思科IQ鏈路操作指南v1.1.0

簡介

Cisco IQ™為客戶提供增強功能和特性，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，使使用者能夠做出主動的、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

管理員應使用以下憑證登入到Cisco IQ Link:

- 預設使用者名稱：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

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

設定本地管理員安全

您可以通過系統配置中的Local Admin Security選單更改密碼並設定安全問題。

您在十(10)分鐘內三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60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。

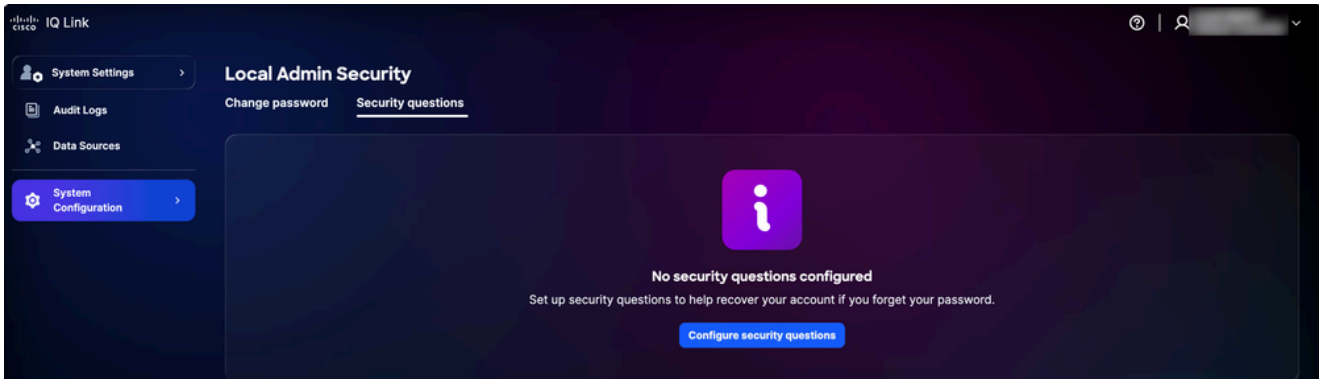
您的帳戶將在60分鐘後自動解鎖，此時您可能會嘗試登入或重置密碼。

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。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。

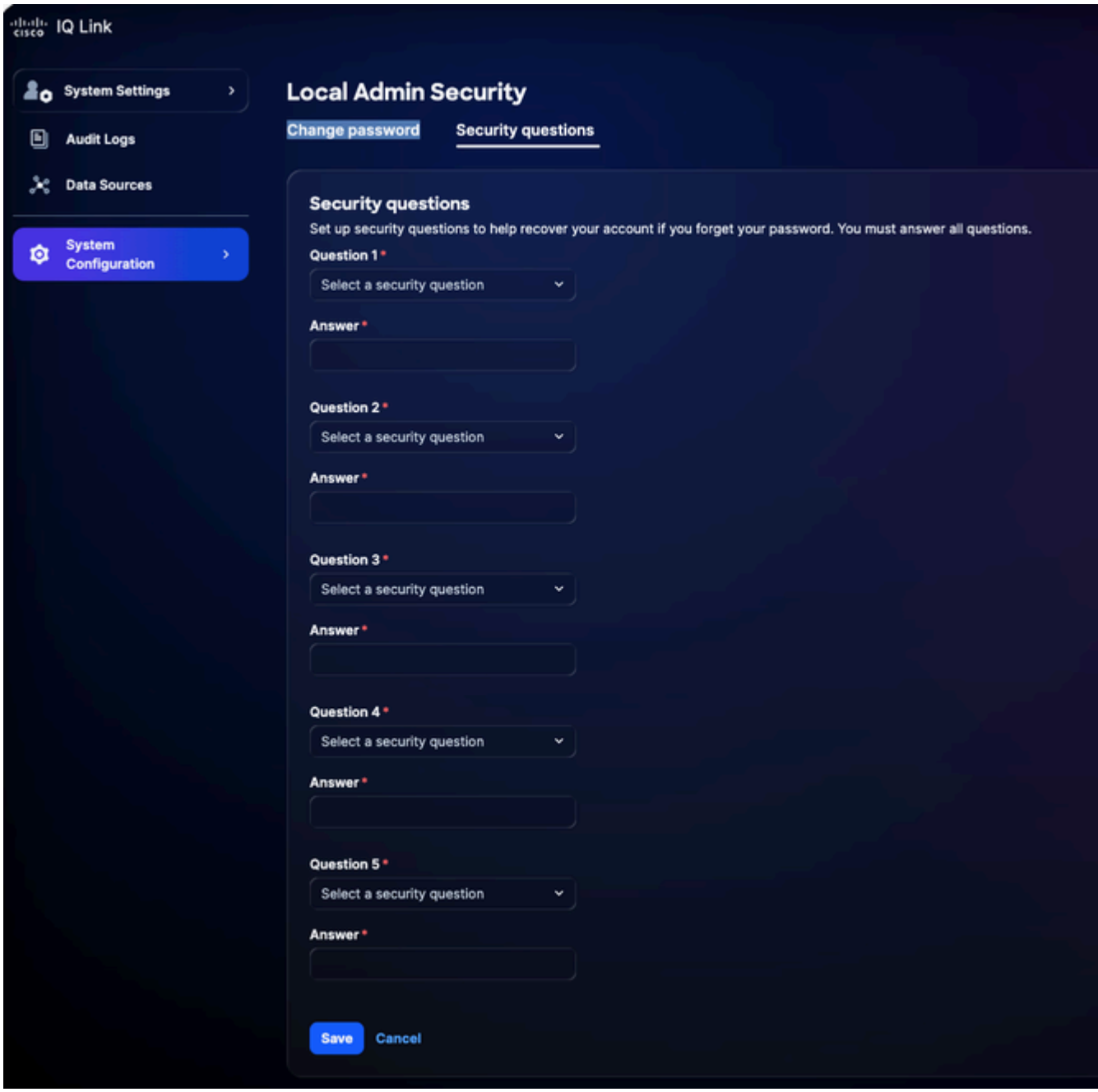
要設定安全問題，請執行以下操作：

1. 在System Settings中選擇System Configuration > Local Admin Security > Security Questions。



安全問題

2. 按一下配置安全問題。



安全問題

3. 從下拉選單中選擇任意五(5)個安全問題。

4. 輸入每個問題的回答。

5. 按一下「Save」。

附註：
·答案不區分大小寫，例如，「SMITH」和「smith」被認為是相同的
·忽略多餘的空格，這意味著「Smith」和「Smith」會得到相同的處理

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

只有本地管理員可以管理Cisco IQ的密碼。

必要條件

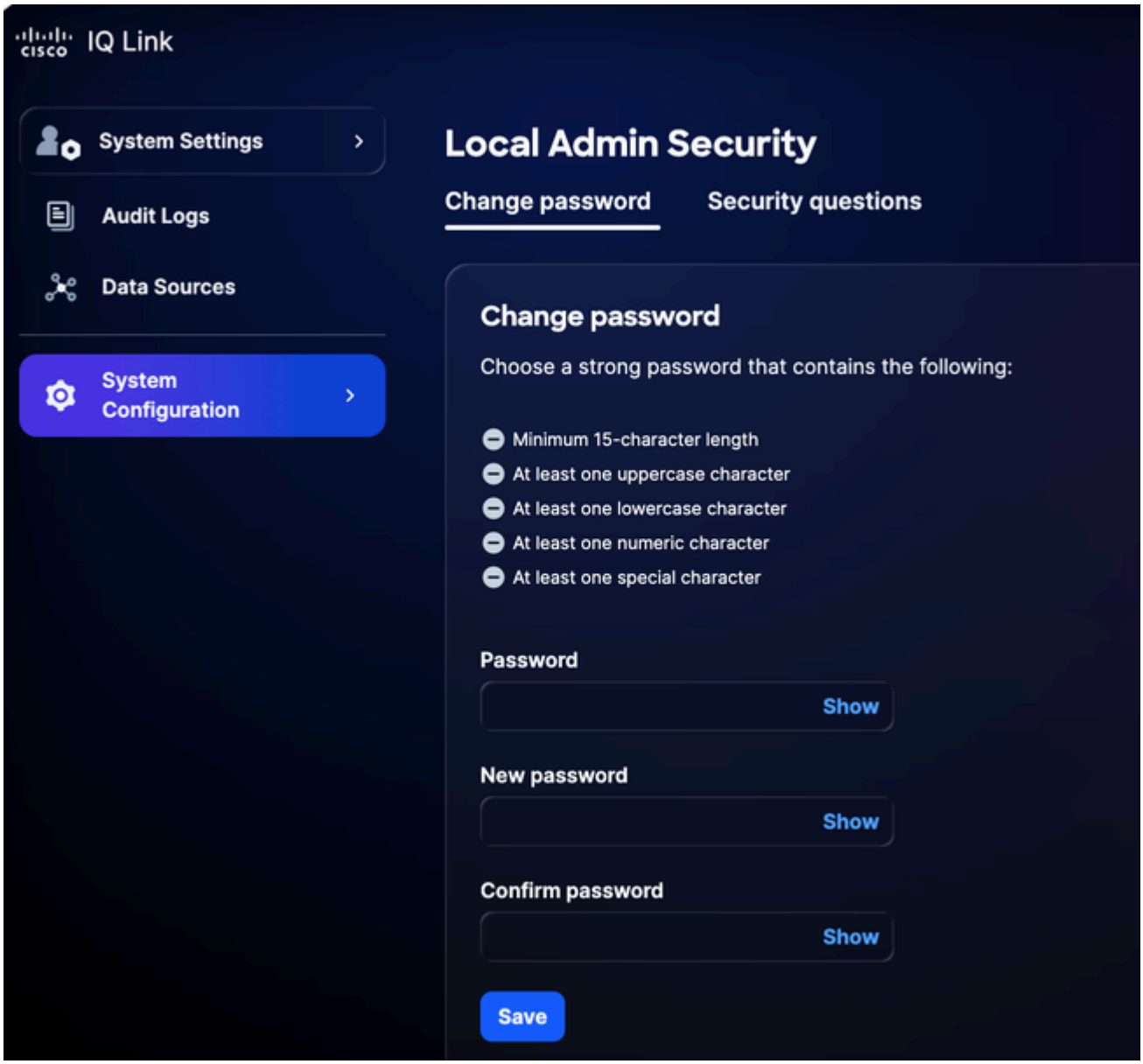
要管理密碼，必須滿足以下條件：

- 您是本地管理員
- 您正在使用本地管理員帳戶(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System Settings中，導航到System Configuration > Local Admin Security > Change Password。



更改密碼

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

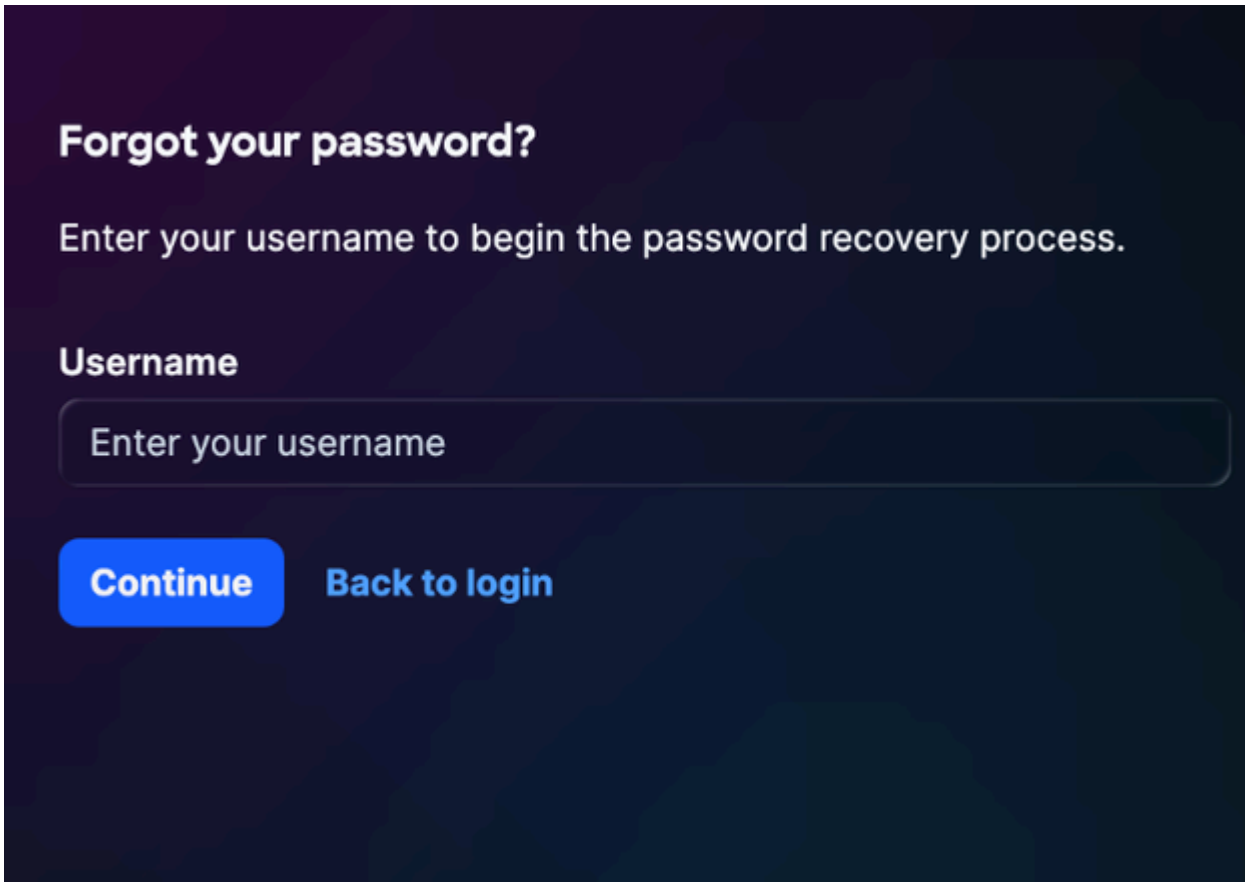
密碼在Cisco IQ系統中更新，包括Cisco IQ虛擬機器(VM)。

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。

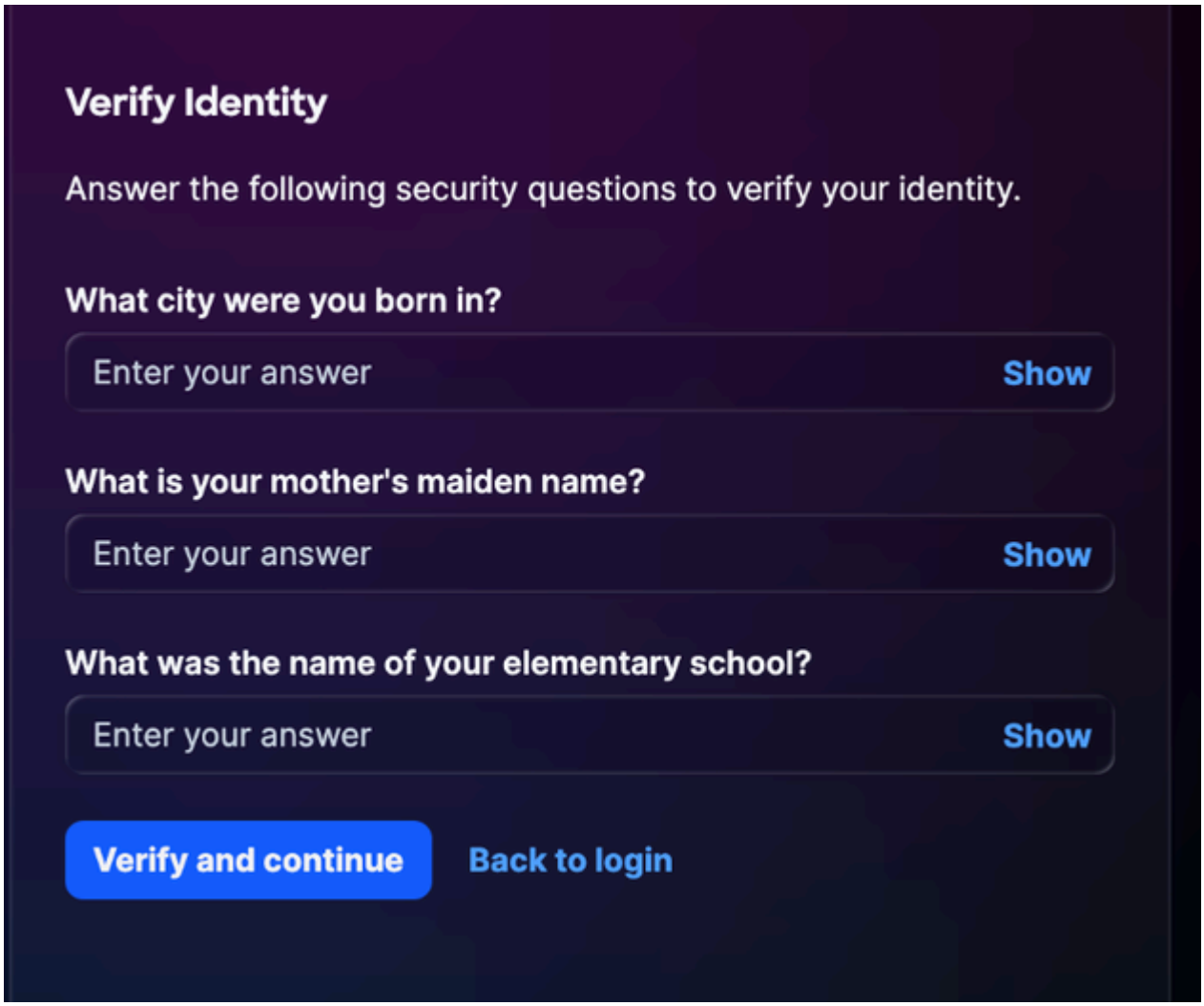
要重置忘記的密碼：

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



忘記密碼

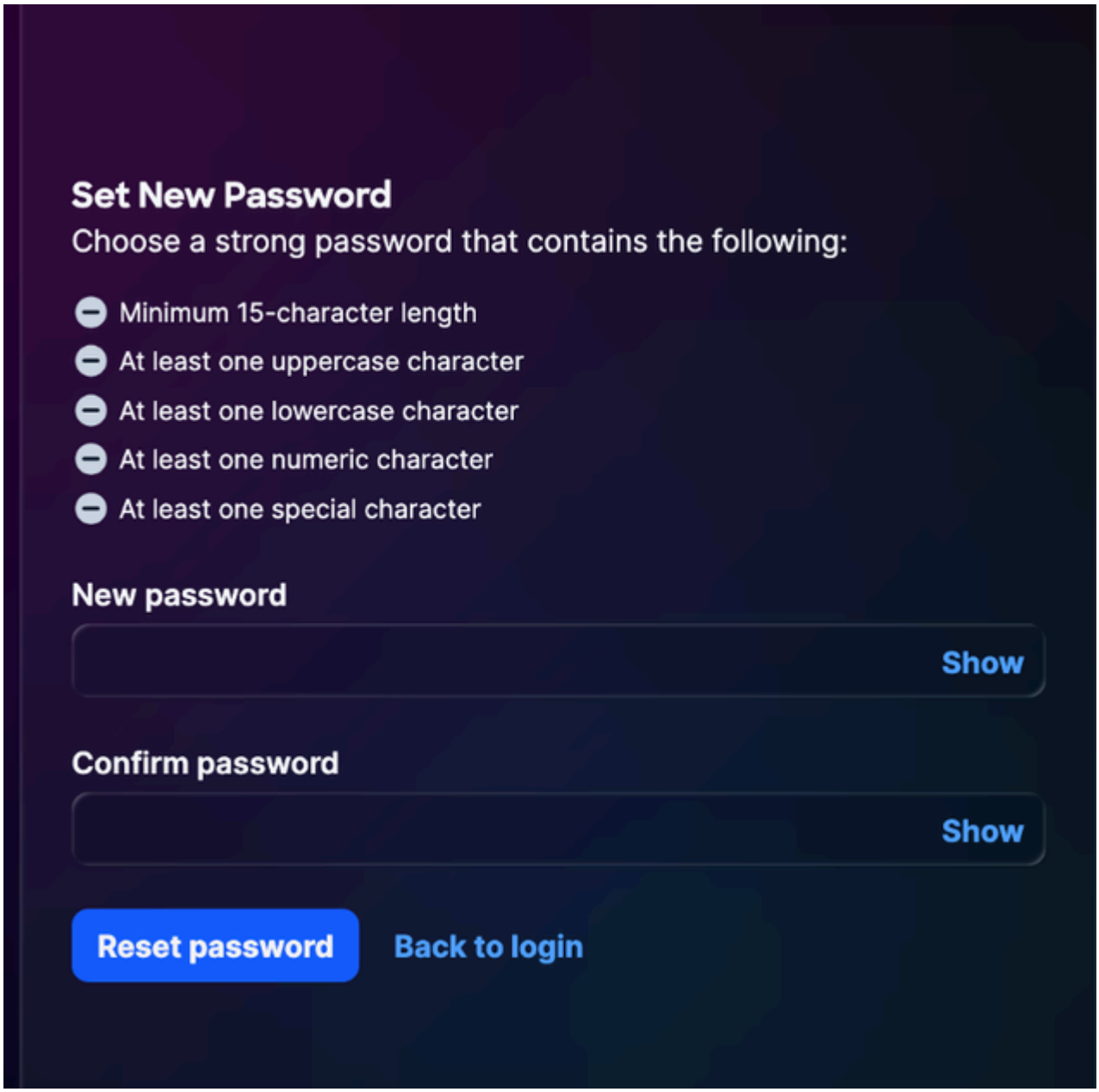
3. 輸入Username。
4. 按一下「Continue」（繼續）。Verify Identity頁顯示先前配置的五(5)個問題中的三(3)個隨機安全問題。



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「Verify」，然後繼續。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

附註：您在十(10)分鐘時間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60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。

您的帳戶將在60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. 再次輸入密碼以確認。
9. 按一下「Submit」。

配置身份提供程式

登入到Cisco IQ Link後，管理員可以配置各種設定。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

- 本地管理員對Cisco IQ Link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。
2. 為Cisco IQ Link例項設定以下屬性。

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」

SAML配置引數

參數	組態	範例
受眾（實體ID）	FQDN名稱	mymanagementhost.mydomain.com
單一登入URL	SAML 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. 在應用程式中配置單一註銷(SLO)設定。

SLO配置設定

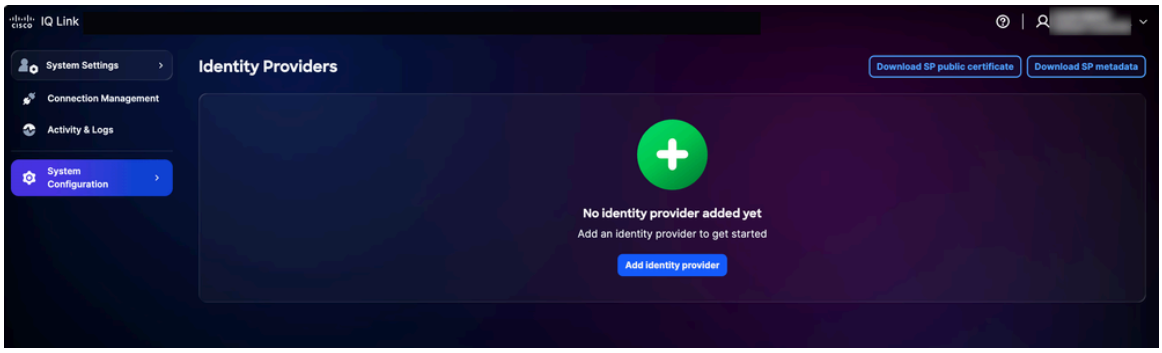
欄位	價值
簽名證書	對於Okta，只有當您選擇啟用SLO時才需要此證書。使用身份提供程式中的下載SP證書來下載簽名證書。將檔案另存為sp-public-key.crt。如需詳細資訊，請參閱單一註銷組態。
SP後設資料	SP後設資料僅用於ADFS IDP（而非Okta）。
是否要啟用單一註銷	是或否
單一註銷URL	https://mymanagementhost.mydomain.com/saml/logout
SP頒發者（受眾/實體ID或ACS URL）	https://mymanagementhost.mydomain.com

5. 按一下Download圖示下載「SP Metadata」檔案。
6. 根據提供商的要求設定或建立應用程式。

新增IDP

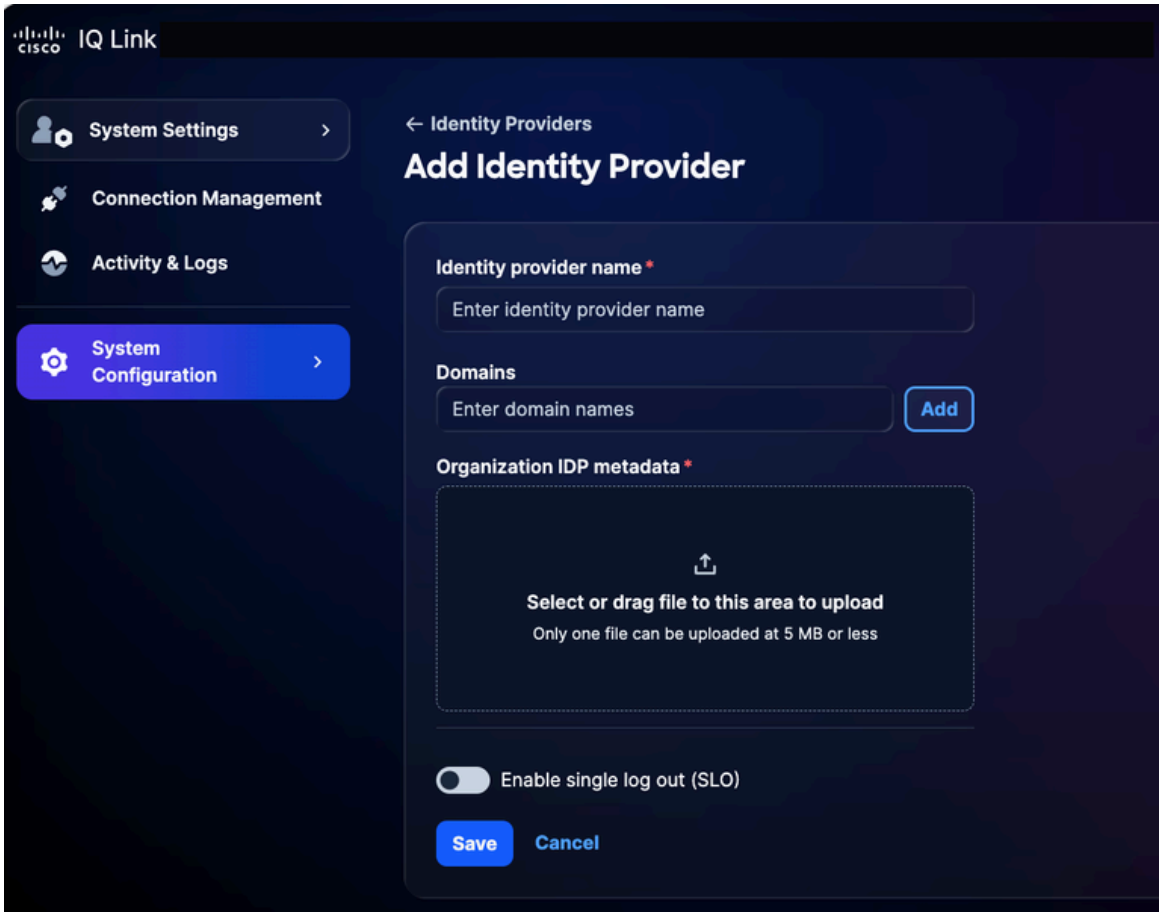
在Cisco IQ Link中新增IDP:

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. 輸入身份提供方名稱。

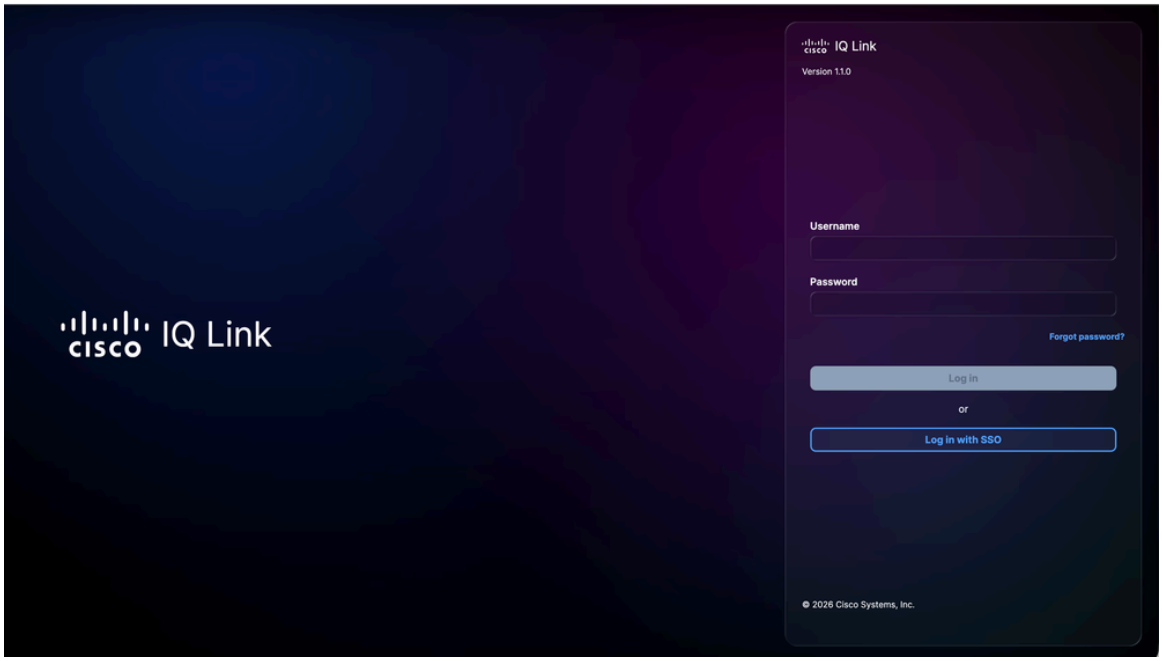
4. 點選Add將已配置Cisco IQ Link的域名新增到Domains欄位。

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）開啟Enable single logout切換按鈕。您也可以稍後啟用SLO。

7. 按一下「Save」。

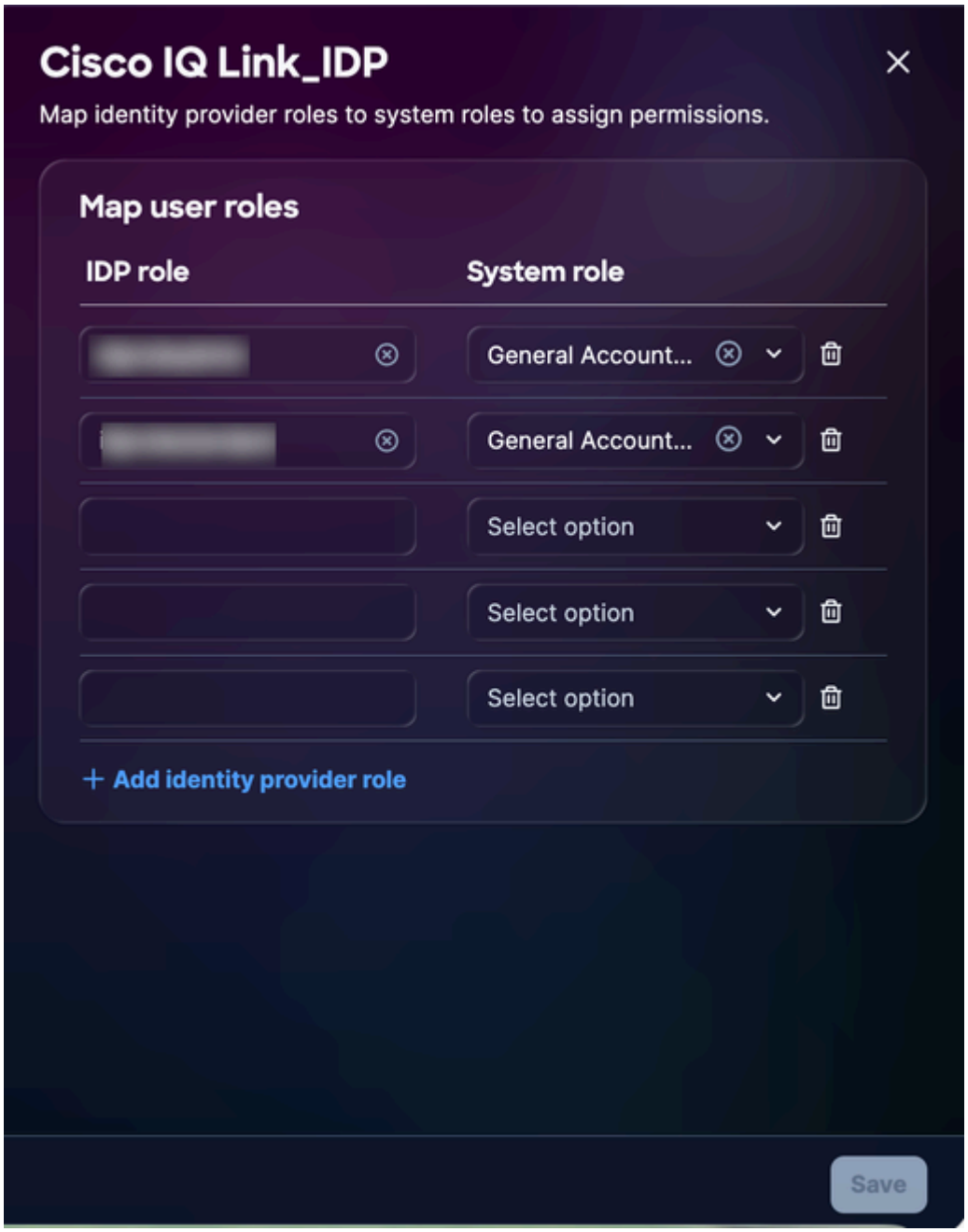
8. 配置後，登入頁面將顯示使用SSO（通過IDP）登入的選項。



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。

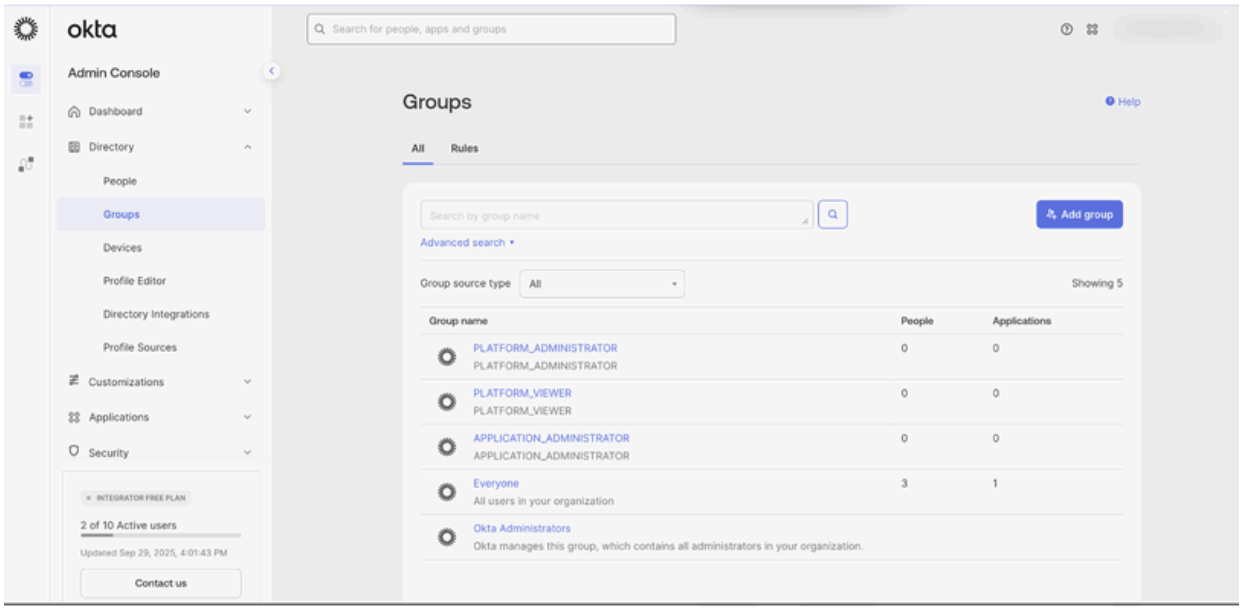


使用者角色對映

2. 為所選系統角色輸入IDP角色。支援以下系統角色：

   - general_account _administrator:一般帳戶管理員具有執行產品中所有操作的完全許可權
   - general_account _viewer: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

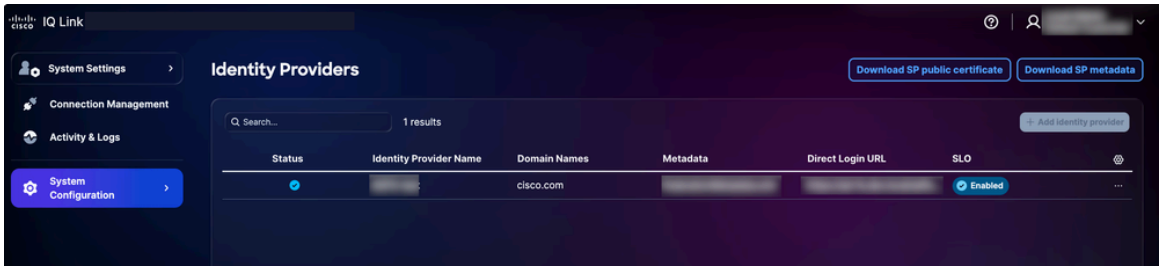
3. 通過按一下新增身份提供程式角色根據需要對映其他角色。

4. 按一下「Save」。

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. 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

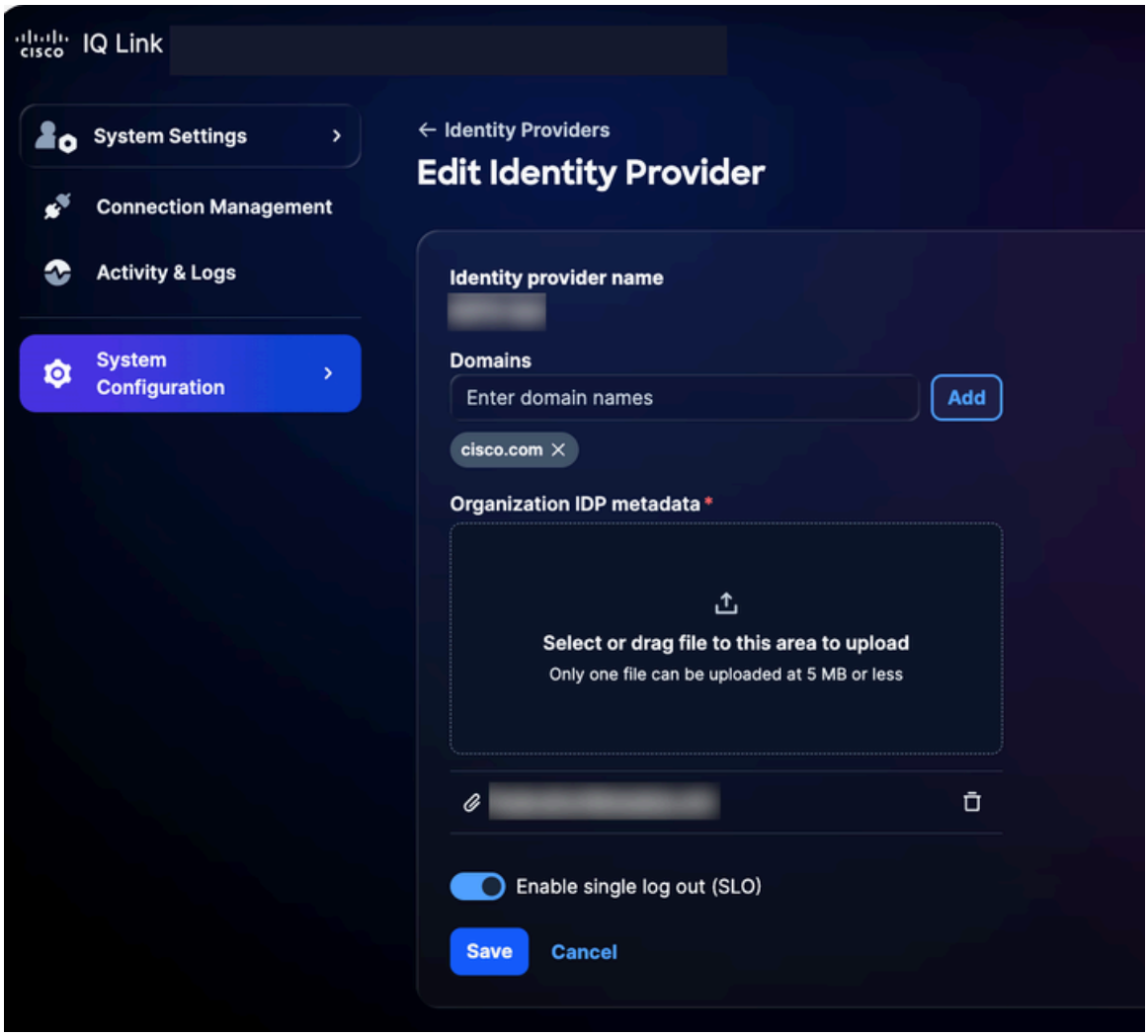
2. 將下載檔案另存為sp-public-key.crt。

3. 導航到您的IDP門戶。

4. 上載在IDP SAML Configuration for SSO部分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. 上傳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：

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Active Directory整合

- ADFS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
- ADFS伺服器配置詳細資訊（如下表中所列）

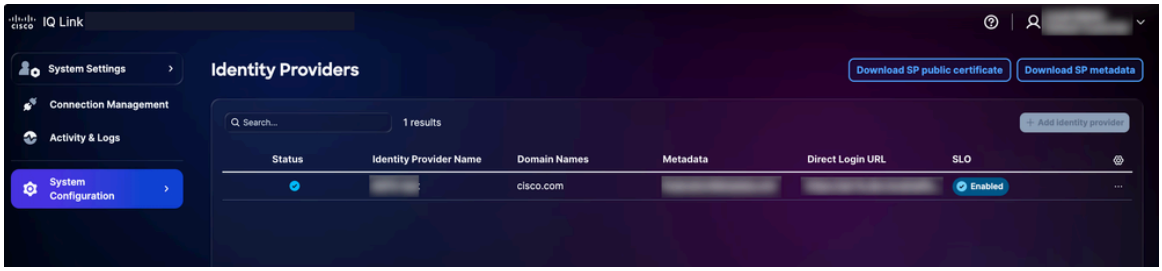
ADFS伺服器配置

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	Active Directory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（從檔案匯入有關信賴方的資料）。
10. 按一下Browse以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「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。

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。

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

領款申請	目的	來源
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 A
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/ws/2005/05/identity/claims/ema

@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.Issu

@RuleName = “Send Group Membership”
c:[Type == “http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname”, Issuer == “AD A
=> issue(store = “Active Directory”, types = (“http://schemas.xmlsoap.org/claims/Group”), query = “;memb
’@@
```

3. 通過運行以下命令應用宣告規則：

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

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

- 將頒發的CA證書匯入受信任的根證書頒發機構儲存

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

3. 通過重新啟動ADFS服務應用更改。

```
Restart-Service adfssrv
```

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。

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. 導覽至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。

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. 輸入身份提供方名稱。
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

在繼續配置角色對映之前，請確保可以從Active Directory中找到用於對映的組。要從Active Directory中查詢組，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LDAP查詢Active Directory，無需其他模組。組資訊以完整的可分辨名稱(DN)格式返

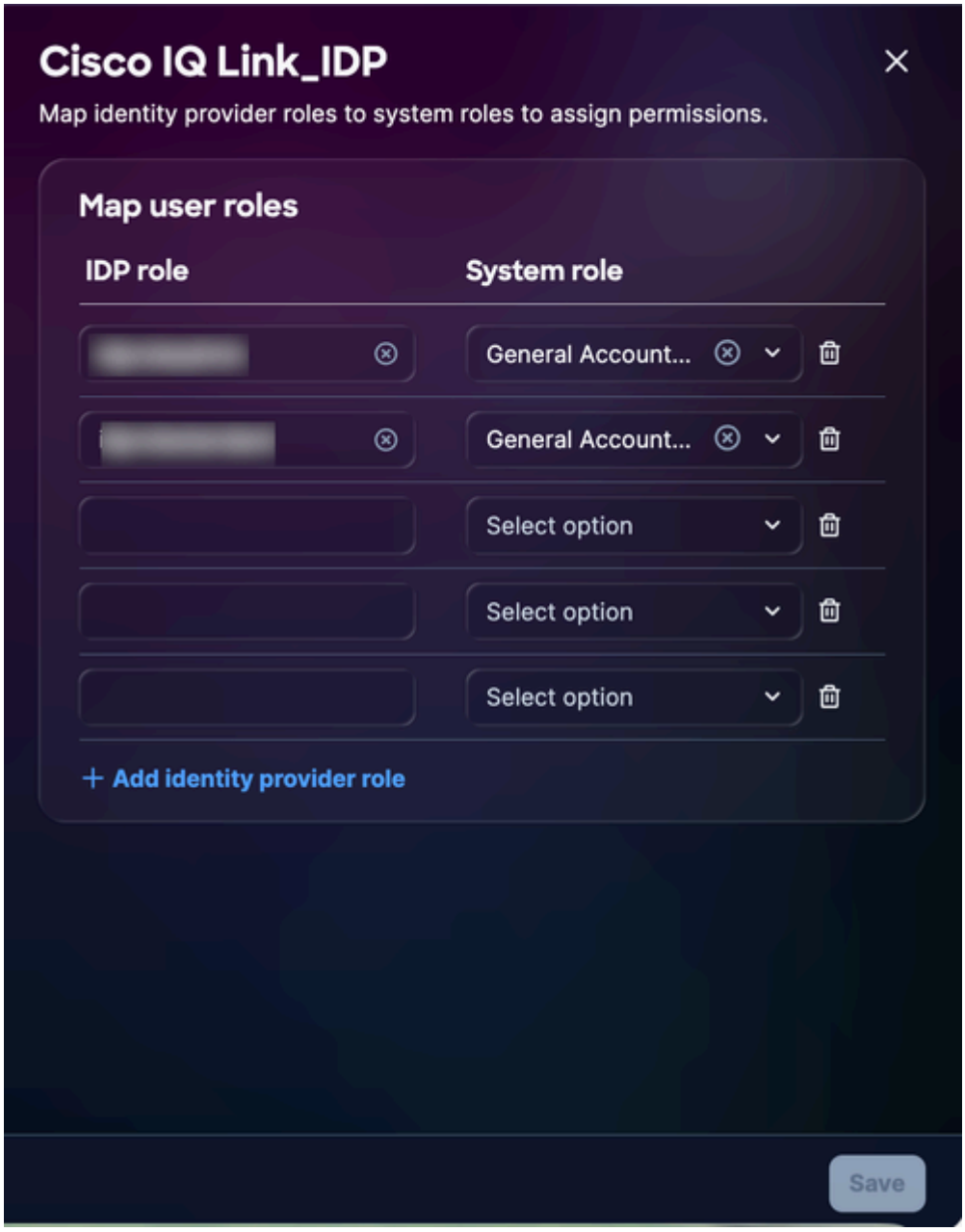
回，例如：

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，則管理員必須在Active Directory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：

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：

   - general_account _administrator: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。
   - general_account__viewer:常規帳戶檢視器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。

驗證和測試

測試身份驗證

1. 在Incognito或Private模式瀏覽器中，導航至https://your-cisco-iq-domain.com/login。
2. 使用域\username或user@domain.local格式的Active Directory憑據登入。
3. 驗證您是否重新導向至Cisco IQ Home頁（在成功驗證之後）。
4. 確認分配的角色在使用者配置檔案中顯示正確的分析組名稱（例如CXIQ Developers）。

測試註銷

要測試註銷，請點選從Cisco IQ註銷。系統隨即會顯示「Logging out， please wait..」（註銷，請稍候……）訊息，系統會將您重新導向至Cisco IQ登入頁面。系統也會終止ADFS會話。如果您嘗試直接訪問ADFS，系統會提示您重新登入。

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。

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	● Missing claim rule: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/claims/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	● ACS URL無效:驗證：https://your-fqdn/saml/acs ● Cookie mismatch: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

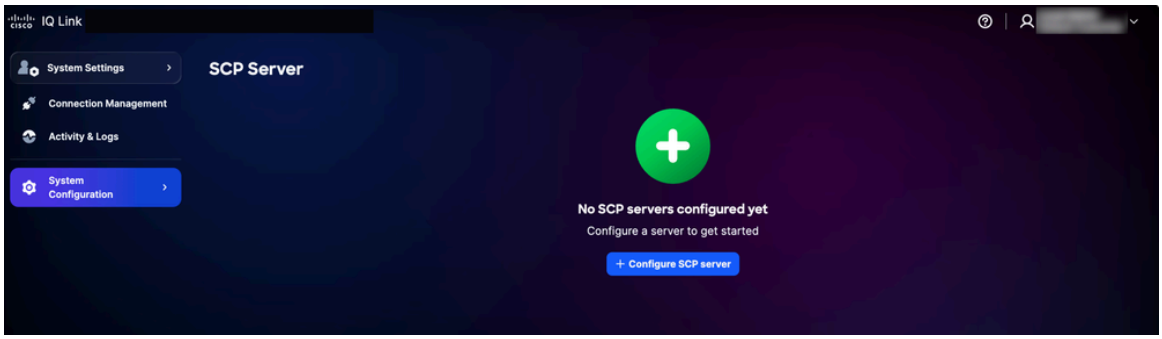
```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object SamlEndpoints
```

新增SCP伺服器

此安全複製協定(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。

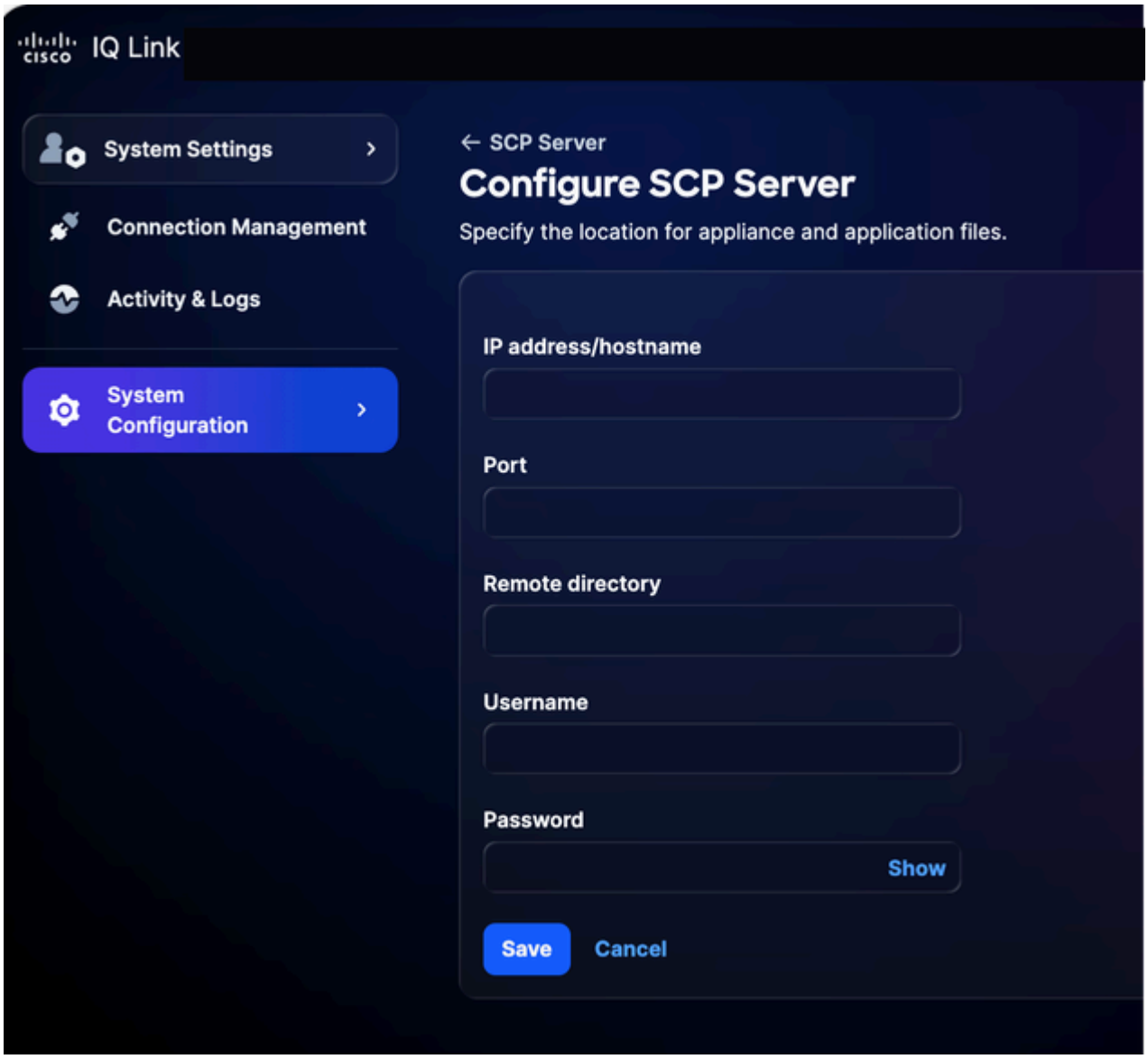
新增SCP伺服器的步驟：

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。



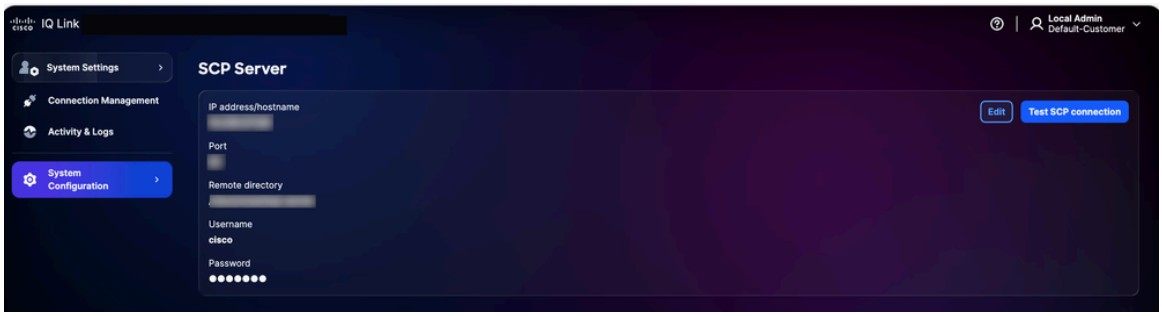
配置SCP伺服器

3. 輸入IP地址/主機名。
4. 輸入端口號。
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

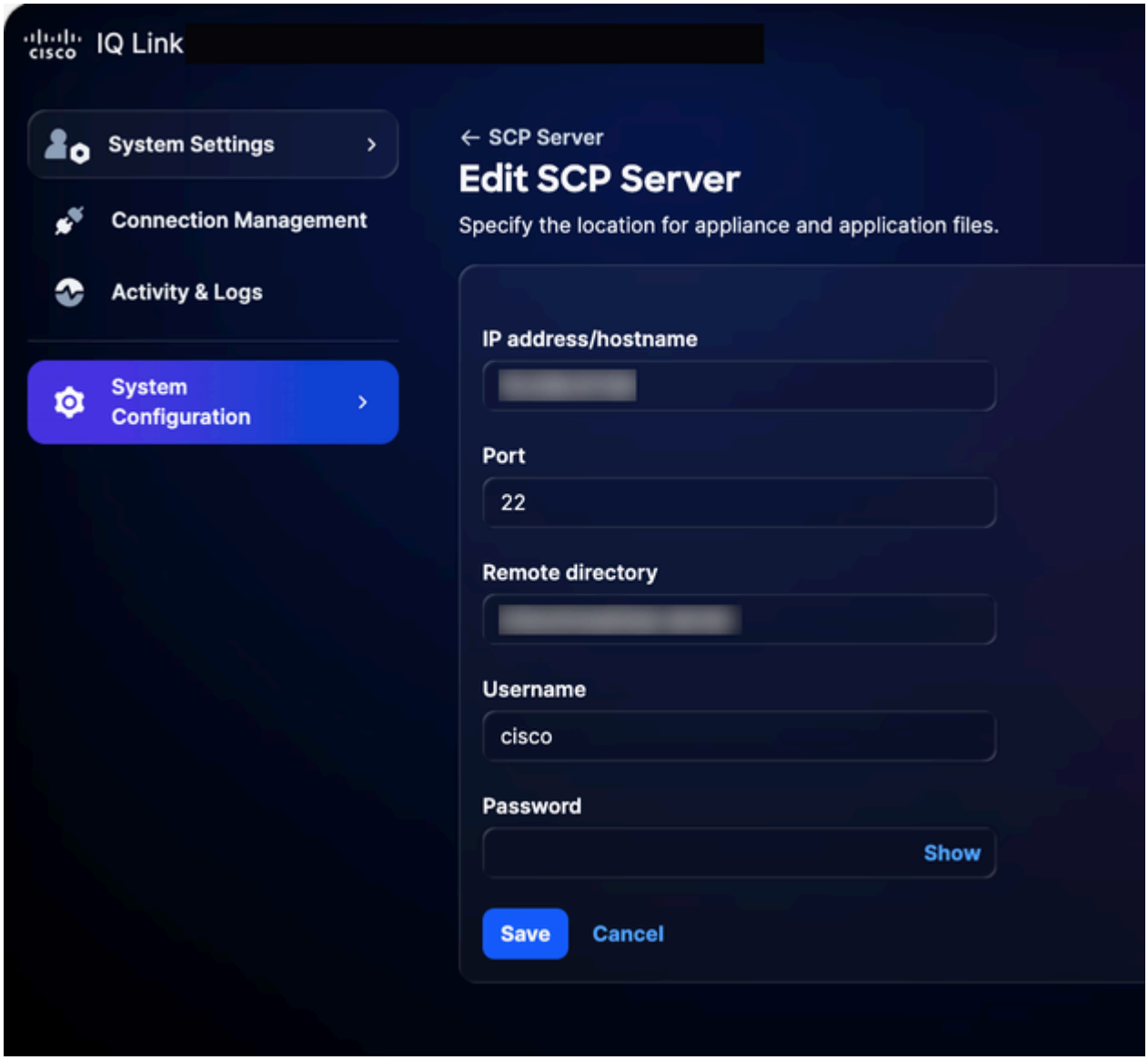
要編輯現有SCP伺服器，請執行以下操作：

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。

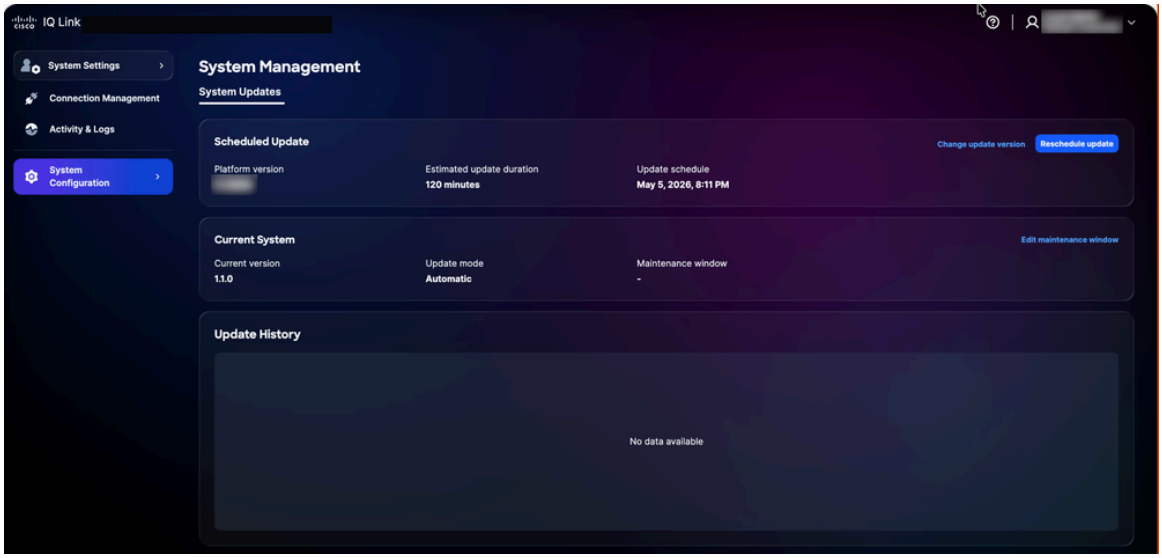
4. 按一下「Save」。

系統管理

客戶可以通過UI升級到最新的Cisco IQ Link版本。您也可以從Cisco IQ Data Connector頁面進行驗證。

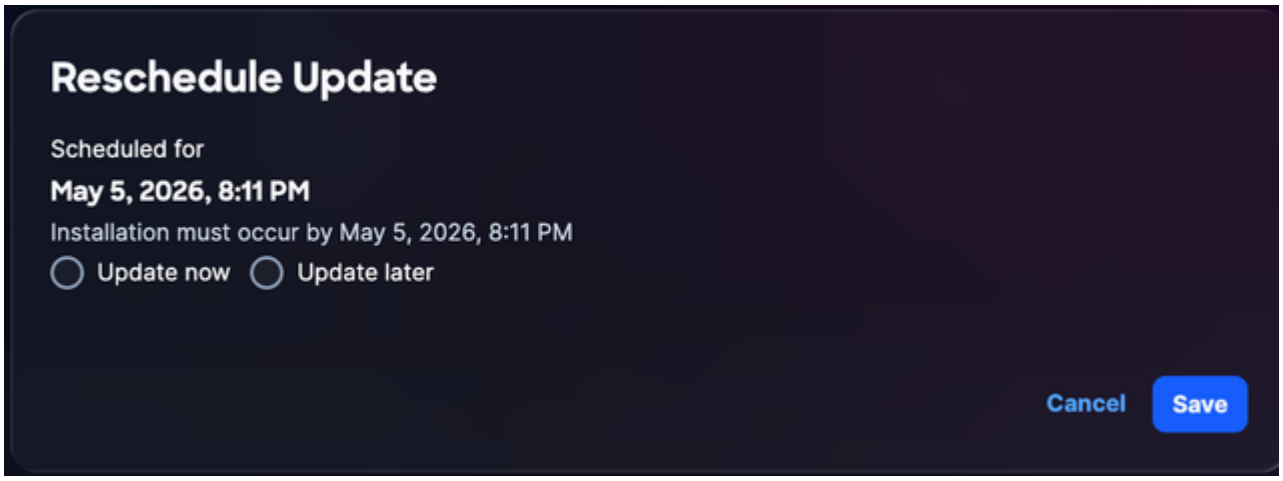
要重新計畫系統更新，請執行以下操作：

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。



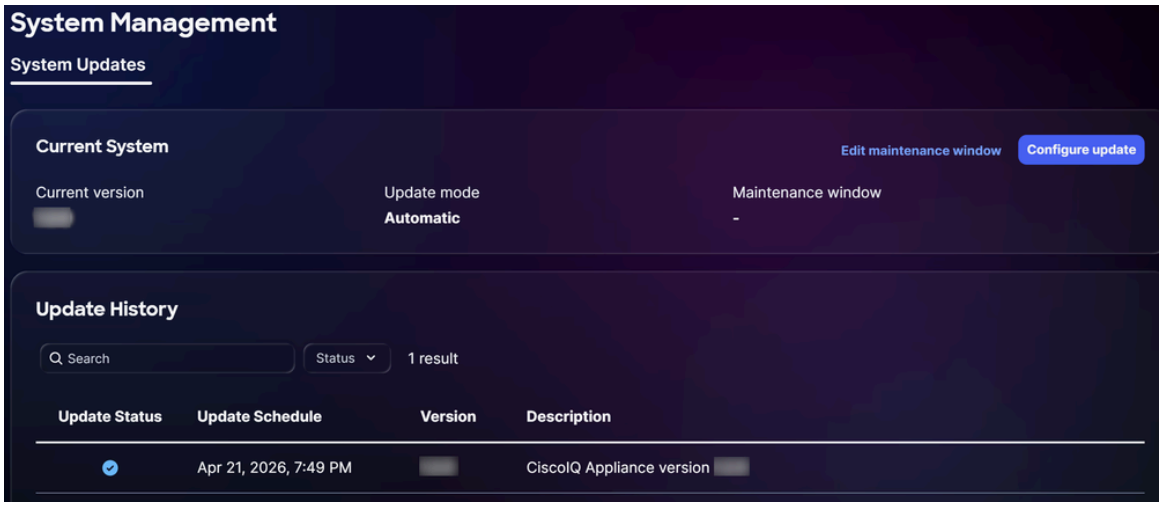
系統升級

2. 按一下Reschedule update。



重新計畫升級

3. 按一下Update Now立即重新計畫，或按一下Update Later安排其他時間。
4. 按一下「Save」。系統將顯示一條確認消息，並且系統會將您重新定向至系統更新首頁。



升級成功

SSL證書配置

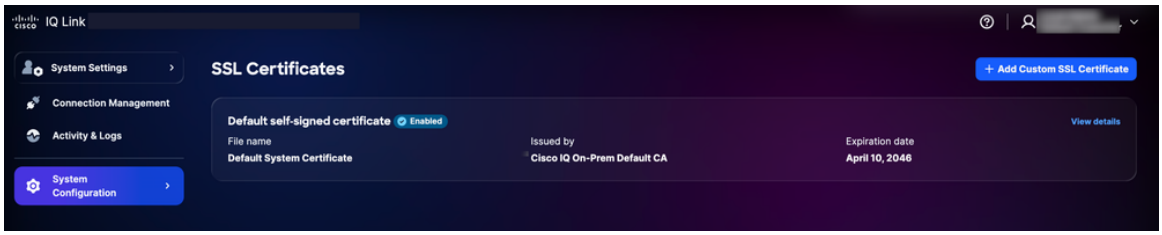
Cisco IQ中預安裝並啟用了預設自簽名證書，但使用者可以上傳自定義SSL證書。啟用自訂SSL憑證時，會將其用於HTTPS連線；如果證書被禁用或刪除，系統會自動恢復為預設證書。

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，客戶必須按照Okta IDP或ADFS IDP的完成SLO配置部分中的說明上傳新的SSL。

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。

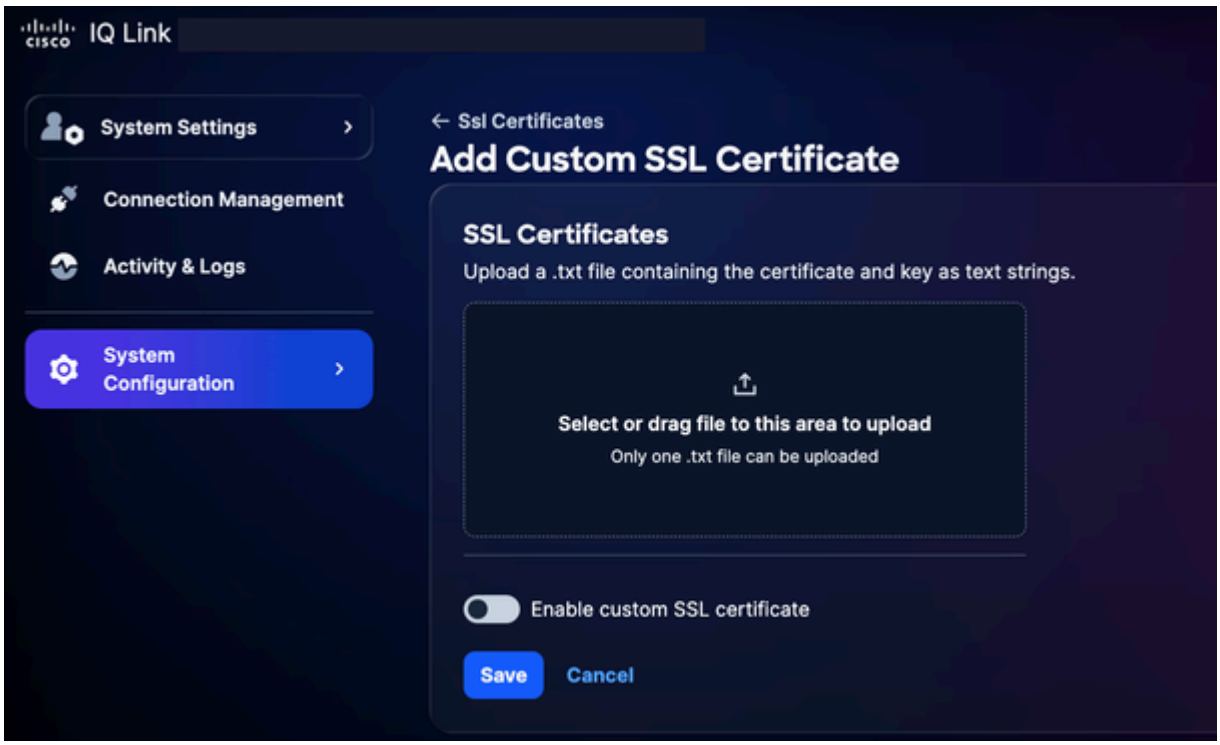


新增SSL證書

2. 按一下「Add Custom SSL Certificate」。

附註：

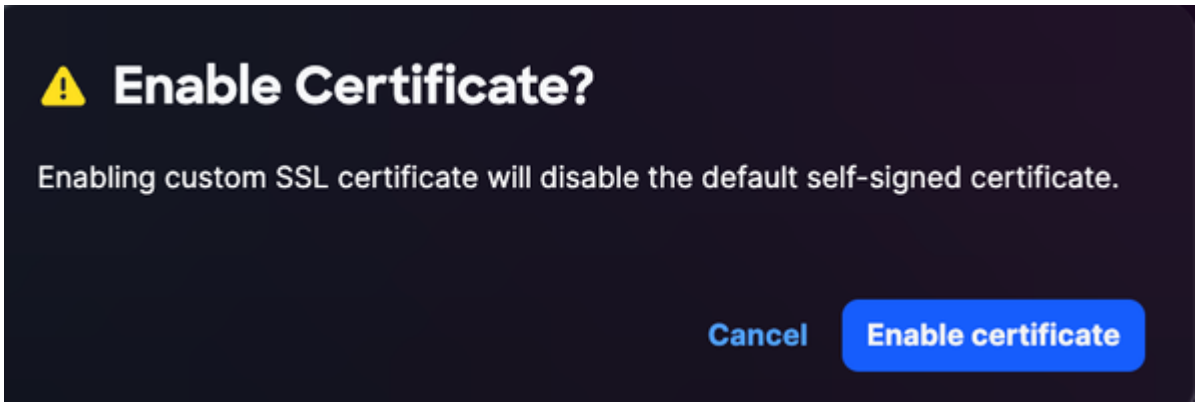
·上傳.txt檔案，其中包含隱私增強型郵件編碼證書和作為文本字串的金鑰
·一次只能上傳一個.txt檔案
·檔案必須同時包含證書和私鑰



上傳SSL證書

3. 將自訂SSL憑證拖放或上傳到SSL Certificate欄位。

4. 啟用Enable custom SSL certificate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」。

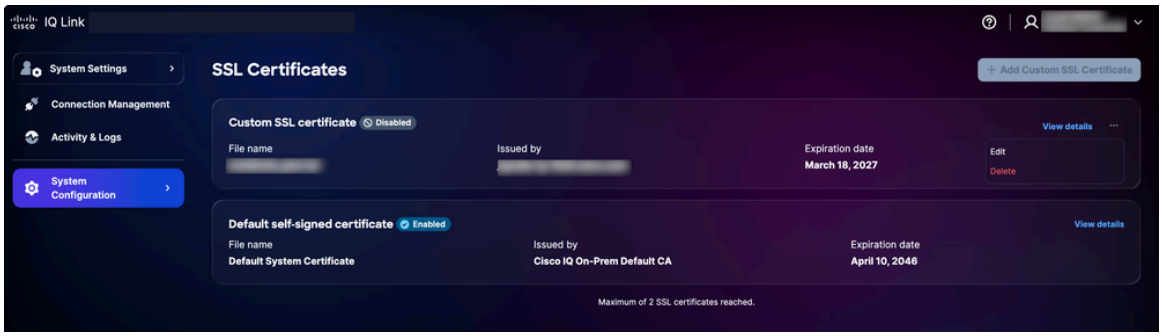
6. 按一下「Save」。

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。



編輯SSL證書

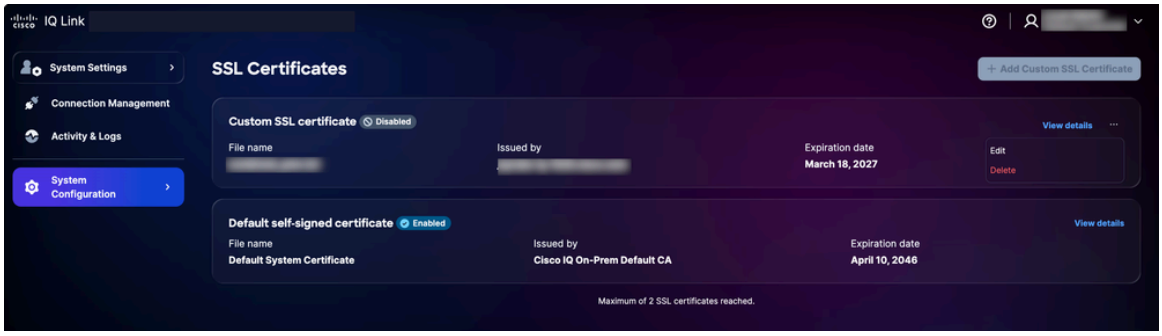
2. 選擇更多選項圖示> 編輯。系統隨即會顯示Edit SSL Certificate頁面。
3. 根據需要編輯證書詳細資訊。
4. 按一下「Save」。

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. 導航到所需的個人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

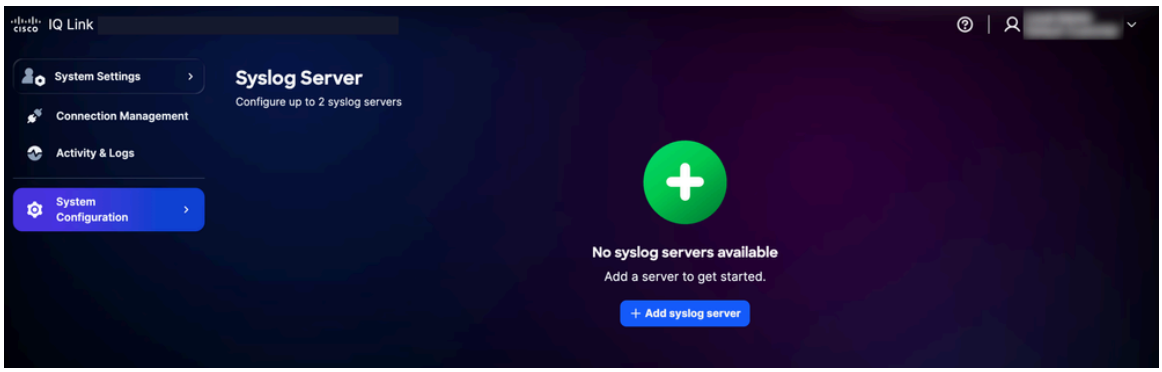
具有管理員角色的使用者可以配置外部系統日誌伺服器以匯出系統日誌。最多可以配置兩(2)台系統日誌伺服器。

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

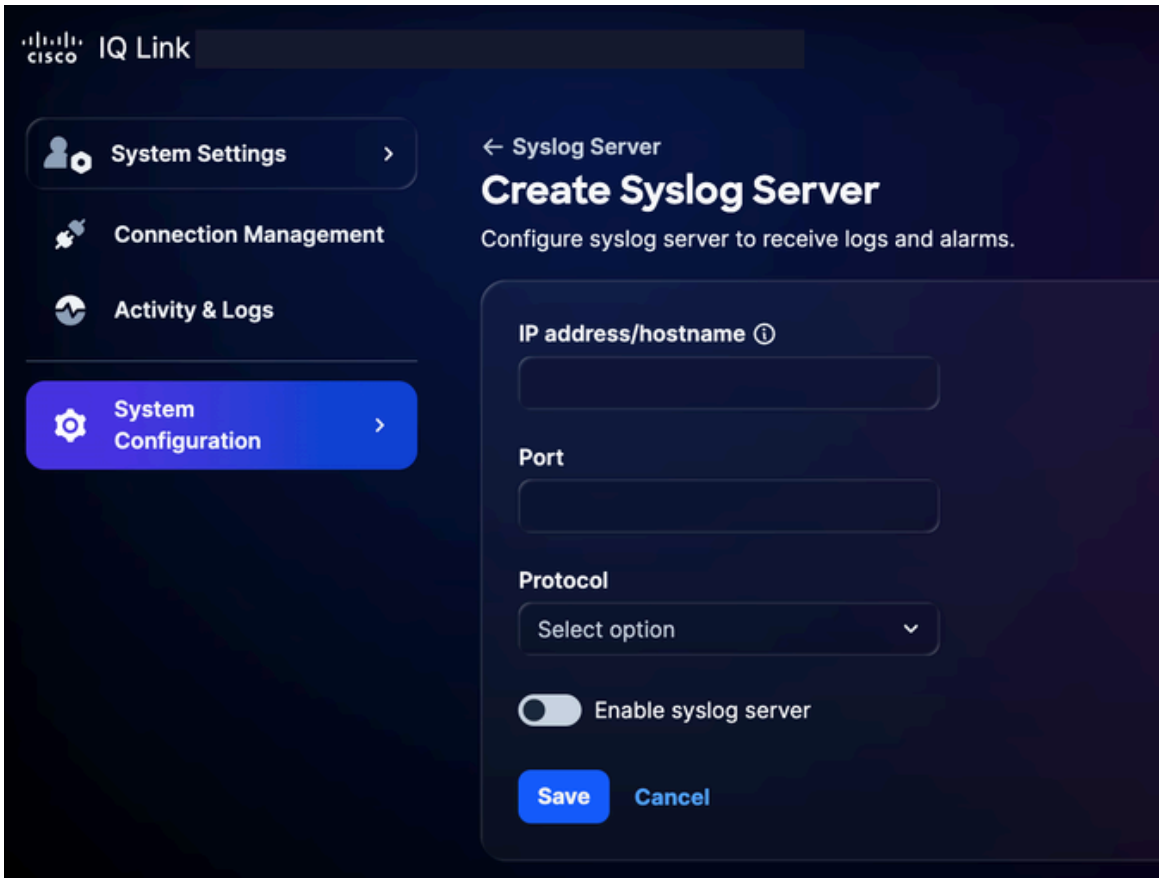
新增系統日誌伺服器：

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。



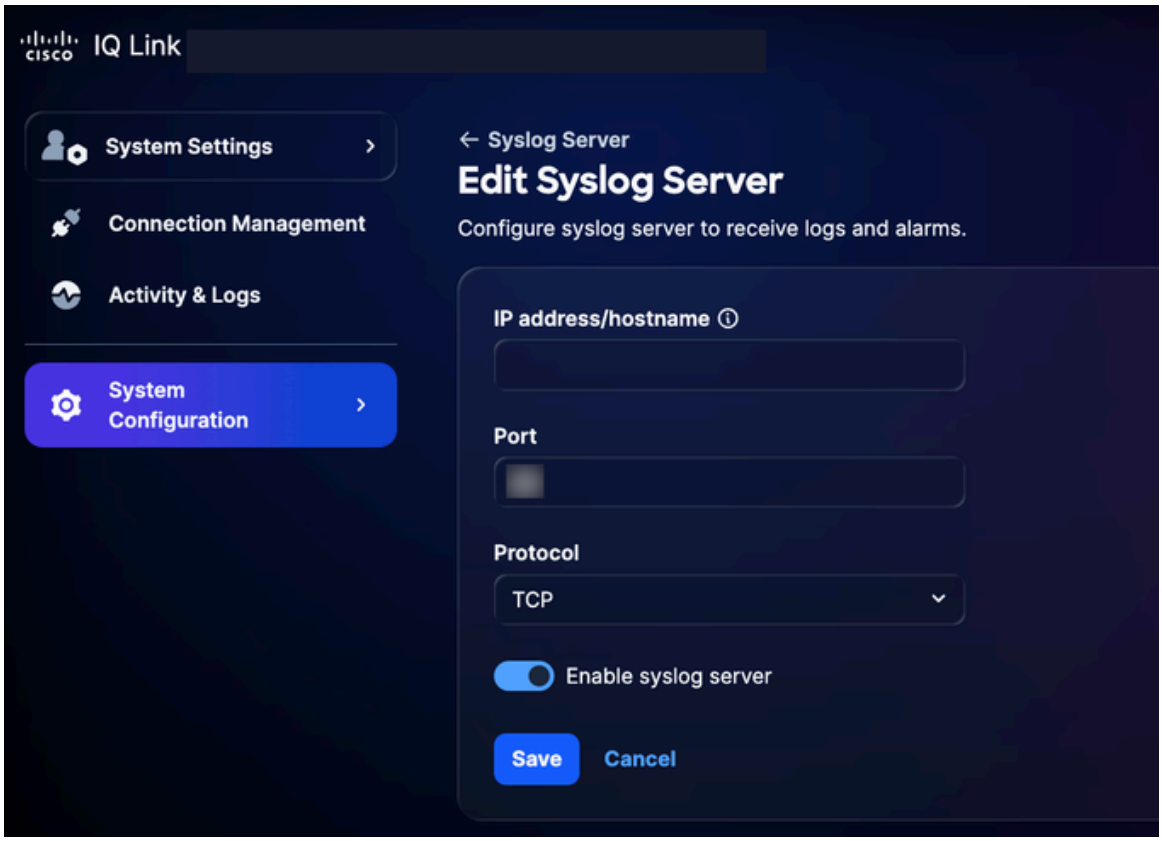
建立系統日誌伺服器

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。



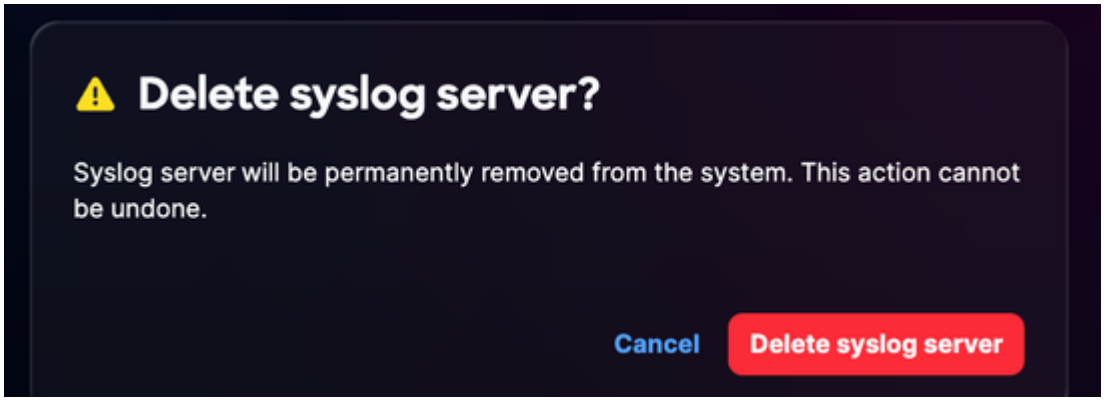
編輯系統日誌伺服器

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。

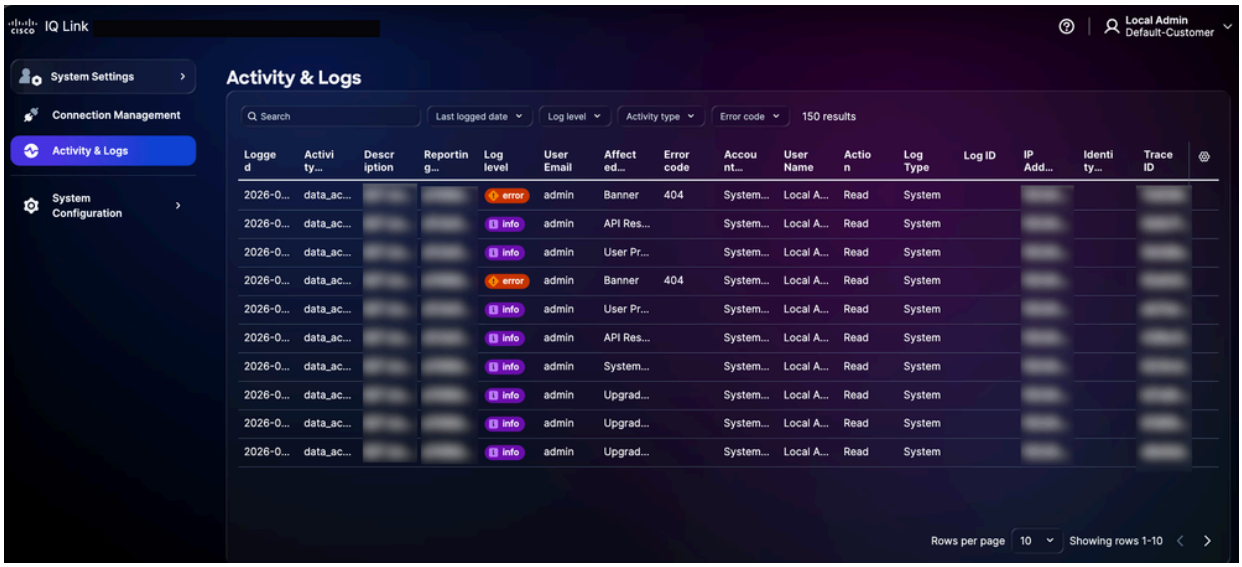


確認

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，使管理員能夠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，幫助輕鬆查詢和管理資訊
- 在網關級別記錄所有API操作

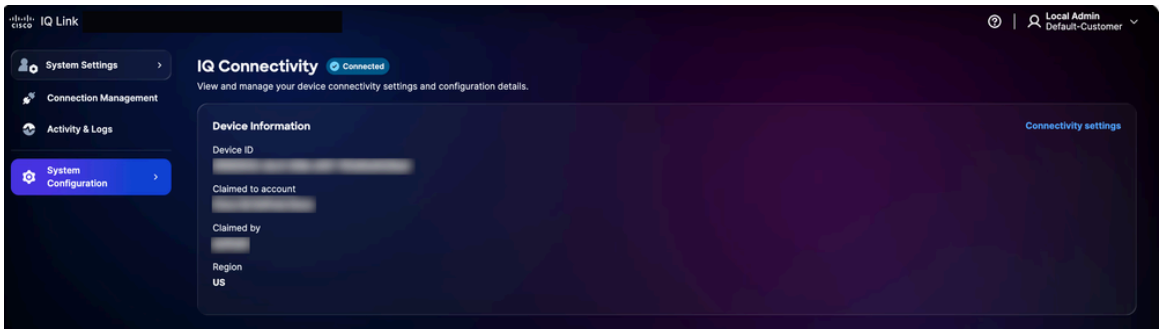
可以使用以下過濾器選項：

- 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

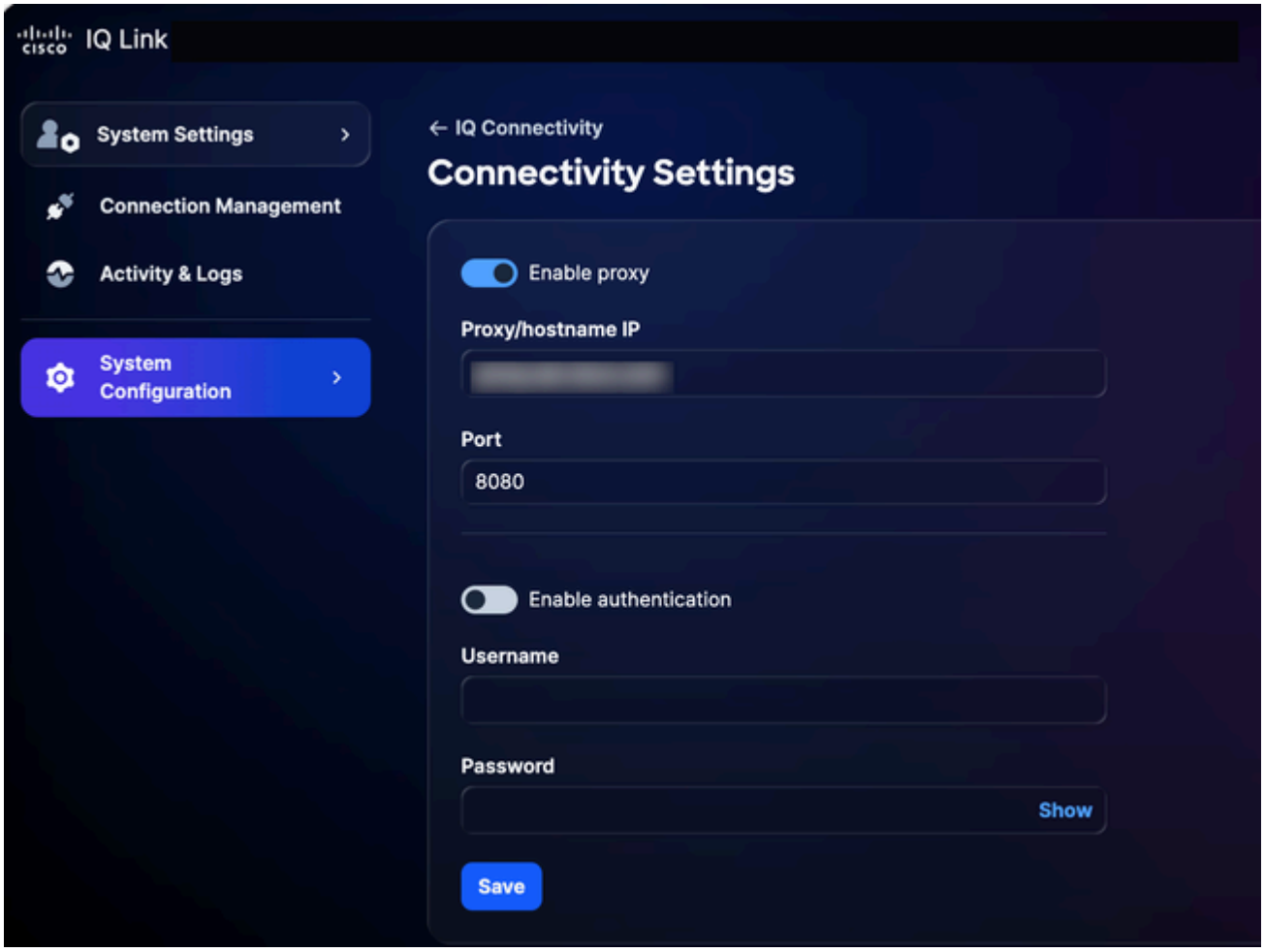
要檢視和管理裝置連線設定和配置詳細資訊，請執行以下操作：

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）

思科IQ Link是內部部署的網路資料收集解決方案，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。配置資料收集可總結為如下共用：

- 正在建立憑據集:建立驗證通訊協定（例如SNMP v1/v2c/v3）以與您的網路裝置通訊。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。

附註：Cisco IQ Link要求在裝置上配置許可權級別15的使用者帳戶對直接連線的資產進行身份驗證。

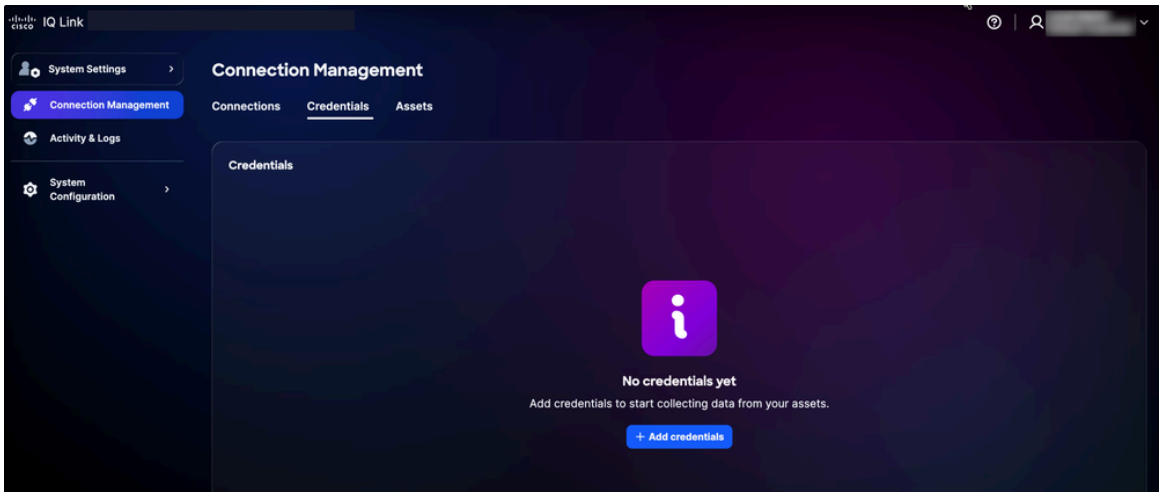
- 將憑證對映到庫存:將憑證集與清單資產進行對映以自動執行身份驗證過程。通過建立將特定IP範圍連結到已定義的憑據集的規則，系統在資料收集期間自動應用正確的身份驗證。這消除了手動輸入錯誤，並確保隨著網路的增長您的配置保持準確。

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

新增憑據

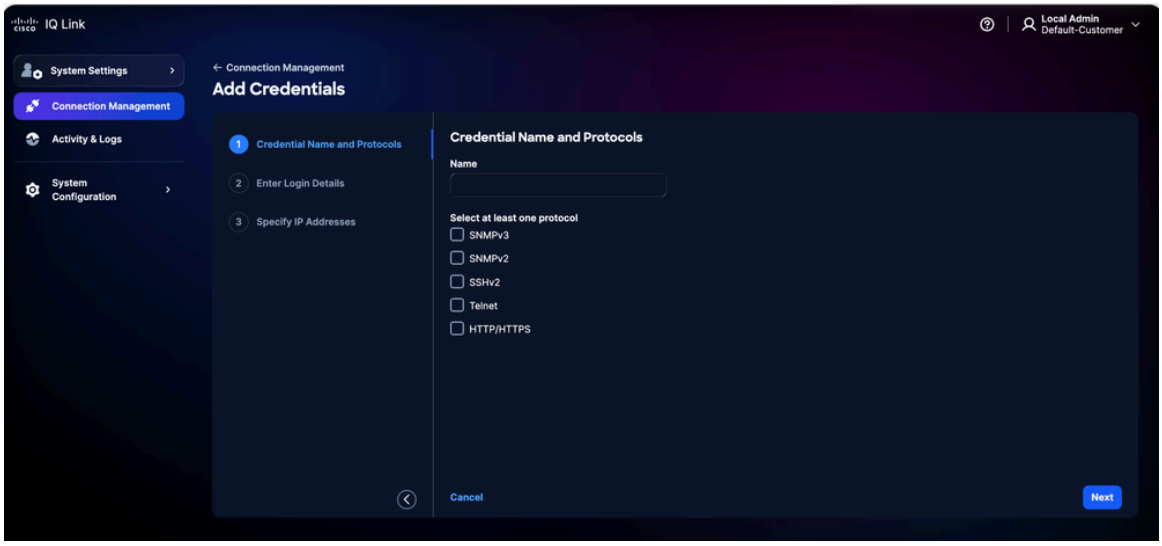
必須先新增憑據才能執行資料收集。要新增憑據，請執行以下操作：

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。

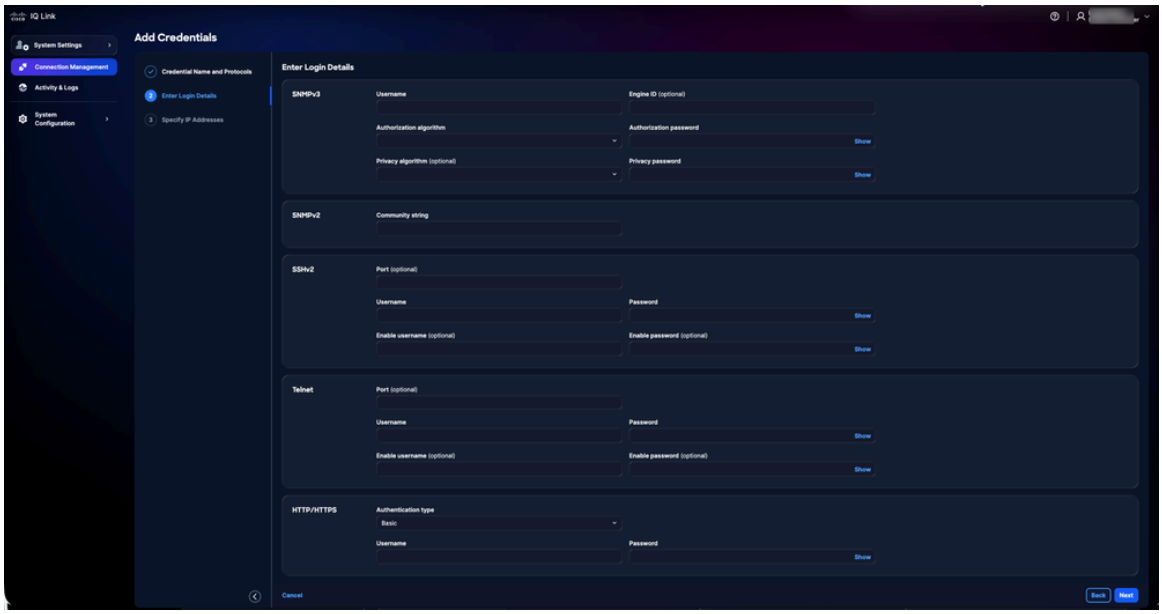


新增憑據

4. 輸入Name。

5. 選中所有適用的協定覈取方塊。

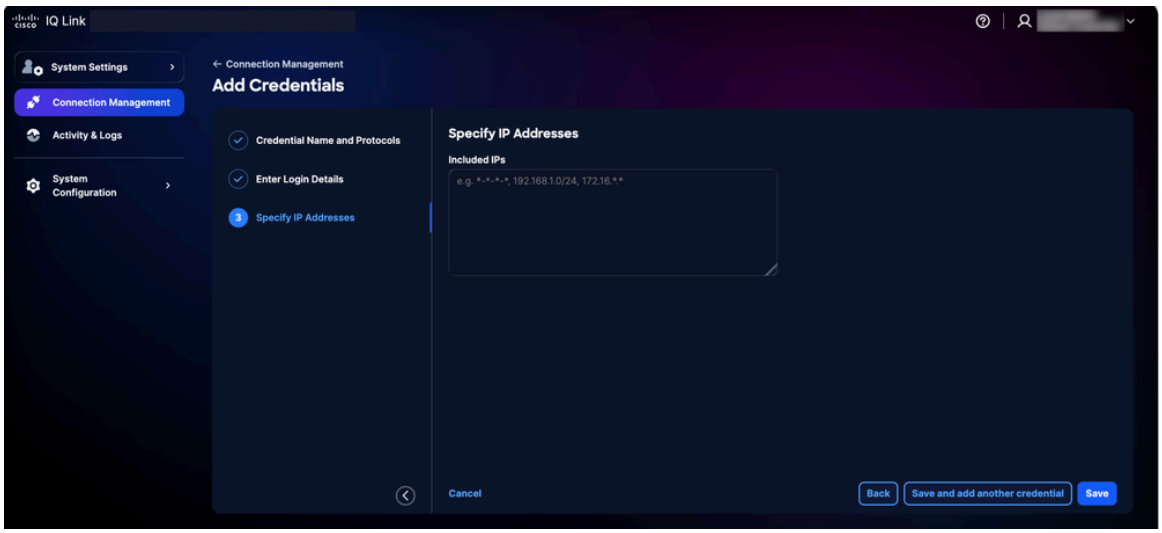
6. 按「Next」（下一步）。



新增憑據詳細資訊

附註：對於上圖，我們說明了在上一步中選擇所有協定時的檢視。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「Next」（下一步）。

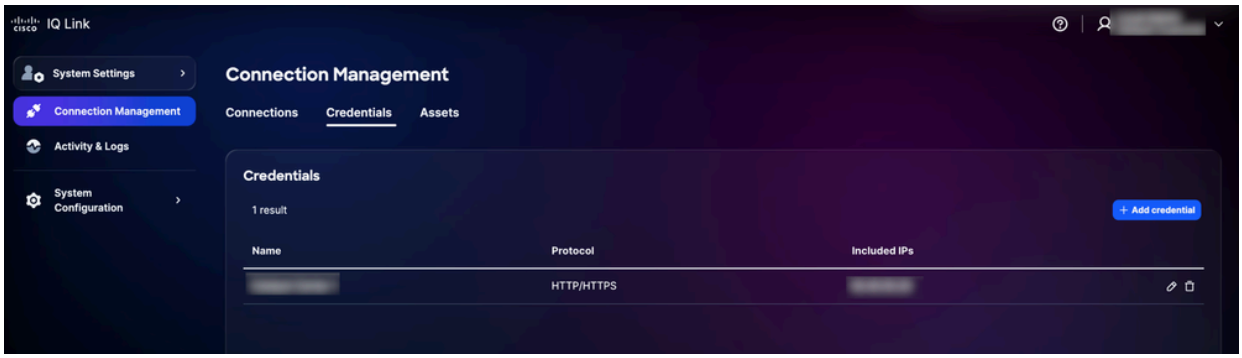


指定IP地址

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.*（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。

憑據選擇示例

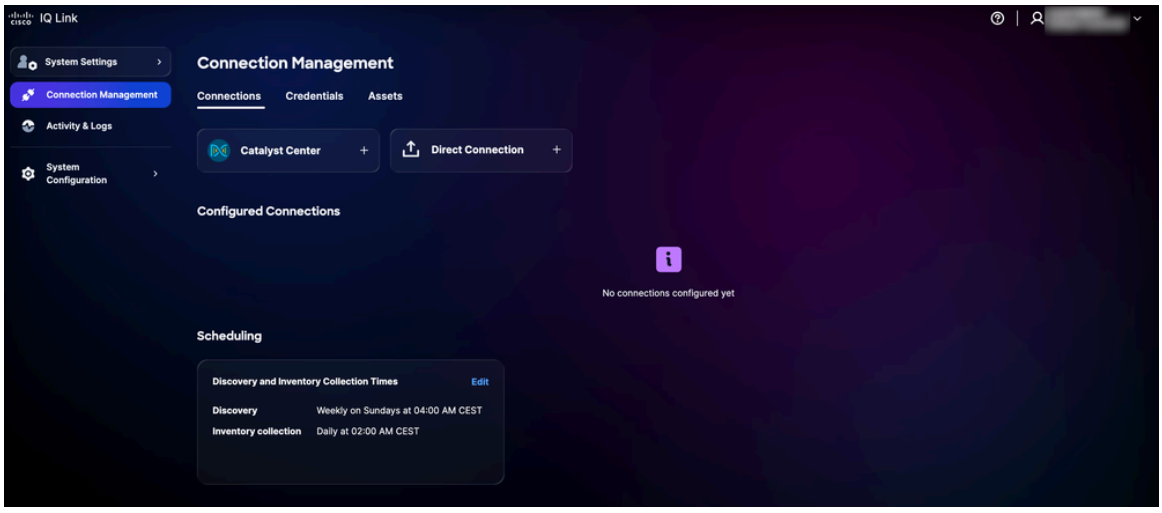
裝置IP	可用的憑據集	所選憑據集
10.10.1.5	10.10.1.5、10.10.1、10.10.*	10.10.1.5（完全匹配）
10.10.2.15	10.10.2.、10.10..*	10.10.2.*（更詳細）
10.10.5.50	10.10...	10.10..（更具體一些）

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

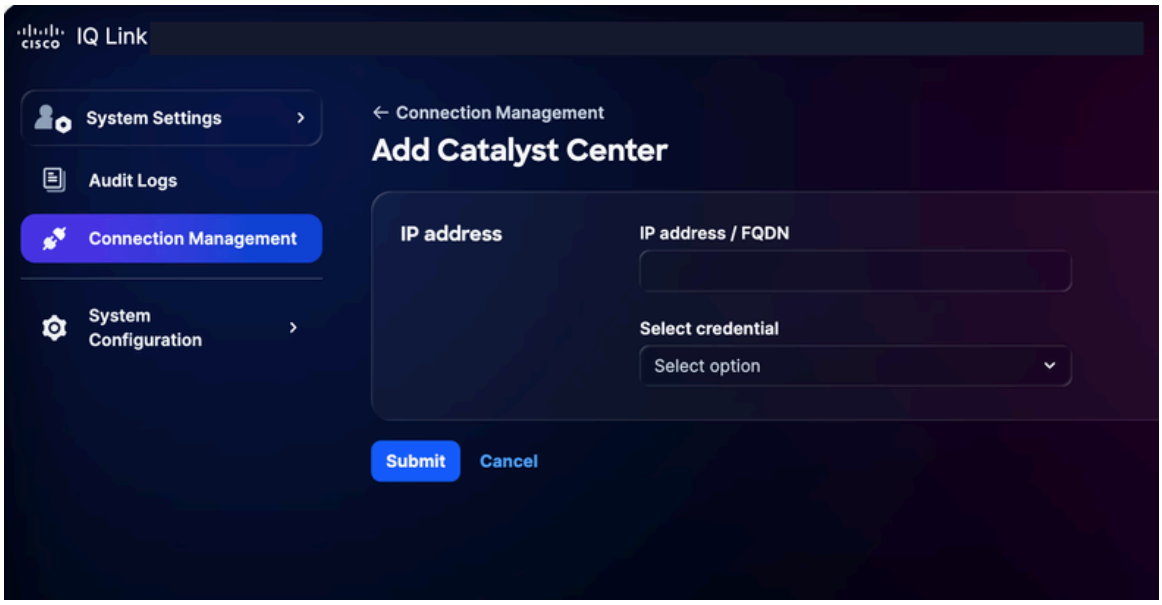
對於使用Catalyst Center進行資料收集：

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。

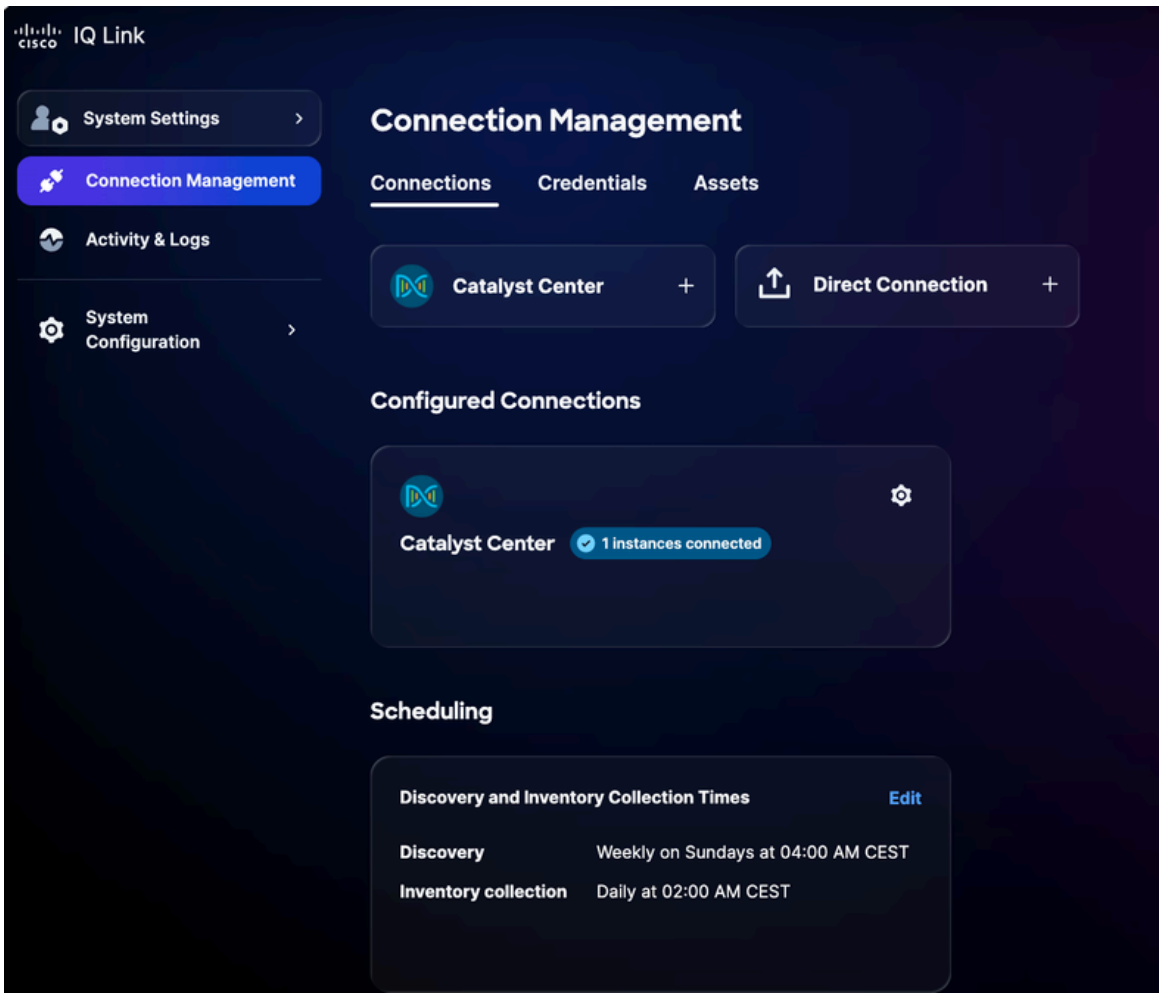


新增Catalyst Center

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

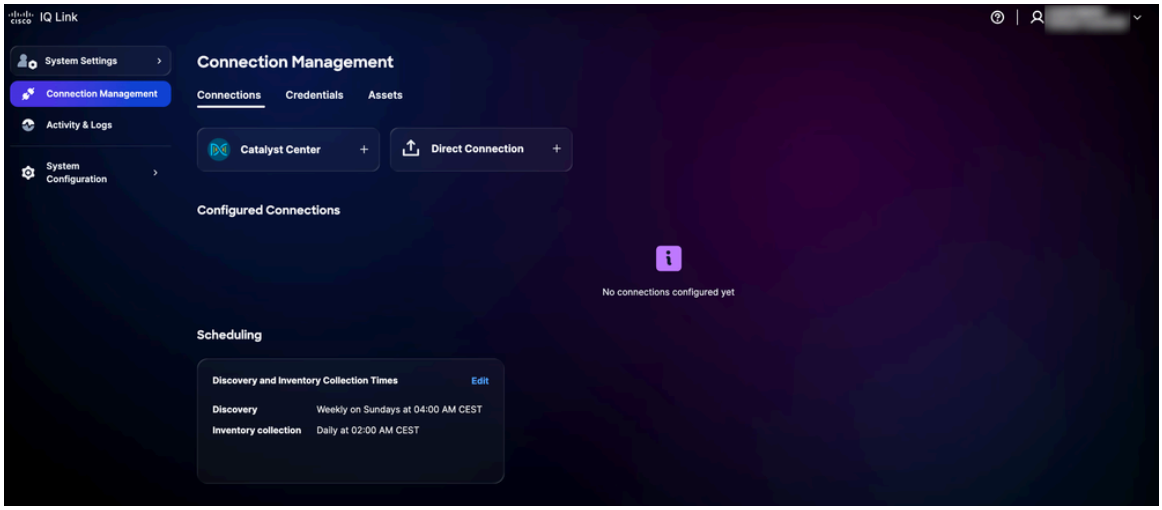
6. 計畫收藏。有關詳細資訊，請參閱計畫。

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

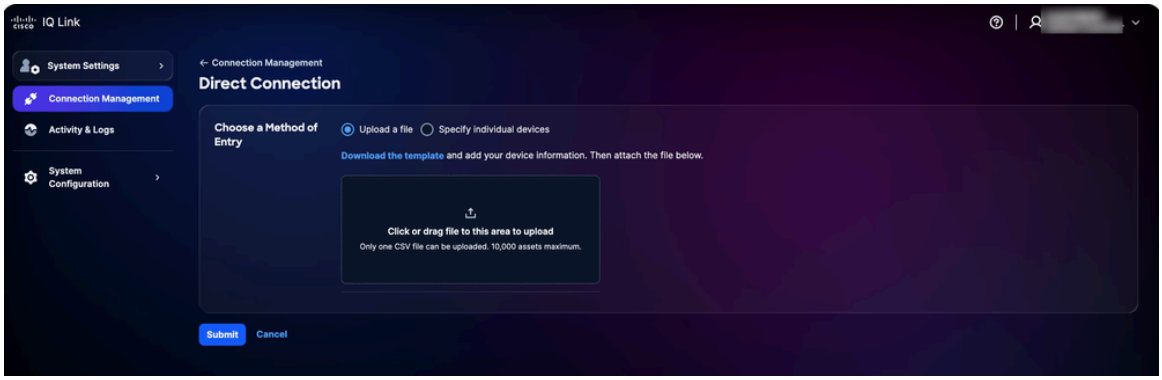
要新增直接連線的裝置，請執行以下操作：

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



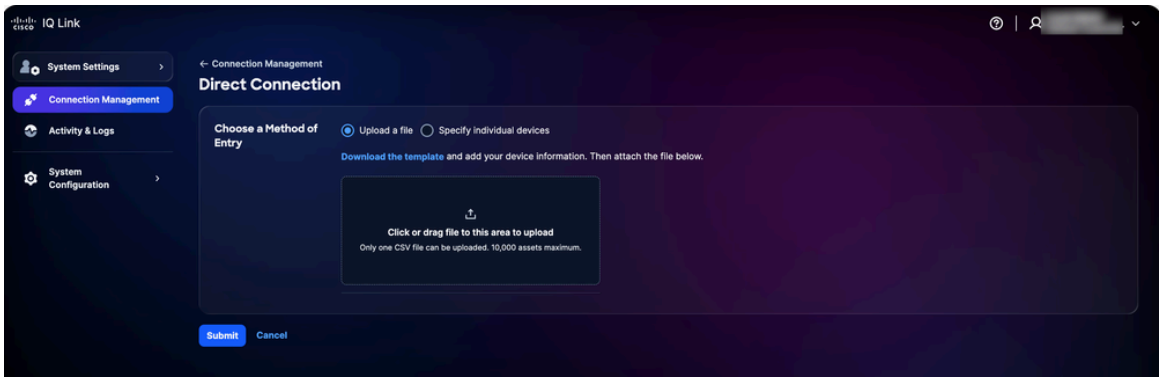
連線管理

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。



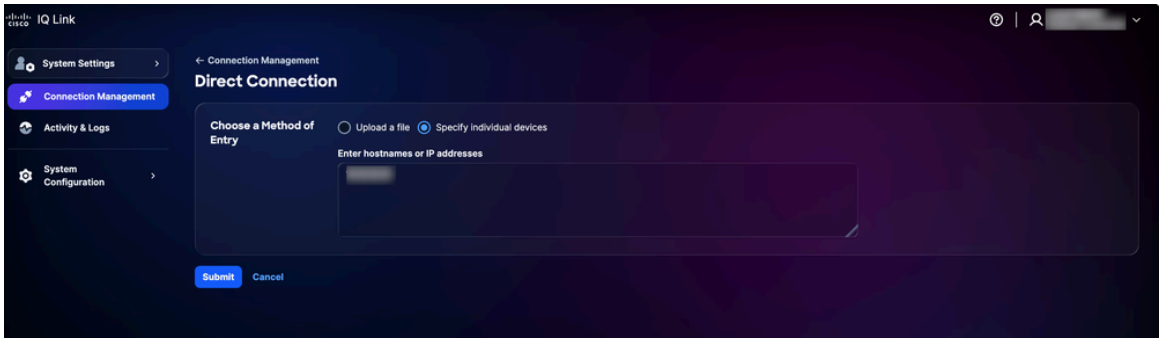
上傳檔案

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。

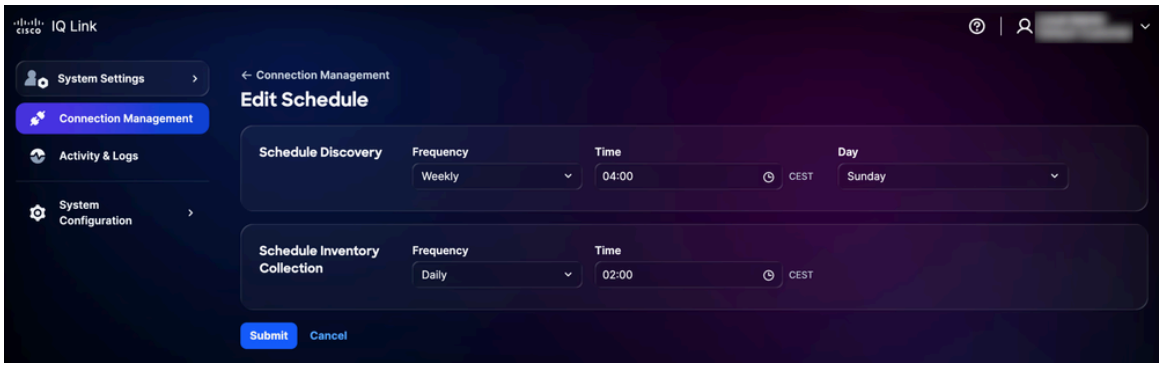
4. 計畫收藏。有關詳細資訊，請參閱計畫。

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

管理員可以配置跨應用程式顯示的自定義橫幅。

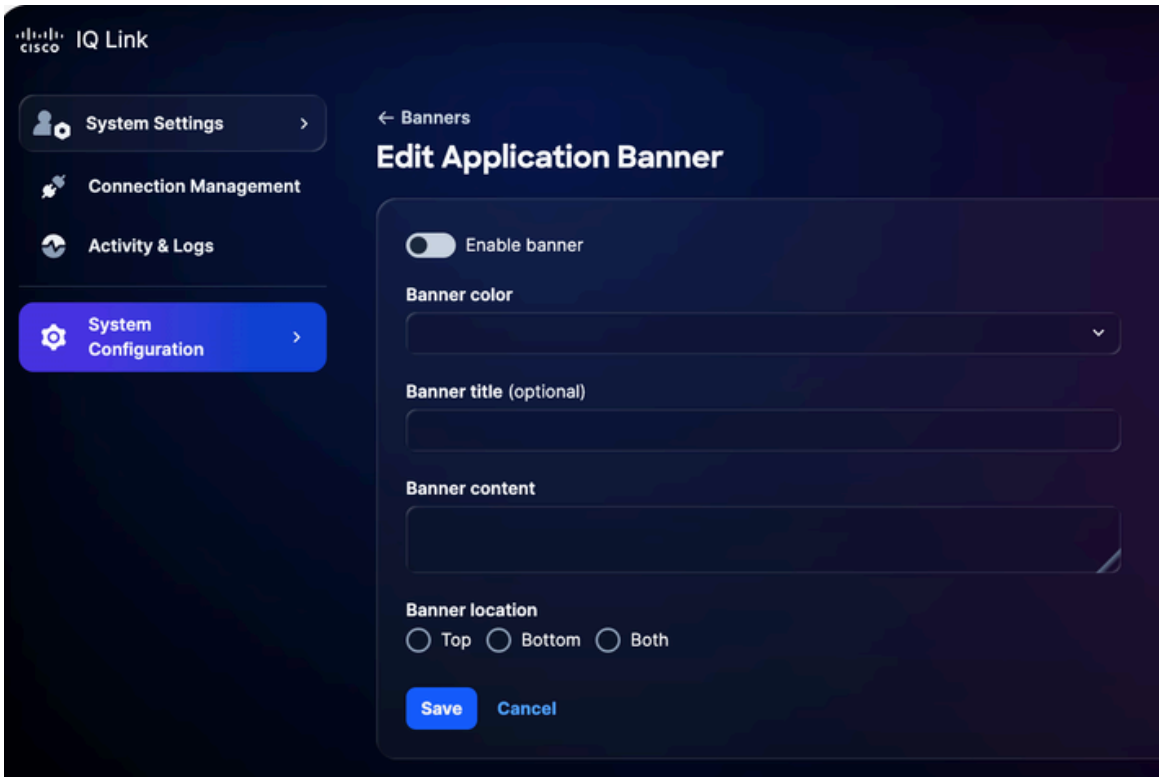
配置橫幅

配置標語：

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「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。

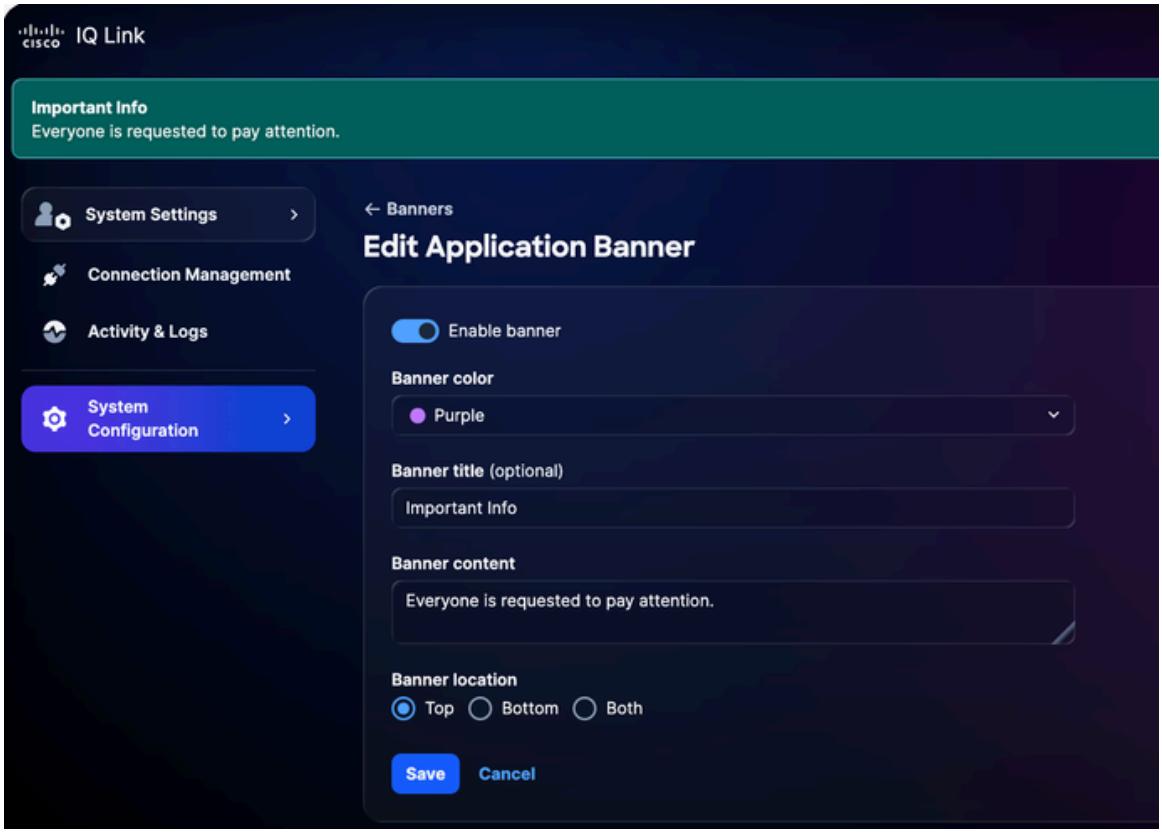
編輯橫幅

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

客戶可以從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診斷操作

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）。