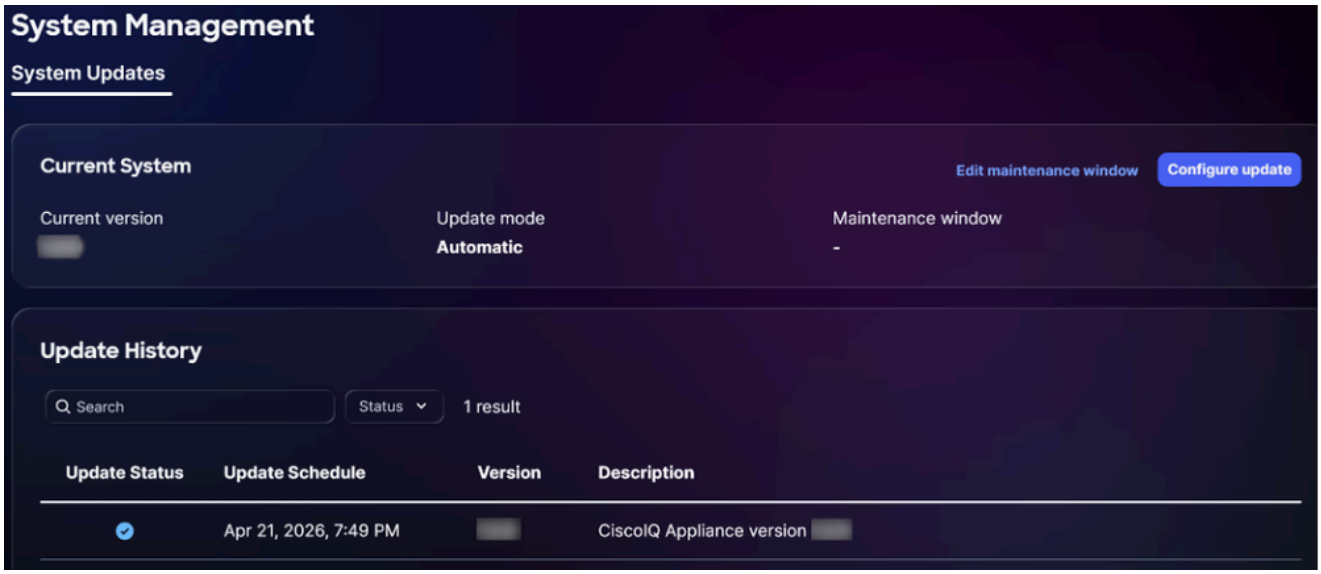
系統升級

2. 按一下Reschedule update。



重新計畫升級

3. 選擇Update Now單選按鈕以立即重新安排，或選擇Update Later單選按鈕以安排其他時間。
4. 按一下「Save」。系統會顯示一條確認消息，並且您將被重定向到系統更新首頁。

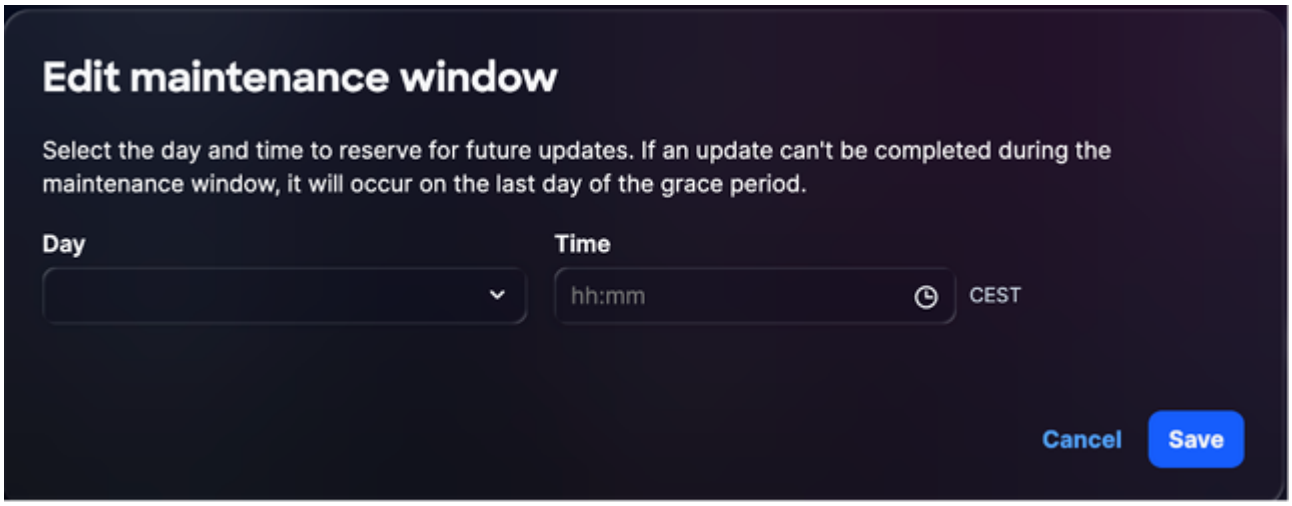


升級成功

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：

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



編輯維護視窗

2. 從Day和Time下拉選單中選擇一個選項。

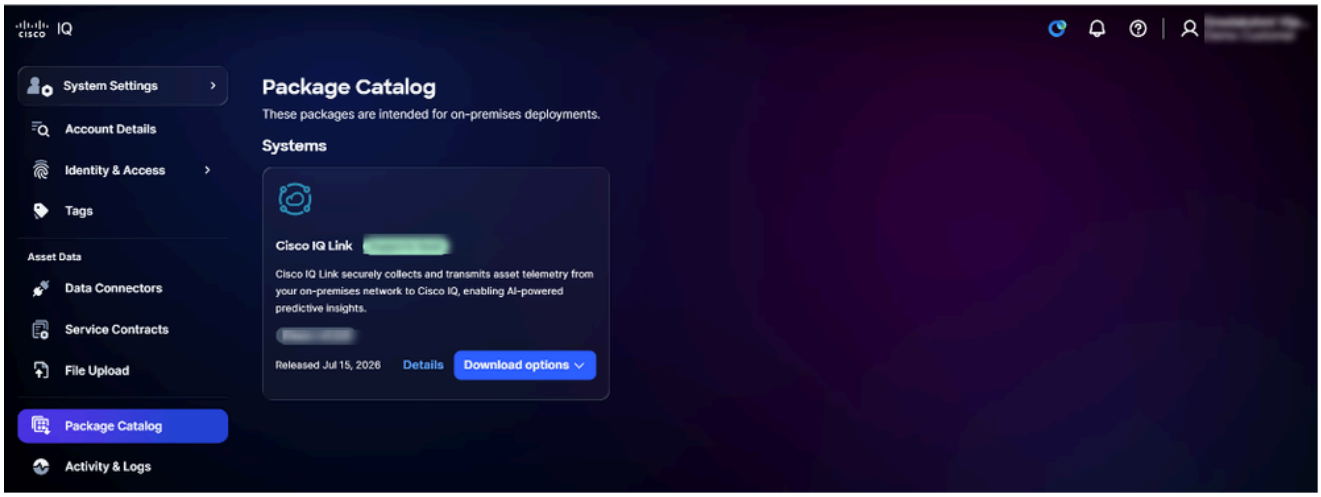
3. 按一下儲存。已成功計畫維護視窗。根據顯示的計畫觸發更新。

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，則預設為四(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，系統最多執行兩(2)次自動重試。已安排第三次嘗試，但需要手動啟動。

手動升級系統

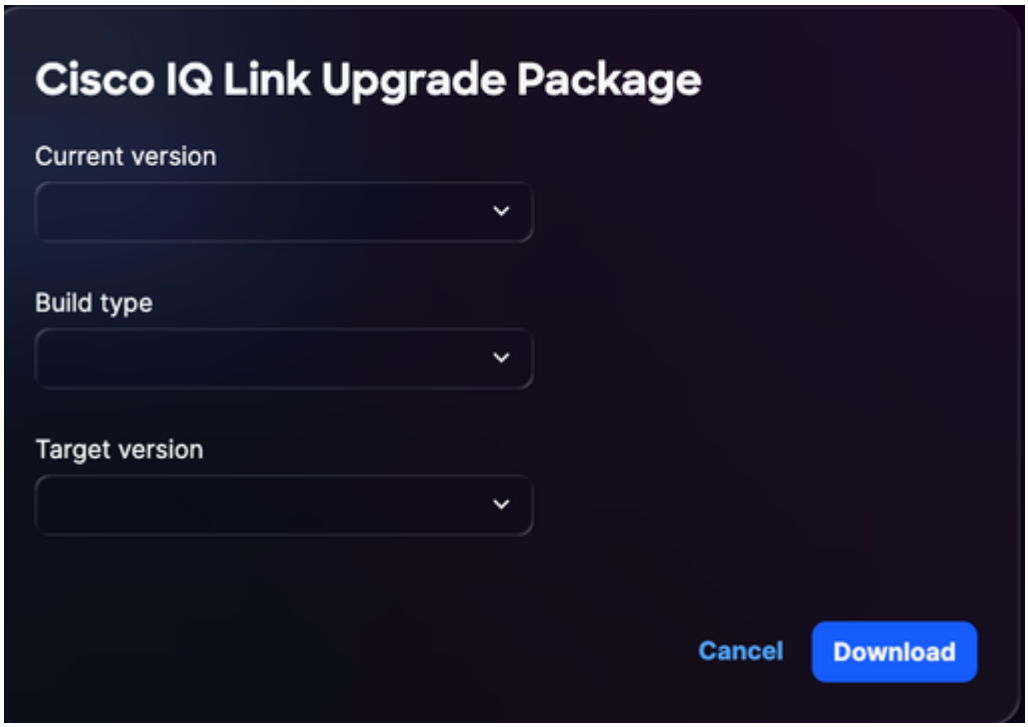
如果來自Cisco IQ SaaS的自動分發不可用或延遲，您可以直接從Cisco IQ SaaS下載升級捆綁包手動執行系統升級。要手動升級系統，請執行以下操作：

1. 登入Cisco IQ SaaS 依序選擇「Home」>「System Settings」>「Package Catalog」。



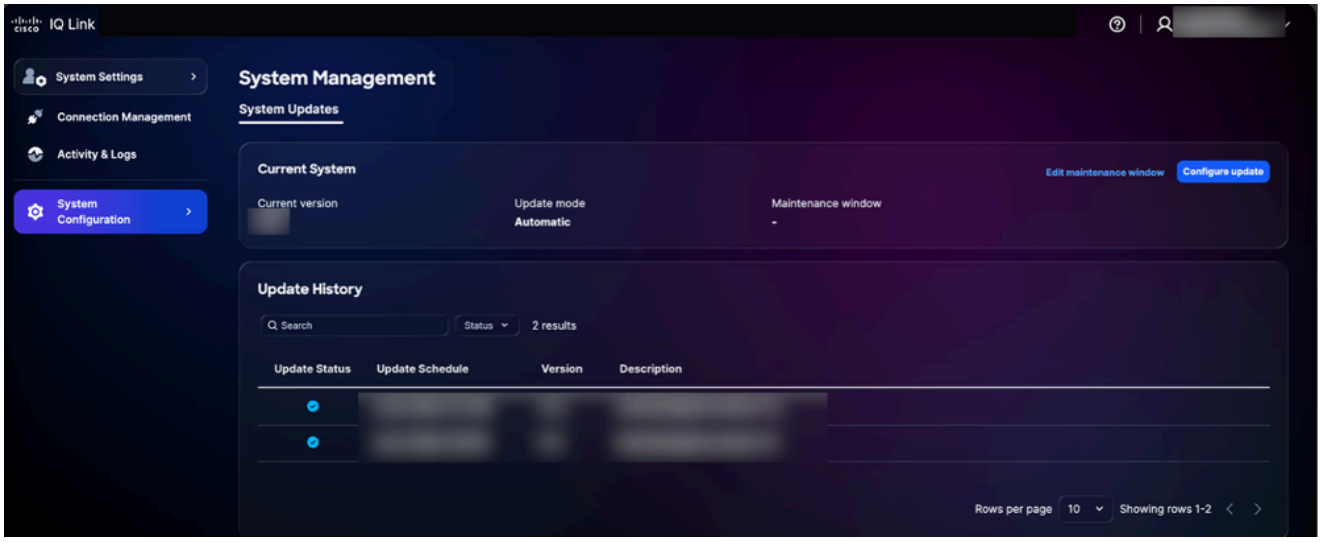
包目錄

2. 在Cisco IQ Link部分，按一下Download options > Upgrade packages。



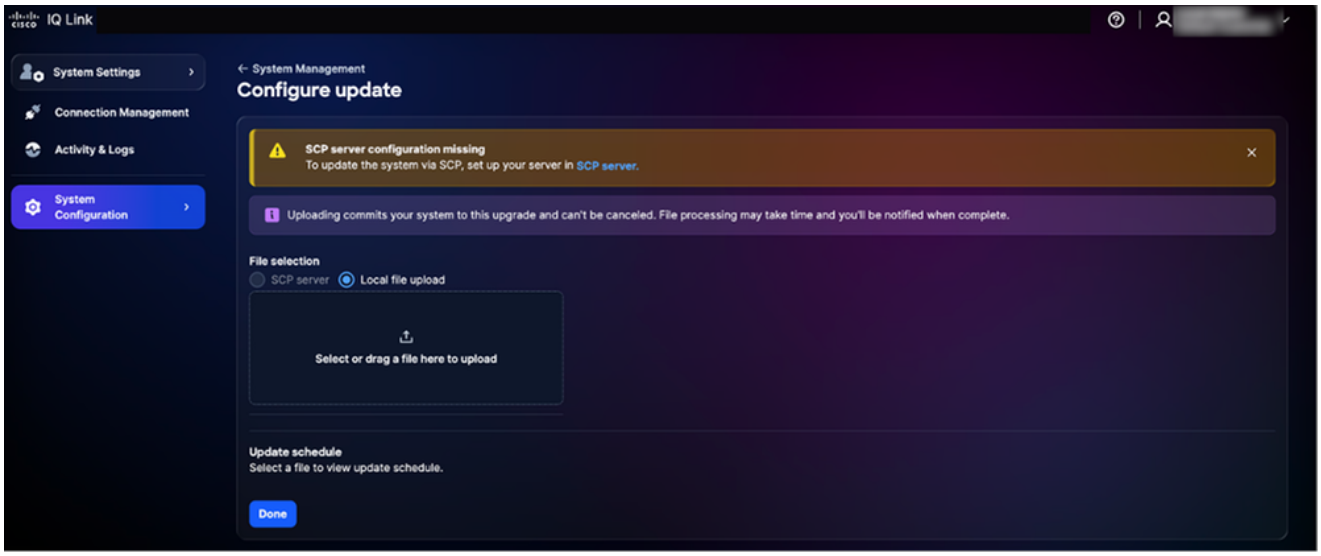
升級包

3. 從下拉選單中選擇Current version。
4. 從下拉選單中選擇Build type。
5. 從下拉選單中選擇Target version。
6. 按一下「Download」。下載升級套件組合。
7. 導航至Cisco IQ Link。
8. 在System Settings中選擇System Configuration > System Management。



配置更新

9. 按一下「Configure update」。



本地檔案上傳

10. 按一下「Local file upload」單選按鈕。

11. 選擇下載的升級套件組合檔案或將其拖到上傳欄位中。
12. 按一下「完成」。系統成功更新後，將顯示一條確認消息。

SSL證書配置

Cisco IQ中預安裝並啟用了預設自簽名證書，但您可以上傳自定義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。

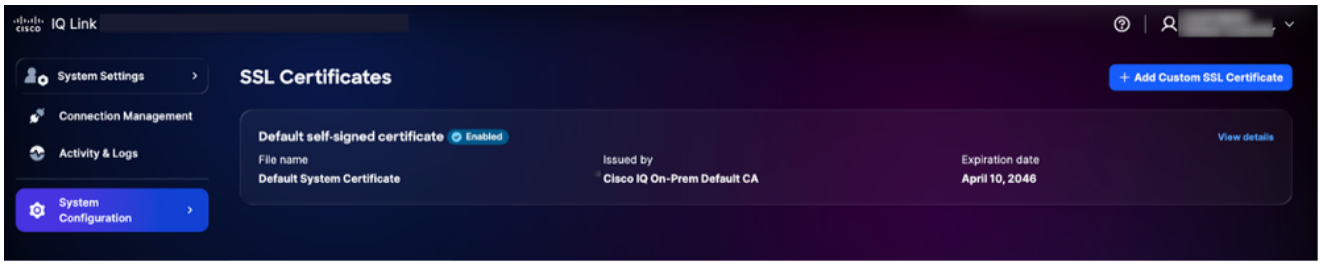
附註：證書的有效期必須至少為90天。如果證書到到期的剩餘時間少於90天，則將其視為「接近到期」。

新增、編輯或刪除SSL證書後，必須按照Single Logout Configuration中所述為Okta IDP或ADFS IDP上載新的SSL證書。

新增自定義SSL證書

新增自定義SSL證書的步驟：

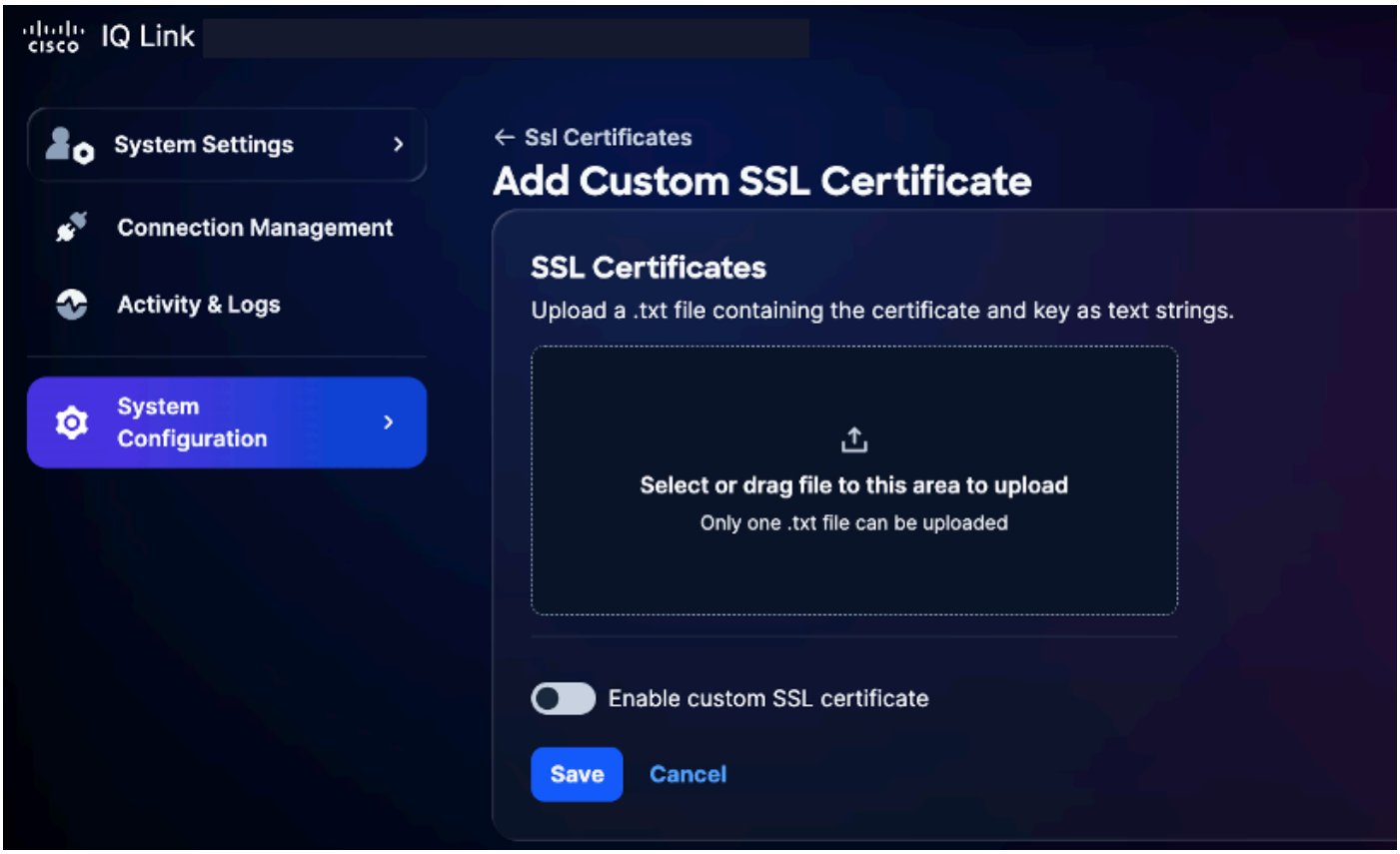
1. 在System Settings中選擇System Configuration > SSL Certificates。將顯示SSL Certificates頁面，其中列出了系統的所有SSL證書。



新增SSL證書

2. 按一下「Add Custom SSL Certificate」。

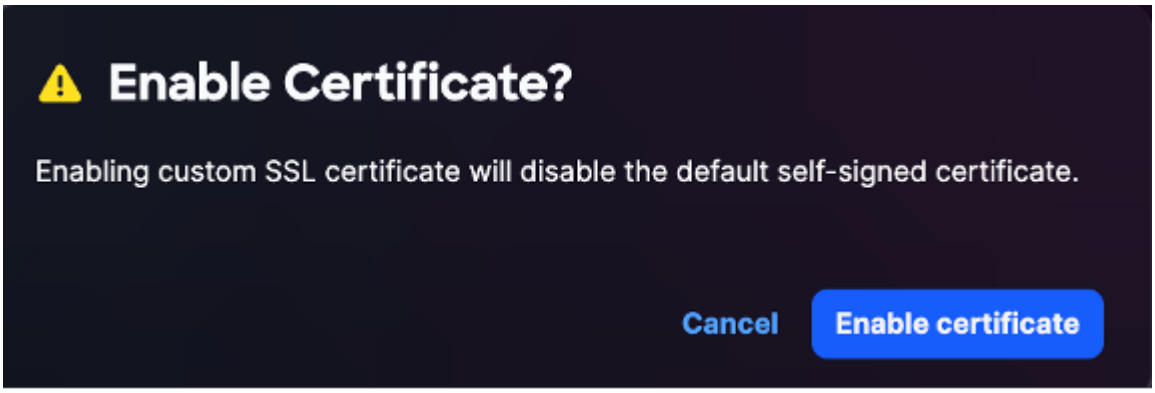
附註：
— 上傳.txt檔案，該檔案包含Privacy-Enhanced Mail-encoded證書和作為文本字串的金鑰
— 一次只能上傳一個.txt檔案
— 檔案必須同時包含證書和私鑰



上傳SSL憑證

3.將自訂SSL憑證拖放或上傳到「SSL憑證」欄位。

4.啟用Enable custom SSL certificate切換按鈕。



編輯SSL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.按一下啟用證書。

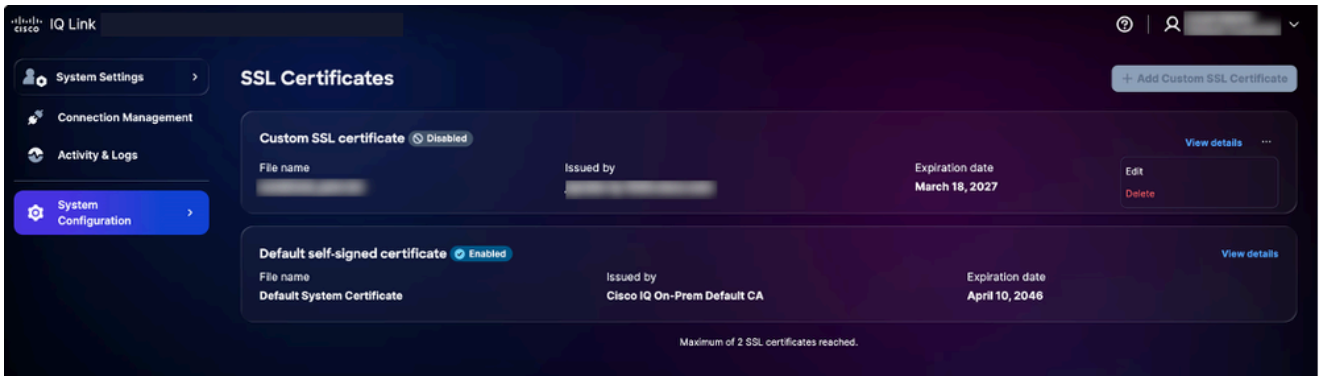
6.按一下Save。

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。



編輯SSL證書

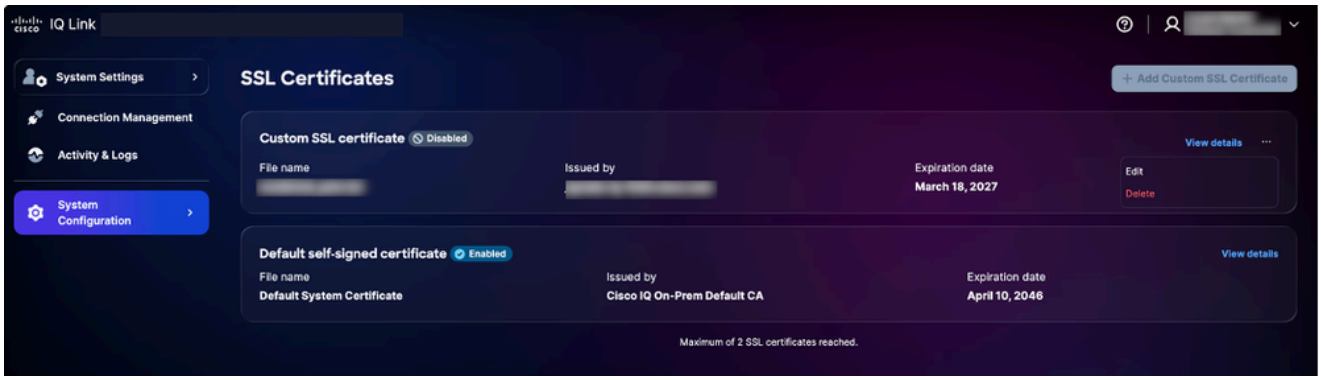
2. 選擇更多選項圖示> 編輯。系統隨即會顯示Edit SSL Certificate頁面。
3. 根據需要編輯證書詳細資訊。
4. 按一下「Save」。

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. 導航到所需的自定義SSL證書。



刪除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

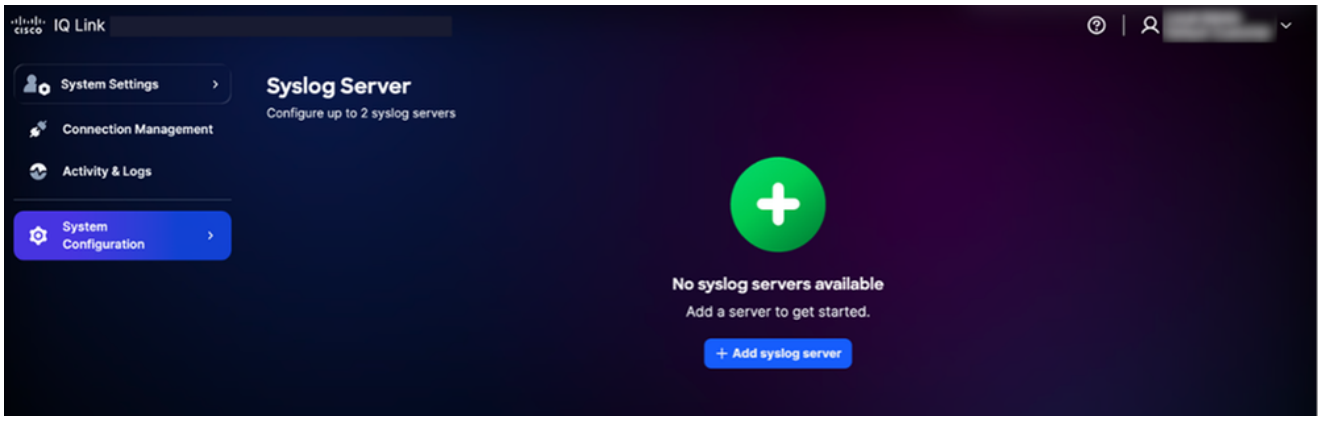
具有帳戶管理員角色的使用者可以配置外部系統日誌伺服器以匯出系統日誌。最多可以配置兩(2)台系統日誌伺服器。

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

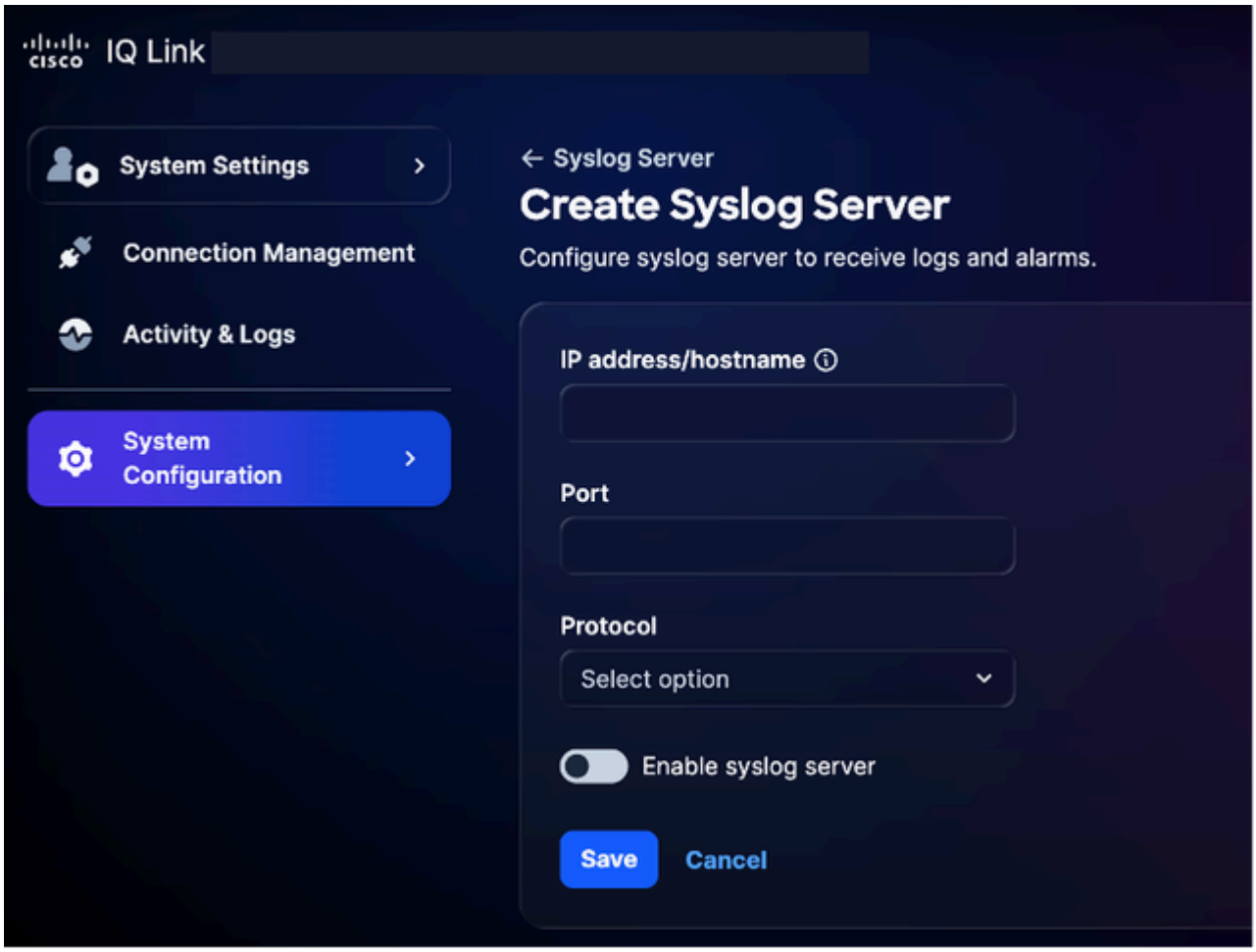
新增系統日誌伺服器：

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. 輸入埠號。

5. 從Protocol下拉選單中選擇適用的協定（例如UDP或TCP）。

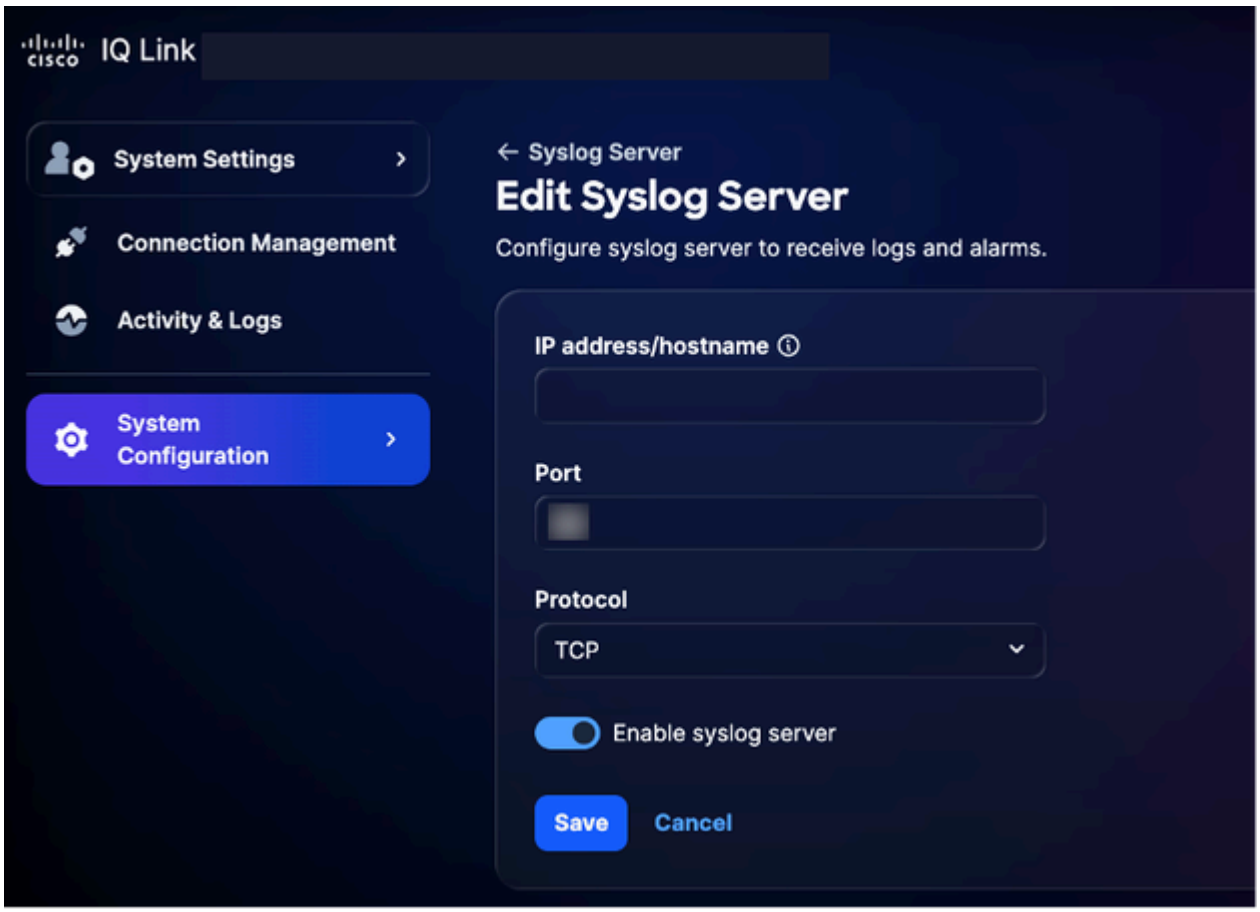
6. 開啟Enable syslog server切換按鈕。

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系統日誌服務器首頁上。

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。



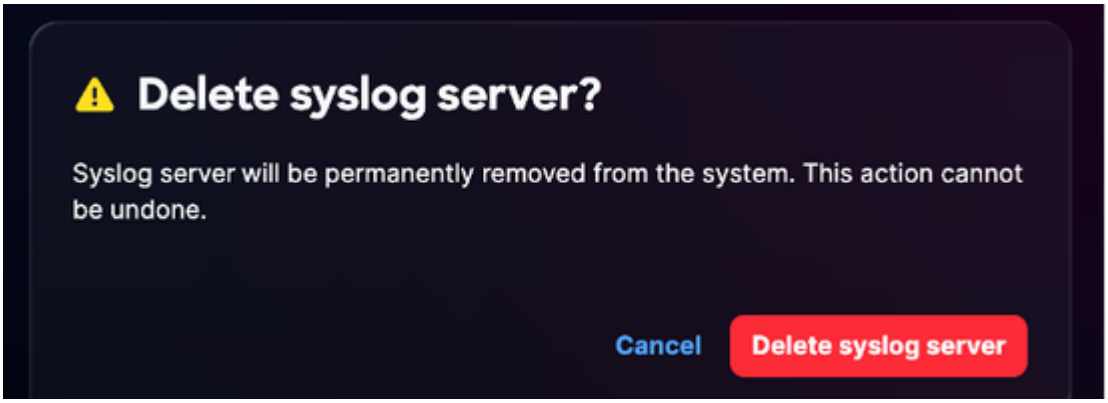
編輯系統日誌伺服器

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。

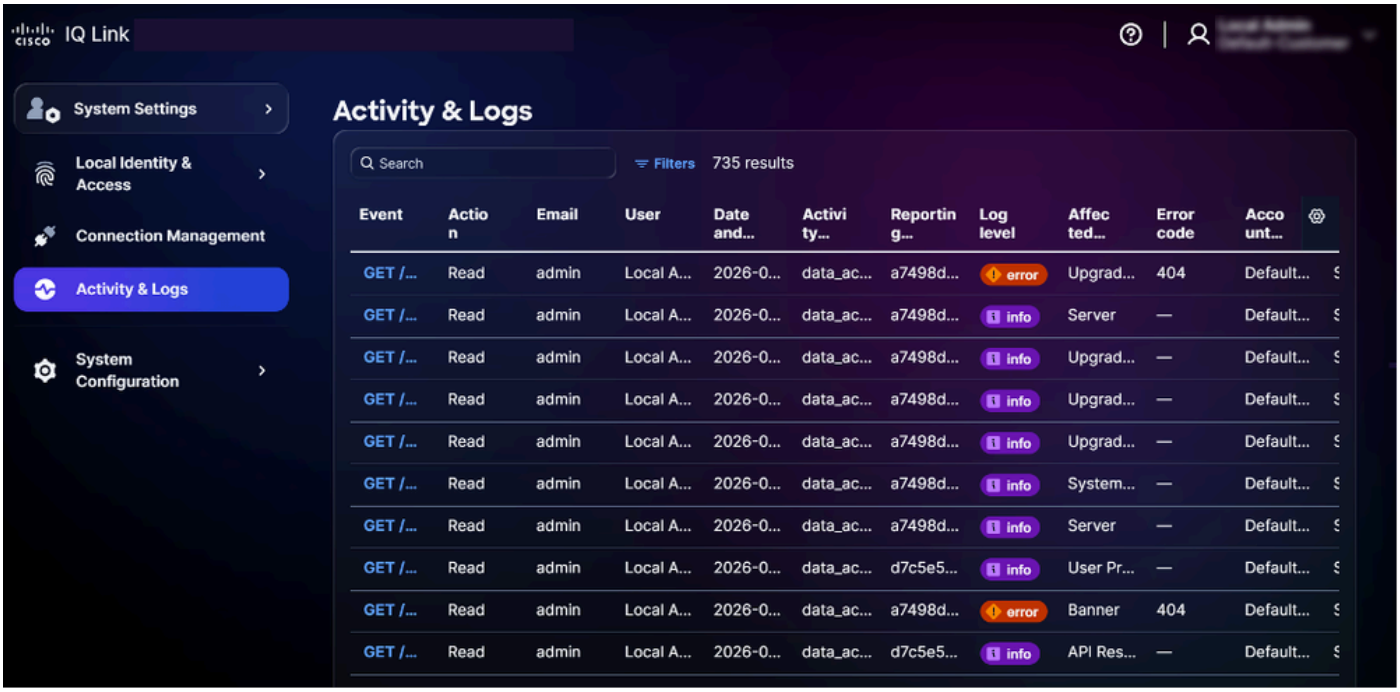


確認

3.按一下Delete syslog server。

活動和日誌

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



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：

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

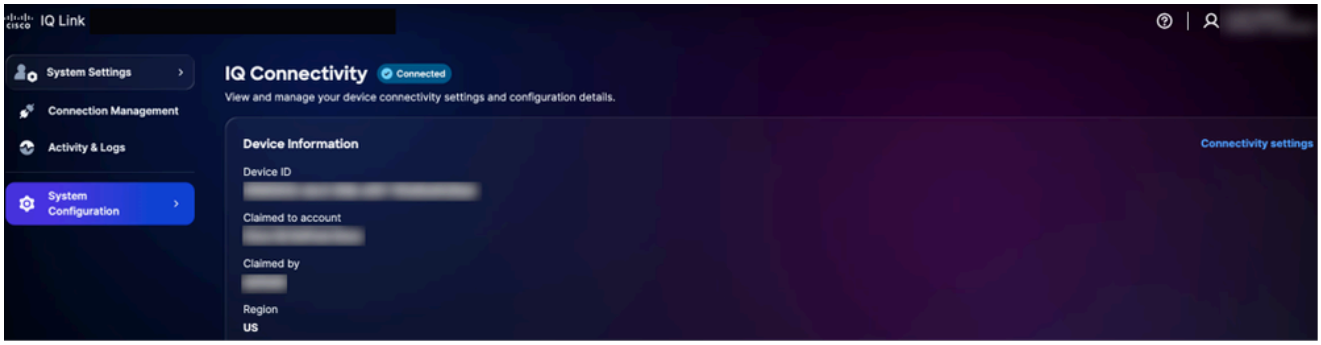
可以使用以下過濾器選項：

- 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:過濾特定錯誤代碼的日誌

IQ連線

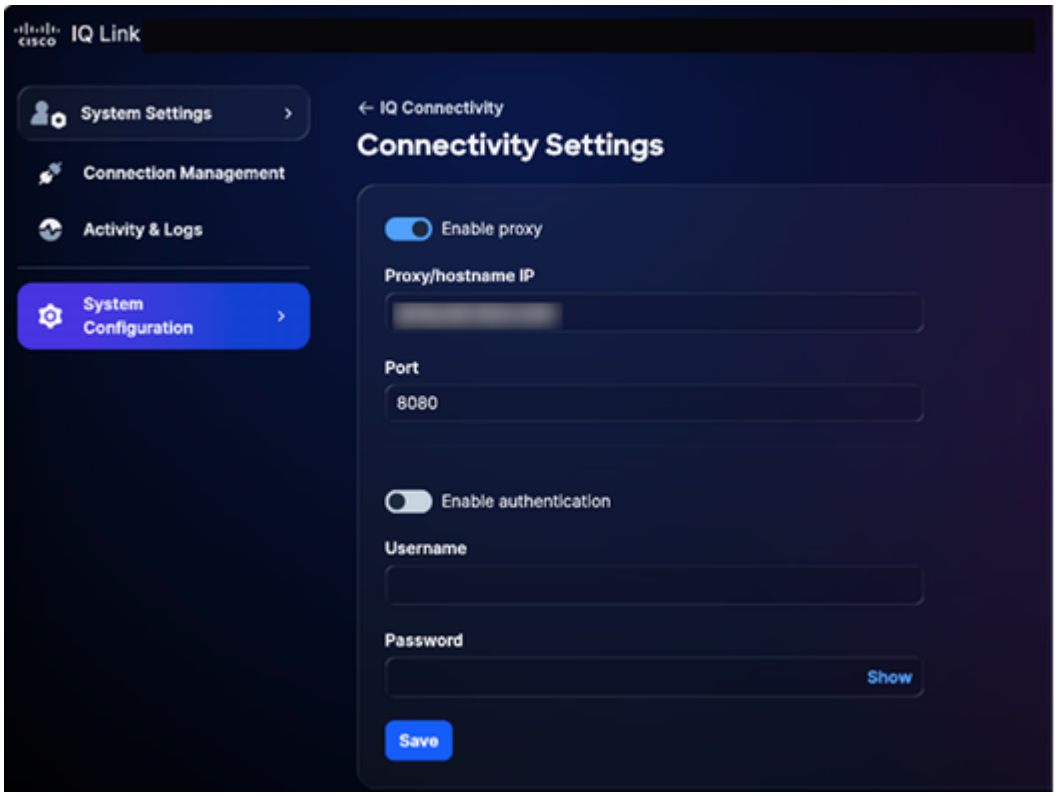
要檢視和管理裝置連線設定和配置詳細資訊，請執行以下操作：

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



IQ連線

2. 按一下Connectivity settings。



連線設定

3. 根據需要更新詳細資訊。
4. 按一下「Save」。

連線管理（資料收集）

Cisco IQ Link是用於網路資料收集的本地解決方案，旨在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。配置資料收集概述如下：

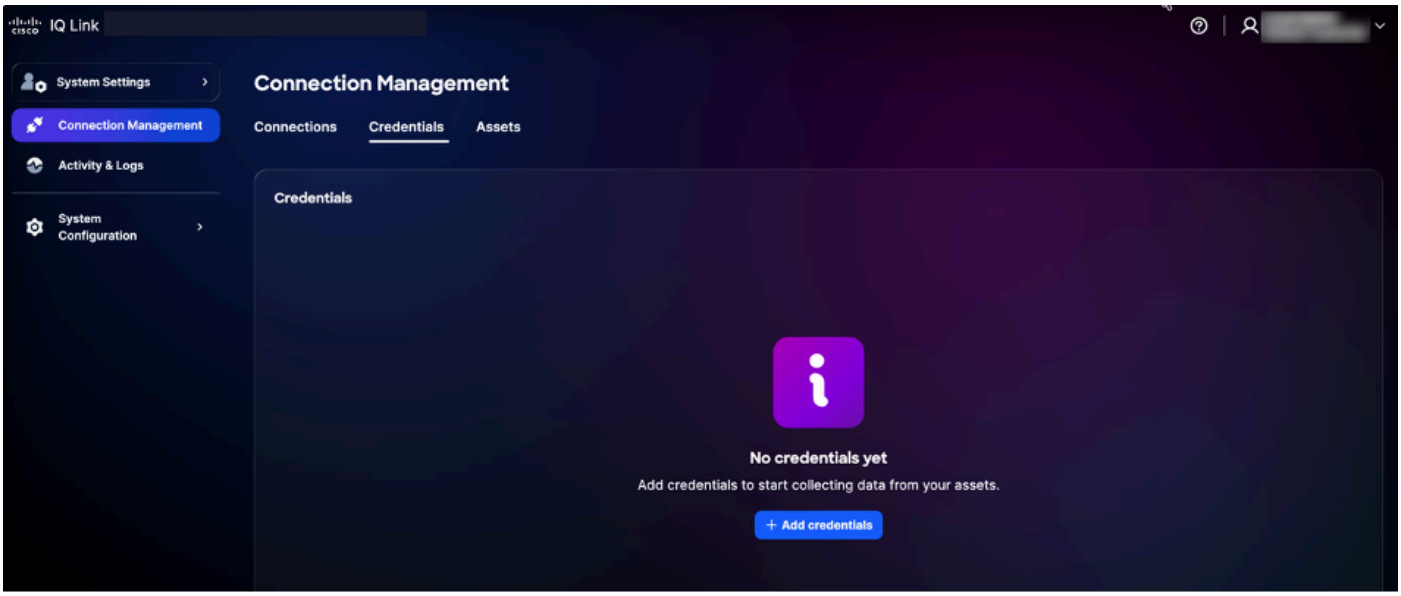
- 正在建立憑據集:建立驗證通訊協定(例如簡易網路管理通訊協定(SNMP)v1/v2c/v3)以與網路裝置通訊。通過按安全區域或位置集中憑據（例如，「SanJose-SNMPv3」），您可以在一個位置更新密碼，更改會自動傳播到所有關聯裝置。
- 將憑證對映到庫存:將憑證集與清單資產進行對映以自動執行身份驗證過程。通過建立將特定IP範圍連結到已定義的憑據集的規則，系統在資料收集期間自動應用正確的身份驗證。這消除了手動輸入錯誤，並確保隨著網路的增長您的配置保持準確。

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

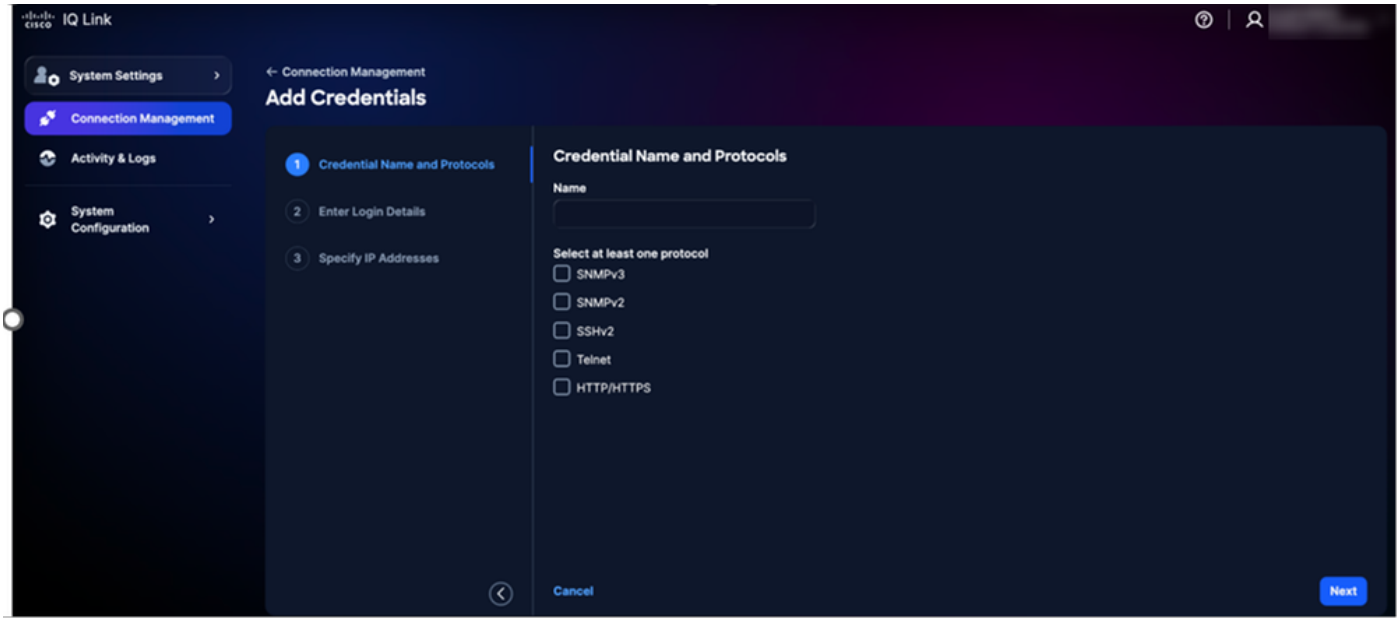
必須先新增憑據才能執行資料收集。要新增憑據，請執行以下操作：

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.按一下新增憑據。

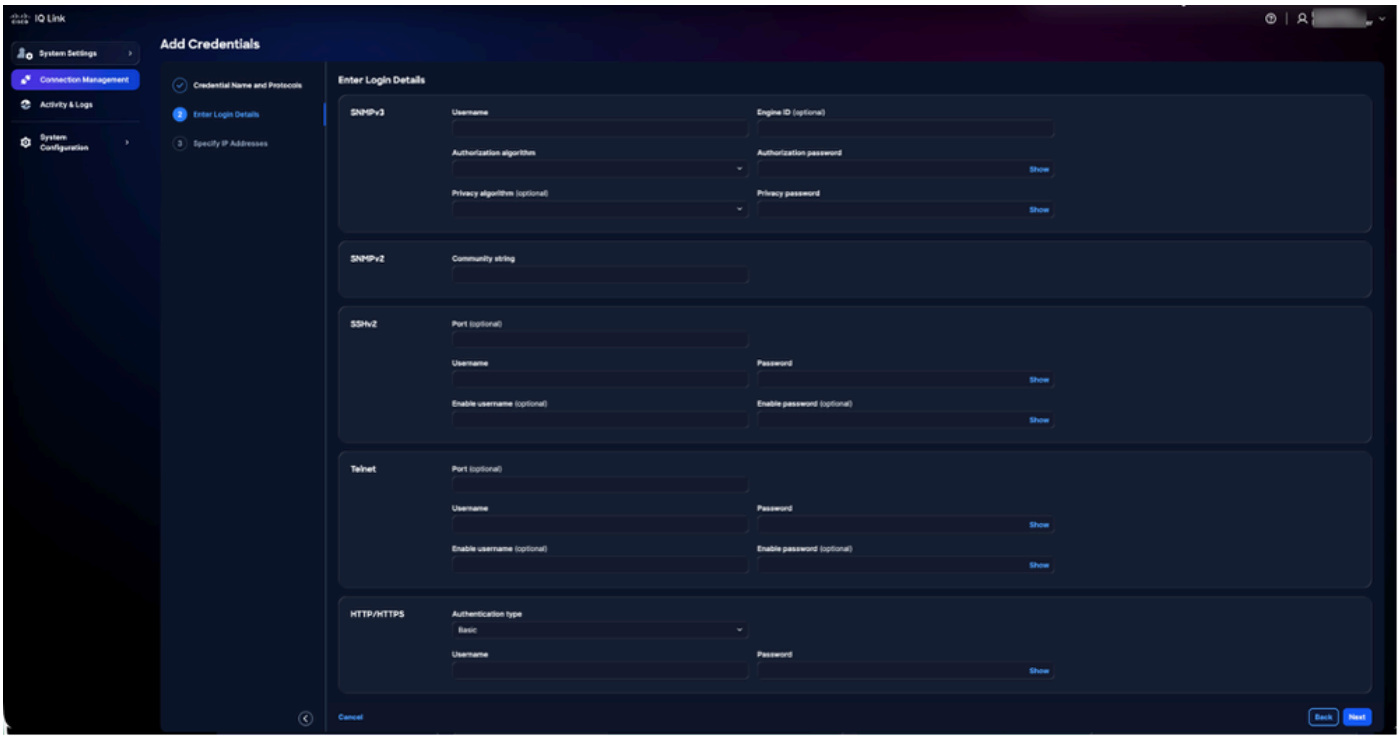


新增憑據

4.輸入名稱。

5.選中所有適用的協定覈取方塊。

6.按一下下一步。

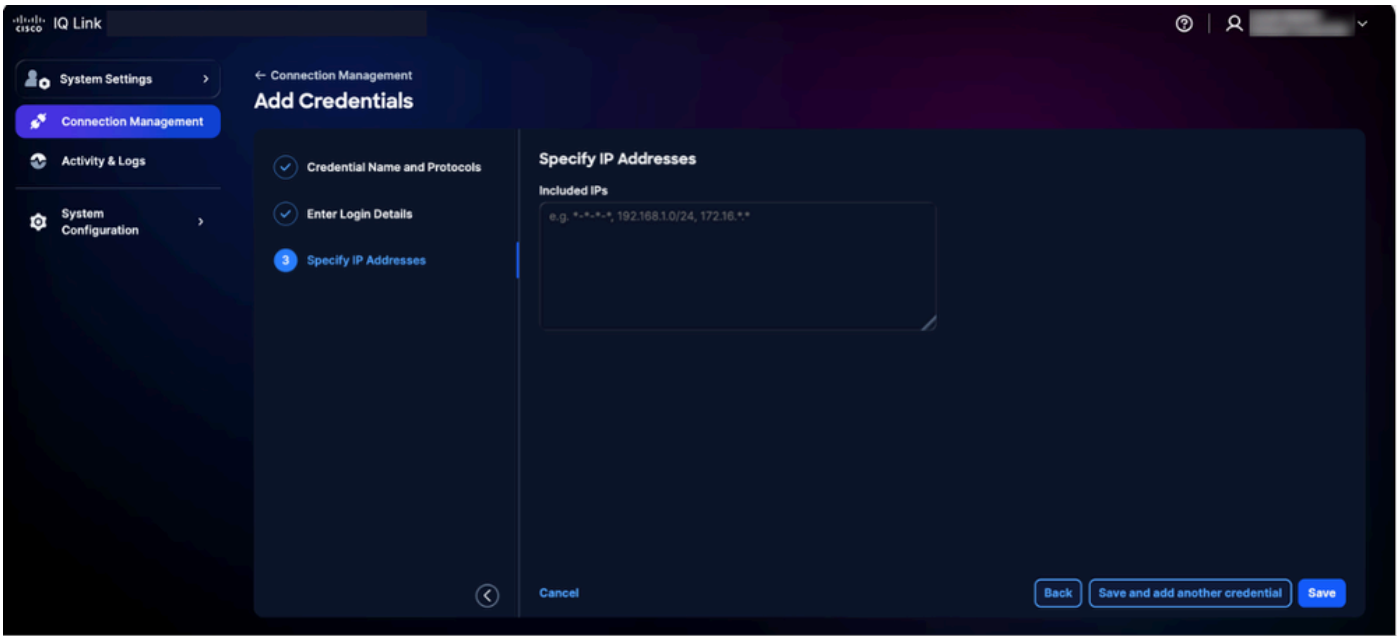


新增憑據詳細資訊

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

7.輸入每個選定協定的登入詳細資訊。

8.按一下下一步。

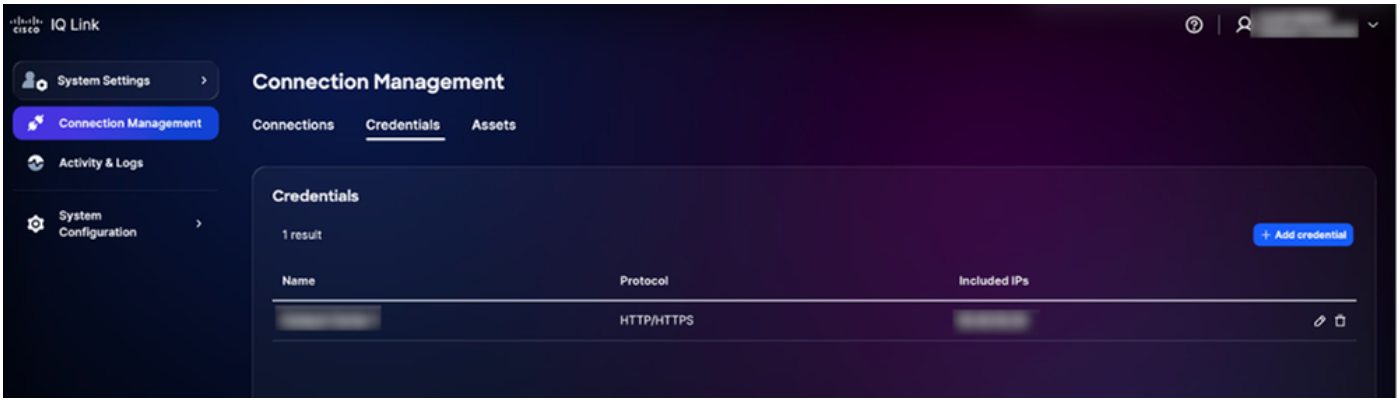


指定IP地址

9.輸入包含的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的數量；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.*（萬用字元中的最高優先順序）

    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 13：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）

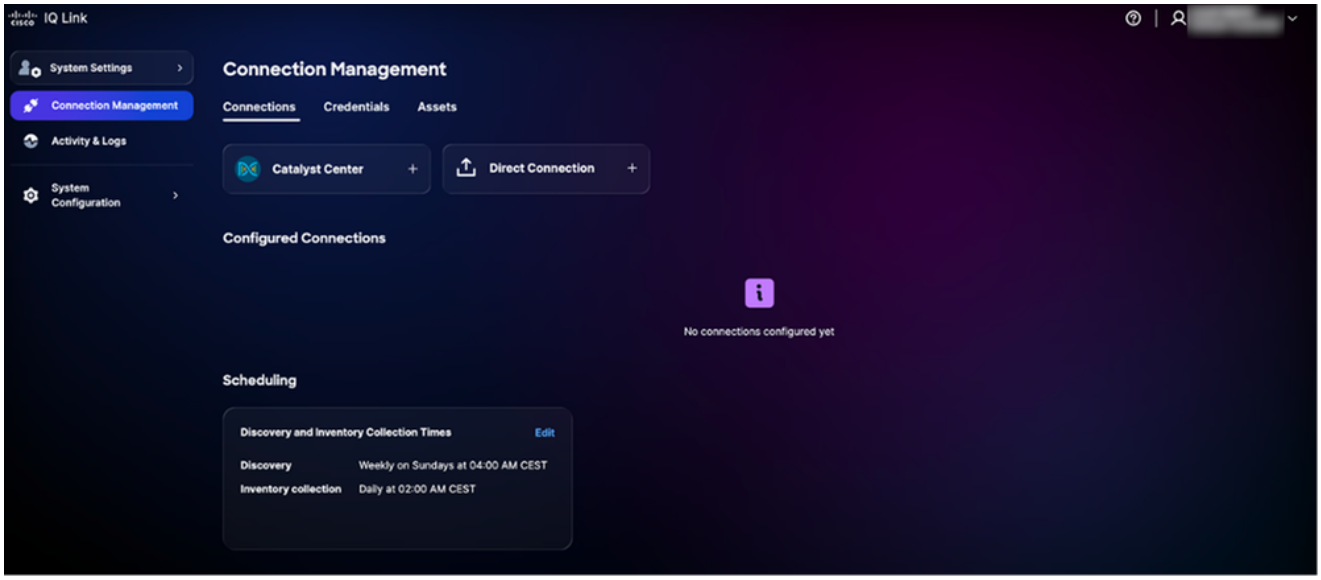
附註：如果裝置屬於多個重疊類別，系統總是選擇具有最高特異性的憑證集（換句話說，尾隨萬用字元最少）。

使用Catalyst Center進行資料收集

每個Cisco IQ Link例項最多可連線20個Catalyst Center（非集群）。

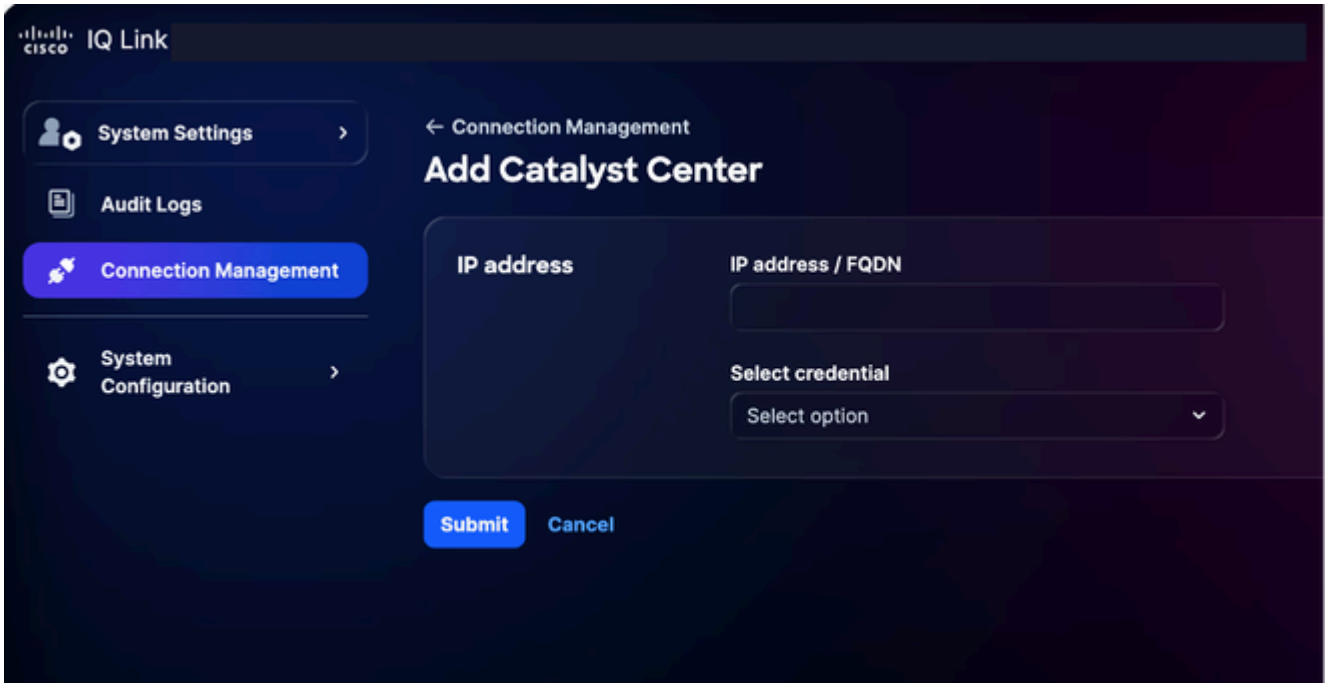
對於使用Catalyst Center進行資料收集：

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



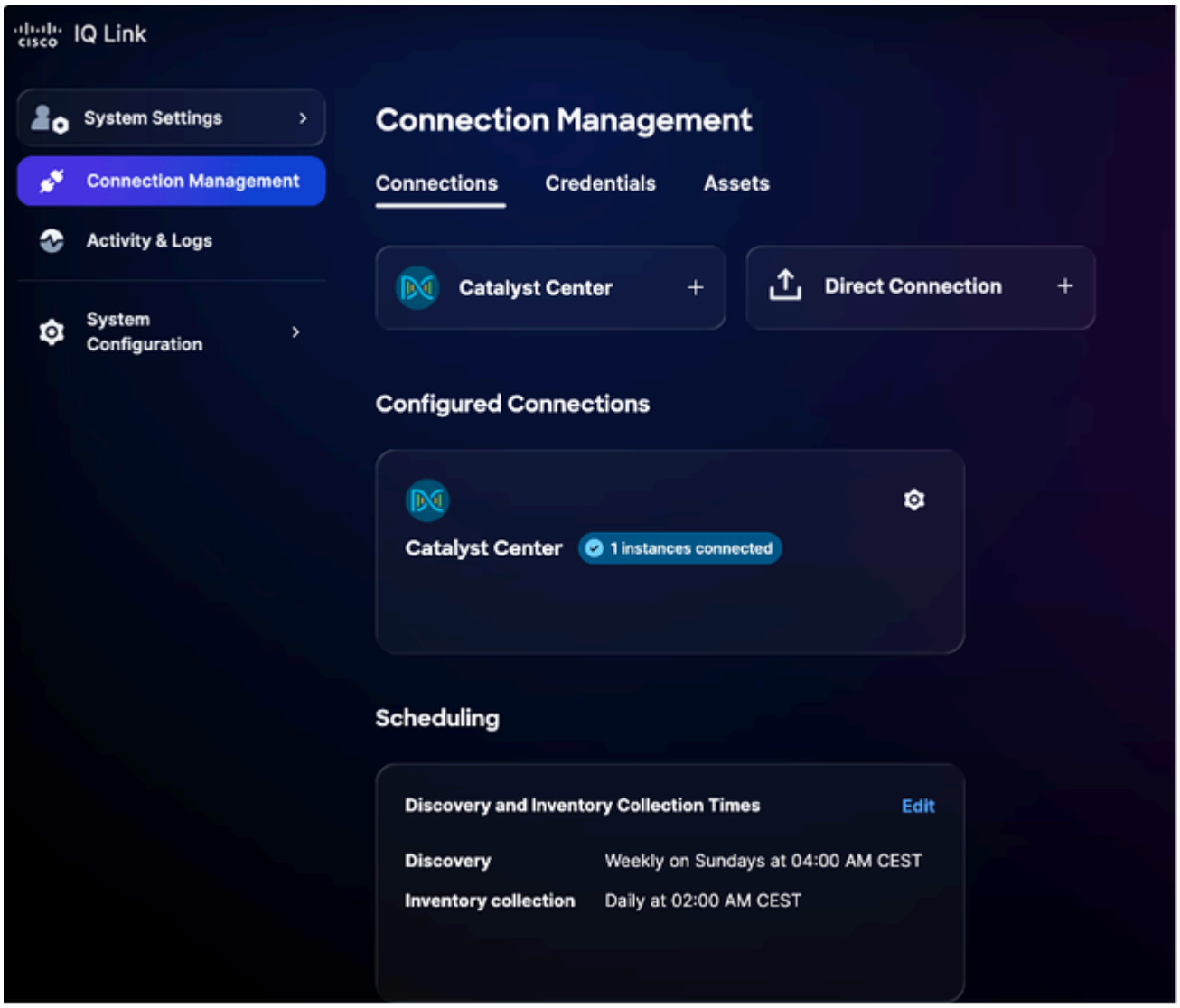
連線管理

2. 按一下Catalyst Center選項。



新增Catalyst Center

3. 輸入IP Address或FQDN。
4. 從下拉選單中選擇配置的HTTP/HTTPS憑據。
5. 按一下「Submit」。系統會顯示確認（最多可能需要75分鐘）。 您可以在Configured Connections下檢視新增的Catalyst Center。



已成功新增Catalyst Center

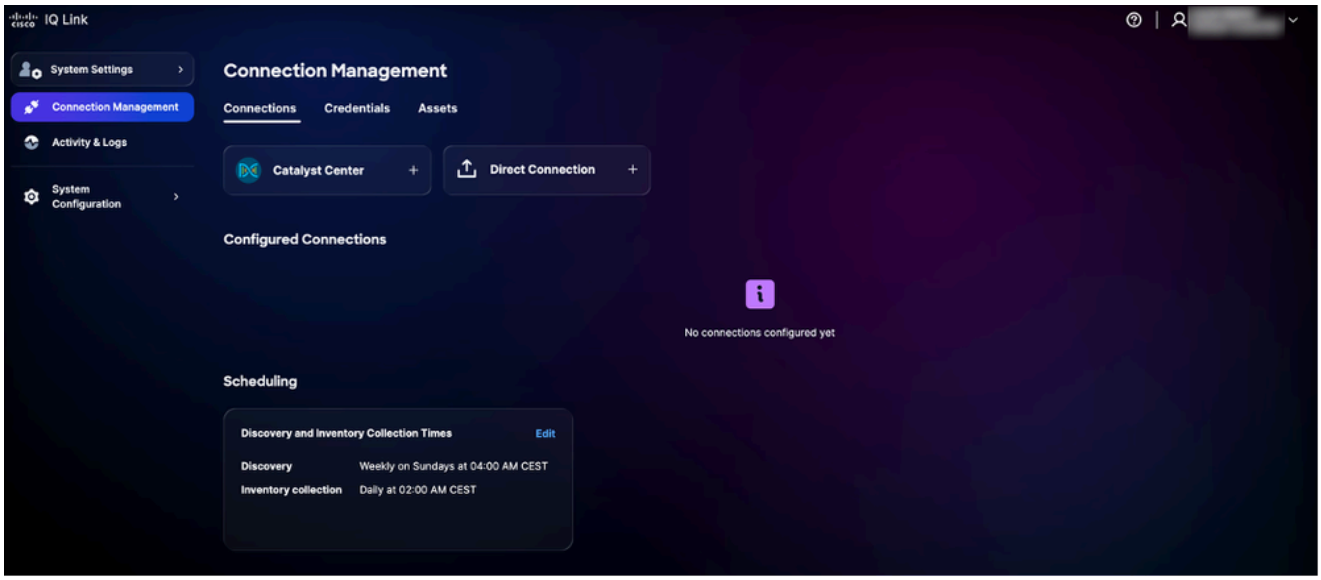
6. 計畫收藏。有關詳細資訊，請參閱計畫。

附註：Cisco IQ Link已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。

直接連線

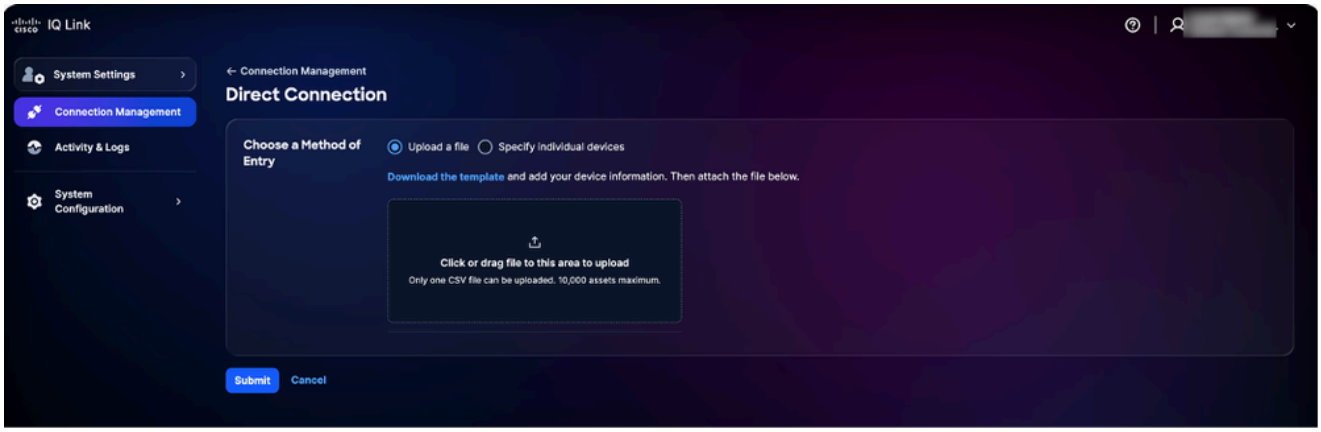
要新增直接連線的裝置，請執行以下操作：

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



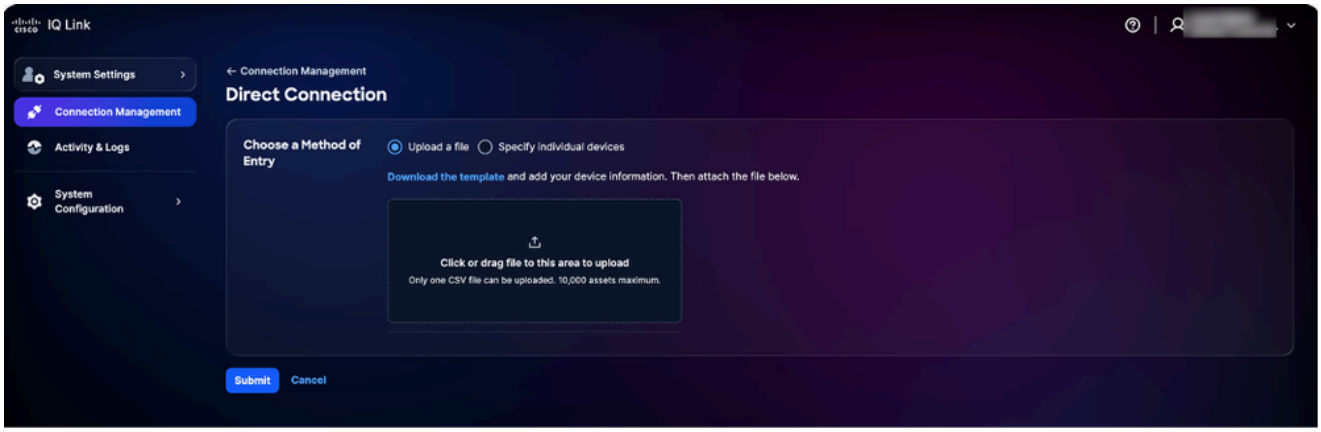
連線管理

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



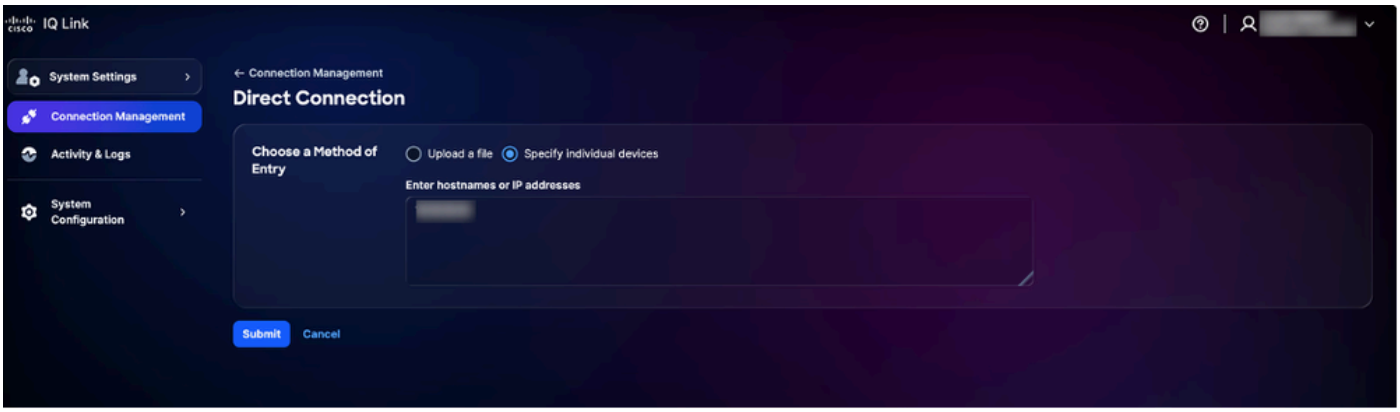
上傳檔案

3. 按一下Choose a Method of Entry的首選選項，然後使用以下方法之一提交裝置：



上傳檔案

- 上傳檔案:按一下或拖放檔案，然後按一下Submit



指定單個裝置

- 指定單個裝置:輸入單個主機名、IP地址或以逗號分隔的主機名和/或IP地址清單，然後按一下Submit

成功提交後，系統會將您重新導向到Assets索引標籤。

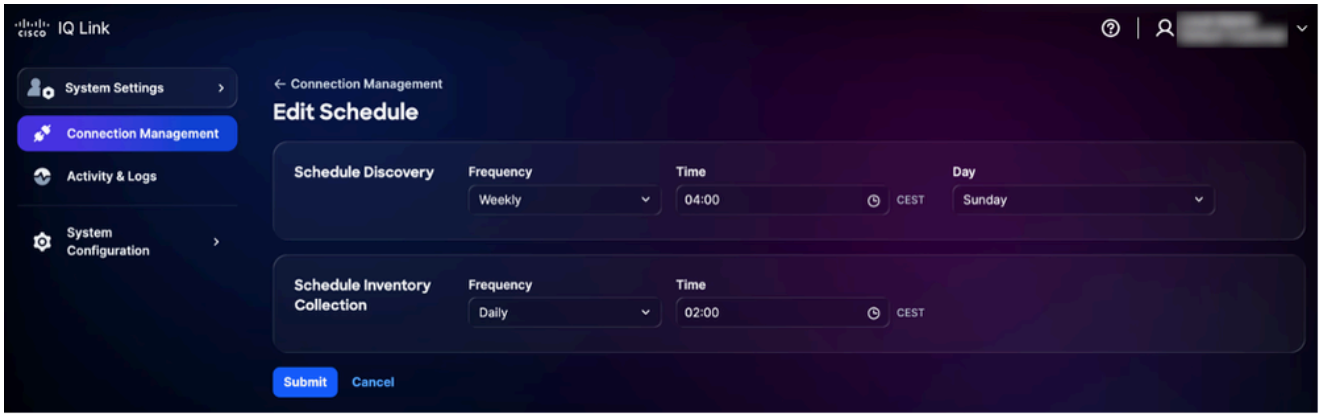
4.計畫收藏。有關詳細資訊，請參閱計畫。

> 附註：Cisco IQ Link已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。

日程安排

計畫允許您定義Cisco IQ Link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「編輯計劃」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：對於對發現或收集計畫所做的任何更改，留出5-10分鐘的時間在Cisco IQ Link中進行同步和準確反映。

橫幅

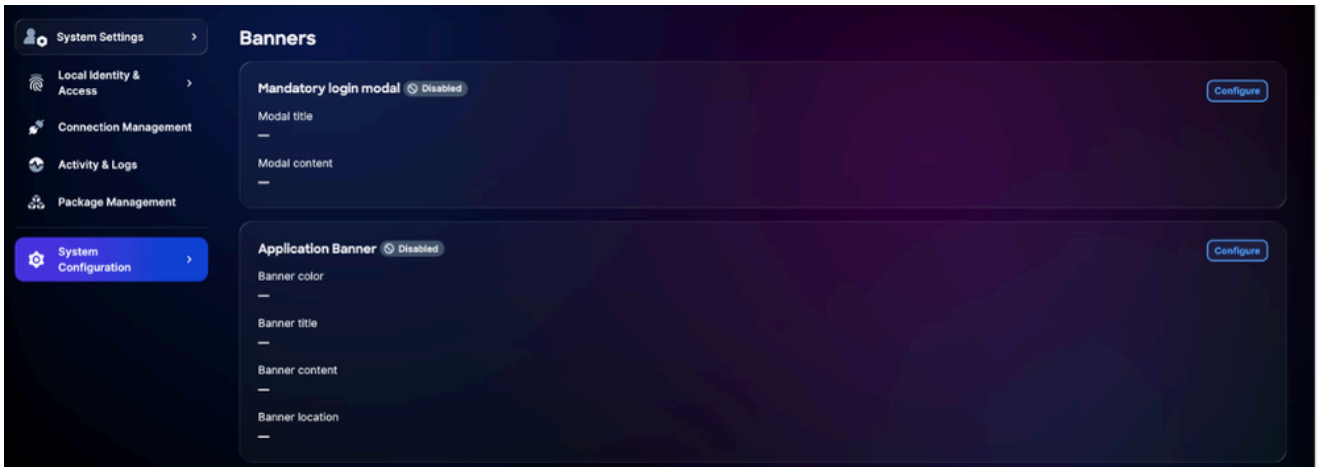
帳戶管理員可以配置系統範圍的橫幅以符合安全和合規標準。

- 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

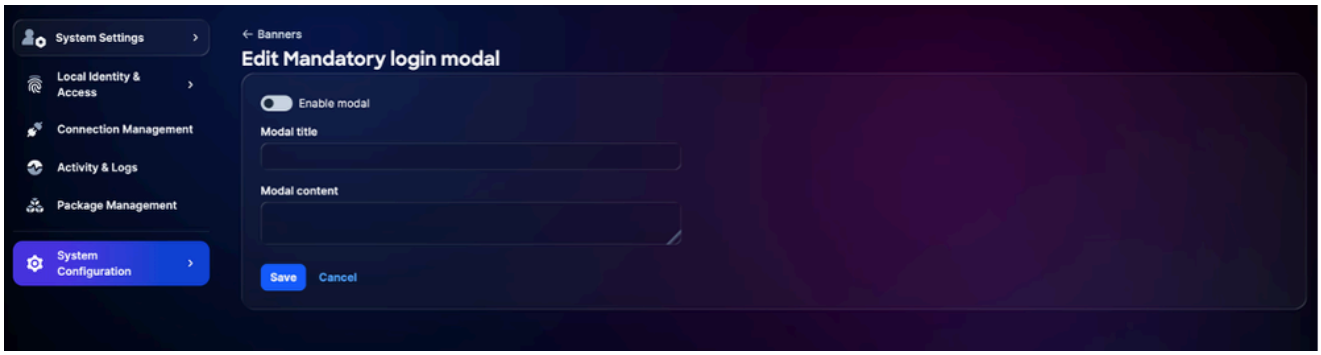
要配置強制性標語，請執行以下操作：

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。



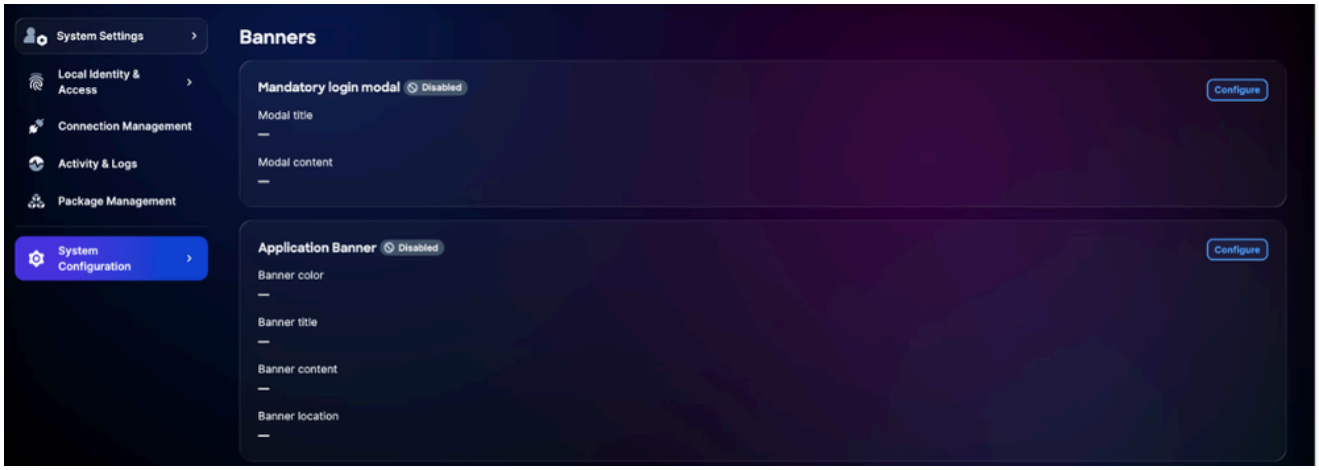
編輯強制登入模式橫幅

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

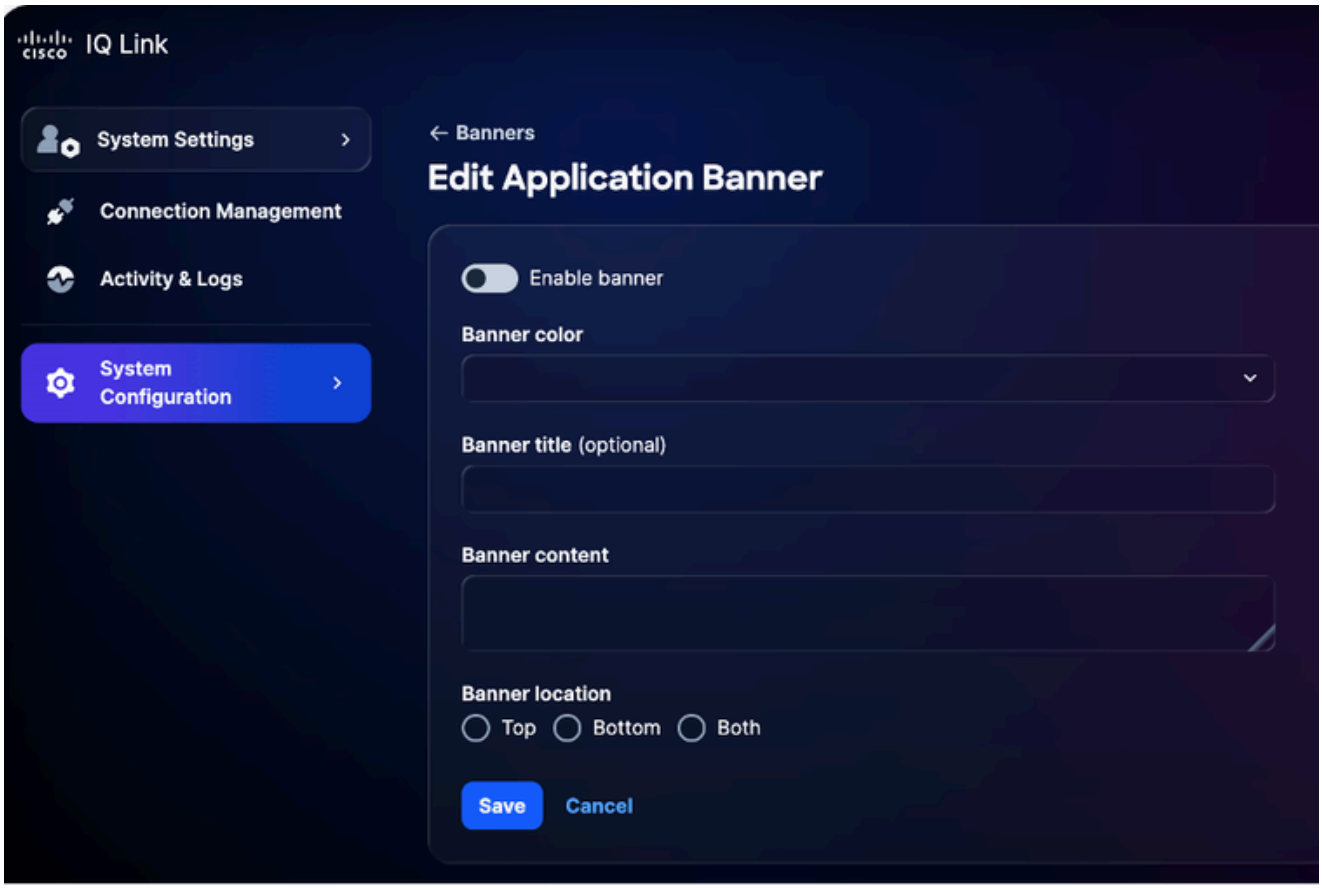
要配置應用程式橫幅，請執行以下操作：

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

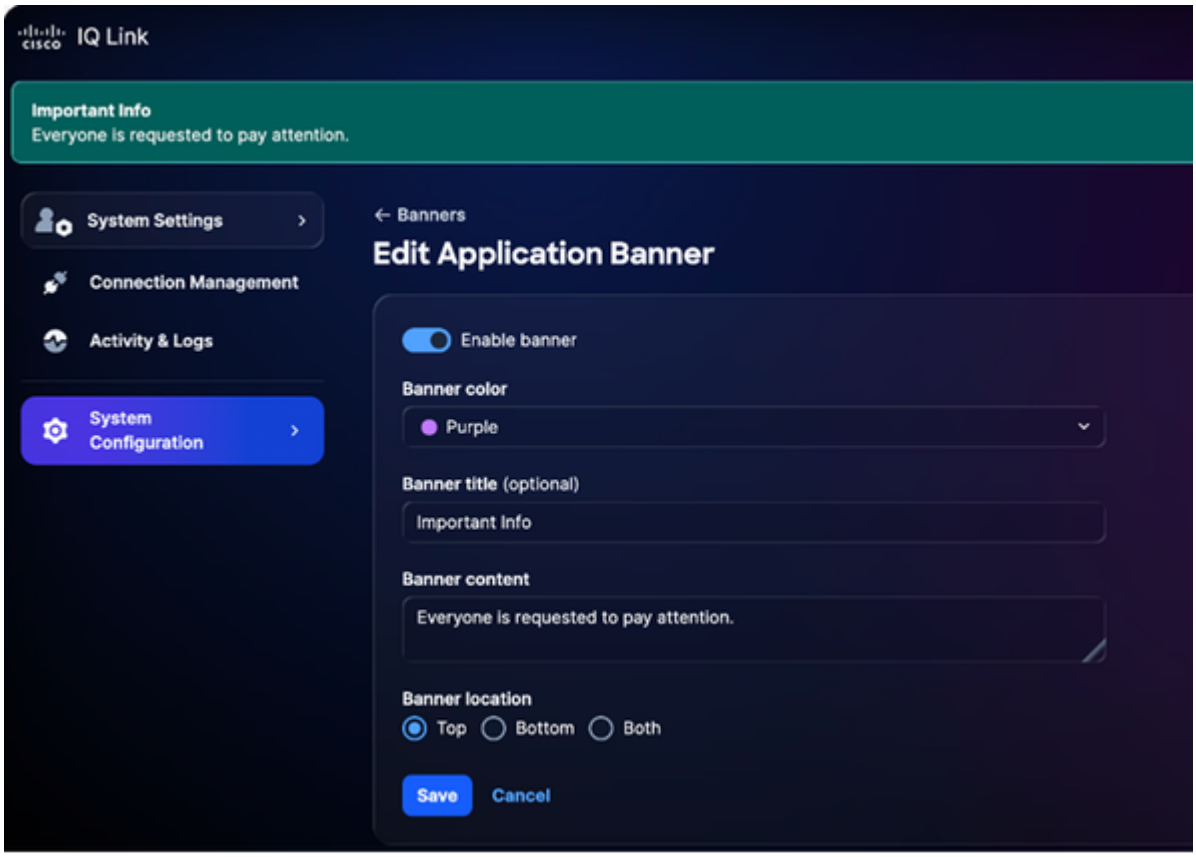
3. 按一下切換以啟用或禁用標語。
4. 選擇標語顏色。
5. 輸入標語標題。
6. 輸入Banner內容。
7. 選擇標語位置。
8. 按一下「Save」。橫幅顯示於整個應用程式中。

編輯橫幅

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

編輯應用程式橫幅

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：

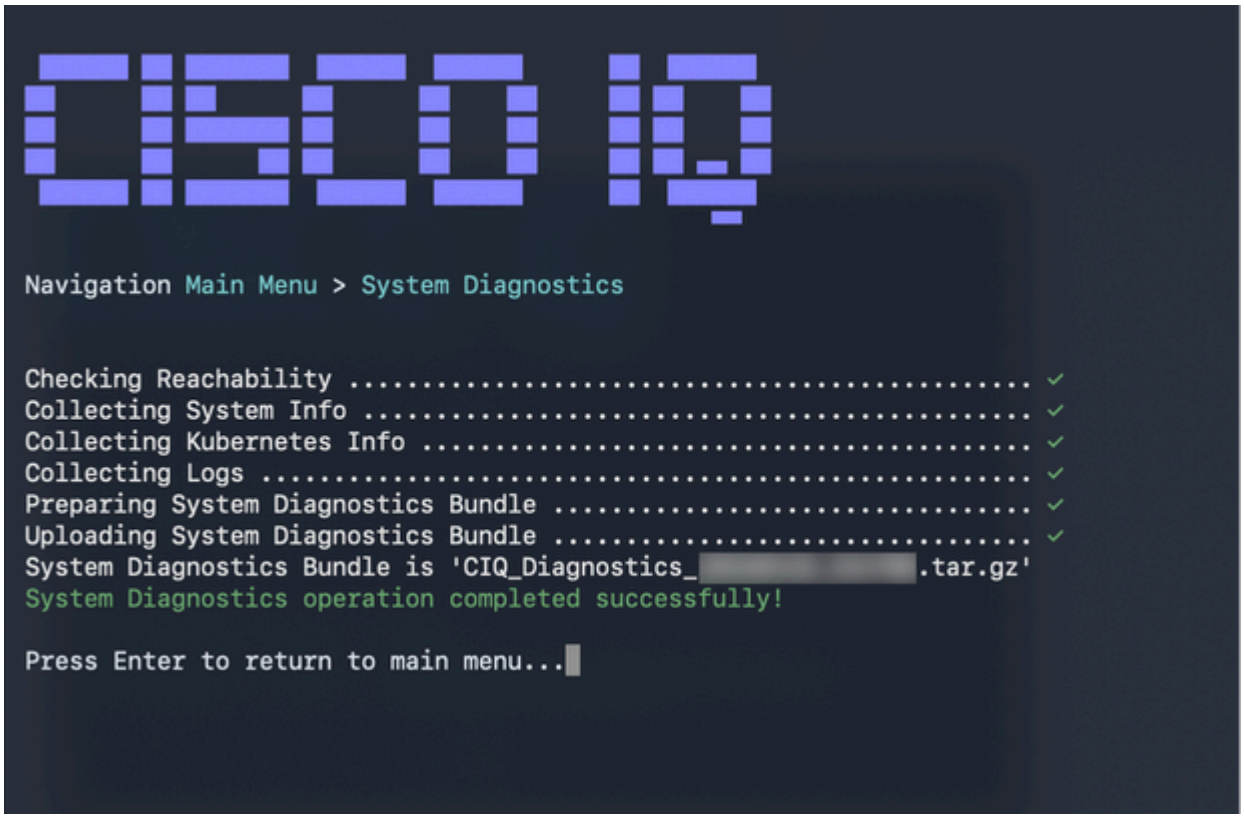
1. 登入到Cisco IQ。

主選單

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

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. 選擇協定。
7. 輸入Username。
8. 輸入Password。
9. 輸入「C」並按Enter以繼續系統診斷。



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。

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）。