Cisco IQ Link操作ガイドv1.2.0

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洞察の提供、およびケース管理の合理化を目的として設計された拡張機能を提供します。さらに、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

アカウント管理者は、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
- デフォルトアカウントコンテキスト:Default-Customer

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、ホームページのユーザプロファイルメニューから行うことができます。

ロックアウト設定

次のアカウントロックアウト設定は、導入時に設定可能です。

- ロックアウト・ステータス：アカウントのロックアウト機能を有効または無効にします。
- Maximum Login Attempts：アカウントがロックされるまでに連続して失敗できる最大試行回数を設定します (デフォルト： 3、範囲： 0 ~ 10) 。
- Rolling Time Window：失敗した試行を追跡する期間を定義します (デフォルト：15分、範囲：0 ~ 60分) 。
- Duration：最大試行回数に達した後もアカウントがロックされたままになる期間を設定します (デフォルト： 30分、範囲： 0 ~ 60分) 。

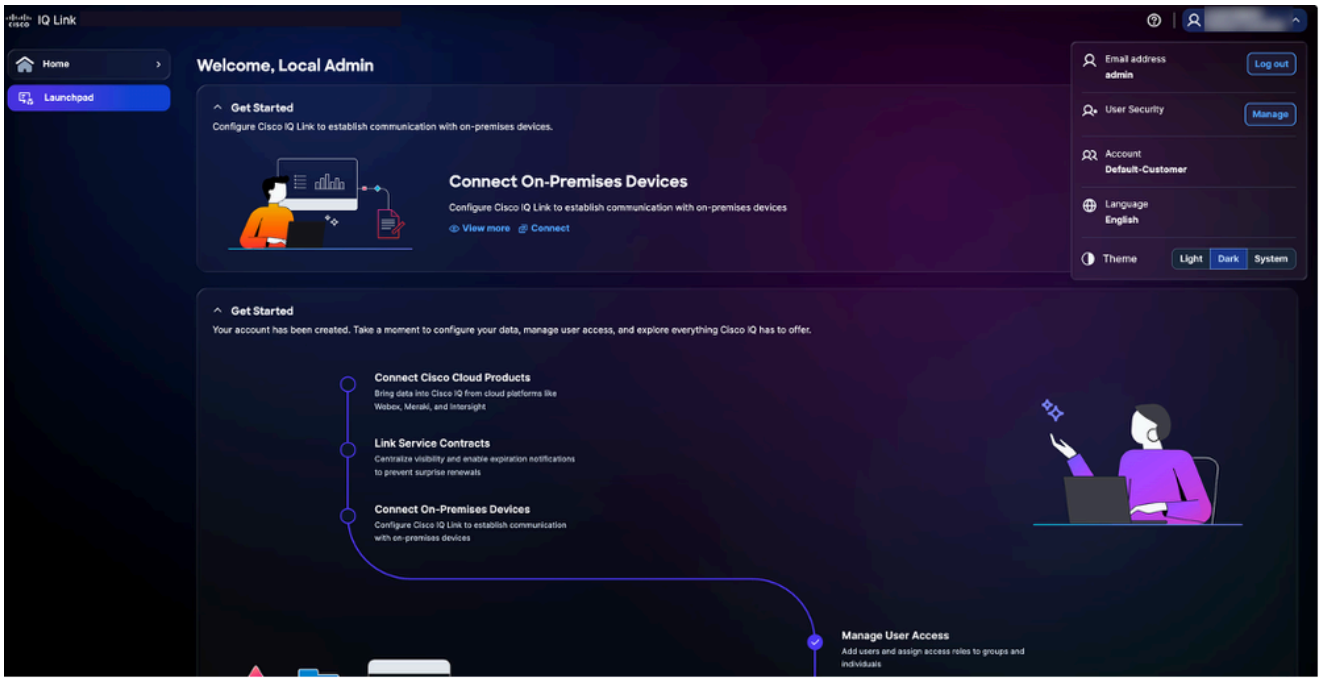
注：15分以内に3回、正しいパスワードを入力しようとしました。3回の試行がすべて失敗した場合、セキュリティを保護するためにアカウントが一時的に30分間ロックされます。ロックアウト期間中はログインできません。失敗した試行回数が多すぎるため、「アカウントがロックされました。Please try again later.」が表示されます。
アカウントは30分後に自動的にロック解除され、その時点でログインまたはパスワードのリセットを試みることができます。

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。アカウント管理者は、パスワードのリセット機能を有効にするために、5つの秘密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. ホームページで、ユーザプロファイルアイコンをクリックします。ドロップダウンメニューが開きます。

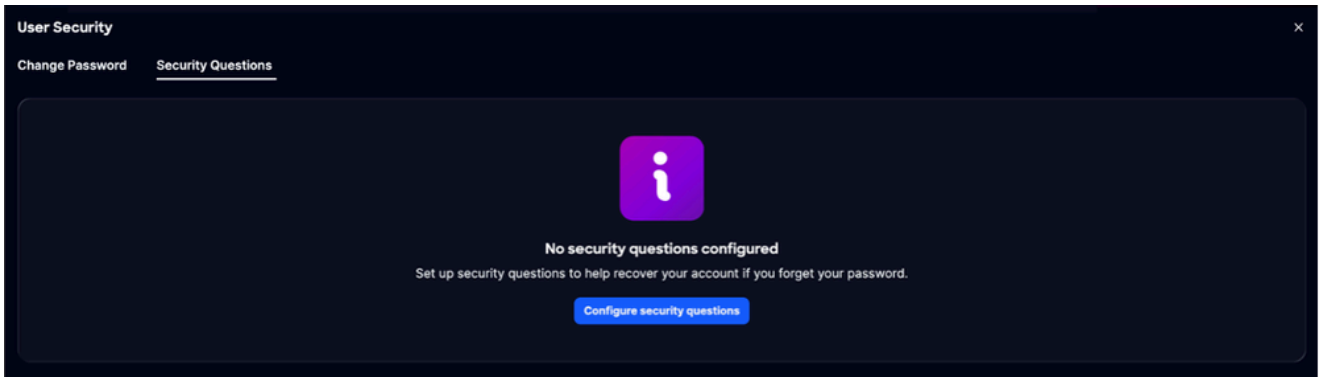


ユーザプロファイルメニュー

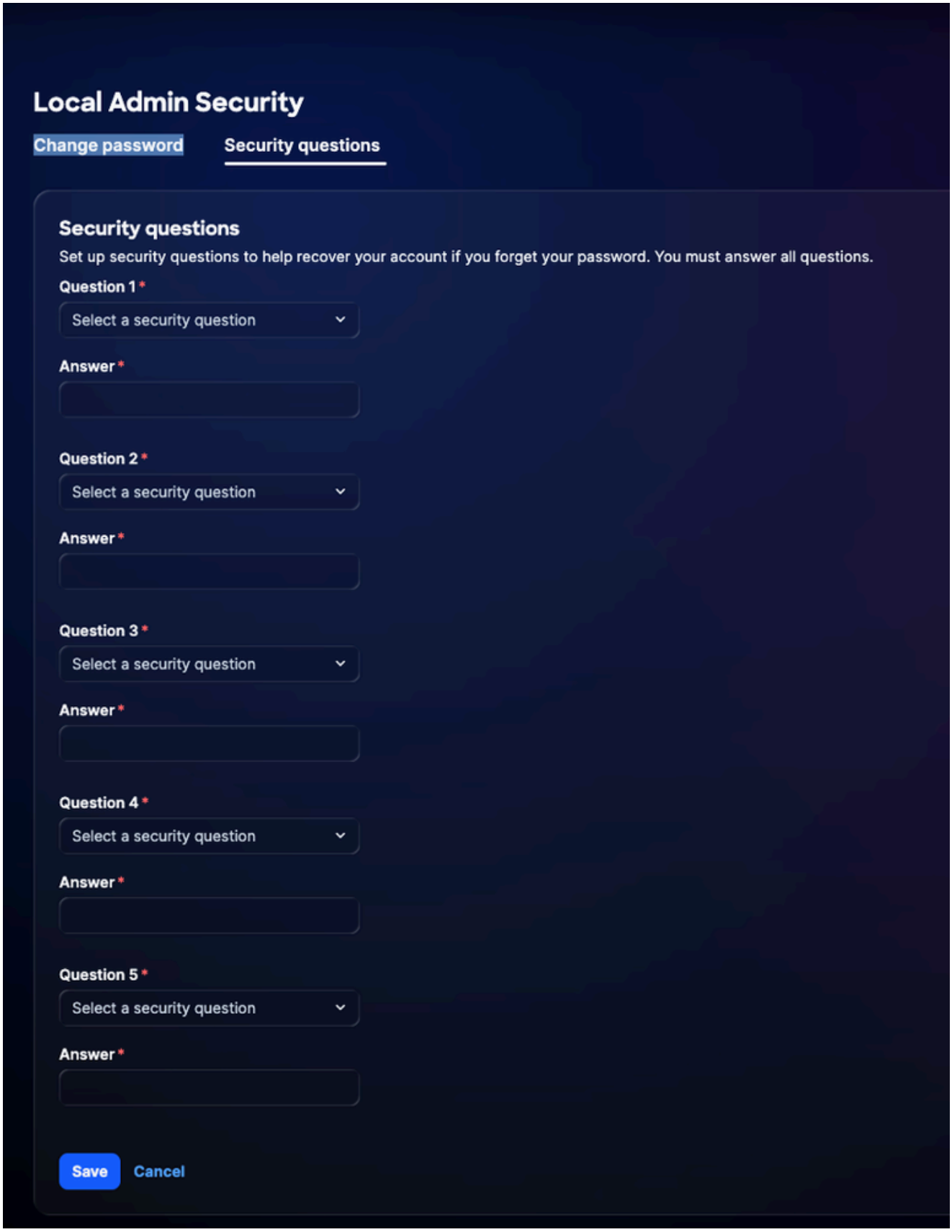
2. User SecurityでManageをクリックします。User Securityページが表示されます。

パスワードの変更

3. Security Questionsをクリックして、タブを開きます。



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



5. 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。

6. 各質問に対する回答を入力します。

7. [Save] をクリックします。

注：回答では大文字と小文字は区別されません。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ます。たとえば、「Smith」と「smith」は同じと見なされます。

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

アカウント管理者とローカルユーザは、Cisco IQのパスワードを管理できます。

アカウントのセキュリティを確保するために、次のパスワードポリシーが適用されます。

- 再利用の制限：新しいパスワードは、以前の5つのパスワードのいずれとも一致しません。このポリシーは、サインアップ、パスワードを忘れた場合、およびパスワードを変更する場合のフローに適用されます。
- 文字のバリエーション：認証中にパスワードを変更する場合は、現在のパスワードと少なくとも8文字が新しいパスワードで異なっている必要があります。
- 最小変更間隔：デフォルトでは、パスワードを再度変更する前に24時間待機する必要があります。別の間隔が設定されている場合、その時間が経過するまでパスワードを更新できません。
- パスワードの有効期限：パスワードは60日ごとに有効期限が切れます。有効期限後に初めてログインすると、システムにアクセスする前に新しいパスワードを設定する必要があります。（0に設定すると、パスワードの有効期限は無効になります）。

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。

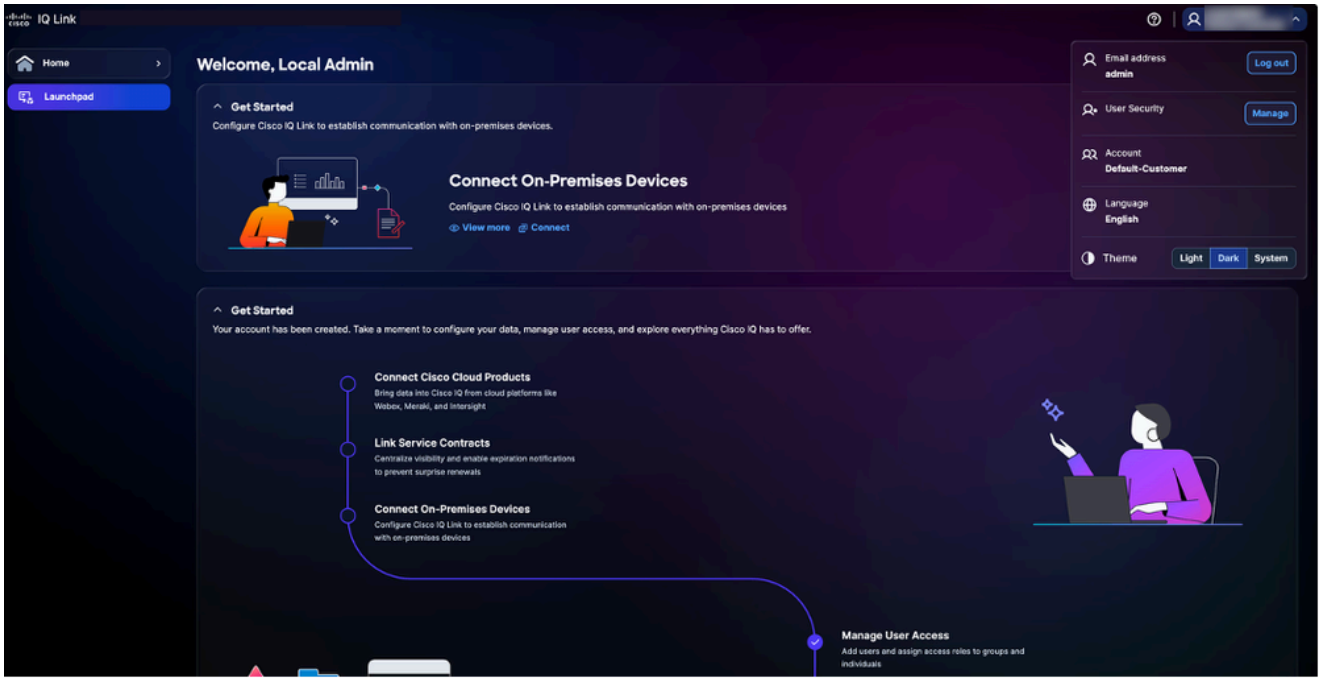
- ローカルアカウントの管理者またはユーザーである

- ローカルアカウントを使用している(シングルサインオン(SSO)または外部認証ではない)
- Cisco IQ Link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、次の手順に従います。

1. ホームページで、ユーザプロファイルアイコンをクリックします。ドロップダウンメニューが開きます。



ユーザプロファイルメニュー

2. User SecurityでManageをクリックします。User Securityページが表示されます。

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

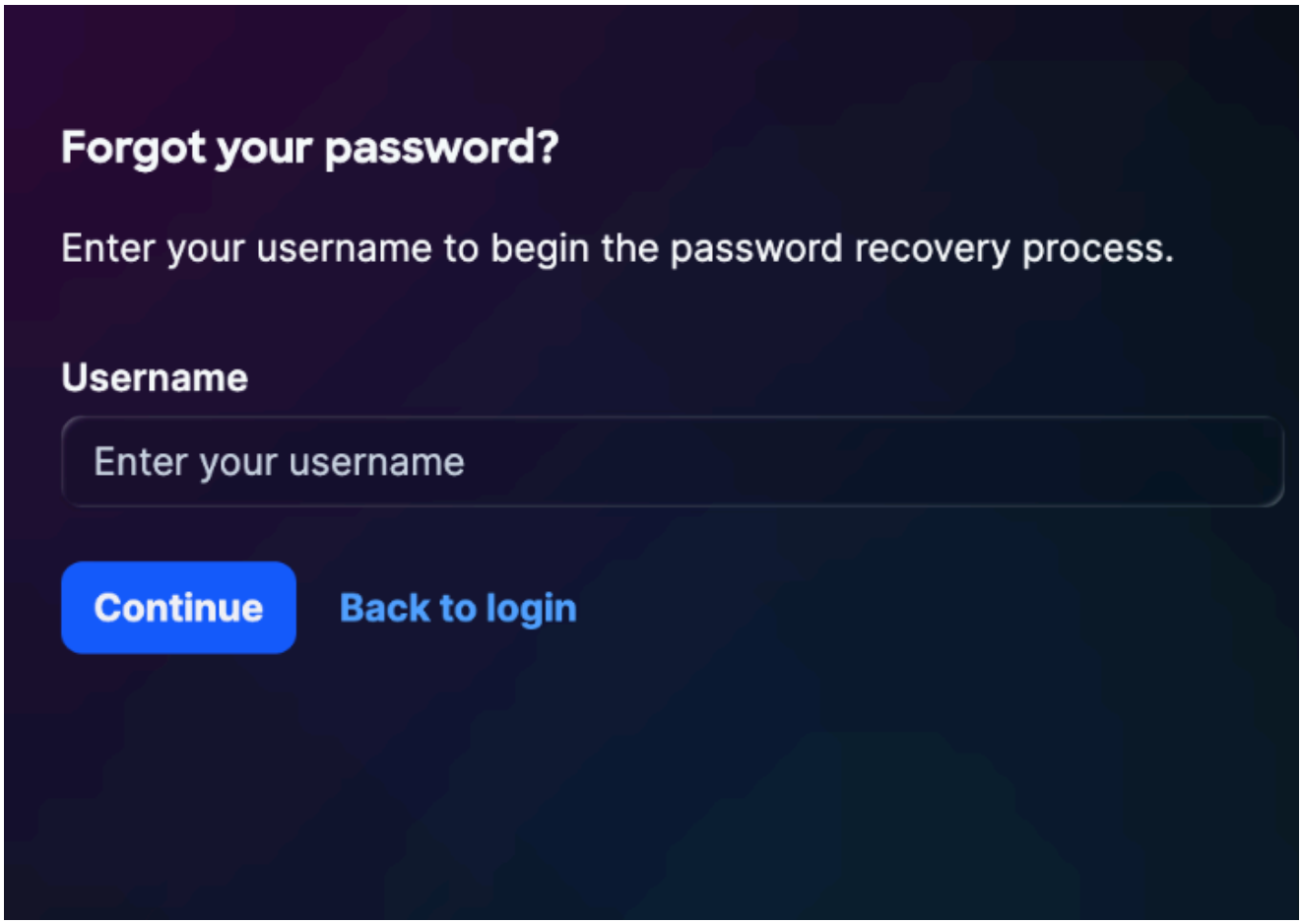
パスワードは、Cisco IQ仮想マシン(VM)を含むCisco IQシステムで更新されます。

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。

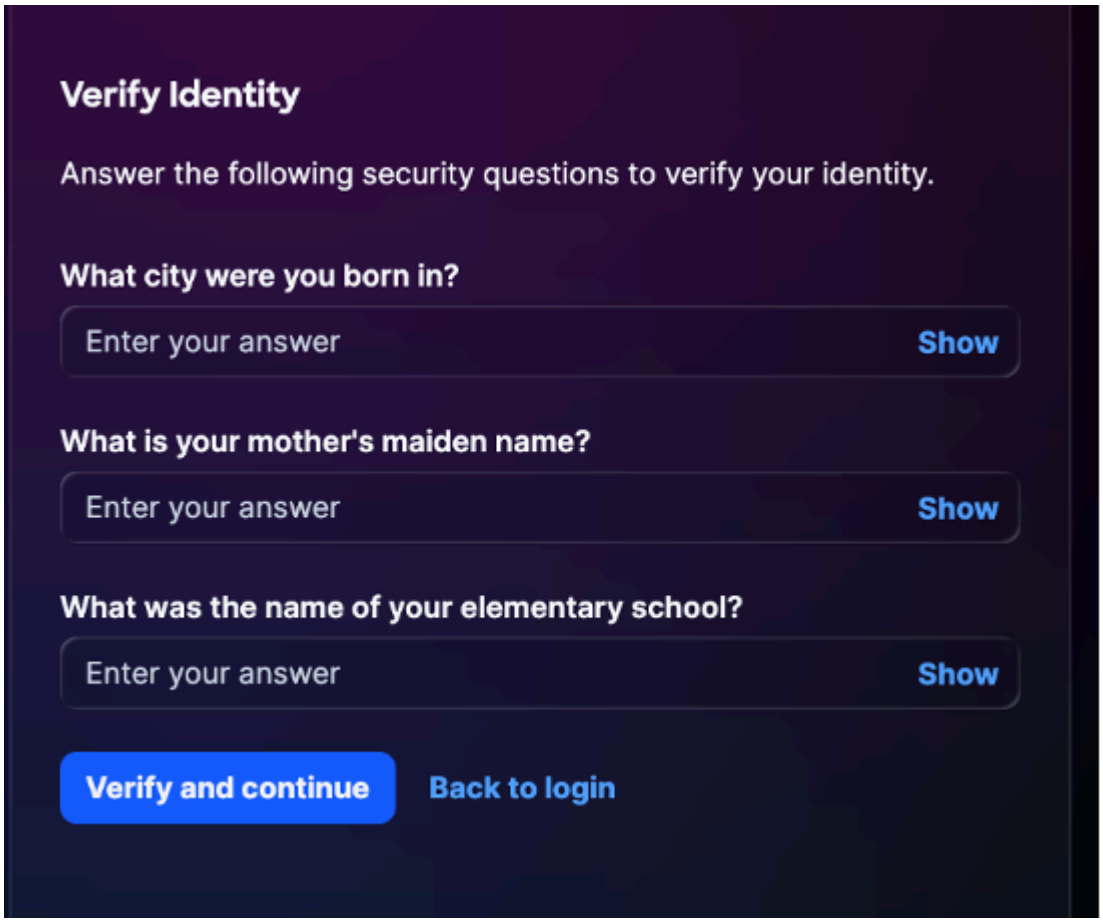
忘れたパスワードをリセットするには、次の手順を実行します。

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。



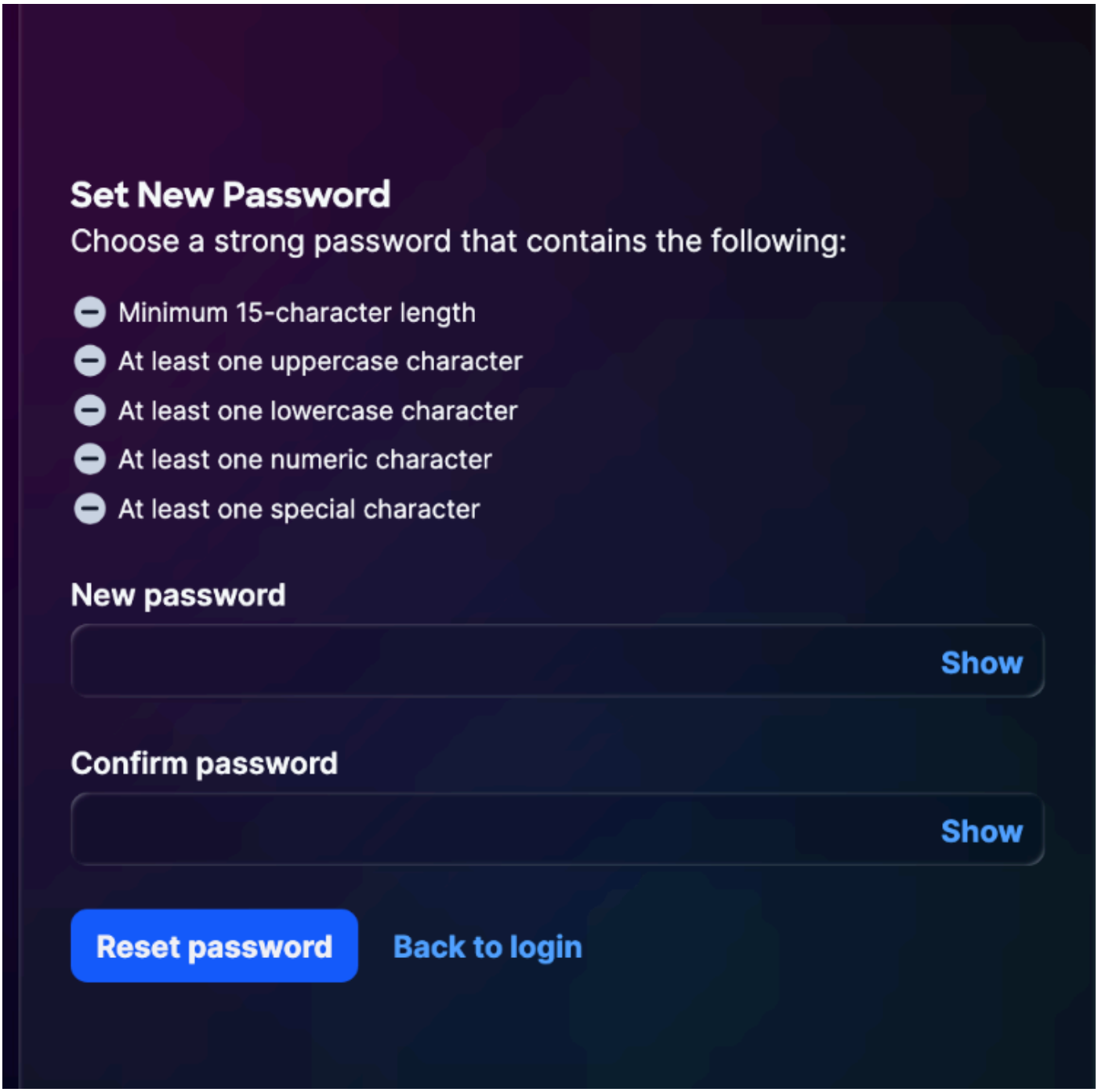
IDの確認

✎ 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

15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30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30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。

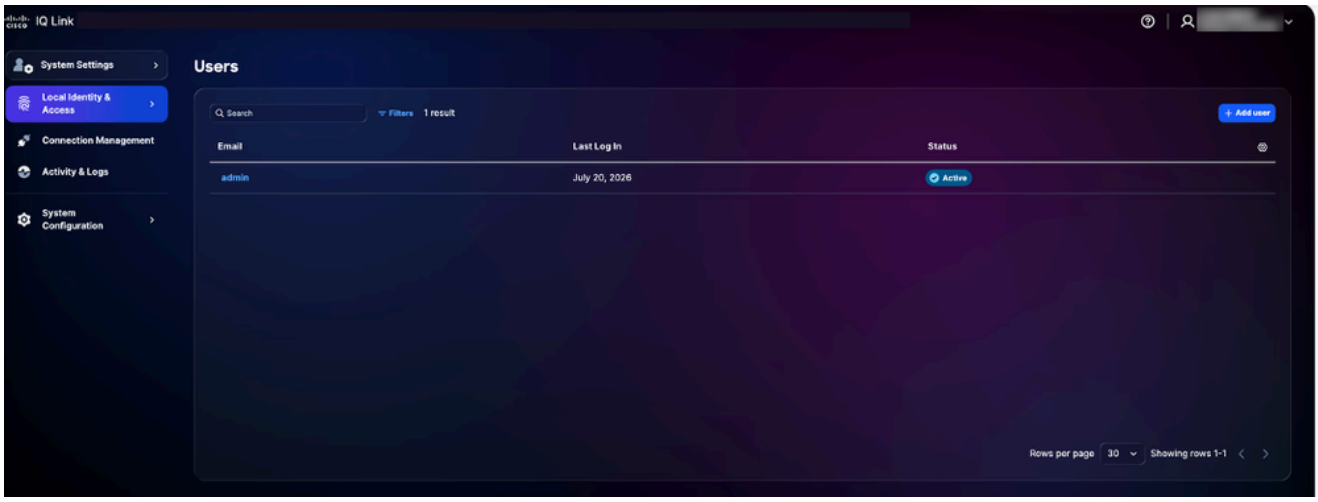
8. 確認のため、パスワードを再入力します。

9. Submitをクリックします。

ローカルユーザの追加

アカウント管理者は、Cisco IQアカウントにユーザを追加できます。新しいユーザを追加するには、次の手順を実行します。

1. System Settings > Local Identity & Access > Usersの順に移動します。Usersページが表示されます。既存のすべてのローカルユーザとそのステータスが表示されます。

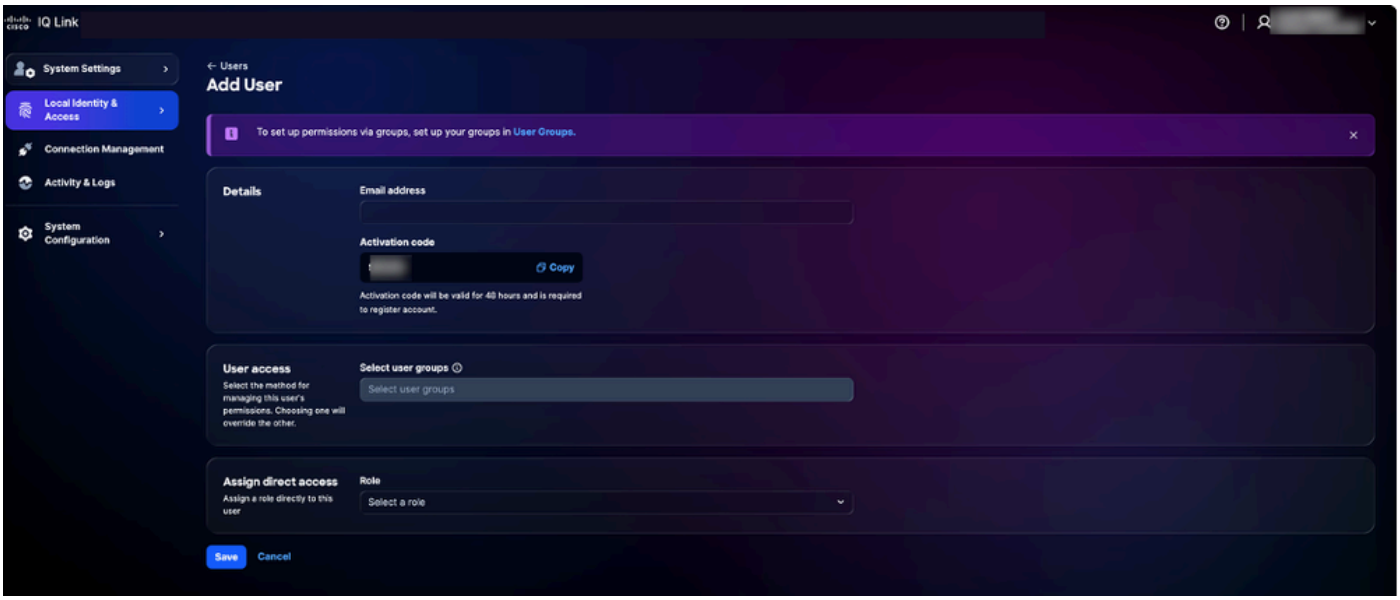


ユーザページ

注: (上の図に示すように) アカウント管理者にはその他のオプションアイコンは表示されません。

---

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



ユーザの追加

3. 「電子メール・アドレス」を入力します。

4. アクティベーションコードを入力します。

注：アクティベーションコードはデフォルトで表示されます。登録を完了する必要があるため、ユーザと共有します。

---

5. 「ユーザー・アクセス」で、「ユーザー・グループの選択」ドロップダウン・リストからユーザー・グループを選択します。

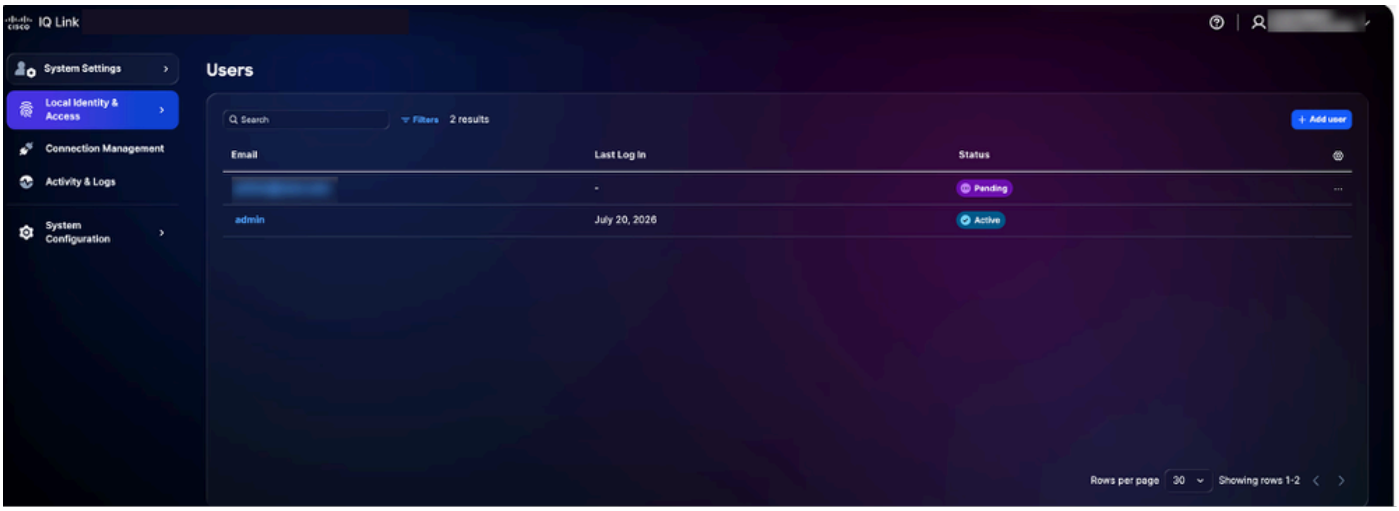
注：ユーザは選択したグループからアクセス権を継承します。

---

6. Assign direct accessで、Roleドロップダウンリストからroleを選択します。次の2つのロールを使用できます。

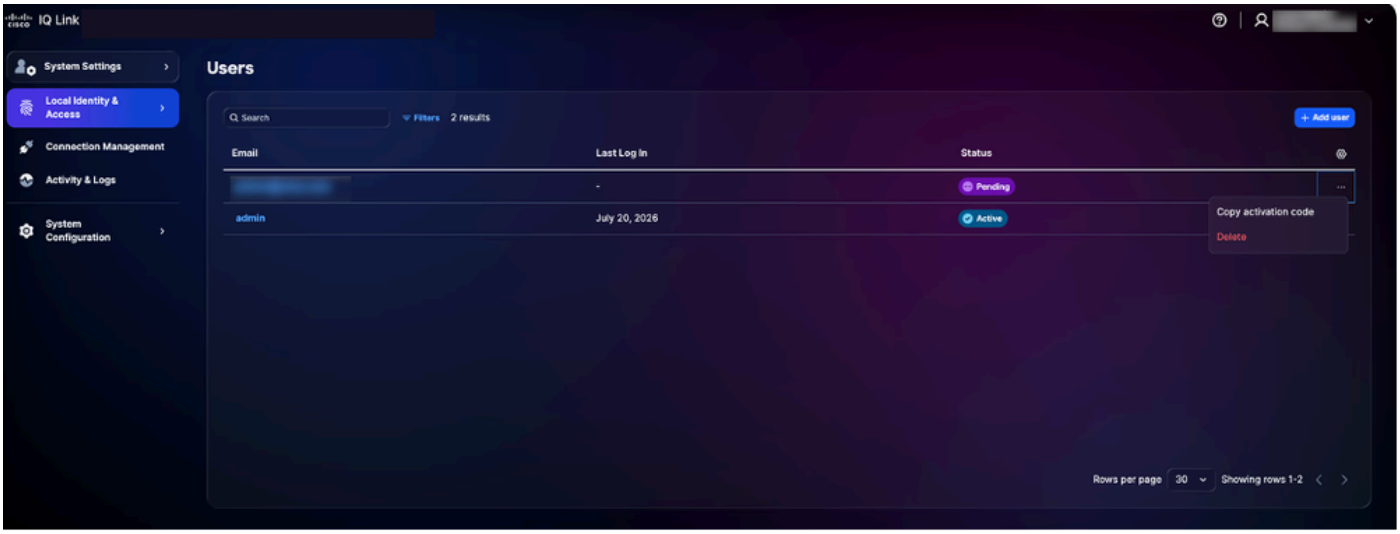
- ビューア：アプリケーションの表示とアクセス
- 管理者：アプリケーションにアクセスし、システム管理とIDPを除くシステム設定を管理します

7. Saveをクリックします。新しいユーザが作成され、ユーザリストにPending状態で表示されます。保留中は、ユーザーがまだセルフアクティブ化を完了していないことを示します。



新しく追加されたユーザー

8. リストで新しく作成されたユーザーを検索し、「ステータス」列に「保留中」と表示されていることを確認します。



アクティベーションコードのコピー

9. 新しく作成したユーザの横にあるその他のオプションアイコン>アクティベーションコードのコピーをクリックします。アクティベーションコードがクリップボードにコピーされます。

10. このコードをユーザーと安全に（例えば、安全な内部チャネルを介して）共有します。 アクティベーションコードは1回限りの使用であり、登録を完了するために必要です。

注：非セキュアチャネルではアクティベーションコードを共有しないでください。コードが紛失または改ざんされた場合は、メニューアイコンを使用して新しいアクティベーションコードを再生成すると、以前のアクティベーションコードが無効になります

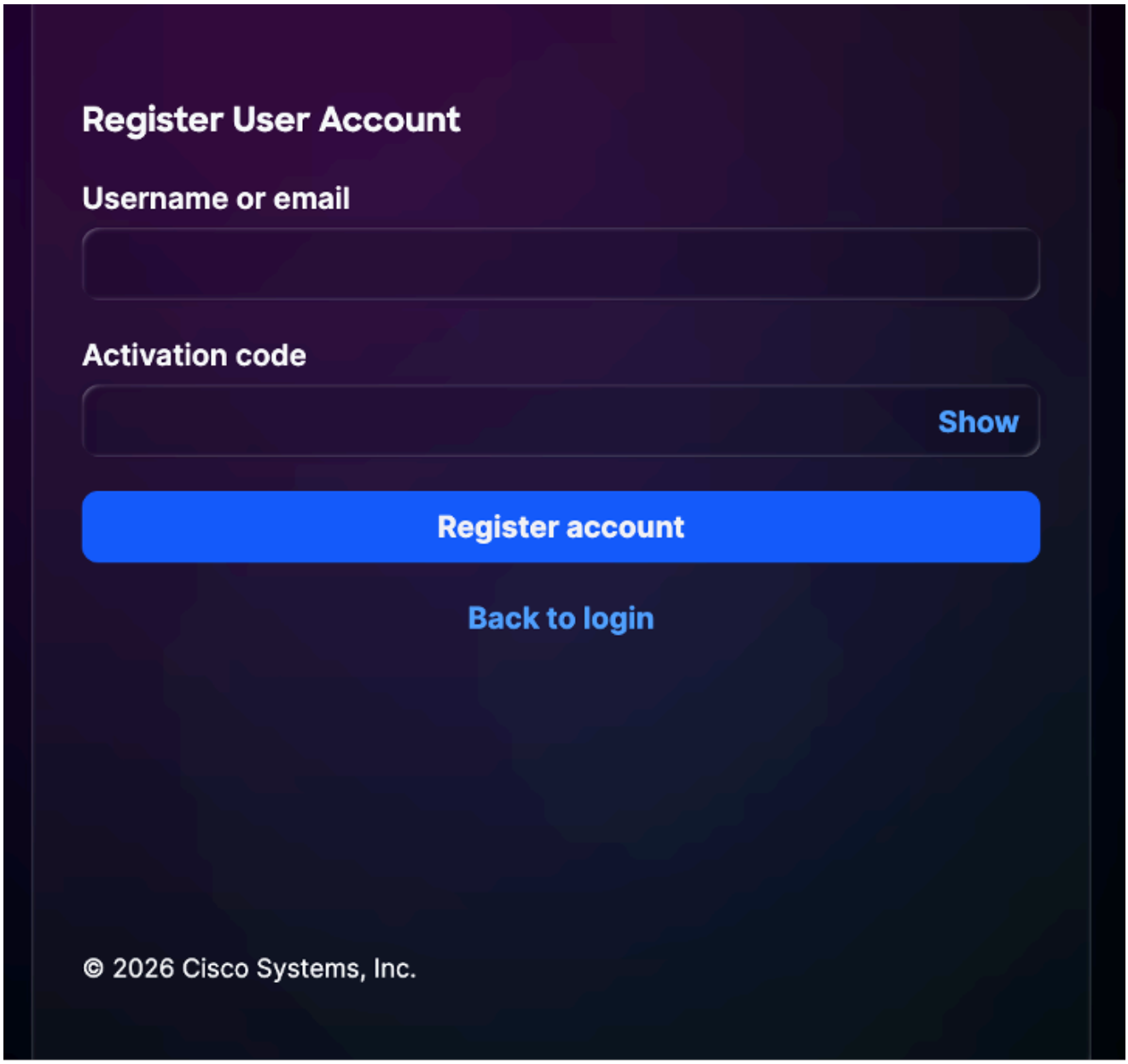
注：アクティベーションコードは48時間有効です。コードの有効期限が切れた場合は、アカウント管理者に新しいコードをリクエストしてください。

11. ログアウトするには、右上隅にあるUserアイコンをクリックして、Logoutを選択します。Cisco IQログインページに戻ります。

新しいユーザーアカウントの登録

新しいユーザアカウントを登録するには、次の手順を実行します。

1. ログインページで、Register a new user accountリンクをクリックします。

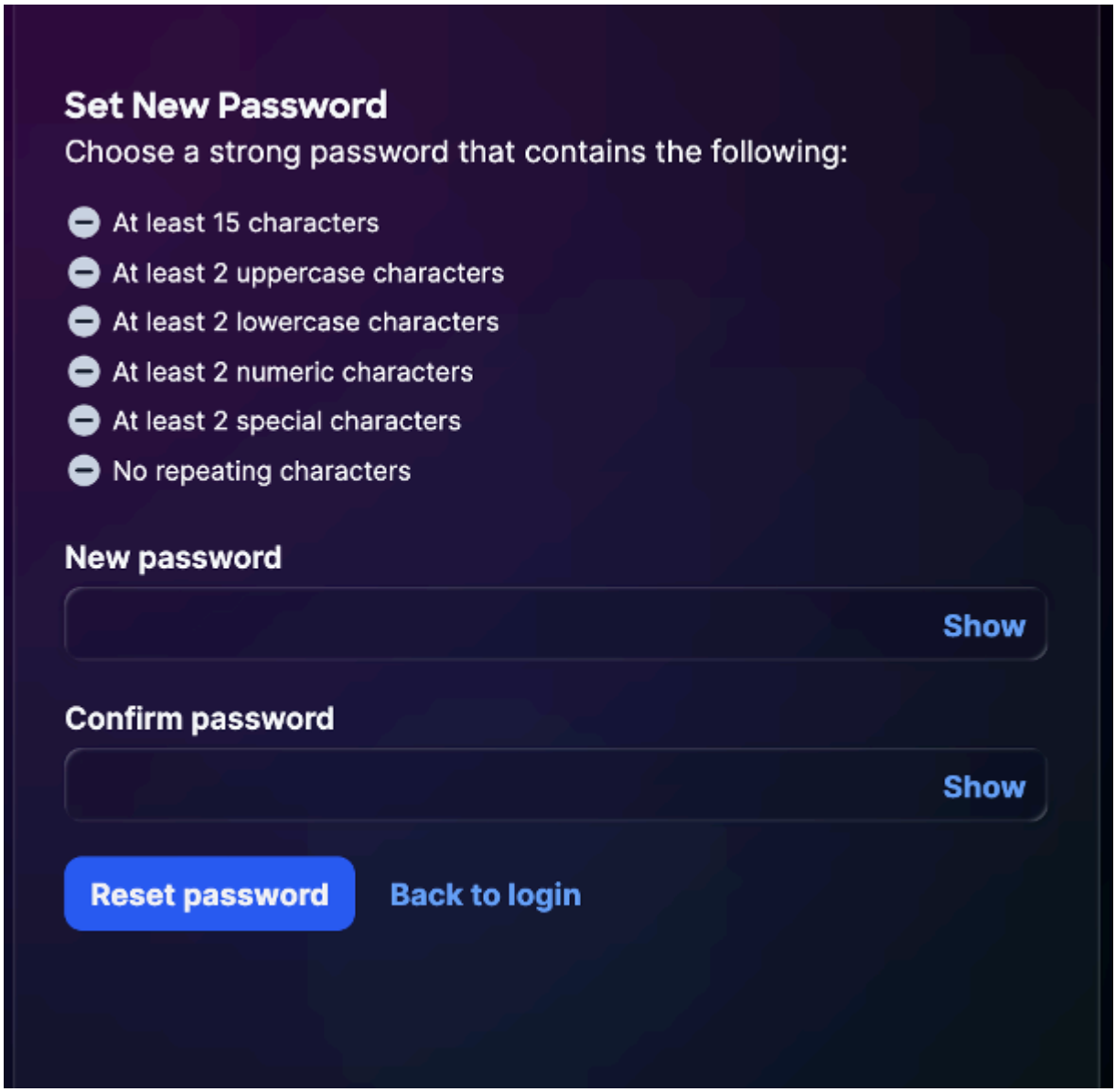


新しいユーザーアカウント

2. ユーザの作成時に使用したユーザ名または電子メールアドレスを入力します(例：user1@abc.com)。

3. アカウント管理者が共有するアクティベーションコードを入力します。

4. Register accountをクリックします。Set New Passwordウィンドウが表示されます。



新しいユーザーアカウントパスワード

5. 新しいパスワードを入力します。

6. 「パスワードの確認」にパスワードをもう一度入力します。

7. 最初のログインが成功すると、5つのセキュリティ質問を設定するように求められます(詳細については、「セキュリティ質問と回答の設定」を参照してください)。

ローカル・ユーザー・グループの管理

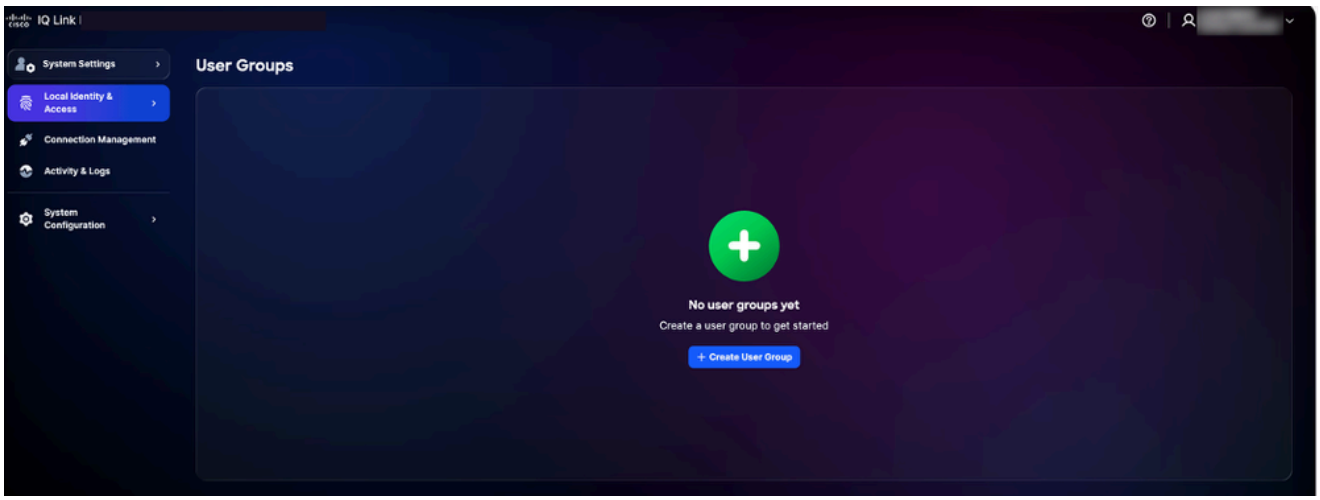
ユーザー・グループを使用すると、アカウント管理者は、複数のローカル・ユーザーの役割を同時に管理できます。アカウント管理者は、各ユーザーに個別にロールを割り当てる代わりに、グループを作成し、ロールと一連のユーザーをそのロールに割り当て、ロールまたはメンバーシップを1か所で更新できます。ユーザグループの管理はすべて、Local Identity & Accessページから実行します。

注：ユーザーグループを作成、編集、または削除できるのは、アカウント管理者だけです。グループは既存のローカルユーザで構成されます。ユーザをグループに追加するには、ユーザを作成する必要があります。

ユーザグループの作成

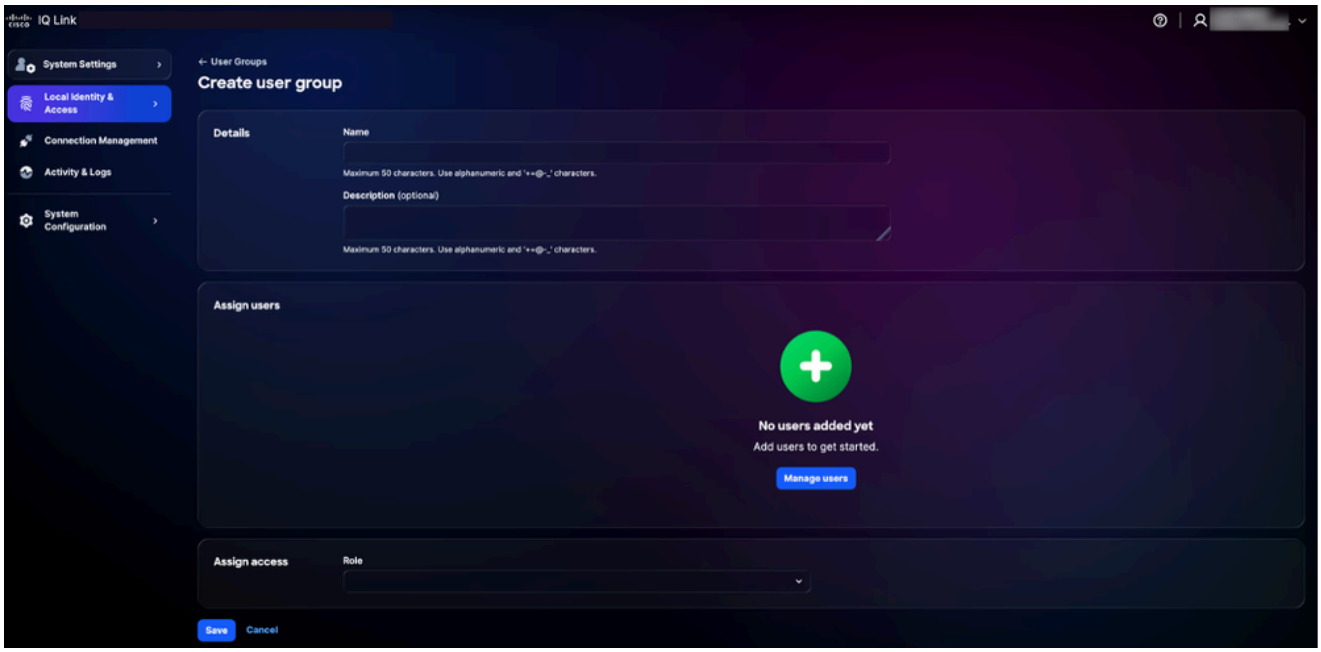
ユーザー・グループを作成するには、次の手順に従います。

1. System Settingsで、Local Identity & Access > User Groupsの順に選択します。User Groupsページが表示されます。



ユーザーグループ

2. Create User Groupをクリックします。Create user groupページが表示されます。



ユーザグループの作成

3. 次のセクションを完了します。

- 詳細
  - 名前：グループの一意の名前を入力します（例：読取り専用演算子）。
  - Description（オプション）：グループの簡単な説明（最大50文字、英数字、+ = @ - _文字を使用できます）。

- ユーザの割り当て

  グループに追加する1人以上の既存のローカルユーザを検索して選択します。

  注：まだ表示されていないユーザを追加するには、ユーザの管理をクリックします。

- アクセス権の割り当て

  - ロール：このグループのすべてのメンバーに割り当てるシステムロールを選択します。次のロールを使用できます。

    - Viewer：アプリケーションの表示とアクセス（読み取り専用）
    - 管理者：アプリケーションにアクセスし、システム設定を管理します

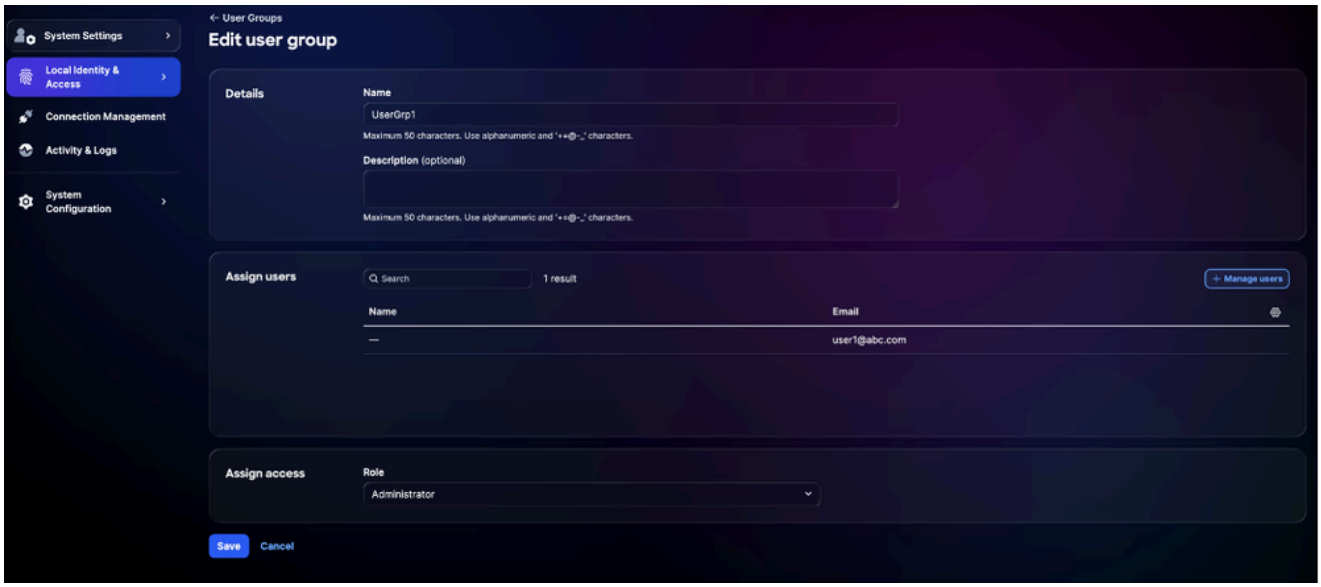
4. Saveをクリックします。

新しいユーザグループが、割り当てられたロールとメンバ数とともにユーザグループのリストに表示されます。

ユーザグループの編集

ユーザー・グループを編集するには、次の手順に従います。

1. User Groupsリストから、変更するグループを探します。
2. グループの横にあるMoreアイコンをクリックして、Editを選択します。Edit user groupページが表示されます。



ユーザグループの編集

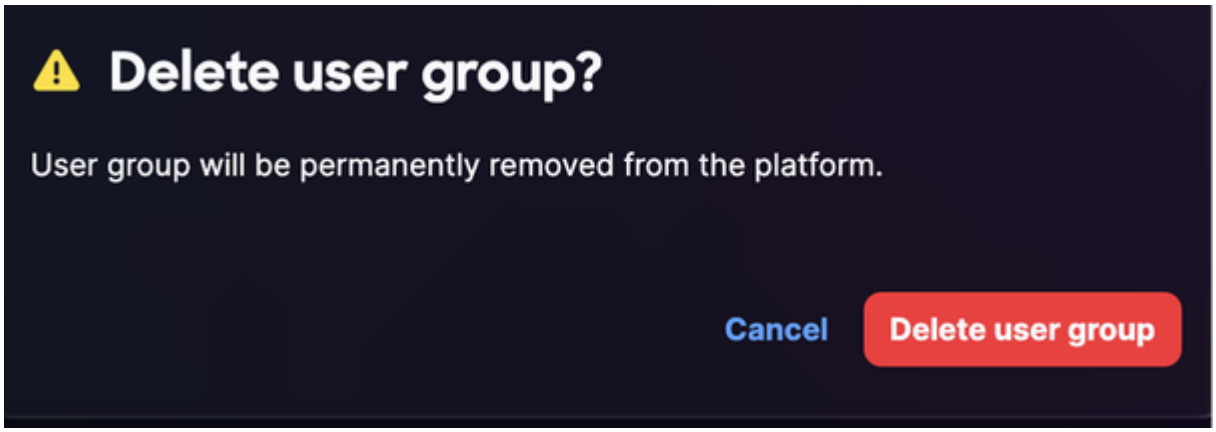
3. 必要な変更を行います。
4. [Save] をクリックします。

更新されたグループが[ユーザグループ]リストに表示されます。新しいロールは、グループのすべてのメンバーに対して有効になります。

ユーザグループの削除

ユーザー・グループを削除するには、次の手順に従います。

1. User Groupsリストから、削除するグループを探します。
2. グループの横にあるMore Optionsアイコンをクリックして、Deleteを選択します。



ユーザグループの削除

3. プロンプトが表示されたら、削除を確認します。

User Groupsリストからグループが削除されます。

注：ユーザグループを削除すると、グループベースのロール割り当てがすべてのメンバから削除されます。個々のユーザアカウントは削除されません。

IDプロバイダーの設定

Cisco IQ Linkにログインすると、アカウント管理者はさまざまな設定を行うことができます。アカウント管理者は、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へのローカルアカウント管理者アクセス
- 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属性を設定します。
表1: Cisco IQ Linkの属性

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
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。

表2: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）	完全修飾ドメイン名(FQDN)	mymanagementhost.mydomain.com
シングルサインオンURL	SAML Assertion Consumer Service(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構成します。

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。

表3: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またはACS URL）	https://mymanagementhost.mydomain.com

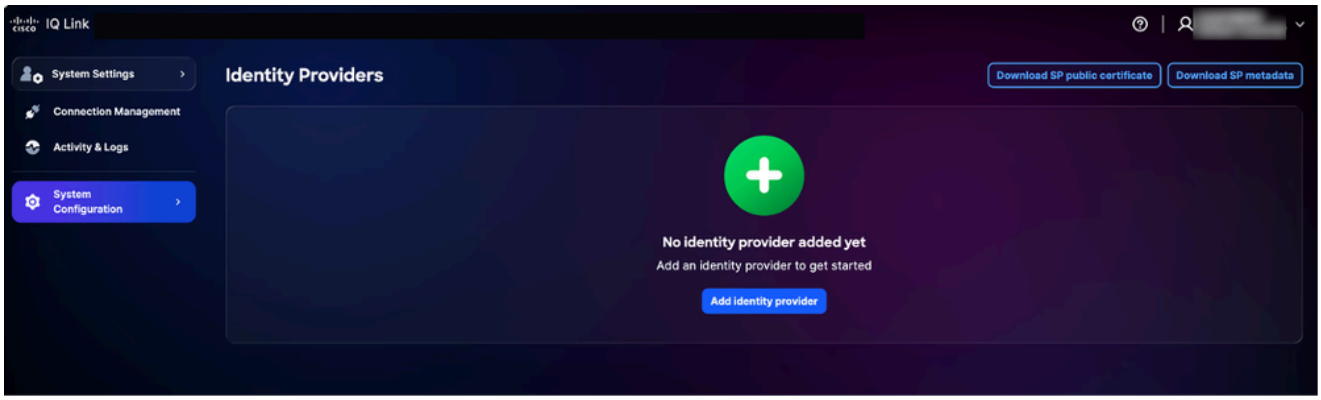
5. 「ダウンロード」アイコンをクリックして、「SPメタデータ」ファイルをダウンロードします。

6. プロバイダ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。

Okta IDPの追加

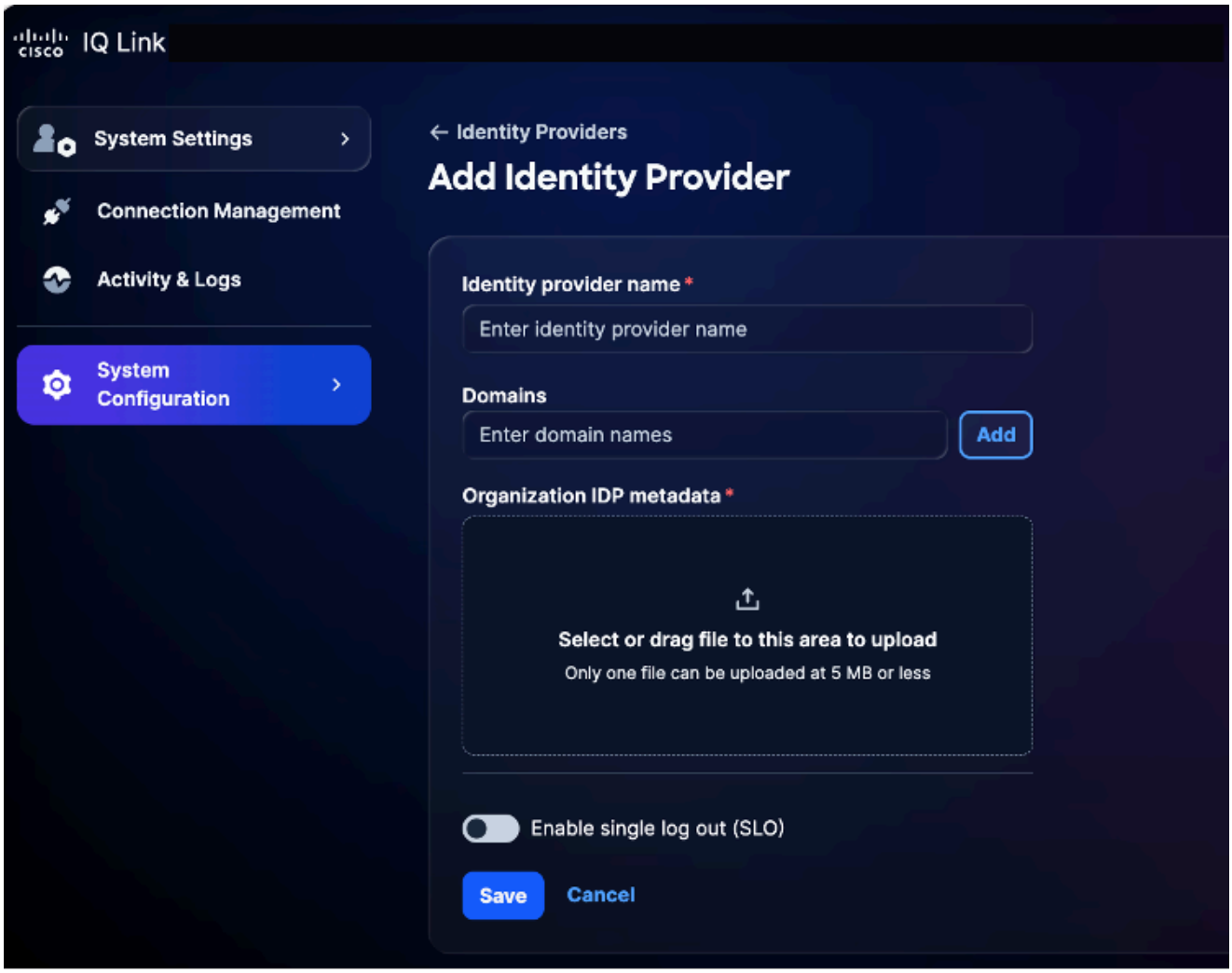
Cisco IQ LinkでIDPを追加するには：

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。

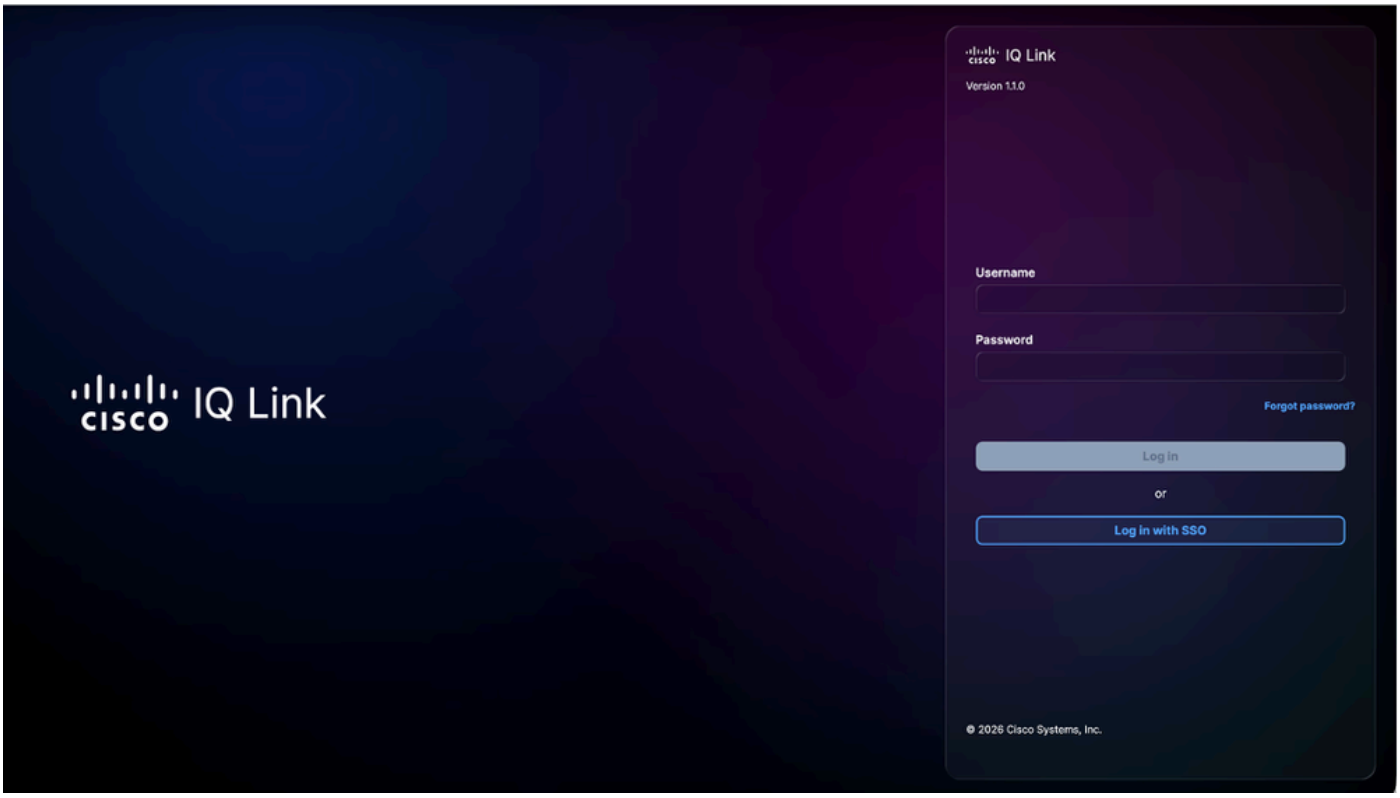
4. Addをクリックして、Cisco IQ Linkで設定されたドメイン名をDomainsフィールドに追加します。

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）シングルログアウトを有効にする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。

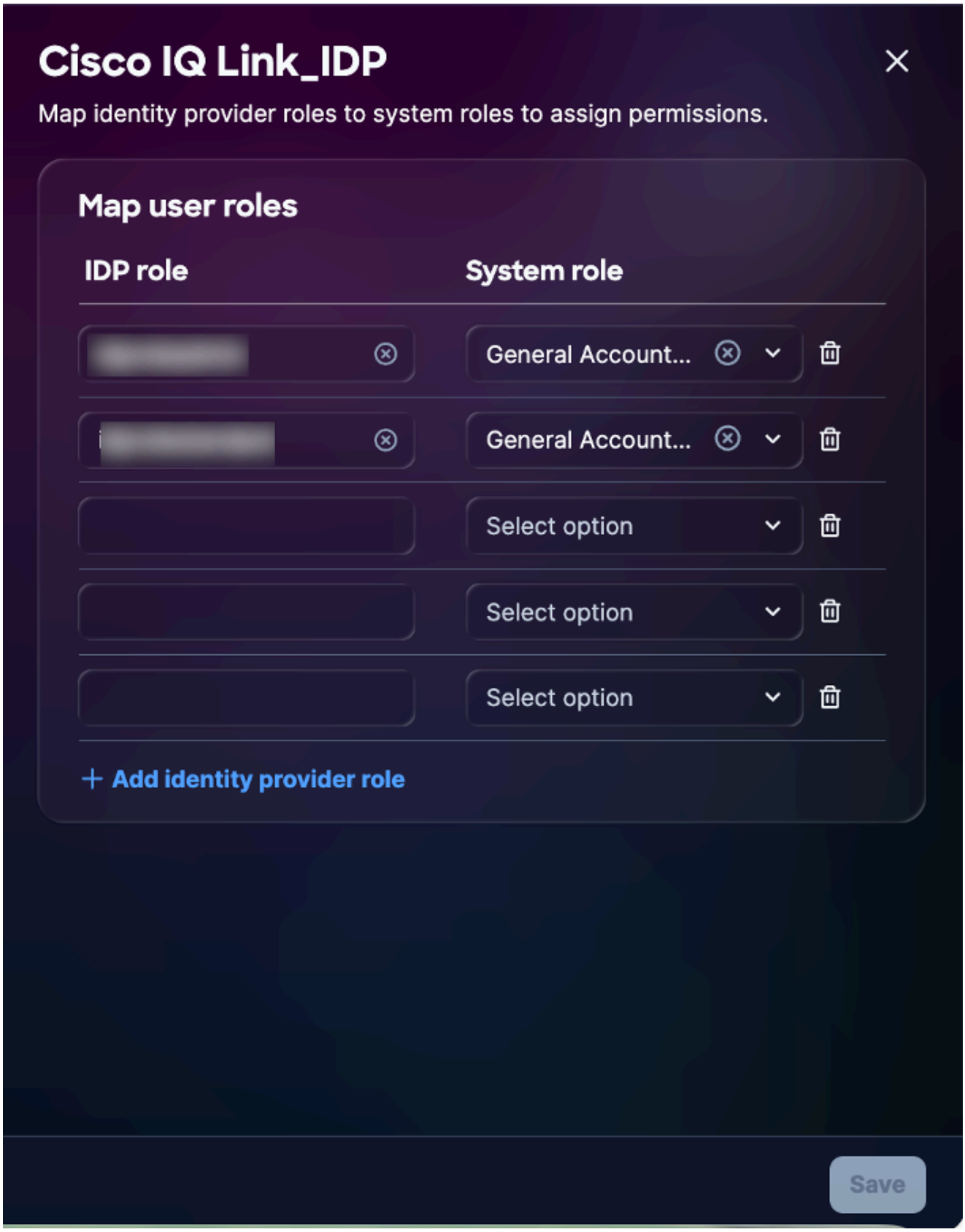
設定が完了すると、ログインページにSSO（IDP経由）でログインするためのオプションが表示されます。



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

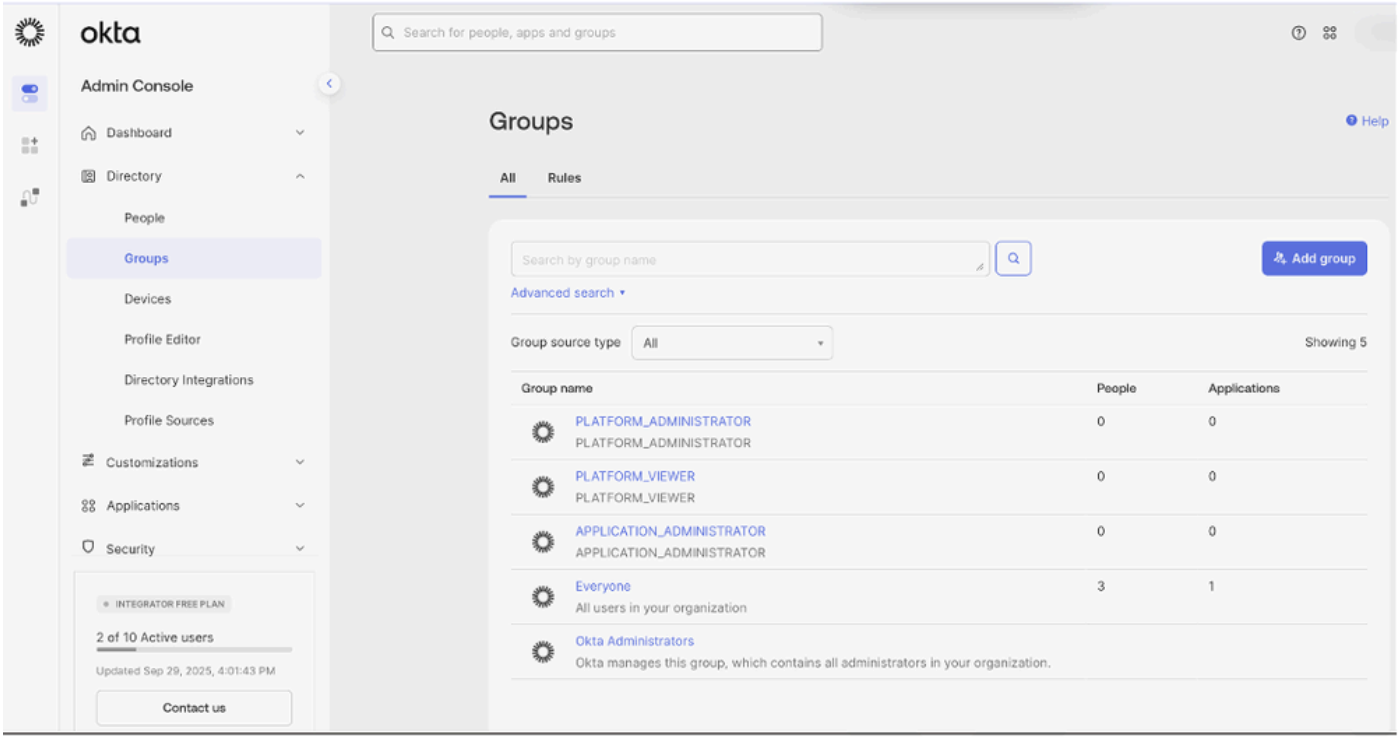
2. 選択したシステムロールのIDPロールを入力します。次のシステムロールがサポートされています。

- 一般アカウント管理者：一般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

- 一般アカウントビューア：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. 「アイデンティティプロバイダロールの追加」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

シングルログアウト構成(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

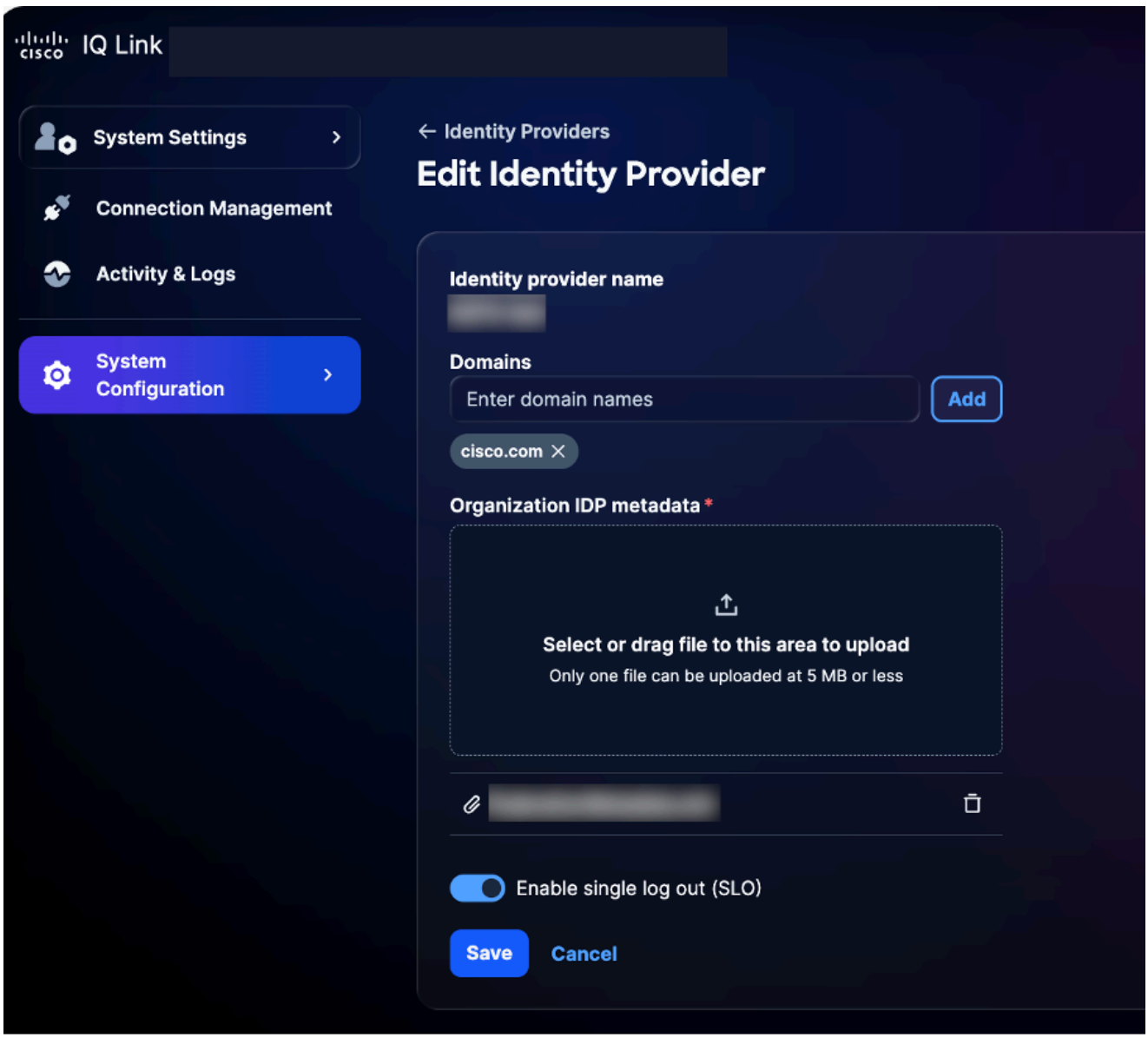
2. ダウンロードファイルをsp-public-key.crtとして保存します。

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：

- ローカルアカウント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。

表4：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(AD)フェデレーションサービス(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+
- AD統合の設定
- ADFSでのSSL/Transport Layer Security(TLS)証明書
- アカウント管理者によるCisco IQへのアクセス
- 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）

表5: 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	ADグループドメイン名(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. ステップ3の一部として保存されているファイルから詳細を取得するには、証明書利用者に関するデータをファイルからインポートするをクリックします。
10. BrowseをクリックしてSP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。

注: ADFSサーバーに登録済みのMulti-Factor Authentication (MFA)アダプター(たとえば、Azure MFAまたは*Time-Based One-Time Password (TOTP))がない場合、[MFAを持つすべてのユーザーを許可する]を選択しないでください。
このポリシーが、設定されたMFAプロバイダーなしで有効になっている場合、ADFSはユー

ザーを認証しますが、最終的にはステータス urn:oasis:names:tc:SAML:2.0:status:RequestDeniedの要求を拒否します。SAML応答にアサーションが含まれていないため、プラグインが失敗し、「Missing Email」エラーが報告されます。

問題:[MFAを持つすべてのユーザを許可する]が選択されている。

回避策:PowerShellで次のコマンドを実行して、現在のポリシーを確認します。

```
Get-AdfsRelyingPartyTrust -Name “

     ”).AccessControlPolicyName
```

「Permit everyone」（MFA要件なし）を設定するには、次のコマンドを実行します。

```
Set-AdfsRelyingPartyTrust -TargetName “

     ” -AccessControlPolicyName “Permit everyone”
```

PowerShellを使用して証明書利用者信頼を作成することもできます。

```
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
```

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。

表6：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
UPN	公開キーインフラストラクチャ(PKI)/証明書認証	ADFSは、ユーザプリンシパル名(UPN)を介してクライアント証明書をADユーザにマッピングします
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. ユーザー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
=> 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. 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

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

警告：各ADユーザアカウントにはメール属性を設定する必要があります。この属性が欠落している場合、SAMLアサーションには電子メール要求が含まれないため、認証が拒否されます。

ユーザーの電子メールアドレスを更新するには、次のPowerShellコマンドを実行します。

```
Set-ADUser -Identity “

     ” -EmailAddress “

      ”
```

ユーザグループの確認

1. ユーザ名を設定して、ユーザのグループメンバーシップを確認します。

```
$username = “testuser”
```

2. 次のコマンドを実行して、ユーザーのアカウントを検索します。

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

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

3. ユーザー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

- SP証明書が（自己署名ではなく）CAによって発行される場合は、発行側CA証明書をルート証明書ストアにインポートします。

```
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
```

PKI/証明書認証の設定

このセクションでは、パスワードと共に証明書ベース（スマートカードまたはソフトウェア証明書）の認証を追加する方法について説明します。パスワードのみの認証で十分な場合は、このセクションをスキップできます。

AD CS CAロールのインストール

AD証明書サービス(CS)CAロールをインストールするには、次の手順を実行します。

1. 次のコマンドを実行して、エンタープライズCAがドメインにすでに存在するかどうかを確認します。

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

コマンドが有効な応答を返した場合、このセクションの残りの部分は省略できます。環境はすでに設定されています。コマンドがCAが見つからないことを示す場合は、手順2に進みます。

2. 次のコマンドを実行して、CAロールをインストールします。

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

3. 次のコマンドを実行して、CAロールを設定します。

```
Install-AdcsCertificationAuthority `
    -CAType EnterpriseRootCA `
    -CACommonName “



     ” `
    -KeyLength 2048 `
    -HashAlgorithmName SHA256 `
    -CryptoProviderName “RSA#Microsoft Software Key Storage Provider” `
    -ValidityPeriod Years `
    -ValidityPeriodUnits 10 `
    -Force
```

4. 次のコマンドを実行してインストールします。

```
certutil -ca
```

5. 次のコマンドを実行して、サービスがアクティブで到達可能であることを確認します。

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

証明書テンプレートの設定

Client Authentication Enhanced Key Usage(EKU)を使用して証明書テンプレートを設定するには、次の手順を実行します。

1. certsrv.mscを開き、CAノードを展開します。
2. Certificate Templatesを右クリックし、Manageを選択します。

3. ユーザテンプレートを複製します。

注：組み込みユーザテンプレートは、そこから発行された証明書にクライアント認証EKUが含まれている場合にのみ機能するか有効です。

---

4. 次のタブで設定を構成します。

- General：有効期間を1年として、Nameフィールドに「CIQ User Authentication」と入力します。
- Request Handling: Purposeドロップダウンリストから Signature and encryptionを選択し、Allow private key to be exportedチェックボックスにチェックマークを入れます
- Subject Name:Build from Active Directory Informationを選択し、SubjectフィールドとSANフィールドの両方にEメールを入力します。

警告: SubjectフィールドとSANフィールドには、ユーザのUPNまたはADアカウントと一致する電子メールを入力する必要があります。ADFSは、これらのフィールドを使用して、証明書をADユーザにマッピングします。

- 拡張機能:アプリケーションポリシーに「Client Authentication (1.3.6.1.5.5.7.3.2)」が含まれていることを確認します。
- Security：ドメインユーザを追加し、ユーザにReadおよびEnroll権限を付与します。

5. 次のコマンドを使用してテンプレートを発行します。

```
Add-CATemplate -Name “CIQUserAuthentication” -Force
```

ユーザ証明書の登録

1. ターゲット・ユーザーとしてログインします。
2. 次のコマンドを実行して、証明書を登録します。

```
certreq -enroll -user “CIQUserAuthentication”
```

3. 次のコマンドを実行して、証明書のインストールを確認します。

```
Get-ChildItem Cert:| Where-Object {
    $_.EnhancedKeyUsageList.ObjectId -contains “1.3.6.1.5.5.7.3.2”
} | Format-Table Subject, Thumbprint, NotAfter -AutoSize
```

Windowsからのユーザ証明書のエクスポートとクライアントへのインストール(Mac)

WindowsからMacにユーザ証明書をエクスポートするには、次の手順を実行します。

1. 次のコマンドを実行して、Windowsから証明書をPFXファイルとしてエクスポートします。

```
$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. user-cert.pfxファイルをMacデバイスに転送します。

3. 次のコマンドを実行して、証明書をMacキーチェーンにインポートします。

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

     ”
```

注：証明書をインポートした後、認識されるためにはブラウザを閉じてから再度開く必要が

あります。

4. Mac上のCAを信頼するために、次のコマンドを実行します。

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

ADFS証明書認証エンドポイントの有効化

ADFS証明書認証エンドポイントを有効にするには、次の手順を実行します。

1. 次のコマンドを実行して、必要なADFS証明書エンドポイントを有効にします。

```
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. 次のコマンドを実行して、すべてのエンドポイントが有効になっていることを確認します。

```
Get-AdfsEndpoint | Where-Object { $_.AddressPath -like “*cert*” } |

Format-Table AddressPath, Enabled, Proxy -AutoSize
```

プライマリとしての証明書認証の有効化

プライマリとして証明書認証を有効にするには、次のコマンドを実行します。

1. 次のコマンドを使用して、イントラネットおよびエクストラネットアクセスのプライマリ認証プロバイダーを設定します。

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

2. 次のコマンドを使用して、両方のリストにCertificateAuthenticationとFormsAuthenticationが含まれていることを確認します。

```
(Get-AdfsGlobalAuthenticationPolicy).PrimaryIntranetAuthenticationProvider

(Get-AdfsGlobalAuthenticationPolicy).PrimaryExtranetAuthenticationProvider
```

3. 次のコマンドを使用して、現在のTLSクライアントポート設定を確認します。

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

4. TlsClientPortが49443定されていない場合は、次のコマンドを使用してポートを更新し、ADFSサービスを再起動します。

```
Set-AdfsProperties -TlsClientPort 49443

Restart-Service adfssrv
```

SChannel/TLSの修正（PKIに対して重要）

次のセクションの手順では、証明書認証の動作を妨げるCERT_E_UNTRUSTEDROOT(0x800B0109)エラーを解決します。

ポート49443でのSSL証明書のバインディング

ポート49443でSSL証明書をバインドするには、次の手順を実行します。

1. 次のコマンドを使用して、ポート49443の既存のSSL証明書バインドをすべて削除します。

```
netsh http delete sslcert hostnameport=

    :49443
```

2. 次のコマンドを使用して、クライアント証明書ネゴシエーションを有効にした新しいバインドを作成します。

```
netsh http add sslcert hostnameport=


     :49443 `
    certhash=


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

3. 次のコマンドを使用して、クライアント証明書ネゴシエーションが有効になっていることを確認します。

```
netsh http show sslcert hostnameport=


     :49443
```

証明書ストアのクリーンアップ (重要)

証明書ストアをクリーンアップするには、次の手順を実行します。

警告：自己署名証明書ではない証明書が信頼されたルートストアに存在する場合、Windowsチャネルはすべてのクライアント証明書を拒否します。これは、PKI障害の主な根本原因です。

---

1. 次のコマンドを実行して、信頼されたルートストア内の自己署名証明書ではない証明書を特定します。

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

2. 次のコマンドを実行して、これらの証明書を中間CAストアに移動します。

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

3. 次のコマンドを実行して、自己署名証明書ではない証明書がルートストアに残っていないことを確認します。

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

SChannelレジストリ修正(CRITICAL)

適切な証明書認証を確保するようにSChannelレジストリを設定するには、次のコマンドを実行します。

1. 次のコマンドを使用して、レジストリパス変数を定義します。

```
$regPath = “HKLM:”
```

2. 次のコマンドを使用して、次の表に定義されているレジストリ設定を適用します。

```
Set-ItemProperty -Path $regPath -Name “ClientAuthTrustMode” -Value 2 -Type DWord

Set-ItemProperty -Path $regPath -Name “SendTrustedIssuerList” -Value 0 -Type DWord
```

表7：チャネルレジストリの設定

設定値	値	目的
クライアント認証信頼モード	2	排他的CA信頼を有効にして、既定の検証パスを修正します。
SendTrustedIssuerList	0	TLSハンドシェイク中にサーバーが完全な信頼された発行者リストを送信しないようにします。

CA証明書ストアの確認

CA証明書ストアを確認するには、次の手順を実行します。

注：ユーザ証明書を発行するCA証明書が正しく認識されるためには、そのCA証明書がSystemCertificatesstoreに存在している必要があります。

1. 次のコマンドを使用して、CA証明書の拇印を定義します。

```
$caThumbprint = “

    ”
```

2. 次のコマンドを使用して、CA証明書がすでにLocalMachinestoreにあることを確認します。

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

証明書が見つからない場合は、LocalMachinestoreにインポートします。

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

ADFSサーバのリブート (必須)

次のコマンドを使用して、ADFSサーバを再起動します。

```
Restart-Computer -Force
```

注:ClientAuthTrustModeレジストリの変更は、サーバの再起動後にのみ有効になります。

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メタデータをエ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。

Cisco IQでの設定

Cisco IQでを設定するには、次の手順に従います。

1. adfs-metadata.xmlをワークステーションに転送します。
2. Cisco IQで、System Settings > System Configuration > Identity Providersの順に移動します。
3. ADFSメタデータファイルをアップロードして、IDP証明書、エンティティID、およびSSO

URLを自動的に抽出します。

4. 設定を保存します。

注:ADFSがトークン署名証明書の自動ロールオーバーを実行する場合、認証を続行するには、メタデータファイルを再エクスポートしてCisco IQにアップロードする必要があります。

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. Domain(s)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トグル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

役割マッピングの設定に進む前に、マッピングに使用するグループをADから検索できることを確認してください。AD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”] }
```

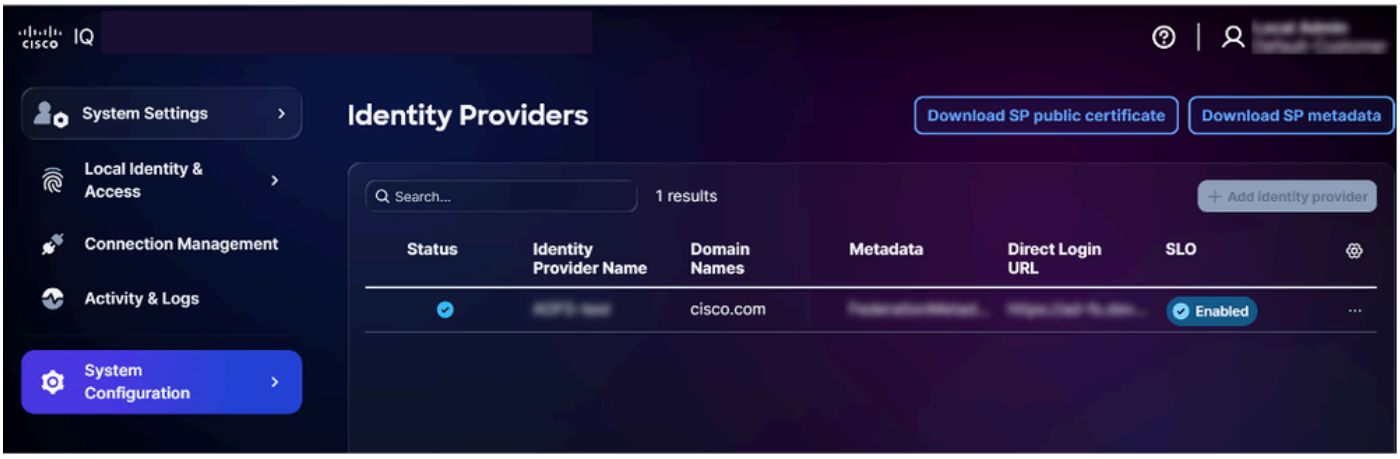
システムはLightweight Directory Access Protocol(LDAP)を介してADに直接クエリーを実行するため、追加のモジュールは必要ありません。グループ情報は、完全な識別名(DN)形式で返されます。次に例を示します。

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

Viewer,OU=Groups,DC=dev,DC=example,DC=com

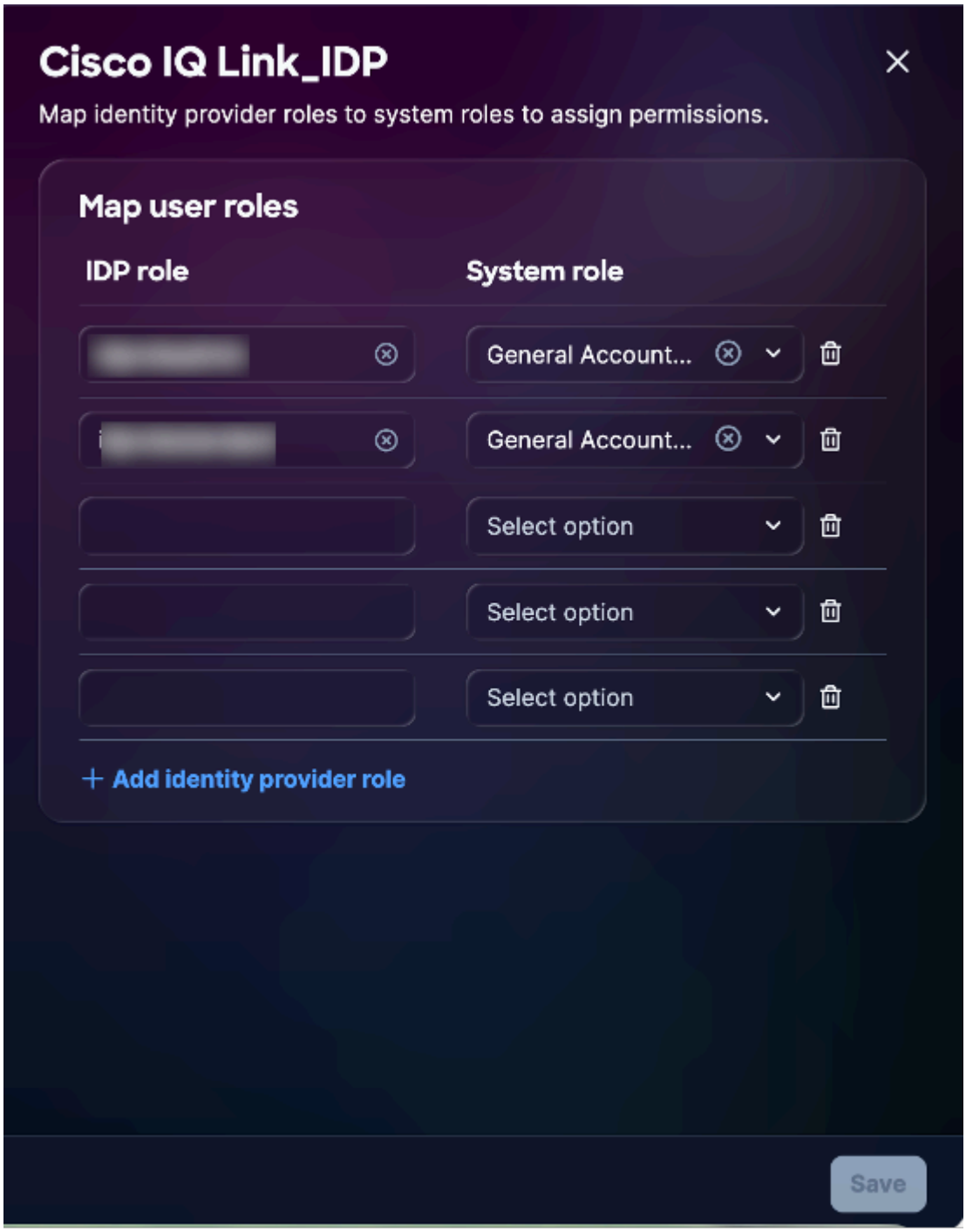
必要なグループがリストされていない場合は、ADFS役割のマッピングを完了する前に、アカウント管理者がADでグループを作成する必要があります。

役割マッピングを構成するには、次の手順に従います。



ロールのマッピング

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。

- 一般アカウント管理者：一般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権があります。IDPロール（解析名）はCXIQ Adminsです。
- 一般アカウントビューア：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。

チャネルクライアント証明書テスト

クライアント証明書を受け入れるようにSChannelが正しく構成されていることを確認するには、新しいPowerShellウィンドウを開き、次のコマンドを実行します。

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


     :49443/adfs/ls/”
```

正常な出力はHTTP応答（リダイレクトやADFSページなど）です。 TLSハンドシェイクエラーが発生した場合、接続は失敗しています。

PKIフローのエンドツーエンドブラウザテスト

PKIフローのエンドツーエンドブラウザテストを開始する前に、ユーザ証明書がmacOSキーチェーンにインストールされていることを確認します(詳細については、「証明書ベースの認証の設定」の「クライアントマシン(macOS)へのユーザ証明書のインポート」を参照してください)。

テスト方法：

1. アプリケーションのSAMLログインURLに移動します。ADFSは証明書とパスワードのオプションを提供します。
2. Certificate Authenticationを選択します。ブラウザに証明書の入力を求めるプロンプトが表示されます。
3. 証明書をアップロードします。ADFSはユーザを認証し、SAML応答で要求をリダイレクトし、新しいセッションを確立します。

パスワードフローに関するエンドツーエンドのブラウザテスト

パスワードフローのエンドツーエンドブラウザテストを開始する前に、次の手順を実行します。

1. アプリケーションのSAMLログインURLに移動します。ADFSは証明書とパスワードのオプションを提供します。
2. Password/Forms Authenticationを選択します。
3. ユーザ名を入力します。
4. パスワードを入力します。
5. ログインが成功したことを確認します。

注：両方のフローが同時に動作する必要があります。

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。

表8: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	• 要求ルールが見つかりません: ADFS要求ルール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/cla ims/Groupである必要があります • ユーザーがADグループに含まれていません
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の不一致：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
```

SSO用のMicrosoft Entry ID SAML設定

このセクションでは、Microsoft Entra ID(Entra ID)をCisco IQのSAML IDPとして設定し、パスワードベースの認証とPKI/証明書ベースの認証(CBA)の両方をサポートする方法について説明します。

SSOのエントリID SAMLを設定するための前提条件

- Microsoft Entra IDテナント（例：「ciqtestdev.onmicrosoft.com」）
- Cisco IQへのグローバル管理者またはアプリケーション管理者ロールのアクセス

- Entra ID（クラウド）とCisco IQ間の接続
- エンタープライズCAがインストールされているか、到達可能である（PKIのみに必要）
- インターネットから到達可能な証明書失効リスト(CRL)配布ポイント（PKIだけに必要）

表9:Enter IDサーバの設定

項目	説明	例
テナントID	IDテナントIDの入力	37352d8f-0ebe-4762-8161-8775ffe897cb
Cisco IQ FQDN（オプション）	配置ホスト名	<YOUR-CIQ-FQDN>
IDPエンティティID	ID発行者のURLを入力	https://sts.windows.net/<テナントID>/
IDP SSOのURL	SAMLログインエンドポイント	https://login.microsoftonline.com/<テナントID>/saml2
会社のドメイン	ユーザの電子メールドメイン	<お客様のドメイン>

エントリID SAMLアプリケーションの設定

エンタープライズアプリケーションの作成

1. Microsoft Entra管理センターにサインインします。
2. Identity > Applications > Enterprise applicationsの順に移動します。
3. New application > Create your own applicationの順にクリックします。
4. 名前を入力します（「Cisco IQ」など）。
5. Integrate any other application you don't find in the gallery (Non-gallery)を選択します。
6. [Create] をクリックします。

SAMLシングルサインオンの設定

SAMLシングルサインオンを設定するには、SPメタデータファイルをアップロードする必要があります。仮想アプライアンス(VA)から次の手順を実行して、これを取得できます。

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 metadataをクリックしてダウンロードします。このダウンロードされたSPメタデータファイルは、SAMLシングルサインオンの設定を完了するためにアップロードされます。

3. Upload Metadata fileボタンをクリックして、SPメタデータファイルをアップロードします。アップロードが成功すると、SPメタデータファイルのデータがSAMLベースのシングルサインオン画面に自動入力されます。

これらの詳細を手動で入力して、シングルサインオンの設定を構成することもできます。
SAMLシングルサインオンを手動で設定するには、次の手順を実行します。

1. エンタープライズアプリケーションで、シングルサインオンに移動し、SAMLを選択します。

2. Basic SAML Configurationセクションで、Editをクリックし、次のように入力します。

   a. 識別子（エンティティID）:<YOUR-CIQ-FQDN>

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

   c. サインオンURL:https://<YOUR-CIQ-FQDN>/saml/login

   d. ログアウトURL:https://<YOUR-CIQ-FQDN>/saml/logout

3. [Save] をクリックします。

注：エンティティIDは、Cisco IQがSPエンティティIDとして使用するIDと正確に一致している必要があります。これは通常、展開のFQDNです。

---

4. SAML属性および要求を構成するには、[属性および要求]セクションで[編集]をクリックします

。

5. 次の要求を構成します。

表10：必須のSAML要求

請求	ソース属性	名前空間
一意のユーザー識別子(NameID)	ユーザー.userprincipalname	（デフォルト）
電子メールアドレス	ユーザー。メール	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
givenname	ユーザー.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
姓	ユーザ。姓	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
name	ユーザー.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims
[グループ（groups）]	ユーザー。タスクの対象となるユーザー	（EMPTY – 名前空間をクリアします）

注:groups要求の場合：
– ソースとしてuser.assignedrolesを使用します。 ユーザー。グループ
- Namespaceフィールドは空でなければなりません。これにより、SAMLアサーションの属性名が完全なUniform Resource Identifier(URI)ではなく単なるグループになります
- user.groupsに重複するグループ要求を追加しないでください。追加すると、競合が発生します

アプリケーションロールの設定

アプリケーションロールは、アプリケーション登録（エンタープライズアプリケーションではない）で設定します。アプリケーションロールを設定するには、次の手順を実行します。

1. Identity > Applications > App registrationsの順に移動します。
2. アプリケーションを検索して選択します。
3. App roles > Create app roleの順に選択します。
4. 必要なロールごとに、次の項目を設定します。

- 表示名：例：Cisco IQ Admins
- 許可されるメンバーの種類：ユーザー/グループ
- 値：例：Cisco IQ Admins
- 説明：例：Cisco IQ Administrators

5. Applyをクリックします。

注:Cisco IQロールマッピング要件に一致するロールを作成します（例：CXIQ Admins、CXIQ Developers、CXIQ Viewer）。

次の理由により、グループ要求の代わりにアプリケーションロールが使用されます。

- クラウド専用テナントは、P1またはP2ライセンスなしではグループ表示名を送信できません
- sAMAccountNameは、オンプレミスADから同期されたグループに対してのみ機能します
- グループIDソースは、マッピングが困難なユニバーサル一意識別子(UUID)を送信します
- アプリケーションロールは、Cisco IQロールの期待に一致する正確な文字列値を送信します

アプリケーションロールへのユーザの割り当て

ユーザをアプリケーションロールに割り当てるには、次の手順に従います。

1. Enterprise Application > Users and groupsの順に戻ります。
2. Add user/groupをクリックします。
3. ユーザを選択し、適切なアプリケーションロールを割り当てます。
4. Assignをクリックする。ロール値は、読み取り可能な文字列としてSAMLアサーショングループ属性に表示されます。

IDPメタデータおよび証明書のダウンロード

IDPメタデータと証明書をダウンロードするには、次の手順に従います。

1. エンタープライズアプリケーションから、シングルサインオン > SAML署名証明書セクションに移動します。
2. フェデレーションメタデータXMLをダウンロードします（entra-id-metadata.xmlとして保存）。

   または

   証明書のダウンロード(Base64)（手動入力用）
3. 「設定」セクションの次の値をメモしておきます。

- ログインURL(IDP SSO URL)
- Azure AD識別子（IDPエンティティID）
- ログアウトURL(IDP SLO URL)

注：エントリIDは署名証明書を定期的にローテーションするため、アクティブな証明書が変更されるたびに、SSOサービスが中断されないようにメタデータを再ダウンロードしてVAにアップロードする必要があります。

エントリID IDPの追加

注:SAMLのAPISIXルートは、IDPがCisco IQに追加されると自動的に作成されるため、手動でルートを設定する必要はありません。

エントリID IDPを追加するには、次の手順に従います。

1. アカウント管理者としてVAにログインします。
2. System Settings > System Configuration > Identity Providersの順に移動します。
3. Add identity providerをクリックします。
4. IDPの名前を入力します（たとえば、「Entra ID」）。
5. ドメインを入力します（例：「ciqtestdev.onmicrosoft.com」、社内ドメイン）。
6. （オプション）必要に応じて、Enable single logoutトグルボタンをオンにします。
7. Upload IDP MetadataフィールドのEntra IDから取得したentra-id-metadata.xmlファイルをドラッグアンドドロップするか、アップロードします。
8. [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」のままです。これは正常な動作です。

ロールマッピングの設定

ロールマッピングを設定するには、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。
2. 各システムロールの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。

表11：システムロール

システムロール	IDPロール（アプリケーションロール値）	説明
一般的なアカウント管理者	CXIQ管理者	すべてのアクションに対するフルアクセス許可
一般アカウントビューアー	CXIQ開発者	読み取り専用アクセス
一般アカウントビューアー	CXIQビューア	読み取り専用アクセス

注：アプリケーションロール値の文字列は、Entra IDで設定したとおりに使用してください(詳細については、「Entra ID SAMLアプリケーションの設定」の「アプリケーションロールの設定」を参照してください)。

3. Saveをクリックします。ステータスがSuccessに更新されます。

SAMLフローの確認（パスワード認証）

SAMLフローを確認するには、次の手順を実行します。

1. ブラウザをIncognitoモードまたはプライベートモードで開きます。
2. https://<YOUR-CIQ-FQDN>/saml/loginに移動します。
3. Microsoftログインページにリダイレクトされることを確認します。
4. クレデンシャル（および設定されている場合はMFA）で認証します。
5. 認証後、/saml/acsに再びリダイレクトされ、Cisco IQアプリケーションが表示されることを確認します。
6. 次のコマンドを実行して、グループ抽出を確認します。

```
kubectl -ncxue logs deployment/apisix –since=5m | grep -E “authentication successful|Extracted group|To
```

予想される出力

```
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
```

証明書ベース認証の設定

このセクションでは、パスワードとともにCBAを追加する方法について説明します。パスワードのみの認証で十分な場合は、このセクションをスキップできます。

CBAの前提条件

- エンタープライズCAが構成されたAD証明書サービス(CS)（例：「DEV-ADCS-CA」）がインストールされたWindows Server
- CAサーバでのPowerShell管理者アクセス
- 証明書UPNはエントリID userPrincipalNameと一致する必要があります。
- インターネットからCRL配布ポイントにアクセスできる必要があります

AD CSでの証明書テンプレートの作成

1. CAサーバでcerttmpl.mscを開きます。
2. ユーザテンプレートを複製し、「EntraUserCert」という名前を付けます。
3. テンプレートを設定します。

- 一般：表示名EntraUserCert、有効期間1 ~ 2年
- 要求処理：目的=署名と暗号化
- サブジェクト名:要求内の供給を選択します
- 拡張：アプリケーションポリシーにクライアント認証(1.3.6.1.5.5.7.3.2)を含める必要があります
- Security：認証されたユーザにGrant ReadおよびEnroll権限

4. 次のコマンドを使用してテンプレートを発行します。

```
Add-CATemplate -Name “EntraUserCert” -Force
```

ユーザ証明書の要求と発行

1. 次のPowerShellスクリプトを使用して、証明書構成(INF)ファイル(たとえば、C:-cert.inf)を作成します。

```
@”
[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. <USER-UPN>を自分のEntra ID UPN(user@ciqtestdev.onmicrosoft.comなど)に置き換えます。

3. 証明書を生成するには、次のコマンドを実行します。

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

4. CAに要求を送信するには、次のコマンドを実行します。

```
certreq -submit -config “

     \CA-NAME>” C:-cert.csr C:-cert.cer
```

5. CAに証明書をインストールするには、次のコマンドを実行します。

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

証明書のエクスポート

- ユーザ証明書をPFXファイル（クライアント用）としてエクスポートするには、次のスクリプトを実行します。

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

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

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

- CAルート証明書（Entra ID用）をエクスポートするには、次のスクリプトを実行します。

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

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

クライアントマシン(macOS)でのユーザ証明書のインポート

- ユーザ証明書(PFX)をインポートするには、次のコマンドを実行します。

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

    "
```

- CAルート証明書をインポートするには、次のコマンドを実行します。

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

- CA証明書をキーチェーンアクセスで常に信頼するように設定するには、次の手順を実行します。
    1. キーチェーンアクセスを開きます。
    2. CA証明書を見つけ、Get Infoをクリックします。
    3. Trustで、Always Trustに設定します。

注：インポート後、ブラウザを終了して再度開くと、証明書が認識されます。

CAルート証明書のエントリIDへのアップロード

1. Microsoft Entra管理センターにサインインします。
2. Protection > Security > Certificate authoritiesの順に移動します。
3. Uploadをクリックして、ca-root.cerファイルを選択します。

4. それをルートCA証明書としてマークします。
5. CRL配布ポイントのURLを入力します（パブリックに到達可能である必要があります）。

Entra ID認証方式でのCBAのイネーブル化

1. Protection > Authentication methods > Policiesの順に移動します。
2. Certificate-based authenticationをクリックして設定します。
3. CBAを有効にし、ターゲットユーザまたはグループを追加します。
4. Configureで、保護レベルをSingle-factor authenticationに設定します。

ユーザ名バインディングの設定

CBA設定で、Username bindingタブに移動し、次のバインディングを設定します。

- 証明書フィールド：PrincipalName
- ユーザ属性:userPrincipalName

これにより、証明書のSubject Alternative NameのUPNがEntra IDユーザにマッピングされます。

CBAフローの確認

1. ブラウザをIncognitoモードまたはプライベートモードで開きます。
2. https://<YOUR-CIQ-FQDN>/saml/loginに移動します。
3. Microsoftログインページで、ユーザの電子メールを入力し、Nextをクリックします。
4. Use a certificate or smart cardを選択します（または自動プロンプトが表示される場合があります）。
5. ブラウザに証明書の選択を求めるプロンプトが表示されたら、適切なユーザ証明書を選択します。
6. Entra IDが証明書を検証し、SAML応答でリダイレクトして、セッションを作成することを確認します。

注：正しいクライアント証明書を選択していることを確認してください。誤った証明書（別

のユーザの証明書や期限切れの証明書など）を選択すると、認証が失敗します。

エントリIDの問題のトラブルシューティング

Entra ID SAMLの設定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可能なソリューションの概要を次に示します。

表12：トラブルシューティング

お問い合わせ内容	原因	修正
無効なSAML応答 – 電子メールがありません	SAMLアサーションにNameIDまたは電子メール属性がありません	Entra ID要求の設定を確認します(詳細については、「Entra ID SAMLアプリケーションの設定」の「SAMLシングルサインオンの設定」を参照してください)。 ユーザにメール属性が設定されていることを確認します。
抽出されたグループの合計：0	グループ要求が構成されていないか、ソースが正しくありません	ソースとしてuser.assignedrolesを使用します。ユーザがアプリケーションロールに割り当てられていることを確認します(詳細については、「エントリID SAMLアプリケーションの設定」の「アプリケーションロールへのユーザの割り当て」を参照してください)。
重複するグループ要求	user.groupsとuser.assignedrolesの両方がアクティブ	user.groups要求を削除します。user.assignedrolesのみを保持します。
UUIDとして表示されるグループ	ソース属性は「グループID」です。	アプリケーションロールの方法を使用します(詳細については、「エントリID SAMLアプリケーションの設定」の「アプリケーションロールの設定」を参照)。
属性名が長いURIを示しています	名前空間フィールドが空ではありません	グループ要求の設定のNamespaceフィールドをクリアします。
無効なSAML署名	IdP証明書がローテーションされているか、不一致です	Entra IDからメタデータを再ダウンロードし、Cisco IQに再アップロードします。
AADSTS500191	インターネットからCRLに到達できない	一般にアクセス可能なURLにCRLを発行するか、自己署名CA方式を使用します(詳細については、『ラボ環境におけるCRLの回避策』を参照してください)。
証明書は要求されません	証明書がキーチェーンにない、CAがクライアントで信頼されていない、またはCBAが有効になっていない	ユーザ証明書がmacOSキーチェーンアクセスでインポートされていること(詳細については、「証明書ベース認証の設定」の「クライアントマシン(macOS)でのユーザ証明書のインポート」を参照)、Entra IDで

お問い合わせ内容	原因	修正
		CBAが有効になっていること(詳細については、「証明書ベース認証の設定」の「Entra ID認証方式でのCBAの有効化」を参照)を確認し、変更を適用するためにChromeを再起動します。
SAMLアサーションの期限切れ	システム間のクロックスキュー	プラグイン設定でclock_skew_secondsを増やします(デフォルトは300。ラボでは30000を使用)。
VAのステータスが「Incomplete」	ロールマッピングはまだ構成されていません	ロールマッピングを実行します(詳細については、『ロールマッピングの設定』を参照してください)。

到達可能性の問題に対するCRLの回避策

CAのCRL分散ポイントがインターネットから到達可能でない場合（ラボのセットアップでは一般的）、CRL要件のない自己署名CAを使用します。

```
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=



       ”
)
```

ルートCA証明書のみをEntra IDにアップロードします。CDPなしで自己署名されているため、Entra IDはCRL検証を試行しません。

設定チェックリストの完了

このセクションでは、Microsoft Entra ID SAMLアプリケーションとオプションのCBAを使用してVAを設定するための完全なセットアップチェックリストについて説明します。

IDの入力SAMLアプリケーションの設定

- エントリIDにエンタープライズアプリケーション（非ギャラリー）を作成
- SPメタデータを手動で入力して基本的なSAML構成を構成する
- 属性と要求の設定（user.assignedrolesを使用した電子メール、名前、グループなど）
- アプリケーション登録でのアプリケーションロールの作成
- アプリケーションロールへのユーザの割り当て
- フェデレーションメタデータXMLのダウンロード

Cisco IQの設定

- Entra IDメタデータをアップロードして、Cisco IQにアイデンティティプロバイダーを追加
- アプリケーションロール値をCisco IQシステムロールにマッピングするためのロールマッピングの設定
- パスワードベースのログインがエンドツーエンドで機能することを確認します。
- ログでグループが正しく抽出されたことを確認します。

証明書ベースの認証（オプション）

- クライアント認証EKUを使用したAD CSでの証明書テンプレートの作成

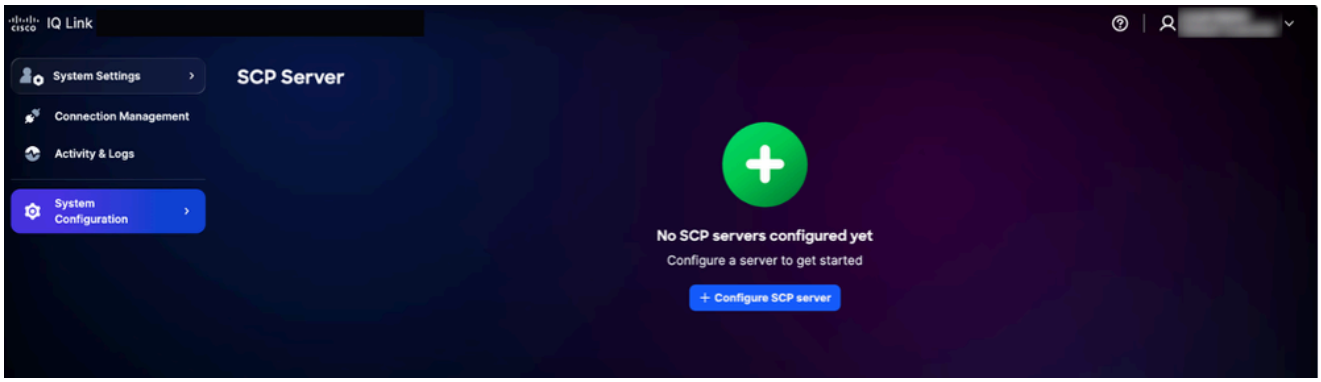
- Entra IDユーザに一致するUPNを使用してユーザ証明書を発行する
- ユーザ証明書をPFXとしてエクスポートし、クライアントマシンにインストール
- クライアントマシン上のCA証明書を信頼する
- Protection > Certificate authoritiesで、CAルート証明書をEntra IDにアップロードします。
- 認証方法でCBAを有効にする
- ユーザ名バインディングの設定(PrincipalNameおよびuserPrincipalName)
- CBAログインがエンドツーエンドで動作することを確認します。

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、またはパッチ適用に不可欠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。

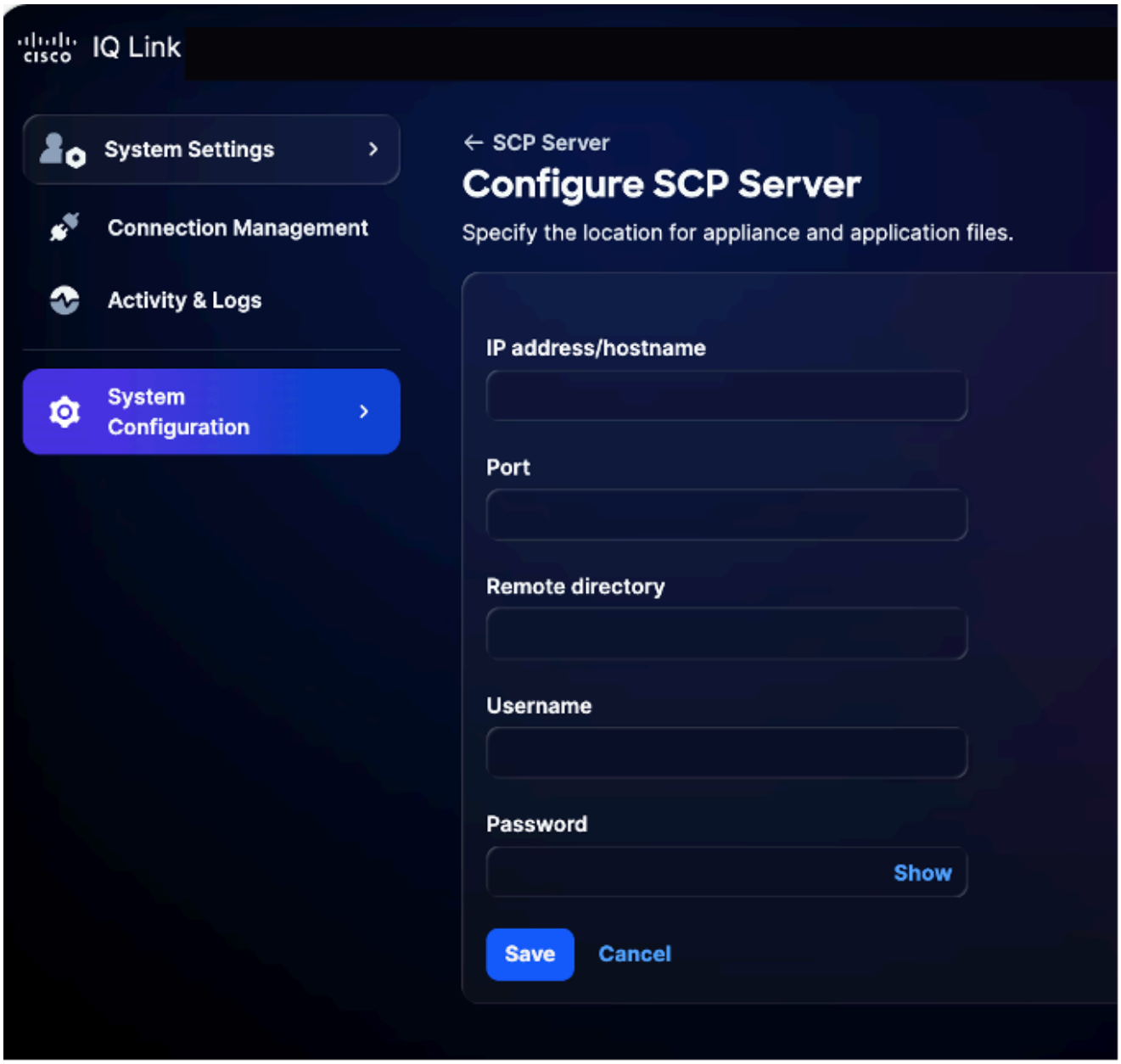
SCPサーバを追加するには

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。

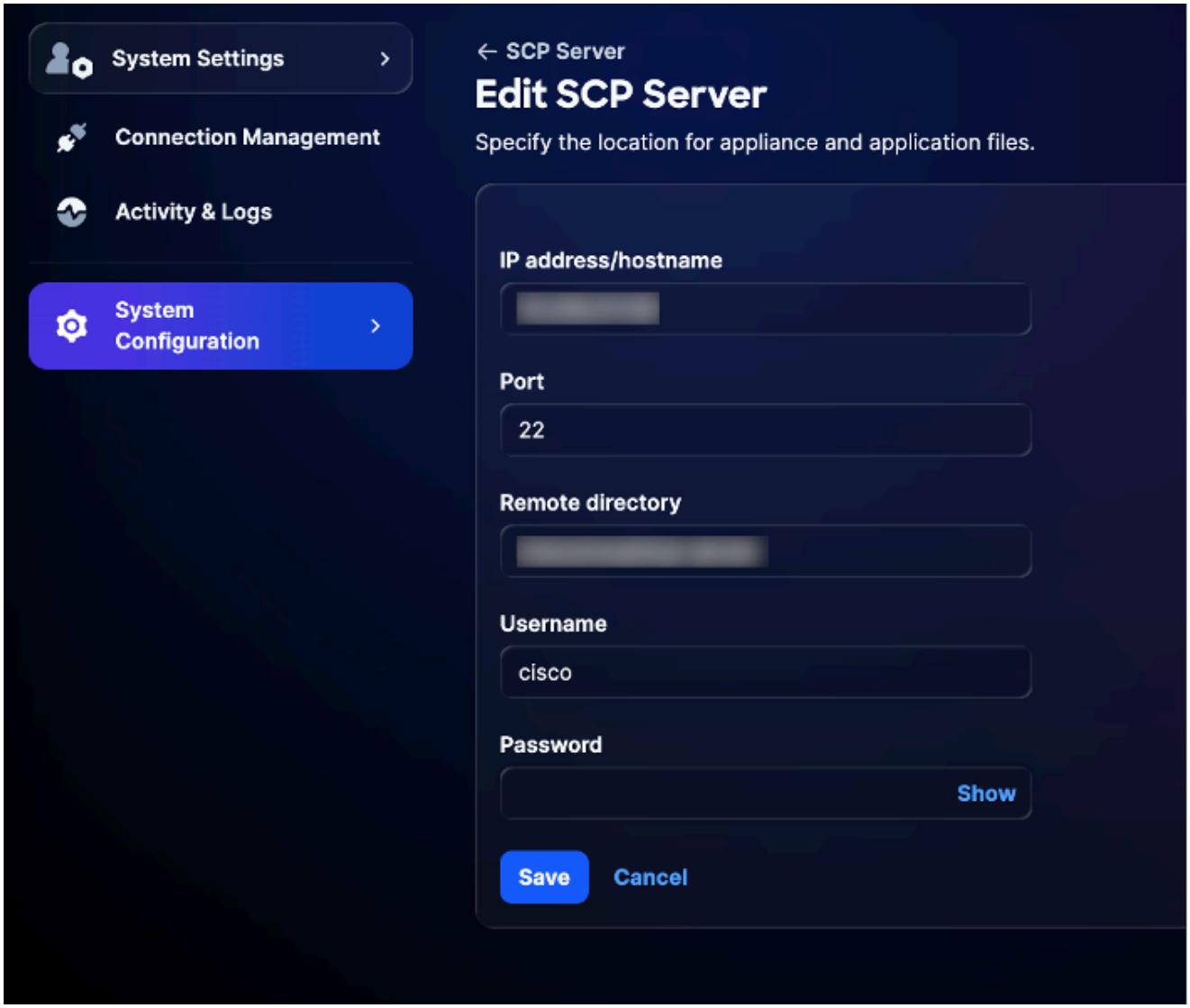
既存のSCPサーバの編集

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。

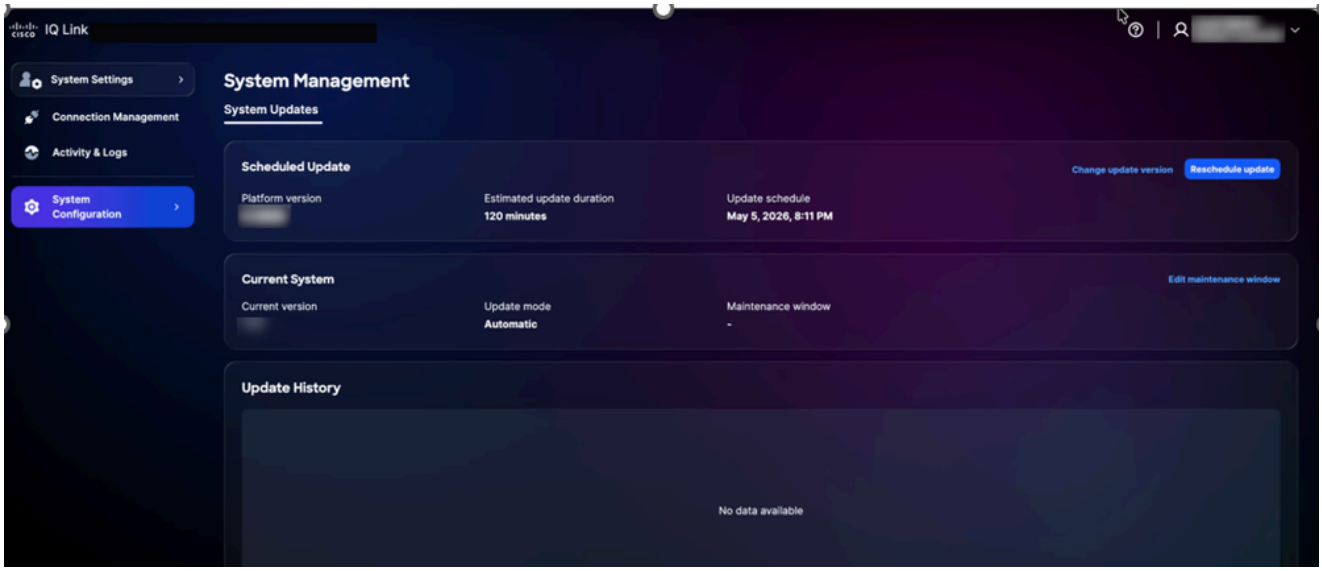
システム管理

UIを使用して最新のCisco IQ Linkバージョン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。

システム更新の再スケジュール

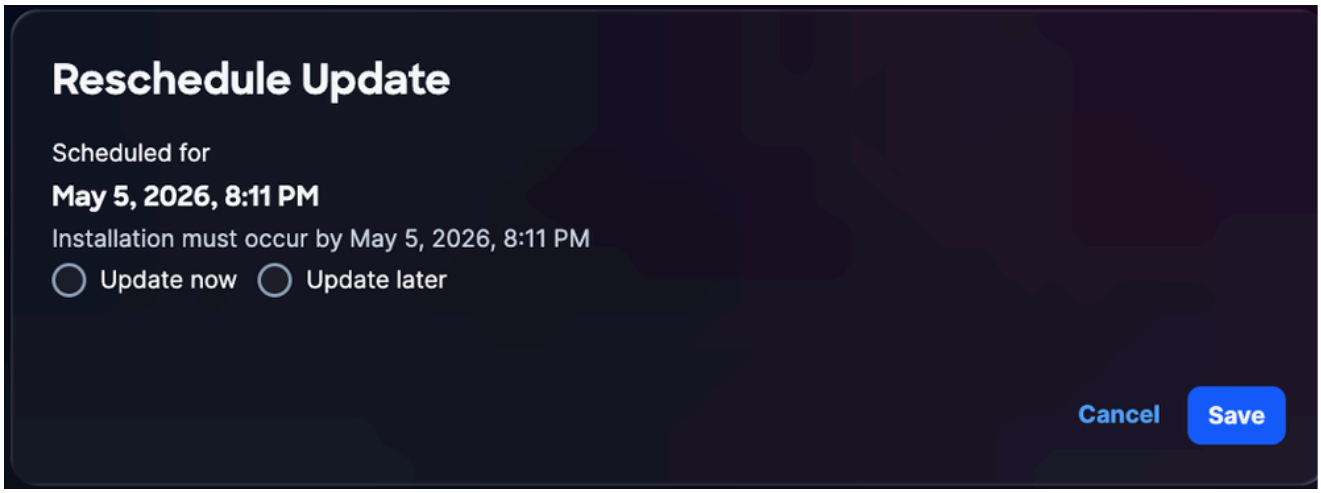
システム更新を再計画する手順は、次のとおりです。

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

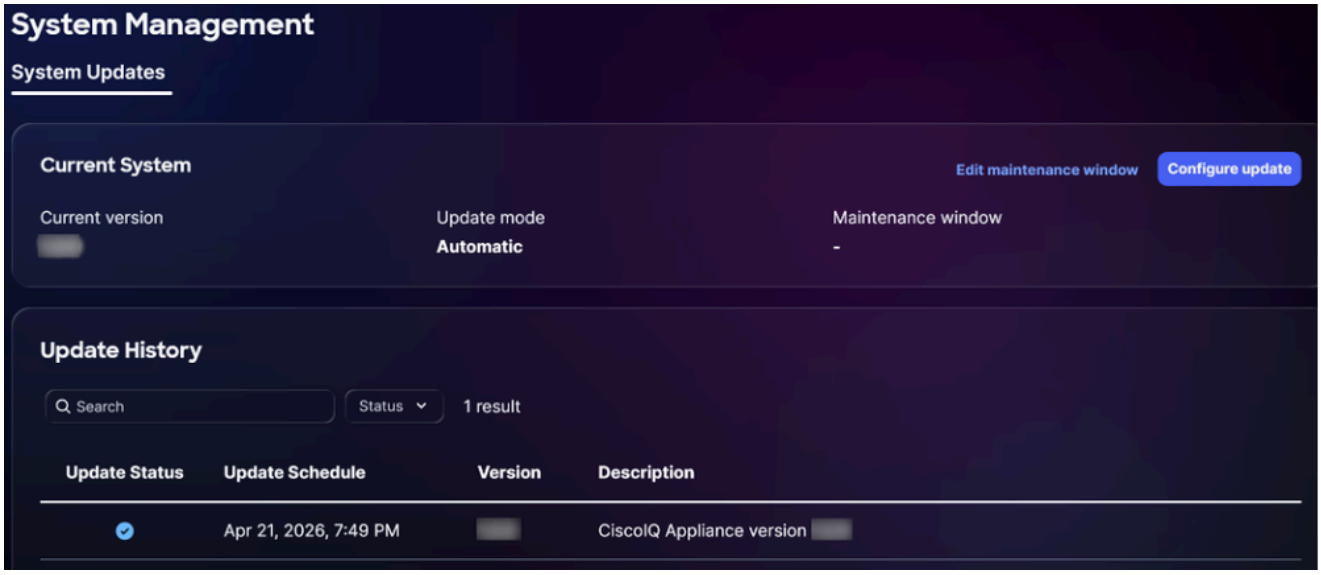
2. Reschedule updateをクリックします。



アップグレードの再スケジュール

3. 即時に再計画する場合は「今すぐ更新」ラジオ・ボタンを、別の日時をスケジュールする場合は「後で更新」ラジオ・ボタンを選択します。

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。

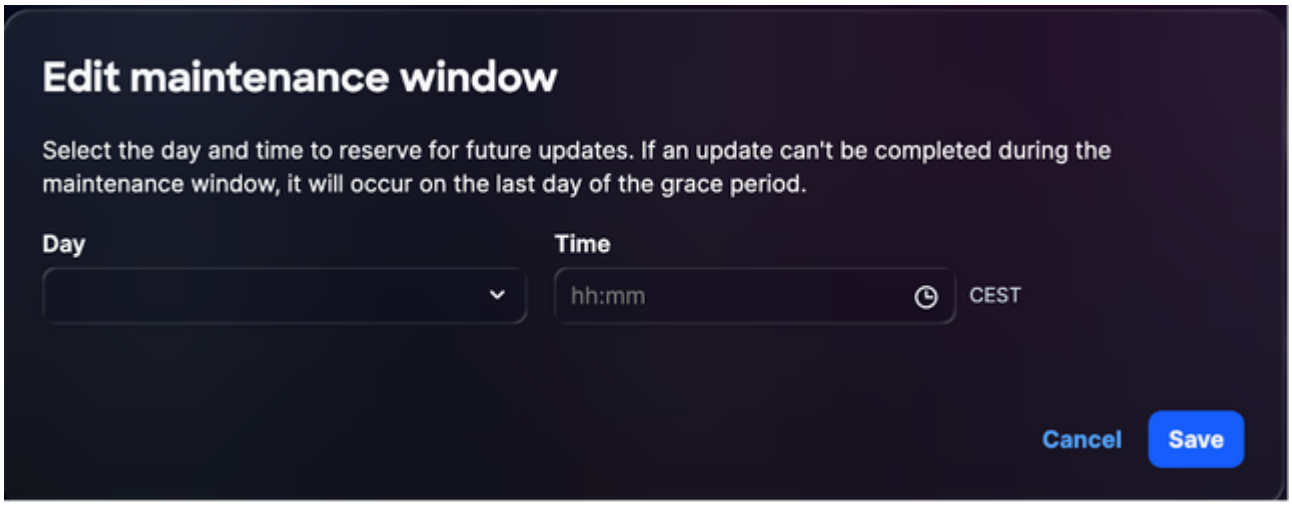


正常なアップグレード

システムアップグレードスケジュールの編集

システムアップグレードのカスタムスケジュールを作成できます。カスタムスケジュールが設定されている場合、アップグレードは最大の猶予期間内であれば、ユーザ定義の日付に実行されます。システムアップグレードスケジュールを作成するには、次の手順を実行します。

1. System ManagementページのCurrent Systemセクションで、Edit maintenance windowをクリックします。



メンテナンスウィンドウの編集

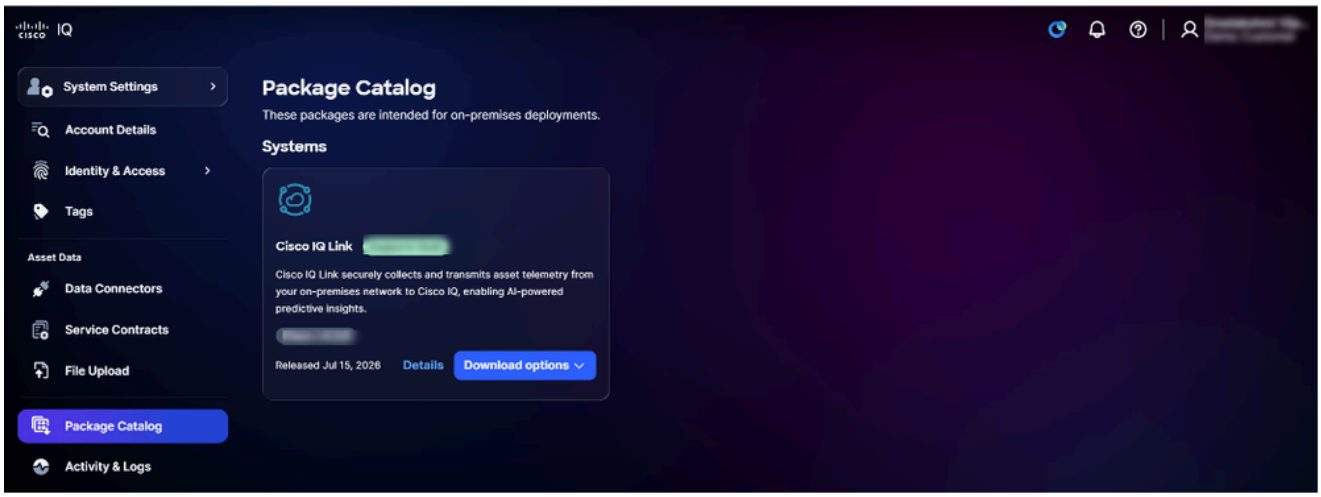
2. DayおよびTimeドロップダウンリストからオプションを選択します。
3. [Save] をクリックします。 メンテナンスウィンドウが正常にスケジュールされました。表示されたスケジュールに従って更新がトリガーされます。

注：
– アップグレードスケジュールが設定されていない場合、システムはデフォルトで、リブートなしのアップグレードでは2週間、リブートを必要とするアップグレードでは4週間の猶予期間を設定します。これらの猶予期間後は、更新を手動で実行する必要があります。
– アップグレードに失敗した場合、システムは最大2回の自動再試行を実行します。3回目の試行がスケジュールされますが、手動で開始する必要があります。

システムの手動アップグレード

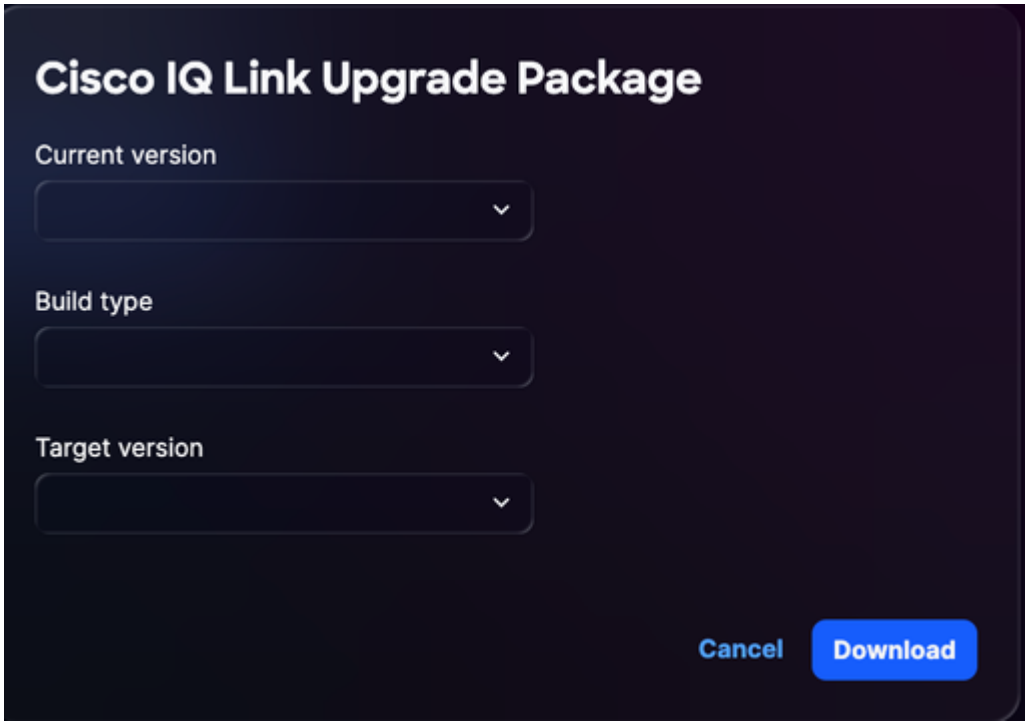
Cisco IQ SaaSからの自動配信が利用できないか、遅延しているシナリオでは、Cisco IQ SaaSからアップグレードバンドルを直接ダウンロードして、システムアップグレードを手動で実行できます。システムを手動でアップグレードするには、次の手順を実行します。

1. Cisco IQ SaaSにログインし、Home > System Settings > Package Catalogの順に選択します。



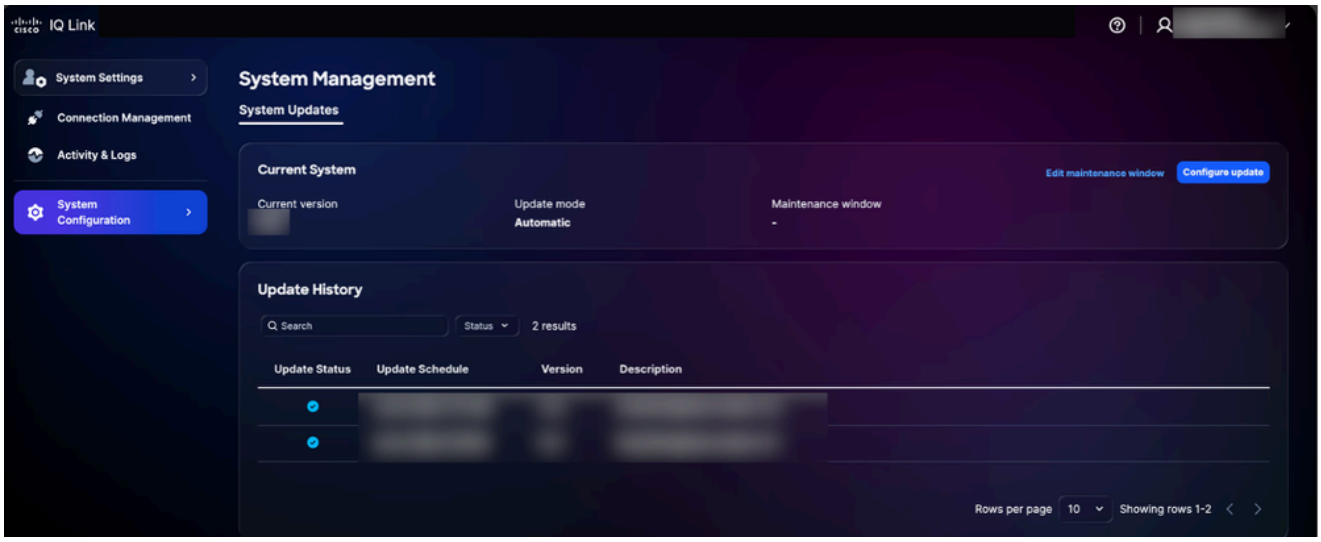
パッケージカタログ

2. Cisco IQ Linkセクションで、Download options > Upgrade packagesの順にクリックします。



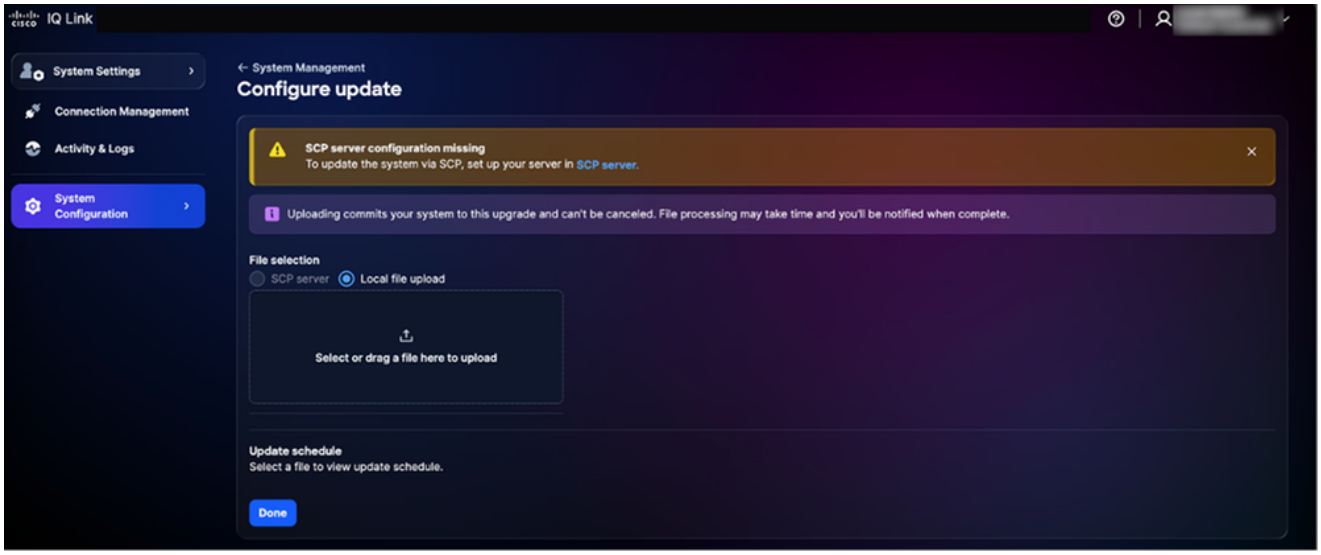
アップグレードパッケージ

3. ドロップダウンリストから現在のバージョンを選択します。
4. ドロップダウンリストから構築タイプを選択します。
5. ドロップダウンリストからターゲットバージョンを選択します。
6. [Download] をクリックします。アップグレードバンドルのダウンロード。
7. Cisco IQ Linkに移動します。
8. System Settingsで、System Configuration > System Managementの順に選択します。



更新の構成

9. Configure updateをクリックします。



ローカルファイルのアップロード

10. Local file uploadオプションボタンをクリックします。
11. ダウンロードしたアップグレードバンドルファイルを選択するか、アップロードフィールドにドラッグします。
12. [Done] をクリックします。システムが正常に更新されると、確認メッセージが表示されます。

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、カスタムSSL証明書をアップロードすることもできます。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。

デフォルトのSSL証明書は編集または削除できません。

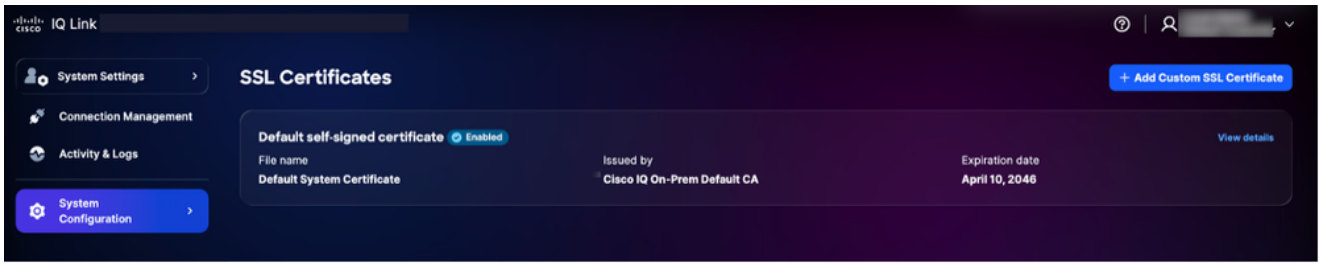
注：証明書の有効期間は90日以上残っている必要があります。証明書の有効期限が切れるまでの残り日数が90日を下回ると、証明書は「期限切れ間近」と見なされます。

SSL証明書を追加、編集、または削除したら、「Okta IDPまたはADFS IDPの単一ログアウト設定」の説明に従って新しいSSL証明書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。

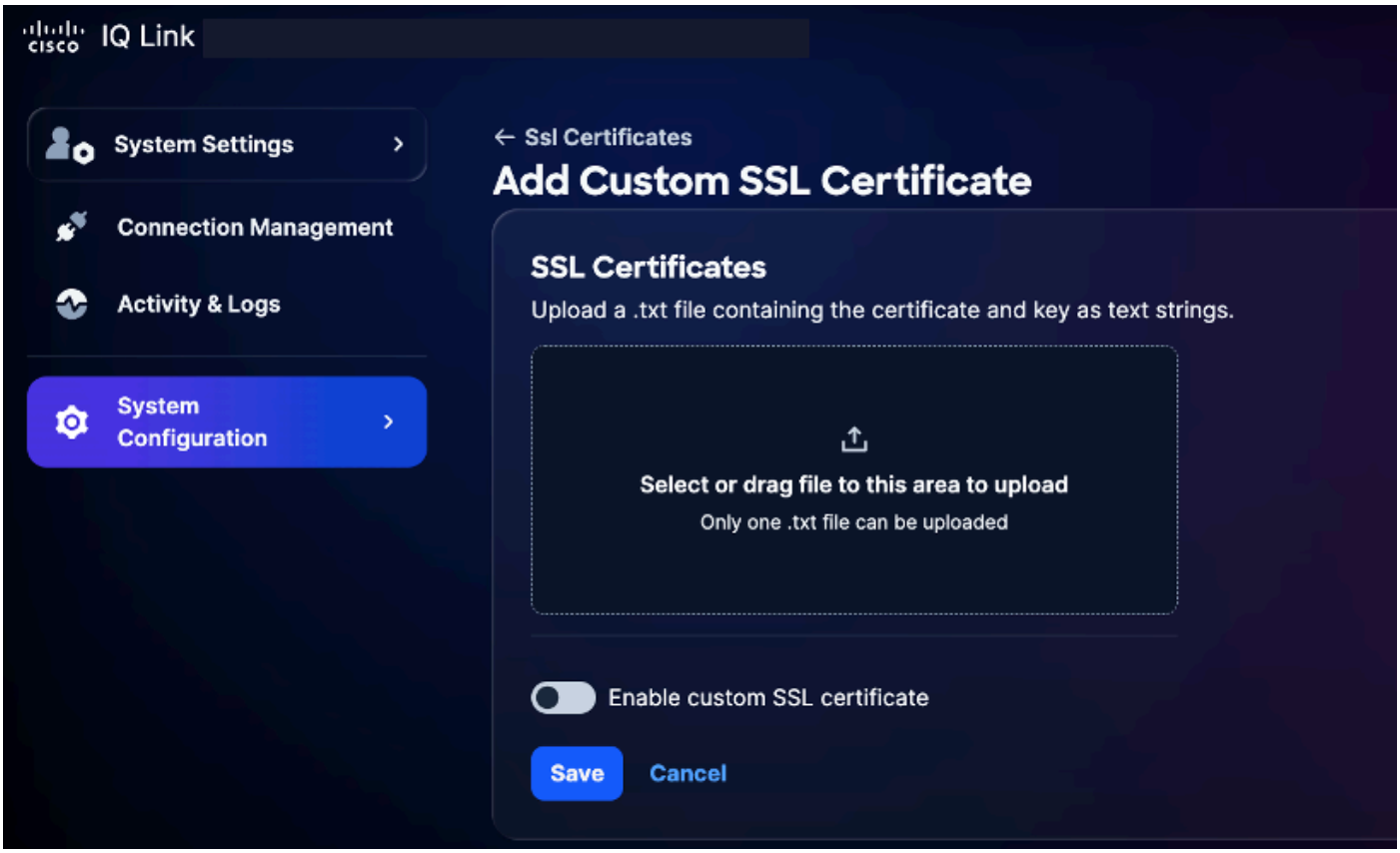
1. System Settingsで、System Configuration > SSL Certificatesの順に選択します。SSL Certificatesページが表示され、システムのすべてのSSL証明書がリストされます。



SSL証明書の追加

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

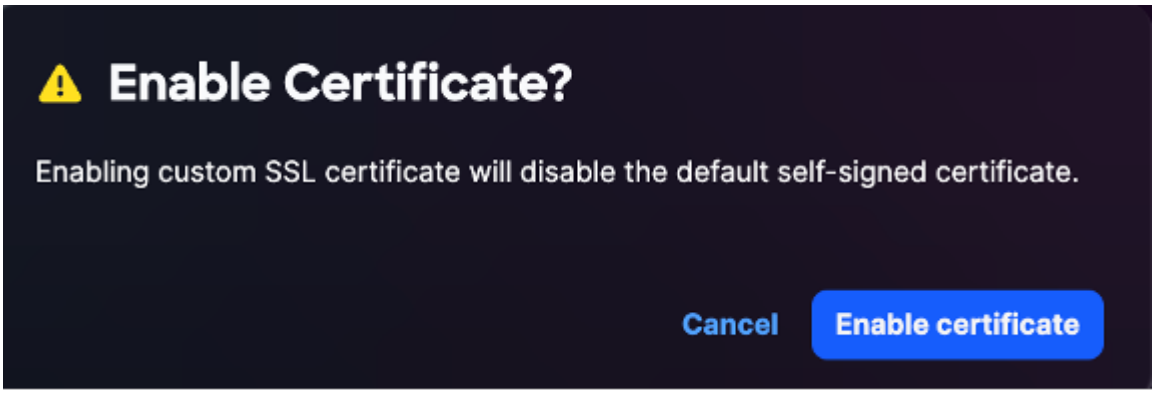
注：
- Privacy-Enhanced Mail(PEM)でエンコードされた証明書とキーの両方をテキスト文字列として含む.txtファイルをアップロードします。
– 一度にアップロードできる.txtファイルは1つだけです
– ファイルには、証明書と秘密キーの両方が含まれている必要があります



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. [カスタムSSL証明書を有効にする] トグルボタンをオンにします。



SSL証明書の編集

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。

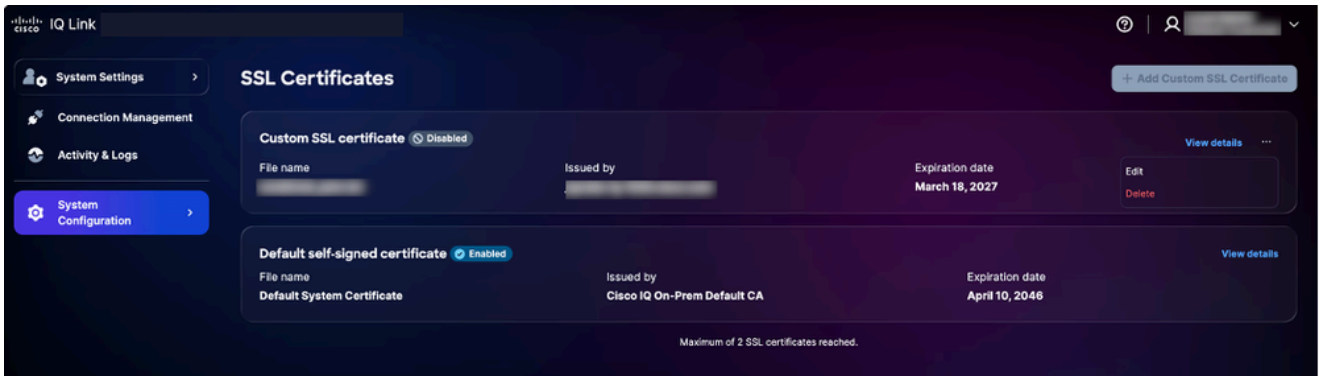
6. Saveをクリックします。

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

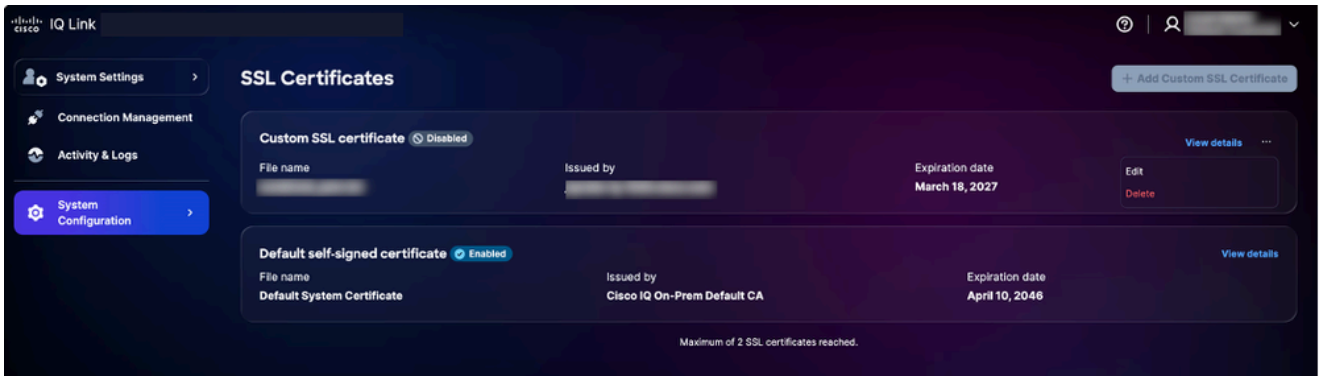
2. More Optionsアイコン> Editの順に選択します。Edit SSL Certificateページが表示されます。
3. 必要に応じて、証明書の詳細を編集します。
4. [Save] をクリックします。

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. 目的のカスタム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

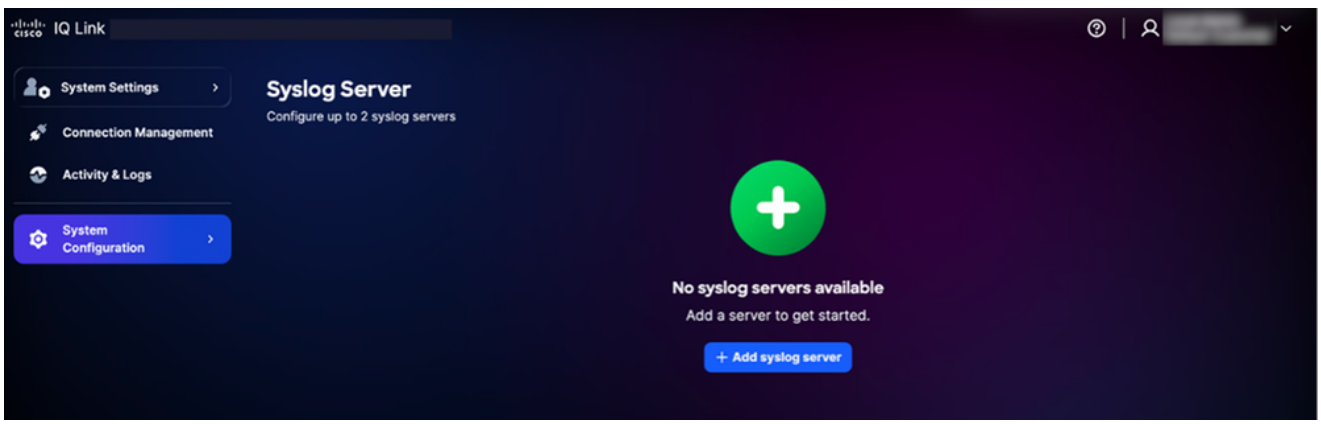
アカウント管理者ロールを持つユーザは、システムログをエクスポートするように外部syslogサーバを設定できます。最大2つのsyslogサーバを設定できます。

注:Syslogサーバは、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

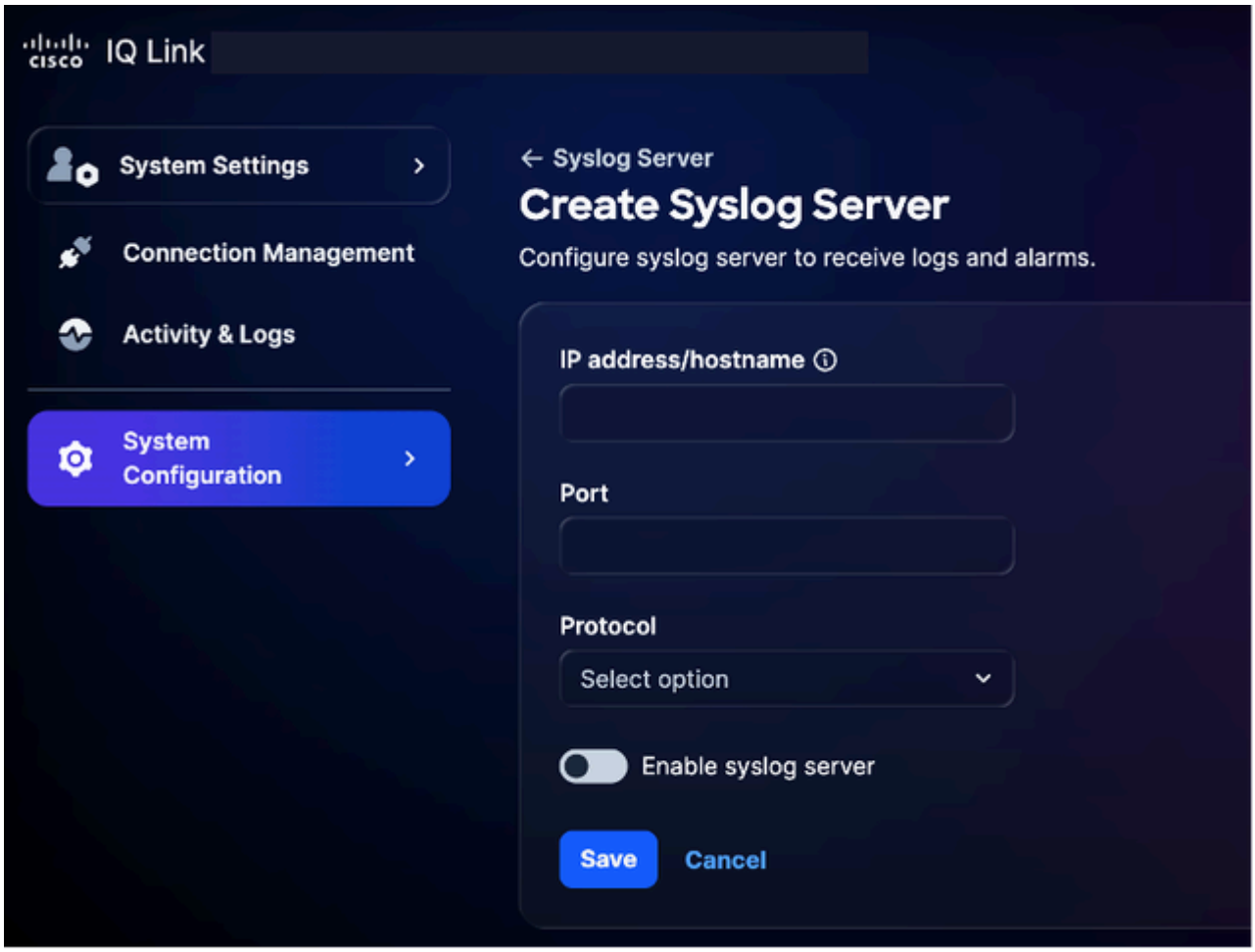
syslogサーバを追加するには、次の手順を実行します。

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。



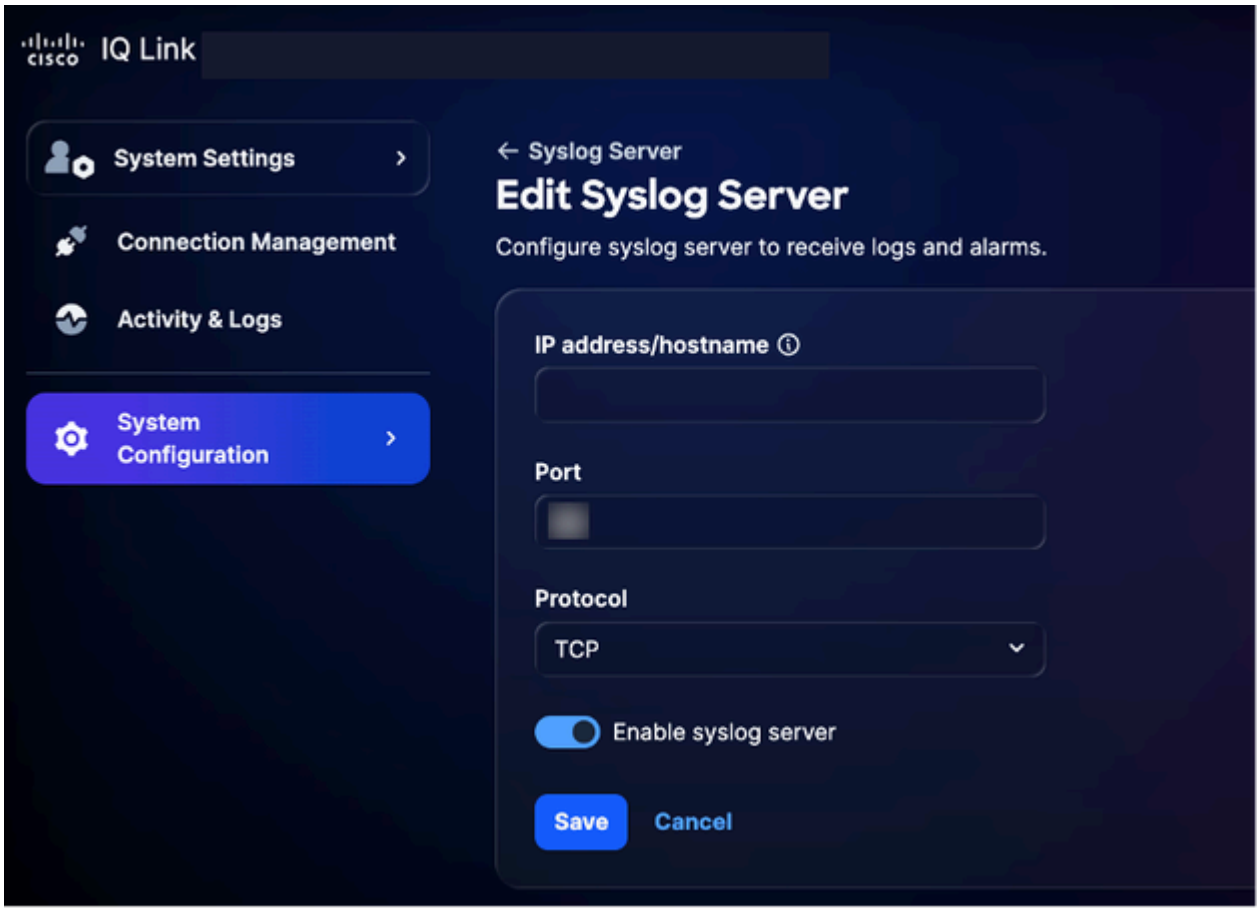
Syslogサーバの作成

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。



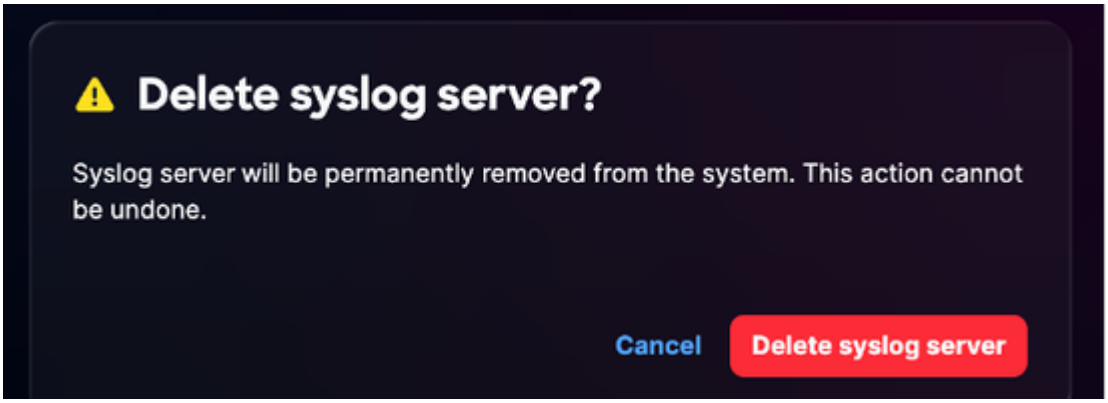
Syslogサーバの編集

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。

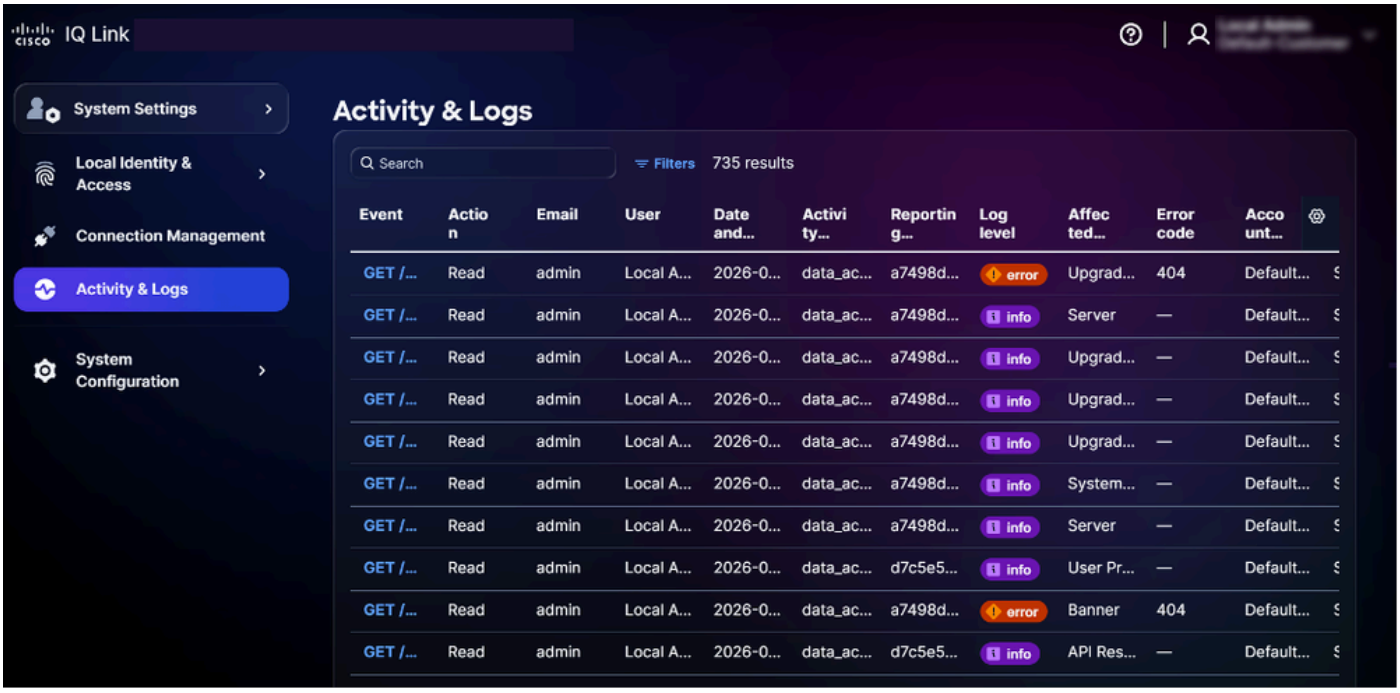
1. 目的のsyslogサーバに移動します。
2. More Optionsアイコン> Deleteの順に選択します。確認が表示されます。



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ます。これにより、アカウント管理者はユーザアクティビティを追跡し、透明性を維持できます。



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。

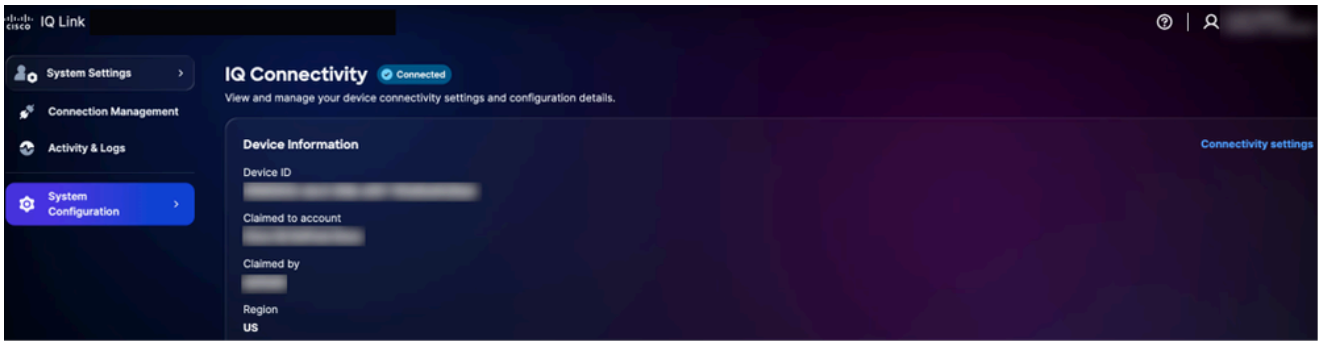
- Date：ログを特定の時間範囲でフィルタします。
- ログレベル：重大度（エラー、警告、情報など）でログをフィルタリングします。

- 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

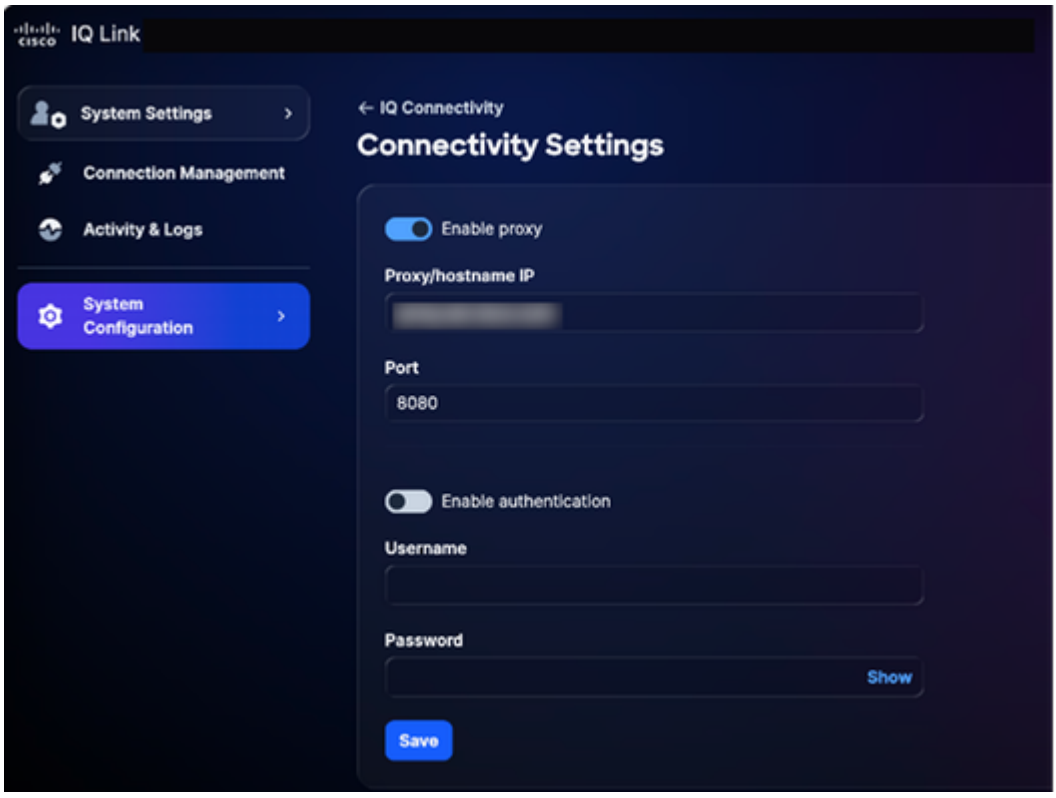
デバイスの接続設定と構成の詳細を表示および管理するには、次の手順を実行します。

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のオンプレミスソリューションで、インフラストラクチャを詳細に可視化す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。データ収集の構成の概要を次に示します。

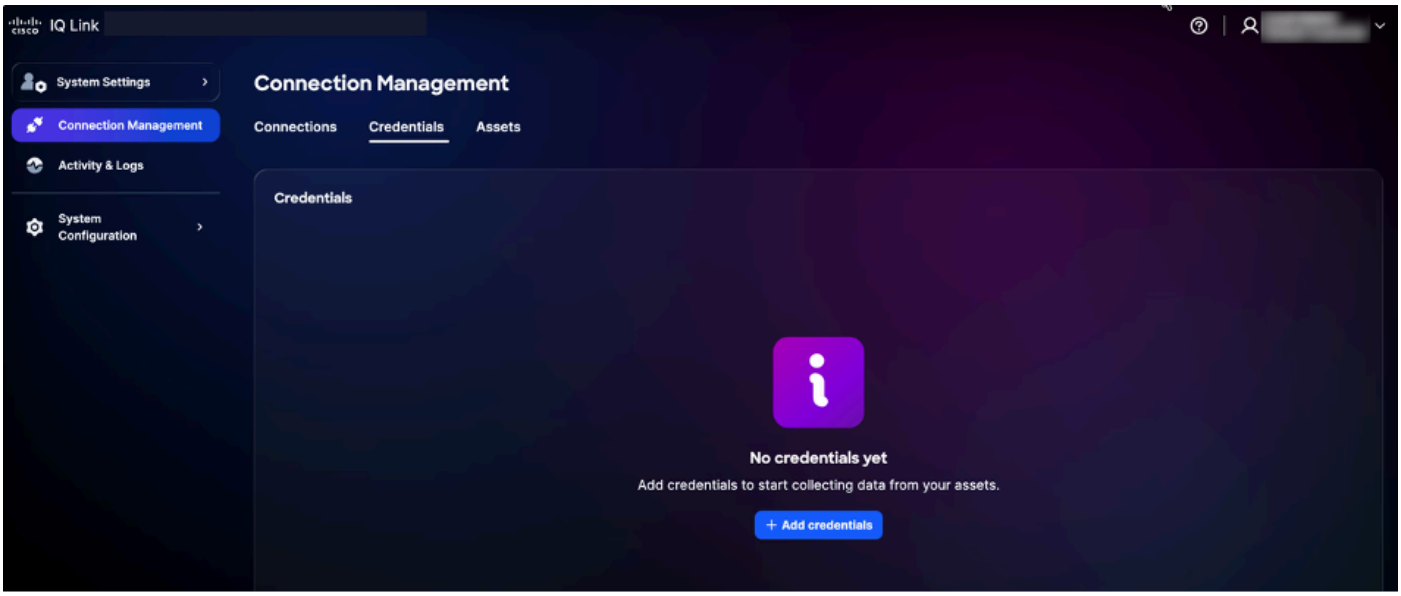
- クレデンシャルセットの作成：ネットワークデバイスと通信するための認証プロトコル(たとえば、Simple Network Management Protocol(SNMP)v1/v2c/v3)を確立します。セキュリティゾーンまたは口ケーションごとにクレデンシャルを一元化すると（「SanJose-SNMPv3」など）、1つの口ケーションでパスワードを更新し、関連するすべてのデバイスに変更を自動的に伝播することができます。
- 資格情報をインベントリにマッピングする：資格情報セットをインベントリ資産にマッピングして、認証プロセスを自動化します。特定のIP範囲を定義済みのクレデンシャルセットにリン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が必要です。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

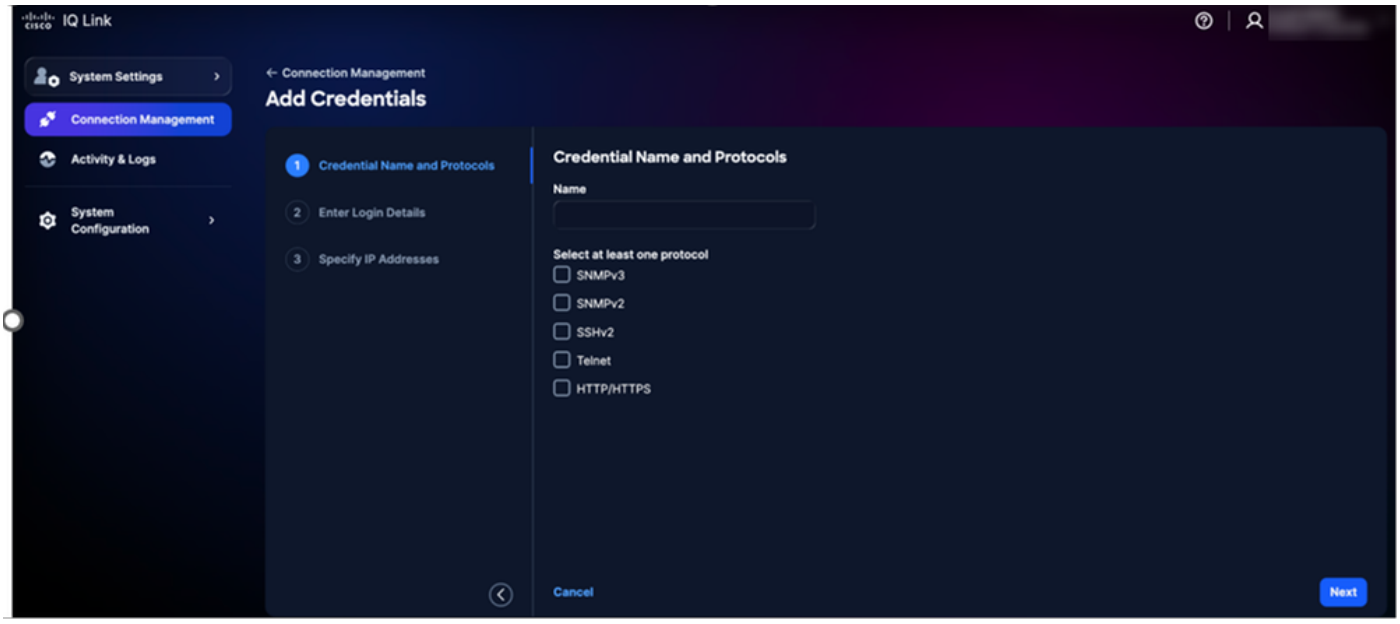
データ収集を実行するには、最初に資格情報を追加する必要があります。認証情報を追加するには、次の手順を実行します。

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。

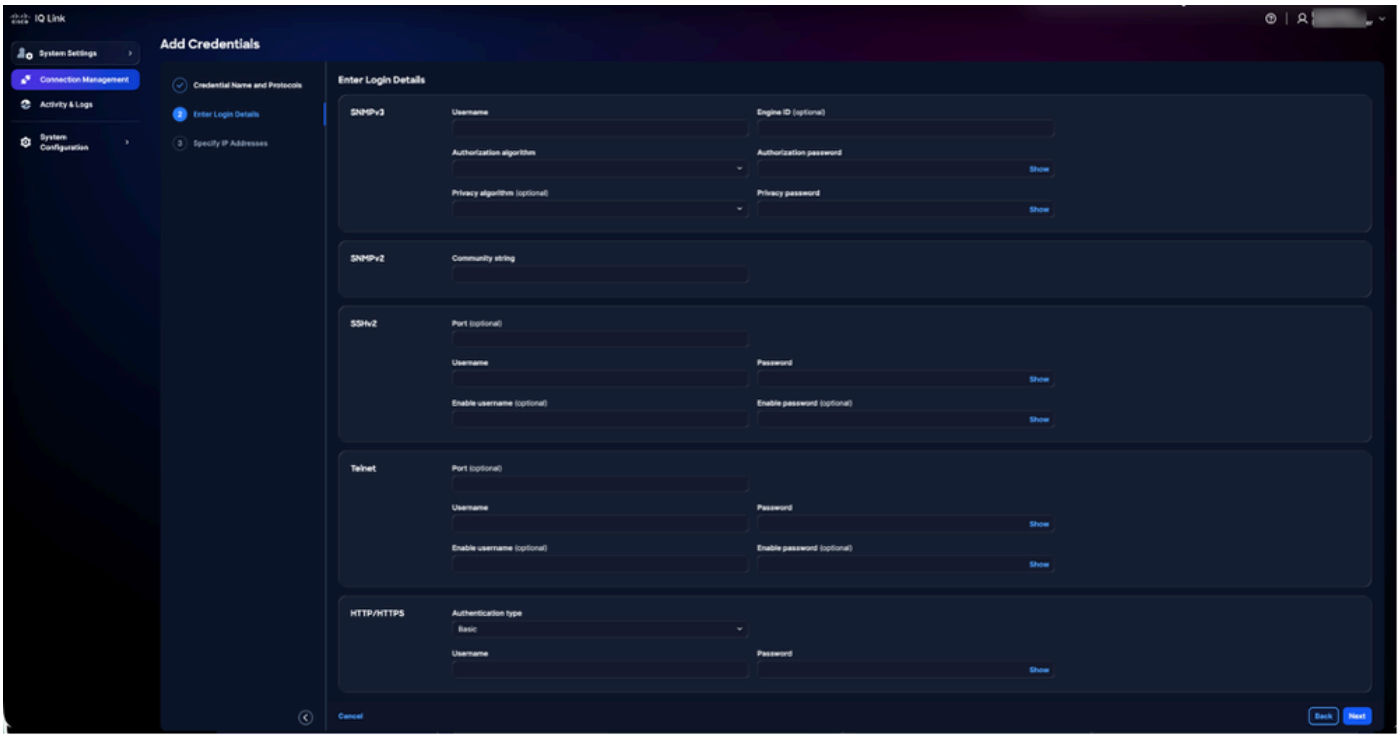


資格情報の追加

4. 名前を入力します。

5. 該当するすべてのプロトコルの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。

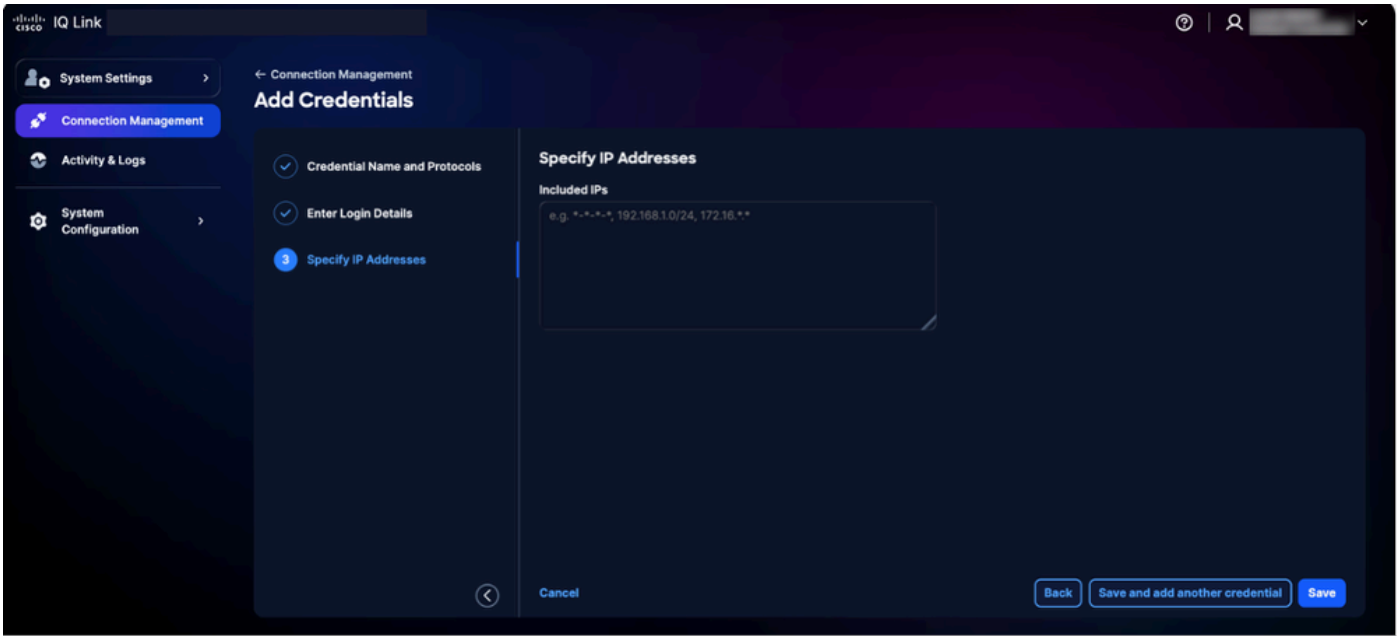


資格情報の詳細の追加

注：上の図では、前の手順ですべてのプロトコルが選択されたときのビューが示されています。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。



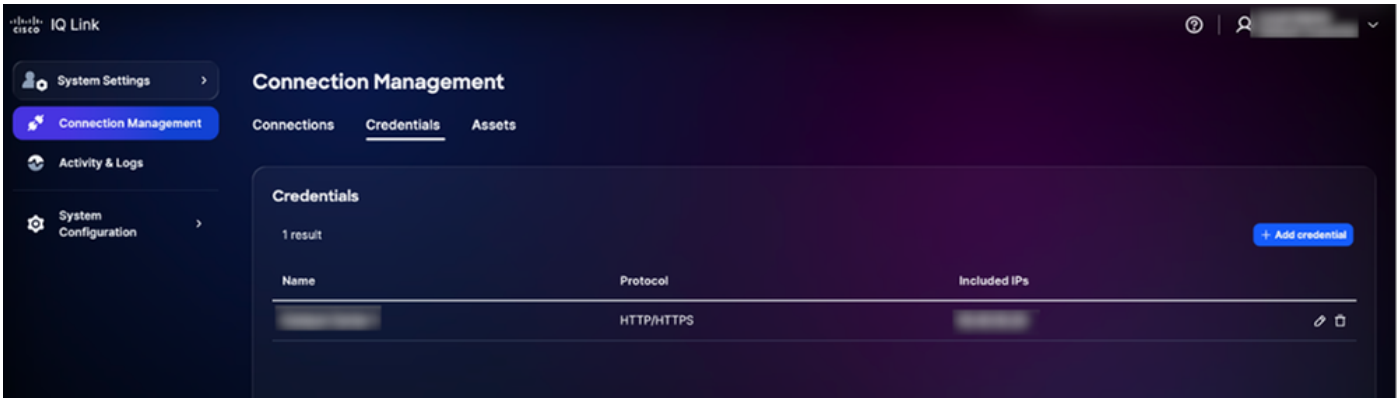
IPアドレスの指定

9.含まれるIPを入力します。

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、より具体的に一致し、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。

表13：クレデンシャルの選択例

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）

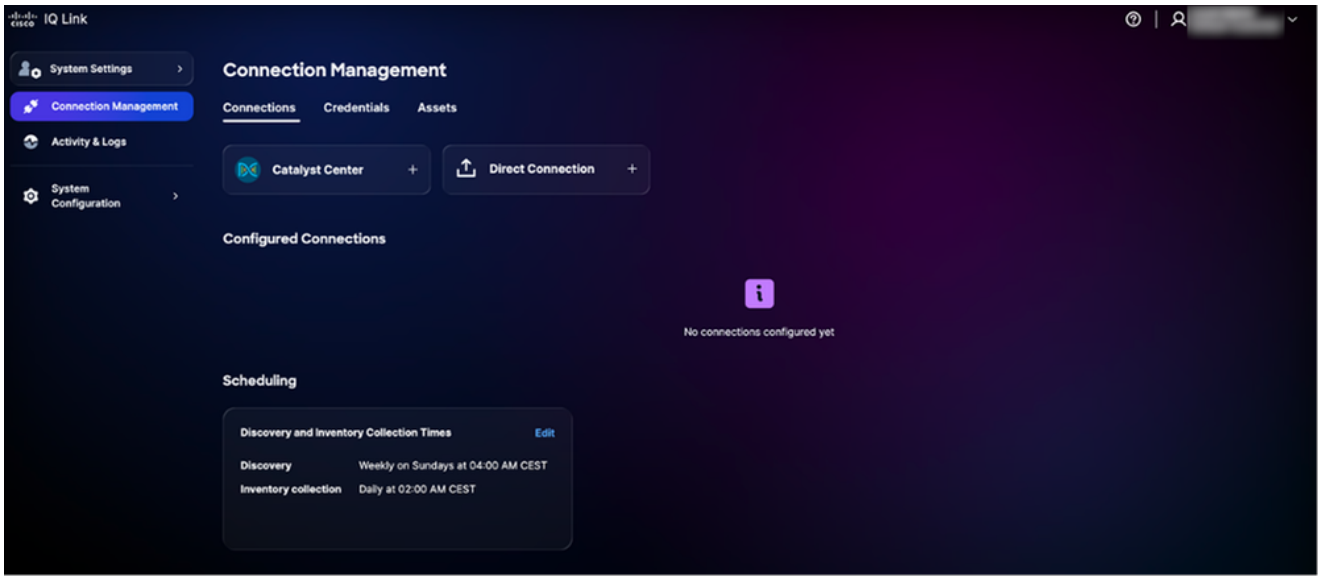
注：デバイスが複数の重複カテゴリに分類される場合、システムは常に最も特異性の高い（つまり、末尾のワイルドカードが最も少ない）クレデンシャルセットを選択します。

Catalyst Centerを使用したデータ収集

Cisco IQ Linkのインスタンスごとに、最大20のCatalyst Center（非クラスタ）を接続できます。

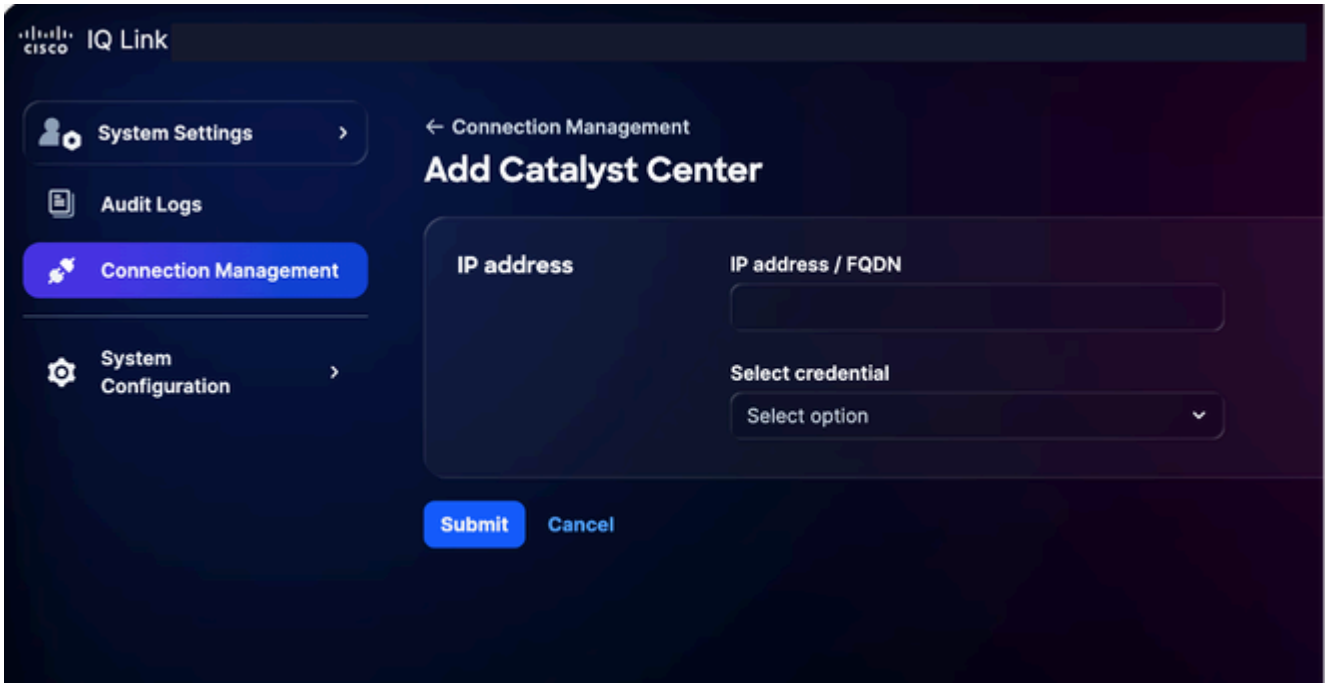
Catalyst Centerを使用したデータ収集：

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。

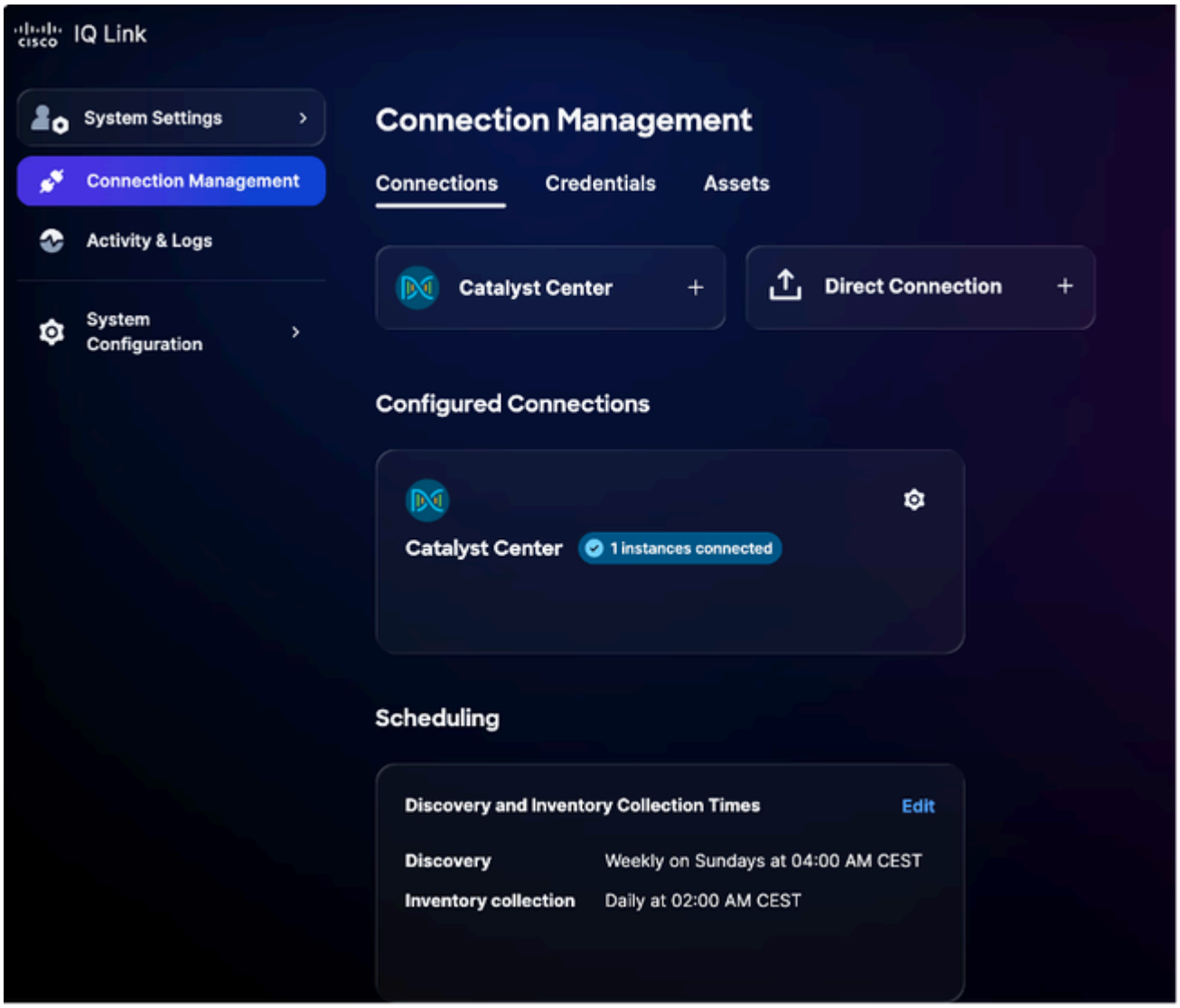


Catalyst Centerの追加

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

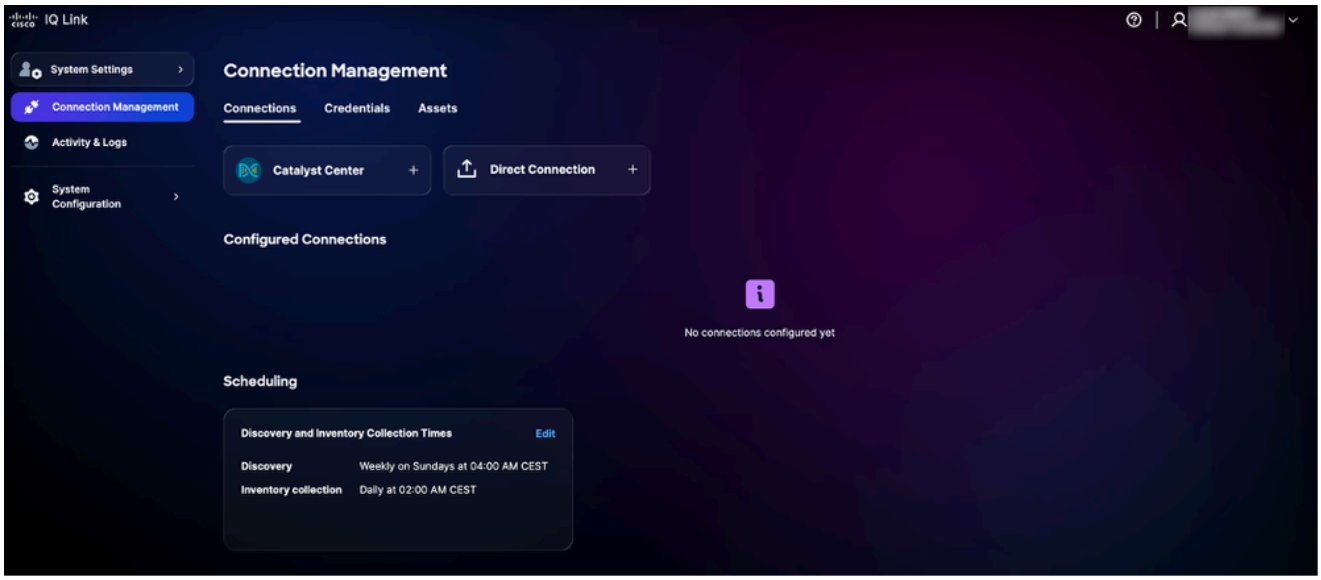
6. コレクションをスケジュールします。詳細は、『スケジューリング』を参照してください。

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

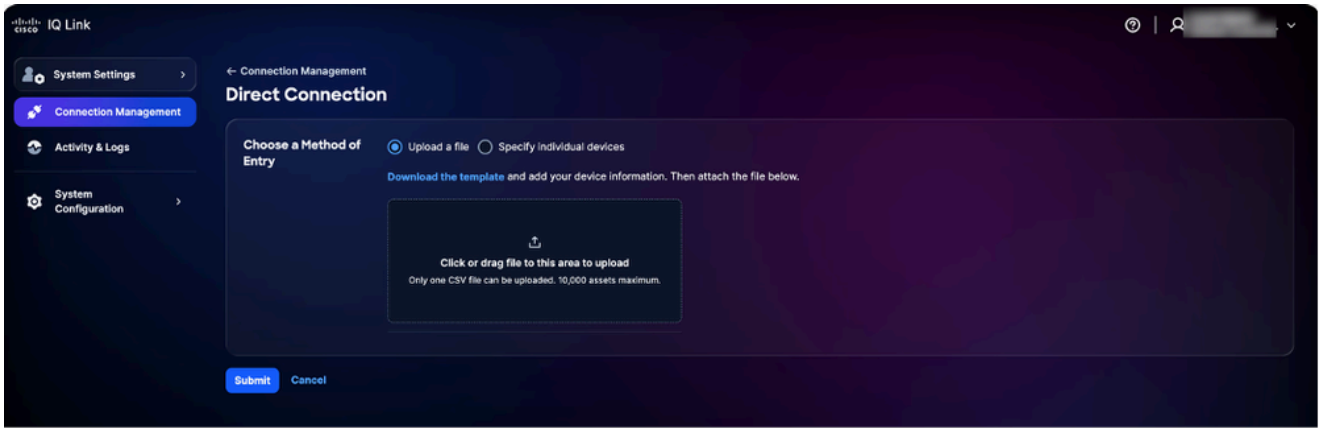
直接接続のデバイスを追加するには、次の手順に従います。

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。



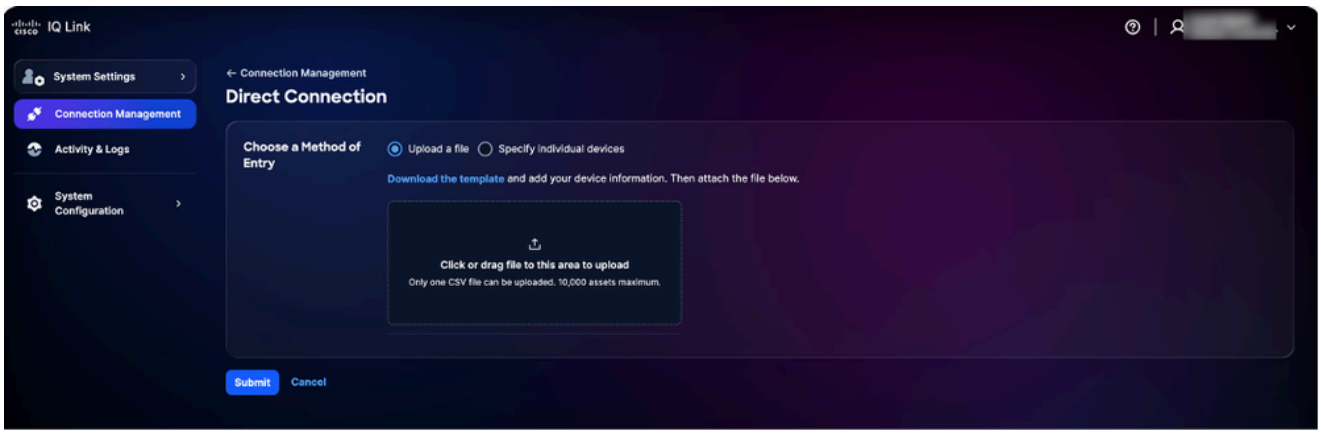
接続管理

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。



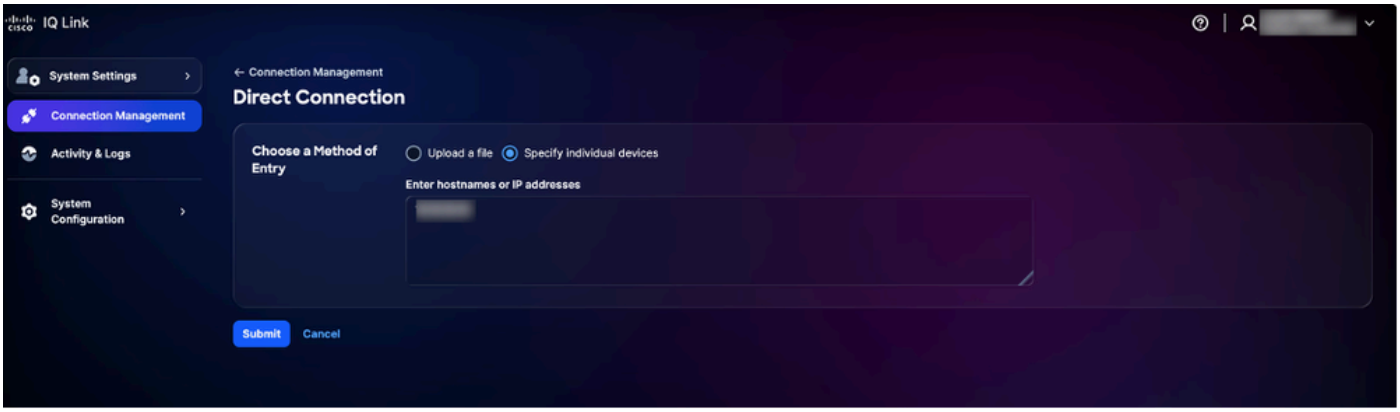
ファイルのアップロード

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。

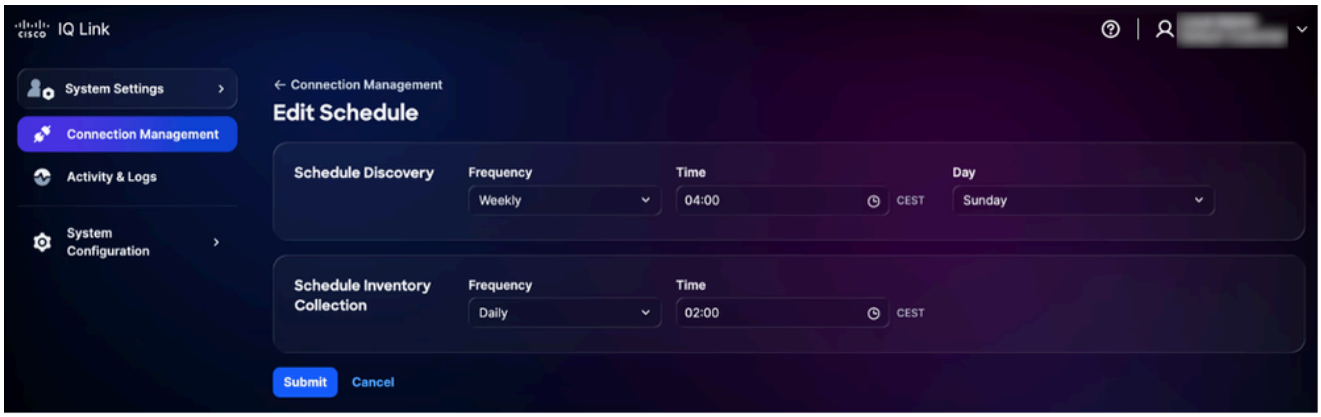
4. 収集をスケジュールします。詳細は、『スケジューリング』を参照してください。

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

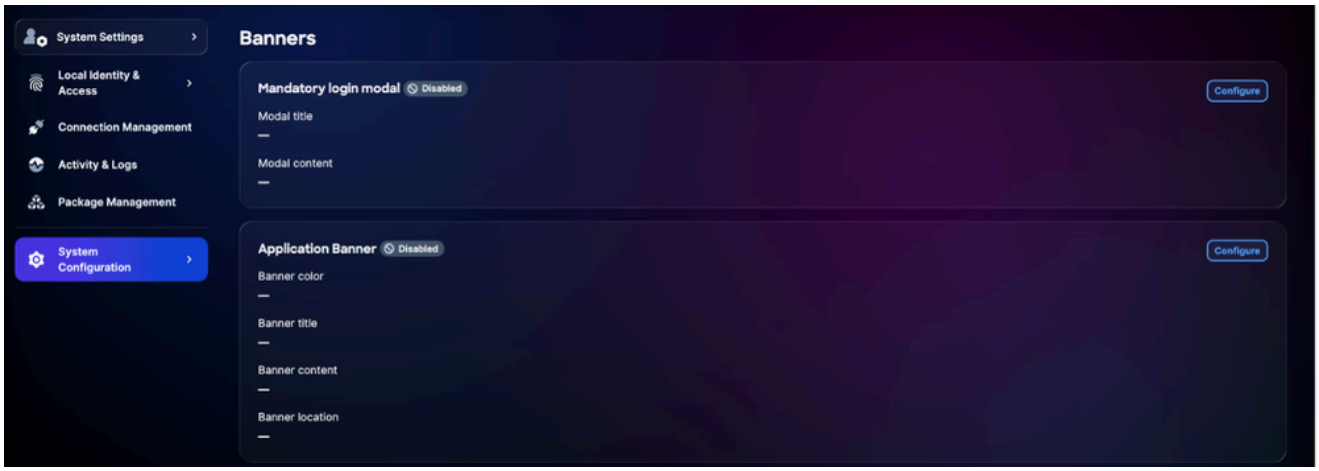
アカウント管理者は、システム全体のバナーを設定して、セキュリティおよびコンプライアンス標準を満たすことができます。

- 必須ログインモーダル：ログイン画面に進む前に、必須バナーを確認する必要があります。
- アプリケーションバナー：これは、認証が成功した後にアプリケーション全体に表示される、カスタマイズされたバナーです。

必須ログインモーダルバナーの設定

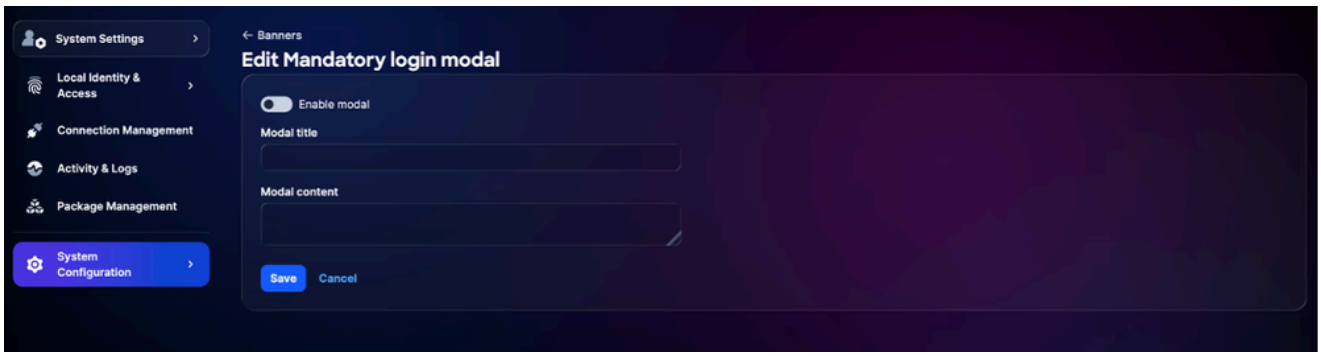
必須バナーを設定するには、次の手順を実行します。

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。



必須バナーの設定

2. Mandatory login modalでConfigureをクリックします。Edit Mandatory login modalページが表示されます。



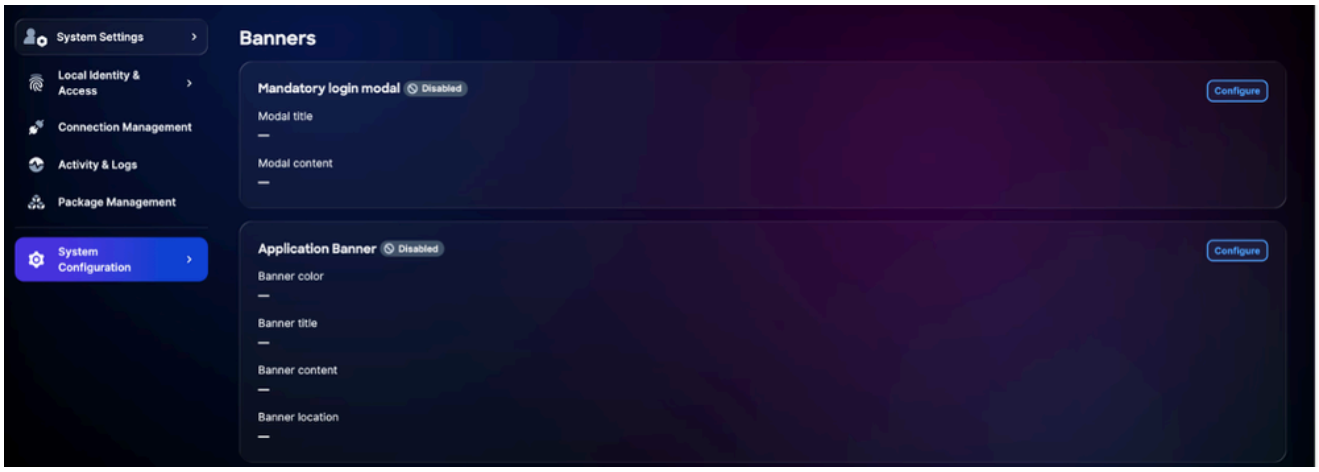
必須ログインモーダルバナーの編集

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. モーダルタイトルを入力します。
5. モーダルコンテンツを入力します。
6. [Save] をクリックします。必須ログインモーダルが保存されます。

アプリケーションバナーの設定

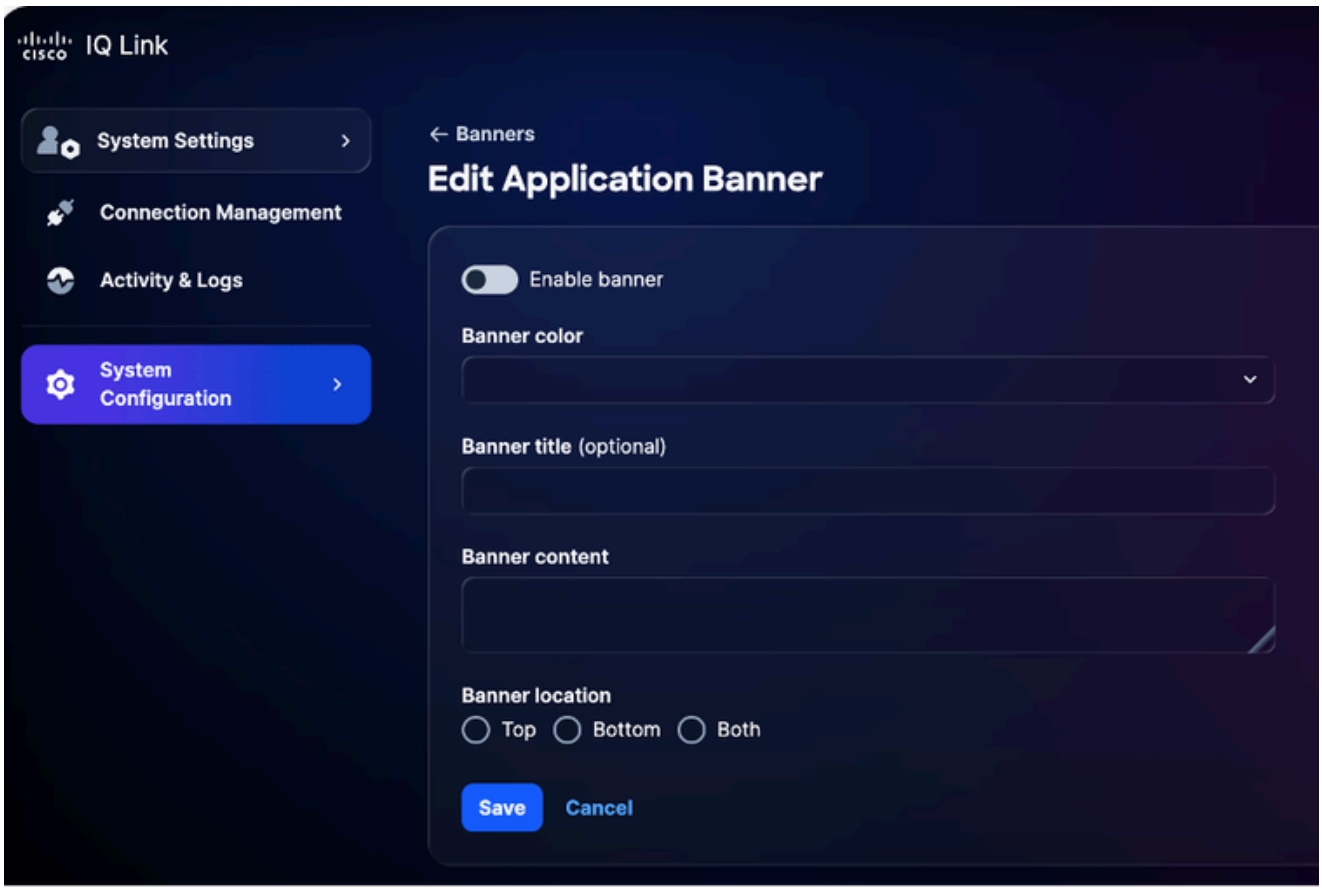
アプリケーションバナーを設定するには、次の手順を実行します。

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. アプリケーションバナーの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。

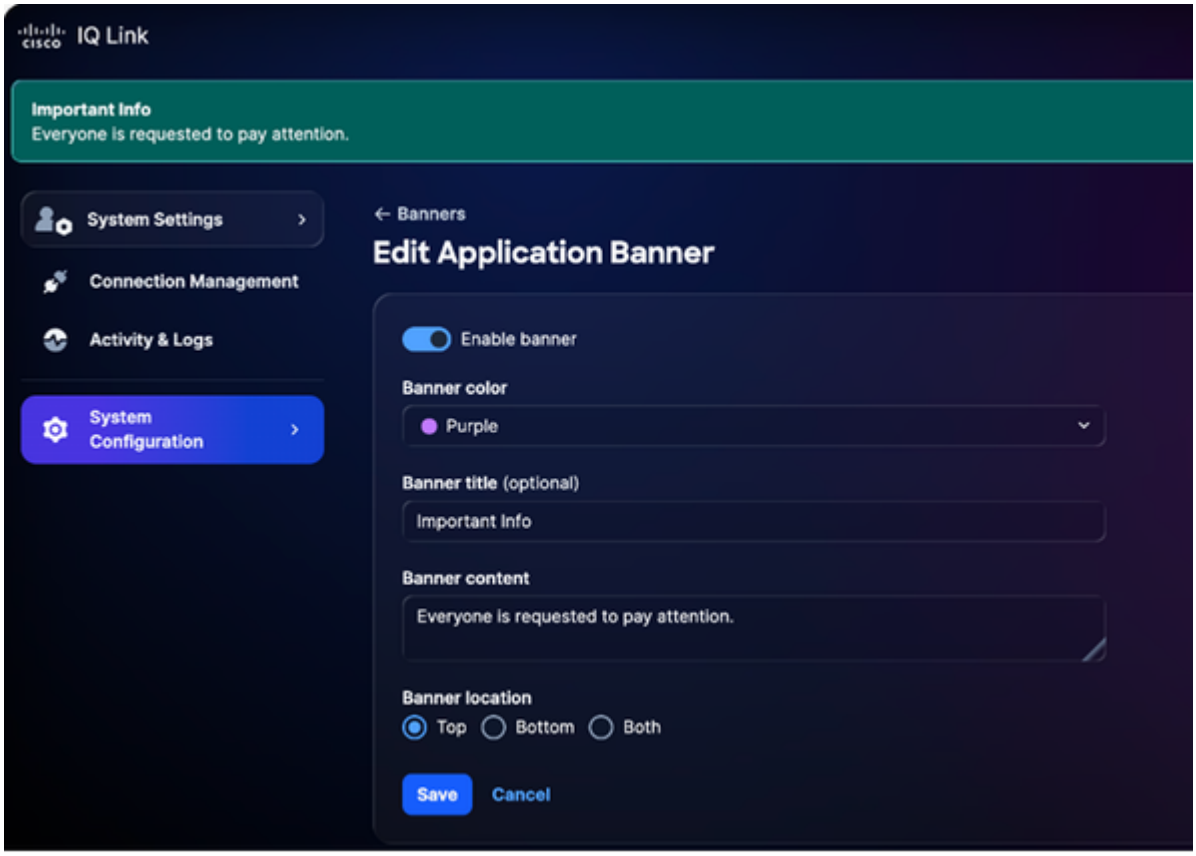
7. バナーの場所を選択します。
8. [Save] をクリックします。バナーはアプリケーション全体に表示されます。

バナーの編集

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。

アプリケーションバナーの編集

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

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て、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。

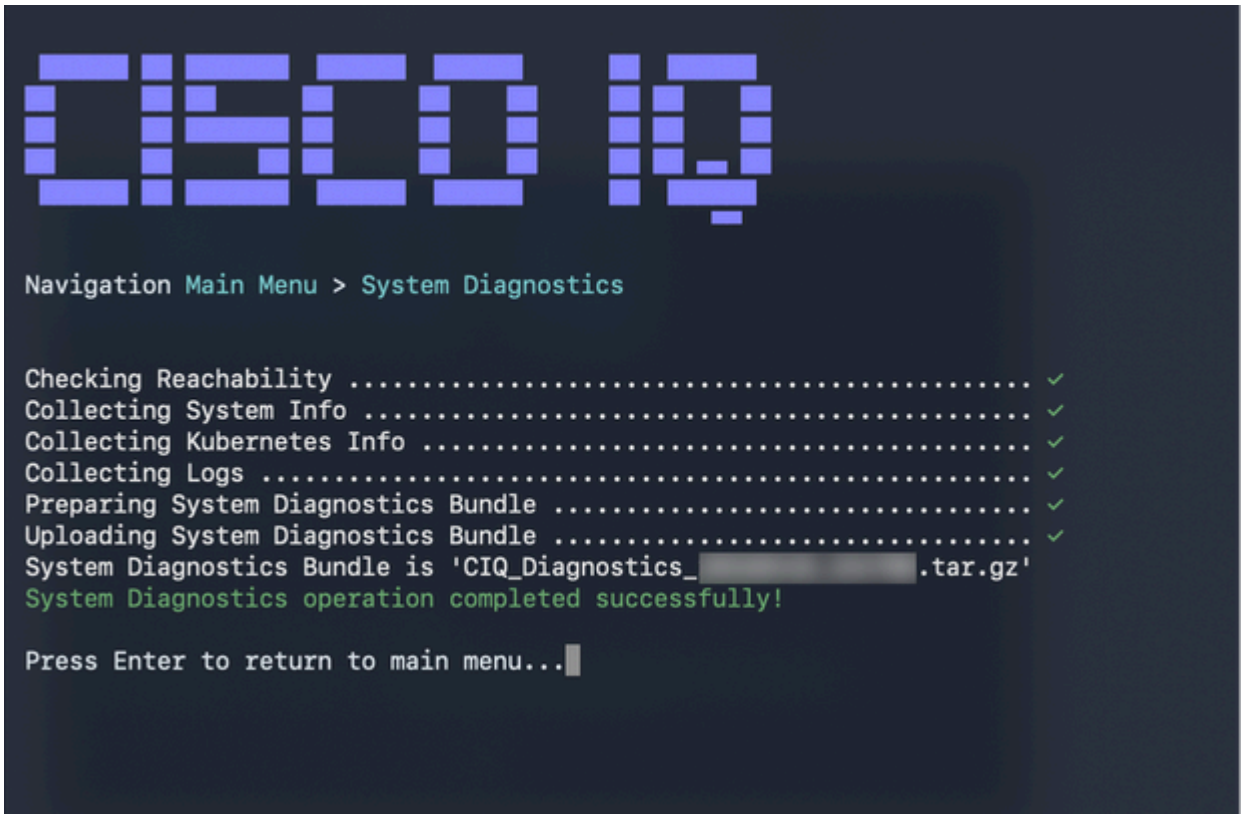
1. Cisco IQにログインします。

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。



システム診断操作の完了

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。