Cisco IQ Link操作ガイドv1.1.0

はじめに

Cisco IQ™は、資産の可視性の向上、環境全体にわたるよりスマートなインサイトの提供、およびケース管理の合理化を目的とした拡張機能と機能をお客様に提供します。さらに、Cisco IQ AI AssistantなどのAI機能は、状況に応じた情報に基づいたプロアクティブな意思決定を可能にし、顧客エンゲージメントと成功のためのプロセスを合理化するコンテキスト把握を提供することで、運用成果とCisco IQのユーザエクスペリエンスを最適化します。

Cisco IQ Linkは、資産テレメトリを安全に収集し、オンプレミスネットワークからCisco IQに送信します。これにより、AIを活用した予測的な洞察が可能になり、ネットワークの可視性を高め、問題を予測し、運用効率を高めることができます。

ローカル認証

管理者は、次のクレデンシャルを使用してCisco IQ Linkにログインする必要があります。

- デフォルトユーザ名:admin
- デフォルトパスワード:Cisco IQ Linkのインストールプロセス中に設定されるパスワード。詳細については、『Cisco IQ Link Getting Started Guide』を参照してください

ログインすると、デフォルトユーザ「admin」とアカウント名「Default-Customer」がホームページに表示されます。

ローカル管理者のセキュリティの設定

パスワードの変更とセキュリティ問題の設定は、System ConfigurationのLocal Admin Securityメニューから行えます。

10分以内に3回、正しいパスワードを入力しようとしました。3回の試行がすべて失敗した場合、セキュリティを保護するためにアカウントが一時的に60分間ロックされます。

ロックアウト期間中はログインできません。失敗した試行回数が多すぎるため、「アカウントがロックされました。Please try again later.」が表示されます。

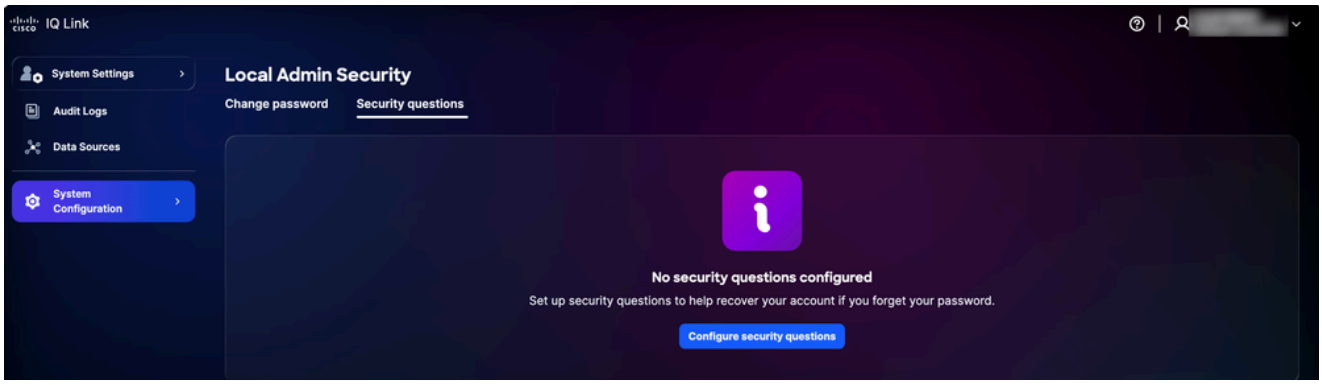
アカウントは60分後に自動的にロック解除され、その時点でログインまたはパスワードのリセットを試みることができます。

セキュリティに関する質問と回答の設定

パスワードを忘れた場合は、秘密の質問を使用して本人確認を行います。パスワードのリセット機能を有効にするには、管理者は5つのセキュリティの質問に対する回答を設定する必要があります。これは1回限りの設定です。

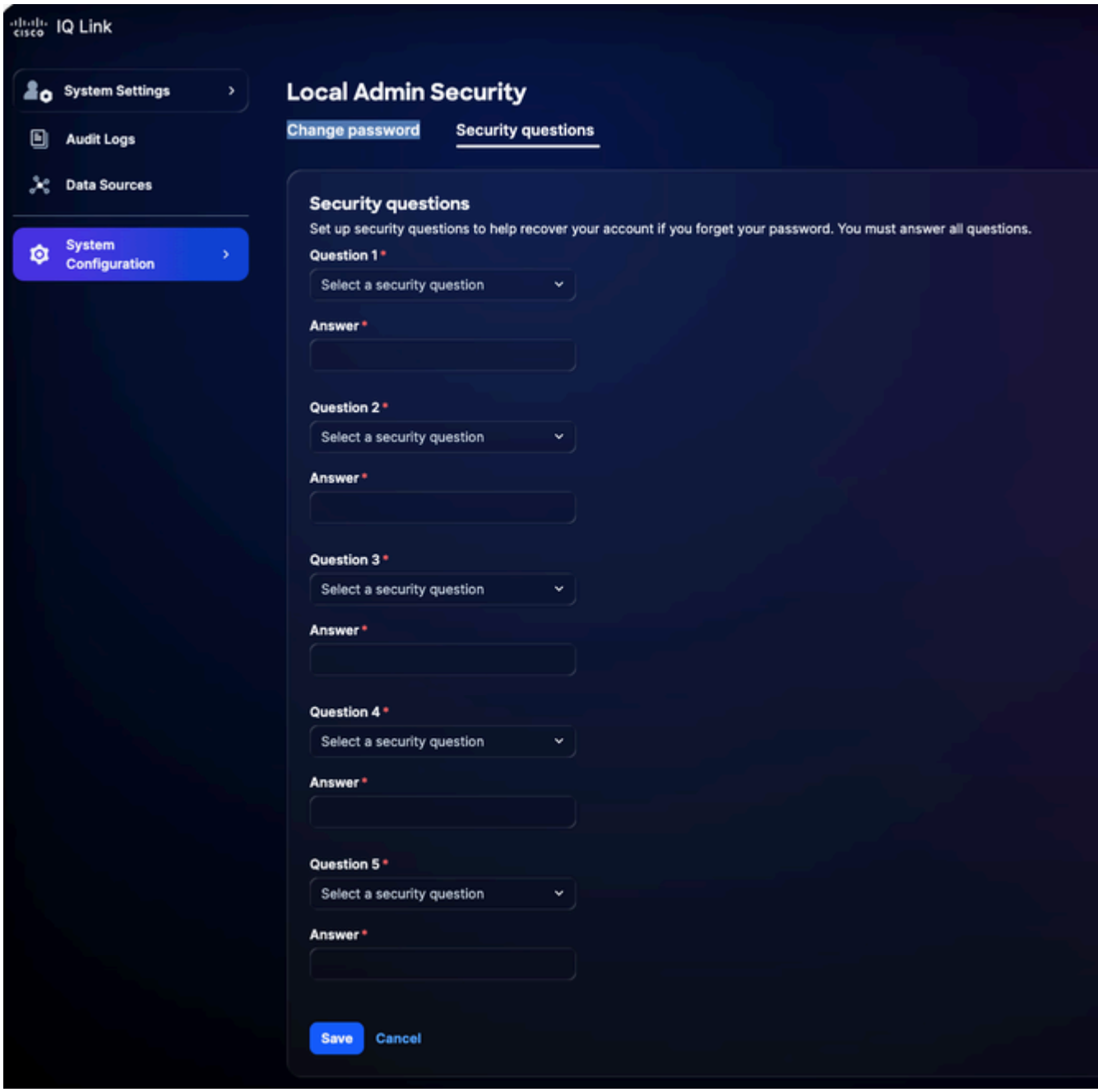
秘密の質問を設定するには、次の手順に従います。

1. System Settingsで、System Configuration > Local Admin Security > Security Questionsの順に選択します。



セキュリティの質問

2. Configure security questionsをクリックします。



セキュリティの質問

3. ドロップダウンリストから5つのセキュリティの質問を選択します。

4. 各質問に対する回答を入力します。

5. [Save] をクリックします。

注：
・ 回答は大文字と小文字が区別されません。たとえば、「SMITH」と「smith」は同じとみなされます
・ 余分なスペースは無視され、「 Smith 」と「 Smith 」は同じように扱われます

注：必要に応じて、後で回答を更新できます。回答を更新すると、以前の回答はすべて置き換えられるため、変更する質問だけでなく、5つの質問すべてに対して再度回答を入力する必要があります。

パスワードの管理

Cisco IQのパスワードを管理できるのは、ローカルの管理者だけです。

前提条件

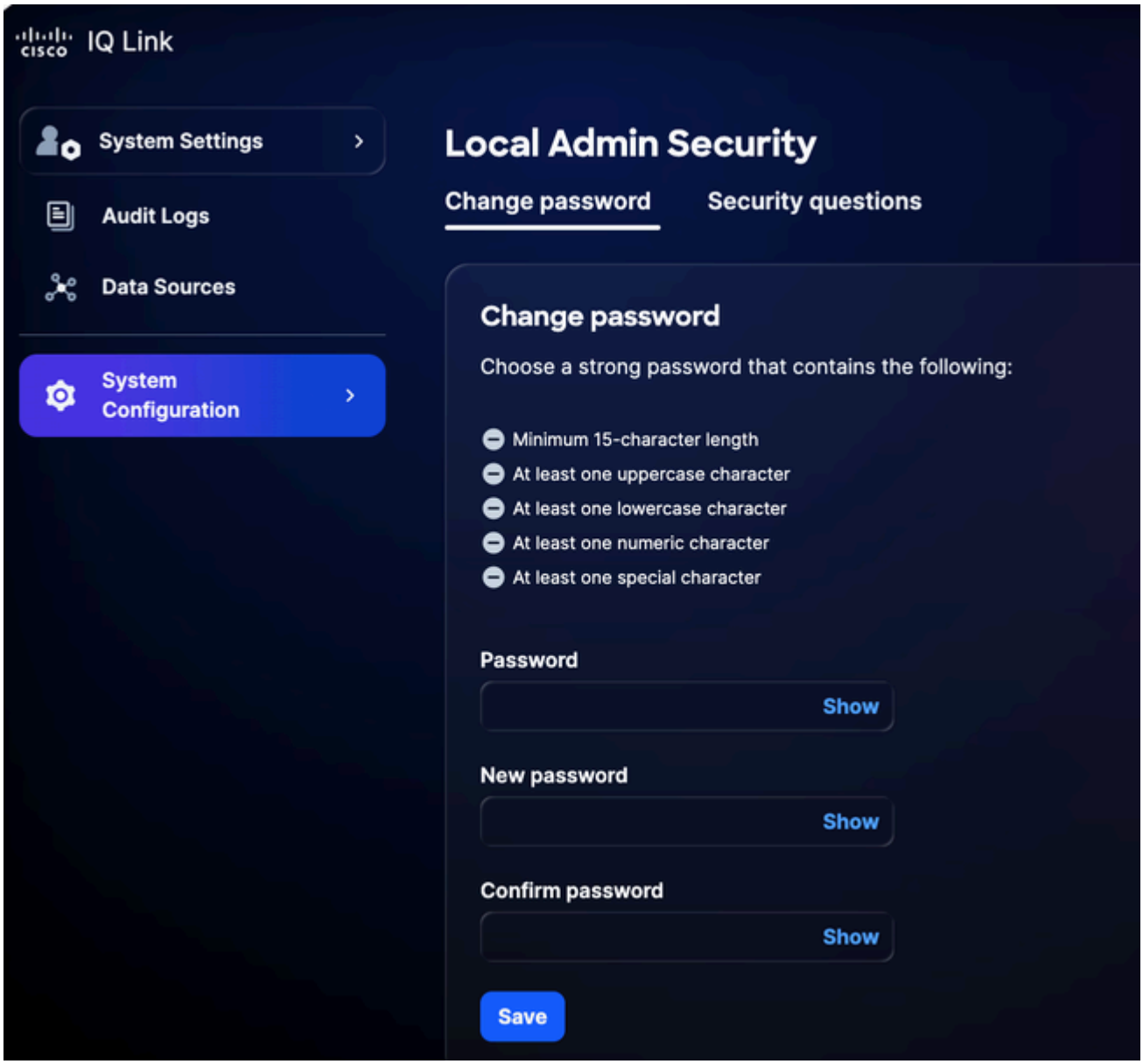
パスワードを管理するには、次の条件を満たす必要があります。

- ローカル管理者である
- シングルサインオン(SSO)または外部認証ではなく、ローカル管理者アカウントを使用している
- Cisco IQにログインしています
- 現在のパスワードがわかっている

パスワードの変更

パスワードを変更するには、次の手順を実行します。

1. System Settingsで、System Configuration > Local Admin Security > Change Passwordの順に選択します。



パスワードの変更

2. 現在のパスワードを入力します。
3. 新しいパスワードを入力します。
4. 確認のため、新しいパスワードをもう一度入力します。
5. [Save] をクリックします。

パスワードは、Cisco IQ仮想マシン(VM)を含むCisco IQシステムで更新されます。

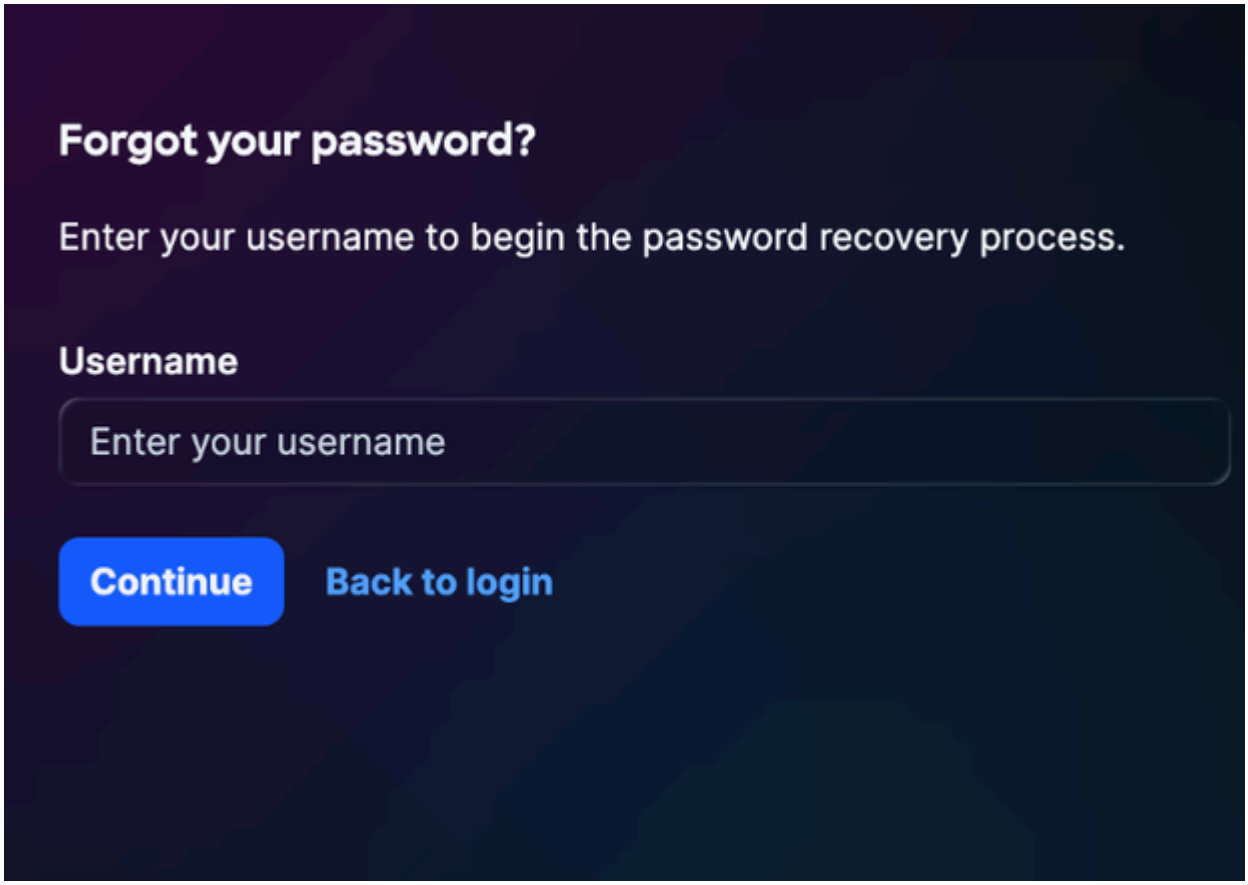
パスワードを忘れた場合のリセット

前の手順でセキュリティの質問を設定している場合は、セキュリティの質問の検証プロセスを使用して、忘れたパスワードをリセットできます。詳細については、「セキュリティに関する質問

と回答の設定」を参照してください。

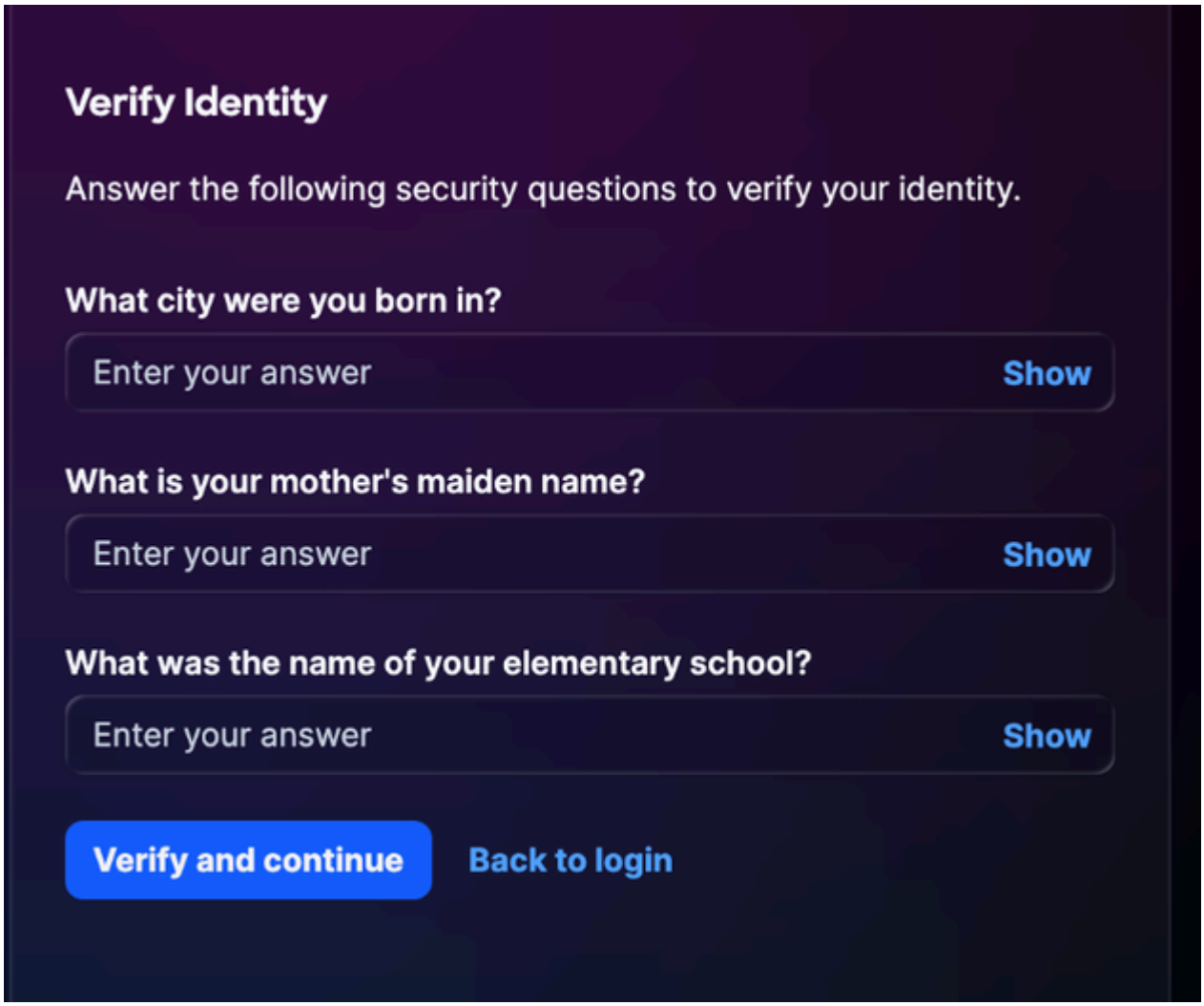
忘れたパスワードをリセットするには、次の手順を実行します。

1. Cisco IQ Linkのログインページに移動します。
2. Forgot Passwordをクリックします。



パスワードを忘れた

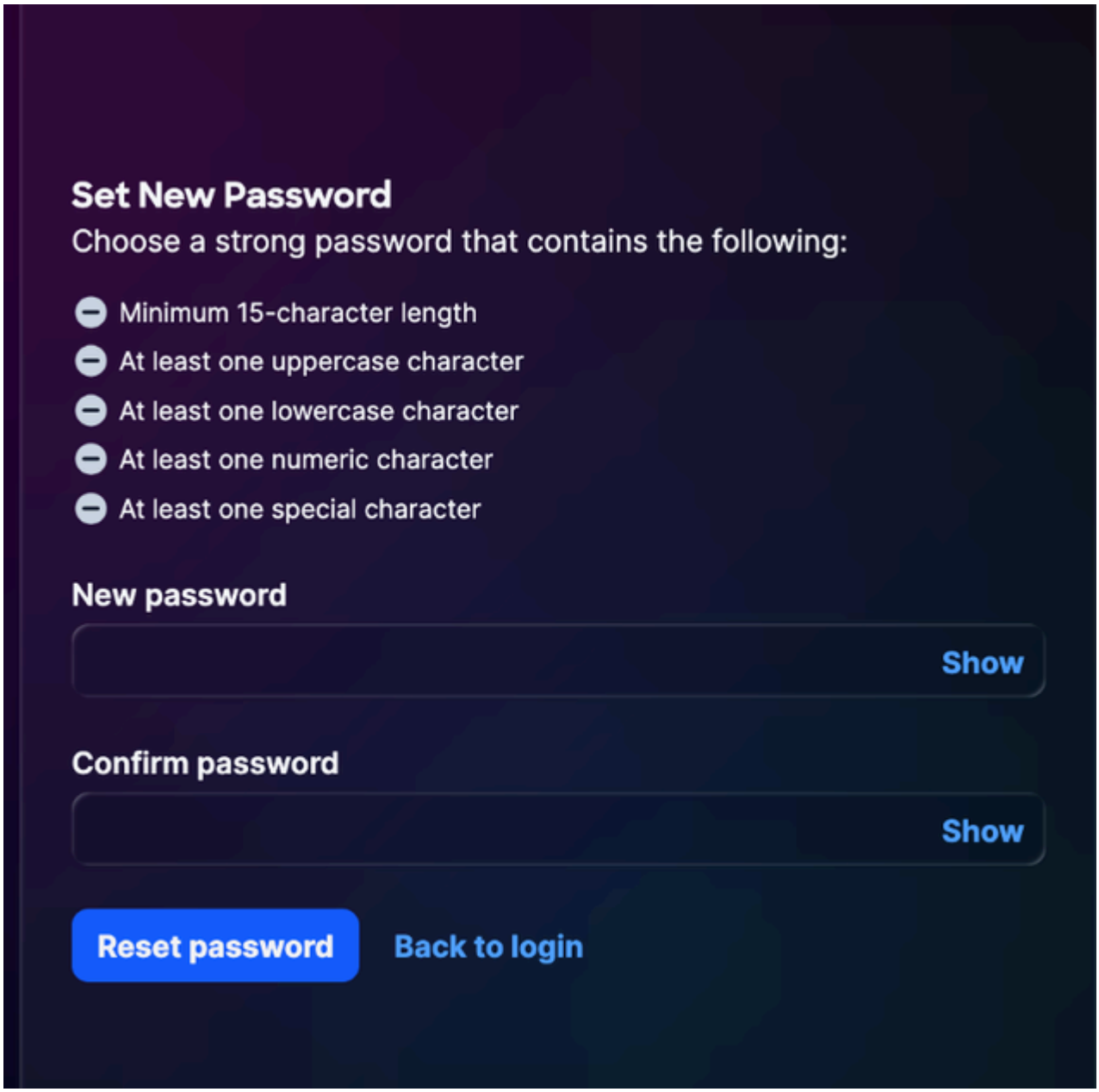
3. ユーザ名を入力します。
4. [Continue] をクリックします。Verify Identityページには、以前に設定した5つの質問のうち、ランダムな3つの質問が表示されます。



IDの確認

注：上記のセキュリティに関する質問はユーザ固有であり、状況に応じて異なります。

5. 表示された3つの質問すべてに対する回答を入力します。
6. Verifyをクリックして、続行します。送信された応答が以前に保存した応答と一致する場合は、新しいパスワードの入力を求められます。



パスワードのリセット

注:10分間に3回、セキュリティの質問に正しく回答しようとしました。3回の試行がすべて失敗した場合、セキュリティを保護するためにアカウントが一時的に60分間ロックされます。

ロックアウト期間中はパスワードをリセットできません。システムに「Account locked due to too many failed verification attempts.Please try again later.」が表示されます。

アカウントは60分後に自動的にロック解除され、その時点でログインまたはパスワードのリセットを試みることができます。

---

7. 新しいパスワードを入力します。
8. 確認のため、パスワードを再入力します。

9. [Submit] をクリックします。

IDプロバイダーの設定

Cisco IQ Linkにログインすると、管理者はさまざまな設定を行うことができます。管理者は、ローカル管理またはアイデンティティプロバイダー(IDP)設定を使用してCisco IQ Linkにログインできます。

SSOのOkta IDP SAML設定

IDP SAMLを設定するための前提条件

- Cisco IQ Linkへのローカル管理者アクセス
- IDPポータルへのアクセス

SSOのIDP SAML設定

SSO用にIDP Security Assertion Markup Language(SAML)を設定するには、次の手順を実行します。

1. IDPポータルに移動します。
2. Cisco IQ Linkインスタンスに次のアトリビュートを設定します。

Cisco IQ Link属性

フィールド	値
アプリケーション名	<アプリケーション名>
環境	ESPビジネスアプリケーション
アプリケーション所有者グループ	IDP設定の所有者
チームメーラー	チームのメーラー

フィールド	値
対象者	非従業員
オンボーディングカテゴリ	「新規オンボーディング」を選択します。

SAML設定パラメータ

項目	コンフィギュレーション	例
対象ユーザー（エンティティID）	FQDN名	mymanagementhost.mydomain.com
シングルサインオンURL	SAML ACSエンドポイント	https://mymanagementhost.mydomain.com/saml/acs
名前IDの形式	電子メールアドレス	NA
アプリケーションユーザ名	ユーザ名	NA

3. 次の必須属性ステートメントを設定します。

注:IDP属性の変更は、特定のプロバイダーと設定によって異なります。例として、Cisco IDPとその属性を次で共有します。

- 最初のエントリ
    - 名前：ユーザ名
    - 値: user.login
- 2番目のエントリ
    - 名前：プライマリ電子メール
    - 値:user.email
- グループ属性ステートメント

- 名前:groups
- フィルタ: REGEX
- 値: .*

4. アプリケーションのシングルログアウト(SLO)設定を構成します。

SLOの設定値

フィールド	値
署名証明書	Oktaの場合、この証明書はSLOを有効にする場合にのみ必要です。Identity ProvidersのDownload SP Certificateを使用して、署名証明書をダウンロードします。ファイルをsp-public-key.crtとして保存します。詳細は、『シングルログアウト設定』を参照してください。
SPメタデータ	SPメタデータは、ADFS IDPにのみ必要です（Oktaには必要ありません）。
シングルログアウトを有効にしますか	YesまたはNo
シングルログアウトURL	https://mymanagementhost.mydomain.com/saml/logout
SP発行者（対象ユーザー/エンティティIDまた	https://mymanagementhost.mydomain.com

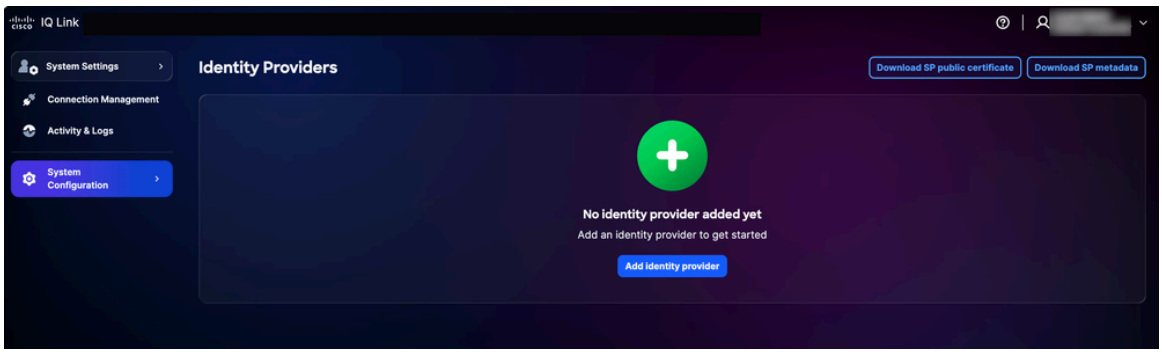
フィールド	値
は ACS URL ）	

5. Downloadアイコンをクリックして、「SP Metadata」ファイルをダウンロードします。
6. プロバイダーの要求に応じてアプリケーションをプロビジョニングまたは作成します。

IDPの追加

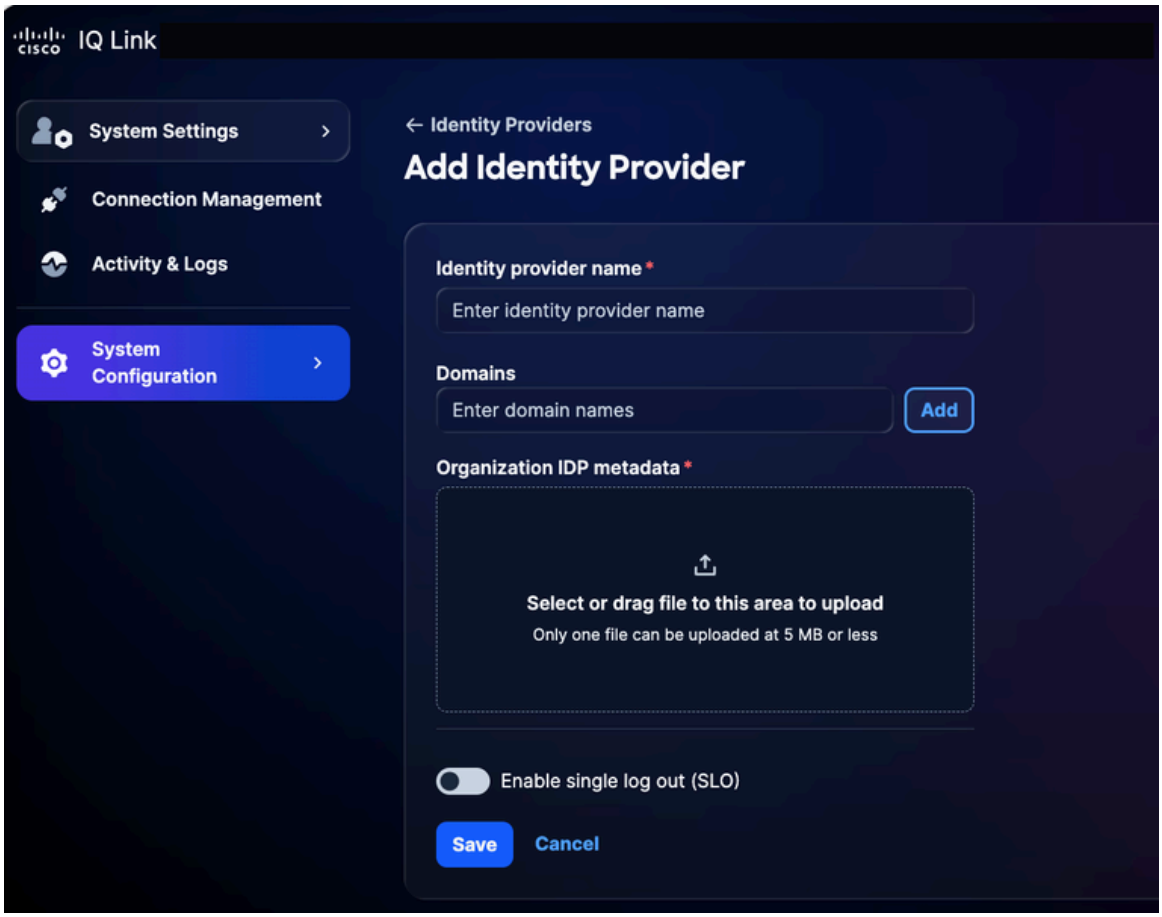
Cisco IQ LinkでIDPを追加するには：

1. System Settingsで、System Configuration > Identity Providersの順に選択します。Identity Providersページが表示されます。



IDPホームページ

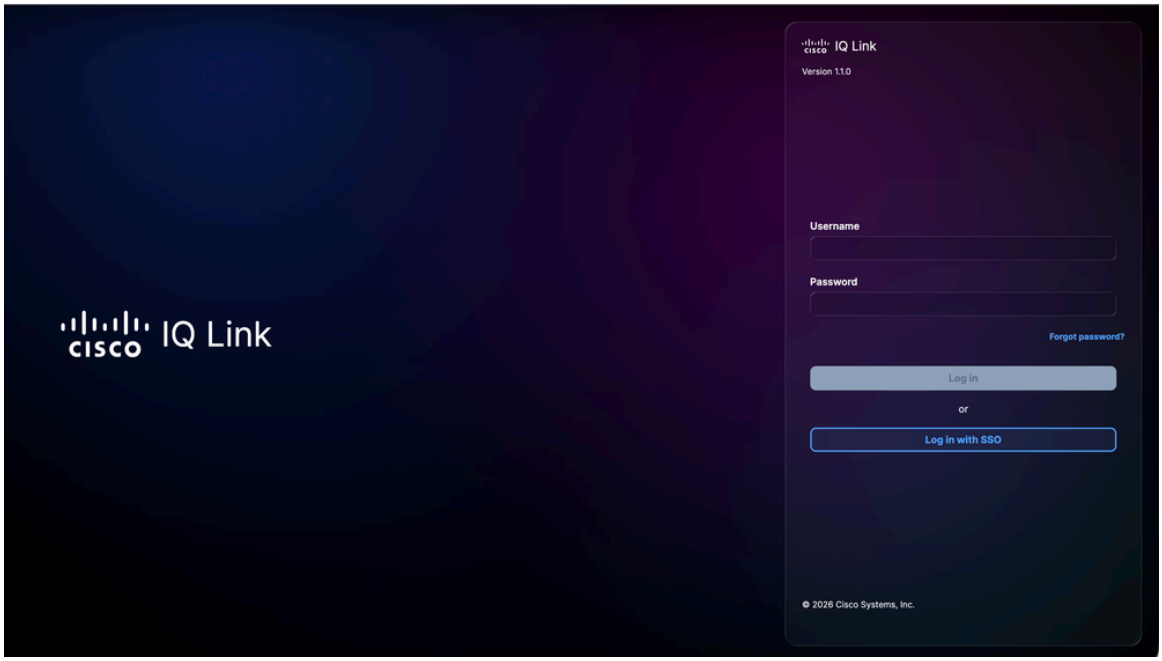
2. Add Identity Providerをクリックします。Add Identity Providerページが表示されます。



IDプロバイダーの追加

> 注：一度に追加できるIDPは1つだけです。

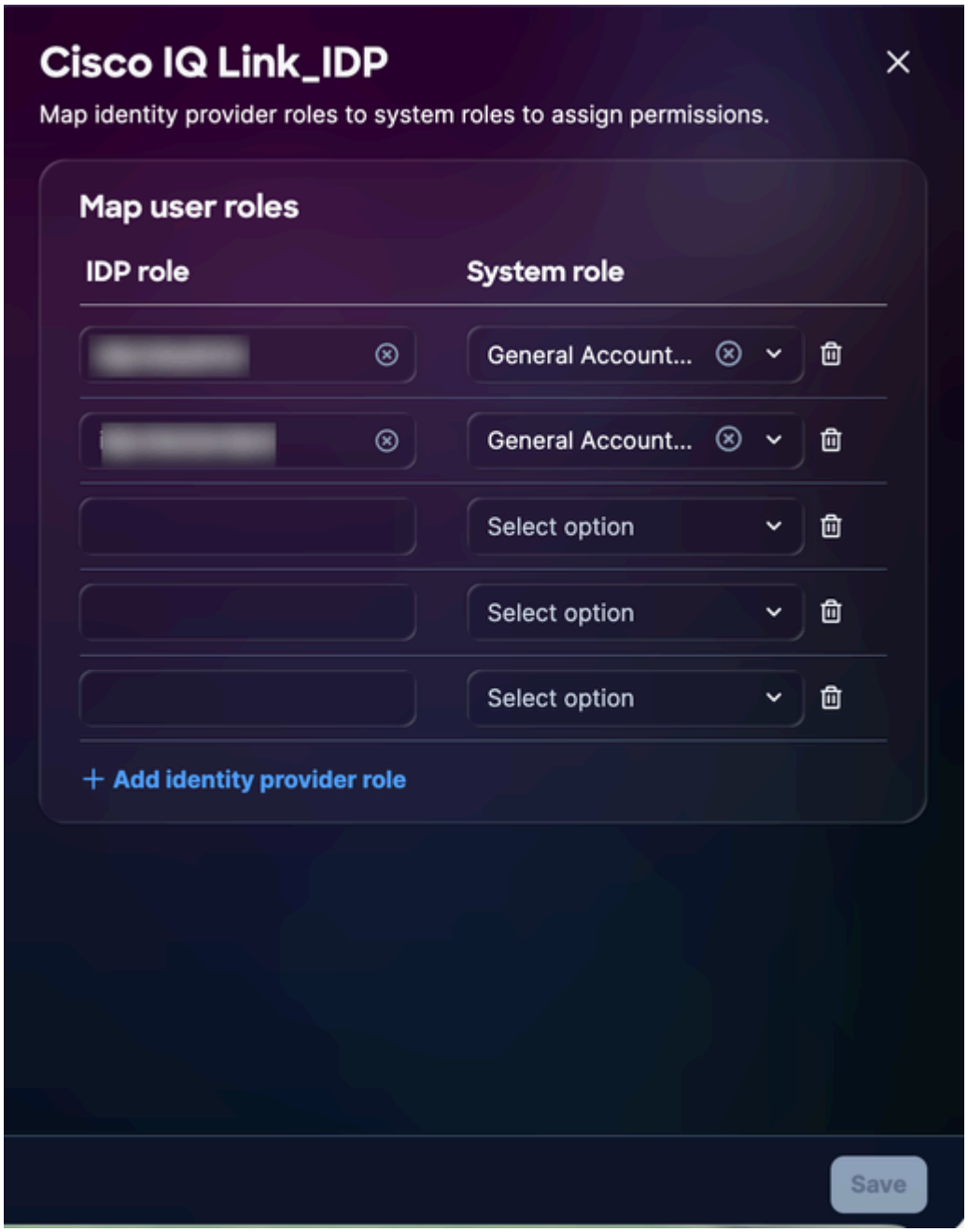
3. IDプロバイダー名を入力します。
4. Addをクリックして、Cisco IQ Linkで設定されたドメイン名をDomainsフィールドに追加します。
5. IDPアプリケーションから取得したSAMLメタデータファイルを組織IDPメタデータフィールドにドラッグアンドドロップするか、アップロードします。このファイルには、証明書の詳細とサービスプロバイダー(SP)エンティティの詳細が含まれています。
6. （オプション）Enable single logoutトグルボタンをオンにします。SLOは後で有効にすることもできます。
7. [Save] をクリックします。
8. 設定が完了すると、ログインページにSSO（IDP経由）でログインするためのオプションが表示されます。



Cisco IQ Linkログイン

ロールマッピングの設定

1. 追加されたIDPから、More Optionsアイコン> Map Rolesを選択します。Map user rolesページが表示されます。

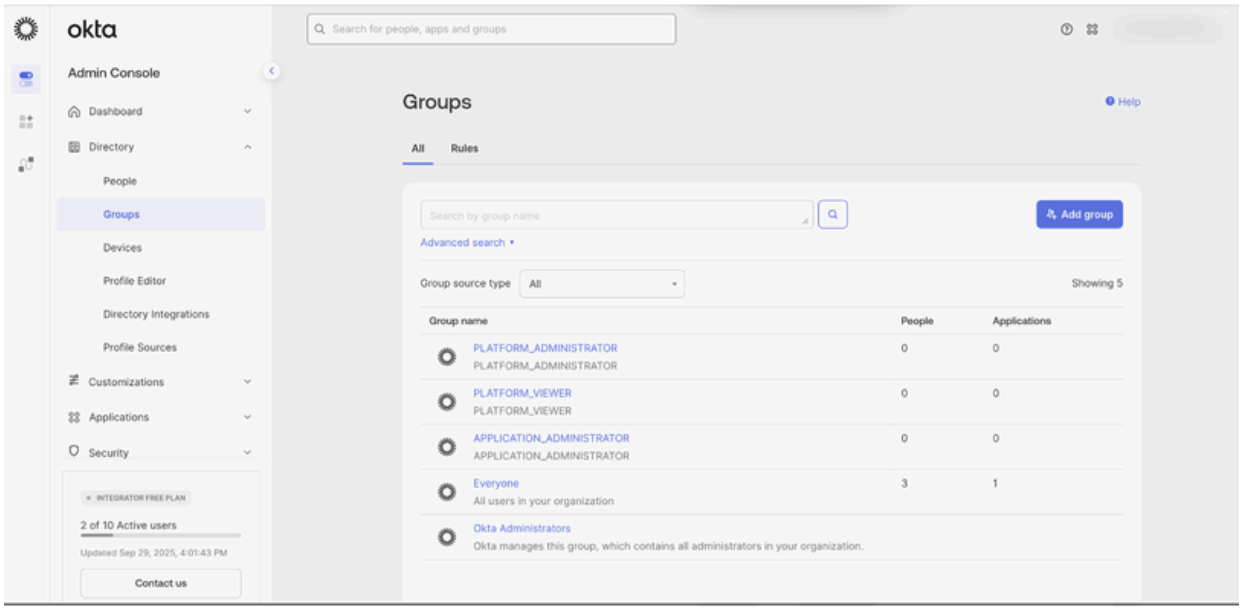


ユーザロールのマッピング

2. 選択したシステムロールのIDPロールを入力します。次のシステムロールがサポートされています。

    - general_account _administrator：汎用アカウント管理者には、製品のすべてのアクションを実行するフルアクセス許可があります
    - general_account _viewer：一般アカウントビューアには読み取り専用アクセス権があります

注：IDPロールはオープンテキストフィールドです。組織のIDPで設定されているグループ名またはロール名と正確に一致している必要があります。Oktaグループの例を次に示します。



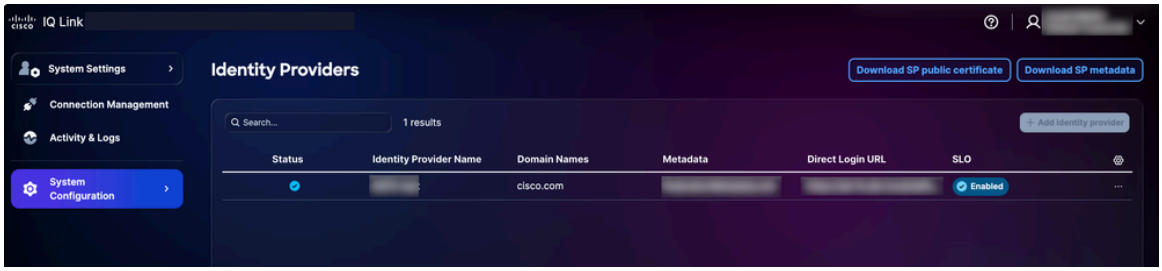
ロールマッピングの参照

3. Add identity provider roleをクリックして、必要に応じて追加のロールをマッピングします。
4. [Save] をクリックします。

シングルログアウトの設定

SLOを有効にする場合は、SLO URLを含むメタデータをアップロードする必要があります。この設定を行うには、IDプロバイダーの設定を編集して、シングルログアウトの有効化のトグルをオンにします。SLOの設定を完了するには：

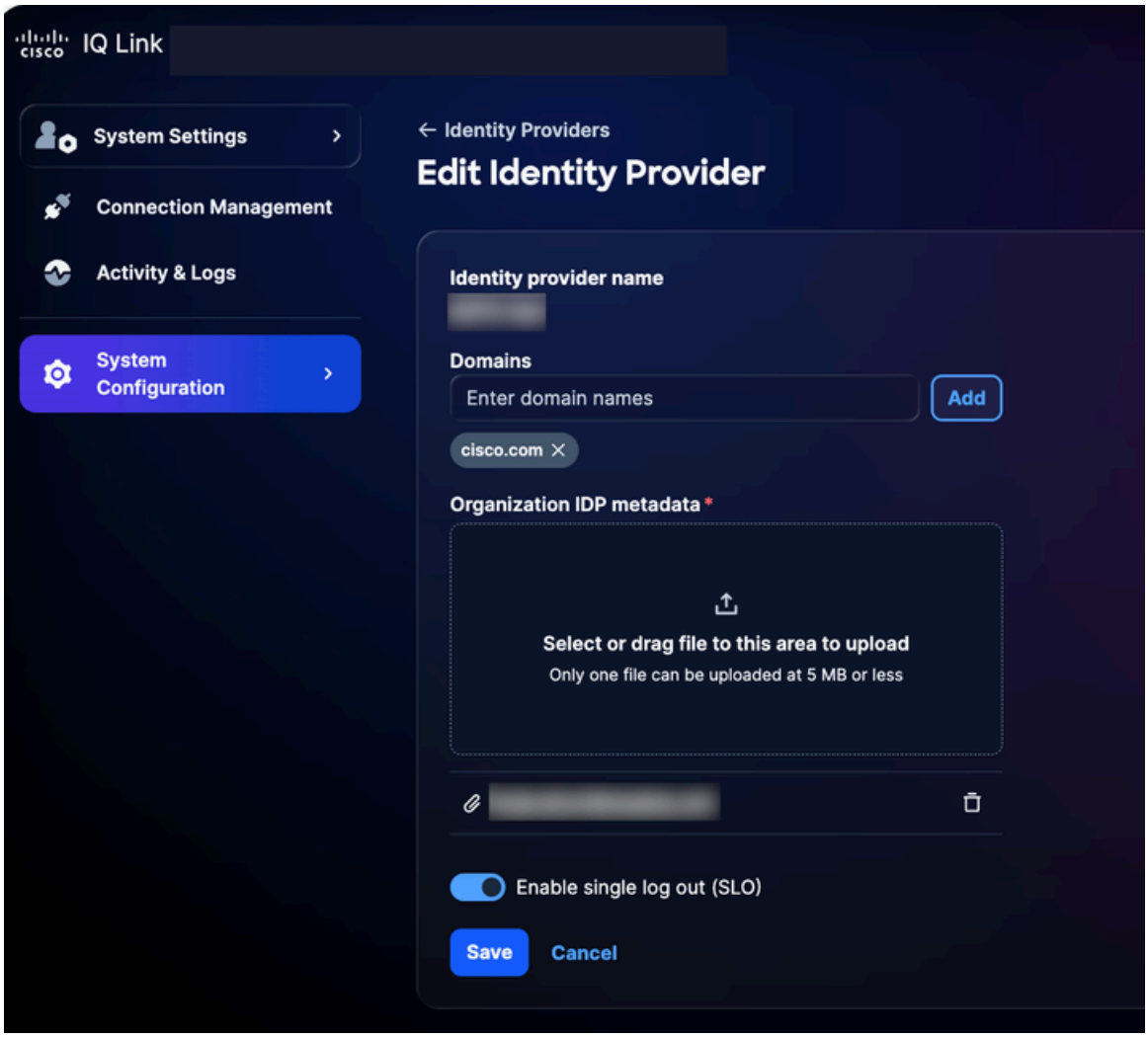
1. Identity Providersページで、Download SP public certificateをクリックします。



公開証明書のダウンロード

2. ダウンロードファイルをsp-public-key.crtとして保存します。
3. IDPポータルに移動します。
4. SSO用のIDP SAML設定セクションで生成された署名証明書ファイルをアップロードします。
5. IDPメタデータファイルを再度ダウンロードします。

6. Identity Providersページで、追加されたIDPのMore Optionsアイコン> Editを選択します。



IDプロバイダーの編集

7. Enable single log out (SLO)トグルボタンをオンにします。
8. 新しくダウンロードしたメタデータファイルをアップロードします。
9. 次のチェックリストを使用して、SSOおよびSLO機能を確認します。

検証チェックリスト：

- ローカル管理者のログインに成功しました
- IDPポータルの設定とプロビジョニング
- IDPがCisco IQに「Success」ステータスで追加される
- 役割のマッピングの構成とテスト
- SPメタデータがダウンロードされ、証明書が抽出されます

- SLOが有効になっている場合、SLOの設定は実際の署名証明書で完了します
- エンドツーエンドのSSO/SLOフローが正常にテストされる

IDP問題のトラブルシューティング

次のリストは、IDPステータス、証明書エラー、SSOログイン障害、およびSLO設定に関連する問題を迅速に特定して解決するのに役立つ、一般的な問題と考えられる解決策の概要を示しています。

トラブルシューティング

お問い合わせ内容	ソリューション
IDPステータスが「Incomplete」と表示される	ロールマッピングの設定を確認する
証明書エラー	証明書の形式と有効性の確認
SSOログインの失敗	属性マッピングとグループ割り当ての検証
SLOが期待どおりに動作しない	証明書が正しくアップロードされ、SLO URLが設定されていることを確認します

SSO用のADFS IDP SAML設定

このセクションでは、Cisco IQのSAML IDPとしてMicrosoft Active Directory Federation Services(ADFS)を設定する方法について説明します。

SSO用にADFS IDP SAMLを設定するための前提条件

- ADFS 6.0+を推奨
- Windows Server 2012 R2+
- Active Directory統合の設定
- ADFS上のSSL/TLS証明書
- Cisco IQへの管理者アクセス
- ADFSサーバへの管理アクセス(Windows Server)
- ADFSサーバー上のPowerShellアクセス
- ADFSとCisco IQ間のネットワーク接続
- ADFSサーバ設定の詳細（下の表に記載）

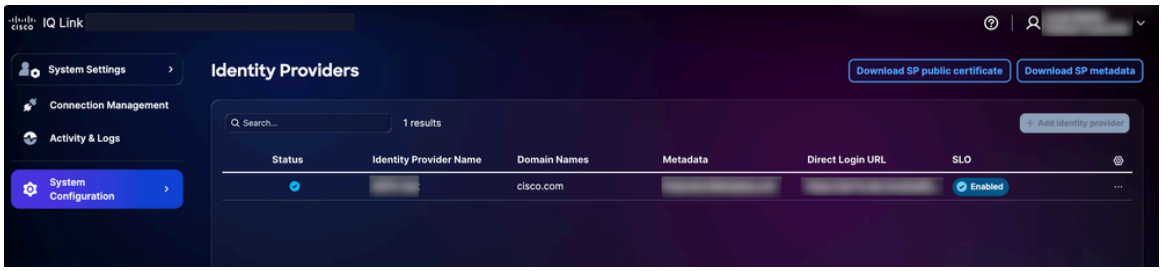
ADFSサーバの設定

項目	説明	例
Cisco IQ FQDN（オプション）	ユーザー配置ホスト名	devxx-23.cx-xxx-xxx.cisco.com
ADFSサーバーURL	ユーザADFSサーバアドレス	https://ad-fs.dev.local
会社のドメイン	電子メールドメイン	company.com
ADグループ	Active Directoryグループのドメイン名(DN)	CN=Role - CXIQ開発者

ADFSサーバーの構成

ADFSを設定するには、次の手順に従います。

1. System Settingsで、System Configuration > Identity Providersの順に選択します。Identity Providersページが表示されます。



ダウンロードオプション

2. Download SP public certificateおよびDownload SP metadataをクリックして、これらのファイルをダウンロードします。
3. service-provider-metadata.xmlファイルとservice-provider-certificate.crtファイルをコピーし、ADFSディレクトリ（たとえば、C:-certificate.crt）に保存します。
4. ADFSサーバにログインします。
5. ADFS Managementメニューから、Relying Party Trustsをクリックします。
6. 証明書利用者信頼メニューから、証明書利用者信頼の追加をクリックします。新しいウィザードが開きます。
7. Claims Awareオプションボタンをクリックします。
8. Startをクリックして、設定を続行します。
9. Import data about the relying party from a fileをクリックします。
10. Browseをクリックして、サービスプロバイダーのメタデータファイルを選択し、ファイルのアップロードを完了します。
11. [Next] をクリックします。
12. 表示名（「CIQ-Stage」など）を入力し、関連するメモを追加して、Nextをクリックします。
13. Choose Access Control Policyページで、Permit everyone（または、組織のセキュリティ設定で必要なポリシー）をクリックします。
14. 残りの画面でNextをクリックします。
15. Closeをクリックして、証明書利用者信頼の設定を完了します。

ADFS要求規則の構成

ADFS要求ルールを構成するには、次のセクションに記載されている手順を実行します。

必要な請求

必要な請求については、次の表を参照してください。

必要な請求

請求	目的	出典
Email	ユーザーID	ADメール
Display Name	ユーザーのフルネーム	AD表示名
名前ID	SAMLサブジェクト	電子メールから変換
[グループ（Groups）]	ロールベースのアクセス	ADグループメンバーシップ(memberOf)

クレームルールの適用

1. 証明書利用者信頼の名前を定義します（たとえば、「Cisco IQ - Stage」）。

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

2. ユーザ情報とグループメンバーシップをCisco IQに送信するクレームルールを定義します。

```
$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 = “;mem
’@@
```

3. 次のコマンドを実行して、要求ルールを適用します。

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

ユーザグループの確認

1. ユーザのグループメンバーシップを確認するためのユーザ名を設定します。

```
$username = “testuser”
```

2. ユーザのアカウントを検索するには、次のコマンドを実行します。

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

3. ユーザが属するグループを表示します。

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

出力例：

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

SP署名証明書を信頼するためのADFSの設定

1. ADFSサーバで、SP証明書をTrustedPeopleストアにインポートします。

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

2. 次のいずれかのオプションを選択します。

注:SP証明書は、ADFSが標準の信頼チェーン経由で検証できない内部認証局(CA)によって発行されます。

- この証明書利用者のチェーン検証をグローバルに無効にする

```
Set-AdfsRelyingPartyTrust `
    -TargetIdentifier “


     ” `
    -SigningCertificateRevocationCheck None `
    -EncryptionCertificateRevocationCheck None
```

または

- 発行元CA証明書を信頼されたルート証明機関ストアにインポートする

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

3. ADFSサービスを再起動して変更を適用します。

```
Restart-Service adfssrv
```

ADFSメタデータのエクスポート

ADFSメタデータは、PowerShellまたはWebブラウザーを使用してダウンロードできます。

PowerShell

PowerShellを使用してADFSメタデータをエクスポートするには、次の手順に従います。

1. ADFSサーバでPowerShellを開きます。
2. 次のコマンドを実行して、メタデータファイルをダウンロードします。

```
$metadataUrl = (Get-AdfsEndpoint | Where-Object {$_.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
```

コマンドの実行後、メタデータファイルはC:-metadata.xmlに保存されます。

Web ブラウザ

Webブラウザを使用してADFSメタデータを工クスポートするには、次の手順に従います。

1. https://<your-adfs-server>/FederationMetadata/2007-06/FederationMetadata.xmlに移動します。
2. <your-adfs-server>はADFSサーバのホスト名で置き換えます。
3. プロンプトが表示されたら、メタデータXMLファイルをコンピュータに保存します。

ADFS IDPの追加

1. Identity Providersページで、Add identity providerをクリックします。
2. IDプロバイダー名を入力します。
3. ドメインを入力します(company.comなど)。
4. （オプション）必要に応じて、Enable single logout toggleボタンをオンにします。
5. IDPアプリケーションから取得したSAMLメタデータファイルをUpload IDP Metadataフィールドにドラッグアンドドロップするか、アップロードします。
6. [Save] をクリックします。

注：ロールのマッピングが完了するまで、ステータスは「Incomplete」と表示されます。これは正常な動作です。

ロールマッピングの設定

役割マッピングの構成に進む前に、マッピングに使用するグループをActive Directoryから検索できることを確認してください。Active Directoryからグループを検索するには、次のPowerShellコマンドを実行します。

```
$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”] }
```

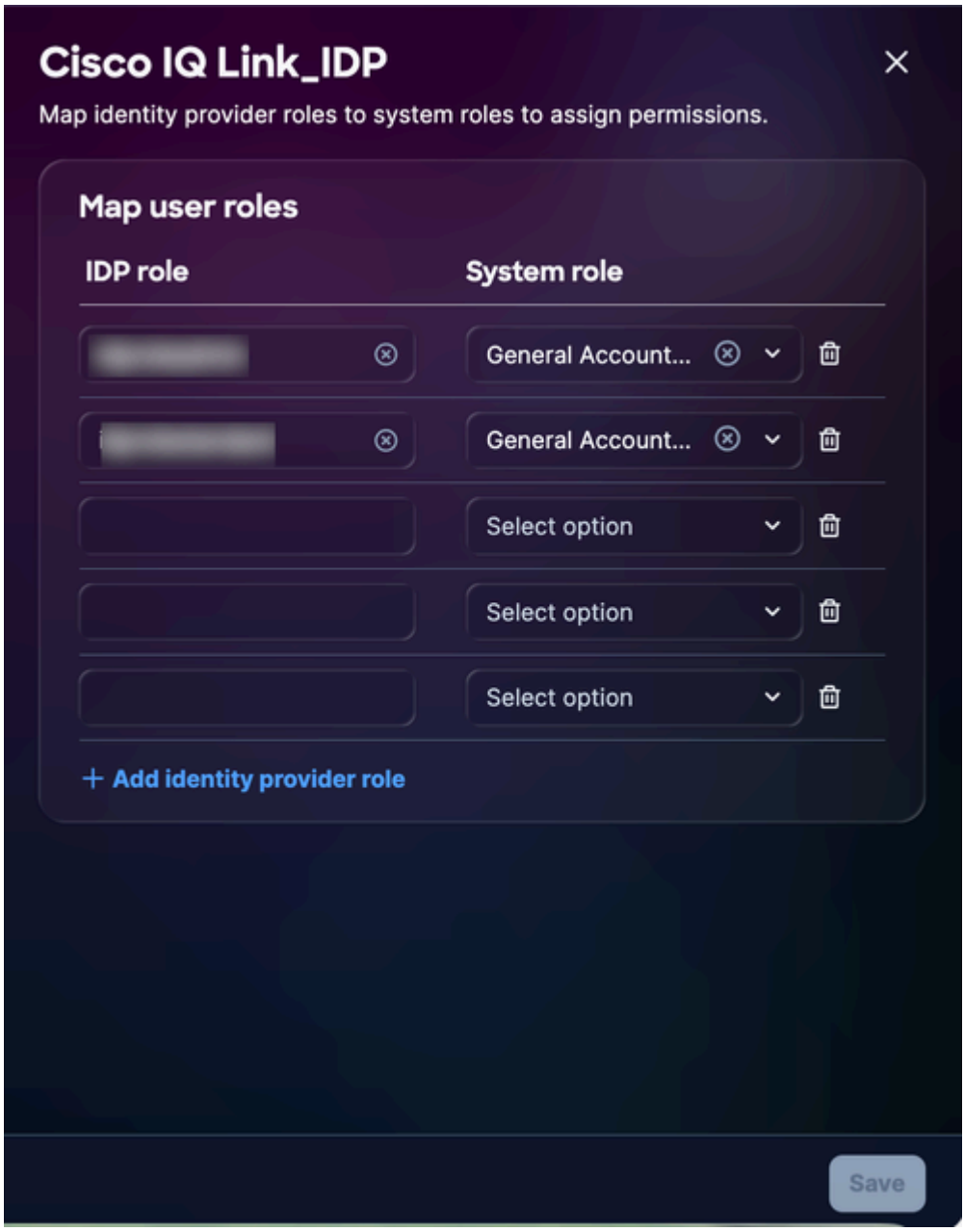
システムはLDAPを介してActive Directoryに直接クエリーを送信するため、追加のモジュールは必要ありません。グループ情報は、完全な識別名(DN)形式で返されます。次に例を示します。

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

必要なグループがリストされていない場合は、ADFS役割のマッピングを完了する前に、管理者がActive Directoryでグループを作成する必要があります。

役割マッピングを構成するには、次の手順に従います。

1. 追加されたIDPから、More Optionsアイコン> Map Rolesの順に選択します。Map user rolesページが表示されます。



ロールマッピング

2. 選択したシステムロールのIDPロールを入力します。次のシステムロールがサポートされています。

   - general_account _administrator：汎用アカウント管理者には、製品のすべてのアクションを実行するフルアクセス許可があります。IDPロール（解析名）はCXIQ Adminsです。
   - general_account__viewer：一般アカウントビューアには読み取り専用アクセス権があります。IDPロール（解析名）はCXIQ DevelopersおよびCXIQ Viewerです。

   > 注：完全なドメイン名ではなく、解析済みの名前（CXIQ開発者など）を使用してください。

3. [Save] をクリックします。ステータスがSuccessに更新されます。

検証およびテスト

認証のテスト

1. Incognitoまたはプライベートモードブラウザで、https://your-cisco-iq-domain.com/loginに移動します。
2. domain\usernameまたはuser@domain.local形式のActive Directoryクレデンシャルを使用してログインします。
3. 認証が成功した後、Cisco IQ Homeページにリダイレクトされることを確認します。
4. ユーザプロファイルで、割り当てられたロールに、正しく解析されたグループ名（CXIQ Developersなど）が表示されることを確認します。

ログアウトのテスト

ログアウトをテストするには、Cisco IQからのログアウトをクリックします。「ログアウトします。お待ちください...」というメッセージが表示され、Cisco IQ Loginページにリダイレクトされます。また、ADFSセッションも終了します。ADFSに直接アクセスしようとすると、再度ログインするように求められます。

ADFS問題のトラブルシューティング

ADFSの状態、証明書のエラー、SSOログインの失敗、およびSLOの構成に関連する問題を迅速に特定して解決するために役立つ、一般的な問題と考えられる解決策の概要を次に示します。

ADFSの問題

お問い合わせ内容	症状/説明	原因/チェック/回避策と修正
グループが抽出されていません	ログイン後にロールがない	● 要求規則が見つかりません: 「ADFS要求規則の構成」の手順を再実行してください。 ● 間違ったグループ属性 :http://schemas.xmlsoap.org/claims/Groupである必要があります。

お問い合わせ内容	症状/説明	原因/チェック/回避策と修正
		●ユーザがADグループに含まれていない
解読に失敗しました	ログの「Failed to decrypt assertion」	ADFS証明書設定の設定を確認します
ログインループ	認証またはログインループでのスタック	● 無効なACS URL：確認：https://your-fqdn/saml/acs ● Cookie mismatch：正しいドメインのブラウザCookieを確認してください

トラブルシューティングのための診断コマンド

ADFS環境とCisco IQの統合を確実に成功させるには、次の診断コマンドを使用します。これらのコマンドは、メタデータのアクセシビリティ、証明書の構成、およびエンドポイントの設定を確認するのに役立ちます。

- ADFSメタデータのアクセス可能性の確認:ADFSフェデレーションメタデータが到達可能で、だれでもアクセス可能であることを確認します。これは、最初の信頼を確立するための重要な手順です

```
curl -k https://

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

- 暗号化証明書の検証：正しい暗号化証明書がCisco IQ証明書利用者信頼に関連付けられていることを確認します。

```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object EncryptionCertificate | Format-List
```

- SAMLエンドポイント設定の確認:Cisco IQ TrustのSAMLエンドポイントが正しく設定されていること、および認証要求とアサーションが予期されるURLにルーティングされていることを確認します

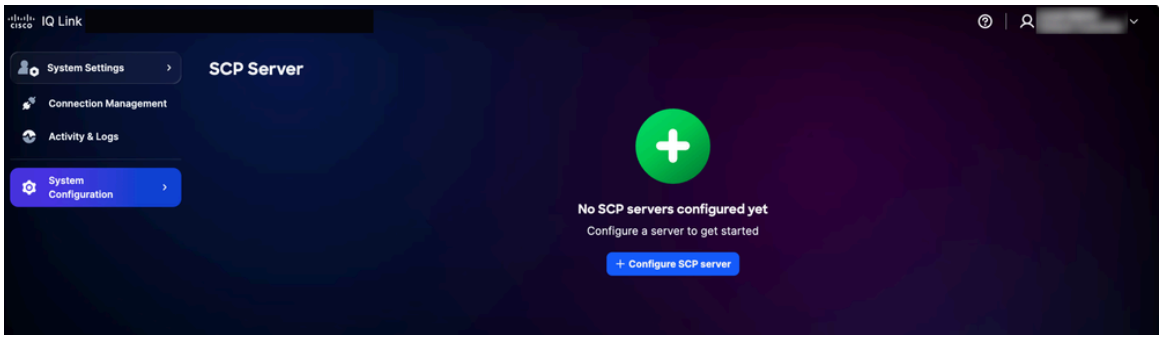
```
Get-AdfsRelyingPartyTrust -Name “Cisco IQ - Stage” | Select-Object SamlEndpoints
```

SCPサーバの追加

このSecure Copy Protocol(SCP)サーバは、Cisco IQインストールの追加、アップグレード、または修正に必要なアップグレードファイルをインポートするための前提条件です。

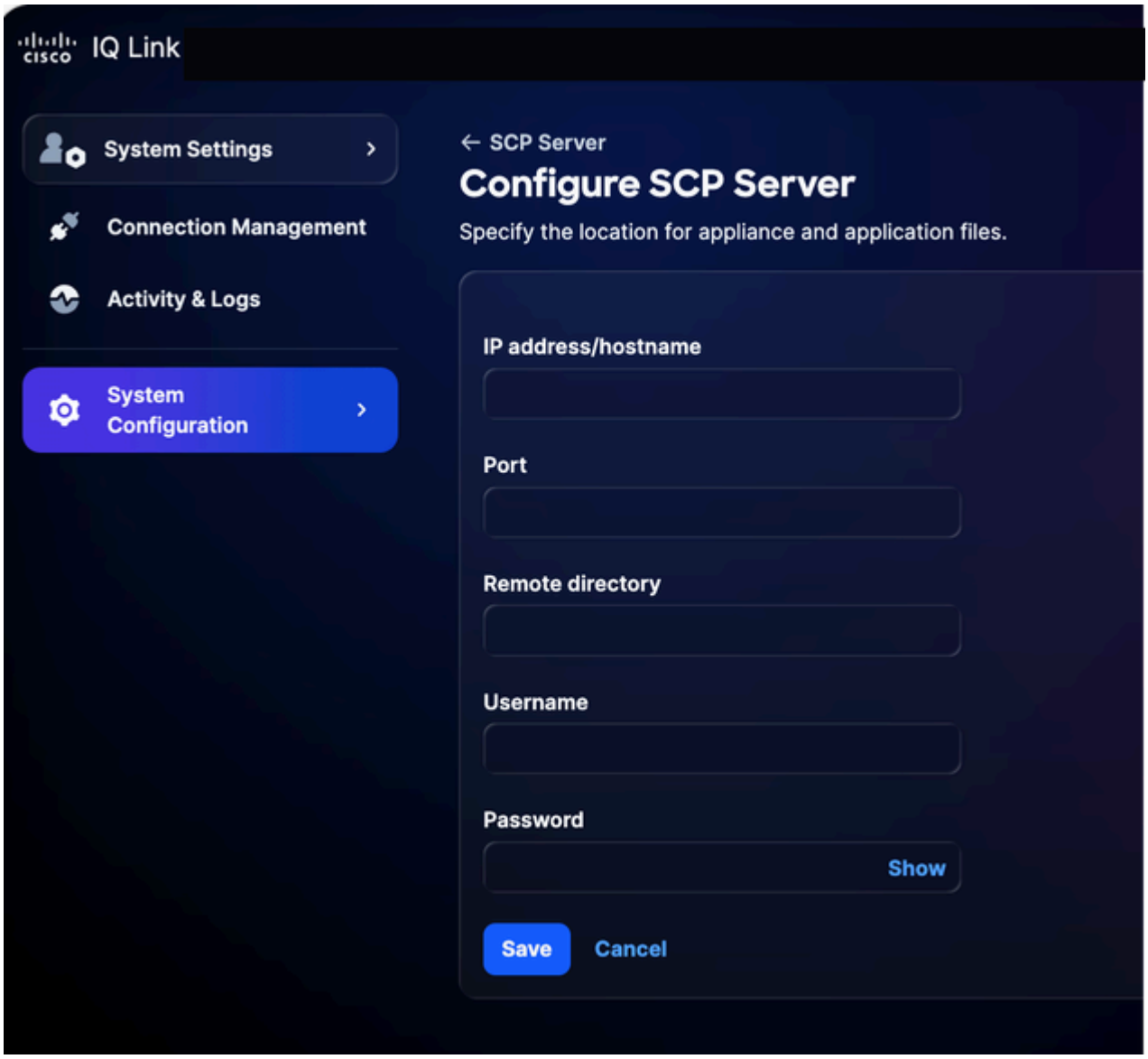
SCPサーバを追加するには

1. System Settingsで、System Configuration > SCP Serverの順に選択します。SCPサーバページが表示されます。



SCPサーバのホームページ

2. Configure SCP Serverをクリックします。



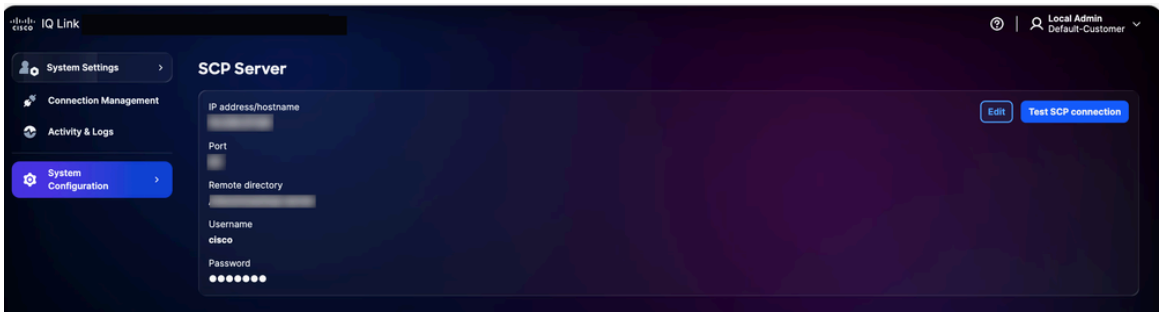
SCPサーバの設定

3. IPアドレス/ホスト名を入力します。
4. ポート番号を入力します。
5. リモートディレクトリを入力します。
6. ユーザ名を入力します。
7. password を入力します。
8. [Save] をクリックします。確認が表示されます。

既存のSCPサーバの編集

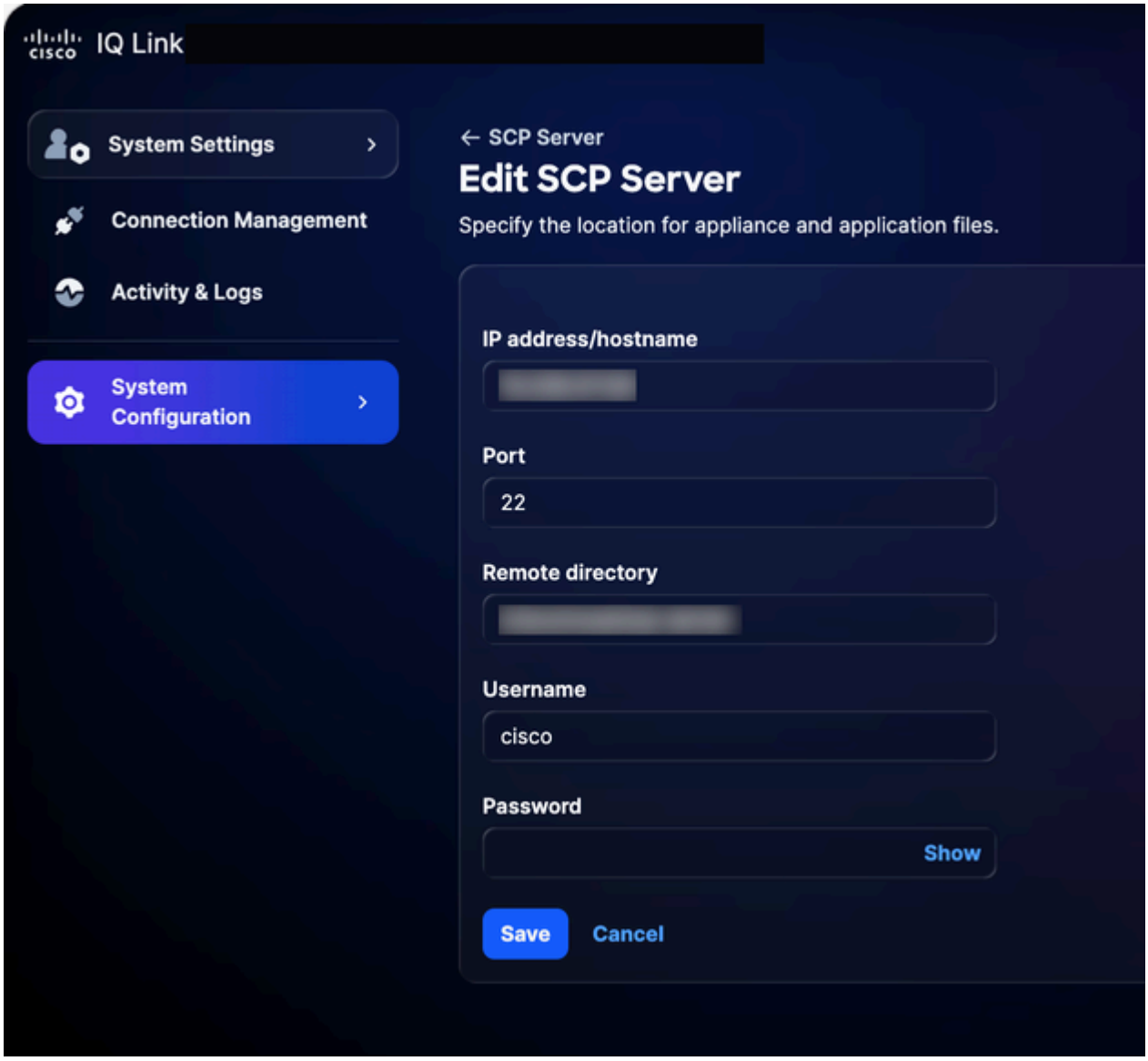
既存のSCPサーバを編集するには、次の手順を実行します。

1. SCPサーバページに移動します。



SCPサーバ

2. 必要な既存のSCPサーバのEditをクリックします。



SCPサーバの編集

3. 必要に応じて詳細を変更します。

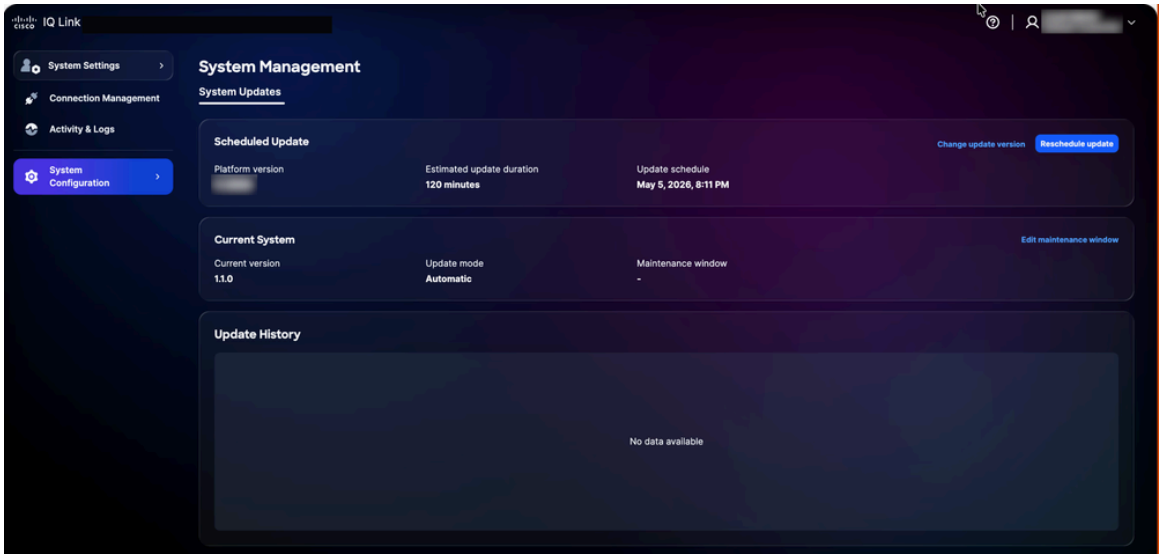
4. [Save] をクリックします。

システム管理

お客様は、UIを使用して最新バージョンのCisco IQ Linkにアップグレードできます。Cisco IQ Data Connectorsページでも確認できます。

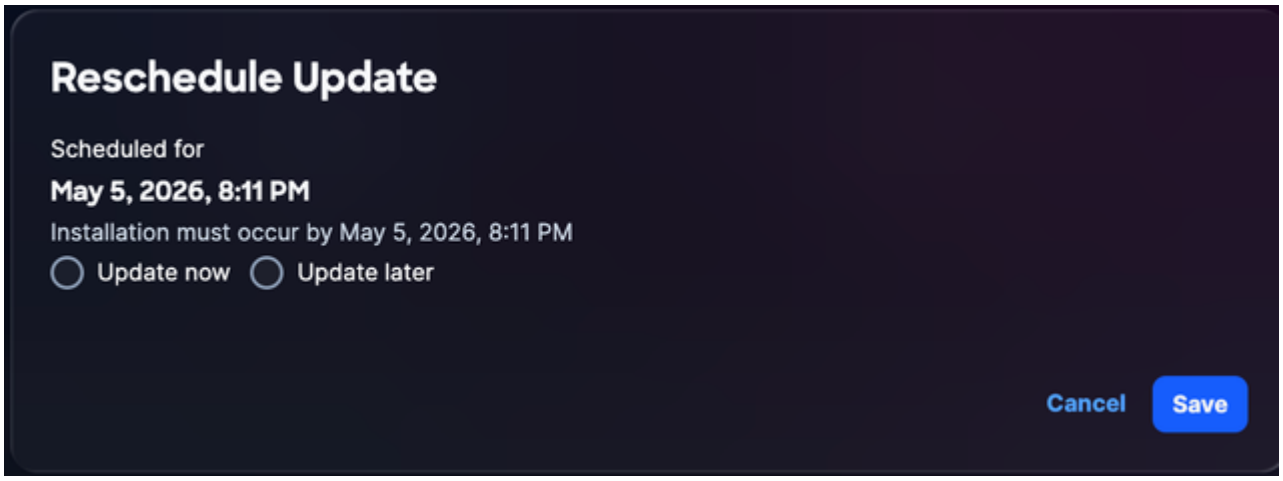
システム更新を再計画する手順は、次のとおりです。

1. Administrationで、System Configuration > System Managementの順に選択します。System Managementページが表示されます。このページには、現在実行中のシステムバージョンが表示されます。更新が設定されていない場合、「更新履歴」セクションは空になります。



システムアップグレード

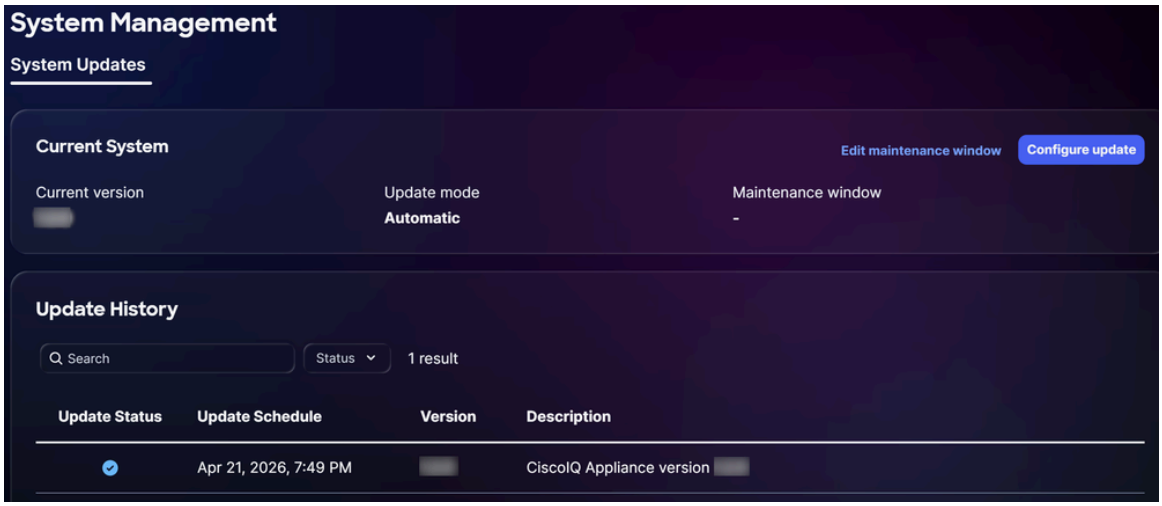
2. Reschedule updateをクリックします。



アップグレードの再スケジュール

3. 即時に再スケジュールする場合はUpdate Nowを、別の日時をスケジュールする場合はUpdate Laterをクリックします。

4. [Save] をクリックします。確認が表示され、System Updateホームページにリダイレクトされます。



正常なアップグレード

SSL証明書の設定

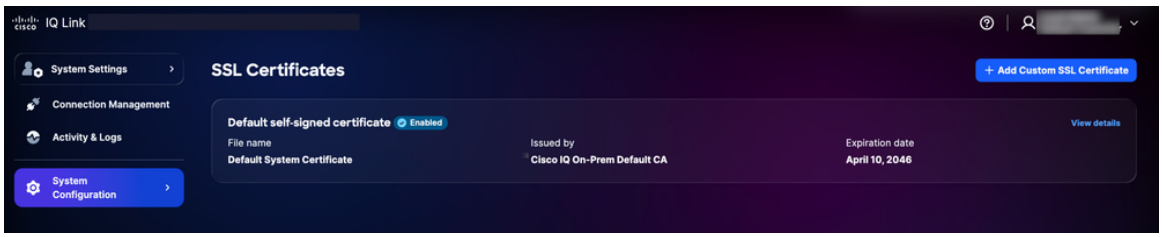
デフォルトの自己署名証明書がCisco IQにプリインストールされて有効になりますが、ユーザはカスタムSSL証明書をアップロードできます。カスタムSSL証明書を有効にすると、HTTPS接続に使用されます。証明書を無効にするか削除すると、システムは自動的にデフォルトの証明書に戻ります。

注：証明書の有効期間は90日以上残っている必要があります。証明書の有効期限が切れるまでの残り日数が90日を下回ると、証明書は「期限切れ間近」と見なされます。SSL証明書を追加、編集、または削除したら、Okta IDPまたはADFS IDPの「SLO設定の完了」の項の説明に従って、新しいSSLをアップロードする必要があります。

カスタムSSL証明書の追加

カスタムSSL証明書を追加するには、次の手順に従います。

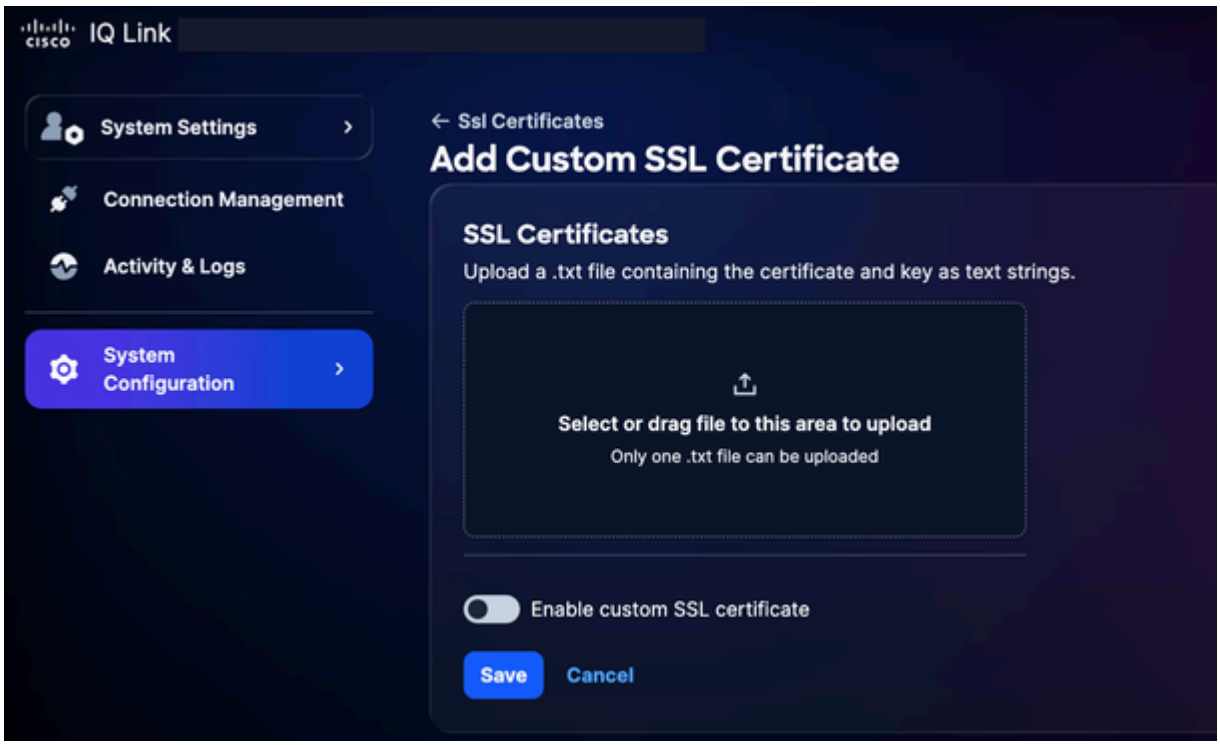
1. System Settingsで、System Configuration > SSL Certificatesの順に選択します。SSL Certificatesページが表示され、システムのすべてのSSL証明書がリストされます。



SSL証明書の追加

2. Add Custom SSL Certificateをクリックします。

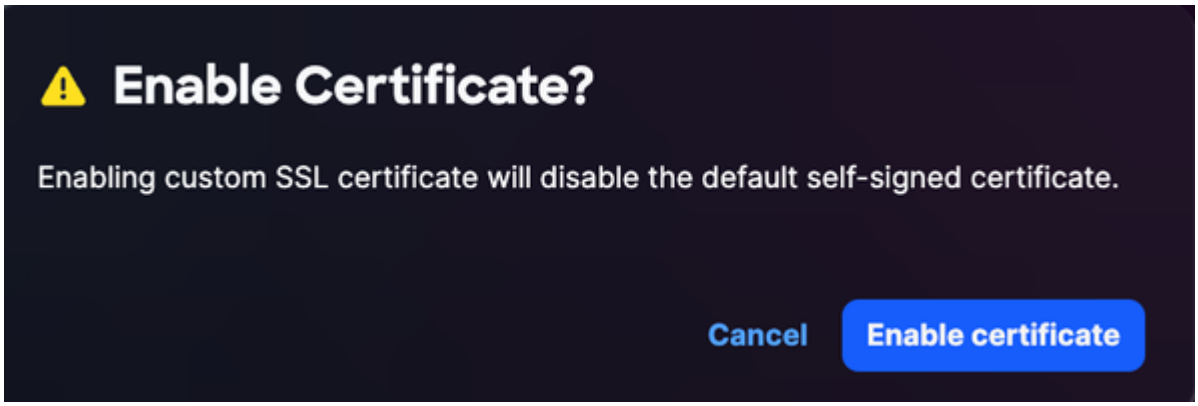
注：
・ Privacy-Enhanced Mailでエンコードされた証明書とキーの両方をテキスト文字列として含む.txtファイルをアップロードします
・ 一度にアップロードできる.txtファイルは1つだけです
・ ファイルには証明書と秘密キーの両方が含まれている必要があります



SSL証明書のアップロード

3. カスタムSSL証明書をSSL Certificateフィールドにドラッグアンドドロップするか、アップロードします。

4. Enable custom SSL certificateトグルボタンをオンにします。



証明書の有効化

> 注：証明書をすぐにアクティブ化せずにアップロードする場合は、このチェックボックスにチェックマークを付けないでください。

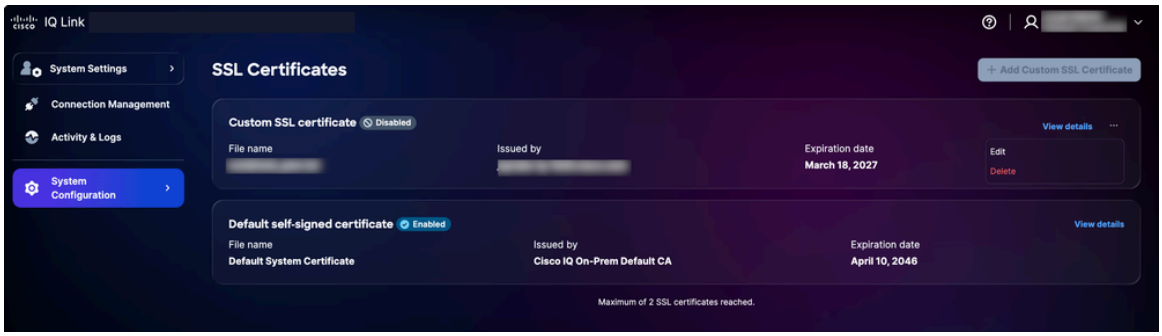
5. Enable certificateをクリックします。
6. [Save] をクリックします。

カスタムSSL証明書が有効でアクティブになっている。デフォルトのシステム証明書は自動的に無効になります。

カスタムSSL証明書の編集

カスタムSSL証明書を編集して、新しい証明書をアップロードしたり、現在有効な証明書を無効にすることができます。編集するには：

1. 目的のカスタムSSL証明書に移動します。



SSL証明書の編集

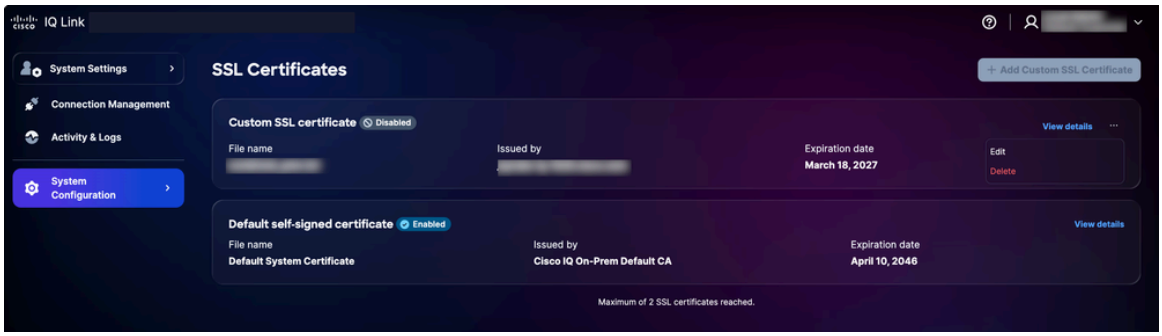
2. More Optionsアイコン> Editの順に選択します。Edit SSL Certificateページが表示されます。
3. 必要に応じて、証明書の詳細を編集します。
4. [Save] をクリックします。

カスタムSSL証明書の削除

> 警告：カスタムSSL証明書はいつでも削除できますが、これは元に戻せない操作です。削除後はいつでも新しいカスタム証明書をアップロードできます。

To Delete:

1. 目的のパーソナルSSL証明書に移動します。



SSL証明書の削除

2. More Optionsアイコン> Deleteの順に選択します。
3. Delete Certificateをクリックします。カスタム証明書が削除され、デフォルトの証明書が自動的に再アクティブ化されます。

Syslogサーバの設定

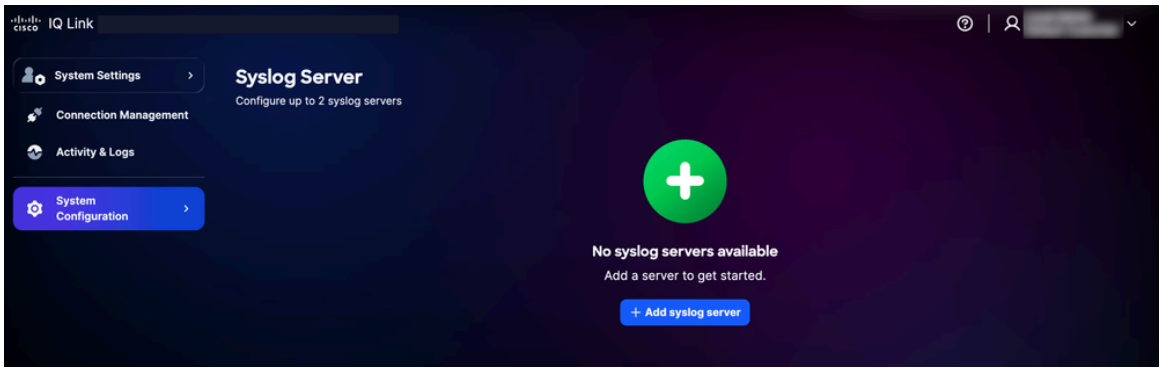
Administratorロールを持つユーザは、システムログをエクスポートするように外部syslogサーバを設定できます。最大2つのsyslogサーバを設定できます。

注:Syslogサーバは、完全修飾ドメイン名(FQDN)ではなく、IPアドレスとして指定する必要があります。

Syslogサーバの追加

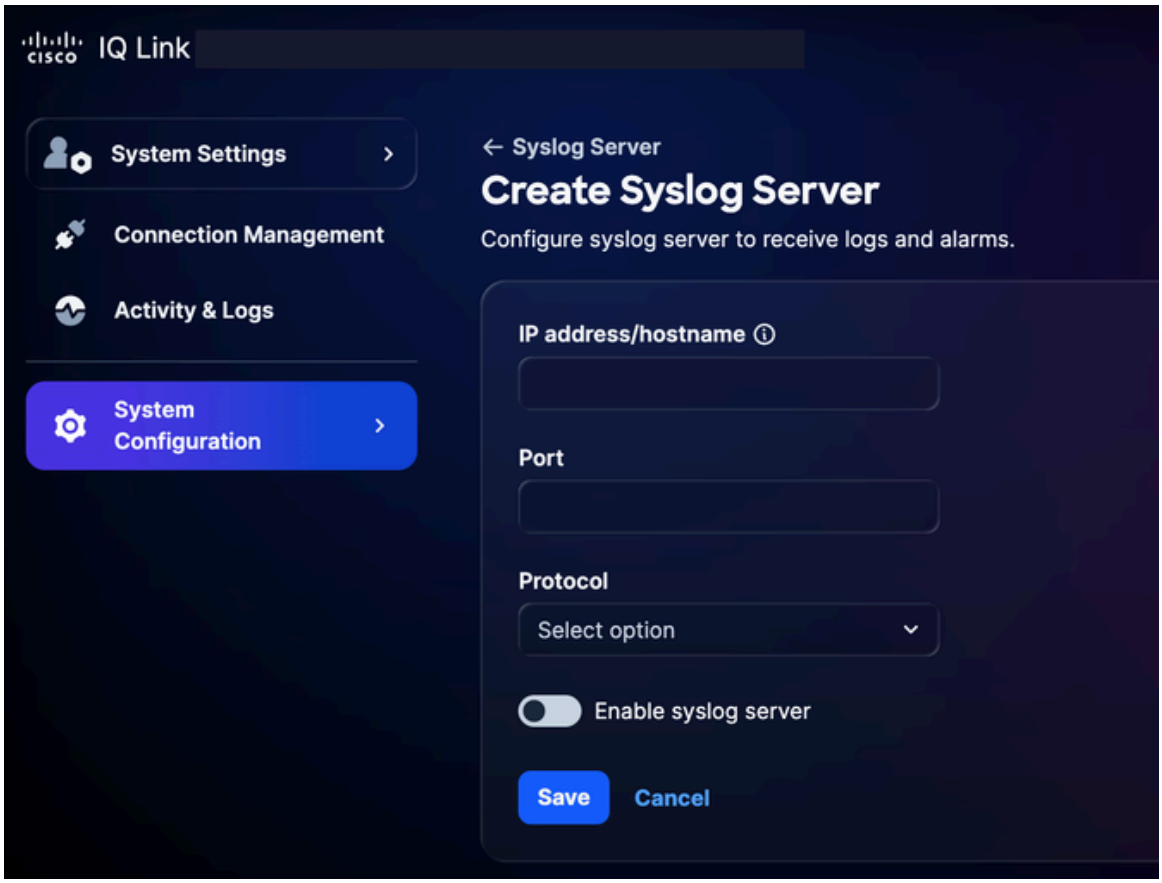
syslogサーバを追加するには、次の手順を実行します。

1. System Settingsで、System Configuration > Syslog Serverの順に選択します。Syslog Serverページが表示されます。



Syslogサーバの追加

2. Add syslog serverをクリックします。Create Syslog Serverページが表示されます。



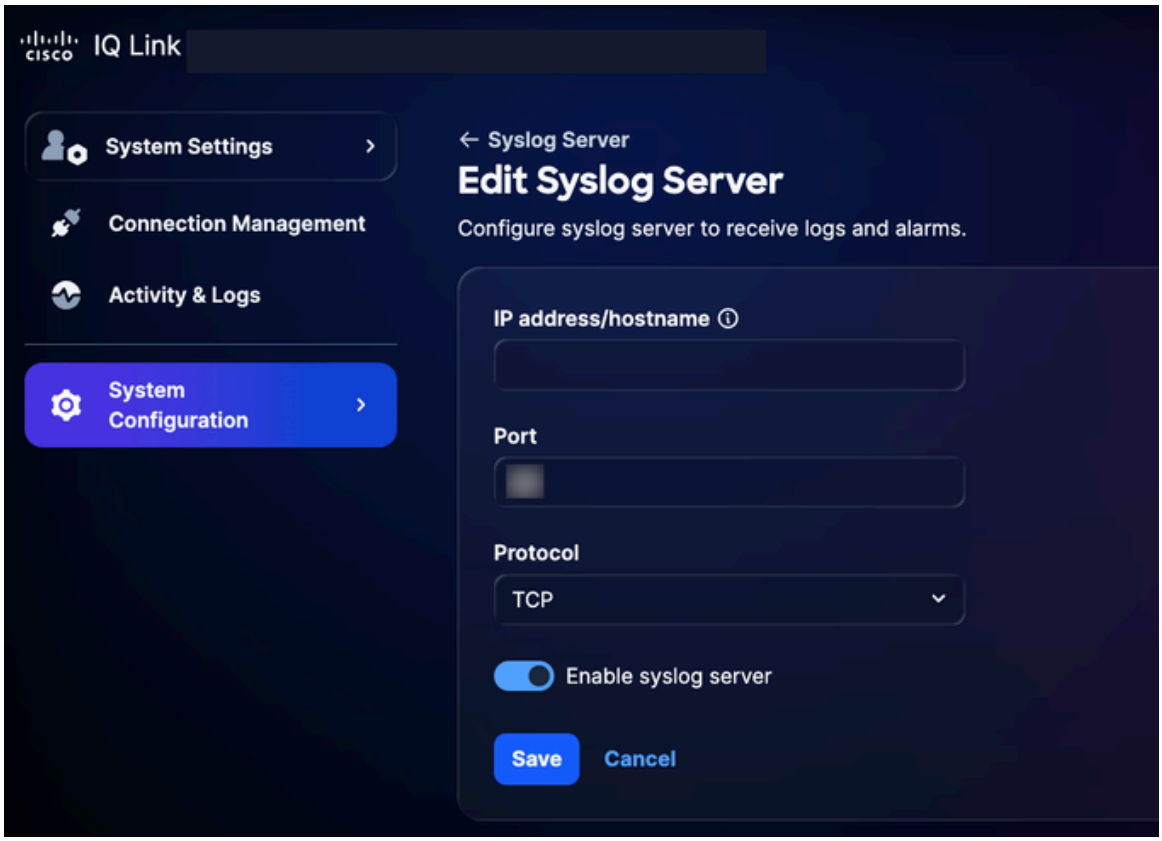
Syslogサーバの作成

3. IPアドレス/ホスト名を入力します。
4. ポート番号を入力します。
5. Protocolドロップダウンリストから、適切なプロトコル（UDPやTCPなど）を選択します。
6. Enable syslog serverトグルボタンをオンにします。
7. [Save] をクリックします。確認が表示され、新しく追加されたsyslogサーバがSyslogサーバのホームページに表示されます。

設定されたSyslogサーバの編集

設定されたsyslogサーバを編集するには、次の手順を実行します。

1. 目的のsyslogサーバに移動します。
2. More Optionsアイコン> Editの順に選択します。Edit Syslog Serverページが表示されます。



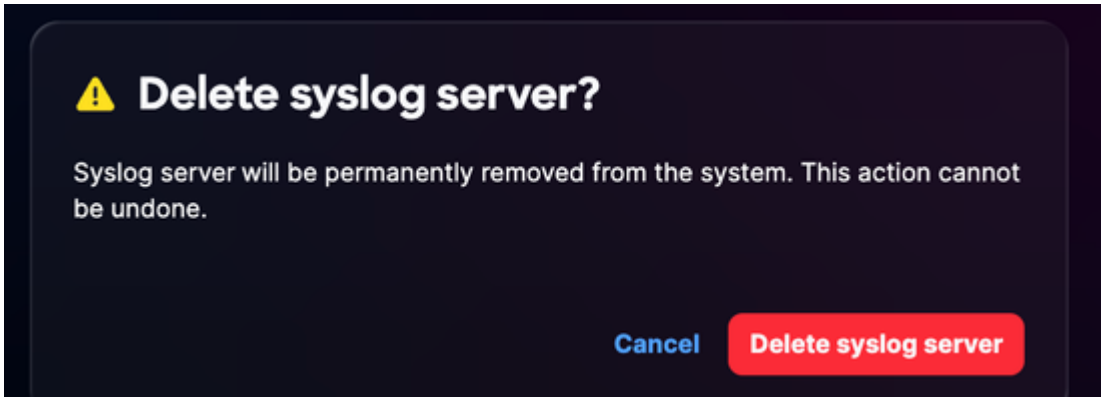
Syslogサーバの編集

3. 必要に応じて、詳細を編集するか、syslogサーバの有効化の切り替えをオフにします。
4. [Save] をクリックします。

設定されたSyslogサーバの削除

設定されたsyslogサーバを削除するには、次の手順を実行します。

1. 目的のsyslogサーバに移動します。
2. More Optionsアイコン> Deleteの順に選択します。確認が表示されます。

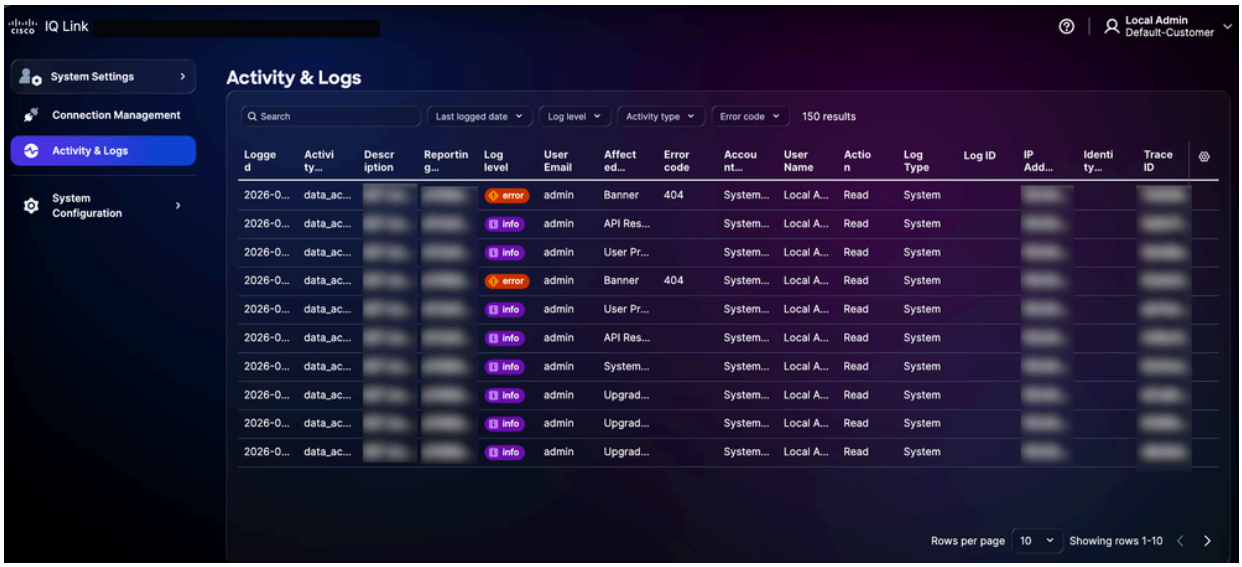


確認

3. Delete syslog serverをクリックします。

アクティビティとログ

アクティビティとログは、Cisco IQにおけるユーザアクションと変更の詳細な記録を提供し、管理者がユーザアクティビティを追跡して透明性を維持できるようにします。



アクティビティとログ

アクティビティとログを表示するには、System SettingsメニューからActivity & Logsを選択します。

アクティビティとログ：

- フィルタ、ページネーション、検索機能をサポートし、情報の検索と管理を容易にします。
- すべてのAPI操作をゲートウェイレベルで記録

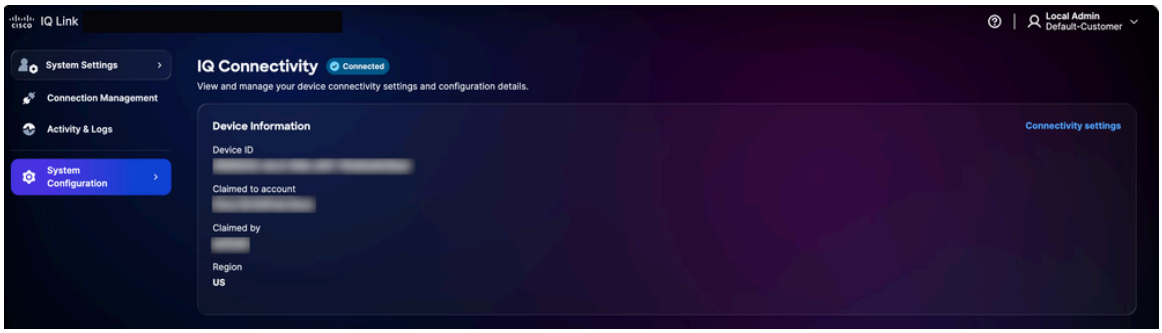
次のフィルタオプションを使用できます。

- Date：ログを特定の時間範囲でフィルタします。
- ログレベル：重大度（エラー、警告、情報など）でログをフィルタリングします。
- アクティビティタイプ：システムアクティビティのタイプによってログをフィルタリングします。
- エラーコード：特定のエラーコードのログをフィルター処理します

IQ接続

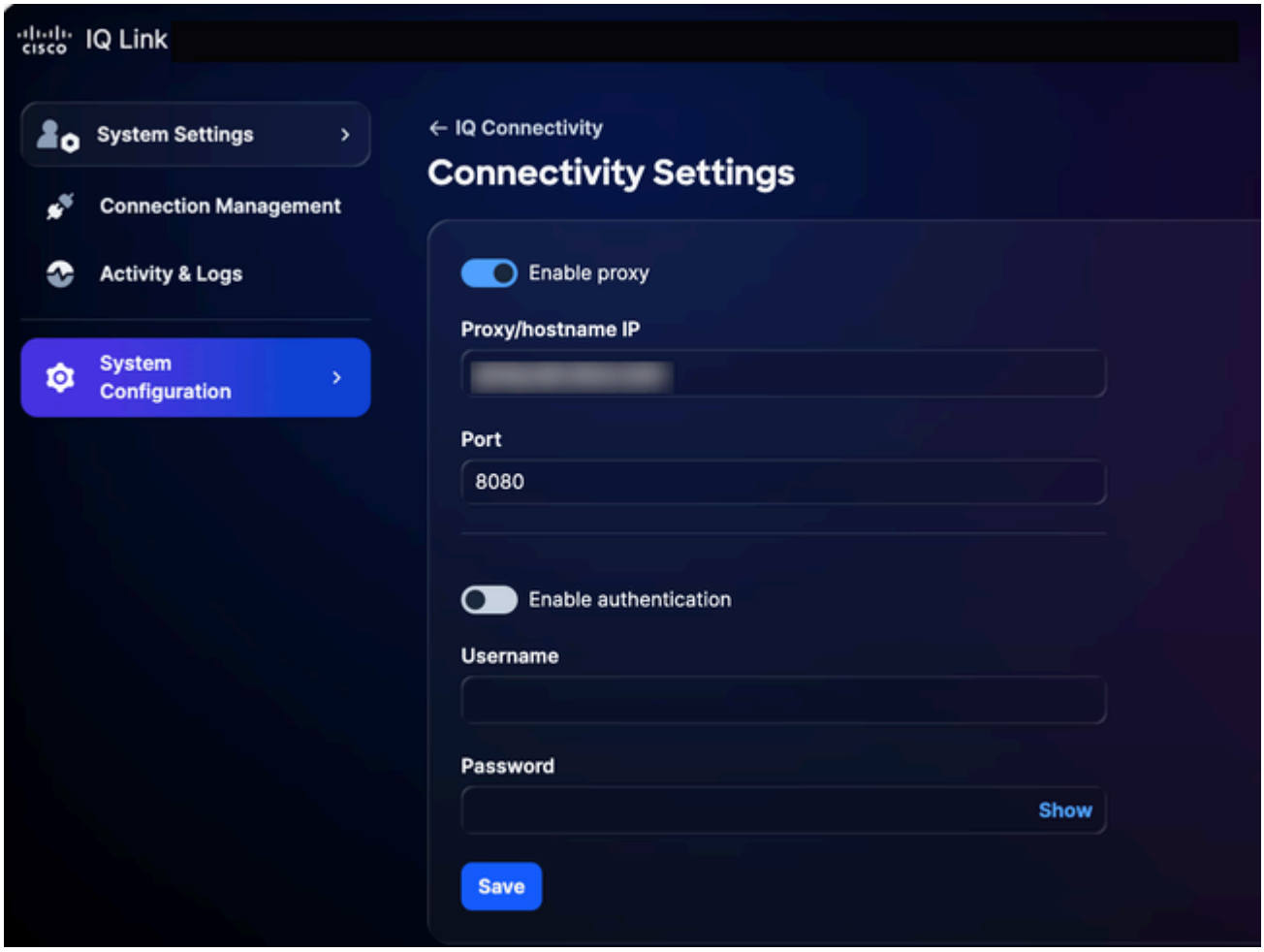
デバイスの接続設定と構成の詳細を表示および管理するには、次の手順を実行します。

1. System Settingsで、System Configuration > IQ Connectivityの順に選択します。IQ Connectivityページが表示されます。



IQ接続

2. Connectivity settingsをクリックします。



接続設定

3. 必要に応じて詳細を更新します。

4. [Save] をクリックします。

接続管理（データ収集）

Cisco IQ Linkは、ネットワークデータ収集用にオンプレミスで導入されるソリューションで、インフラストラクチャの可視性を高めるように設計されています。Catalyst CenterおよびDirect Connectionを介してデータを収集します。ネットワーク認証とデバイス検出の管理方法が簡素化されます。データ収集の構成は、次のように共有できます。

- クレデンシャルセットの作成：ネットワークデバイスと通信するための認証プロトコル（SNMP v1/v2c/v3など）を確立します。セキュリティゾーンまたは口ケーションごとにクレデンシャルを一元化すると（「SanJose-SNMPv3」など）、1つの口ケーションでパスワードを更新し、関連するすべてのデバイスに変更を自動的に伝播することができます。

注:Cisco IQ Linkでは、直接接続された資産を認証するために、デバイス上で特権レベル15が設定されたユーザアカウントが必要です。

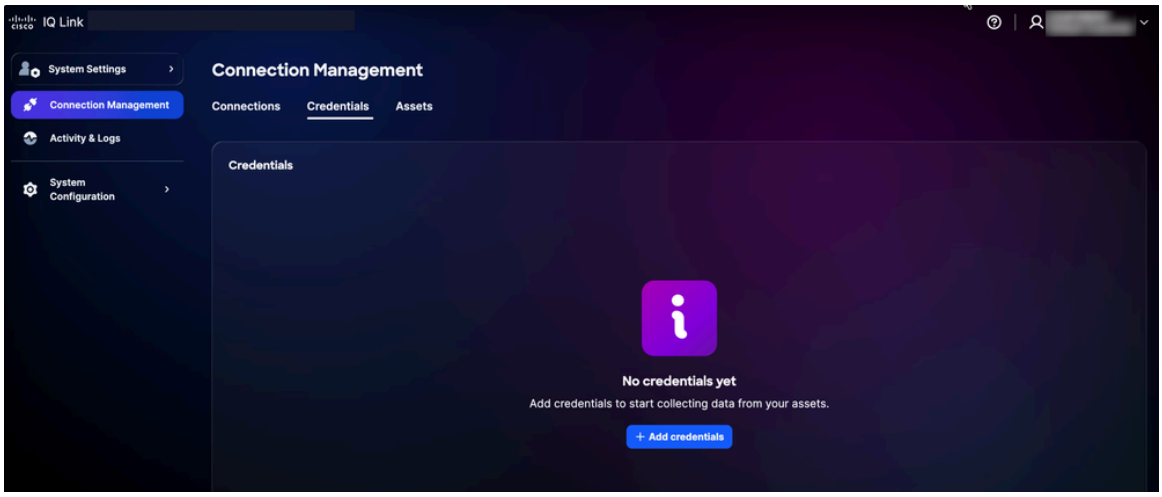
- 資格情報をインベントリにマッピングする：資格情報セットをインベントリ資産にマッピングして、認証プロセスを自動化します。特定のIP範囲を定義済みのクレデンシャルセットにリンクするルールを作成することで、データ収集時に適切な認証が自動的に適用されます。これにより、手動による入力工ラーが排除され、ネットワークの拡大に合わせて設定の正確性が維持されます。

注：デバイス検出にはSNMPv2c/SNMPv3およびSSHが必要で、Catalyst Centerを設定する前にHTTP/HTTPSクレデンシャルを入力する必要があります。

資格情報の追加

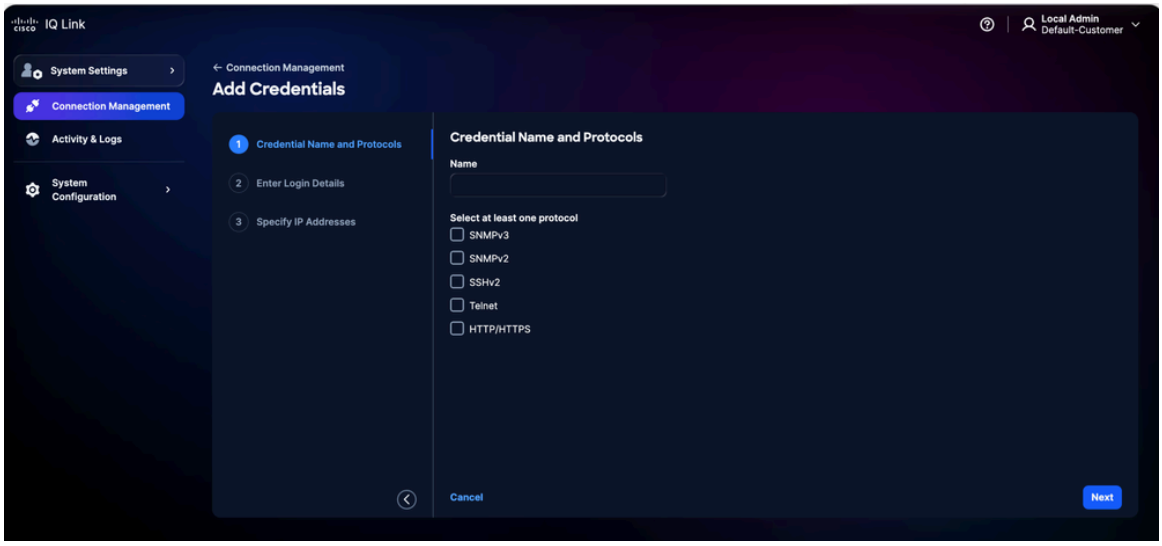
データ収集を実行するには、最初に資格情報を追加する必要があります。認証情報を追加するには、次の手順を実行します。

1. System Settingsから、Connection Managementを選択します。Connection Managementページが表示されます。
2. Credentialsタブをクリックします。



Credentialsタブ

3. Add credentialsをクリックします。

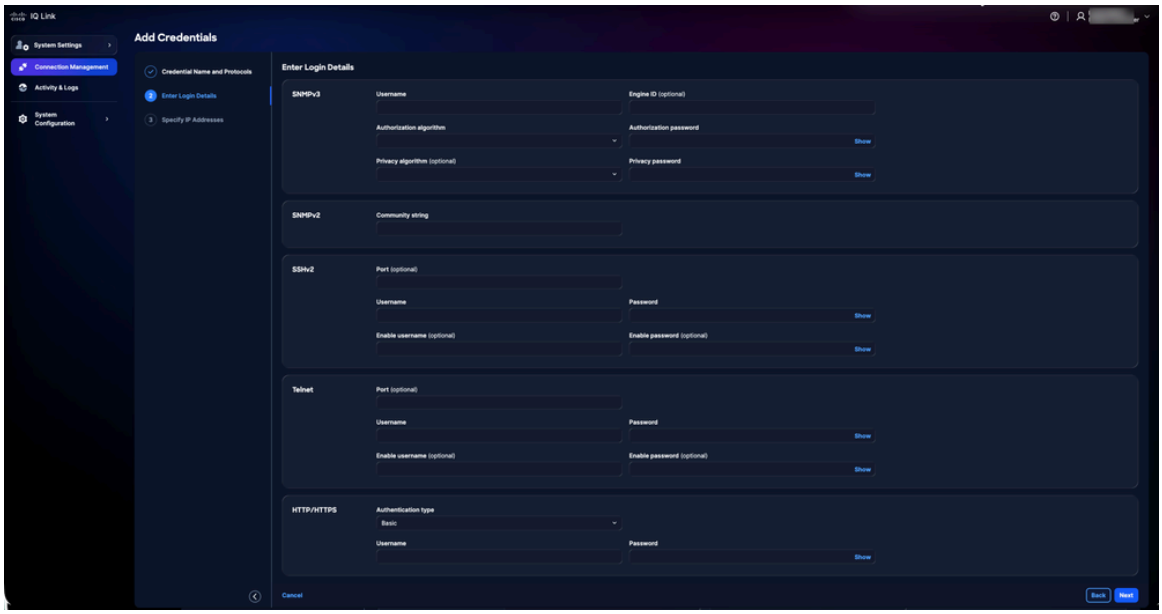


資格情報の追加

4. 名前を入力します。

5. 該当するすべてのプロトコルチェックボックスをオンにします。

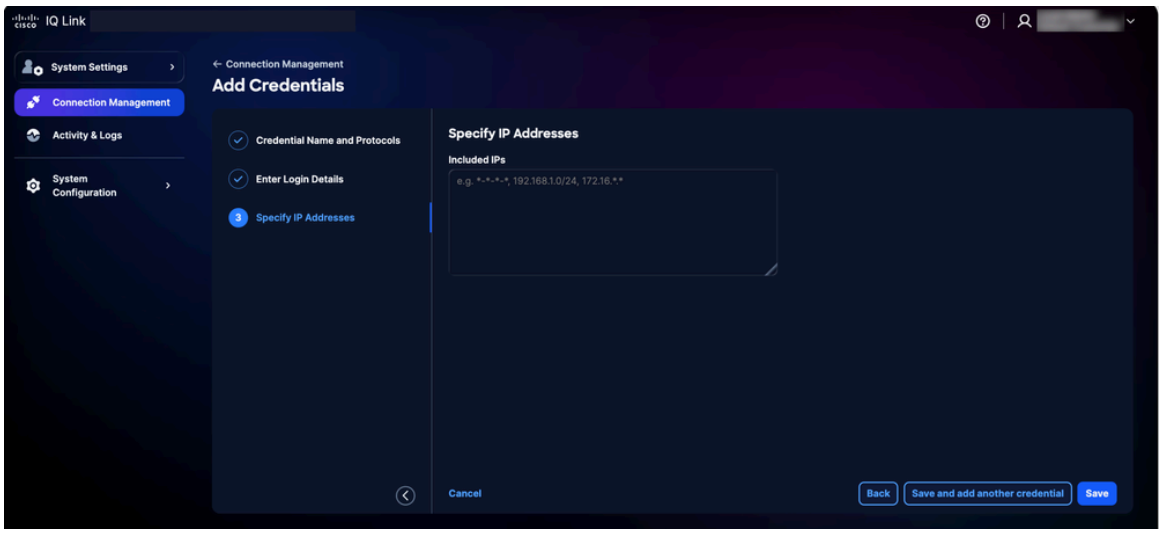
6. [Next] をクリックします。



資格情報の詳細の追加

注：上の図では、前の手順ですべてのプロトコルを選択したときのビューを示しています。インターフェイスには、選択した特定のプロトコルだけが表示されます。

7. 選択した各プロトコルのログイン詳細を入力します。
8. [Next] をクリックします。

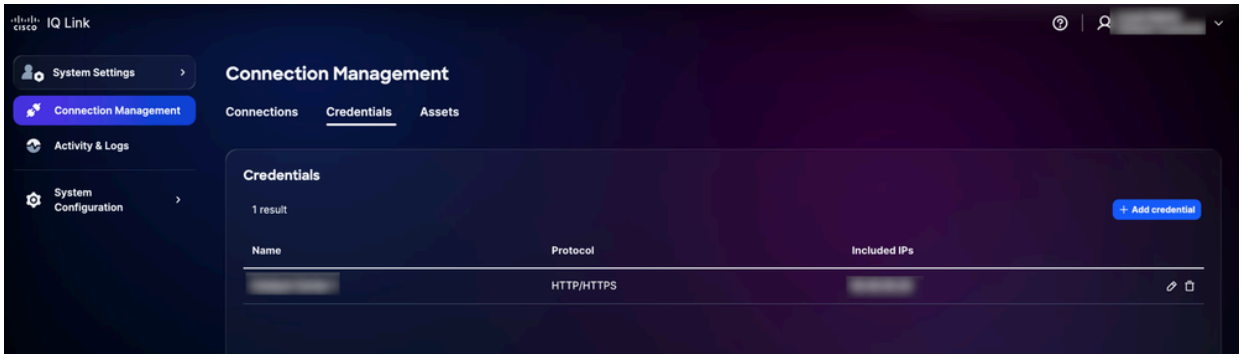


IPアドレスの指定

9. Included IPsと入力します。

注：このフィールドでは、クレデンシャルを使用して接続を確立できるIPアドレスまたはIP範囲を定義します。IPとIPマスクの組み合わせをサポートします（ワイルドカード表記を使用）。 サポートされている形式の詳細については、「クレデンシャルの選択と照合ロジック」を参照してください。

10. [Save] をクリックします。確認が表示され、「クレデンシャル」タブにリダイレクトされます。



追加された資格情報

クレデンシャルを編集するには編集アイコンをクリックし、削除するには削除アイコンをクリックします。

クレデンシャルの選択と照合ロジック

テレメトリエンジンは、優先順位ベースの照合ロジックを使用して、検出時および収集時に適用するクレデンシャルを決定します。この階層を理解することで、目的のデバイスに対して正しいクレデンシャルが使用されます。

- 優先順位ランキング：複数の資格情報セットが1つのデバイスに適用されると、Cisco IQではデバイスとの照合順序に基づいてそれらの資格情報セットを評価します。システムは次の優先順位を適用し、より具体的な一致が優先されます。
    - 正確なIP一致：最も優先度が高い
    - 末尾のワイルドカード一致:** **優先順位は末尾の星の数によって異なります。星が少ないほど、より具体的に一致するため、優先順位が高くなります
- ワイルドカード形式の規則：ワイルドカード(*)は、IPアドレスの末尾の文字としてのみサポートされています。右から左に適用する必要があります。
    - サポートされるフォーマット：

      1.2.3.*（ワイルドカードの中で最も高い優先順位）

      1.2.*.*

      1.*.*.*

      ..*.*（最低の優先度）
    - サポートされていない形式：

先頭のワイルドカード（*.1.2.3など）

オクテット間のワイルドカード（10.10.*.20など）

ダッシュやその他の非標準区切り記号の使用

クレデンシャル選択の例:

次の表は、デバイスが複数の定義済みパターンに一致する場合に、テレメトリエンジンが最も適切なクレデンシャルセットをどのように選択するかを示しています。

クレデンシャル選択の例

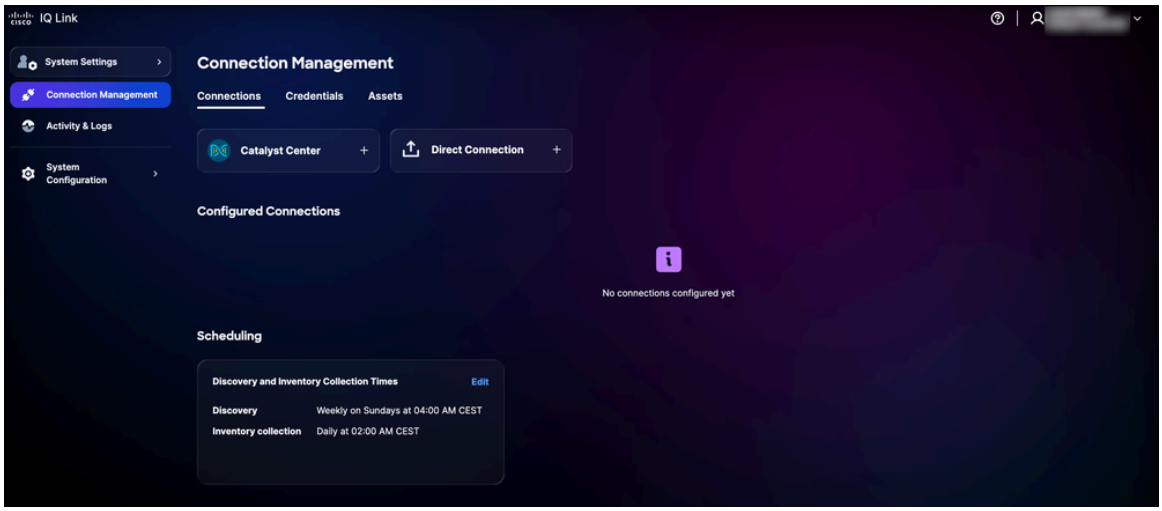
デバイスIP	使用可能なクレデンシャルセット	選択した資格情報セット
10.10.1.5	10.10.1.5、10.10.1.、10.10..*	10.10.1.5（完全一致）
10.10.2.15	10.10.2.、10.10..*	10.10.2.*（より具体的）
10.10.5.50	10.10...、..	10.10..（より詳細に）

注：デバイスが複数の重複カテゴリに分類される場合、システムは常に最も特異性の高い（つまり、末尾のワイルドカードが最も少ない）クレデンシャルセットを選択します。

Catalyst Centerを使用したデータ収集

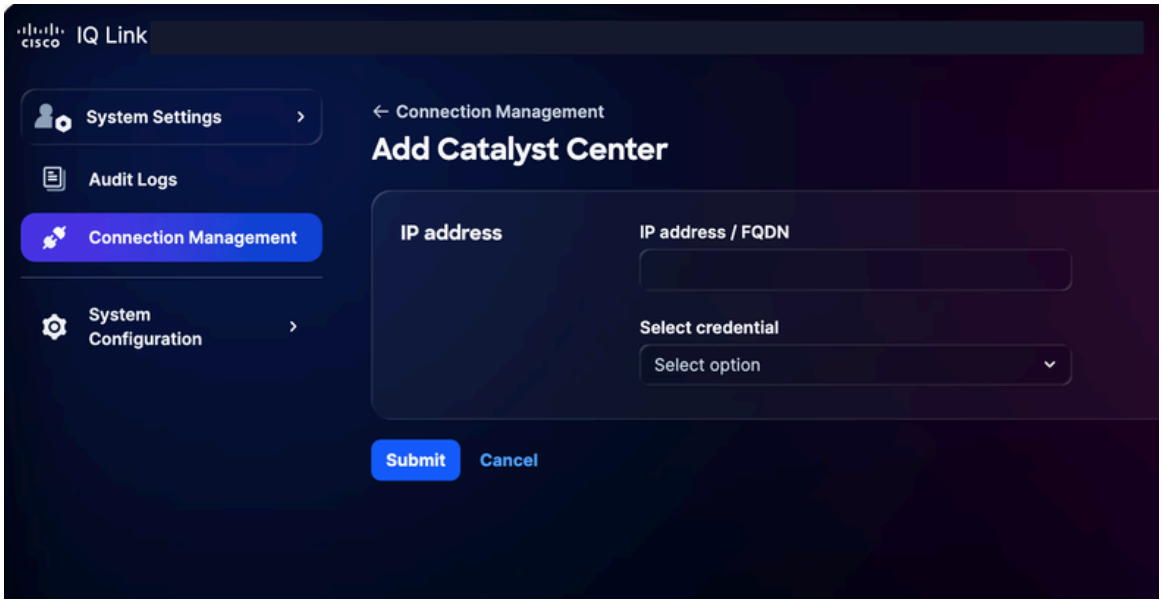
Catalyst Centerを使用したデータ収集：

1. System Settingsから、Connection Managementを選択します。Connection Managementページが表示されます。



接続管理

2. Catalyst Centerオプションをクリックします。

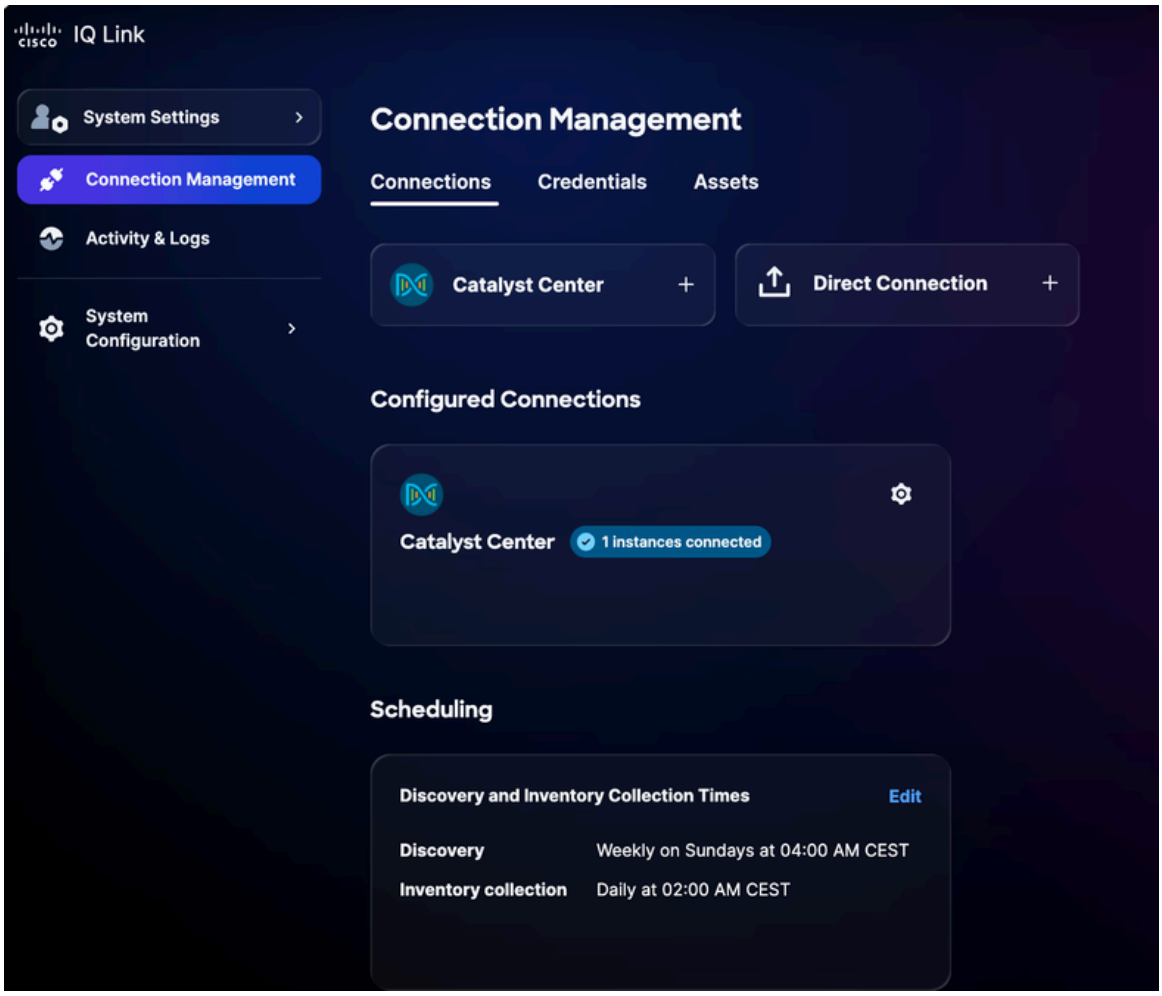


Catalyst Centerの追加

3. IPアドレスまたはFQDNを入力します。

4. ドロップダウンリストから、設定済みのHTTP/HTTPSクレデンシャルを選択します。

5. [Submit] をクリックします。確認が表示されます（最長75分かかる場合があります）。 新しく追加されたCatalyst Centerは、Configured Connectionsの下に表示されます。



Catalyst Centerが正常に追加されました

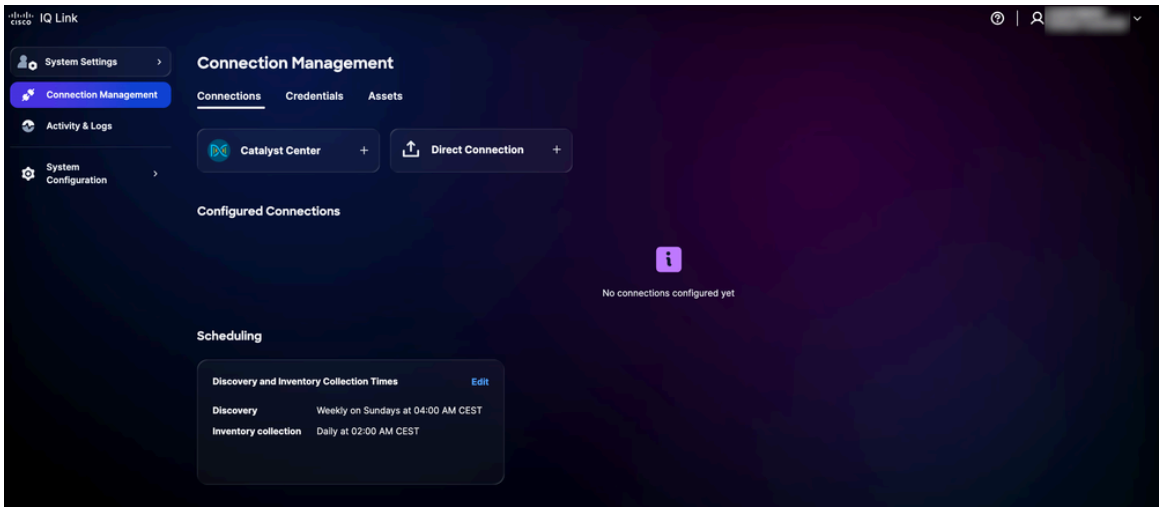
6. コレクションをスケジュールします。詳細は、『スケジューリング』を参照してください。

注:Cisco IQ Linkは自動スケジューリング設定で事前設定されており、システムはデフォルトの自動収集スケジュールを開始します。スケジュールを編集して、組織の要件とメンテナンス期間に合わせることを強くお勧めします。

直接接続

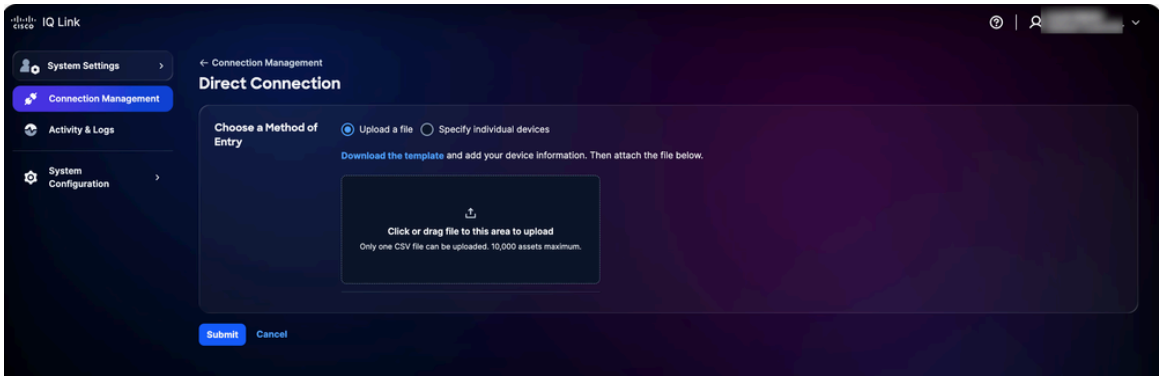
直接接続のデバイスを追加するには、次の手順に従います。

1. System Settingsから、Connection Managementを選択します。Connection Managementページが表示されます。



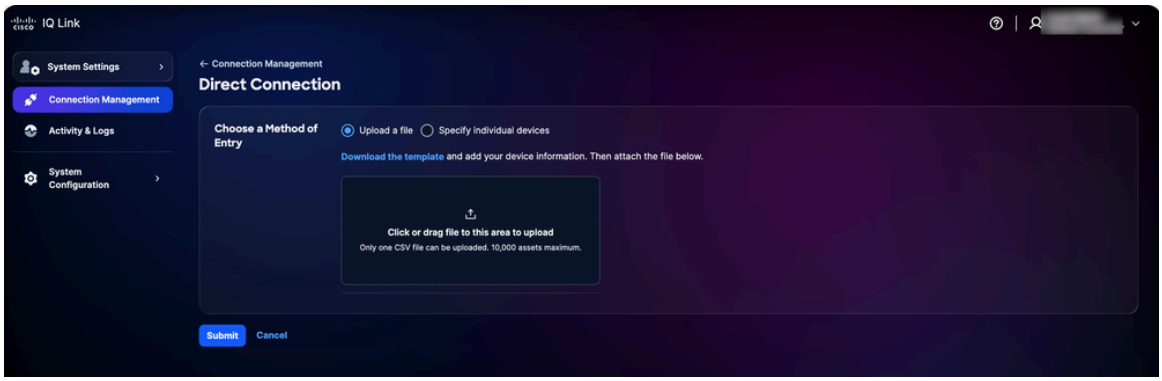
接続管理

2. Direct Connectionをクリックします。直接接続ページが表示され、データを収集するための2つのオプションが示されます。



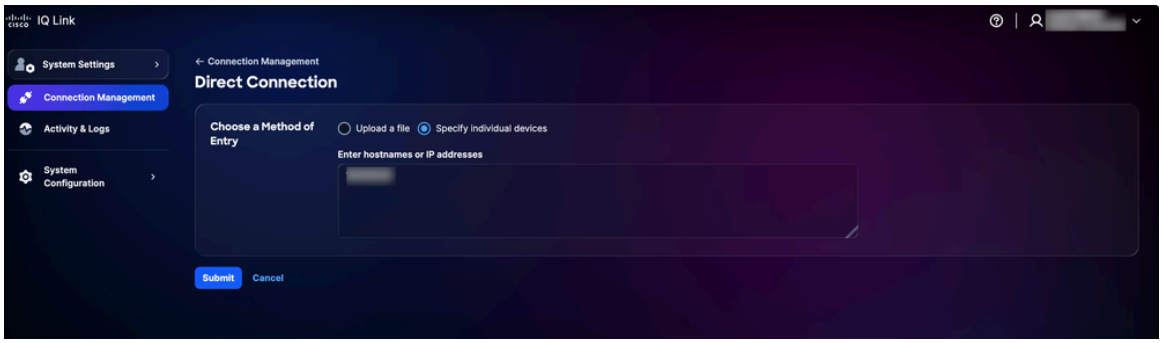
ファイルのアップロード

3. Choose a Method of Entryの適切なオプションをクリックし、次のいずれかの方法でデバイスを送信します。



ファイルのアップロード

- ファイルのアップロード：ファイルをクリックまたはドラッグアンドドロップして、[送信]をクリックします。



個々のデバイスの指定

- 個々のデバイスの指定：単一のホスト名、IPアドレス、またはホスト名とIPアドレスのカンマ区切りのリストを入力し、Submitをクリックします。

正常に送信されると、「Assets」タブにリダイレクトされます。

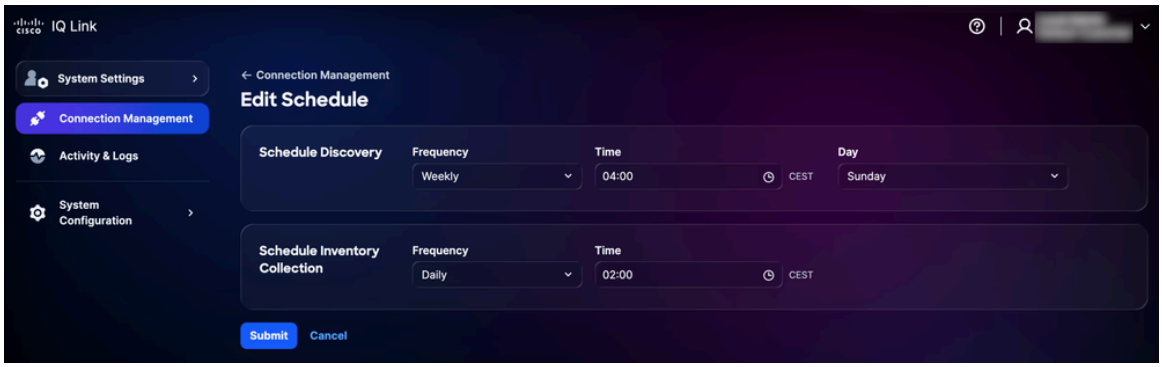
4. コレクションをスケジュールします。詳細は、『スケジューリング』を参照してください。

注:Cisco IQ Linkは自動スケジューリング設定で事前設定されており、システムはデフォルトの自動収集スケジュールを開始します。スケジュールを編集して、組織の要件とメンテナンス期間に合わせることを強くお勧めします。

スケジューリング

スケジューリングを使用すると、Cisco IQ Linkが自動データ収集を実行するタイミングを定義できます。収集をスケジュールする手順は、次のとおりです。

1. Connection ManagementページのSchedulingセクションで、変更するスケジュールに対してEditをクリックします。Edit Scheduleページが表示されます。



スケジュールの編集

2. Schedule Discoveryセクションで、ドロップダウンリストから目的のFrequencyとDayを選択し、目的のStart Timeを入力します。

3. Schedule Inventory Collectionセクションで、ドロップダウンリストから希望の頻度を選択し、希望の開始時刻Timeを入力します。

4. [Submit] をクリックします。

注：検出スケジュールまたは収集スケジュールの変更がCisco IQ Link内で正確に同期および反映されるまで、5 ~ 10分待ちます。

バナー

管理者は、アプリケーション全体で表示されるカスタマイズされたバナーを設定できます。

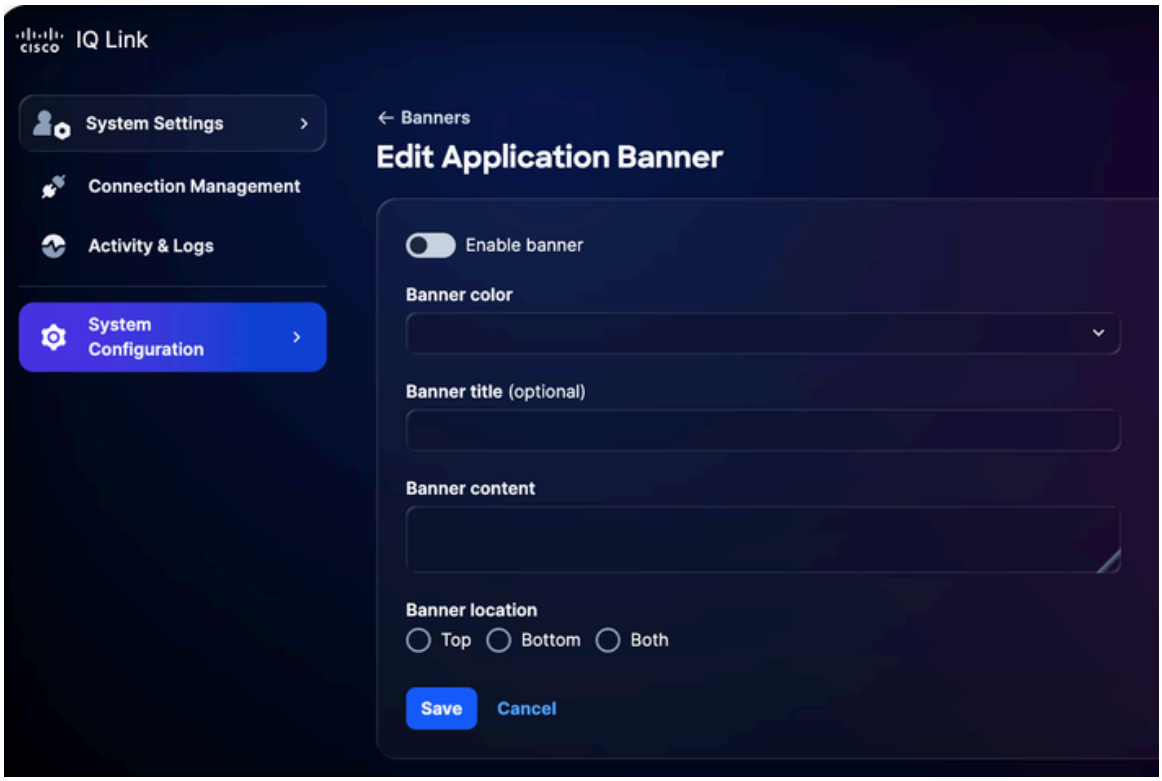
バナーの設定

バナーを設定するには、次の手順を実行します。

1. System Settingsで、System Configuration > Bannersの順に選択します。バナーページが表示されます。

バナーの設定

2. [Configure] をクリックします。Edit Application Bannerページが表示されます。



アプリケーションバナーの編集

3. バナーを有効または無効にするには、トグルをクリックします。
4. バナーの色を選択します。
5. バナータイトルを入力します。
6. バナーの内容を入力します。
7. バナーの場所を選択します。
8. [Save] をクリックします。バナーはアプリケーション全体に表示されます。

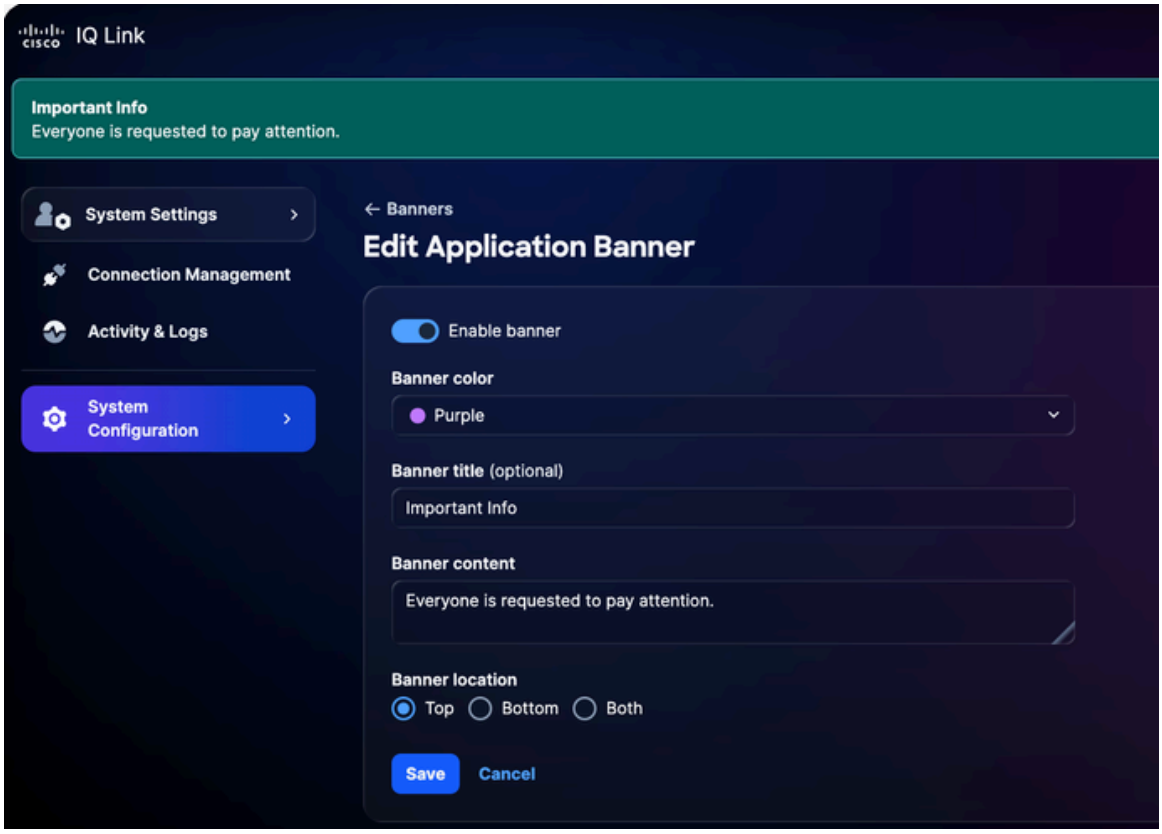
バナーの編集

バナーを編集するには、次の手順を実行します。

1. System Settingsで、System Configuration > Bannersの順に選択します。バナーページが表示されます。

バナーの編集

2. [Edit] をクリックします。Edit Application Bannerページが表示されます。



アプリケーションバナーの編集

3. 必要な詳細を編集します。

4. バナーを有効または無効にするには、トグルをクリックします。

5. [Save] をクリックします。

トラブルシューティング

お客様は、Cisco IQシステムから診断ファイルとログファイルを収集し、SCPサーバに安全に転送できます。これらのファイルは、問題を報告する際にサポートチームと共有でき、有益な情報を提供してトラブルシューティングを支援します。

診断ファイルとログファイルを収集するには、次の手順を実行します。

1. Cisco IQにログインします。

メインメニュー

2. Cisco IQ Main Menuで、「3」と入力してEnterキーを押し、System Diagnosticsを選択します。

システム診断

3. SCP/SFTPサーバアドレスを入力します。

4. SCP/SFTPサーバポートを入力します。
5. SCP/SFTPサーバパスを入力します。
6. プロトコルを選択します。
7. ユーザ名を入力します。
8. パスワードを入力します。
9. 「C」と入力してEnterキーを押し、システム診断を続行します。

システム診断操作CoSystem診断操作完了

診断プロセスが開始され、次のアクションが実行されます。

- 到達可能性の確認
- システム情報の収集
- Kubernetes情報の収集
- ログの収集
- システム診断バンドルの準備
- システム診断バンドルのアップロード

完了すると、生成されたバンドル名を示す確認メッセージが表示されます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。