

Cisco IQ仮想アプライアンス操作ガイドv1.2.0

はじめに

Cisco IQTM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た拡張機能を提供します。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や、顧客エンゲージメントと成功のためのプロセスの合理化を可能にするコンテキスト認識を提供することで、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 On-Prem Air-Gappedは、Cisco IQの導入モードの1つで、コンプライアンス、データの支配権、およびセキュリティに関する厳格な要件を持つ、規制の厳しい業界のお客様向けに設計されています。このモードでは、Cisco IQは自己完結型の仮想マシン(VM)として提供され、Cisco IQ仮想アプライアンス(VA)と呼ばれます。VAは完全にお客様の構内で実行され、外部ネットワークから完全に分離されて動作します。この分離を維持するために、ソフトウェアアップデートとメンテナンスパッケージがCisco IQ SaaSから取得され、承認された手動プロセスを通じてVAに転送されます。

Cisco IQ On-Prem Air-Gappedは、Cisco IQ SaaSの主要機能をエアギャップ環境に拡張し、ミッションクリティカルなチームが、クラウドに接続された企業と同等のスピードと診断インテリジェンスで運用できるようにします。

Cisco IQ VAにアクセスするには、サポートされているブラウザを開いて<https://<fqdn-of-the-appliance>>に移動します。インストールプロセス中に設定されたadminユーザ名とパスワードを使用してログインします。

 注:Cisco IQ VAは現在、限定公開プログラムに登録しているお客様に限定されています。Cisco IQポータルからVAシステムソフトウェアおよび追加の運用パッケージ (モジュール、ルール、権限) をダウンロードするアクセス権は、一部のお客様にのみ付与されます。詳細については、アカウント担当者にお問い合わせください。

接続管理 (データ収集)

Cisco IQ VA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します。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、次の要素で構成されます。

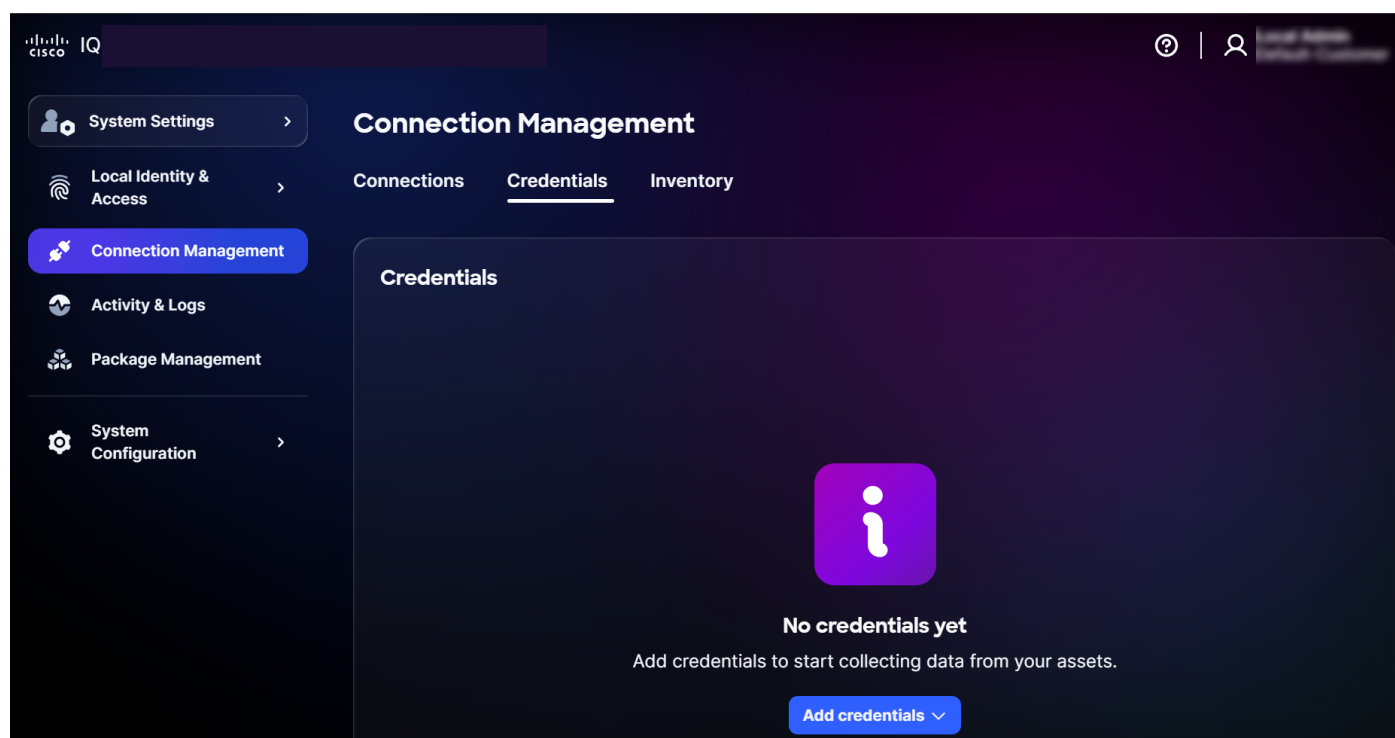
- クレデンシャルセットの作成：ネットワークデバイスと通信するための認証プロトコル(たとえば、Simple Network Management Protocol(SNMP)v1/v2c/v3)を確立します。セキュリティゾーンまたはロケーションごとにクレデンシャルを一元化すると(「SanJose-SNMPv3」など)、1つのロケーションでパスワードを更新し、関連するすべてのデバイスに変更を自動的に伝播することができます。
- 資格情報をインベントリにマッピングする：資格情報セットをインベントリ資産にマッピングして、認証プロセスを自動化します。特定のIP範囲を定義済みのクレデンシャルセットにリン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

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

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。

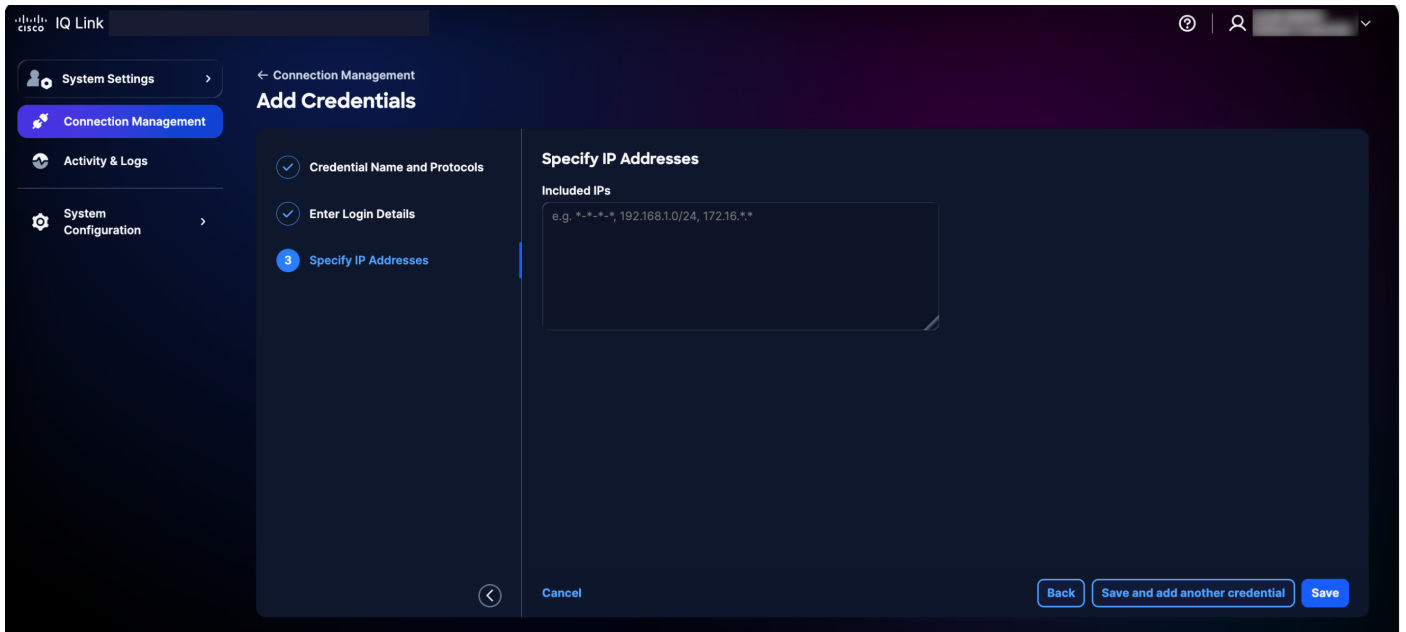
The screenshot shows the 'Add Credentials' screen at Step 2: Enter Login Details. The progress indicator now shows Step 1 as completed with a checkmark, and Step 2 as the active step. The main content area is titled 'Enter Login Details' and shows 'SNMPv3' selected. It contains four input fields: 'Username', 'Engine ID (optional)', 'Authorization algorithm' (a dropdown menu), and 'Privacy algorithm (optional)' (a dropdown menu). The 'Authorization password' and 'Privacy password' fields are masked with 'Show' buttons. At the bottom are 'Cancel', 'Back', and 'Next' buttons.

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表示されています。インターフェイスには、選択した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。

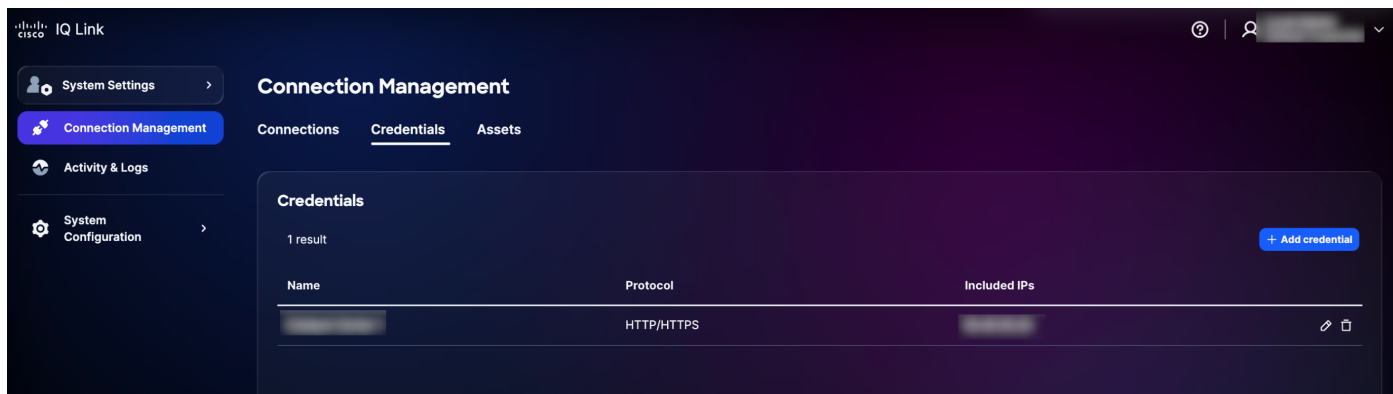


IPアドレスの指定

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.* (最高の優先度)
 - 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1：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)

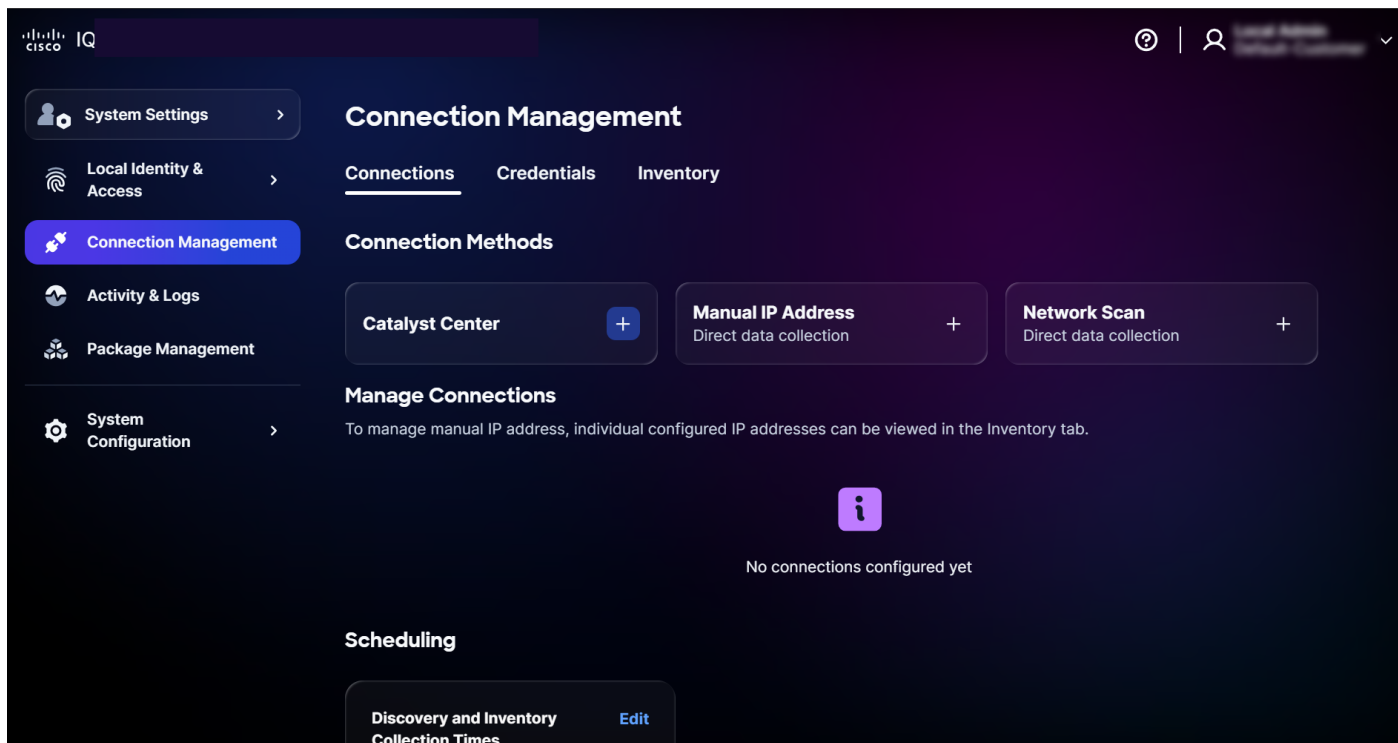
 注:デバイスが複数の重複カテゴリに分類される場合、システムは常に最も特異性の高い (つまり、末尾のワイルドカードの数が最も少ない) クレデンシャルセットを選択します。

Catalyst Centerを使用したデータ収集

Cisco IQ VA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。

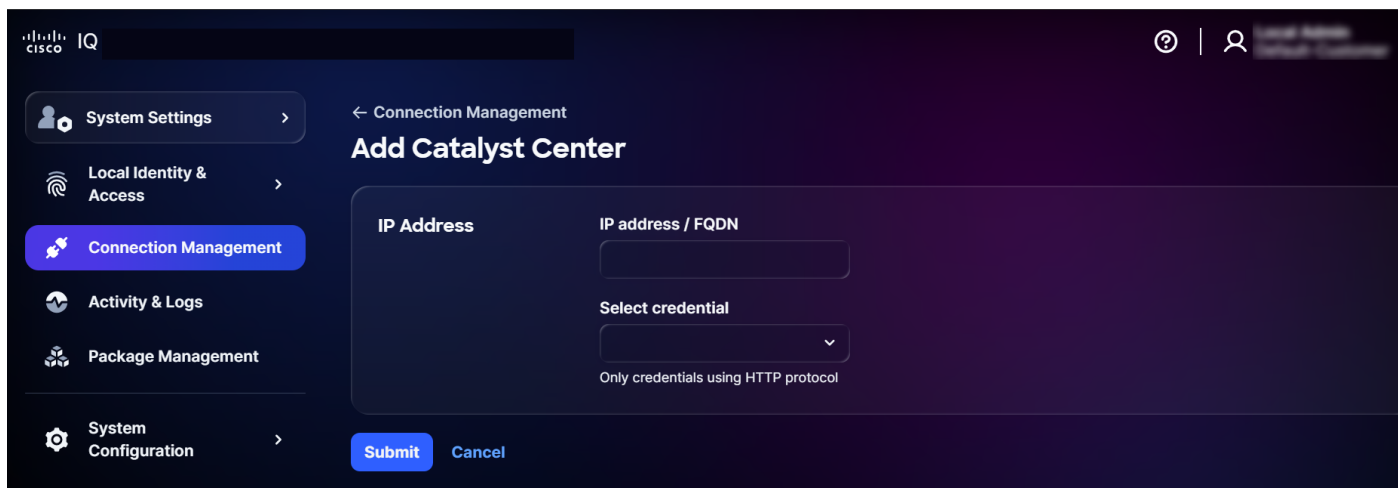
Catalyst Centerを使用したデータ収集：

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. Select credential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 (最大75分かかります)。新しく追加されたCatalyst Centerは、Configured Connectionsの下に表示されます。

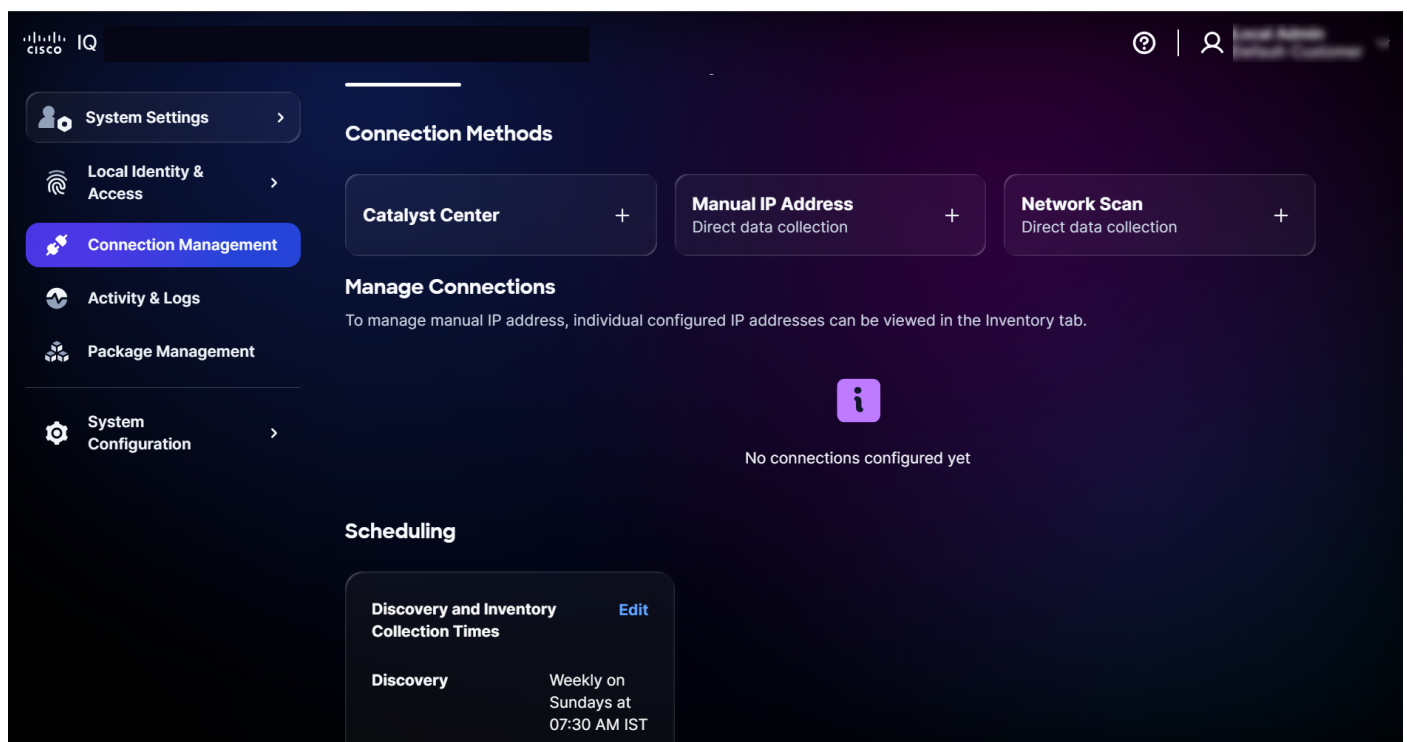
6. コレクションをスケジュールします。詳細は、『[スケジューリング](#)』を参照してください。

 注: Cisco IQ VA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。スケジュールは、組織の要件とメンテナンス期間に合わせて編集することを強くお勧めします。

手動データ収集

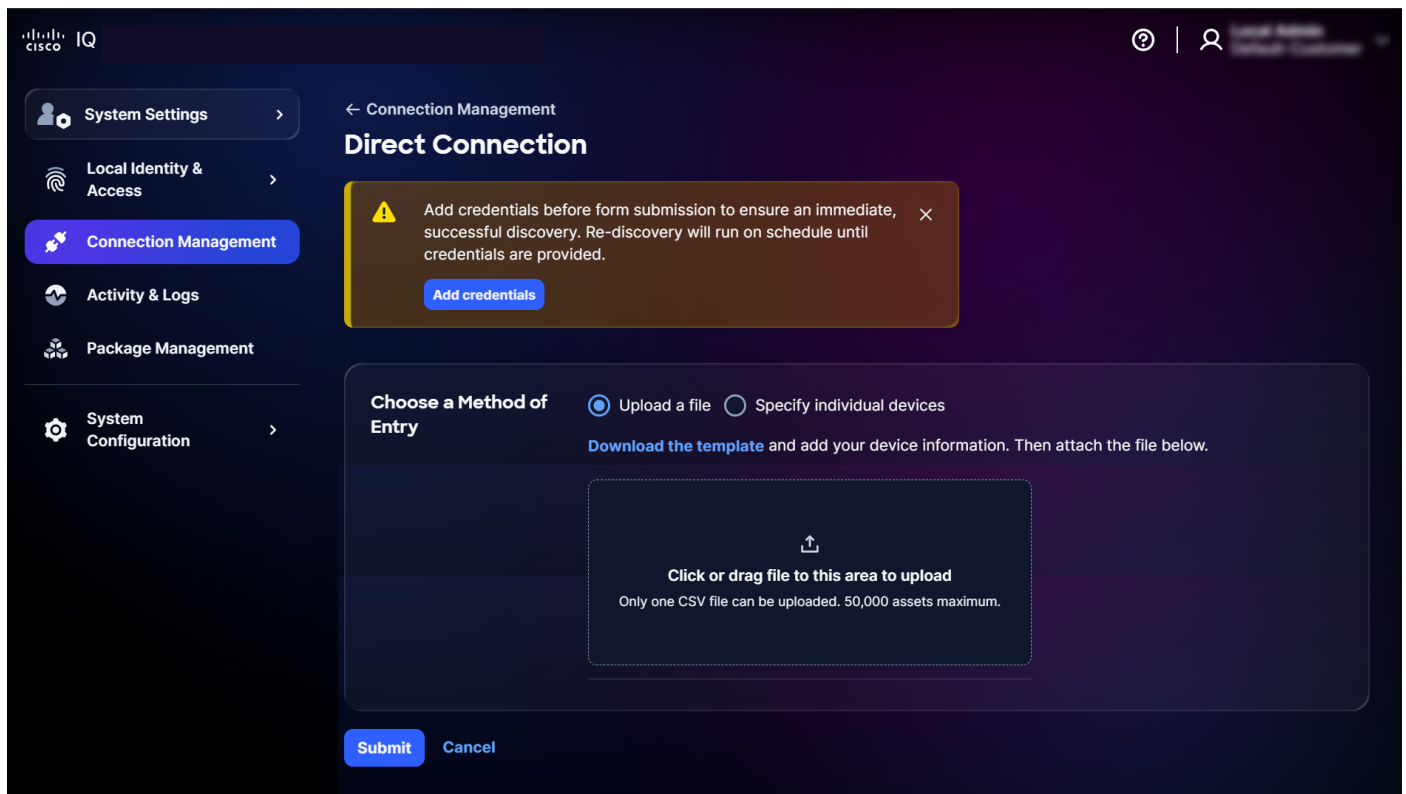
直接データ接続用のデバイスを追加するには、次の手順に従います。

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

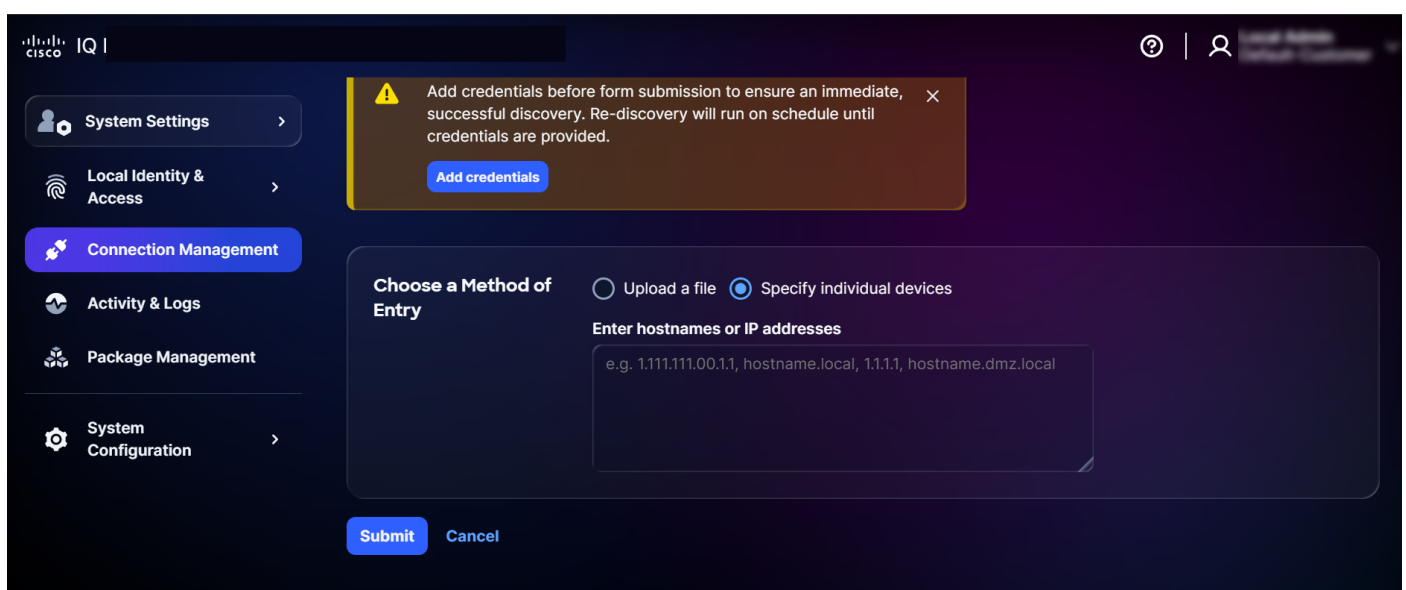
2. Manual IP Addressをクリックします。直接接続ページが表示され、データを収集するための2つのオプションが示されます。



ファイルのアップロード

3. Choose a Method of Entryの中から適切なオプションをクリックし、次のいずれかの方法を使用してデバイス情報を指定します。

- 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。



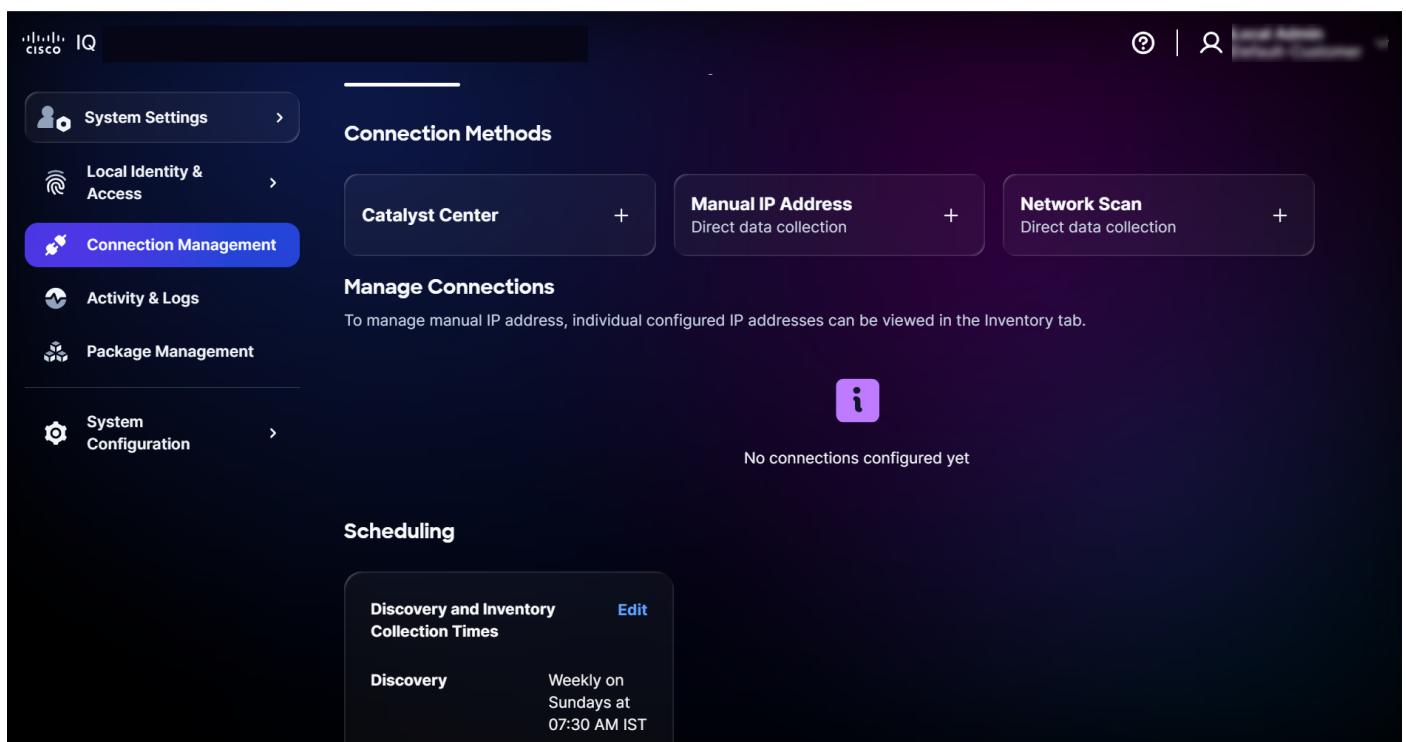
個々のデバイスの指定

- 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リストを入力します
4. [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。
 5. 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 VA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。

ネットワークスキャン

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。



ネットワークスキャン

2. Network Scanをクリックします。Connect Assets by Network Scanページが表示され、3つのオプションがあります。

Cisco IQ

System Settings >

Local Identity & Access >

Connection Management

Activity & Logs

Package Management

System Configuration >

← Connection Management

Connect Assets by Network Scan

Scan Method

☒ Specify IP Range ☐ Specify Discovery Protocol (CDP/LLDP) ☐ File Upload

Name

IP Start IP End

Schedule Scan

Frequency Time

hh:mm IST

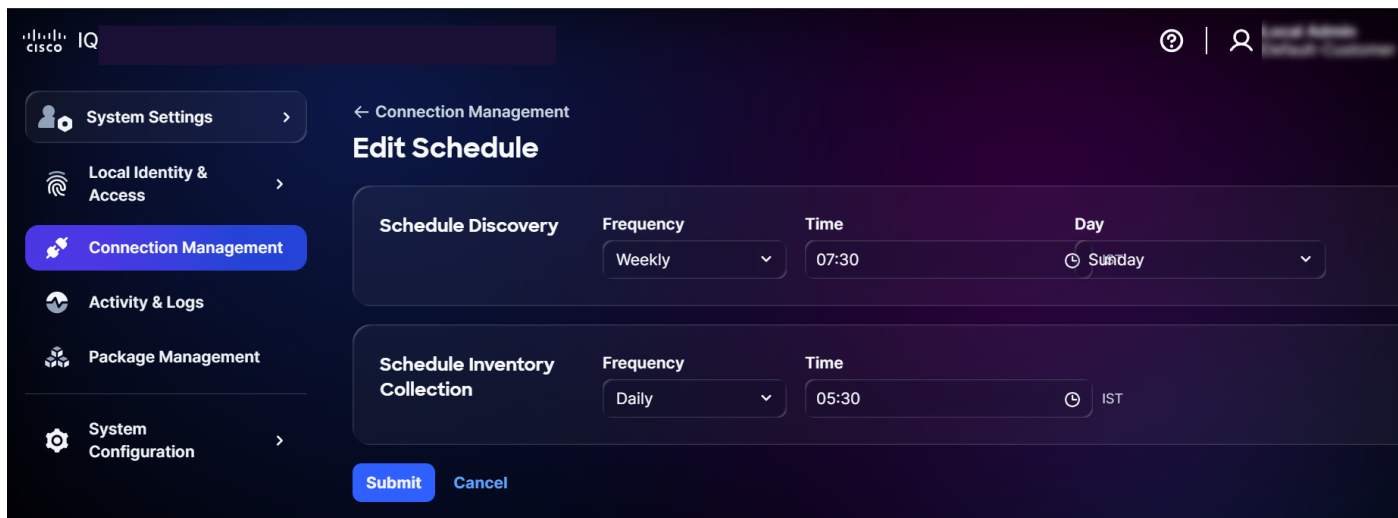
Connect assets Cancel

- IP範囲の指定：ネットワーク検出または管理タスク用に、その範囲内のターゲットデバイスへのIPアドレスの範囲を定義します
 - Specify Discovery Protocol (CDP/LLDP):使用するネットワーク検出プロトコルを選択します。
 - ファイルアップロード：コンフィギュレーションファイルやデータなどのファイルをアップロードします。
3. 名前を入力します。
 4. IP StartとIP Endを入力します。
 5. Schedule Scanの下で、FrequencyとTimeを選択します。
 6. Connect assetsをクリックします。

スケジューリング

スケジューリングを使用すると、Cisco IQ VA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に加えた変更が仮想アプライアンス内で正確に同期および反映されるまで、5 ~ 10分待ちます。

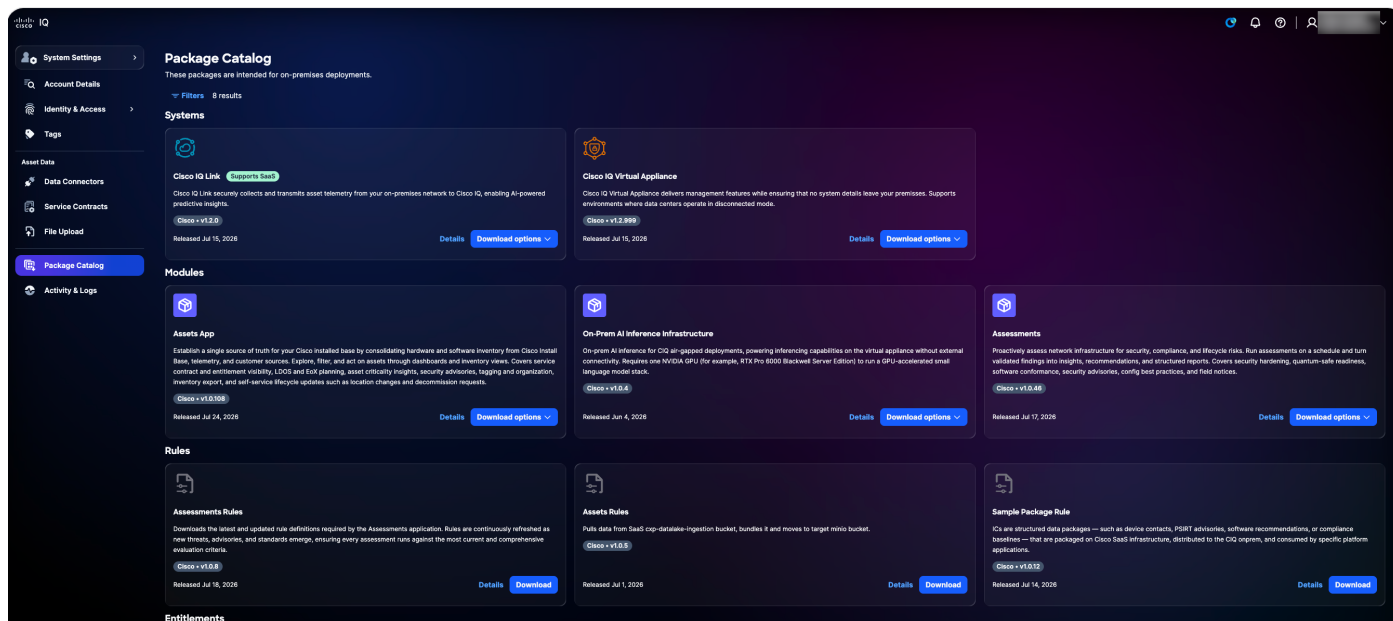
パッケージのインストール（モジュール、ルール、および権限）

VA内のオペレーショナルモジュール、ルール、エンタイトルメント、および専用のAIを活用した機能のソフトウェアライフサイクル（インストールと設定）を管理できます。これらのパッケージは、パッケージカタログに移動し、Cisco IQ(SaaS)から最新バージョンをダウンロードしてインストールできます。パッケージカタログには、使用可能なソフトウェアインスタンスが表示されます。アップデートをシームレスに監視および管理し、システムインスタンスの効率的な追跡と管理を実現します。

モジュールの追加

モジュールは、VA内でコア機能を提供するスタンドアロンソフトウェアパッケージです。独自のライフサイクルを持つ独立したサービスで、インストール、メンテナンス、サイズ変更が可能です。CPU、GPU(Graphics Processing Unit)、RAMなどのリソース消費量は、初期インストール時に選択した展開サイズ（小、中、大）に基づいて動的に割り当てられます。

1. [Cisco IQ](#)にログインします。
2. System Settings > Package Catalogの順に移動します。

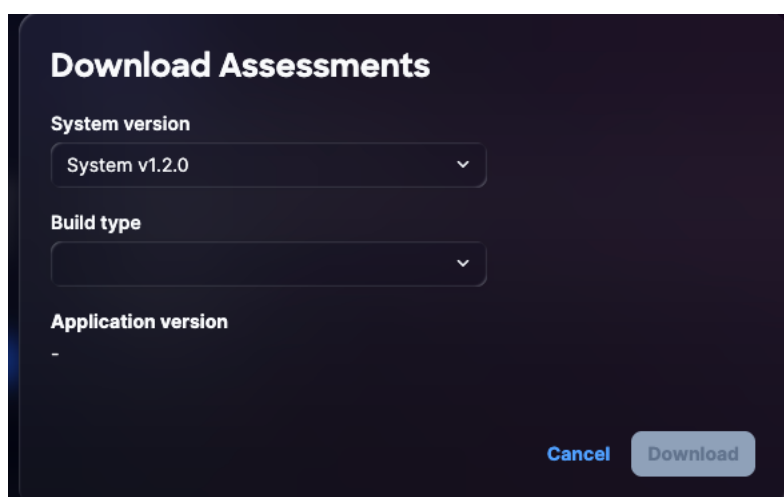


パッケージカタログ

3. 目的のモジュールカードで、Download options > Installation packagesの順にクリックします。Downloadウィンドウが開きます。



注：例のイメージには評価モジュールを使用します。



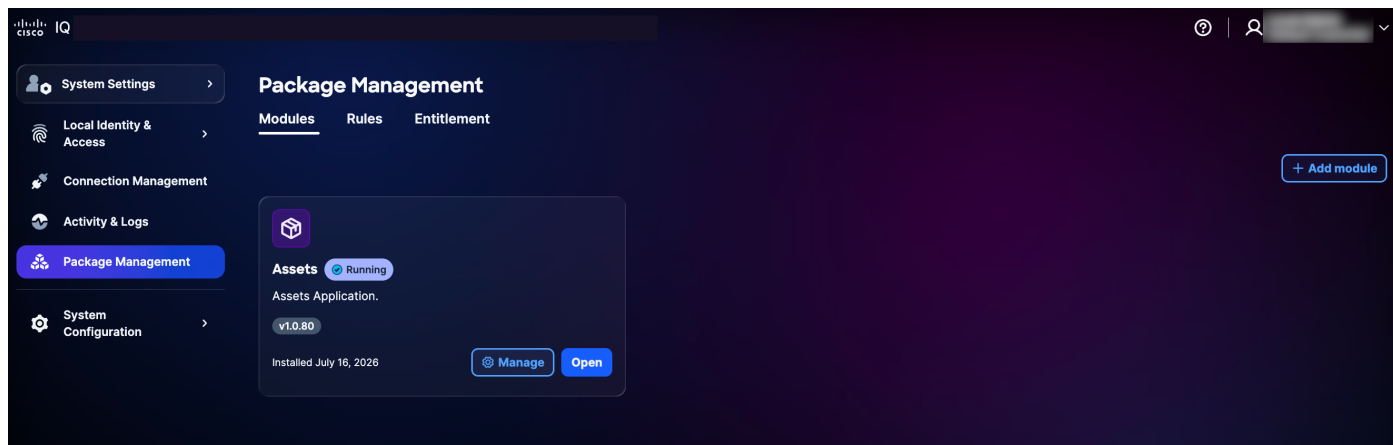
ダウンロード

4. ドロップダウンリストからシステムバージョンを選択します。

5. ドロップダウンリストから構築タイプを選択します。
6. Download をクリックして、ファイルをローカルに保存します。

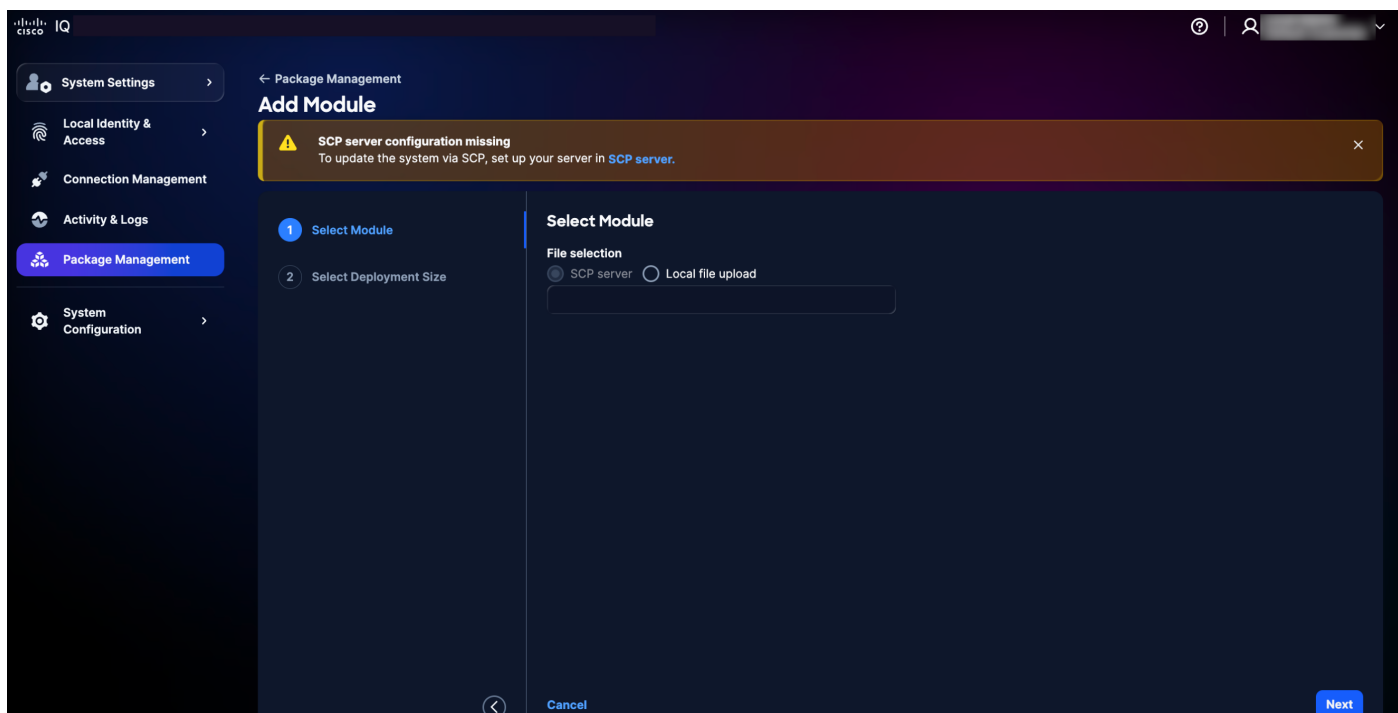
 注：インストールファイルが大きい(10 ~ 25 GB)、ダウンロードする前に十分なディスク領域があることを確認してください。

7. VAに移動します。
8. Home > System Settings > Package Managementの順に移動します。「パッケージ管理」ページが表示され、次のタブが表示されます。
 - Modules
 - ルール
 - 権利



Modules

9. Add moduleをクリックします。

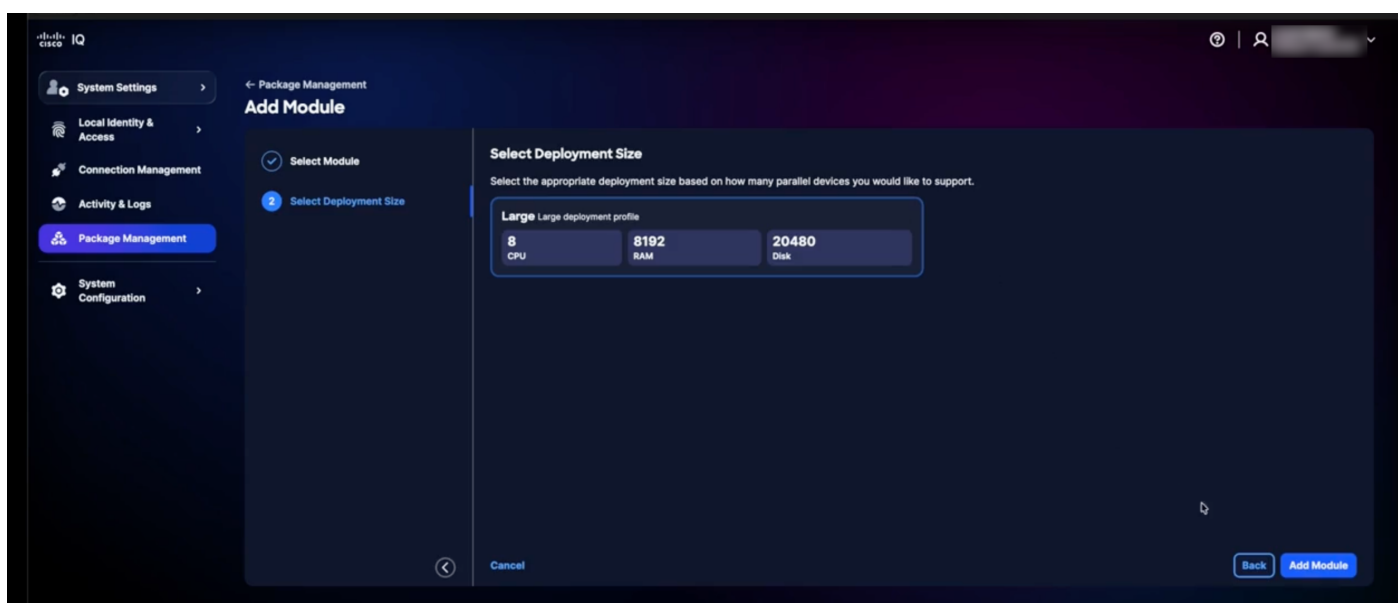


モジュールの追加

10. 希望するファイル選択オプションを選択します。

- SCPサーバ：インストールパッケージの正確なファイル名を入力します（大きなファイルの場合に推奨）。
- ローカルファイルのアップロード：ダウンロードしたインストールファイルをドラッグアンドドロップします（アップロード時間が30 GB以上のファイルには推奨されません）。

11. [Next] をクリックします。

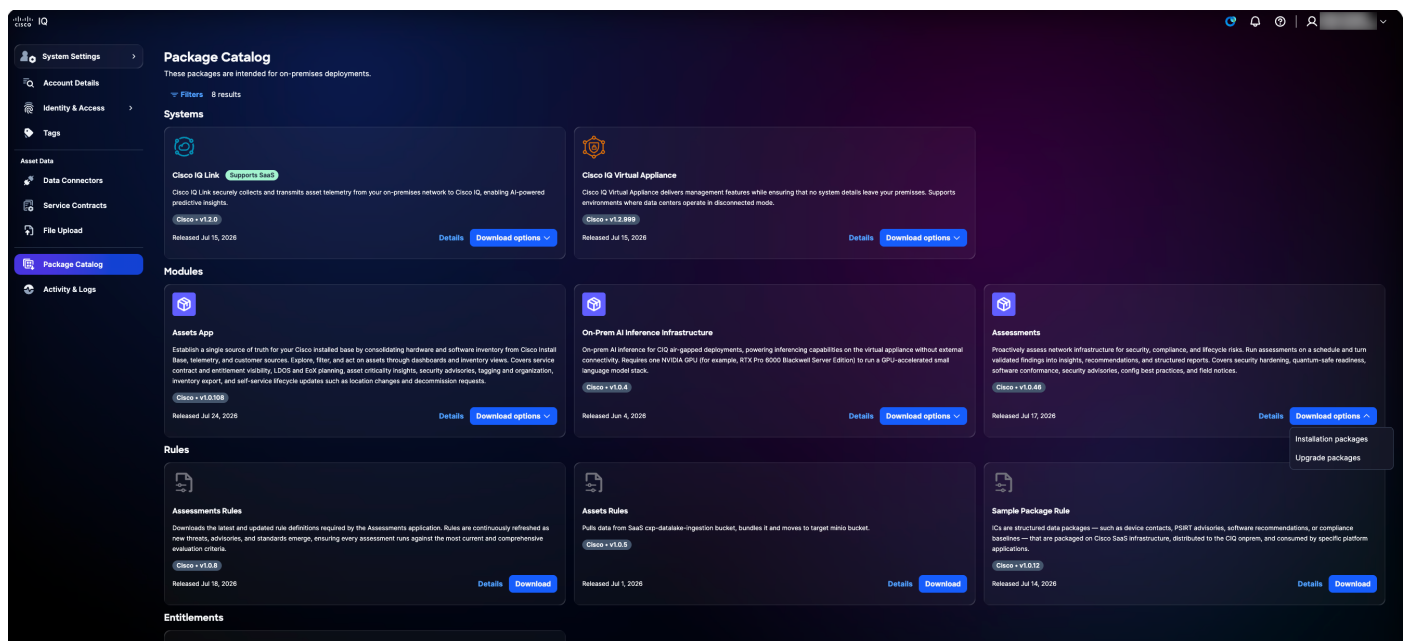


導入規模

12. 導入サイズ (小、中、大など) を選択します。これらのサイズは事前に定義されており、リソース要件を決定します。
13. Add Moduleをクリックします。新しくインストールしたモジュールがPackage ManagementのModulesタブに表示されます。完了すると、モジュールのステータスは「Running」に変わり、Openボタンが使用可能になります。

モジュールのアップグレード

最新のモジュールは、パッケージカタログ(Cisco IQ)で継続的に更新されています。最新バージョンにアップグレードするには：



ネットワークスキャンによるアセットの接続

1. 目的のモジュールカードで、Download options > Upgrade packagesの順にクリックします。Downloadウィンドウが開きます。



注：アセスメントモジュールは、イメージの例として使用されます。

Upgrade Assessments

System version

System v1.2.0



Current app version



Build type



Application version

-

Cancel

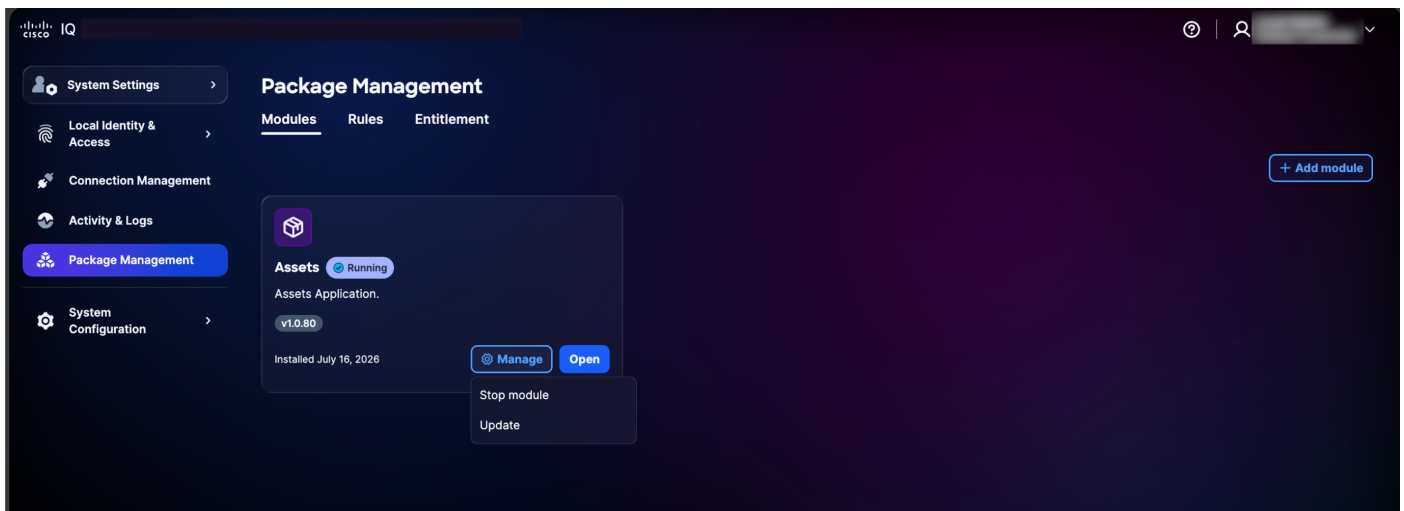
Download

ダウンロード

2. ドロップダウンリストからシステムバージョンを選択します。
3. ドロップダウンリストから、現在のアプリケーション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. Downloadをクリックして、ファイルをローカルに保存します。
6. VAに移動し、ダウンロードしたファイルのインストールを完了します。

モジュールの管理

モジュールを追加したら、Package ManagementページでManageをクリックして、そのモジュールを変更できます。使用できる修正オプションには、サイズ変更や上位バージョンへのアップグレードなどがあります。モジュールを管理するには：



更新の種類

1. Package Managementページで、目的のモジュールに対してManage > Updateの順にクリックします。
2. 更新タイプを選択します。
 - 展開のサイズのみを変更する
 - バージョンの更新
3. Change deployment sizeが選択されている場合は、Nextをクリックして、次のページで新しい配置サイズを選択します。

または

Update Versionを選択すると、File selectionオプションが表示されます。SCP Serverのいずれかを選択し、インストールパッケージの正確なファイル名を入力するか、Local file uploadを選択して、ダウンロードしたインストールファイルをドラッグアンドドロップします。

4. [Next] をクリックします。Select Update Scheduleページが表示されます。
5. スケジュールを更新するには、次のオプションボタンから選択します。
 - 更新する
 - 後で更新



注：一部のモジュールでは、ダウンタイムなしでアップデートがサポートされます。ダウンタイムが必要な場合は、詳細がバナーに表示されます。

6. Update laterを選択した場合、DateとTimeを入力します。

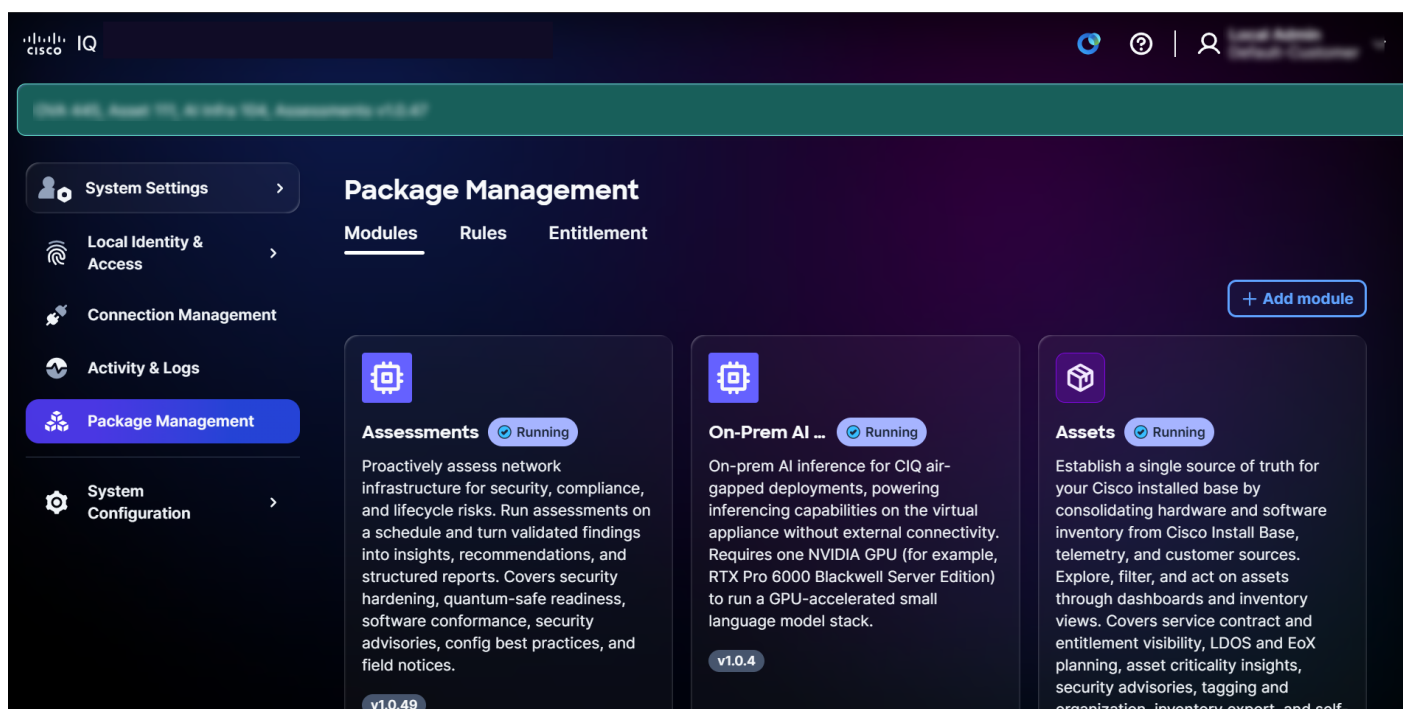
7. [Next] をクリックします。Update Summaryが表示されます。

 注：リリースノートには、「アップデートの概要」からアクセスできます。

8. Update Moduleをクリックし、Moduleタブに移動します。モジュールに「スケジュールされた更新」ステータスが表示されます。

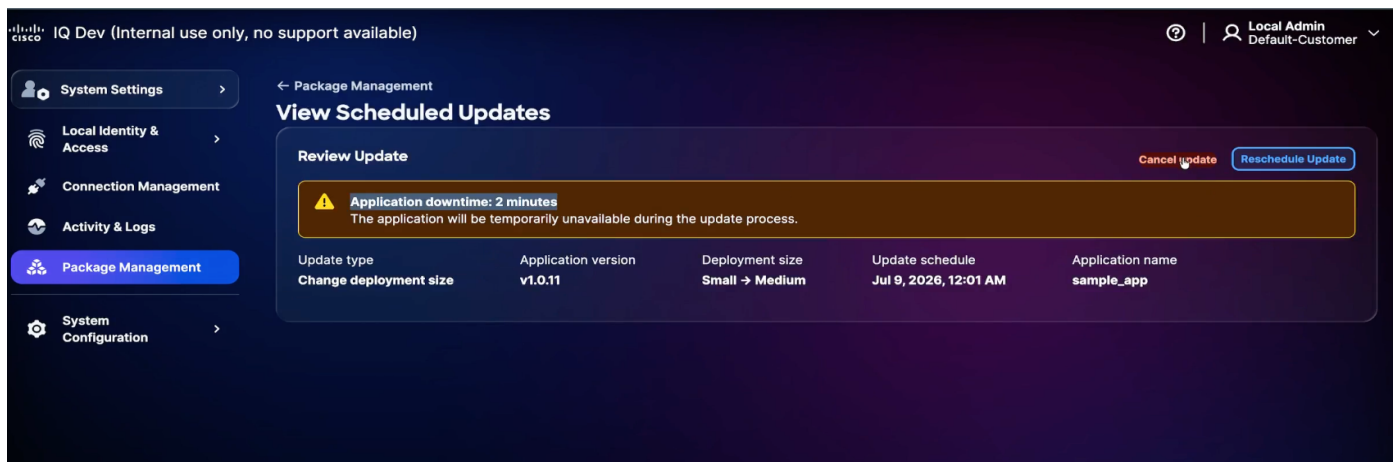
スケジュールの編集

スケジュールされた更新を表示、編集、またはキャンセルすることもできます。スケジュール済の更新を編集またはキャンセルするには、次の手順に従います。



スケジュールの編集

1. Package Managementページで、目的のモジュールのManage > View Scheduled updateの順にクリックします。View Scheduled Updatesウィンドウが表示されます。



スケジュールの更新

2. 必要に応じて、Cancel UpdateまたはReschedule Updateをクリックします。
3. 画面に表示される手順に従って、操作を完了します。

 注：モジュールの操作（インストール、アップグレード、サイズ変更など）が失敗した場合は、次のいずれかのオプションを選択します。

再試行: UIに「再試行」ボタンが表示され、操作を再試行できます。ログ：エラーが引き続き発生する場合は、ログをクリックして詳細な診断情報を表示します。これは、インストールまたはランタイムエラーの原因を特定するための主要な方法です。

ルールのインストール

ルールは、既存のモジュールの機能を拡張または変更する特殊なコンポーネントまたは「アドオン」です。ルールは、スタンドアロンのプログラムとして動作するように設計されていません。特定のルール、ロジック、または機能を提供するためにモジュールに「接続」されます。ルールは特定のモジュールに関連付けられます。ルールがインストールされると、そのルールはサポートするモジュールにリンクされます。ルールにより、コアモジュールを完全にアップグレードしなくても、システムを更新またはカスタマイズできます。新しいルールまたは機能のセットが必要な場合は、既存のモジュールに新しいルールを追加するだけです。

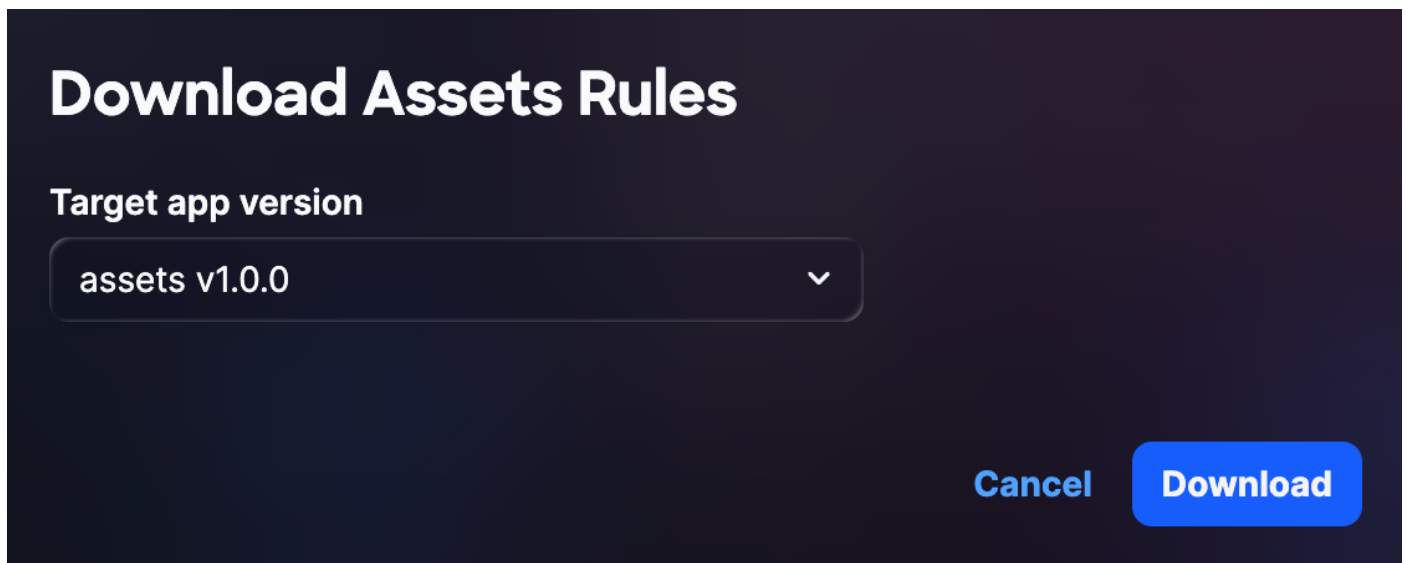
ルールをダウンロードするには、次の手順を実行します。

1. [Cisco IQ](#)にログインします。
2. System Settings > Package Catalogの順に移動します。

3. 目的のルールカードで、Downloadをクリックします。



注意：次の例は、「資産」ルールを示しています。



ダウンロード

4. ドロップダウンリストからターゲットアプリケーションバージョンを選択します。

5. Downloadをクリックして、ファイルをローカルに保存します。



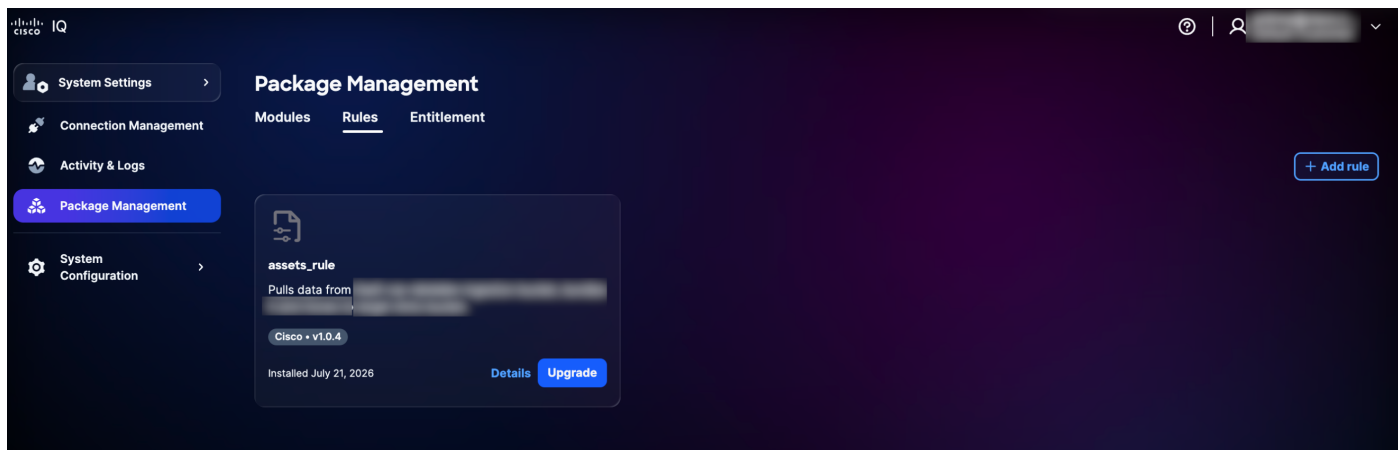
注：インストールファイルが大きいため(10 ~ 25 GB)、ダウンロードする前に十分なディスク領域があることを確認してください。

6. VAに移動します。

7. Home > System Settings > Package Managementの順に移動します。Package Managementページが表示され、次のタブが表示されます。

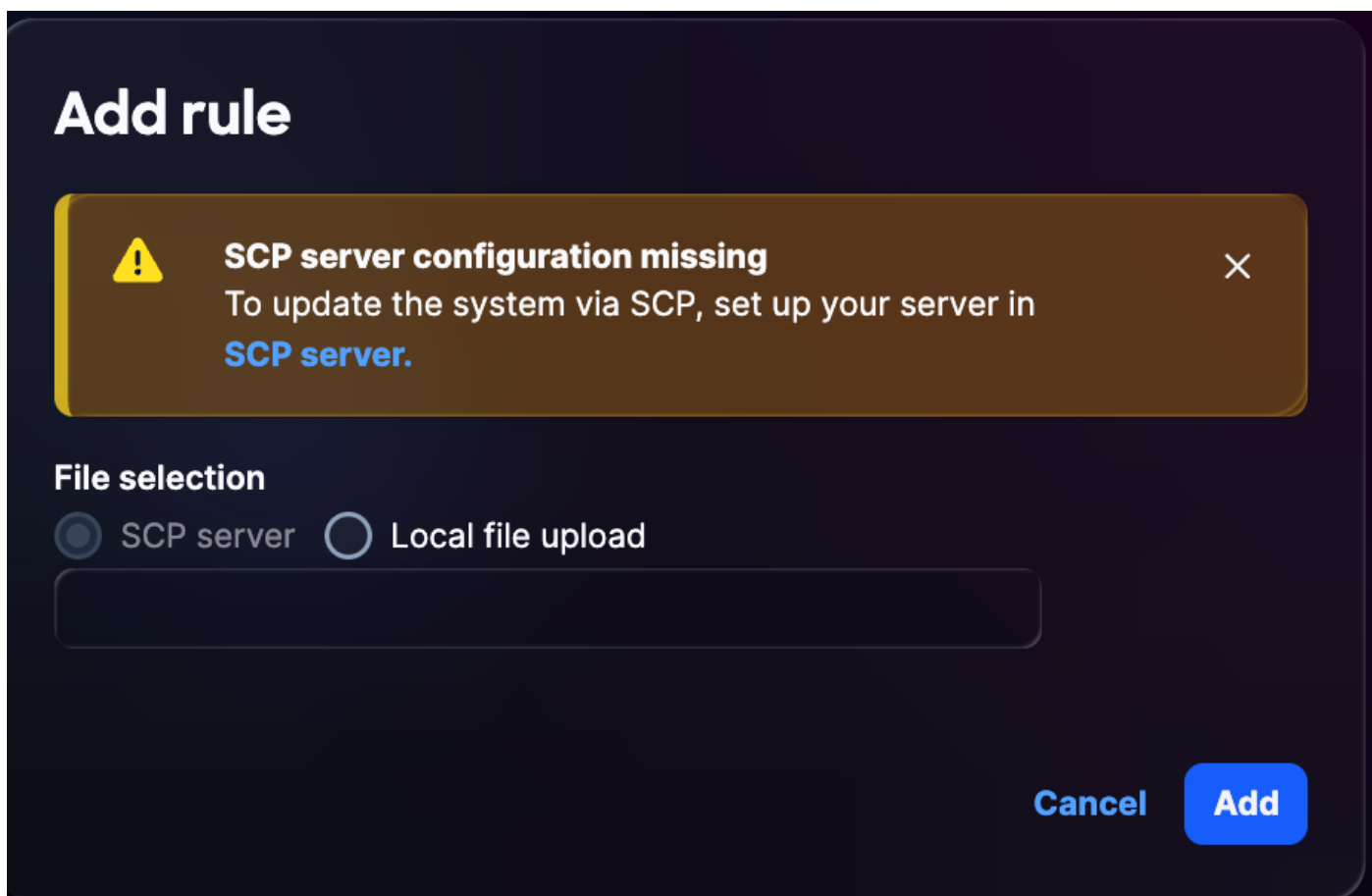
- Modules
- ルール
- 権利

8. Rulesタブをクリックします。



パッケージ管理

9. [Add Rule] をクリックします。



ルールの追加

10. 希望するファイル選択オプションを選択します。

- Secure Copy Protocol(SCP)サーバ：インストールパッケージの正確なファイル名を入力し

ます。この方法は、サイズの大きいファイルに推奨されます。

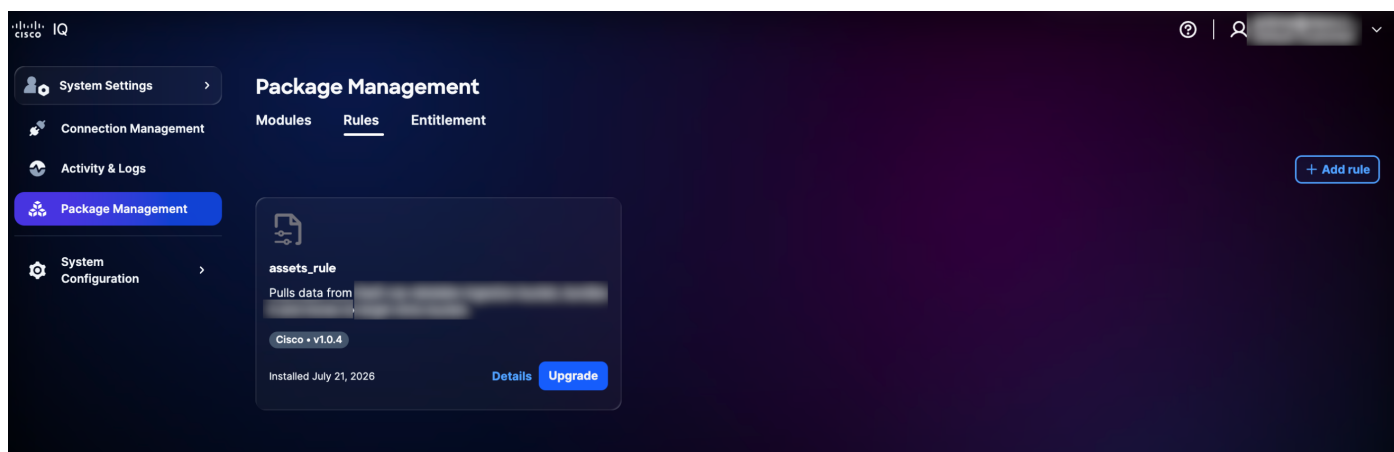
- ローカルファイルのアップロード：ダウンロードしたインストールファイルをドラッグアンドドロップします。

11. [Add] をクリックします。追加した規則が「パッケージ管理」に表示されます。

ルールのアップグレード

ルールをアップグレードするには：

1. VAでSystem Settings > Package Managementの順に移動します。



アップグレード

2. 目的のルールで、Upgradeをクリックします。Upgrade Ruleウィンドウが開きます。

Upgrade Rule

File selection

☒ SCP server ☐ Local file upload

Cancel

Add

アップグレードルール

3. 希望するファイル選択オプションを選択します。

- Secure Copy Protocol(SCP)サーバ：インストールパッケージの正確なファイル名を入力します。この方法は、サイズの大きいファイルに推奨されます。
- ローカルファイルのアップロード：ダウンロードしたインストールファイルをドラッグアンドドロップします。

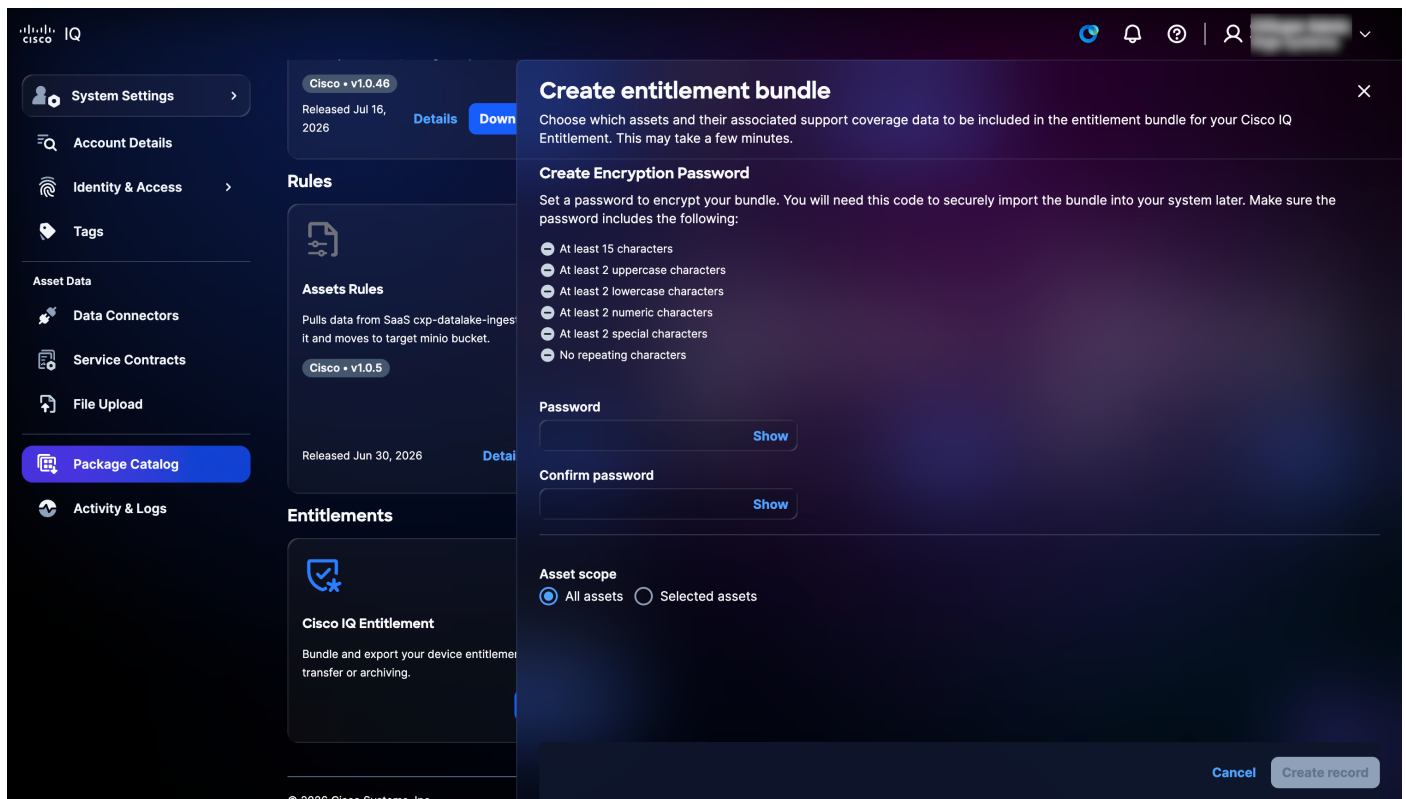
4. [Add] をクリックします。

 注：これらのルールは、定期的なデバイステレメトリの収集時に適用されます。すぐに適用できるように、デバイステレメトリ収集を手動で開始できます。

権利のインストール

権限付与では、特定のソフトウェア機能、モジュール、またはサービスを使用する組織の権利を検証します。権限をインストールするには、次の手順に従います。

1. [Cisco IQ](#)にログインします。
2. System Settings > Package Catalogの順に移動します。
3. 資格カードで、Create recordをクリックします。「エンタイトルメントバンドルの作成」ウィンドウが開きます。



権利バンドルの作成

4. password を入力します。画面に表示されるパスワード作成ルールを参照してください。
5. 「パスワードの確認」に同じパスワードをもう一度入力します。
6. 適切なAsset scopeオプションボタンを選択します。
 - すべての資産：自分にリンクされているすべての資産が含まれます。
 - 選択したアセット：環境に合わせて特定のデバイスを選択できます。このオプションを選択した場合は、該当するすべてのアセットのチェックボックスをオンにします
7. Create recordをクリックして、ファイルをローカルに保存します。

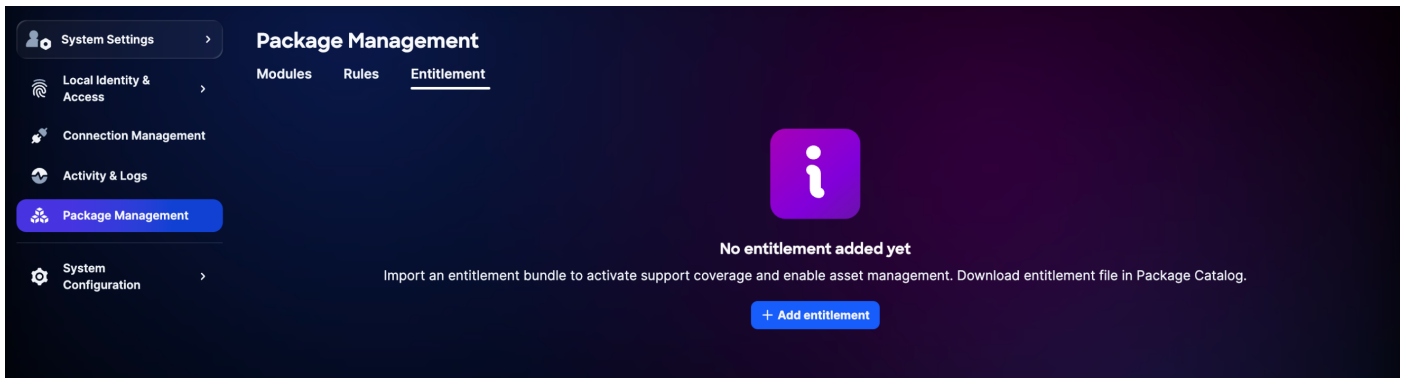
 注：エンタイトルメントバンドルを作成した後は、現在の画面から移動しないでください。別のページに移動すると、バンドルが無効になるため、バンドルを再生成してダウンロードオプションを有効にする必要があります。

 注：インストールファイルが大きいため(10 ~ 25 GB)、ダウンロードする前に十分なディスク領域があることを確認してください。

8. VAにログインします。
9. Home > System Settings > Package Managementの順に移動します。「パッケージ管理」ページには、次のタブがあります。

- Modules
- ルール
- 権利

10. Entitlementsタブをクリックします。



「資格」タブ

11. Add Entitlementをクリックします。

Add Entitlement

File selection

☒ SCP server
 ☐ Local file upload

Decrypt Entitlement Bundle

Enter the entitlement decryption password.

Password *

Enter password

Show

Cancel

Add

権限の追加

12. 希望するファイル選択オプションを選択します。

- Secure Copy Protocol(SCP)サーバ：インストールパッケージの正確なファイル名を入力します。この方法は、サイズの大きいファイルに推奨されます。
- ローカルファイルのアップロード：ダウンロードしたインストールファイルをドラッグアンドドロップ

13. password を入力します。

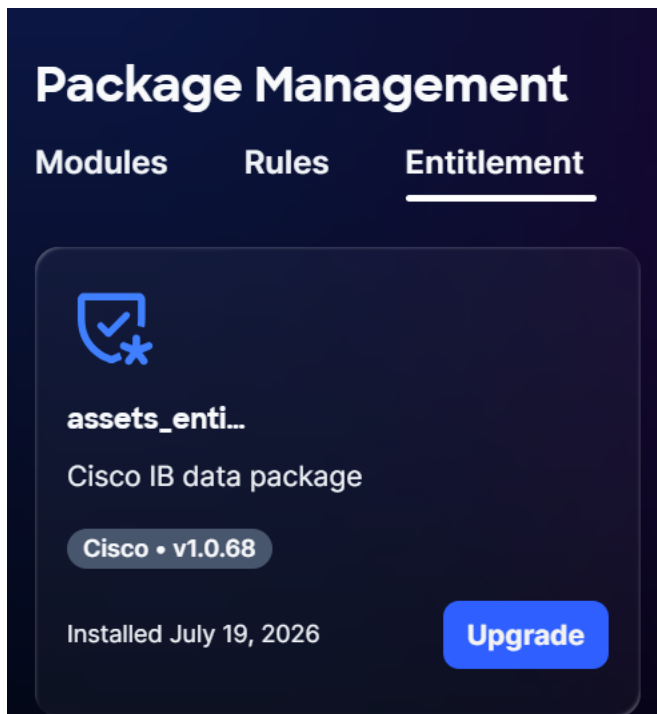
14. [Add] をクリックします。新しくインストールされた権限付与が、Package ManagementのEntitlementタブに表示されます。

15. 権限を有効にするには、権限を追加してから5 ~ 10分待ってから、デバイステレメトリ収集を開始します。

 注：権限付与プロセスでサービス契約を追加すると、その契約にリンクされているすべてのデバイスがオンプレミスデバイスの資産インベントリに追加されます。デバイスをシリアル番号でフィルタリングしたり、複数のアカウントIDを使用したり、特定のデバイスを選択してエンタイトルメントを管理したりすることができます。

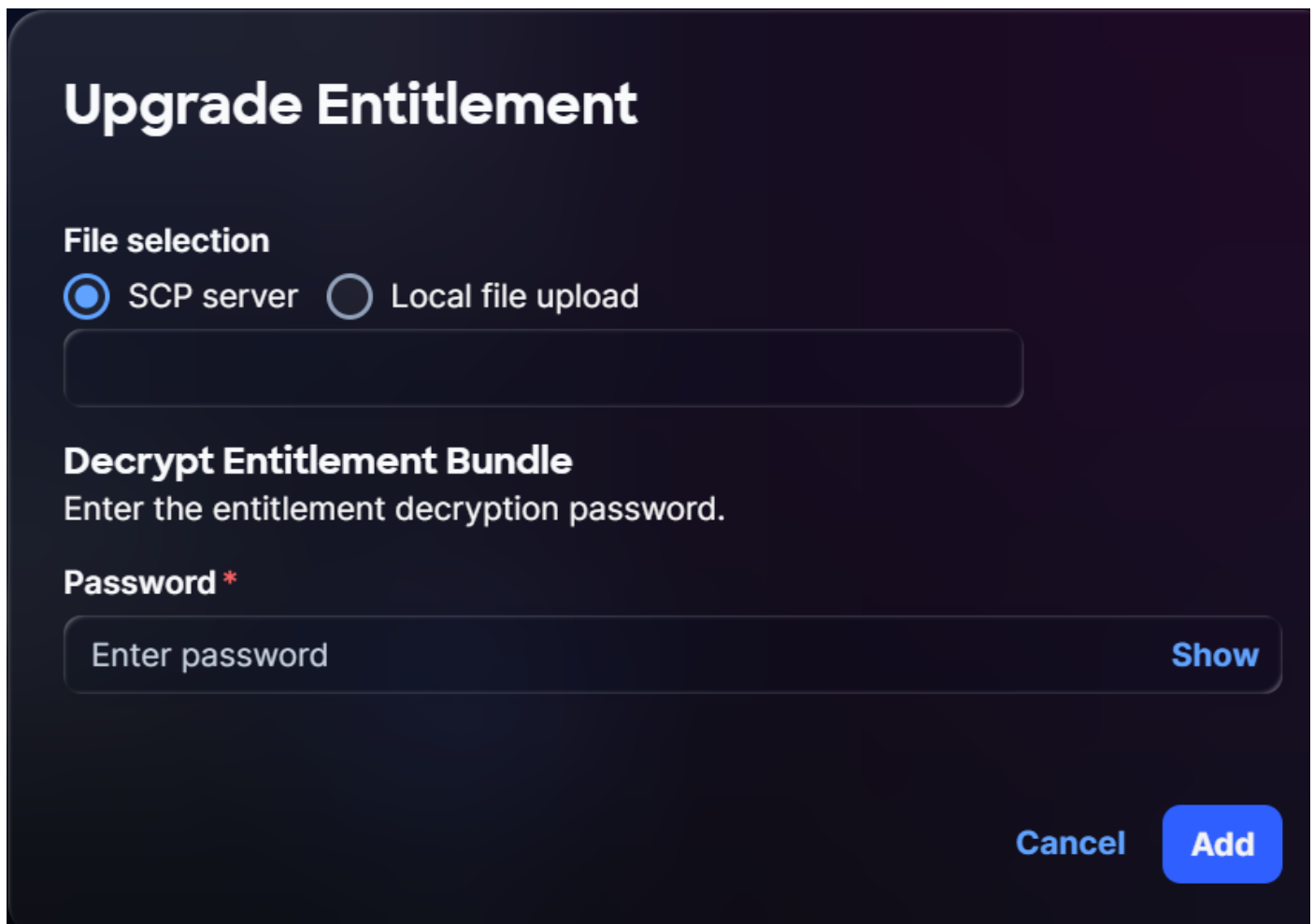
権利のアップグレード

権限をアップグレードするには、次の手順に従います。



権限付与のアップグレード

1. 必要なEntitlementでUpgradeをクリックします。



アップグレード権限

2. 希望するファイル選択オプションを選択します。

- Secure Copy Protocol(SCP)サーバ：インストールパッケージの正確なファイル名を入力します。この方法は、サイズの大きいファイルに推奨されます。
- ローカルファイルのアップロード：ダウンロードしたインストールファイルをドラッグアンドドロップ

3. password を入力します。

4. [Add] をクリックします。

AIを活用した機能

オンプレミスAI推論インフラストラクチャモジュールは、VAのオンプレミスAIを活用した機能を実現します。ローカルでSmall Language Model(SLM)を実行し、AIを利用したプロンプトにシステムが応答できるようにします。インストール後は、VAインターフェイス内で直接やり取りできます。

次のクエリタイプがサポートされています。

- 資産：耐用年数の終了、ソフトウェアの通貨または不適合、セキュリティの脆弱性、および契約のギャップが原因でリスクが生じている資産を特定します。
- インベントリ：インベントリ内の資産に関するAI駆動型分析を要求します。

On-Prem AI Inference Infrastructureインストールパッケージは、Cisco IQ Package Catalogから入手でき、Assetsなどの他のモジュールと同じ方法で配布されます。

 注：オンプレミスAI推論インフラストラクチャは、一度に1つのGPUだけで実行できます。インストールが完了するまでに、約40 ~ 45分かかります。インストールファイルが大きい（約30 GB）。ダウンロードする前に十分なディスク領域があることを確認してください。

オンプレミスAI推論インフラストラクチャの前提条件

オンプレミスAI推論インフラストラクチャをインストールする前に、次の条件を満たす必要があります。

- VAにはGPUアクセスを備えたVMが必要です。SLMはGPUを必要とし、GPUなしでは実行

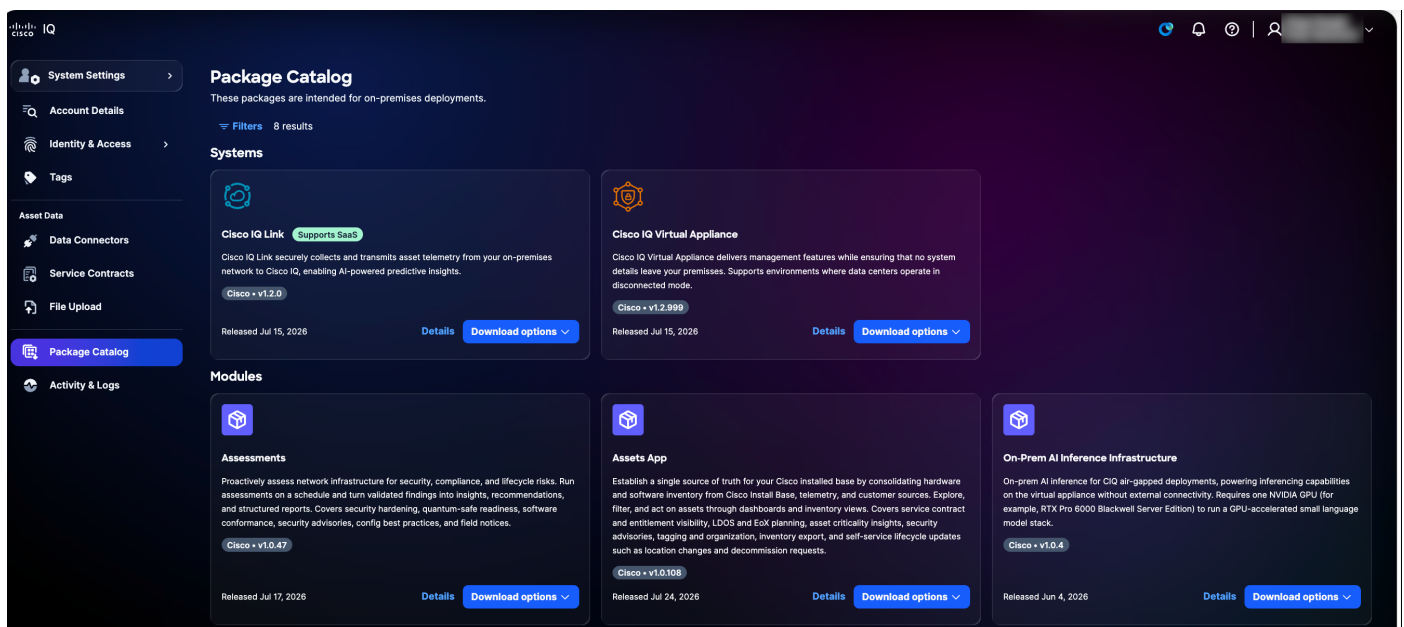
できません

- GPU VMには、80 GB以上のGPU VRAMが必要です

オンプレミスAI推論インフラストラクチャのインストール

オンプレミスAI推論インフラストラクチャをVAにインストールするには、Cisco IQ SaaSからオンプレミスAI推論インフラストラクチャモジュールをダウンロードします。

1. [Cisco IQ](#)にログインします。
2. System Settings > Package Catalogの順に移動します。



パッケージのインストール

3. オンプレミスAI Inference Infrastructureカードで、Download options > Installation packagesの順にクリックします。Download Applicationウィンドウが開きます。

Download On-Prem AI Inference Infrastructure

System version

System vv1.2.0



Build type

Release



Application version

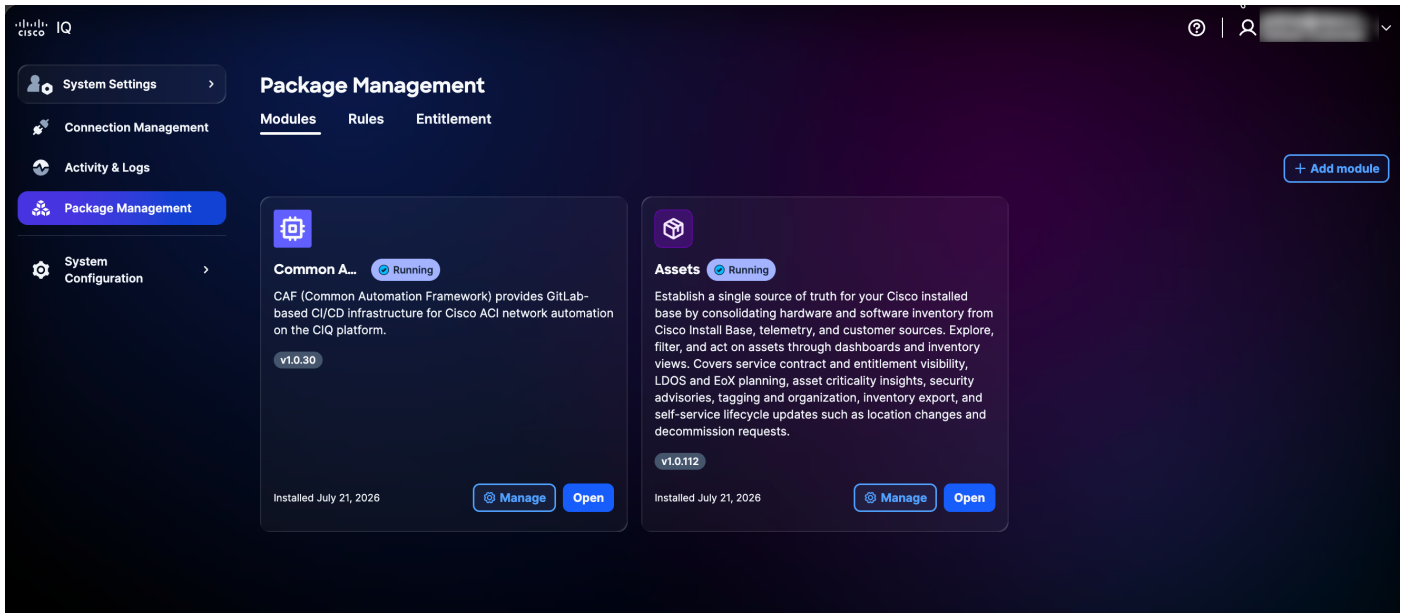
1.0.4

Cancel

Download

AI推論インフラのダウンロード

4. ドロップダウンリストからシステムバージョンを選択します。
5. ドロップダウンリストから構築タイプを選択します。
6. [Download] をクリックします。
7. VAに移動します。

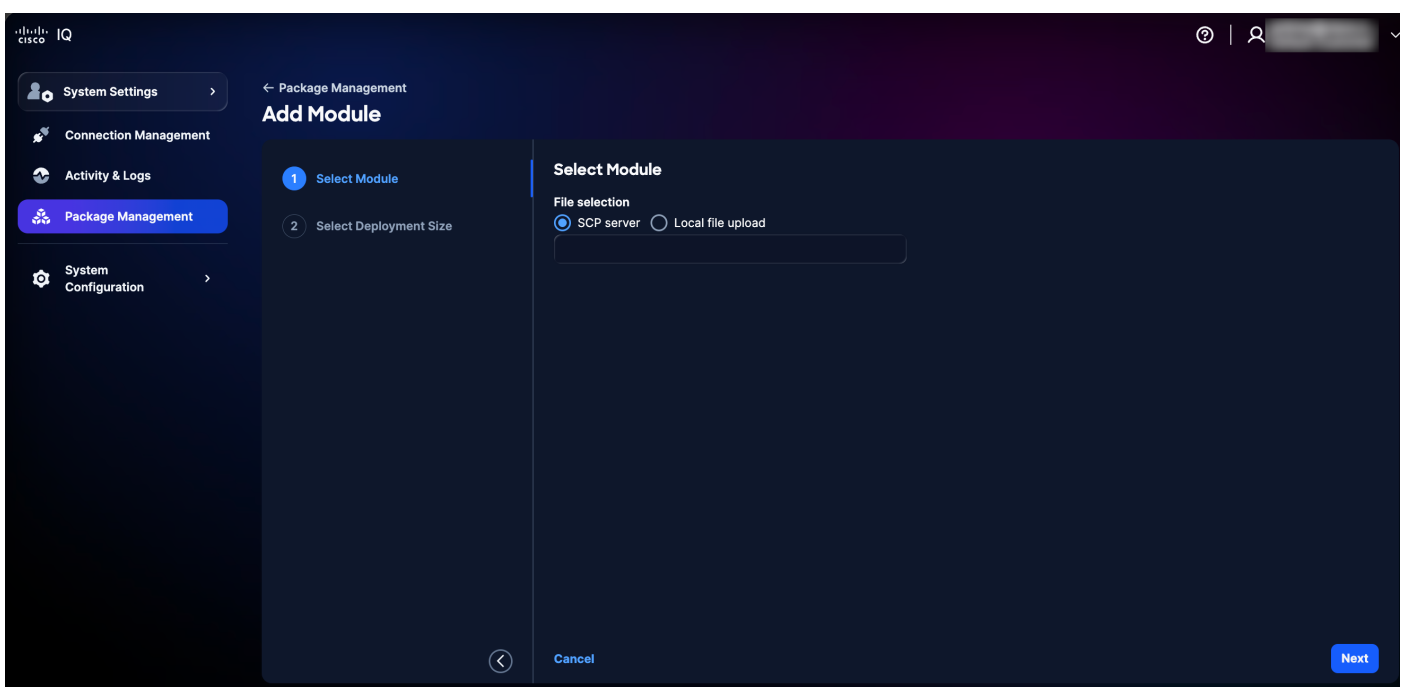


パッケージ管理

8. Home > System Settings > Package Managementの順に移動します。「パッケージ管理」ページが表示され、次のタブが表示されます。

- Modules
- ルール
- 権利

9. Modulesタブで、Add modulesをクリックします。



モジュールの選択

10. 希望するファイル選択オプションを選択します。

- SCPサーバ：インストールパッケージの正確なファイル名を入力します（大きなファイルの場合に推奨）。
- ローカルファイルのアップロード：ダウンロードしたインストールファイルをドラッグアンドドロップします（アップロード時間が30 GB以上のファイルには推奨されません）。注：ローカルファイルのアップロード方式には、20分のしきい値があります。アップロードプロセスがこの期間を超えると、インストールは失敗します。SCPサーバの使用は、正常で安定したインストールを保証するための推奨される方法です。

11. [Next] をクリックします。ファイルのアップロードが開始されます。

12. 導入サイズ（小、中、大など）を選択します。

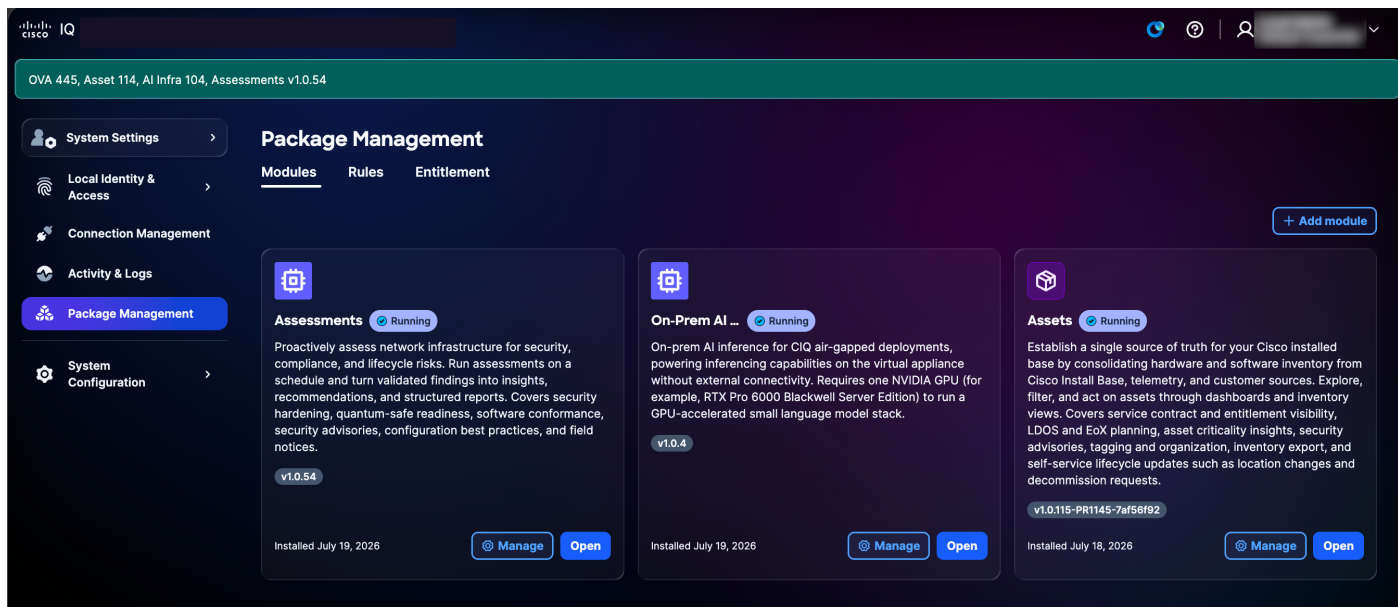
13. Add Moduleをクリックします。インストールが開始され、完了するまでに約40 ～ 45分かかります。

インストールが完了すると、オンプレミスAI推論インフラストラクチャがパッケージ管理のモジュールタブに表示されます。

 注：各GPUで実行できるオンプレミスAI推論インフラストラクチャモジュールは1つだけです。このモジュールはGPU VRAMの約90%を使用します。同じGPUに追加インスタンスをインストールすることはサポートされていません。

オンプレミスAI推論インフラストラクチャモジュールの管理

インストールが完了すると、オンプレミスAI推論インフラストラクチャモジュールは、Package ManagementのApplicationsタブで管理できます。



AI推論インフラストラクチャの編集

モジュールを管理するには、オンプレミスAI推論インフラストラクチャモジュールの横にある管理をクリックします。詳細は、『[モジュールの管理](#)』を参照してください。

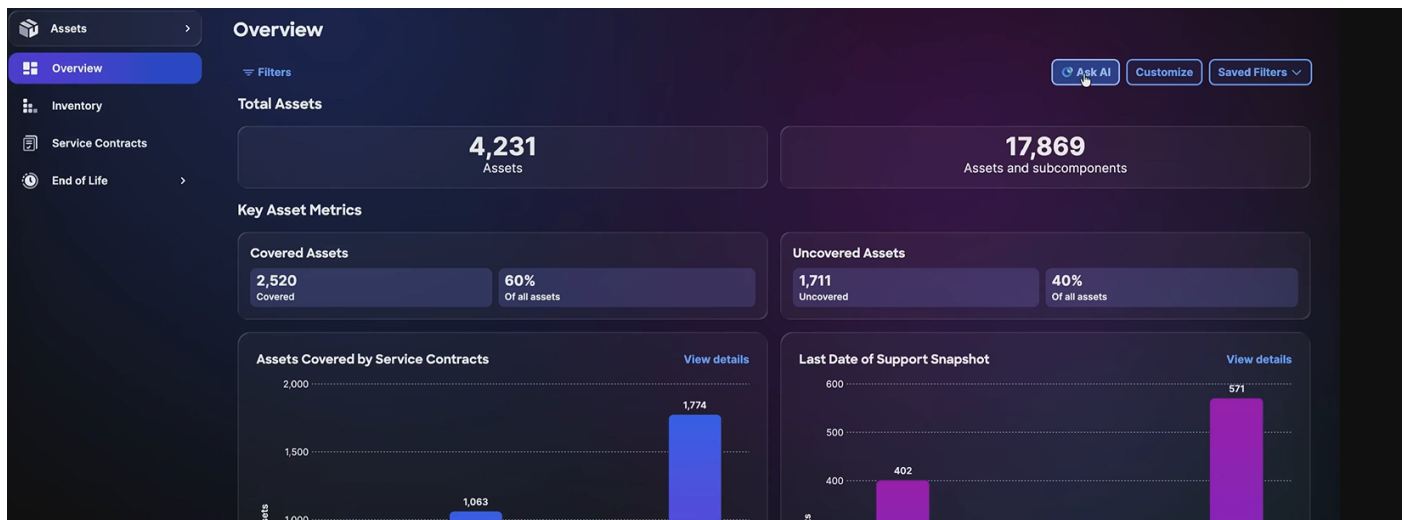
AIを活用した機能の活用

オンプレミスAI推論インフラストラクチャモジュールが正常にインストールされると、VAインターフェイスでAsk AIボタンが使用可能になります。

資産にAIを求める

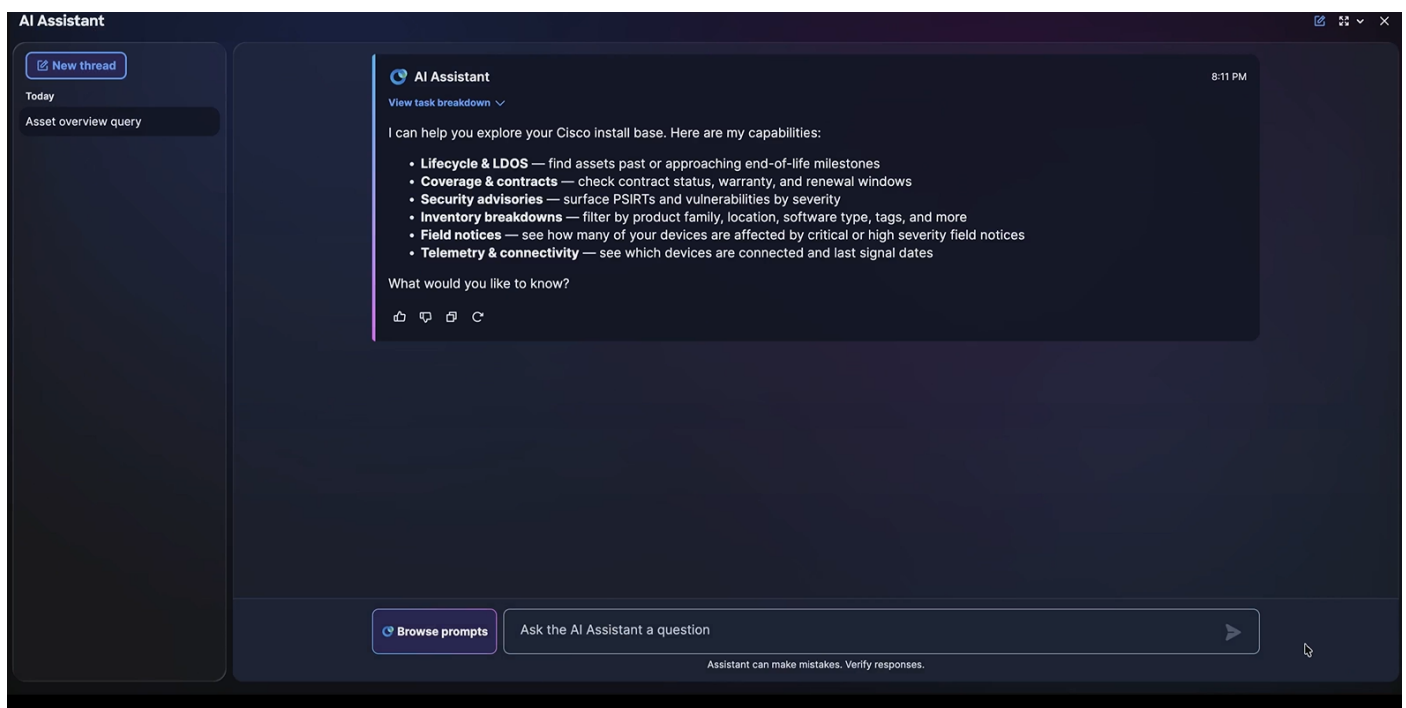
アセットでAsk AIを使用するには：

1. Homeメニュー> Assetsの順に選択する。Assetsページが表示されます。



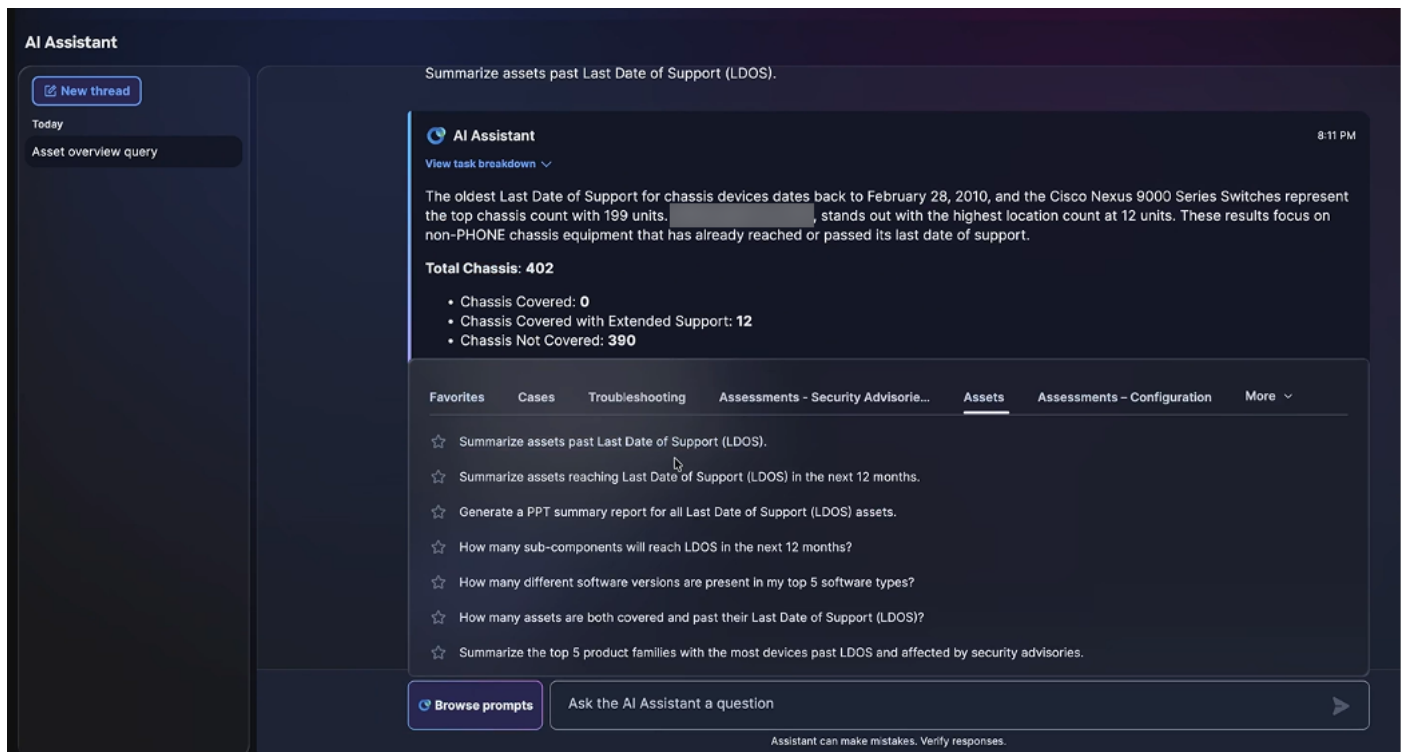
「資産」ページ

2. Ask AIをクリックします。オンプレミスAI推論インフラストラクチャが起動します。



プロンプトの参照

3. Browse promptsをクリックして使用可能なプロンプトを表示するか、Ask the AI Assistant a questionフィールドにカスタム質問を入力します。



プロンプトのセット

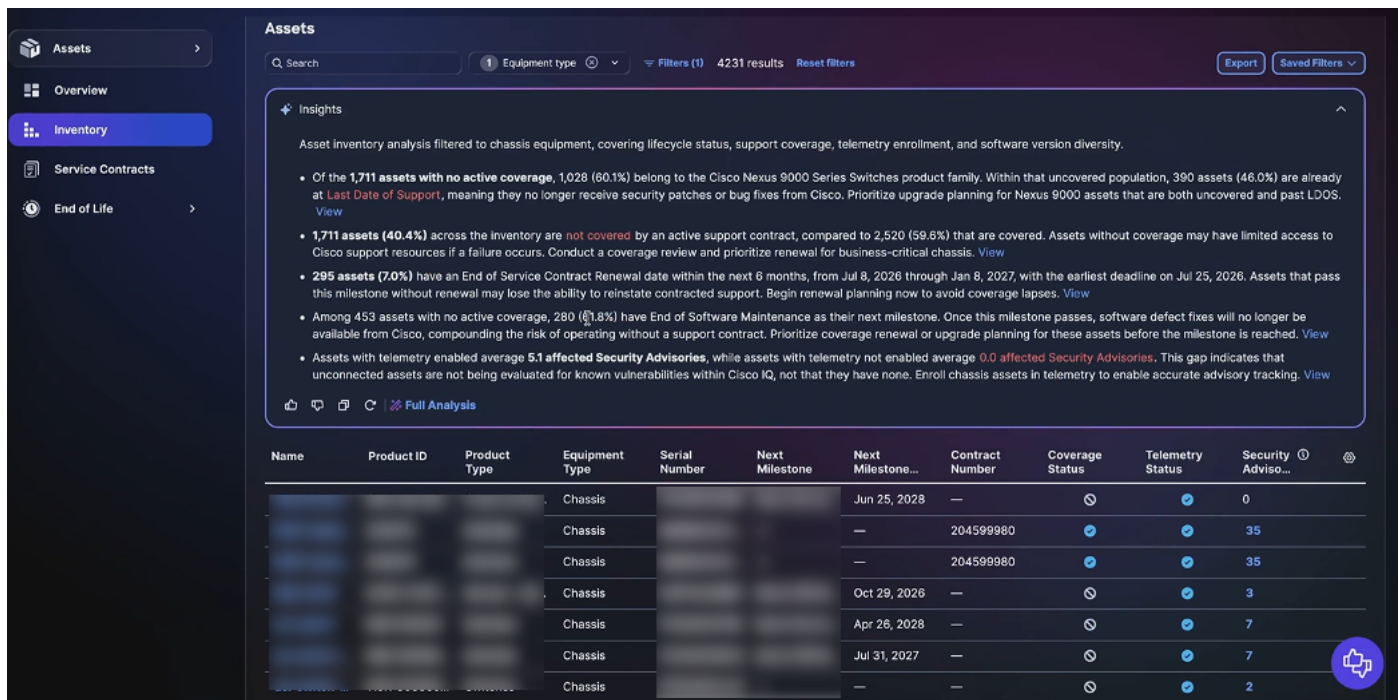
4. 目的のプロンプトをクリックするか、Enterキーを押します。オンプレミスSLMが応答を生成します。

インベントリにおけるAI分析

オンプレミスAI推論インフラストラクチャモジュールは、インベントリセクションで自動化されたAI駆動分析を提供します。インベントリデータが入力されると、分析結果が自動的に表示されます。

InventoryでAI分析を表示するには、次の手順に従います。

1. Homeメニュー> Inventoryの順に選択します。Inventoryページが表示されます。



インベントリ

2. AIで生成された解析を表示します。データが使用可能になると、結果がインベントリレビューに表示されます。

 注：グラフ、ダッシュボード、グラフなどの追加の情報を提供する視覚化については、「完全分析」をクリックしてください。

モジュールの共通機能

このセクションでは、すべてのモジュールで共有されるコア機能について詳しく説明します。これらの機能により、一貫したユーザエクスペリエンス、システムパフォーマンスの最適化、管理ワークフローの合理化が実現します

データの分析

インサイトパネルには、そのページのデータに対するAI駆動型の分析が表示され、ネットワーク環境のセキュリティと健全性を向上させるための実用的なインサイトが提供されます。

 注：分析機能は、選択したページでのみ使用できます。

Assets

Q Search Product family Product ID Location Tags Filters (1) 1716 results Reset filters Export

Insights

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

Full Analysis

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

インサイト・パネル

インサイトパネルでは、次のオプションを使用できます。

- Expandアイコンをクリックしてパネルを展開し、追加の洞察を表示します
- AIで生成された情報に関するフィードバックを表示するには、サムズアップまたはサムズダウンアイコンをクリックします
- Full Analysisをクリックすると、詳細情報、より詳細な分析、グラフ、ダッシュボード、チャートなどの可視化が表示されます

Security Advisories by Coverage Status



This donut chart compares security advisories between devices with active coverage and those without.

KEY INSIGHT

Devices that are **NOT COVERED** account for **6,046 security advisories**, representing **23%** of the total exposure despite being a smaller portion of the inventory.



完全な分析

完全解析では、以下のオプションを使用できます。

- Download PDFをクリックして、分析のオフラインコピーを記録用または共同作業用に保存します

情報のエクスポート

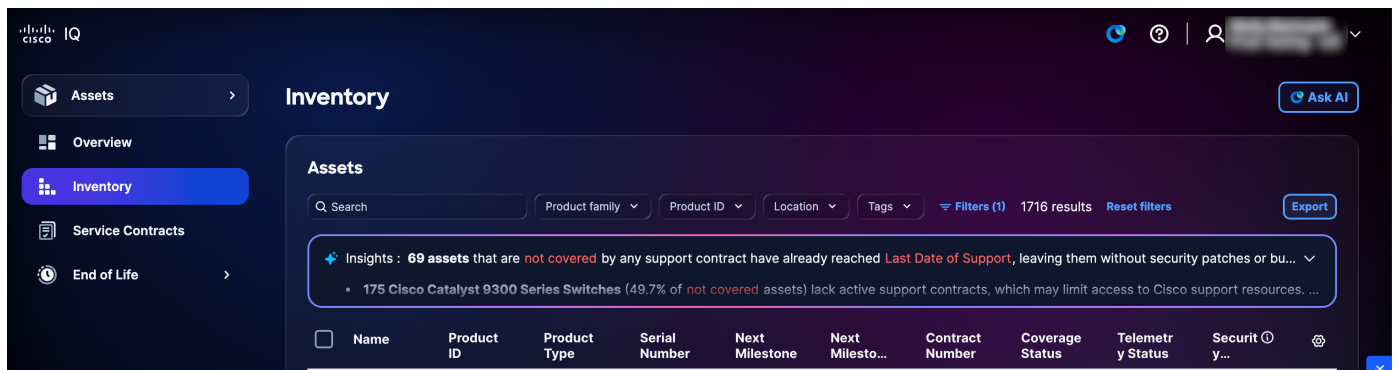
エクスポート機能を使用すると、アセットおよびセキュリティ情報のカスタムビューを.xlsまたは.csv形式でエクスポートできます。



注：エクスポート機能は、選択したページでのみ使用できます。

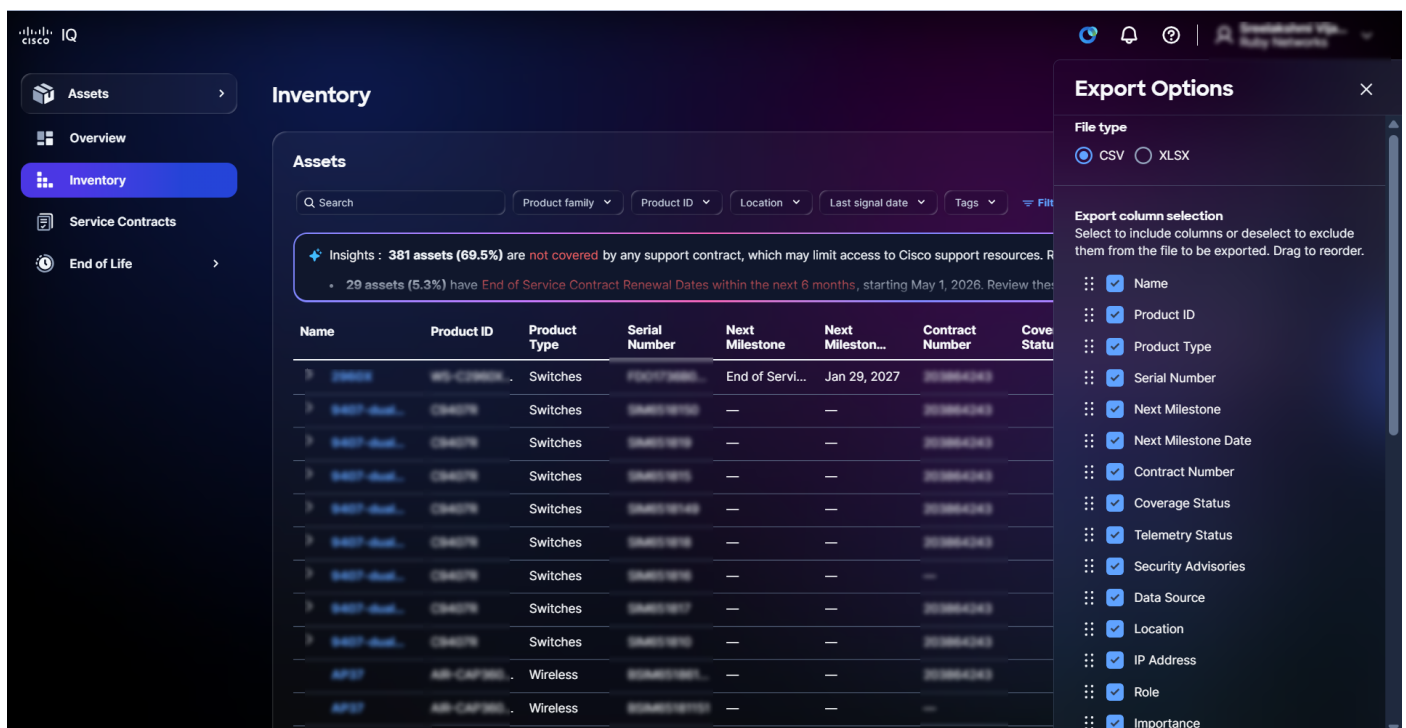
ページから情報をエクスポートするには、次の手順に従います。

1. ページに移動します。



資産モジュールでの在庫のエクスポート

2. [Export] をクリックします。エクスポートオプションが表示されます。



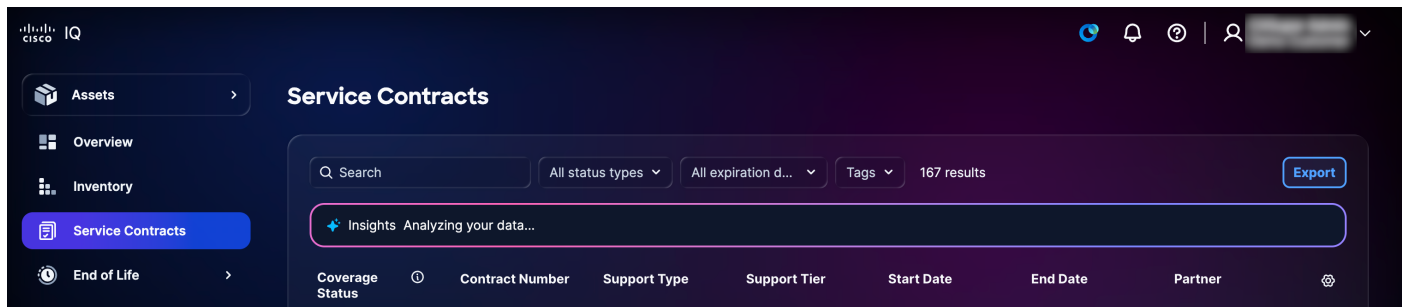
エクスポートオプション

3. ファイルタイプを選択します。
4. 該当する列のチェックボックスをオンにします。
5. [Export] をクリックします。ファイルはブラウザのローカルダウンロードフォルダにダウン

ロードされます。

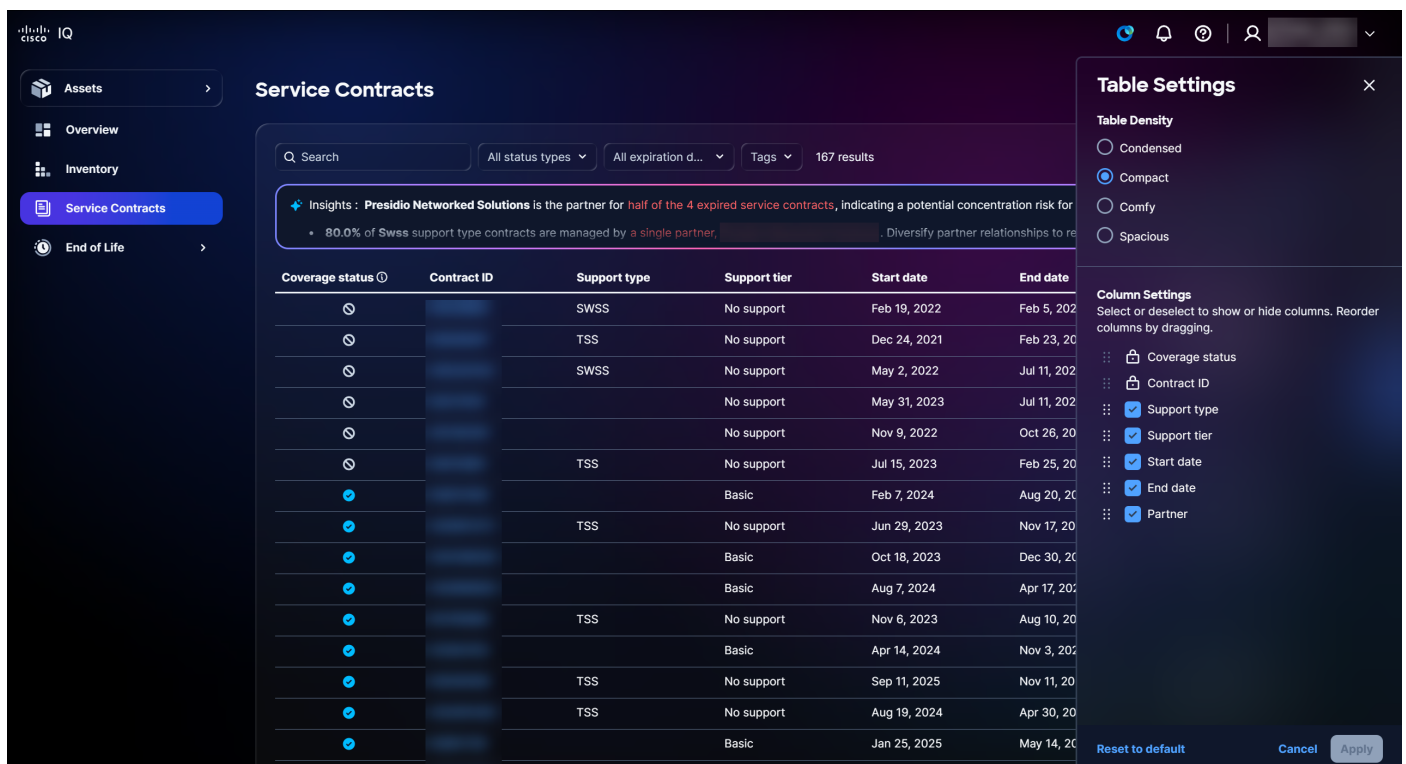
テーブルの設定

テーブル設定を構成して、さまざまなモジュール機能に対してカスタムビューおよび調整されたビューを作成できます。



テーブルの設定

選択したページに表示される列を変更するには、テーブル設定アイコンをクリックします。テーブル設定が表示されます。



テーブル設定オプション

テーブルビューの変更

テーブルビューを変更するには、次の手順を実行します。

1. 次の「テーブル密度」オプションのいずれかを選択します。
 - 簡潔：視覚要素とスペースを最小化して、詳細情報を表示します。
 - コンパクト：空白を減らし、UI要素間の間隔を狭めます。
 - Comfy：エレメント間のスペースを広く取ります。
 - 広い：豊富なホワイトスペースと大きなUI要素を重視
2. [APPLY] をクリックします。

列の追加と削除

列を追加または削除するには

1. Column Settingsチェックボックスをオンまたはオフにします。
2. [APPLY] をクリックします。



注：テーブルビューからName列を削除することはできません。

列の順序の変更

列の順序を変更するには：

1. 列名をドラッグアンドドロップして、項目を目的の順序に並べ替えます。
2. [APPLY] をクリックします。

ダッシュボードのカスタマイズ

カスタムダッシュボード機能を使用すると、直感的な一連のカスタマイズオプションを使用して標準ダッシュボードをカスタマイズできます。

- ・ドラッグアンドドロップ機能を使用したダッシュボードウィジェットまたはパネルの再配置
- ・ワークフローに関係のないコンポーネントを削除します
- ・パーソナライズされたダッシュボードレイアウトはユーザプロファイルに安全に保存され、すべてのセッションとデバイスに自動的に適用されます
- ・簡単なリセットオプションで元のダッシュボードレイアウトを復元

ダッシュボードをカスタマイズするには、次の手順に従います。

1. ダッシュボードに移動します。



カスタマイズ

2. [Customize] をクリックします。



ダッシュボードの編集

3. 必要に応じてダッシュボードを変更します。

- 再配置：ウィジェットを目的のレイアウトにドラッグアンドドロップします
- 削除：ウィジェットを削除するには、削除アイコンをクリックします
- リセット：ダッシュボードを元のレイアウトにリセットするには、[デフォルトにリセット]をクリックします

4. [Save] をクリックします。Dashboard Savedメッセージが表示されます。

ダッシュボードレイアウトは、すべてのセッションとデバイスに自動的に適用されます。

フィルタのカスタマイズ

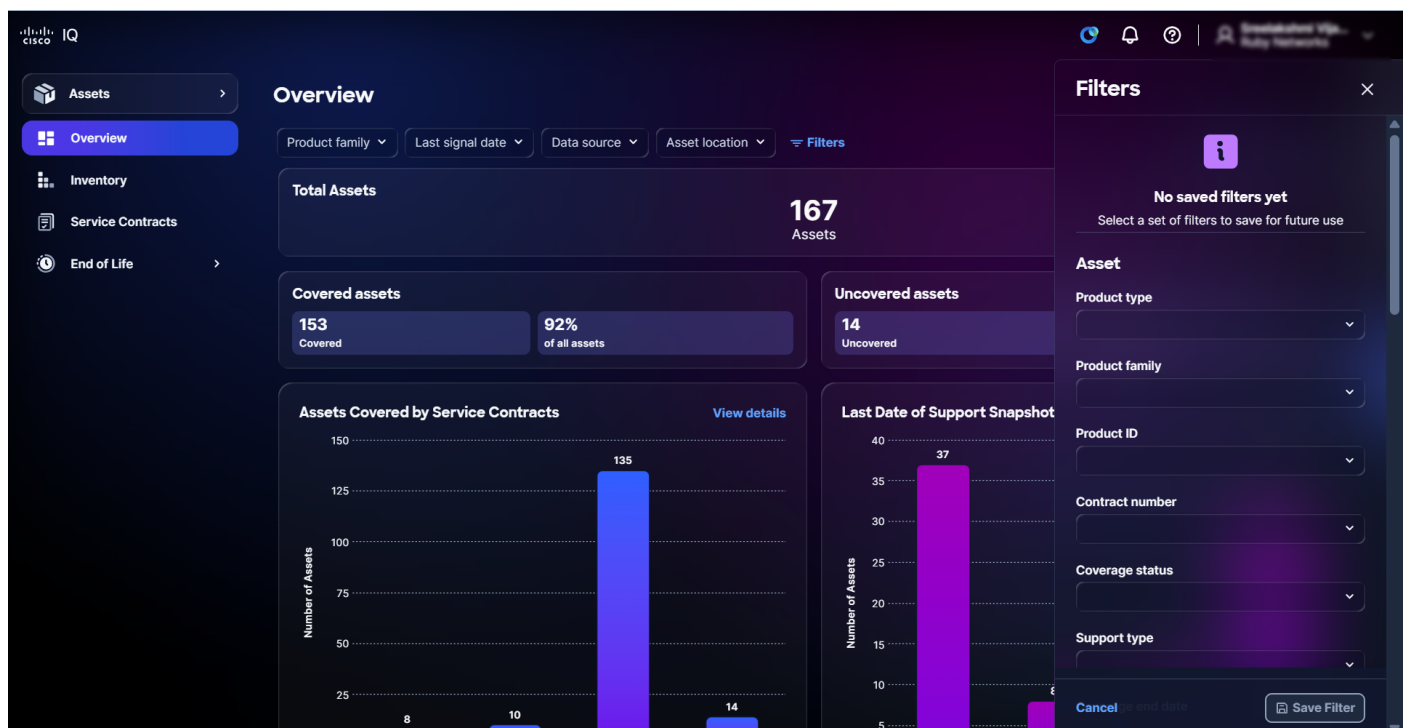
任意のダッシュボードビューのカスタムフィルタ設定を保存できるため、必要に応じて簡単に好みの設定に戻すことができます。すべてのフィルタ設定は、ユーザ単位、アカウント単位で安全

に保存され、Cisco IQにアクセスするたびにパーソナライズされた一貫したエクスペリエンスが確保されます。

フィルタの作成

カスタムフィルタを作成するには、次の手順を実行します。

1. ダッシュボードに移動します。
2. Filtersをクリックします。



フィルタ

3. ドロップダウンリストから目的のフィルタを選択します。
4. Save Filterをクリックします。「保存済みフィルタに名前を付ける」ウィンドウが開きます。

Name saved Filter

Filter name *

Custom Filter |

Cancel

Save Filter

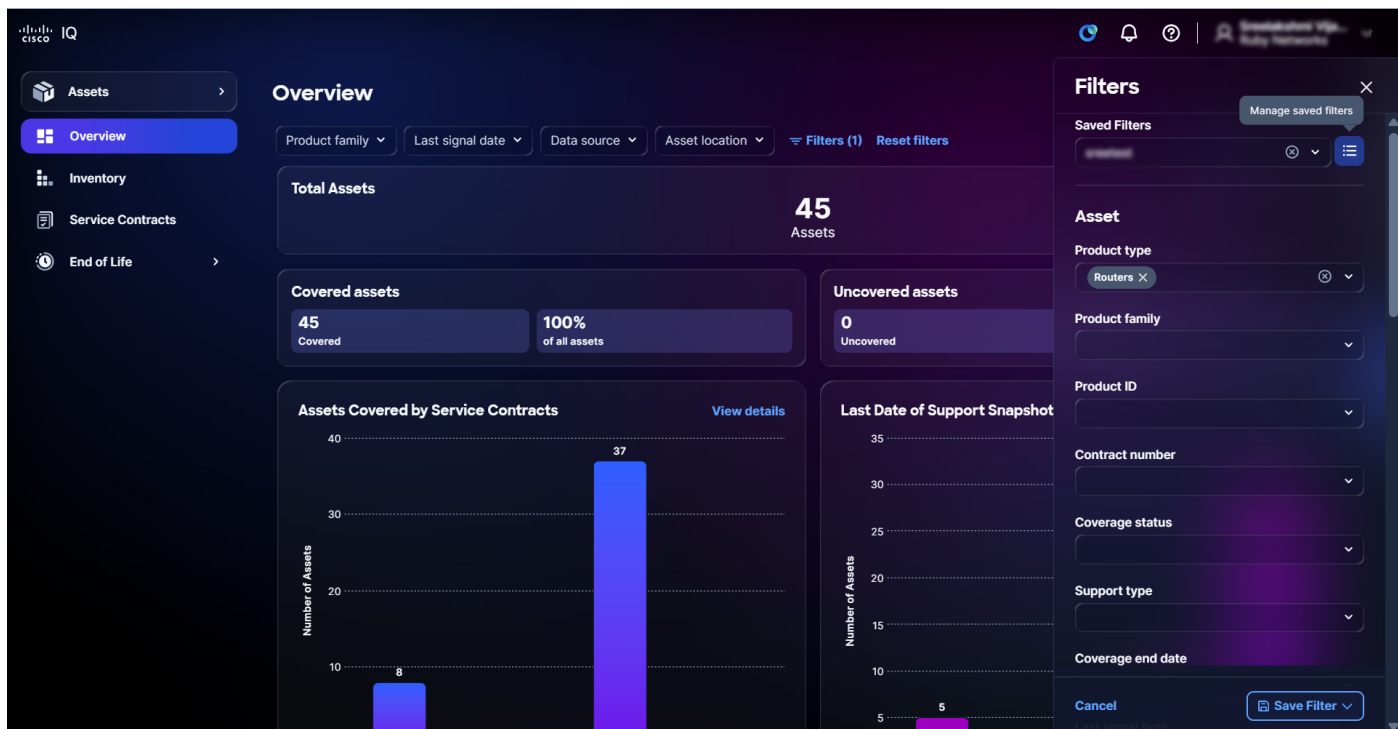
フィルタ名

5. フィルタ名を入力します。
6. Save Filterをクリックして確定します。

フィルタ名の編集

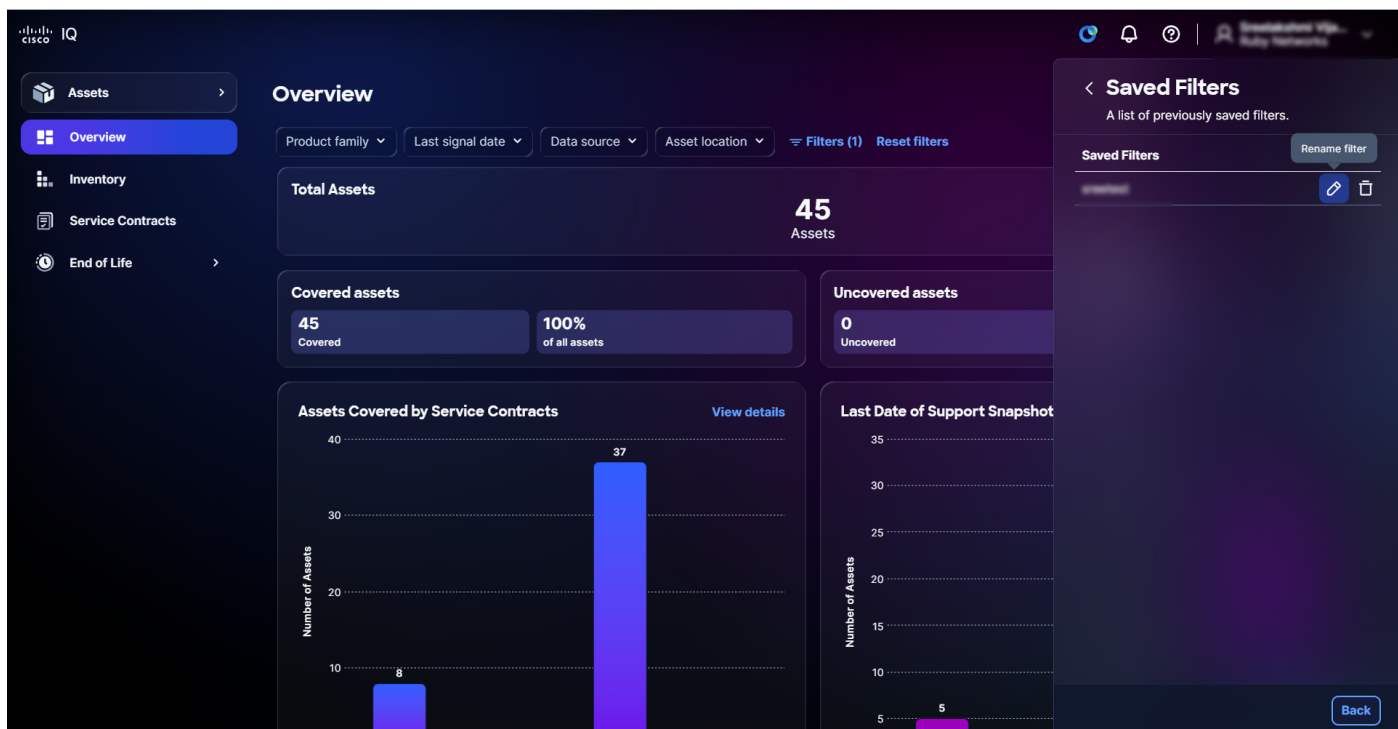
カスタムフィルタを編集するには、次の手順を実行します。

1. Filtersをクリックします。



保存済みフィルタの管理

2. [保存済みフィルタの管理]アイコンをクリックします。
3. フィルタに移動します。



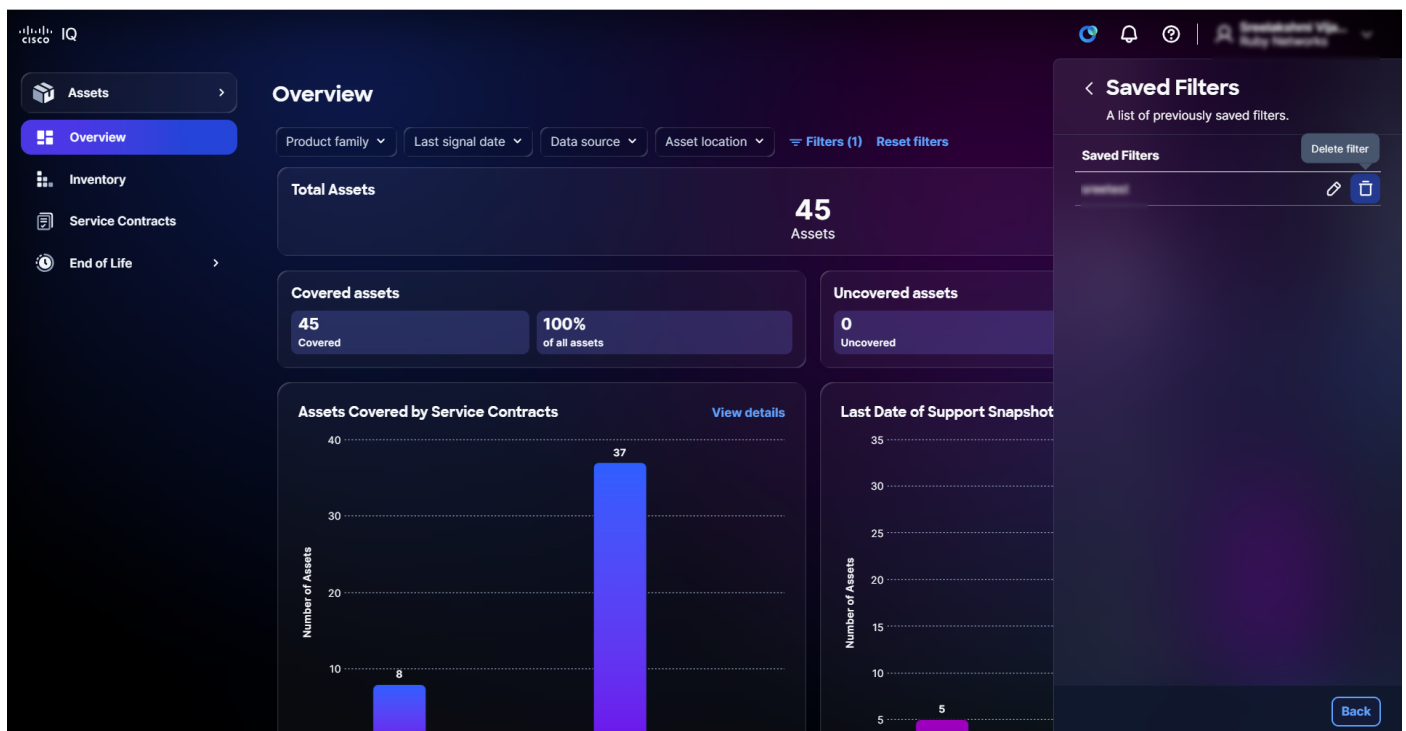
フィルタの編集

4. Editアイコンをクリックします。Name saved Filterウィンドウが開きます。
5. フィルタ名を編集します。
6. Save Filterをクリックして確定します。

フィルタの削除

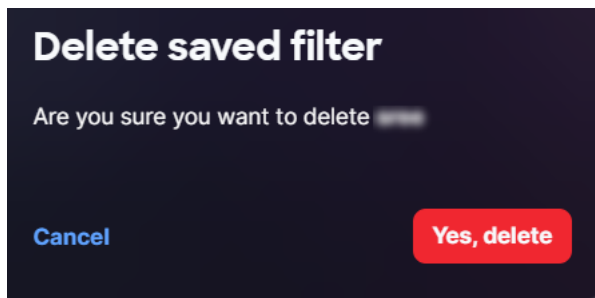
カスタムフィルタを削除するには、次の手順を実行します。

1. Filtersをクリックします。
2. Managed Saved Filtersアイコンをクリックします
3. フィルタに移動します。



保存されたフィルタの削除

4. Delete アイコンをクリックします。Delete saved filterウィンドウが開きます。



保存済みフィルタの削除の確認

5. Yes, deleteをクリックして確定します。

資産モジュール

資産モジュールは、シスコ資産の包括的な可視性と管理機能を提供し、Cisco IQの基盤として機能し、組織内のすべてのデバイスの一元化されたリストを提供します。複数の情報源から情報を収集することで、デバイスインベントリの唯一の正しい情報源として機能します。Cisco IQの他のモジュール（評価モジュールなど）は、デバイスの健全性とセキュリティを評価するためにこのデータに依存しているため、資産リストを完全かつ正確に維持することが不可欠です。

コア概念

Assetsモジュールは、次の基本概念に基づいて構築されています。

- 資産：シスコのサービス提供の一環としてインベントリに登録され、管理される任意の物理デバイス、ハードウェア、またはソフトウェア。ID、機能、サービス適用範囲、およびライフサイクルを詳細に追跡できます。
- 契約ソース資産：テレメトリではなく、リンクされたサービス契約データからインベントリに直接取り込まれる資産。Cisco IQは契約データからシャーシ、モジュール、電源装置、ファンの各機器タイプを取り込みます。これらの資産は、テレメトリ接続がない場合でもインベントリに表示されます
- サポート終了日(LDOS)：シスコ製品のサポート終了日およびサポート終了マイルストーンの追跡
- サービス契約：特定のハードウェアまたはソフトウェアに関連する有効なサポート契約、保証、および資格レベル
- 資産タグ：組織、フィルタリング、および運用ワークフロー用に資産に割り当てられるユーザ定義のラベル

- デバイスシグナル：デバイステレメトリ、サポートケース、および契約更新に基づき、シスコがデバイスを（シリアル番号で）最後に検出した時刻を指します。資産テレメトリデータは、マルチレイヤデータパイプラインを通じて取り込まれ、補強されます。

資産へのアクセス・ モジュール

Cisco IQで資産管理機能にアクセスするには、Homeメニュー> Assetsを選択するか、Homeページ> LaunchpadタブのApplicationセクションにあるAssetsをクリックします。Overviewページが表示されます。

アセットの概要

概要ページには、デバイスの健全性とステータスをすばやく評価できるダッシュボードが表示されます。

100% 400 Assets 100% 400 Assets 100% 400 Assets



Assets



Overview



Inventory



Service Contracts



End of Life



Overview

Filters

Ask AI

Customize

Saved Filters

Total Assets

199

Assets

928

Assets and subcomponents

Key Asset Metrics

Covered Assets

186

Covered

93%

Of all assets

Uncovered Assets

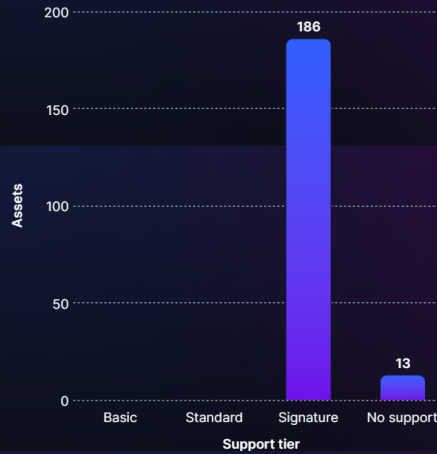
13

Uncovered

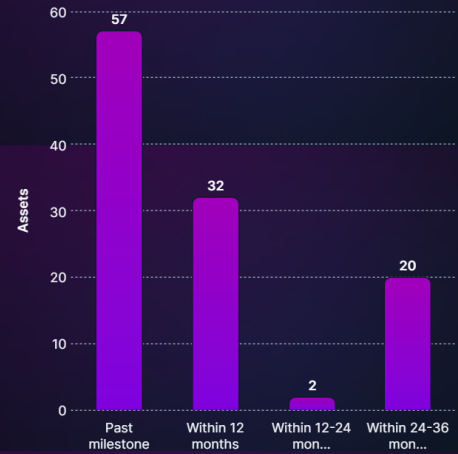
7%

Of all assets

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



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



Assets With Telemetry Enabled

186

With telemetry

93%

Of all assets

Assets Without Telemetry Enabled

13

Without telemetry

7%

Of all assets

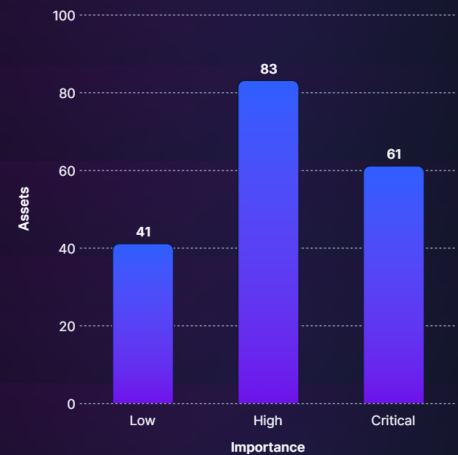
Assets With Critical or High Security Advisories [View details](#)



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

Assets by Importance [View details](#)

Importance can be evaluated for 185 assets.

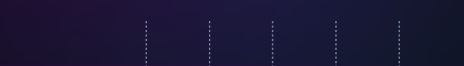


Asset Breakdown

Top 5 Product Families [View details](#)



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



アセットの概要

ダッシュボードには、次の情報が表示されます。

- 総資産: Cisco IQ アカウント内の総資産数
- 主な資産メトリック: テレメトリステータス、重要なセキュリティアドバイザリ、LDOS 情報など、その他の主要メトリック
- 対象資産: サービス契約の対象となる資産の総数と割合
- 契約対象外の資産: サービス契約の対象外の資産の総数と割合
- サービス契約対象の資産: サービス契約対象のハードウェアまたはソフトウェアの資産数が、エンタイトルメントレベル別に分類された内訳。
- サポート終了日のスナップショット: LDOS を過ぎたか、または LDOS に達した資産数の内訳
- テレメトリが有効な資産: テレメトリが有効な資産の総数と割合
- テレメトリが有効でない資産: テレメトリが有効でない資産の合計数と割合
- 重要または高セキュリティアドバイザリがある資産: テレメトリが有効になっていて、重要または高セキュリティアドバイザリがある資産全体の割合
- 重要度別資産: ネットワーク内の他のデバイスに関連する、デバイスに割り当てられた優先度の内訳。
- 資産の内訳: 製品ファミリ、設置場所、ソフトウェアバージョン、資産ロールなどの資産情報の詳細な表示

アセットのビューのフィルタリング

ダッシュボードビューをフィルタリングするには、ドロップダウンリストからフィルタを選択するか、またはフィルタをクリックして、使用可能なフィルタのリストからオプションを選択します。

 注: 一部のフィルタは、画面のズーム設定によっては非表示になる場合があります。ロールと権限に応じて、異なるフィルタを使用できます。

資産の詳細の表示

View Detailsをクリックすると、ページがInventoryページにリダイレクトされます。詳細については、「[インベントリ](#)」を参照してください。

資産の重要度の洞察

Cisco IQには、Assetsモジュールの新機能であるAsset Criticality Insightsが含まれています。この機能により、ネットワークデバイスの機能の役割とビジネス上の重要性が予測されます。デバイス構成と有効な機能を分析することで、ネットワークに最も大きな影響を与える資産を特定し、セキュリティの修復、ソフトウェアのアップグレード、サポート終了(EOL)計画、契約範囲の決定に優先順位を付けることができます。

 注：Asset Criticality Insightsは、アクティブなテレメトリ接続があるStandardまたはSignatureレベルの資産でのみ利用できます。ダッシュボード内でこれらのインサイトを読み込むために、資産が構成要件を満たしていることを確認してください。

Asset Criticality Insightsは、次の分野のAssetsアプリで利用できます。

- 資産概要：資産重要度インサイト属性別に要約ブレイクダウンをフィルタして表示します。
- 資産インベントリ：デバイスをロールおよび重要度別に表示、検索、フィルタリング、並べ替え
- 資産の詳細：個々のデバイスのロールと重要度を表示し、各値を説明する情報ツールチップを表示します。

ロールおよび重要度の分類の上書き

Cisco IQは、テレメトリデータに基づいて各資産の役割と重要性を自動的に予測します。自動予測がネットワーク内の資産の機能や重要度を正確に反映していない場合、アカウント管理者はこれらの分類を手動で修正できます。

 注意：上書きコントロールは、アカウント管理者のみが使用できます。ロールと重要度の値は、他のすべてのユーザロールに対しては読み取り専用です。

在庫表からの分類の上書き

1つ以上の資産のロールまたは重要度を上書きするには、次の手順に従います。

1. Assets > Inventoryの順に移動します。

2. 目的の資産行のチェックボックスをクリックします。複数のアセットを同時に更新するには、複数のチェックボックスをオンにします。

Assets

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

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

4 items selected Cancel Manage Tags

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

役割と重要性

3. RoleまたはImportance列で、資産行ドロップダウンリストから正しい値を選択します。
4. Applyをクリックして、上書きを確定します。

手動でオーバーライドされた値を持つアセットは、[ロール]列または[重要度]列に視覚的インジケータが表示されます。

 注：以前に設定したオーバーライドを削除して自動予測に戻るには、[ロール]または[重要度]ドロップダウンリストからダッシュ(—)オプションを選択します。

資産詳細からの分類の上書き

資産詳細ビューでロールまたは重要度を上書きするには、次の手順に従います。

1. Assets > Inventoryに移動して、アセットをクリックします。
2. アセットの詳細パネルで、RoleフィールドとImportanceフィールドを見つけます。

3. 更新するフィールドのドロップダウンをクリックし、正しい値を選択します。

4. Applyをクリックして確定します。

資産の詳細ビューには、元の自動予測を通知したテレメトリ属性の説明も表示され、上書きが適切かどうかを判断する際に役立ちます。

上書き監査証跡の表示

すべてのロールと重要度の上書きは、勘定科目レベルの監査証跡に記録されます。監査証跡にアクセスするには、次の手順を実行します。

1. Home > System Settings > Activity & Logsの順に選択します。

2. Filters > Action Type > overrideの順に選択すると、上書きイベントのみが表示されます。

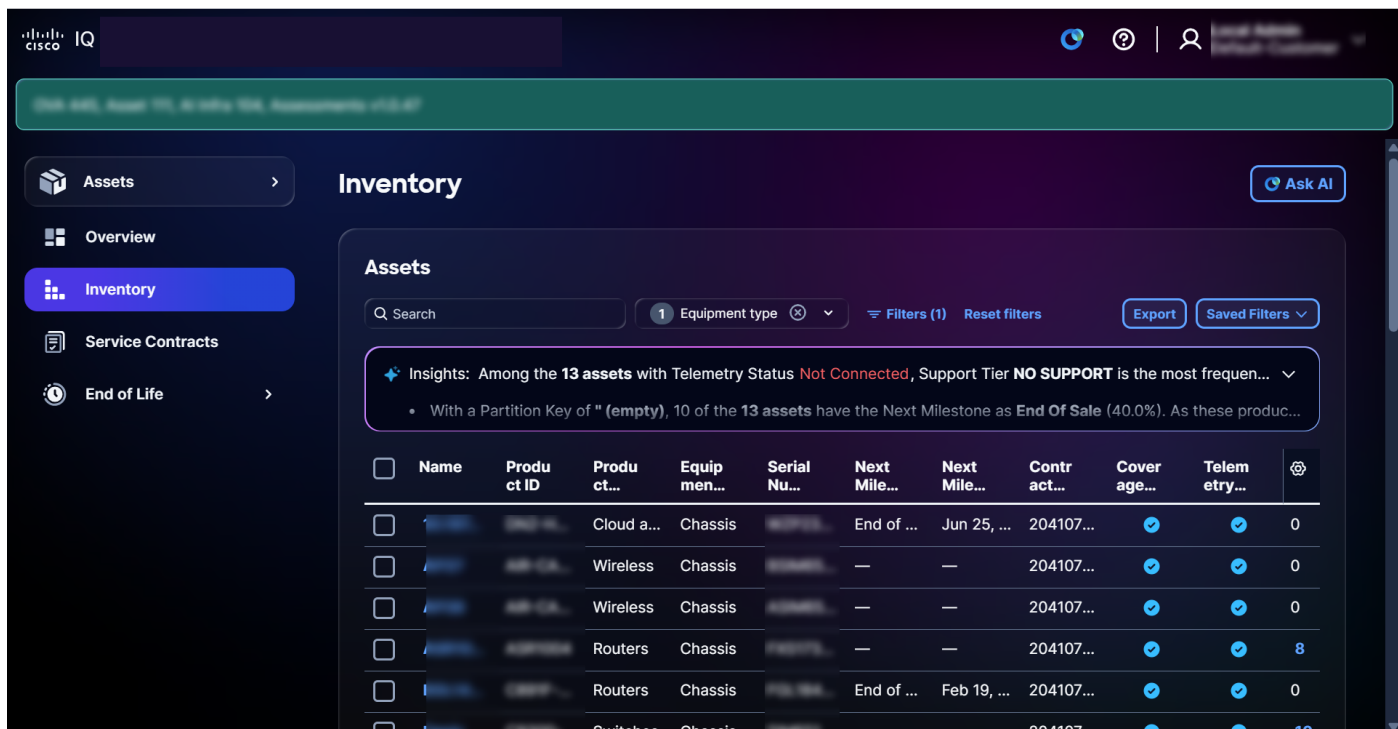
監査証跡には、資産名、以前の値と新しい値、変更を行ったユーザー、および変更の日時が表示されます。監査証跡は、Exportオプションを使用してエクスポートできます。



注意：監査証跡は、日付範囲、ユーザーおよび資産名でフィルタできます。

インベントリ

Inventoryページには、Cisco IQアカウント内のすべてのシスコ資産のリストが表示されます。



インベントリ

資産インベントリのビューの検索とフィルタリング

リストビューをフィルタリングするには、ドロップダウンリストからフィルタを選択するか、Filtersをクリックして、使用可能なフィルタのリストからオプションを選択します。Searchフィールドにアセット名を入力して、アセットを検索することもできます。

 注：

- 画面のズーム設定によっては、一部のフィルタが非表示になる場合があります。
- ロールと権限に応じて、異なるフィルタを使用できます。

インベントリ分析

InventoryページのInsightsパネルには、AIを活用した分析が表示されます。この分析では、サポート範囲、接続性、マイルストーンに重点を置いた資産の概要が提供されます。Full Analysisをクリックすると、グラフ、ダッシュボード、グラフなどの視覚エフェクトが表示され、さらに詳しい情報を確認できます。詳細は、『[共通モジュール機能でのデータの分析](#)』を参照してください。

。

インベントリのエクスポート

Exportをクリックして、フィルタリングされたインベントリリストを.xlsまたは.csv形式で保存します。詳細は、『[共通モジュール機能での情報のエクスポート](#)』を参照してください。

資産詳細の表示

資産をクリックすると、資産の詳細が表示されます。アセットの詳細ビューには、次のタブが表示されます。

- Details：製品、信号データ、ID、場所、保証、カバレッジ情報などの資産の詳細を表示します。

Assets

Overview

Inventory

Service Contracts

End of Life

Inventory

10.197.238.131

Cisco Catalyst Center Appliance (Gen 2) - 44 Core

DetailsProduct AlertsHardwareSoftware

Product

Product ID

Product type

Product family

Last Date of Support

Identity

Serial number

IP address

Hostname

Software version

Role

Importance

Tags

Sold by

Location

Install-at

Signals

Last signal

Last signal type

Telemetry

Telemetry status

Last data collection

Data connector

Warranty

Warranty type

Warranty end date

Coverage

Coverage status

Contract number

Support tier

Coverage end date

Ask AI

資産の詳細

- 製品アラート：セキュリティアドバイザリやField Noticeなどの関連製品アラートを表示し

ます。

- ハードウェア：ハードウェアEOLの詳細なタイムラインビューを提供します(販売終了、最終出荷、およびサポート終了日など)。
- ソフトウェア：ソフトウェアEOLの詳細なスケジュールを表示します。

Asset Tags

資産タグは、Cisco IQでインベントリ資産に割り当てるカスタムラベルです。タグとは、定義するキーと値のペアです。たとえば、Environment:ProdやLabel:Campusなどです。個々の資産または多数の資産に一度にタグを割り当てることができます。また、タグでインベントリをフィルタリングして、対象の資産をすばやく見つけることができます。

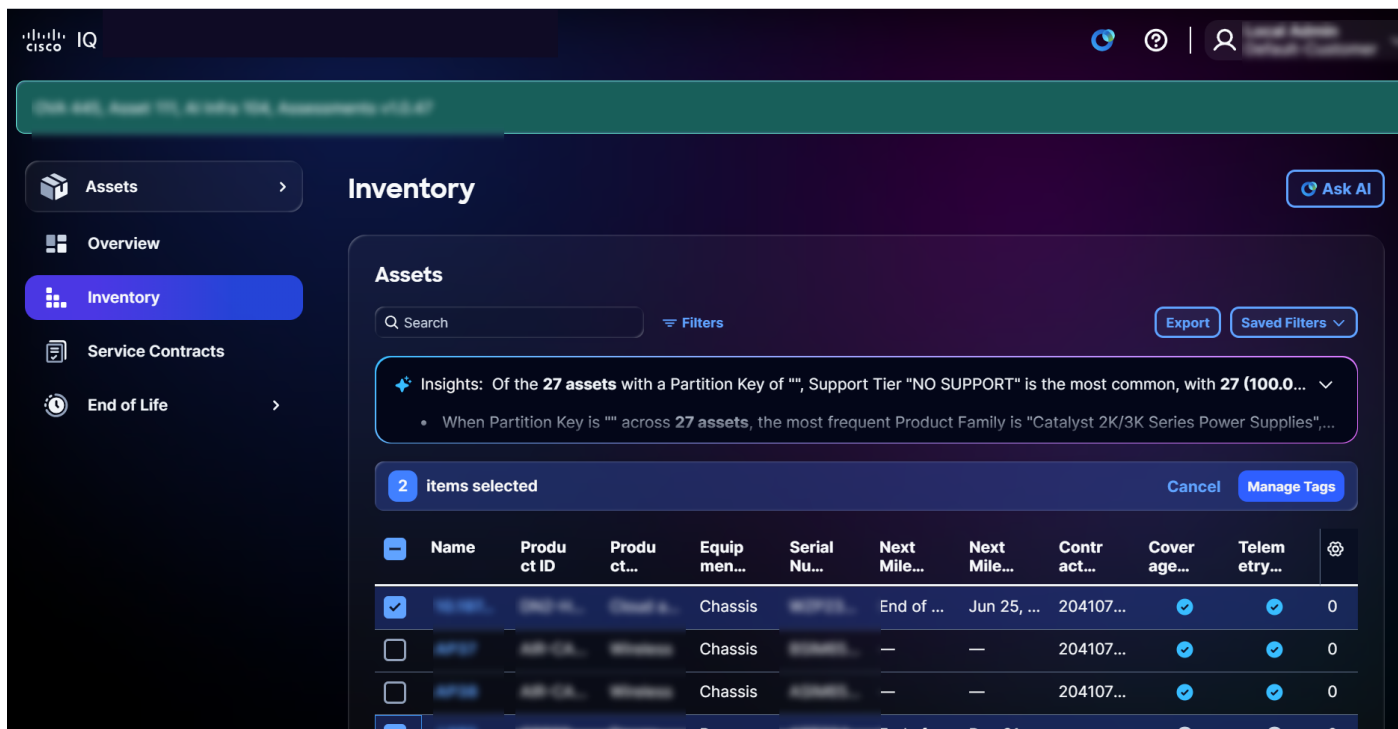
 注：アカウント管理者がタグを作成した後、ユーザはタグを資産に割り当てることができます。

タグの割当て

Inventoryビューで選択した資産にタグを割り当てると、資産の整理と分類が可能になり、フィルタリング、レポート、および管理の機能が強化されます。

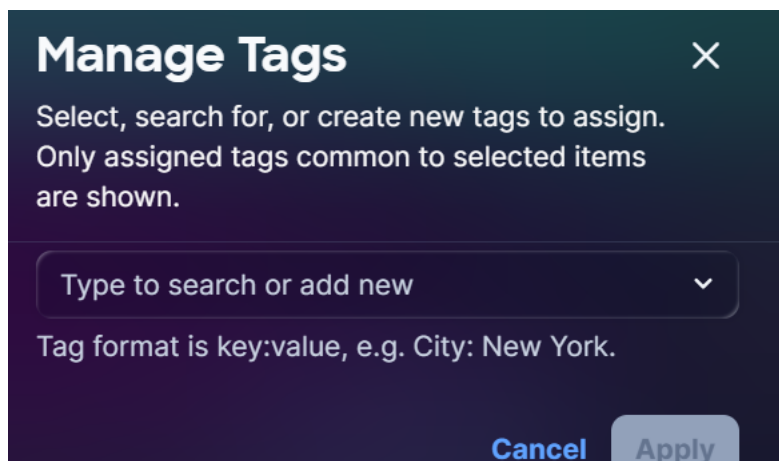
タグをアセットに割り当てるには：

1. Assets > Inventoryの順に移動します。



資産のタグ付け

2. 目的の資産のチェックボックスをオンにします。
3. Manage Tagsをクリックします。タグの管理ウィンドウが開きます。



タグの割当て

4. テキストフィールドで、既存のオプションからタグ名を入力または選択し、Enterを押します。



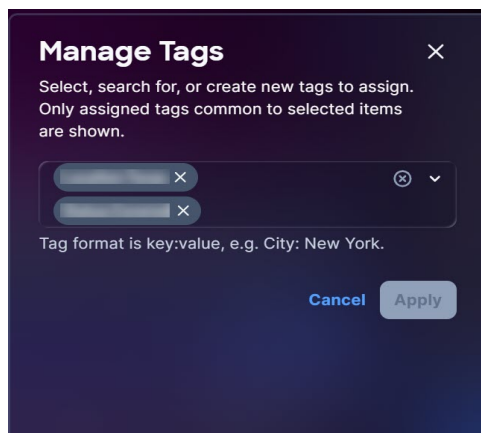
注：タグは、key:value形式（たとえば、City:NYC）です。

5. [APPLY] をクリックします。

資産タグの削除

1つまたは複数のアセットからタグを削除するには：

1. Assets > Inventoryの順に移動します。
2. 1つ以上のアセットの横にあるチェックボックスをオンにします。
3. Manage tagsをクリックします。タグの管理ウィンドウが開きます。



タグの削除

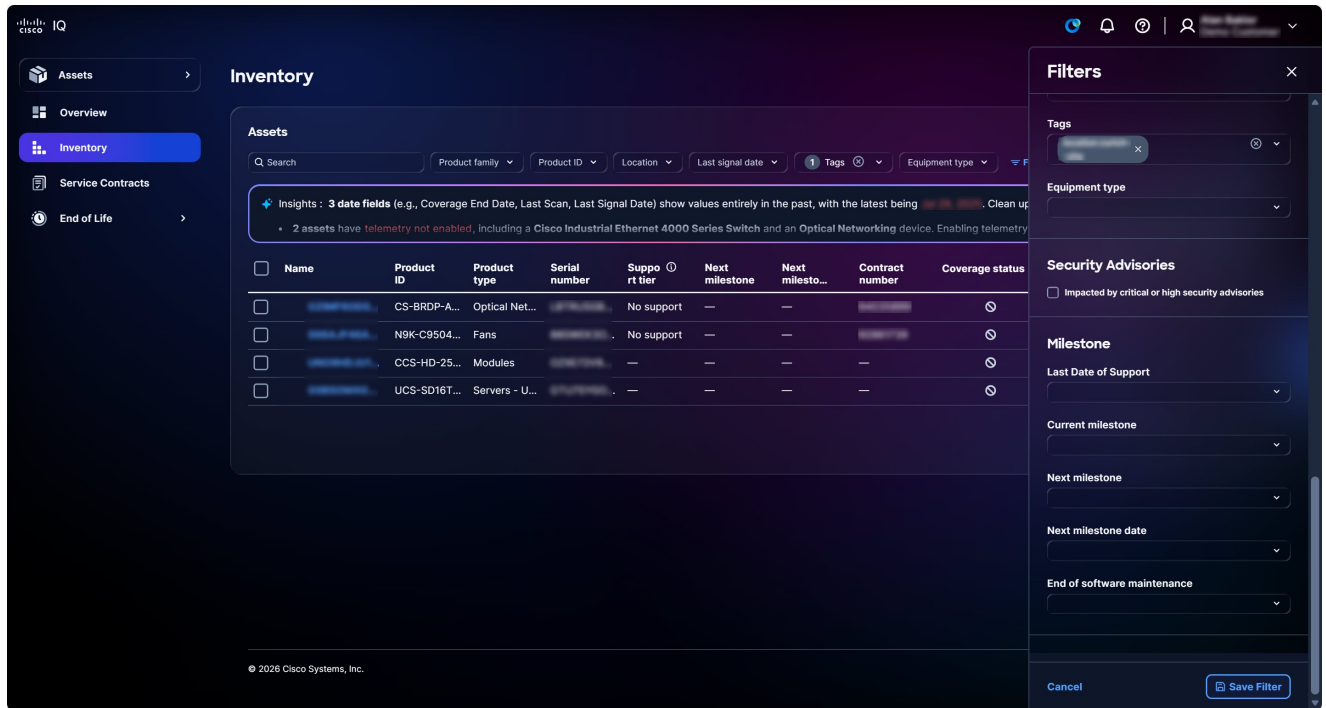
4. 任意のタグのXをクリックして、選択から削除します。
5. [APPLY] をクリックします。

アセットタグをフィルタとして使用する

タグを作成した後、そのタグをフィルタとして使用できます。

タグをフィルタとして使用するには、次の手順に従います。

1. Inventoryページに移動します。
2. Filtersをクリックします。Filtersウィンドウが開きます。

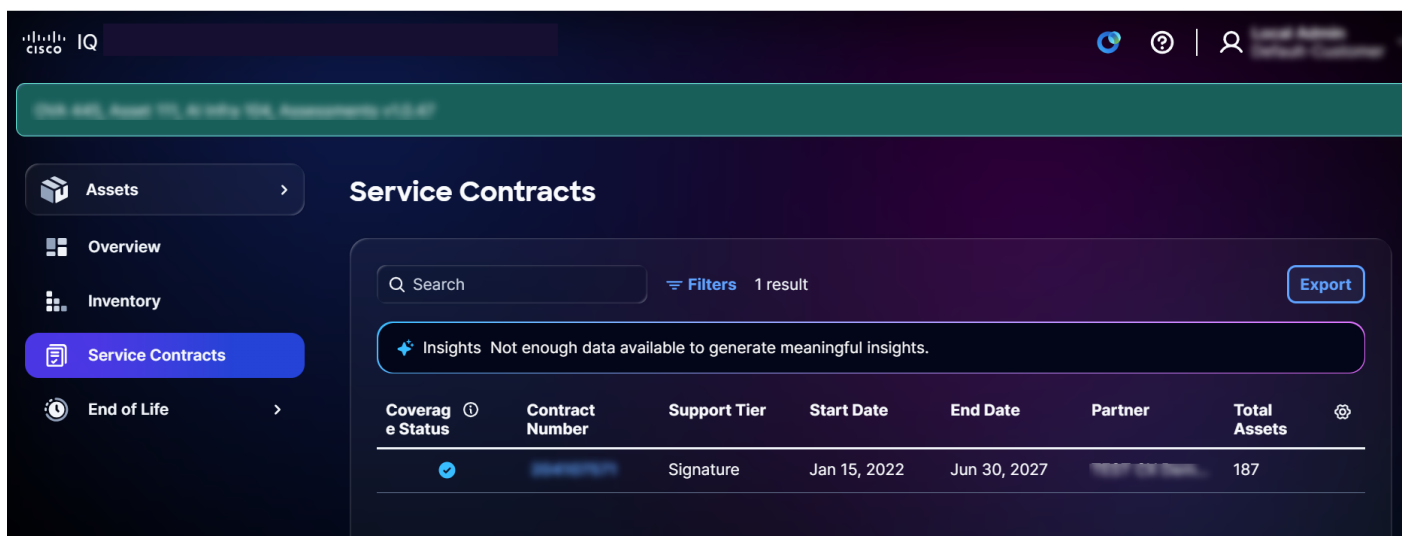


タグをフィルタとして使用

- Tagsドロップダウンリストから、目的のタグのチェックボックスをオンにします。タグを選択すると、「在庫」ページのビューがフィルタされたビューに更新されます。

サービス契約

Service Contractsページでは、要約と詳細な契約情報が提供されるため、サポート契約の監督が合理化され、効率的な更新計画と契約範囲の戦略がサポートされます。



サービス契約

サービス契約のビューの検索とフィルタリング

ド롭ダウンリストからフィルタを選択して、リストビューをフィルタリングできます。Searchフィールドに契約番号を入力して、サービス契約を検索することもできます。

サービス契約のエクスポート

Exportをクリックして、フィルタリングされた契約のリストを.xlsまたは.csv形式で保存します。詳細は、『[共通モジュール機能での情報のエクスポート](#)』を参照してください。

サービスEAの概要

Services Enterprise Agreement(EA)Summaryページには、資産ポートフォリオ全体のインストールベースの増加が統合されて表示されます。データはシスコのインストールベースレコードから直接取得されるため、パートナー様とアカウントチームはポートフォリオの変化を継続的かつ一貫して把握できます。

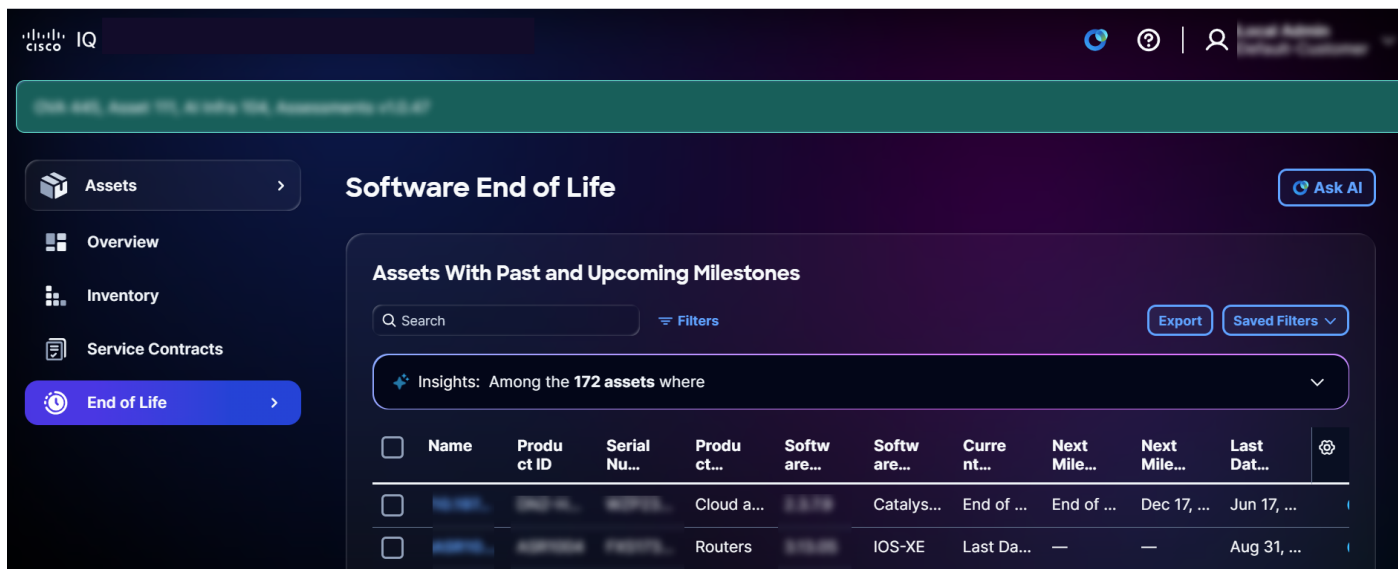
「サービスEA要約」ページには、次の情報が表示されます。

- 追加された資産：レポート期間中にインストールベースに追加された新規資産
- 正味増減：レポート期間中のインストールベースサイズの全体的な増減

 注: 「サービスEAサマリー」ページへのアクセスは、ロールと権限の要件に従う必要があります。このページがナビゲーションに表示されない場合は、アカウント管理者に問い合わせてください。

サポート終了

ハードウェアのサポート終了ページとソフトウェアのサポート終了ページには、詳細なサポート終了情報が記載されており、製品の更新サイクルとサポート範囲をプロアクティブに管理するために必要なサポートがユーザに提供されます。End of Lifeページで資産をクリックすると、Inventoryページの関連する資産にリダイレクトされます。



ソフトウェアのサポート終了

生産終了の分析

End of LifeページのInsightsパネルには、定義されたサポート終了日を持つアセットのAI駆動型の概要が表示されます。Full Analysisをクリックすると、グラフ、ダッシュボード、グラフなどの視覚エフェクトが表示され、さらに詳しい情報を確認できます。詳細は、『[共通モジュール機能でのデータの分析](#)』を参照してください。

サポート終了のエクスポート

Exportをクリックして、EOLアセットのフィルタリストを.xlsまたは.csv形式で保存します。詳細は、『[共通モジュール機能での情報のエクスポート](#)』を参照してください。

評価モジュール

評価モジュールは、評価フレームワークを提供します。これにより、セキュリティ、安定性、キャパシティ、コンプライアンス、およびエージングに関連するリスクを予防的に調査して軽減し、ネットワークの安全性、安定性、および信頼性を維持することができます。

コア概念

評価モジュールは、次の基本概念に基づいて構成されています。

- 評価：パフォーマンス、コンプライアンス、セキュリティ、または運用能力を測定するための事前定義された基準に照らし合わせて、インフラストラクチャエンティティを体系的に評価します。評価は、オンデマンド、スケジュール通り、またはイベントによってトリガーされます
- 評価の実行：評価のインスタンスまたは単一実行。実行ごとに、スコープ、トリガー・メカニズム、タイムスタンプ、および評価によって生成された結果データを追跡する新しい実行レコードが作成されます
- 所見：ギャップ、リスク、問題、または注目すべき状態を特定する、検証済みで実用的な所見。評価結果は、評価時の基礎となるデータを表す
- 洞察：複数の所見のパターンや傾向から導き出される、より高レベルの分析的結論。より広範なビジネスまたは運用のコンテキストにおいて調査結果が意味するものを解釈する洞察
- 推奨事項：結果や洞察にリンクされた具体的で実用的な処方箋。推奨事項には、特定された問題に対処したり機会を活用したりするために必要な手順に関する明確なガイダンスが記載されています。
- レポート：対象となる顧客に関する調査結果、見識、および推奨事項を集約した構造化文書。レポートは、顧客、経営陣、および技術チームに評価の結果を伝えるための主要な成果物です

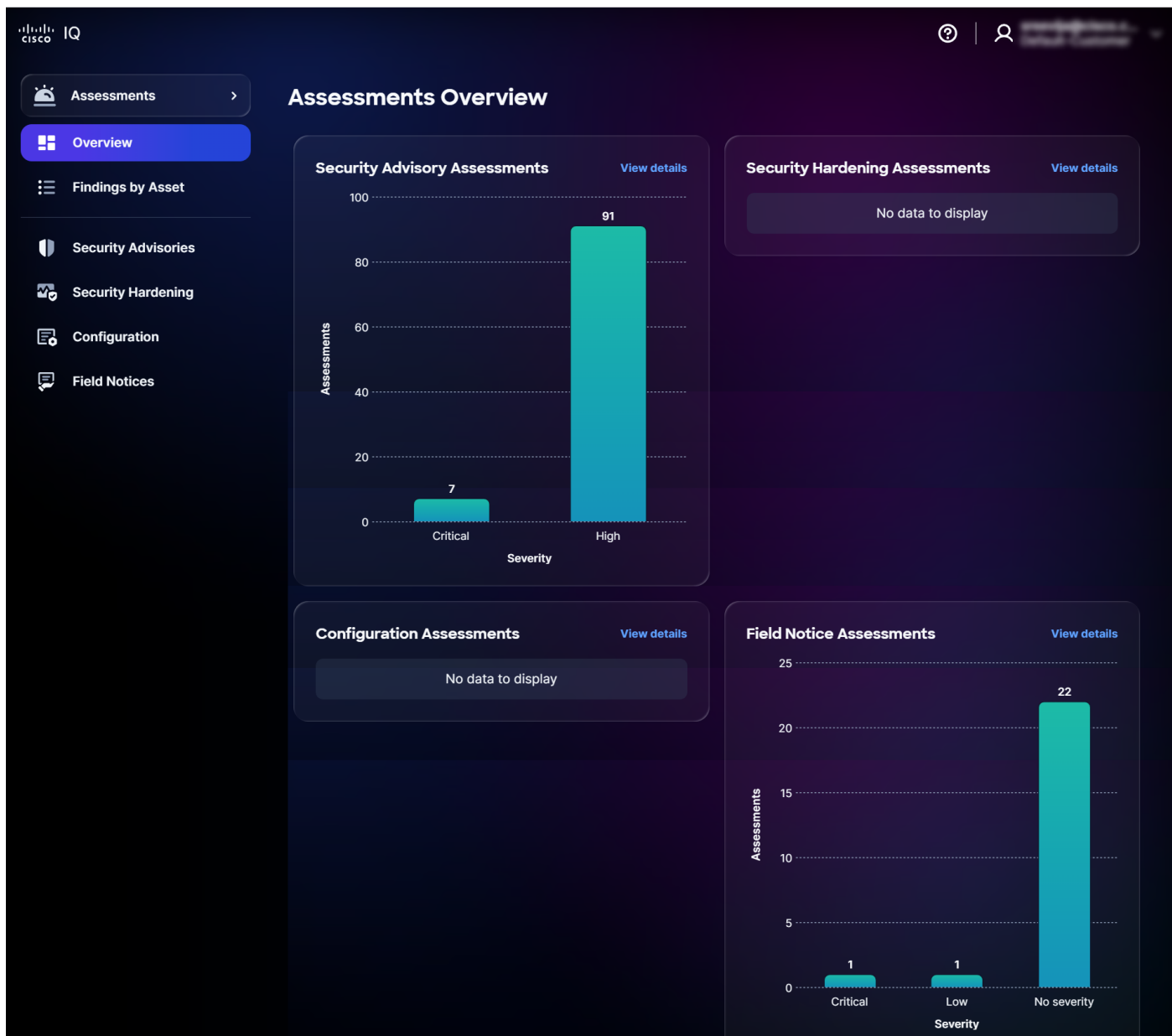
評価モジュールへのアクセス

仮想アプライアンスのセキュリティ機能とアセスメント機能にアクセスするには、ホームメニュー>アセスメントを選択するか、ホームページ>起動パッドタブのアプリケーションセクションからアセスメントをクリックします。「評価の概要」ページが表示されます。

 注：評価モジュールは、System Configuration > Package Managementからも起動できます。

評価の概要

「評価の概要」ページには、次のダッシュボードが表示されます。



評価の概要

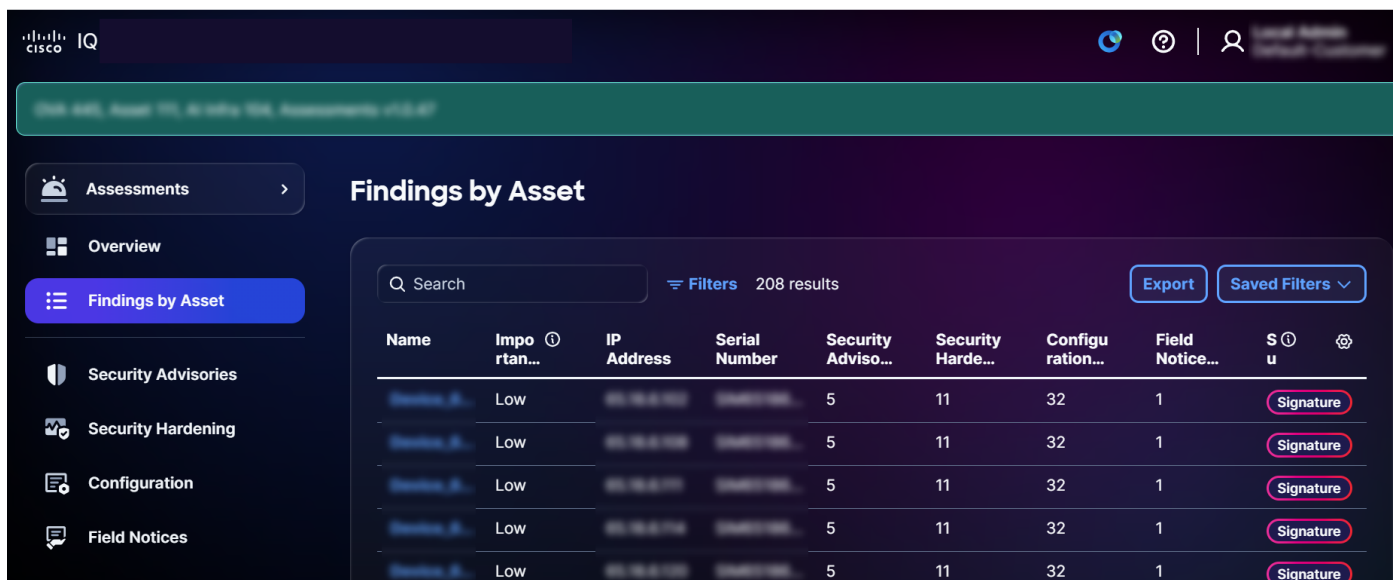
ダッシュボードには、次の情報が表示されます。

- Security Advisory Assessments：セキュリティアドバイザリの評価を重大度の高い順に表示します。
- セキュリティ強化の評価：セキュリティ強化ルールに違反している資産を、重大度（高、中、低、情報）別に表示します。
- 構成アセスメント：構成コンプライアンスルールに違反している資産を、重大、高、中、低、情報の重大度別に分類して表示します
- Field Notice Assessments:Field Noticeのアセスメントを、重大、重大、該当しない重大度別に表示します。

 注：アクセス権を持つ資産のみを表示できます。

資産別の結果

「資産別の結果」ページには、セキュリティアドバイザリ、セキュリティの強化、設定、Field Noticeのアセスメントのうち少なくとも1つを使用して評価された資産のリストが表示されます。



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

資産ごとの結果

資産別の結果のビューの検索およびフィルタ

リストビューをフィルタリングするには、ドロップダウンリストからフィルタを選択するか、Filtersをクリックして、使用可能なフィルタのリストからオプションを選択します。Searchフィールドで、Findings by Assetを検索することもできます。

 注：

- 画面のズーム設定によっては、一部のフィルタが非表示になる場合があります。
- ロールと権限に応じて、異なるフィルタを使用できます。

アセット別の結果のエクスポート

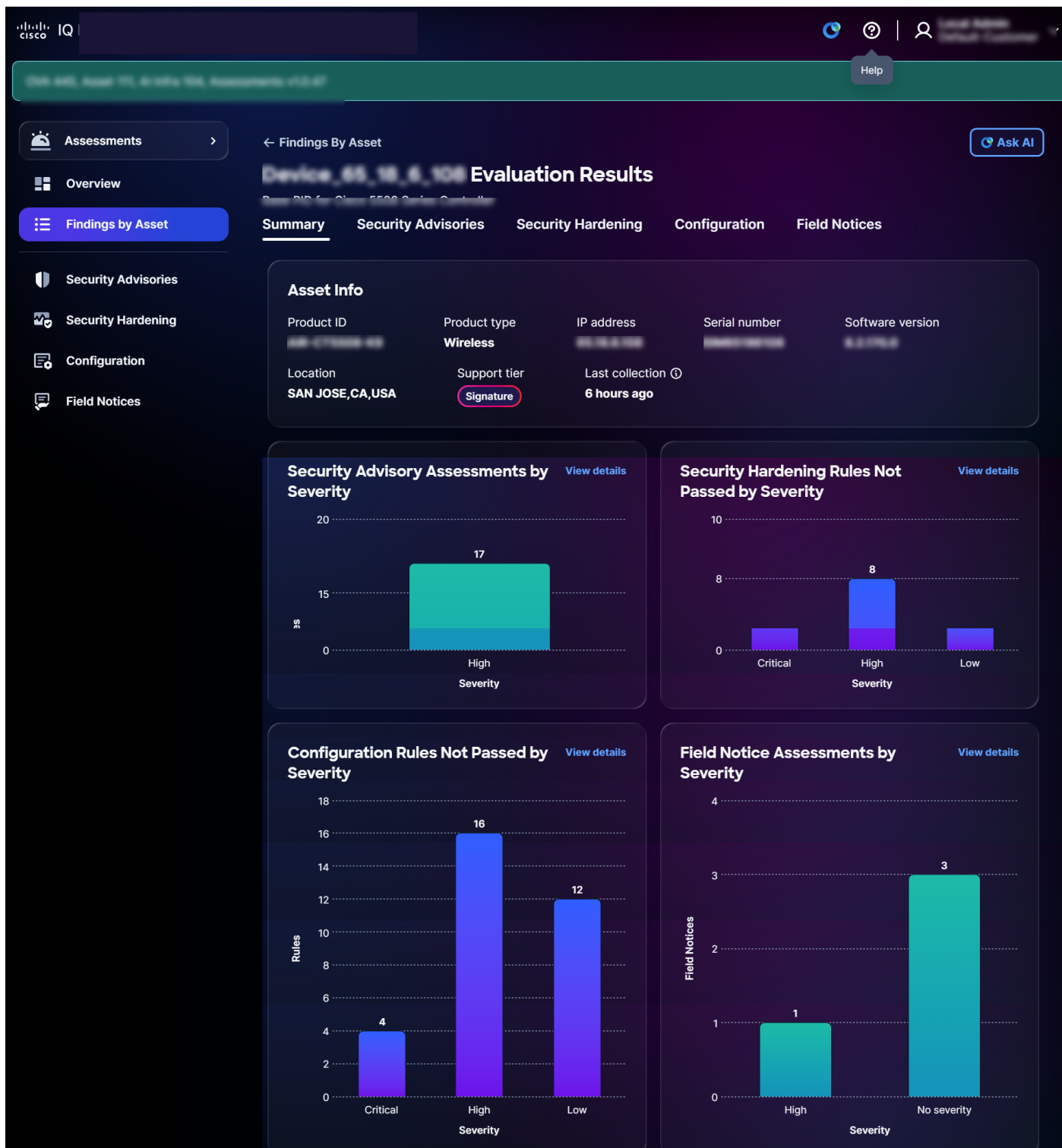
アセット別の結果リストビューをエクスポートするには、エクスポートをクリックします。詳細

は、『[情報のエクスポート](#)』を参照してください。

資産詳細別結果の表示

Findings by Assetの詳細を表示するには、該当するAssetをクリックします。次のタブには、選択したアセットの詳細が表示されます。

- 要約:セキュリティアドバイザリの数、セキュリティの強化、設定、Field Noticeなどの詳細な資産情報を提供します。
- セキュリティアドバイザリ：関連するセキュリティアドバイザリアセスメントのリストを提供します。
- セキュリティの強化：セキュリティ強化ルールに違反している資産の一覧を提供します
- Configuration：設定に失敗したアセットのリスト、ベストプラクティスのルールを示します。
- Field Notice：関連するField Noticeアセスメントのリストを提供します。



資産詳細別の結果

タイトルのView Detailsをクリックすると、ページはモジュール内の関連ページにリダイレクトされます。

View full asset detailsをクリックすると、asset detail viewページが表示されます。

セキュリティ アドバイザリ

セキュリティアドバイザリーアセスメントでは、脆弱性を特定し、そのリスク、重大度、重要度に基づいて優先順位を付けることで、組織のリスク管理機能を強化します。セキュリティアドバイザリは、脆弱性に対する詳細な洞察を提供し、重大な脅威の軽減を促進し、コンプライアンスとビジネス目標との整合性を確保します。これにより、セキュリティポスチャが強化され、リソース割り当てが最適化され、企業全体で進化する脅威に対する復元力が強化されます。セキュリティアドバイザリは、リリースされるとすぐにCisco IQで自動的に更新されます。

セキュリティアドバイザリページには、組織内で検出された脆弱性に関するすべてのセキュリティアドバイザリのリストが表示されます。セキュリティアドバイザリアセスメントリストのアドバイザリをクリックすると、対応する詳細ビューに移動します。

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

セキュリティ アドバイザリ

セキュリティアドバイザリのビューの検索とフィルタリング

ドロップダウンリストからフィルタを選択して、リストビューをフィルタリングできます。検索フィールドにアセスメント名を入力して、セキュリティアドバイザリアセスメントを検索することもできます。

 注：一部のフィルタは、画面ズームの設定によって非表示になります。一部のフィルタは、画面ズームの設定によって非表示になります。ロールと権限に応じて、異なるフィルタを使

 用できます。重大度の値が見つからない場合は、説明ツールチップとともに「-」と表示されます。

セキュリティアドバイザリのエクスポート

セキュリティアドバイザリアセスメントをエクスポートするには、Exportをクリックします。詳細は、『[情報のエクスポート](#)』を参照してください。

セキュリティアドバイザリアセスメントの詳細の表示

アセスメントをクリックすると、そのアセスメントの詳細が表示されます。詳細ページには、Common Vulnerability Scoring System(CVSS)スコア、Common Vulnerabilities and Exposures(CVE)、重大度、参照先のシスコセキュリティアドバイザリへのリンクなどの情報が記載されています。

「評価の結果」テーブルには、次のタイプの結果が表示されます。

- Affected：攻撃者によって不正利用される可能性があり、修復が必要な脆弱性が資産またはコンポーネントに存在することが確認されていることを示します。
- Potentially Affected：資産またはコンポーネントに脆弱性につながる可能性のある兆候が見られるものの、確定的に確認されていないことが示されます。詳細な調査が必要になる場合があります。

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

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

セキュリティアドバイザリの詳細

資産評価結果のビューの検索とフィルタリング

リストビューをフィルタリングするには、ドロップダウンリストからフィルタを選択するか、Filtersをクリックして、使用可能なフィルタのリストからオプションを選択します。Searchフィールドにアセット名を入力して、アセットを検索することもできます。



注：画面のズーム設定によっては、一部のフィルタが非表示になる場合があります。ロールと権限に応じて、異なるフィルタを使用できます。

資産査定結果の表示

評価結果の詳細を表示するには、「Assessment Outcome」テーブルのアセットをクリックします。アセットのアセスメント結果詳細ページが表示されます。

The screenshot displays the Cisco IQ interface for a security advisory. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories (highlighted), Security Hardening, Configuration, and Field Notices. The main content area shows the 'Result' for a 'Cisco Secure Boot Hardware Tampering Vulnerability'. The device ID is 'Device_65_10_4_108'. The assessment status is 'Potentially affected'. The 'Evidence' section lists three matches: software type, chassis product ID, and module product ID. The 'Additional Verification Needed' section provides instructions for manual verification. The 'About the Assessment' section describes the vulnerability and includes a table with severity (High), CVE, CVSS score (6.7), first published date (May 13, 2019), and last updated date (Nov 20, 2019). The 'About the Asset' section provides details about the asset, including product ID, product type (Switches), IP Address, serial number, software version, location (SAN JOSE, CA, USA), and support tier (Signature).

Security Advisories > Cisco Secure Boot Hardware Tampering Vulnerability

Device_65_10_4_108 Result [Ask AI](#)

Assessment: Cisco Secure Boot Hardware Tampering Vulnerability

Result Details Potentially affected

Evidence

- ✓ Matched on software type
- ✓ Matched on chassis product ID
- ✓ Matched on module product ID

Additional Verification Needed

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

About the Assessment

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

[Show more](#)

Severity	CVE	CVSS score
High		6.7
First published	Last updated	
May 13, 2019	Nov 20, 2019	

References

[Security Advisory](#)

About the Asset [View evaluated asset](#)

Product ID	Product type	IP Address
	Switches	
Serial Number	Software version	Location
		SAN JOSE, CA, USA
Support tier		
Signature		

結果の詳細

セキュリティアドバイザリのアセット結果のエクスポート

アセットの結果をエクスポートするには、Exportをクリックします。詳細は、『[情報のエクスポート](#)』を参照してください。

セキュリティの強化

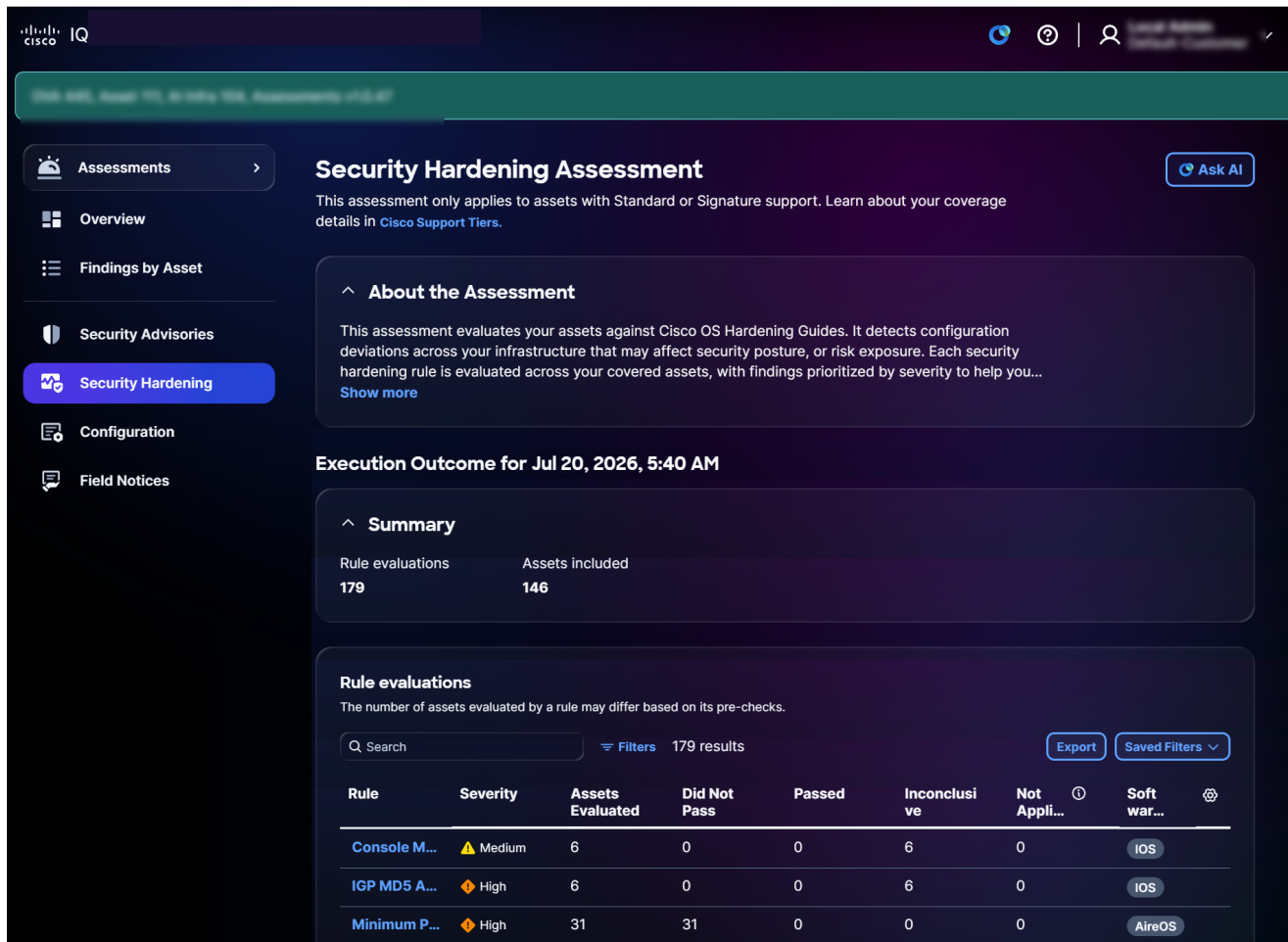
セキュリティの強化：業界標準のベンチマークに照らしてルータ、スイッチ、およびファイアウォールを継続的に評価することにより、ネットワークインフラストラクチャのセキュリティポスチャをほぼリアルタイムで自動的に可視化します。設定のギャップを特定し、実用的な修復ガイダンスを提供することで、アカウント管理者は攻撃対象領域を効果的に縮小し、シスコの厳格なセキュリティのベストプラクティスとの一貫性を維持することができます。コンプライアンスモニタリングを集中化し、強化プロセスを簡素化することで、このモジ

ユーロルはセキュリティ管理を事後対応型タスクから予防的なデータ駆動型戦略に変え、復元力のあるセキュアなエンタープライズネットワークを実現します。

 注：セキュリティ強化アセスメントは、標準サポート階層の資産に対してのみ提供されています。

セキュリティ強化評価の表示

「セキュリティ強化評価」ページには、次の情報が表示されます。



Security Hardening Assessment

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

About the Assessment

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

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

Summary

Rule evaluations	Assets included
179	146

Rule evaluations

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

Search Filters 179 results [Export](#) [Saved Filters](#)

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

セキュリティの強化

- ・ アセスメントについて：アセスメントの目的を要約して詳細を提供します。
- ・ Execution Outcome: ルール評価の総数と含まれる資産数を含む、資産評価結果のサマリーを提供します。
- ・ ルールの評価：ルールに関する詳細情報(重大度、評価済み資産、合格しませんでした、合格、不確定、該当なし、ソフトウェアタイプなど)を提供します。
- ・ 重大度：ルール評価の重要度または影響のレベルを示します。
- ・ 評価済み資産：ルール基準に照らして評価された資産の合計数を示します

- 不合格：評価中にルール基準を満たすことができなかった資産を示します。
- 合格：評価中にルールの基準を満たした資産を提供します。
- 不確定：評価で障害を特定できなかった資産を示します。
- 該当なし：ルールが適用されない、または関連しない資産またはシナリオを示します。
- ソフトウェアタイプ：資産のソフトウェアタイプを提供します。

ルールのビューの検索とフィルタ

リストビューをフィルタリングするには、ドロップダウンリストからフィルタを選択するか、Filtersをクリックして、使用可能なフィルタのリストからオプションを選択します。Searchフィールドにルール名を入力して、ルールを検索することもできます。



注：画面のズーム設定によっては、一部のフィルタが非表示になる場合があります。ロールと権限に応じて、異なるフィルタを使用できます。

ルール評価の詳細の表示

ルール評価の詳細を表示するには、ルールをクリックします。ルールの評価詳細ページが表示され、次の情報が示されます。

The screenshot shows the Cisco IQ interface for a Security Hardening Assessment. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening (highlighted), Configuration, and Field Notices. The main content area is titled 'Minimum Password Length Policy' and shows it was evaluated on Jul 20, 2026, at 5:39 AM. An 'Ask AI' button is in the top right.

About the Rule

Check 'Min. Password length' in show switch config, and warn if it is lower than 8. Proper security configuration protects the wireless infrastructure from unauthorized access, data interception, and compliance violations.

Severity: **High** (High icon) | Software type: **AireOS** | Assets evaluated: **31**

Results Summary 31 assets

0 Passed ✓	31 Didn't pass ✗	0 Inconclusive ⚠	0 Not applicable ⓘ
----------------------	----------------------------	----------------------------	------------------------------

Asset Results

Search: [] Filters: 31 results [Export] [Saved Filters]

Asset	Result	Product ID	Serial Number	IP Address	Support Tier ⓘ
Device_...	✗ Didn't pass	...	...	...	Signature
Device_...	✗ Didn't pass	...	...	...	Signature
Device_...	✗ Didn't pass	...	...	...	Signature
Device_...	✗ Didn't pass	...	...	...	Signature
Device_...	✗ Didn't pass	...	...	...	Signature

ルールビュー

- About the Rule:Severity、Software type、Version、およびAssets evaluatedなどのルールに関する詳細を提供し、関連するソースドキュメントへの説明ラベル付きリンクを含みます
- Results Summary: 「Passed」、「Did not pass」、「Inconclusive」、「Not applicable」など、ルールに関連する資産の結果の概要が表示されます。
- 資産結果：資産のリストと、資産、結果、製品ID、シリアル番号、IPアドレス、およびサポート階層などの詳細を提供します。

 注:Cisco IQでは、アセスメントの結果が「確定的でない」場合に、原因（たとえば、テレメトリの欠落、サポートされていないOSなど）を説明し、データ収集の検証、クレデンシャルの更新、データの更新などの手順を推奨する明確なガイダンスを提供します。問題の解決に役立つ、関連ドキュメントへのラベル付きリンクも提供されます。

アセットルールのビューの検索とフィルタリング

リストビューをフィルタリングするには、ドロップダウンリストからフィルタを選択するか

、Filtersをクリックして、使用可能なフィルタのリストからオプションを選択します。
Searchフィールドに資産名を入力して、資産査定結果を検索することもできます。

 注：画面のズーム設定によっては、一部のフィルタが非表示になる場合があります。
ロールと権限に応じて、異なるフィルタを使用できます。

資産結果のエクスポート

ルールの評価結果をエクスポートするには、Exportをクリックします。詳細は、『[情報のエクスポート](#)』を参照してください。

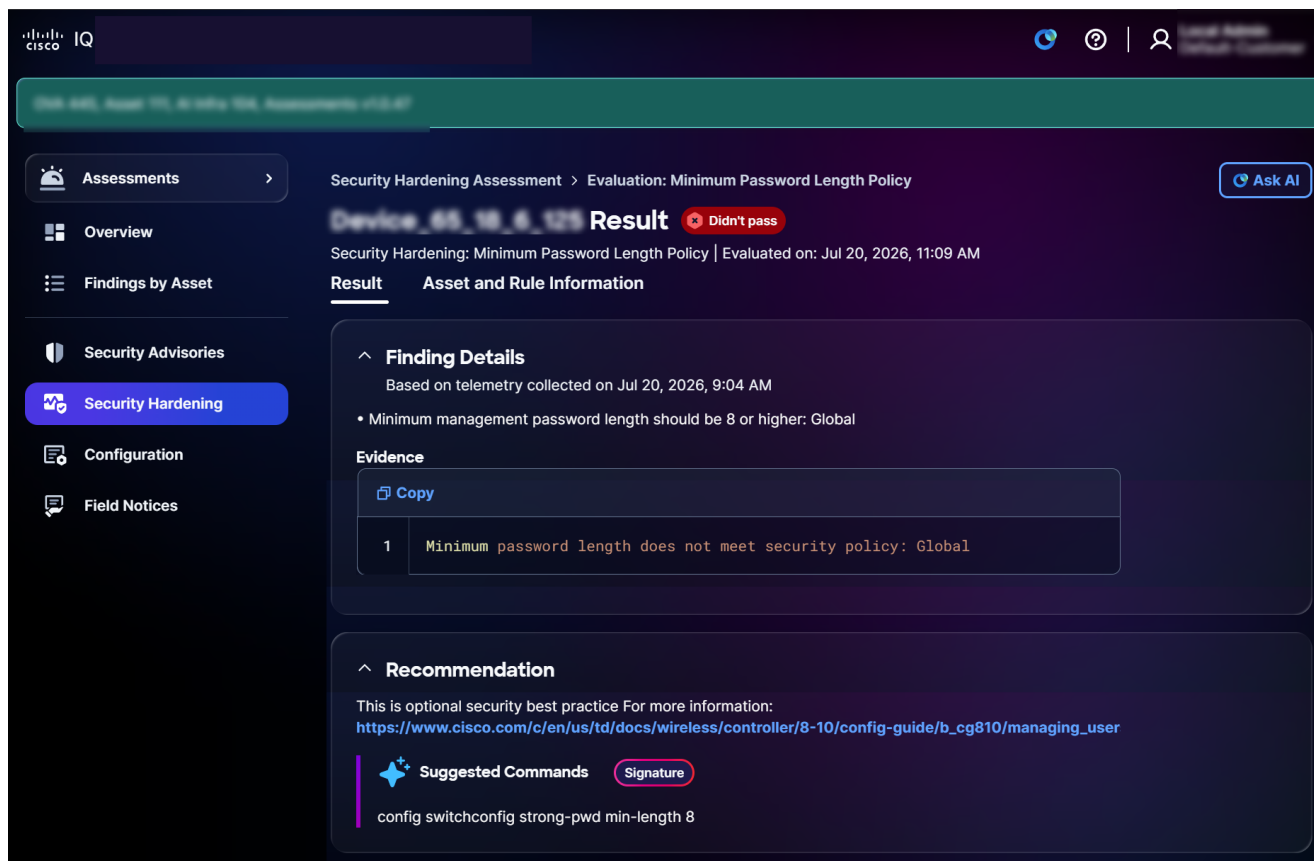
アセット結果のビューの検索とフィルタリング

リストビューをフィルタリングするには、ドロップダウンリストからフィルタを選択するか、Filtersをクリックして、使用可能なフィルタのリストからオプションを選択します。
Searchフィールドにアセット名を入力して、アセットの結果を検索することもできます。

 注：画面のズーム設定によっては、一部のフィルタが非表示になる場合があります。
ロールと権限に応じて、異なるフィルタを使用できます。

セキュリティ強化の資産結果の表示

Asset Resultsでアセットをクリックすると、その詳細が表示されます。アセットの結果の詳細ページには、エンタイトルメントレベルまたはレベルに従って情報が表示されます。



The screenshot displays the Cisco IQ interface for a Security Hardening Assessment. The left sidebar shows navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening (selected), Configuration, and Field Notices. The main content area shows the results for 'Device_69_18_6_125' under the 'Evaluation: Minimum Password Length Policy'. The status is 'Result' with a 'Didn't pass' indicator. The finding details state: 'Based on telemetry collected on Jul 20, 2026, 9:04 AM' and 'Minimum management password length should be 8 or higher: Global'. The evidence section shows a single entry: '1 Minimum password length does not meet security policy: Global'. The recommendation section provides a link to Cisco documentation and suggests the command 'config switchconfig strong-pwd min-length 8'.

セキュリティ強化機能標準階層

- 標準層
- 詳細の検索：評価中に特定された構成の逸脱に関する情報と、証拠ログを提供します。
- 推奨事項：結果に対処し、設定の一貫性を確保するためのガイダンスを提供します。

セキュリティ強化のための資産およびルール情報の表示

アセットとそのルールの詳細を表示するには、アセットとルール情報タブをクリックします。Asset and Rule Infoページが表示されます。

資産について：製品ID、製品タイプ、IPアドレス、シリアル番号、ソフトウェアバージョン、場所、およびサポート階層など、資産の詳細を提供します。

- About the Rule：ルールの詳細(重大度とソフトウェアタイプを含む)と特定の強化チェックの重要性を示します

コンフィギュレーション

構成アセスメントでは、インフラストラクチャ全体の可用性、セキュリティ、またはパフォーマンスに影響を与える可能性がある構成の逸脱を検出するために、シスコの実績ある専門知識に基づいて、推奨されるベストプラクティスに照らして資産を評価します。各ベストプラクティスルールは、対象の資産全体で評価され、結果は重大度によって優先順位付けされ、構成の一貫性、復元力の強化、運用リスクの軽減が確実に行われます。



注：構成アセスメントは、標準サポート階層の資産に対してのみ利用できます。

構成アセスメントの表示

Configuration Assessmentページには、次の情報が表示されます。

Configuration Assessment

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

About the Assessment

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

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

Summary

Rule evaluations	Assets included
729	146

Rule Evaluations

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

Search: Filters: 729 results [Export](#) [Saved Filters](#)

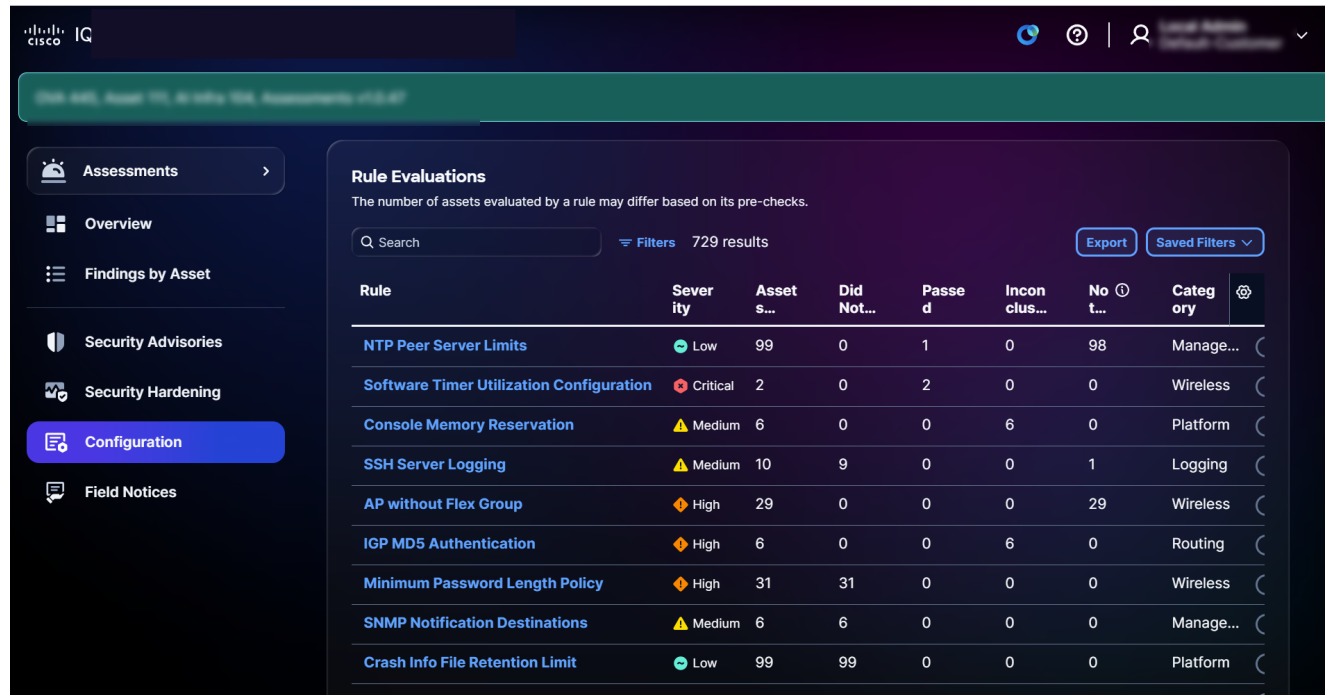
Rule	Severity	Assets	Did Not...	Passed	Inconclus...	No t...	Category
NTP Peer Server Limits	Low	99	0	1	0	98	Manage...
Software Timer Utilization Configuration	Critical	2	0	2	0	0	Wireless
Console Memory Reservation	Medium	6	0	0	6	0	Platform
SSH Server Logging	Medium	10	9	0	0	1	Logging

構成の評価

- アセスメントについて：アセスメントの目的を要約して詳細を提供します。
- Summary: Rules evaluatedやAssets evaluatedなどの設定実行のサマリーを提供します。
- Insights：パターン分析によって生じた特定された構成ギャップに関する洞察と、判明した項目の相関関係を提供します。インテリジェントにグループ化された主要カードとして表示され、注意が必要な最も重要な領域を強調表示します。
- ルールの評価：ルールに関する詳細情報(重大度、評価されたアセット、合格しませんでした、合格しました、結論に達しませんでした、該当なし、カテゴリ、およびソフトウェアタイプなど)を提供します。
- 重大度：ルール評価の重要度または影響のレベルを示します。
- 評価済み資産：ルール基準に照らして評価された資産の合計数を示します
- Did Not Pass：評価中にルール基準を満たすことができなかった資産の総数を示します。
- Inconclusive：アセスメントを実行できなかった資産の総数を示します。

- 合格：評価中にルールの基準を満たした資産を提供します。
- 該当なし：ルールが適用されない、または関連しない資産またはシナリオを示します。
- カテゴリ：ルールが属するドメイン領域を提供します
- ソフトウェアタイプ：ルールが適用されるソフトウェア資産のタイプを示します

ルールのビューの検索とフィルタ



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

ルールの評価

リストビューをフィルタリングするには、ドロップダウンリストからフィルタを選択するか、Filtersをクリックして、使用可能なフィルタのリストからオプションを選択します。Searchフィールドにルール名を入力して、ルールを検索することもできます。



注：画面のズーム設定によっては、一部のフィルタが非表示になる場合があります。ルールと権限に応じて、異なるフィルタを使用できます。

ルール評価の詳細の表示

ルール評価の詳細を表示するには、任意のルールをクリックします。ルールの評価詳細ページが表示され、次の情報が示されます。

The screenshot shows the Cisco IQ Configuration Assessment interface. The main heading is "NTP Peer Server Limits", evaluated on Jul 20, 2026, at 5:40 AM. The interface includes a sidebar with navigation options: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (selected), and Field Notices. The main content area displays the rule details, including its severity (Low), category (Management), software type (IOS-XE), and the number of assets evaluated (99). Below this, a Results Summary shows 1 Passed, 0 Didn't pass, 0 Inconclusive, and 98 Not applicable. The Asset Results section shows a table with columns for Asset, Result, Product ID, Serial Number, IP Address, and Support Tier, with 99 results displayed.

評価

- About the Rule:Severity、Category、Software type、およびAssets evaluatedなどのルールに関する詳細を提供し、関連するソースドキュメントへの説明ラベル付きリンクを含みます。
- Results Summary：ステータスが「Passed」と「Did not pass」と「Inconclusive」および「Not applicable」のアセット数を表示することで、アセットの全体的な結果を提供します
- 資産結果：選択したルールの影響を受ける資産のリストと結果ステータスを表示します。

 注:Cisco IQでは、アセスメントの結果が「確定的でない」場合に、原因（たとえば、テレメトリの欠落、サポートされていないOSなど）を説明し、データ収集の検証、クレデンシャルの更新、データの更新などの手順を推奨する明確なガイダンスを提供します。問題の解決に役立つ、関連ドキュメントへのラベル付きリンクも提供されます。評価モジュールは、ルールに対する複数のカテゴリ選択をサポートし、複数のルールカテゴリに対する同時処理と評価を可能にします。

資産結果のエクスポート

ルールの資産結果をエクスポートするには、Exportをクリックします。詳細は、『[情報の工](#)

[クスポート](#)』を参照してください。

アセット結果のビューの検索とフィルタリング

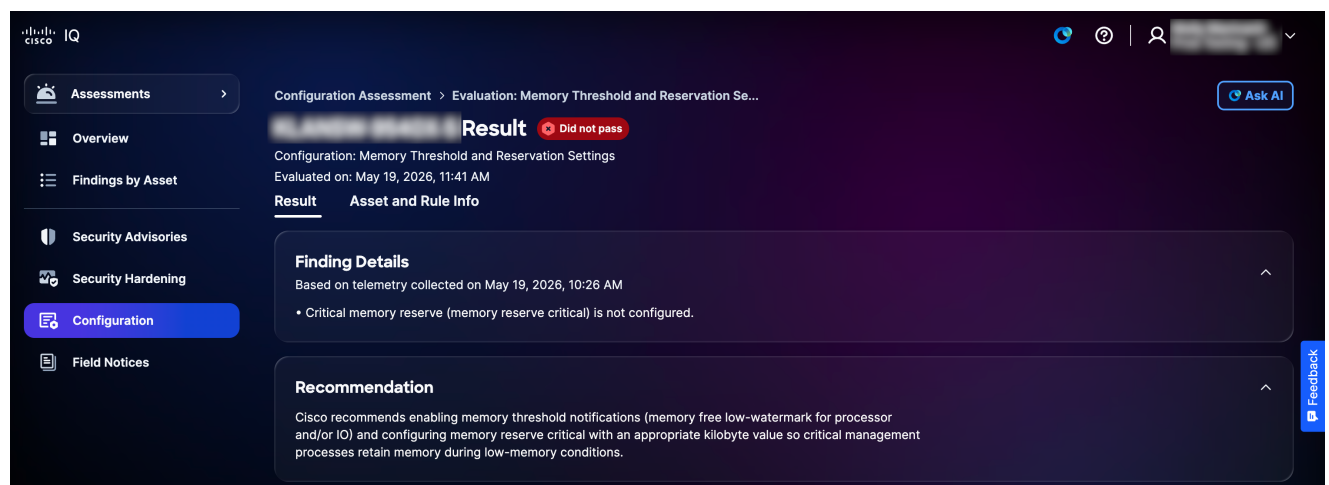
リストビューをフィルタリングするには、ドロップダウンリストからフィルタを選択するか、Filtersをクリックして、使用可能なフィルタのリストからオプションを選択します。Searchフィールドにアセット名を入力して、アセットの結果を検索することもできます。

 注：画面のズーム設定によっては、一部のフィルタが非表示になる場合があります。ロールと権限に応じて、異なるフィルタを使用できます。

構成評価の資産結果の表示

資産結果の詳細を表示するには、資産結果から資産をクリックします。

アセットの結果の詳細ページには、エンタイトルメントレベルまたはレベルに従って情報が表示されます。

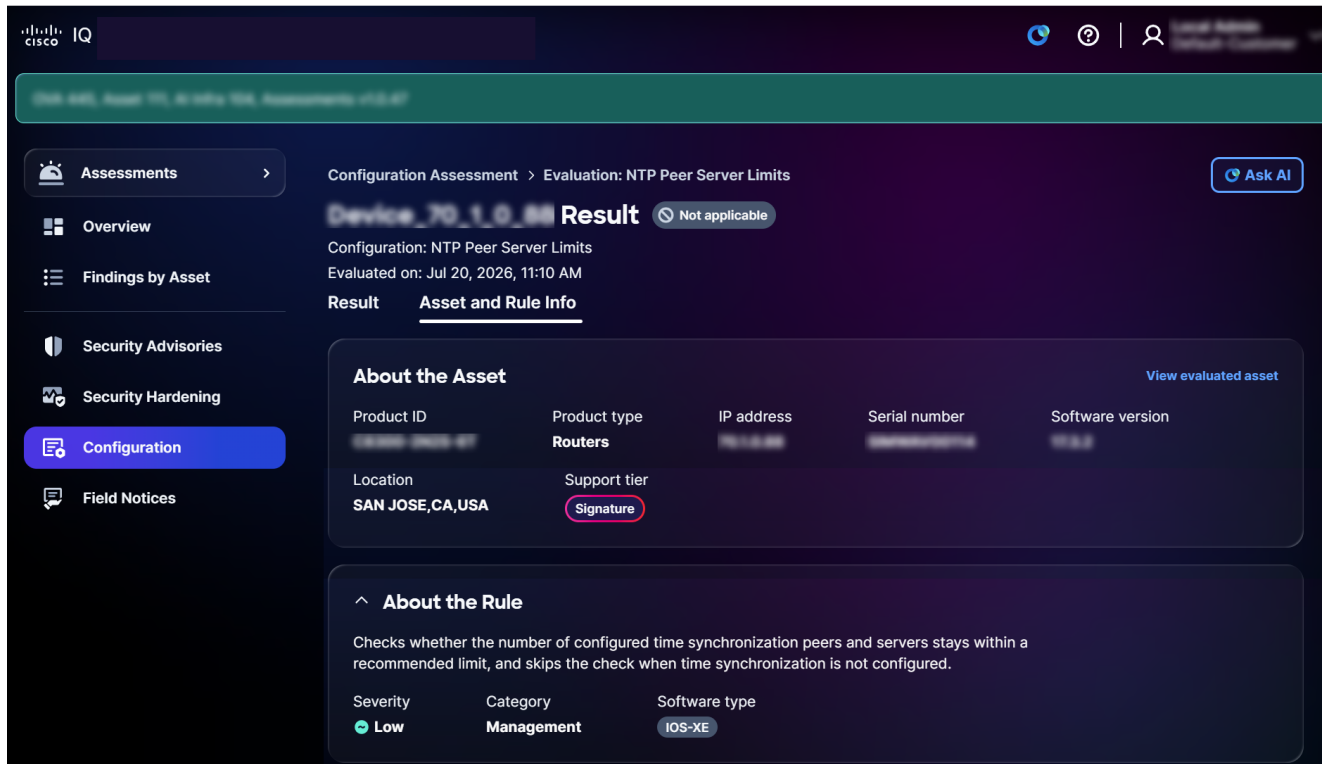


構成標準レベル

- 標準層
- 詳細の検索：評価中に特定された構成の逸脱に関する情報と、証拠ログを提供します。
- 推奨事項：結果に対処し、設定の一貫性を確保するためのガイダンスを提供します。

構成評価の資産およびルール情報の表示

資産およびルール情報の詳細を表示するには、「資産およびルール情報」タブをクリックします。



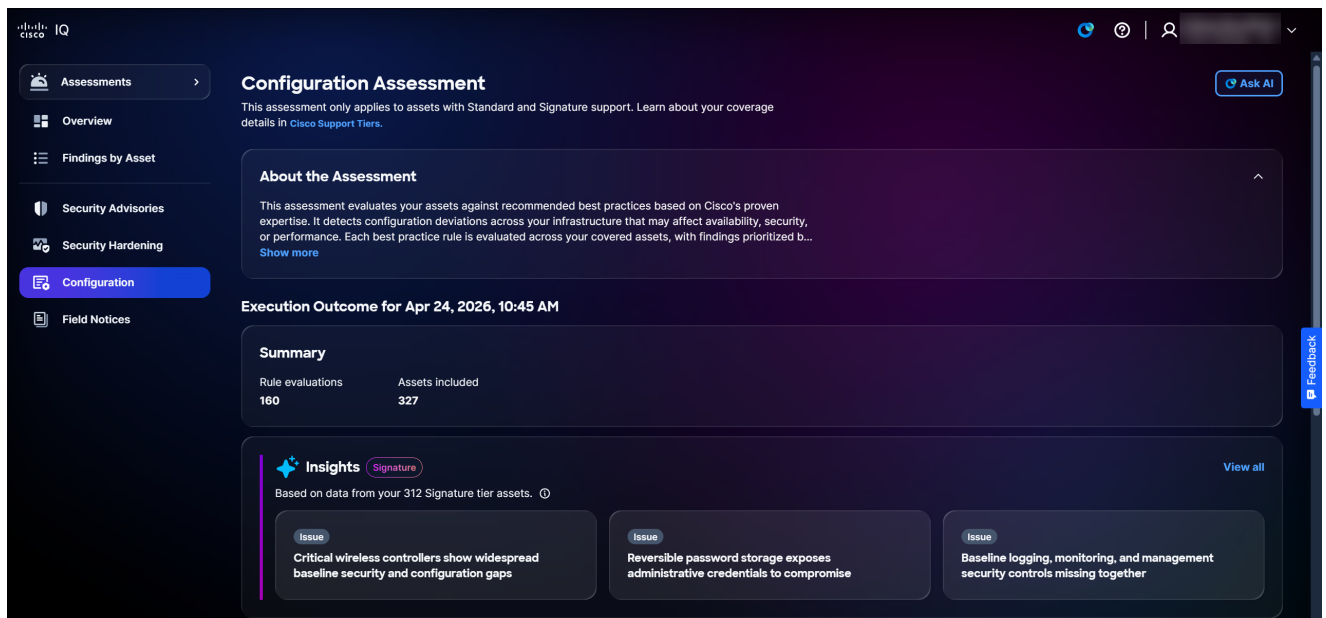
資産とルールの情報

Asset and Rule Infoページが表示され、次の情報が示されます。

- アセットについて：アセットの詳細(製品ID、製品タイプ、IPアドレス、シリアル番号、ソフトウェアバージョン、場所、およびサポート階層など)を提供します。
- ルールについて：ルールの詳細(重大度、カテゴリ、ソフトウェアタイプなど)を示します。

インサイトの表示

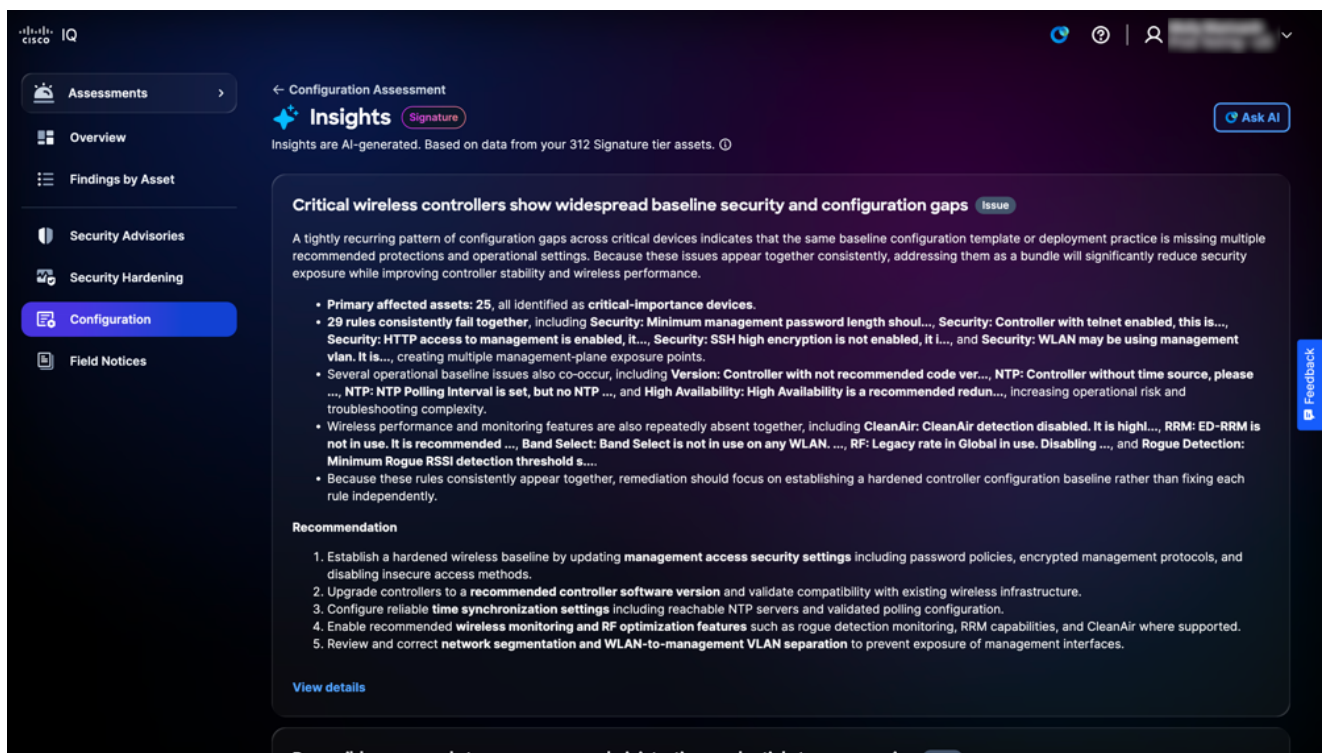
インサイトはAIによって生成され、アセスメントデータを優先順位付けされたキーカードに統合するインテリジェントなダッシュボードとして機能し、複数の結果にわたって重要な構成の違いを強調します。これらの緊急分野に焦点を当てることで、最も影響の大きいインフラストラクチャリスクに効率的に対処できます。また、ベストプラクティスに従ってインフラストラクチャが実行されている領域を特定することで、長所を強調します。



考察

インサイトの詳細を表示するには：

1. インサイトパネルで、「すべて表示」をクリックします。Insightsページには、すべてのインサイトが表示されます。



「インサイト」ページ

2. View detailsをクリックするか、任意のカードをクリックします。次の情報を含むインサイトの詳細ページが表示されます。

The screenshot displays the Cisco IQ Configuration Assessment Insights page. The left sidebar contains navigation links: Assessments, Overview, Findings by Asset, Security Advisories, Security Hardening, Configuration (highlighted), and Field Notices. The main content area is titled 'Critical wireless controllers show widespread baseline security and configuration gaps'. Below the title, it states 'Insights are AI-generated. Based on data from 312 assets with Signature support.' The 'Details' tab is selected, showing an 'Insight' section with a summary and a list of affected assets. The 'Recommendation' section provides five steps for remediation. The 'Affected Assets' section includes a search bar and a table with columns for Name, Product ID, Serial Number, and IP Address.

Insight

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

- **Primary affected assets:** 25, all identified as **critical-importance devices**.
- **29 rules consistently fail together**, including **Security: Minimum management password length should be at least 16 characters**, **Security: Controller with telnet enabled, this is insecure**, **Security: HTTP access to management is enabled, it is insecure**, **Security: SSH high encryption is not enabled, it is insecure**, and **Security: WLAN may be using management vlan. It is insecure**, creating multiple management-plane exposure points.
- Several operational baseline issues also co-occur, including **Version: Controller with not recommended code version**, **NTP: Controller without time source, please use NTP**, **NTP: NTP Polling Interval is set, but no NTP server is configured**, and **High Availability: High Availability is a recommended redundancy feature**, increasing operational risk and troubleshooting complexity.
- Wireless performance and monitoring features are also repeatedly absent together, including **CleanAir: CleanAir detection disabled. It is highly recommended**, **RRM: ED-RRM is not in use. It is recommended**, **Band Select: Band Select is not in use on any WLAN**, **RF: Legacy rate in Global is in use**, **Disabling Rogue Detection: Minimum Rogue RSSI detection threshold should be at least -90 dBm**, and **Rogue Detection: Minimum Rogue RSSI detection threshold should be at least -90 dBm**.
- Because these rules consistently appear together, remediation should focus on establishing a hardened controller configuration baseline rather than fixing each rule independently.

Recommendation

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

Affected Assets

Q Search Product type Product family Product ID Filters 25 results Export

Name	Product ID	Serial Number	IP Address
WLC-3850-1	WLC-3850-1	WLC-3850-1	10.10.10.1
WLC-3850-2	WLC-3850-2	WLC-3850-2	10.10.10.2
WLC-3850-3	WLC-3850-3	WLC-3850-3	10.10.10.3

インサイトの詳細

- **Insight**：複数の所見を包括的に分析して特定された、設定の不整合が繰り返し発生するパターンを強調表示するサマリー、および設定がベストプラクティスに適合する、インフラストラクチャ内の優れた領域を表示します。
 - **推奨事項**：特定された設定ギャップを修正するための実用的な手順を提供します。
 - **影響を受ける資産**：「考察」セクションで定義されているように、設定の変更が特定された特定のデバイスのリストを提供します
3. **Source Findings**をクリックします。ソース結果ページには、考察を裏付ける詳細な個々の結果が表示されます。

Configuration Assessment > Insights

Critical wireless controllers show widespread baseline security and configuration gaps

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

Details Source Findings

Q Search Severity Result 725 results Export

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

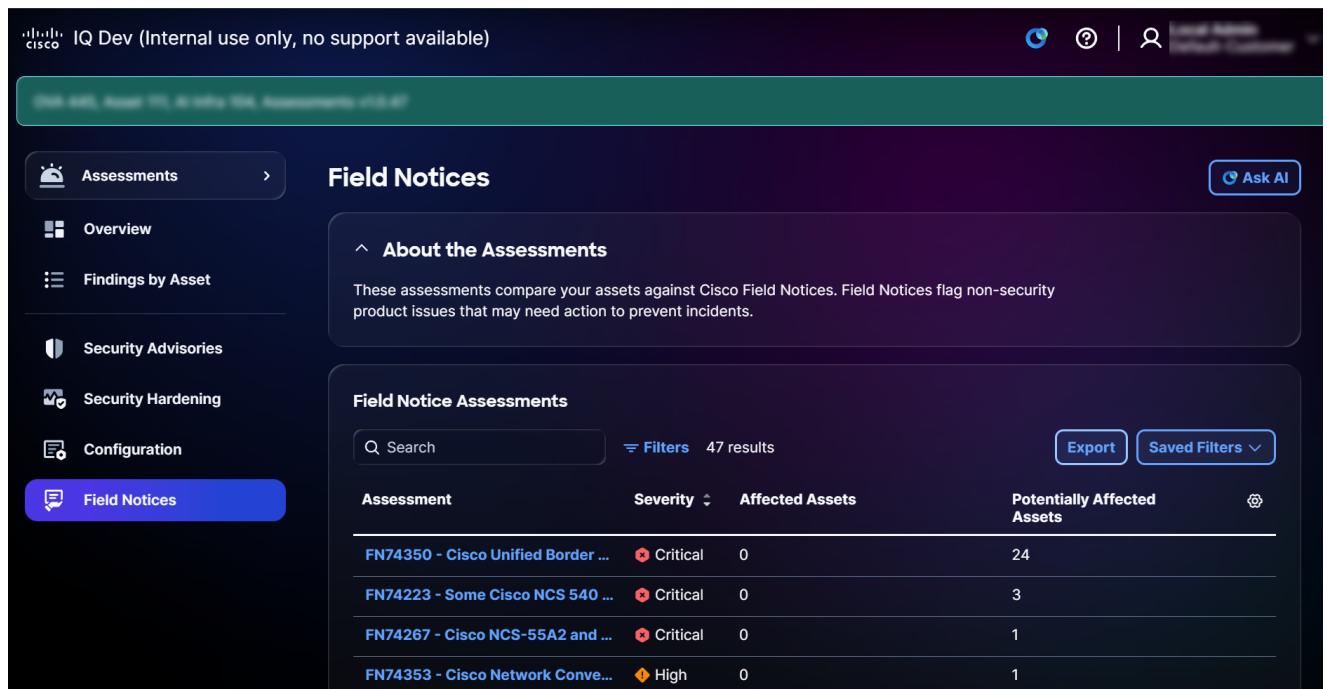
ソースの結果

テーブルビューをフィルタリングするには、重大度および結果のドロップダウンリストからフィルタを選択します。

注：推奨事項と影響を受ける資産は、各インサイトの出力に応じてオプションです。

Field Notice

Field Noticeでは、セキュリティに関連しない重大な製品問題を特定し、その影響の重大度と重要度に基づいて問題を分類することで、製品リスクを管理する組織の能力を強化しています。Field Noticeは、製品の不具合に関する実用的な洞察を提供し、推奨されるアップグレードや回避策を通じて緩和を促進し、運用目標やビジネス目標との整合性を確保します。これにより、製品の信頼性が強化され、リソースの割り当てが最適化され、企業全体で進化する製品の課題に対する復元力が促進されます。



Field Notice

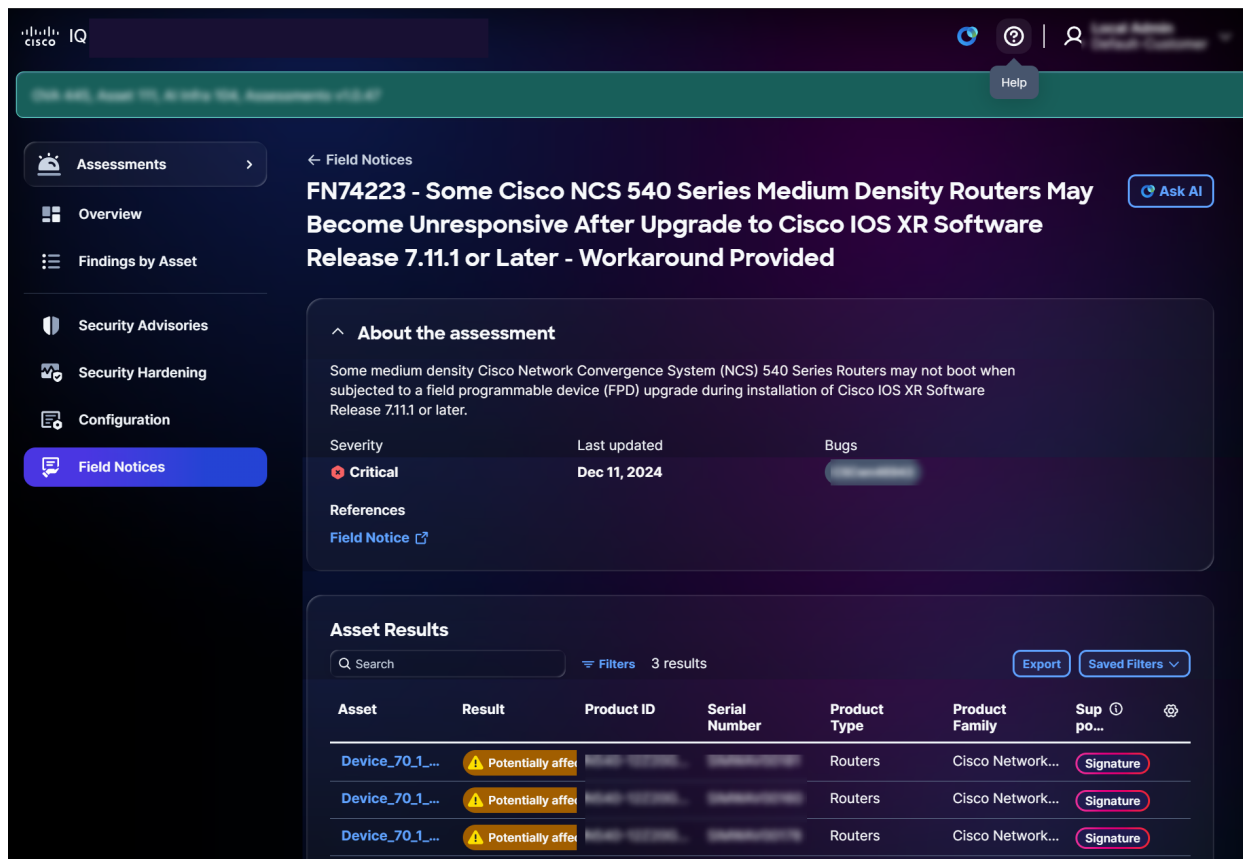
Field Noticeのビューの検索とフィルタリング

ドロップダウンリストからフィルタを選択して、リストビューをフィルタリングできます。Searchフィールドにアセスメント名を入力して、Field Noticeアセスメントを検索することもできます。

Field Noticeのアセスメントの表示

Field Noticeの詳細を表示するには、アセスメントをクリックします。次の評価の詳細が表示されます。

- アセスメントについて：アセスメントの目的を要約して詳細を提供します。
- Field Noticeアセスメント：選択されたField Noticeの影響を受ける資産（脆弱性が検出された資産を含む）のリストを表示します。



Field Noticeのアセスメントの表示

Field Noticeの資産検索結果のビューの検索とフィルタリング

リストビューをフィルタリングするには、ドロップダウンリストからフィルタを選択するか、Filtersをクリックして、使用可能なフィルタのリストからオプションを選択します。Searchフィールドにアセット名を入力して、アセットの結果を検索することもできます。



注：画面のズーム設定によっては、一部のフィルタが非表示になる場合があります。ロールと権限に応じて、異なるフィルタを使用できます。

Field Noticeの資産結果のエクスポート

Field Noticeのアセスメント資産結果をエクスポートするには、エクスポートをクリックします。詳細は、『[情報のエクスポート](#)』を参照してください。

Field Noticeの資産評価結果の表示

資産のアセスメント結果の詳細を表示するには、資産アセスメント結果から資産をクリックします。アセットのアセスメント結果の詳細ページが表示されます。

次のタイプの結果を表示できます。

- Affected:Field Noticeについて自動的にチェックされたすべての基準を満たし、該当することを確認するための追加の手動検証を必要としない資産を示します。

- Potentially Affected:Field Noticeで自動的にチェックされるすべての基準を満たしているが、本当に影響を受けるかどうかを確認するために追加の手動検証が必要な資産を示します。

「評価 – セキュリティ強化」タブでは、次のプロンプトが表示されます。

- ネットワークデバイスに対するシスコのセキュリティ強化のベストプラクティスは何ですか。
- Cisco IOS XEデバイスのセキュリティを強化するにはどうすればよいですか。
- ルータおよびスイッチのセキュリティを強化する主要な手順を列挙する。
- シスコデバイスに推奨されるベースライン強化設定は何ですか。
- セキュリティ強化のベストプラクティスに違反している資産はいくつありますか。

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VAに正常にログインする必要があります。

- デフォルトユーザ名:admin
- Default Password:VA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、『スタートアップガイド』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ィールメニューから行えます。

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）。

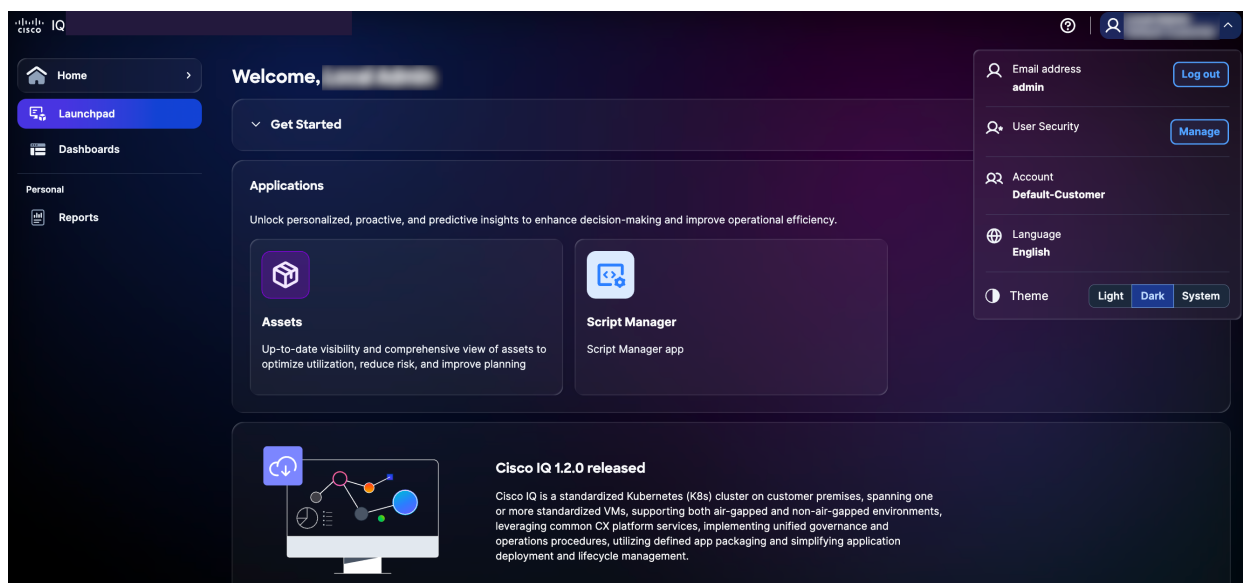
 注:15分間に3回、正しいパスワードの入力を試みています。3回の試行がすべて失敗した場合、セキュリティを保護するためにアカウントが一時的に30分間ロックされます。ロックアウト期間中はログインできません。失敗した試行回数が多すぎるため、「アカウントがロックされました。Please try again later.」が表示されます。アカウントは30分後に自動的にロック解除され、その時点でログインまたはパスワードのリセットを試みることができます。

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. Homeページから、User Profile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。



セキュリティの使用

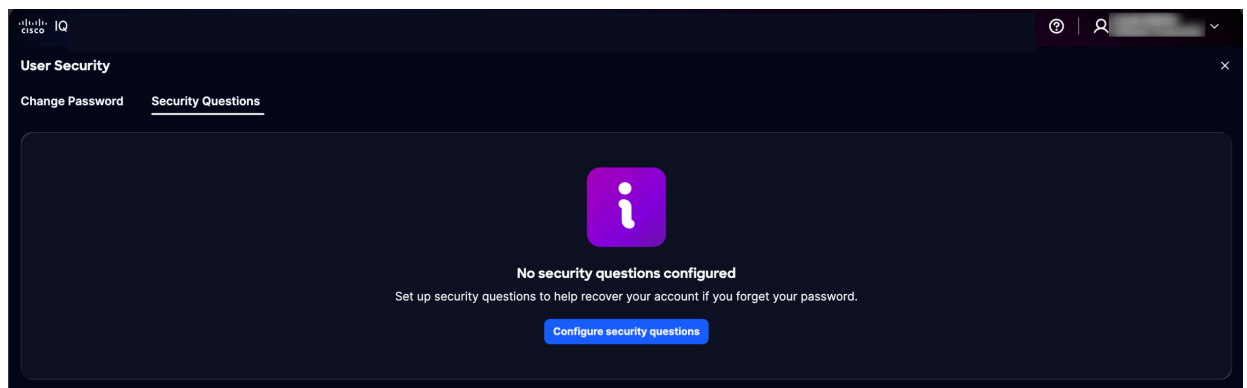
2. User securityでManageをクリックします。User Securityページが表示されます。



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

セキュリティの質問

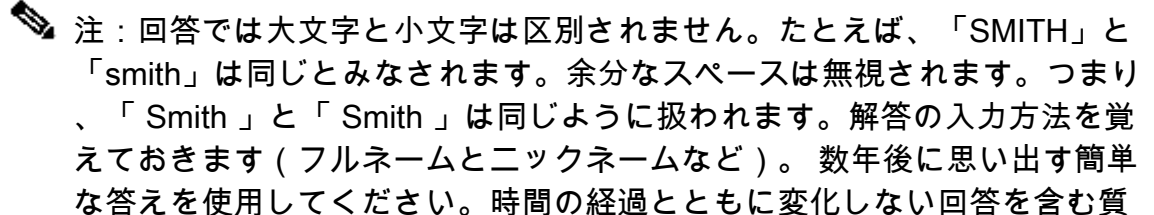
3. Security Questionsをクリックして、タブを開きます。



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

Security Questionsタブ

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



 問を選択してください。

 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。

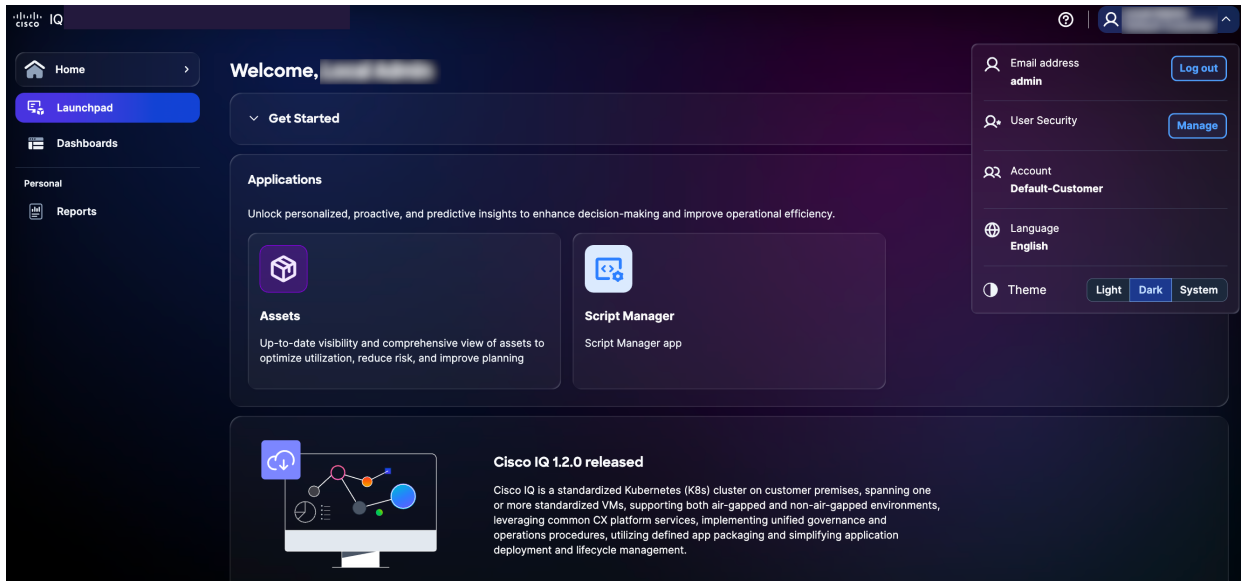
- 。 ローカルアカウントの管理者またはユーザーである
- 。 ローカルアカウントを使用している(シングルサインオン(SSO)または外部認証ではない)
- 。 Cisco IQにログインしています
- 。 現在のパスワードがわかっている

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. ホームページから、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。



ユーザーセキュリティの管理

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. 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。

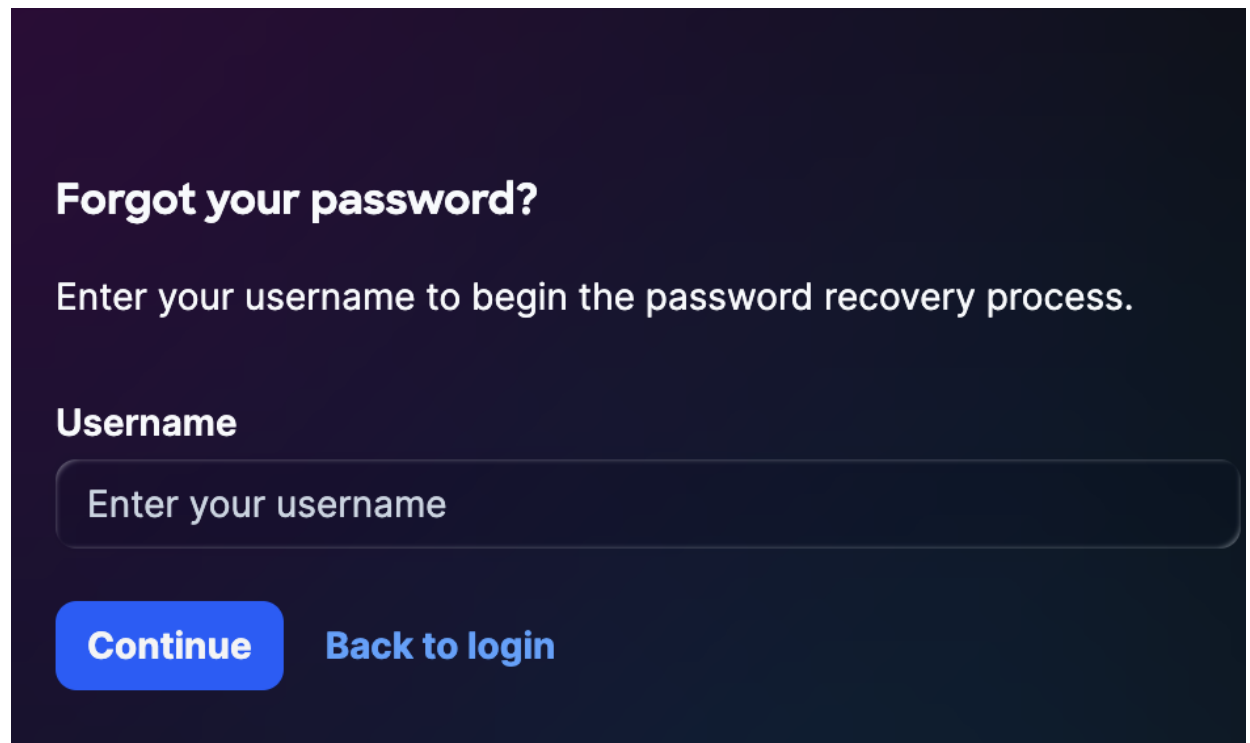
パスワードは、Cisco IQ VMを含むCisco IQシステムで更新されます。

パスワードを忘れた場合のリセット

パスワードは、セキュリティの質問の検証プロセスを使用してリセットできます。

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 VA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。



Forgot your password?

Enter your username to begin the password recovery process.

Username

Enter your username

Continue **Back to login**

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。

Verify Identity

Answer the following security questions to verify your identity.

What city were you born in?

Enter your answer

Show

What is your mother's maiden name?

Enter your answer

Show

What was the name of your elementary school?

Enter your answer

Show

Verify and continue

Back to login

IDの確認

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 and continueをクリックします。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。

Set New Password

Choose a strong password that contains the following:

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

New password

Show

Confirm password

Show

Reset password

Back to login

パスワードのリセット

 注:15分間に3回、正しいパスワードの入力を試みています。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。

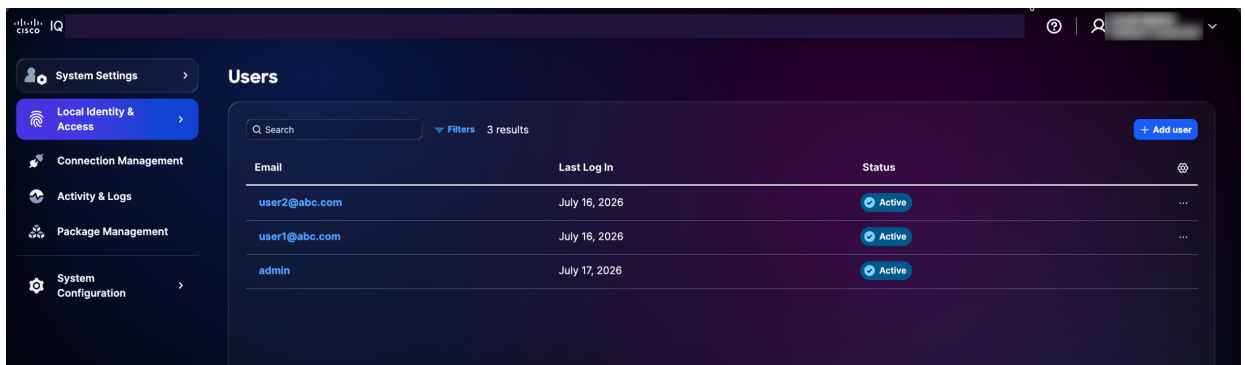
- 新しいパスワードを入力します。
- 確認のため、パスワードを再入力します。
- [Submit] をクリックします。

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。

- System Settings > Local Identity & Access > Usersの順に移動します。Usersペー

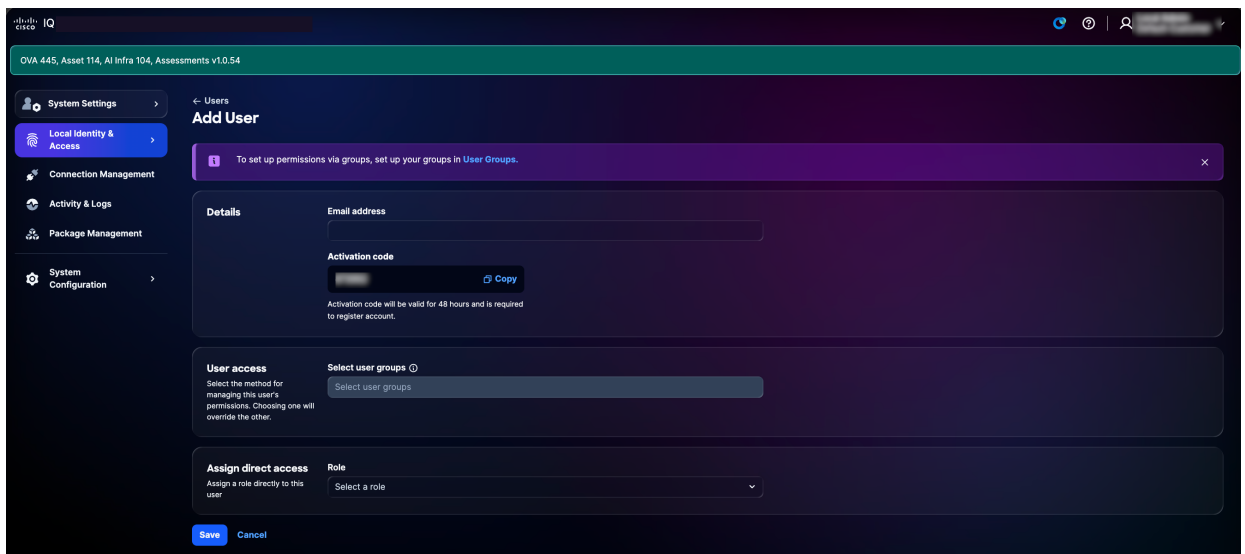
ジが表示されます。既存のすべてのローカルユーザとそのステータスが表示されます。



ユーザページ

 注：非セキュアチャン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。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。

- 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. [Email Address] 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。表示されたアクティベーションコードをユーザと共有します（登録に必要）。

5. User accessで、Select user groupsドロップダウンリストからユーザ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。

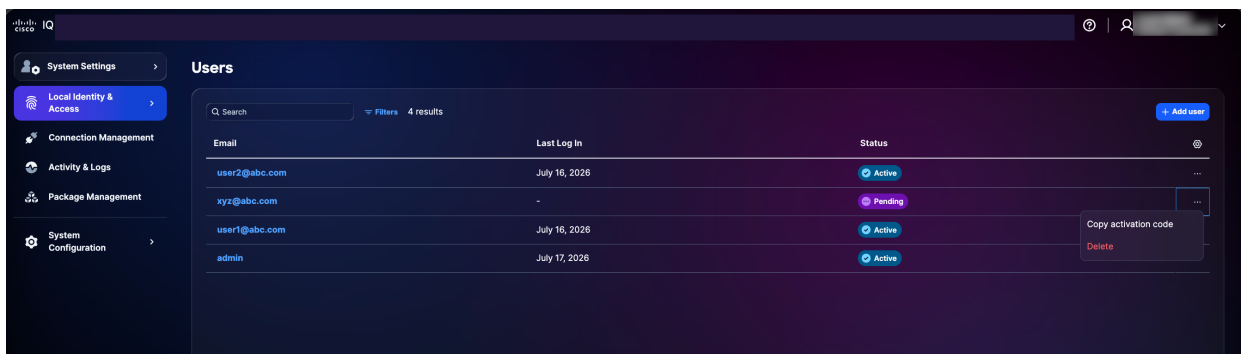
6. Assign direct accessで、Roleドロップダウンリストからroleを選択します。次の2つのロールを使用できます。

- 。 ビューア：アプリケーションの表示とアクセス
- 。 アカウント管理者：モジュールにアクセスし、システム管理とアイデンティティプロバイダー(IDP)以外の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。

8. リストで新しく作成したユーザを検索し、Status列にPendingと表示されていることを確認します。

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をクリックします。



アクティベーションコードのコピー

10. ドロップダウンリストからアクティベーションコードのコピーを選択します。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。
11. このコードを安全にユーザと共有します（たとえば、安全な内部チャネルを通じて）。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。

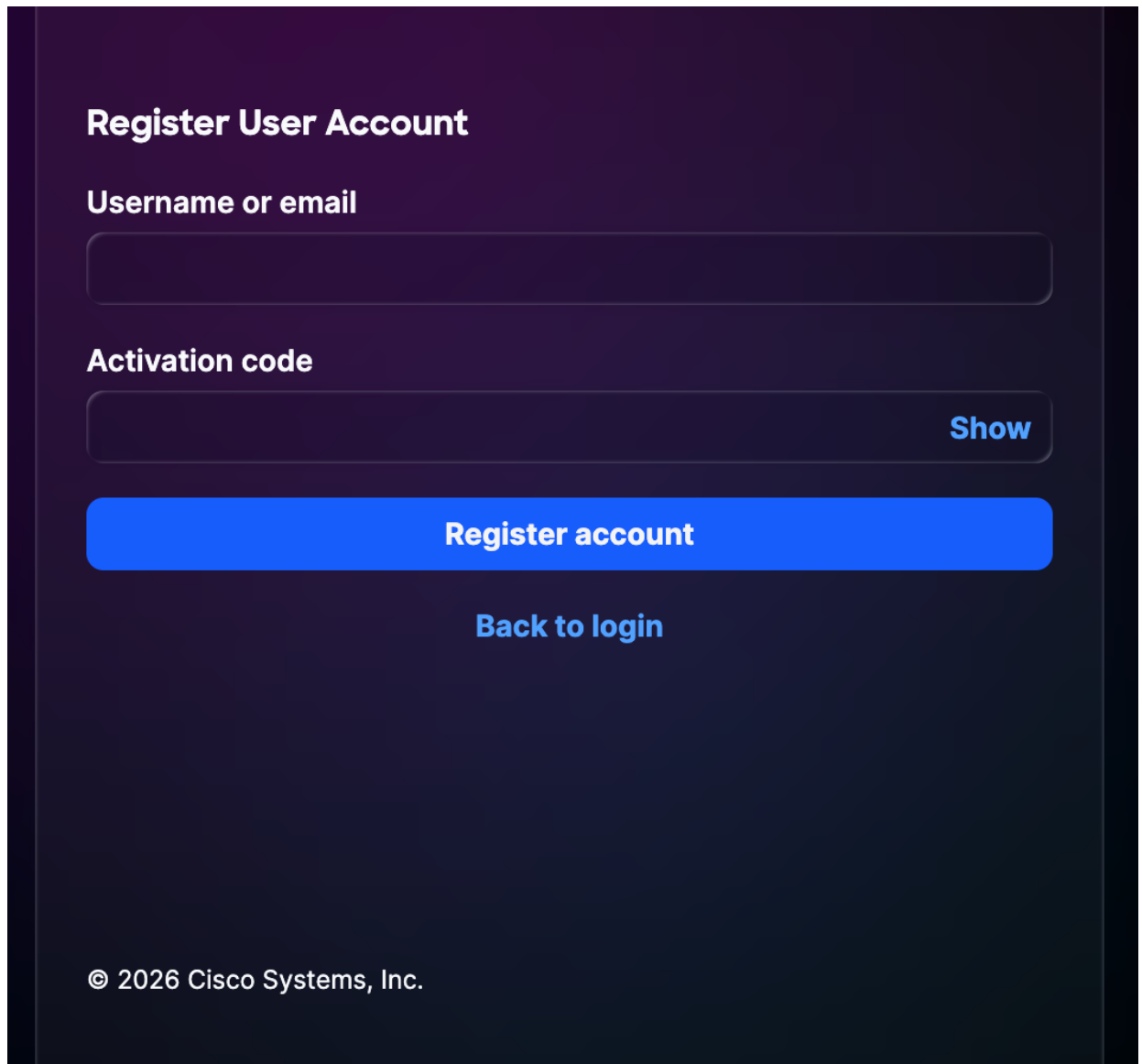
 注：非セキュアチャネルではアクティベーションコードを共有しないでください。コードが紛失または改ざんされた場合は、メニューアイコンを使用して新しいアクティベーションコードを再生成すると、以前のアクティベーションコードが無効になります。アクティベーションコードは48時間有効です。コードの有効期限が切れた場合は、アカウント管理者に新しいコードをリクエストしてください。

12. ログアウトするには、右上隅にあるUser Profile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。

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

Register User Account

Username or email

Activation code [Show](#)

Register account

[Back to login](#)

© 2026 Cisco Systems, Inc.

新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。

Set New Password

Choose a strong password that contains the following:

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

New password

Show

Confirm password

Show

[Reset password](#)

[Back to login](#)

新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、ユーザは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。(「[セキュリティ質問の設定](#)」を参照)。

ローカル・ユーザー・グループの管理

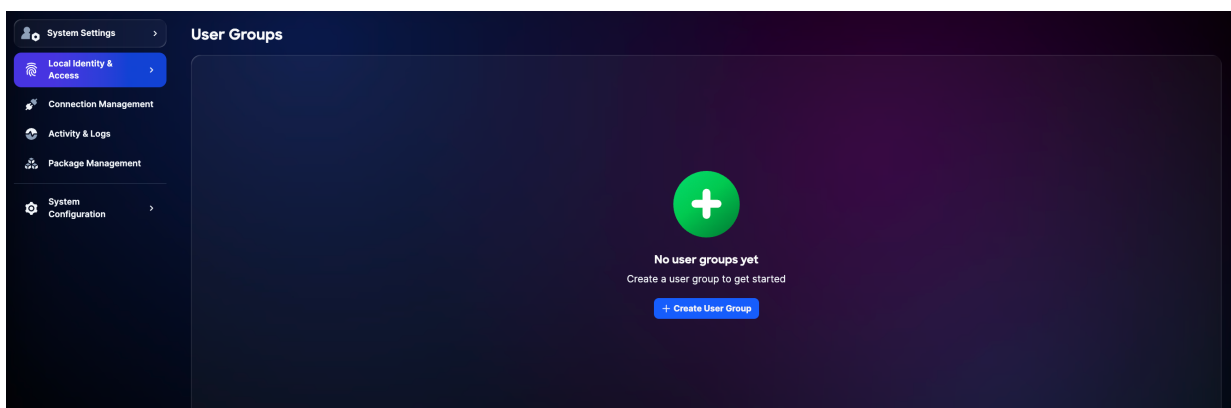
ユーザー・グループを使用すると、アカウント管理者は複数のローカル・ユーザーの役割を一度に管理できます。ロールを各ユーザに個別に割り当てる代わりに、グループを作成し、ロールと一連のユーザをそのロールに割り当て、ロールまたはメンバーシップを1か所で更新できます。ユーザグループの管理はすべて、Local Identity & Accessページから実行します。

 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。詳細は、『[ローカルユーザの追加](#)』を参照してください。

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。

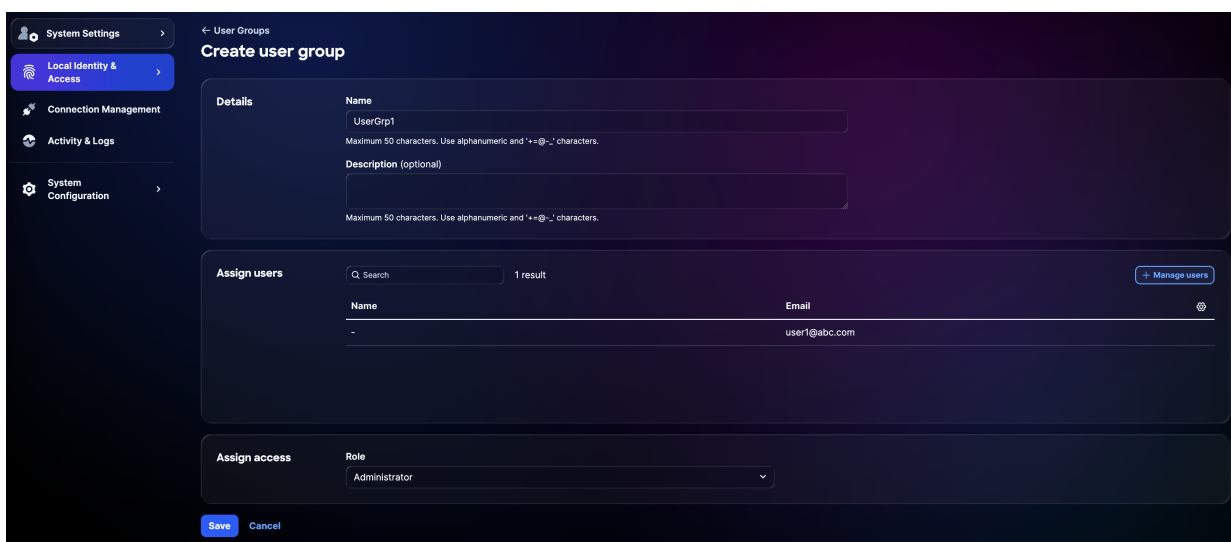
1. System Settingsで、Local Identity & Access > User Groupsの順に選択します。User Groupsページが表示されます。



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文字で、英数字と+ = @ - _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：モジュールの表示とアクセス（読み取り専用）
- 管理者：モジュールにアクセスし、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. 目的のグループのMore Optionsアイコン> 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

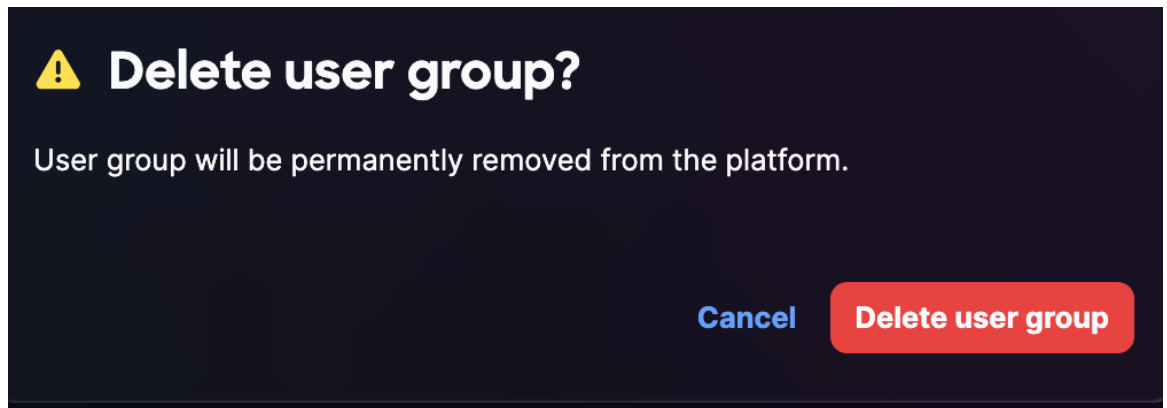
3. 必要な変更を行います。
4. [Save] をクリックします。

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

VA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IDP構成を使用してログインできます。

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。

表2: Cisco IQの特性

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3: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 Customer 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ー名	ユーザ名	NA

5. 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: .*

6. アプリケーションでSingle Logout(SLO)を設定します。

表4: 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	サービスプロバイダー(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

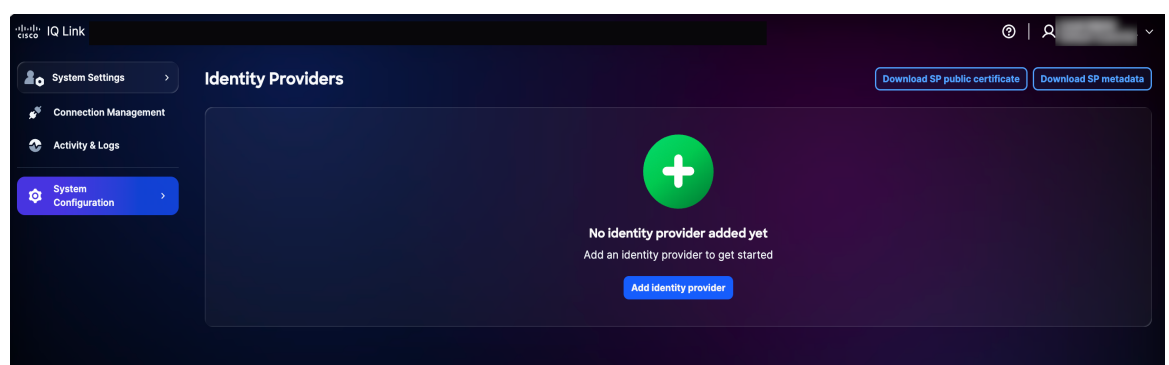
8. Downloadアイコンをクリックして、「IDP Metadata XML」ファイルをダウンロードします。

9. 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。

Okta IDPの追加

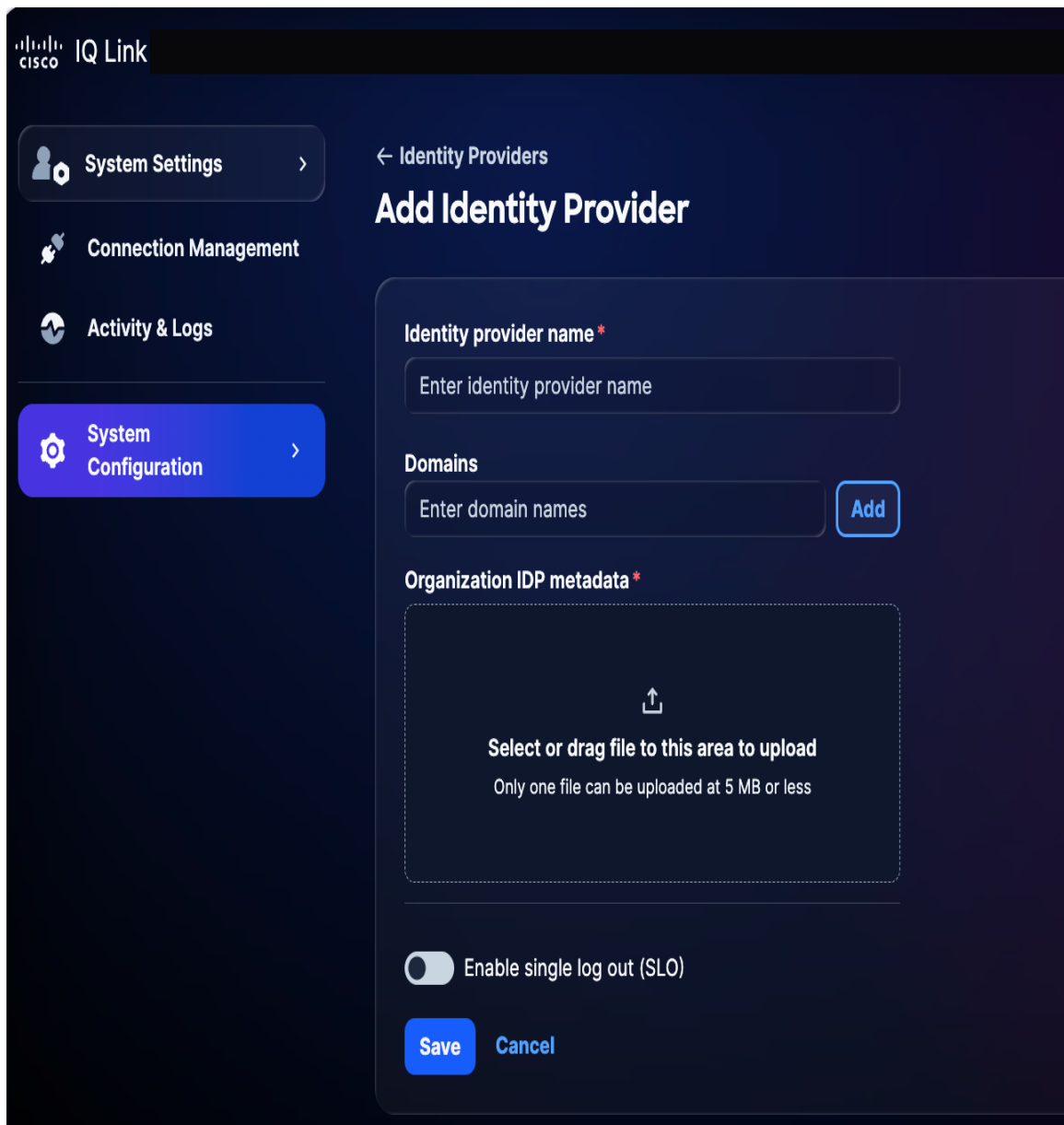
Cisco IQでIDPを追加するには：

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。



 注：一度に追加できるIDPは1つだけです。

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

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で設定されたドメイン名をDomain(s)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。

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の順に選択します。Map user rolesページが表示されます。

×

Map identity provider roles to system roles to assign permissions.

Map User Roles

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

+ Add identity provider role

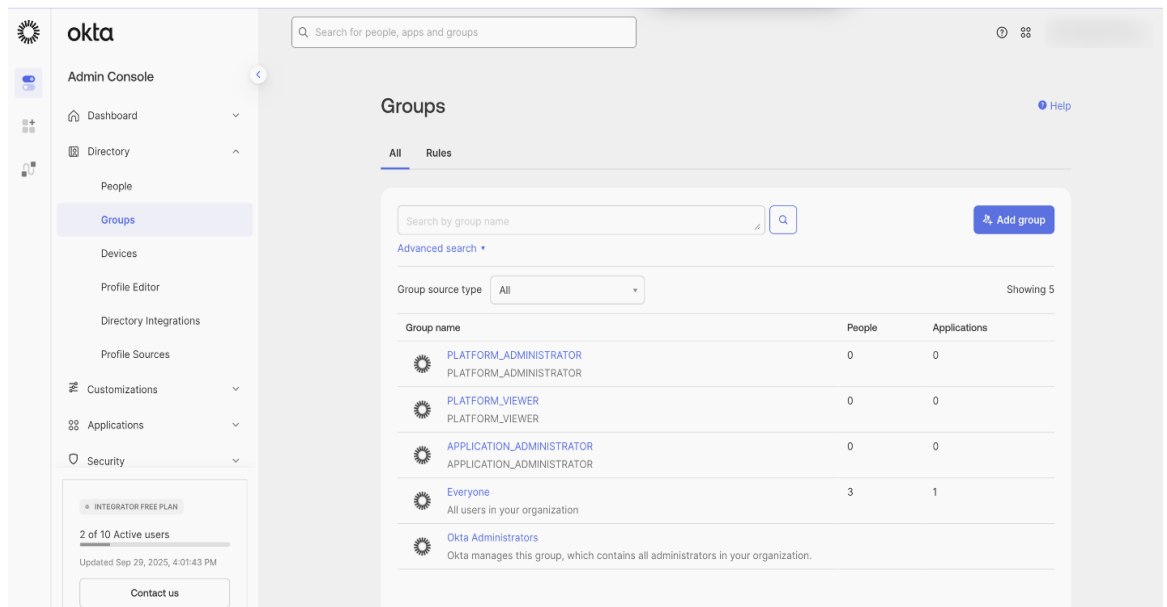
Save

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ル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ル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。



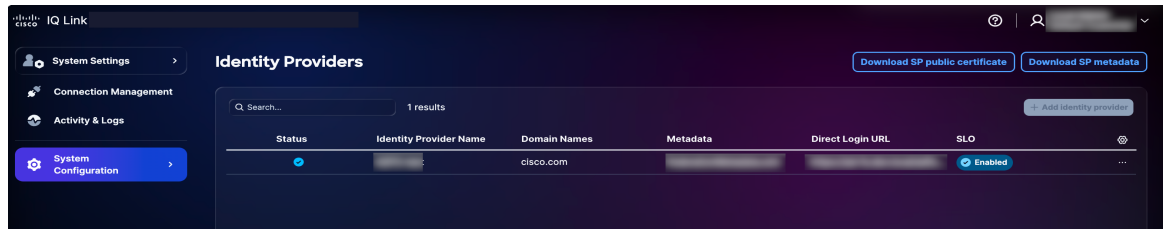
ロールマッピングの参照

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。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。

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. アイデンティティプロバイダーのホームページで、Download SP public certificateをクリックします。



SP公開証明書

2. ダウンロードしたファイルを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. SLO URLを入力します(例：https://ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com/saml/logout)。
6. SP発行者を入力します(例：ciq-xxx-xxx-37-160.cx-hub-rtp.cisco.com)。
7. [Submit] をクリックします。
8. IDPメタデータファイルを再度ダウンロードします。
9. 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。
10. Enable single log out (SLO) トグルボタンをオンにします。
11. 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。
12. 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とSLOのフローが正常にテストされている

IDP問題のトラブルシューティング

次の表に、IDPステータス、証明書エラー、SSOログイン障害、およびSLO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を示します。

表5：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

この項では、パスワードベースおよび公開キーインフラストラクチャ(PKI)または証明書ベースの認証をサポートするCisco IQのSAML IDPとしてMicrosoft Active Directory(AD)フェデレーションサービス(FS)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 2016 + (2019推奨)
- ユーザアカウントとのAD統合の設定
- ADFSサーバ上の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
- エンタープライズ認証局(CA) (インストール済みまたは到達可能)
- ドメイン管理者またはエンタープライズ管理者の権限 (PKIのみに必要)
- ADFSサーバ設定の詳細 (下の表に記載)

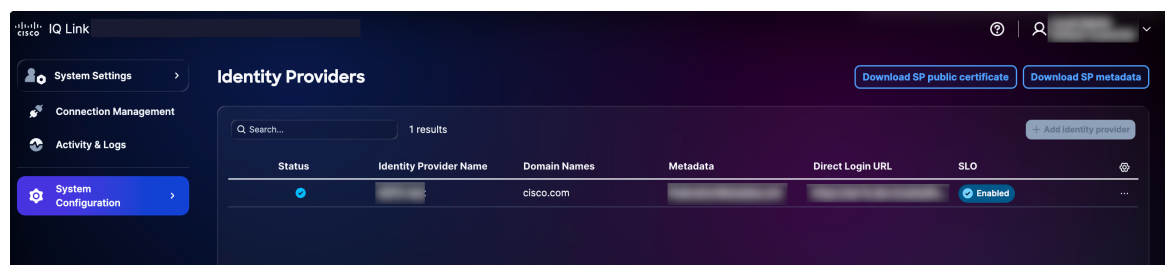
表6：認証フローの概要

項目	説明	例
Cisco IQ FQDN (オプション)	ユーザー配置ホスト名	<Your-CIQ-FQDN>例 : dev35-23.cx-xxx-xxx.cisco.com
ADFSサーバーURL	ユーザADFSサーバアドレス	https://<Your-ADFS-HOSTNAME>(https://adfs.dev.localなど)
会社のドメイン	電子メールドメイン	<お客様のドメイン>
ADグループ	Active Directoryグループのドメイン名(DN)	CN=Role - CXIQ開発者 OU=Groups, DC=dev, DC=local
CA名(PKI)	エンタープライズCA名	<Your-CA名>
証明書認証ポート(PKI)	ADFS代替TLSポート	49443
SSL証明書の拇印	ADFSサーバーSSL証明書	<Your-SSL-CERT-THUMBPRINT>

ベースADFS SAMLの設定

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サーバ(C:\など)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、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 (「Cisco IQ」 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に必要なポリシー) 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(Azure MFA、Time-Based One-Time Password(TOTP)が設定されている。

このポリシーが、構成された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、最終的には要求をステータス `urn:oasis:names:tc:SAML:2.0:status:RequestDenied` で拒否します。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  
To set “Permit everyone” (no MFA requirement), run the following command:  
Set-AdfsRelyingPartyTrust -TargetName “
```

```
”  
-AccessControlPolicyName “Permit everyone”  
You can also create the trust through PowerShell:
```



```

-Add-AdfsRelyingPartyTrust `
=Name “

” `

-Identifier “

” `

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

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

```

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7：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	PKI/証明書認証	ADFSは、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 - Production」)。

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

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"]
=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),
@RuleTemplate = "LdapClaims"
@RuleName = "Send UPN"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"),
query = ";userPrincipalName;{0}", param = c.Value);
@RuleName = "Transform Email to NameID"
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
@RuleName = "Send Group Membership"
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/group"),
query = ";memberOf;{0}", param = c.Value);
'@
```

3. 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
```

書き込みホスト「要求ルールが正常に構成されました。」 -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. 次のコマンドを実行して、ユーザのグループメンバーシップを確認するようにユーザ名を設定します。

```
$username = “username”
```

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. 次のコマンドを使用して、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開発者 , 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を介して検証できない内部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
```

- 。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:-ca.cer” -CertStoreLocation
“Cert:”
```

3. ADFSサービスを再起動して変更を適用します。

再起動サービス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、インストールを確認します。

```
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. 次のタブで設定を行います。

- 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、ユーザのユーザプリンシパル名 (UPN) か、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、テンプレートをパブリッシュします。

```
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,
```

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. 次のコマンドを実行して、Mac上のCAを信頼します。

```
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。

```
EEnable-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
```

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”)
-PrimaryExtranetAuthenticationProvider @(“CertificateAuthentication”, “FormsAuthentication”)
```

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で設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ディングを作成します。

```
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。

```
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)" -Fore
```

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:\IntermediateCA  
Write-Host "Moved $($bad.Count) cert(s) from Root to Intermediate CA store" -Foregroun
```

3. 次のコマンドを実行して、非自己署名証明書が信頼された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、下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8:SChannelレジストリ設定

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ようにするには、そのCA証明書がSystemCertificatesstore内にある必要があります。

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*に存在す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、LocalMachineストアにインポートします。

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

}

ADFSサーバーのリブート (必須)

次のコマンドを使用して、ADFSサーバーを再起動します。

```
Restart-Computer -Force
```



注: ClientAuthTrustModeレジストリの変更は、サーバー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サーバーで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 Service"}).AbsoluteUri
Invoke-WebRequest -Uri $metadataUrl -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ブラウザーを使用して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、「<your-adfs-server>」をADFSサーバーのホスト名に置き換えます。

2. 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。

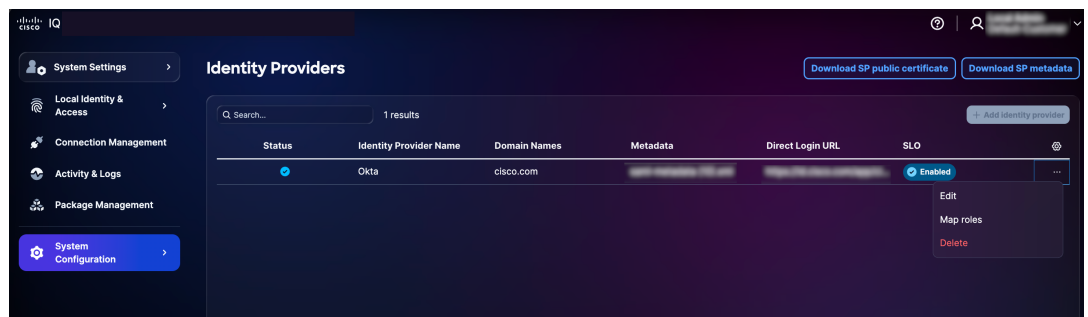
```
$searcher = New-Object DirectoryServices.DirectorySearcher
$searcher.Filter = "(&(objectClass=group)(cn=Role - CXIQ*))"
$searcher.PropertiesToLoad.Add("distinguishedName") | Out-Null
$searcher.PropertiesToLoad.Add("cn") | Out-Null
$searcher.FindAll() | ForEach-Object { $_.Properties["distinguishedname"]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

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。

Cisco IQ Link_IDP

×

Map identity provider roles to system roles to assign permissions.

Map user roles

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

+ Add identity provider role

Save

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DNではなく、解析済みの名前（CXIQ Developers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。

チャン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（「[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）。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. 正常にログインできるかどうかを確認します。

 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9: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
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 無効なACS URL：確認：https://your-fqdn/saml/acs
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	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 - Production" |  
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 - Production" |  
Select-Object SamlEndpoints
```

SSO用のMicrosoft Entra 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または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

- 。 IDテナントの入力 (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10: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アドレスドメイン	<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

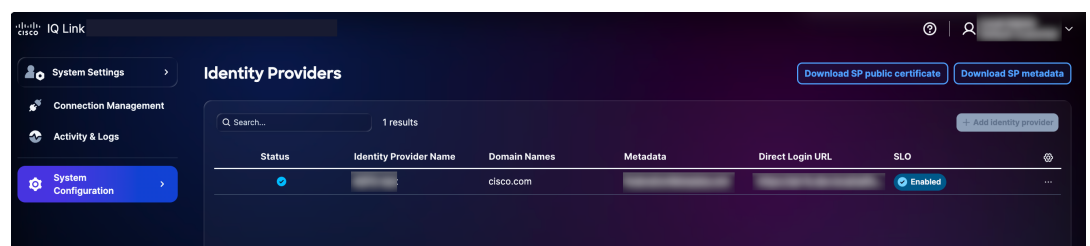
エンタープライズアプリケーションの作成

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。これは、VAから次の手順を実行して取得できます。

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。

4. 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。
5. 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。
 - 識別子 (エンティティID) :<YOUR-CIQ-FQDN>
 - 応答URL(ACS URL):https://<YOUR-CIQ-FQDN>/saml/acs
 - サインオンURL:https://<YOUR-CIQ-FQDN>/saml/login
 - ログアウトURL:https://<YOUR-CIQ-FQDN>/saml/logout
6. [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と正確に一致する必要があります。これは通常、展開のFQDNです。

7. SAML属性および要求を設定するには、属性および要求セクションで編集をクリックします。
8. 次の要求を構成します。

表11：必要な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/cl

請求	ソース属性	名前空間
givenname	ユーザー .givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/cl
姓	ユーザ。姓	http://schemas.xmlsoap.org/ws/2005/05/identity/cl
name	ユーザー .userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/cl
[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.groupsではなくuser.assignedrolesを使用します。
- 。 Namespaceフィールドは空である必要があります。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
- 。 競合が発生するため、user.groupsに重複するグループ要求を追加しないでください

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、または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で、シングルサインオン > SAML署名証明書の順に選択します。
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12：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
general_account_administrator (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
general_account_viewer	CXIQ開発者	読み取り専用アクセス
general_account_viewer	CXIQビューア	読み取り専用アクセス

 注：App Role Value文字列は、Entra IDで設定されたとおりに使用してください(詳細は、「[App Rolesの設定](#)」を参照してください)

4. [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 success"
```

予想される出力

SAML 2.0準拠の認証がユーザuser@domain.comに対してフルネーム
：N/Aおよび1グループで成功しました

抽出されたグループ：CXIQ Admins (元：CXIQ Admins)

抽出されたグループの合計：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 CSを備えたWindows Server (例:「DEV-ADCS-CA」)
- 。 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、テンプレートをパブリッシュします。

```
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

例えば、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>は自分の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. 要求をCAに送信するには、次のコマンドを実行します。

```
certreq -submit -config "
```

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

5. 証明書をCAに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へのユーザ証明書のインポート(MacOS)

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
```

”

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証明書を検索し、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分散ポイントの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を有効にして、ターゲットユーザまたはグループを追加します。
4. [構成]で、[保護レベル]を[単要素認証]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
- 。 ユーザー属性: userPrincipalName

これにより、証明書のサブジェクト代替名(SAN)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 (たとえば、別のユーザの証明書や期限切れの証明書) 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13：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	Entra ID要求の設定を確認します(詳細については、「

お問い合わせ内容	原因	修正
せん	子メール属性がありません	SAMLシングルサインオンの設定 」を参照)。ユーザにmail属性が設定されていることを確認します。 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、「 アプリケーションロールへのユーザの割り当て 」を参照)。
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	
グループ要求の複製	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。 アプリケーションのロールによるアプローチを使用します(詳細は、『 アプリケーションのロールの設定 』を参照してください)。
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。	グループ要求の設定のNamespaceフィールドをクリアします。
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	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。 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、『 到達可能性の問題に対するCRLの回避策 』を参照してください)。
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	MacOSキーチェーンアクセスでユーザ証明書がインポートされていること(詳細は「 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)、必要な設定でEntra IDでCBAが有効になっていること(詳細は「 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が再起動します。
AADSTS500191	インターネットからCRLに到達できない	
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	

お問い合わせ内容	原因	修正
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です。ラボでは30000を使用します)。
仮想アプライアンスのステータスが「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。Cisco Discovery Protocol(CDP)を使用せずに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) を作成する
- 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IDPを追加する
- アプリケーションロールの値を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ユーザと一致する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ファイル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する

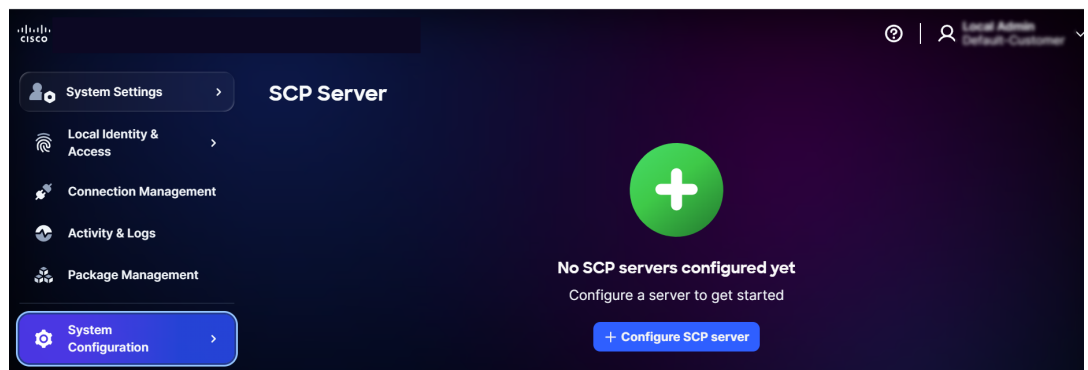
- クライアントマシン上のCA証明書を信頼する
- Protection > Certificate authoritiesで、CAルート証明書をEntra IDにアップロードします。
- 認証方法でCBAを有効にする
- ユーザー名バインドの構成 (PrincipalNameおよび userPrincipalName)
- CBAログインがエンドツーエンドで動作することを確認します。

SCPサーバの追加

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。

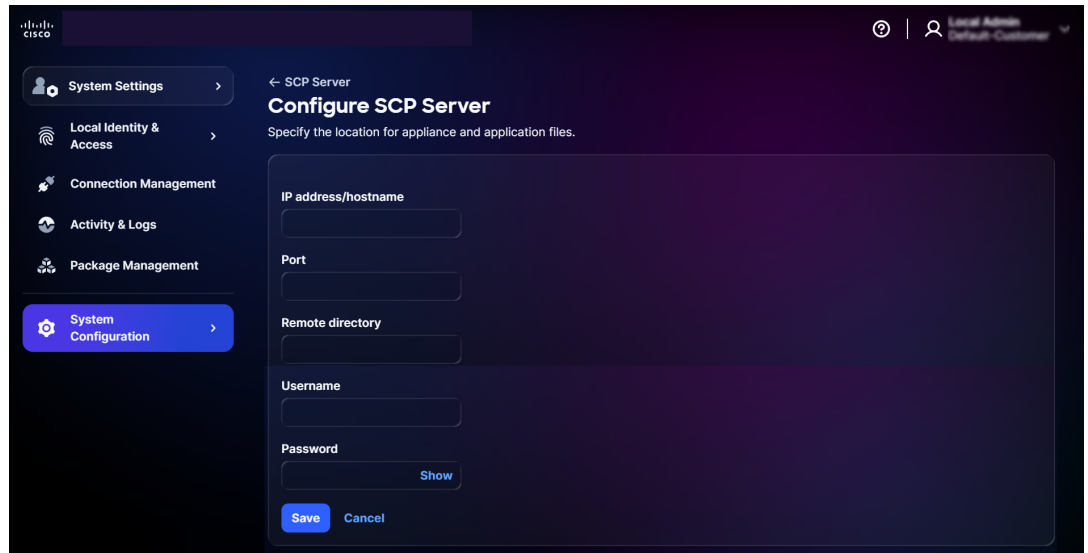
SCPサーバを追加するには

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。Configure SCP Serverページが表示されます。



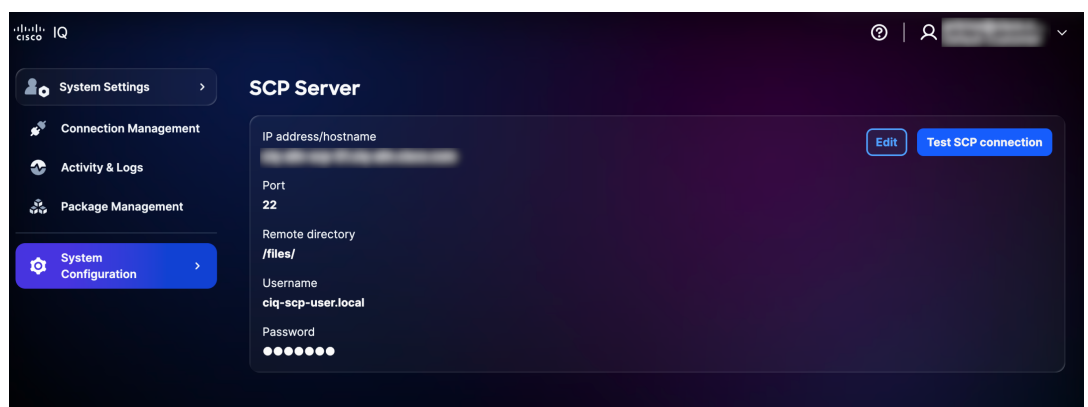
SCPサーバの設定

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

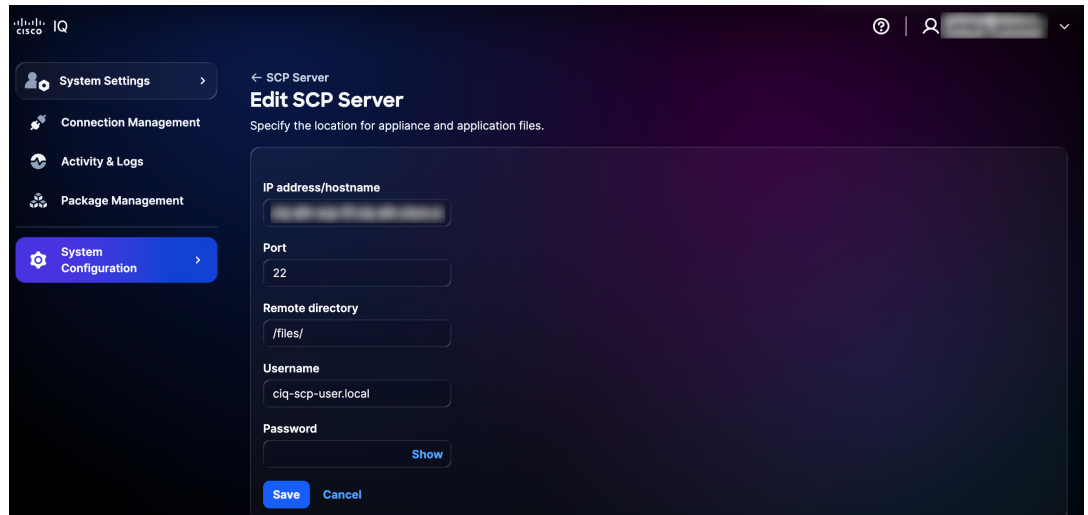
既存のSCPサーバを編集するには、次の手順を実行します。

1. SCPサーバページに移動します。



SCPサーバを追加

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

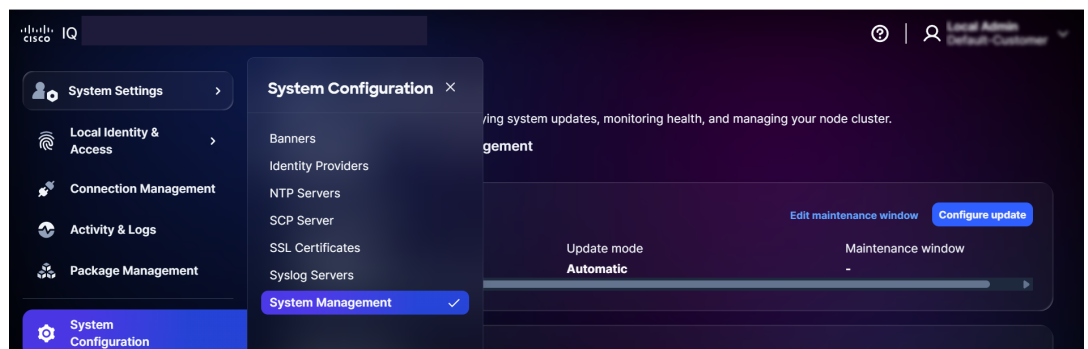
- 必要に応じて詳細を変更します。
4. [Save] をクリックします。

システム管理

UIを使用して最新バージョンのCisco IQ VA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。

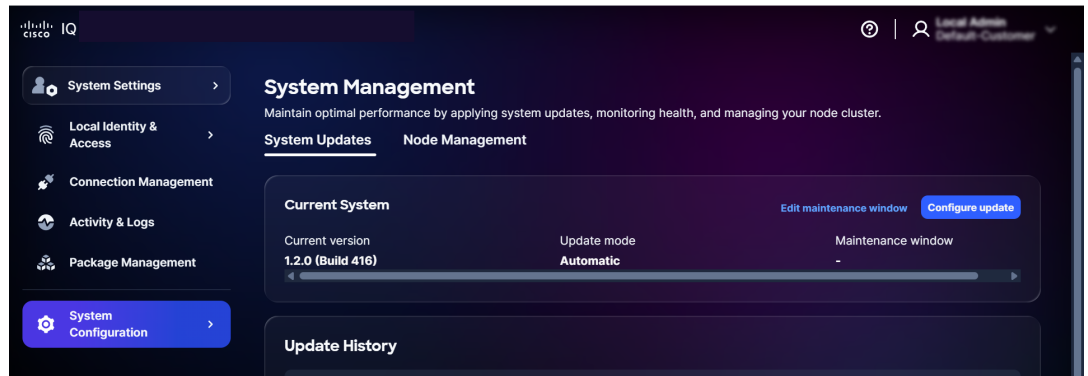
システム更新の再スケジュール

システム更新を再計画する手順は、次のとおりです。



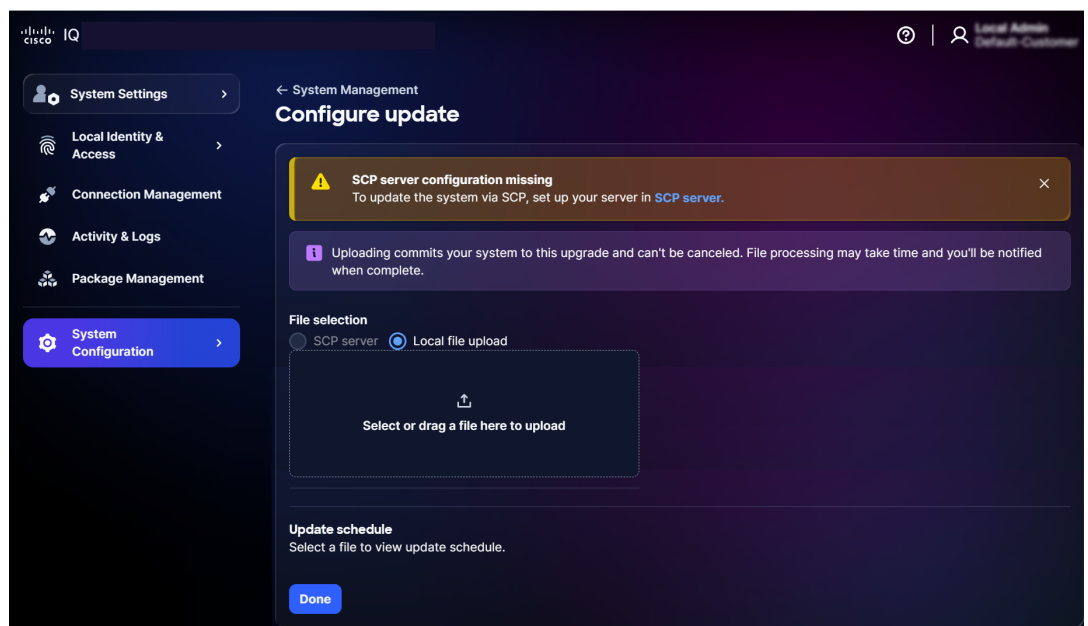
システム管理

1. System Settings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. Configure updateをクリックします。Configure updateページが表示されます。



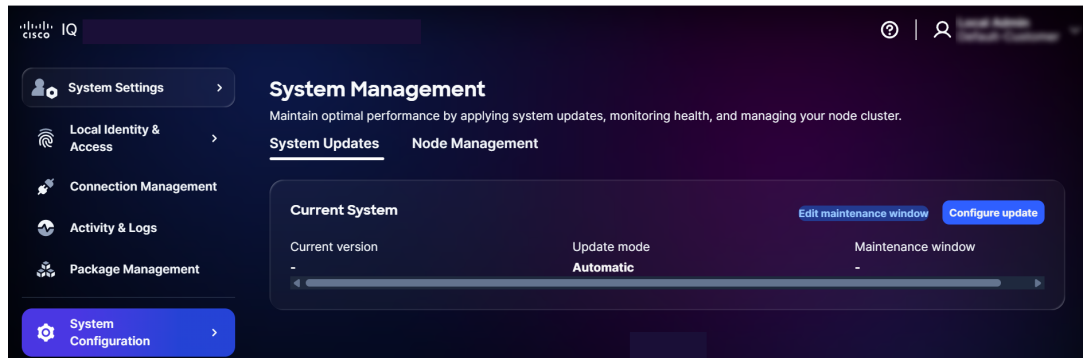
アップグレードの設定

3. 別の日時をスケジュールするには、更新スケジュールを選択します。
4. ファイルのアップロードが完了するのを待ちます。期間はバンドルサイズとネットワーク速度によって異なります。

Update Status列の下に表示されるチェックマークアイコンを確認して、アップデートが正常に行われたことを確認します。

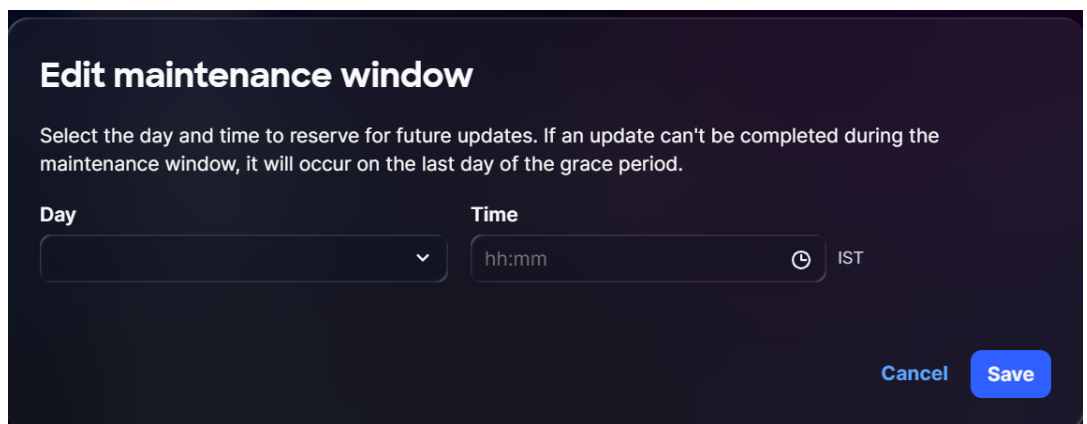
システムアップグレードスケジュールの編集

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、ユーザが定義した日付の猶予期間内であれば、ユーザが定義した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。



メンテナンスの編集

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。



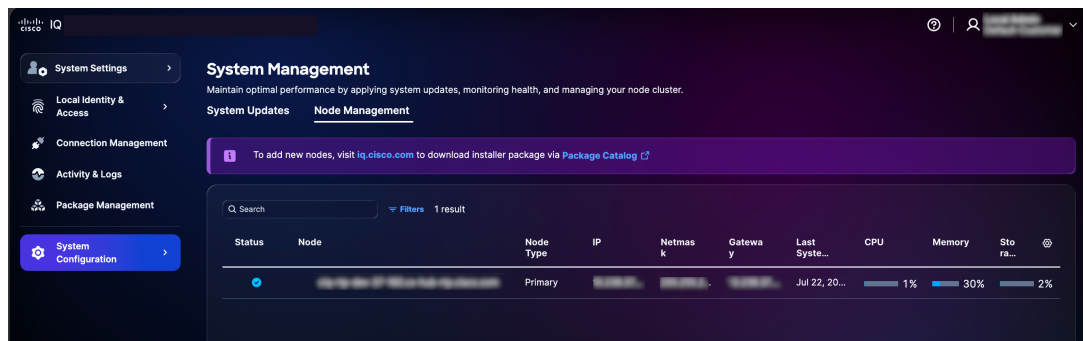
メンテナンスウィンドウの編集

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。これらの猶予期間の経過後は、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。

ノード管理

1. クラスタ内のノードを表示および管理するには、System Configuration > System Management > Node Managementの順に選択します。



ノード管理

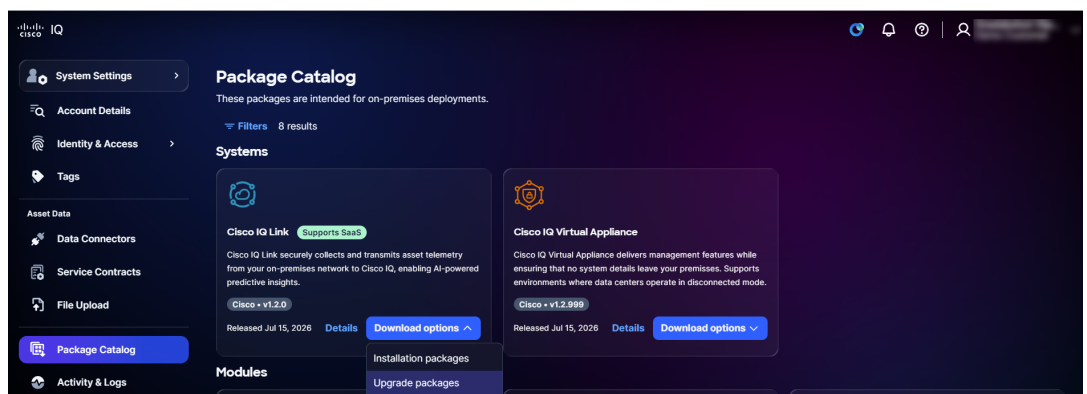
2. ノードリストには、各ノードのステータス、ホスト名、ノードタイプ、IPアドレス、ネットマスク、ゲートウェイ、および最終同期時刻が表示されます。

 注：Status列の青いチェックマークは、ノードがアクティブであることを示します。

システムの手動アップグレード

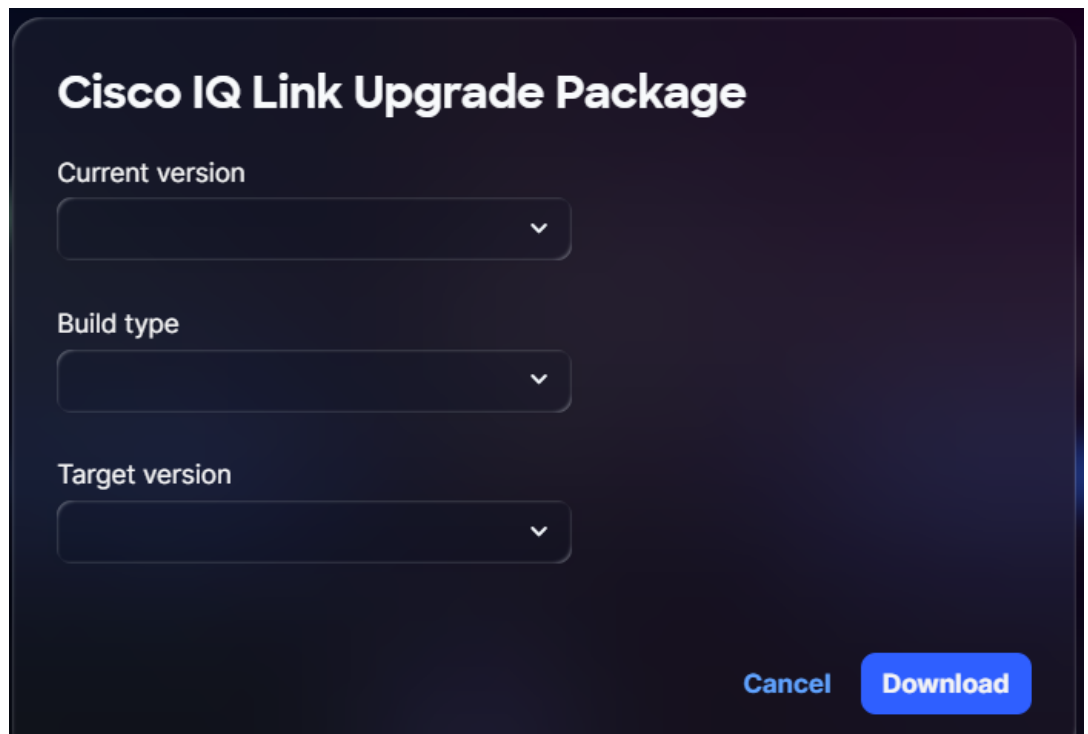
Cisco IQ SaaSからの自動配信が利用できないか、遅延しているシナリオでは、Cisco IQ SaaSからアップグレードバンドルを直接ダウンロードして、システムアップグレードを手動で実行できます。システムを手動でアップグレードするには、次の手順を実行します。

1. [Cisco IQ SaaS](#)にログインします。
2. Home > System Settings > Package Catalogの順に移動します。



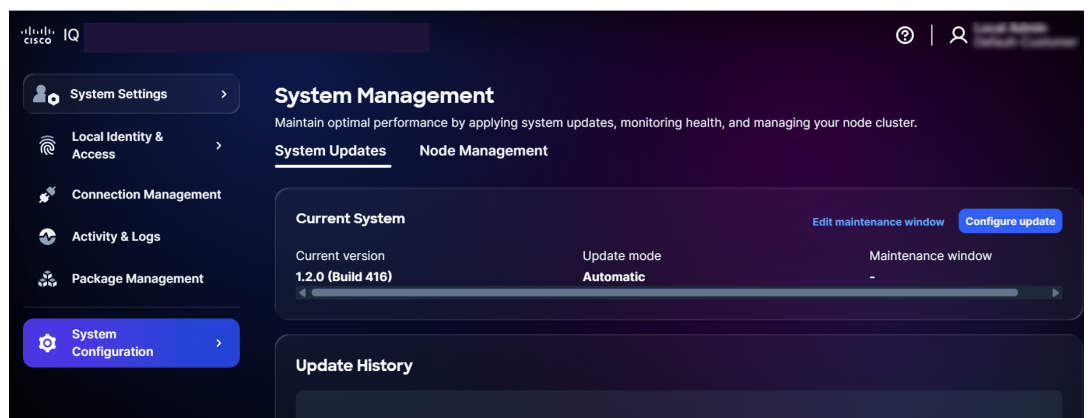
ソフトウェアカタログ

3. Cisco IQ Virtual Applianceカードで、Download options > Upgrade packagesの順にクリックします。



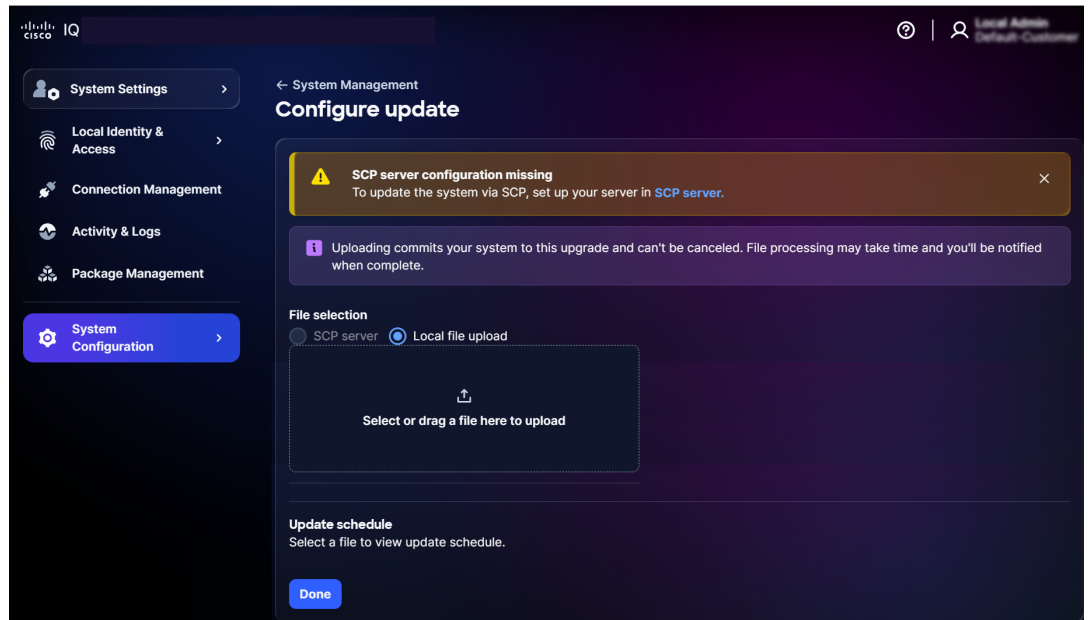
アップグレードパッケージ

4. 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。
5. ドロップダウンリストからビルドタイプを選択します。
6. 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。
7. [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。
8. Cisco IQ VAに移動します。
9. System Settingsで、System Configuration > System Managementの順に選択します。



更新の構成

10. 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

11. Local file upload オプションボタンをクリックします。
12. 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。
13. ファイルのアップロードが完了するのを待ちます。期間はバンドルサイズとネットワーク速度によって異なります。

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（オプション）。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。

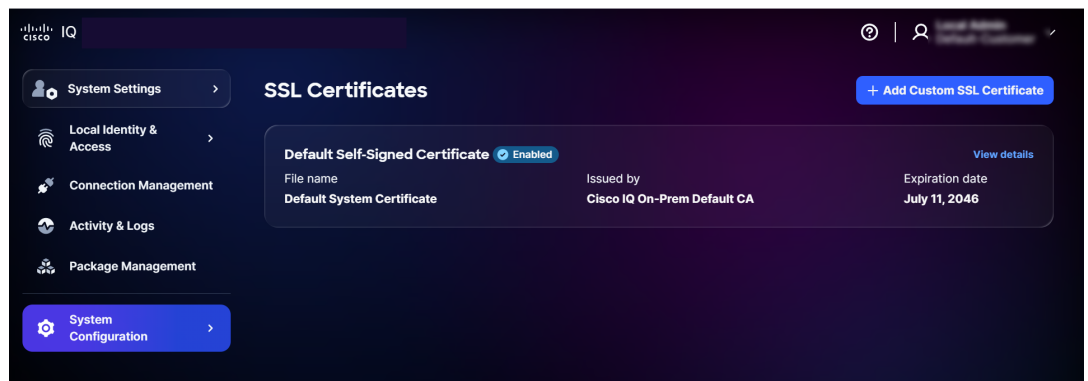
 注：証明書の有効期間は90日以上残っている必要があります。証明書の有効期限が切れるまでの残り日数が90日を下回ると、証明書は「期限切れ間近」と見なされます。SSL証明書を追加、編集、または削除した後で、「[Okta IDPまたはADFS IDP用のSLO設定の完了](#)」の説明に従って新しいSSL証明書をアップロードする必要があります。

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。

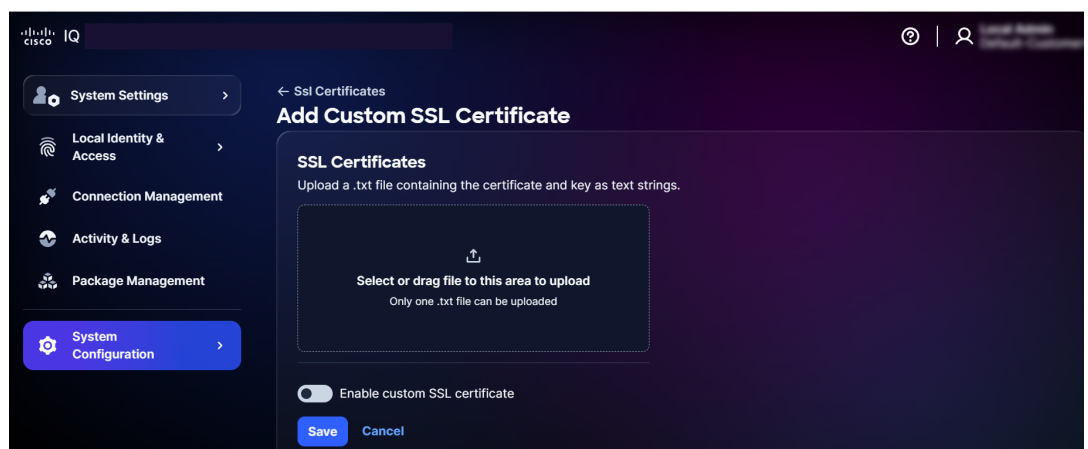


SSL証明書の追加

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. SSL CertificateセクションにカスタムSSL証明書を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。

Enable Certificate?

Enabling custom SSL certificate will disable the default self-signed certificate.

Cancel

Enable certificate

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。
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。
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

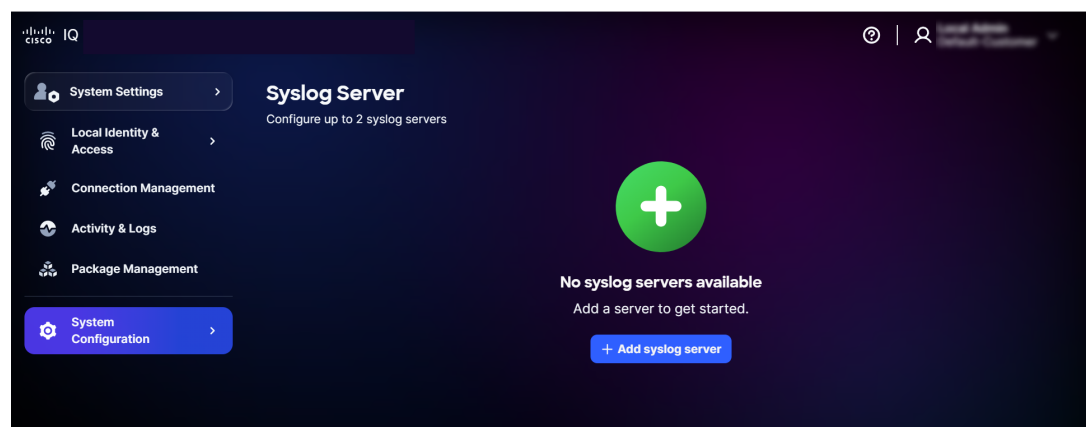
アカウント管理者ロールを持つユーザは、システムログをエクスポートするように外部syslogサーバを設定できます。最大2つのsyslogサーバを設定できます。

 注: Syslogサーバは、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

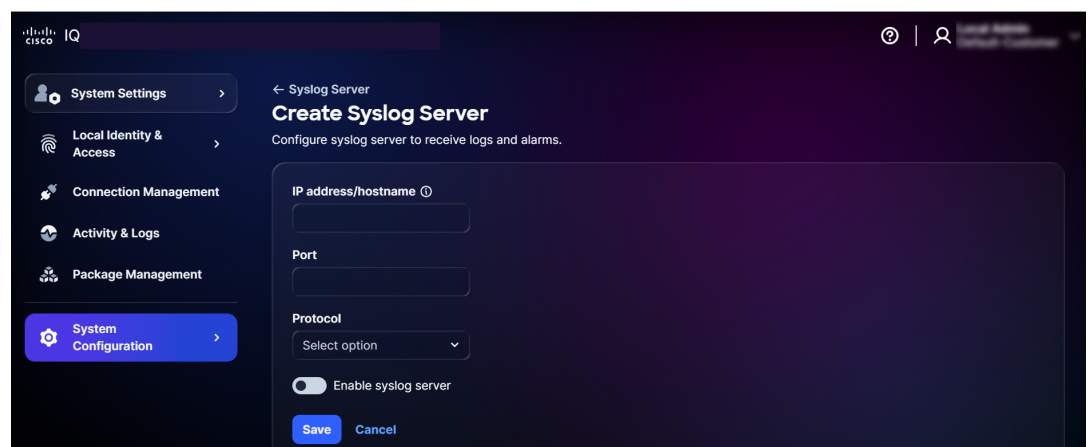
syslogサーバを追加するには、次の手順を実行します。

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. Port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、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。
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。

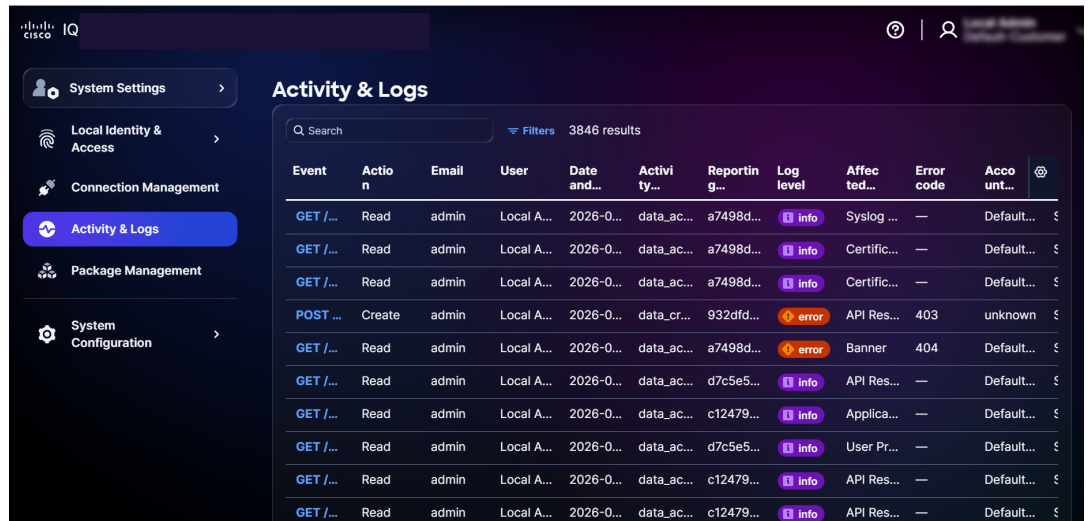
設定されたSyslogサーバの削除

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:

- 。すべてのAPI操作をゲートウェイレベルで記録
- 。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。

次のフィルタオプションを使用できます。

- 。Last logged date : ログを特定の時間範囲でフィルタリングします。
- 。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フィルター

バナー

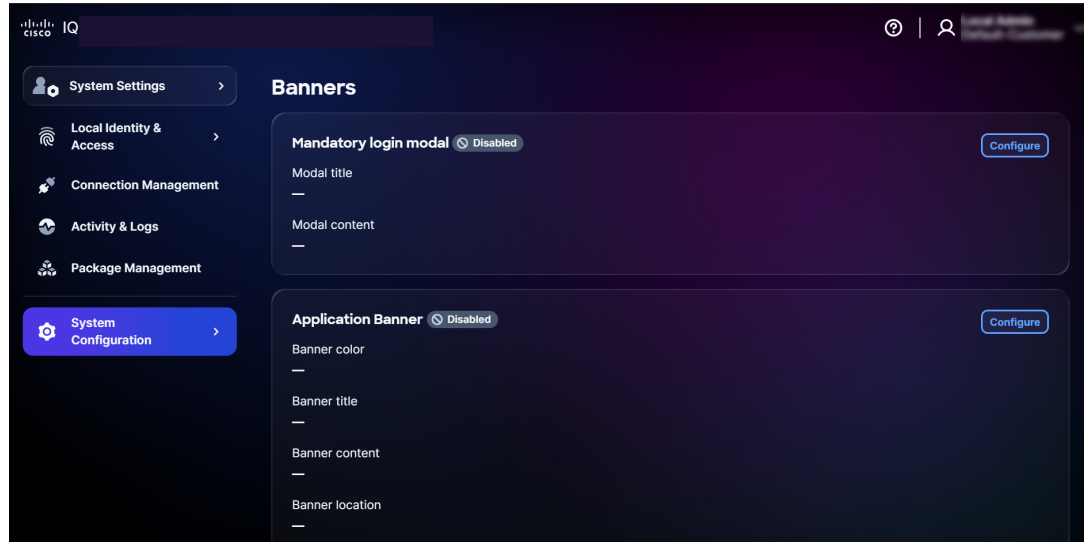
アカウント管理者は、システム全体のバナーを設定して、セキュリティおよびコンプライアンス標準を満たすことができます。

- 。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 : 認証に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

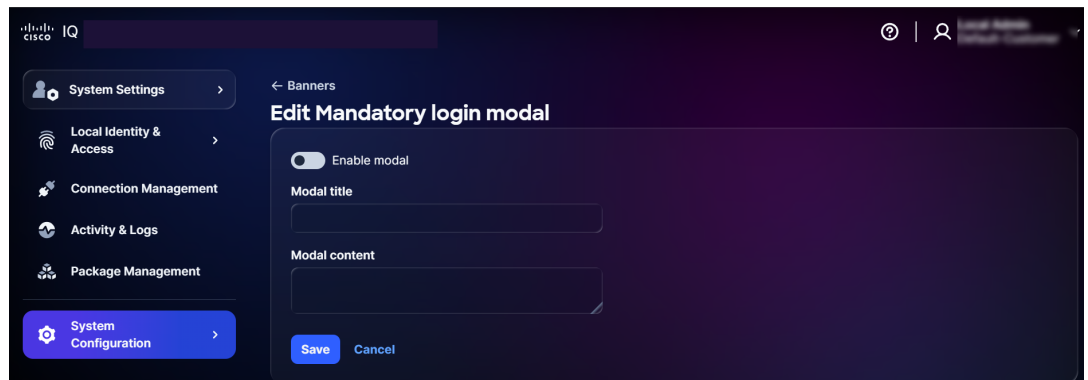
必須バナーを設定するには、次の手順を実行します。

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。



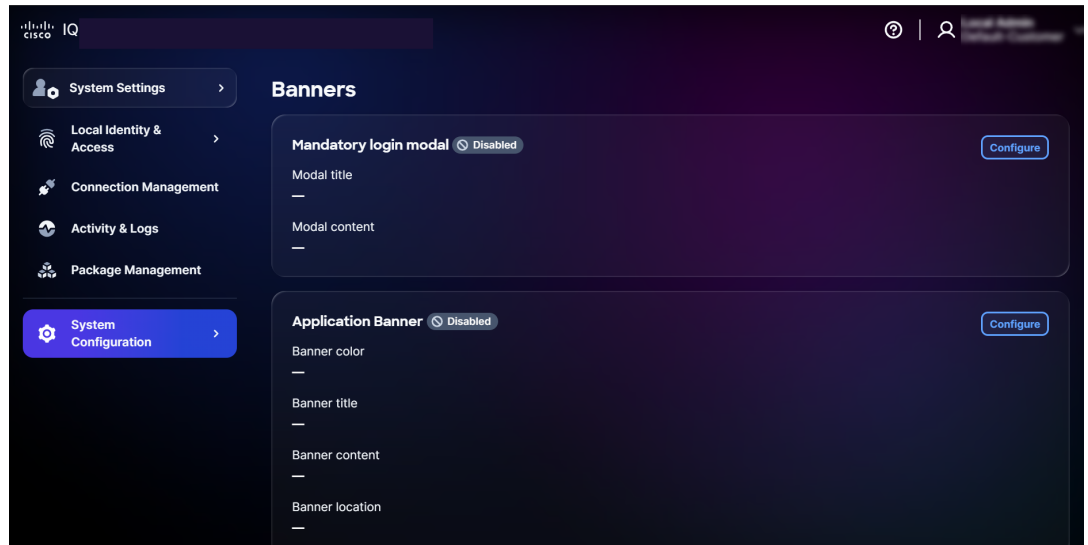
必須ログインモーダルバナーの編集

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

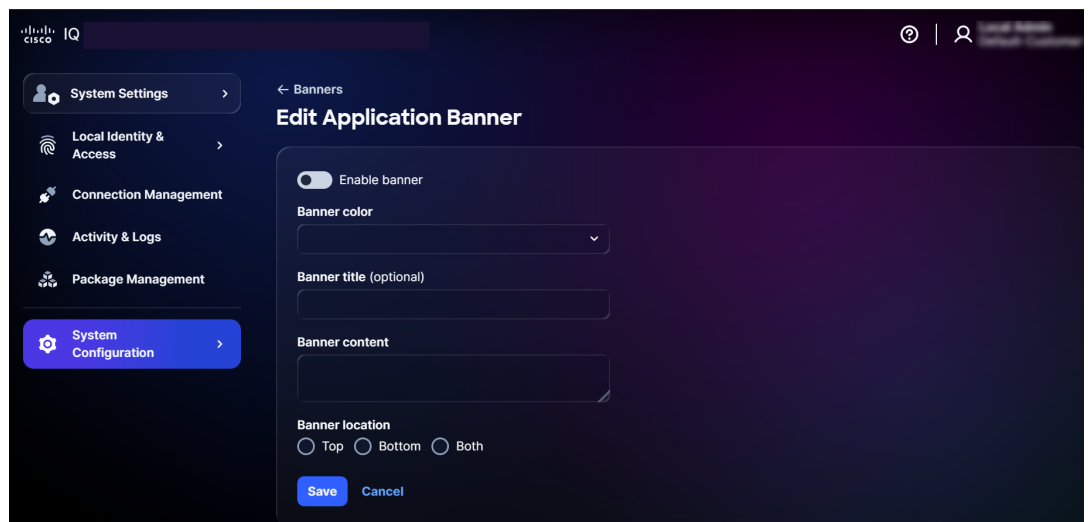
アプリケーションバナーを設定するには、次の手順を実行します。

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

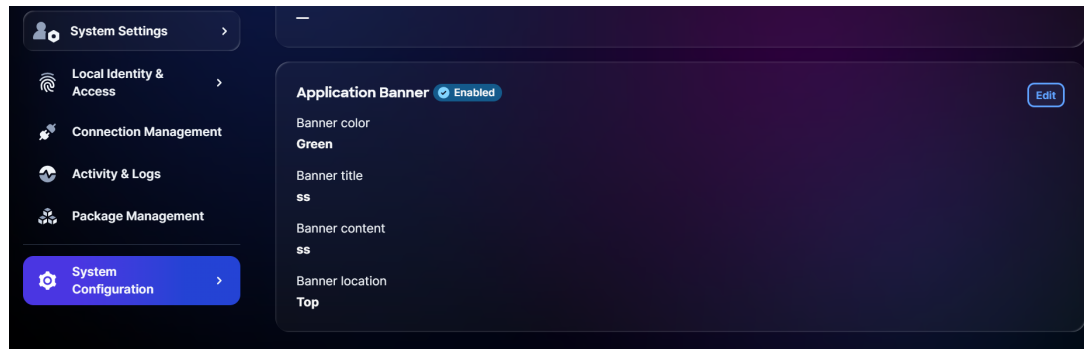
3. バナーを有効または無効にするには、トグルをクリックします。
4. バナーの色を選択します。
5. バナータイトルを入力します。
6. バナーの内容を入力します。
7. バナーの場所を選択します。

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

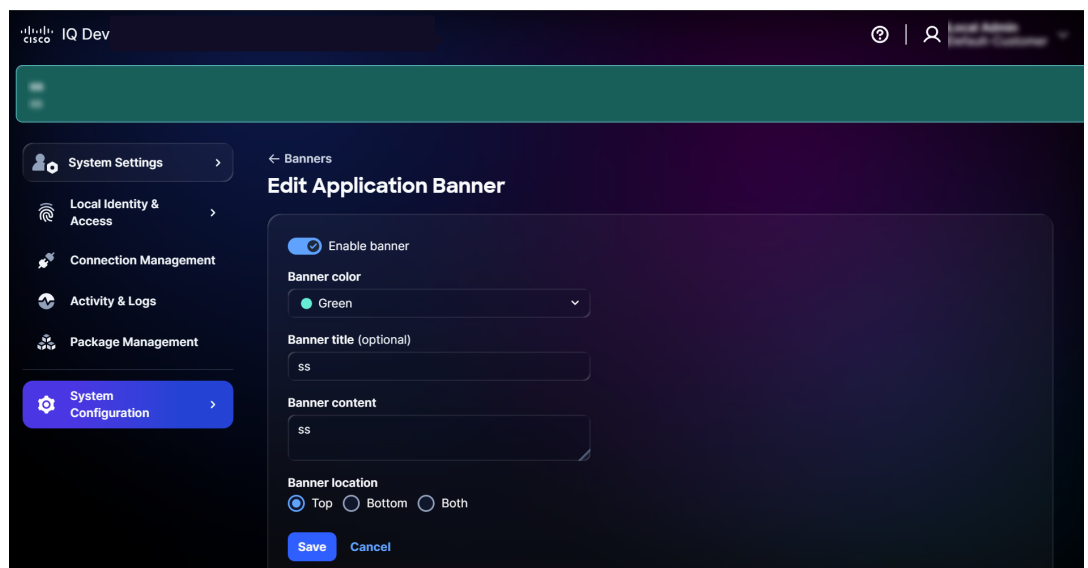
バナーを編集するには、次の手順を実行します。

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

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。

```
Cisco IQ

Navigation Main Menu

SYSTEM STATUS
Cisco IQ On-Prem Installed

CONFIGURATION SETTINGS
IP Address/Mask
Gateway IP
DNS List
Search Domain
NTP List
Hostname

MAIN MENU
[1] Configure Network Settings DISABLED because the platform is installed
[2] Configure System Orchestrator DISABLED because the platform is installed
[3] System Diagnostics
[4] Help
[5] About
[q] Quit
```

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。

```
Cisco IQ

Navigation Main Menu > System Diagnostics

Please provide the following server connection details:

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

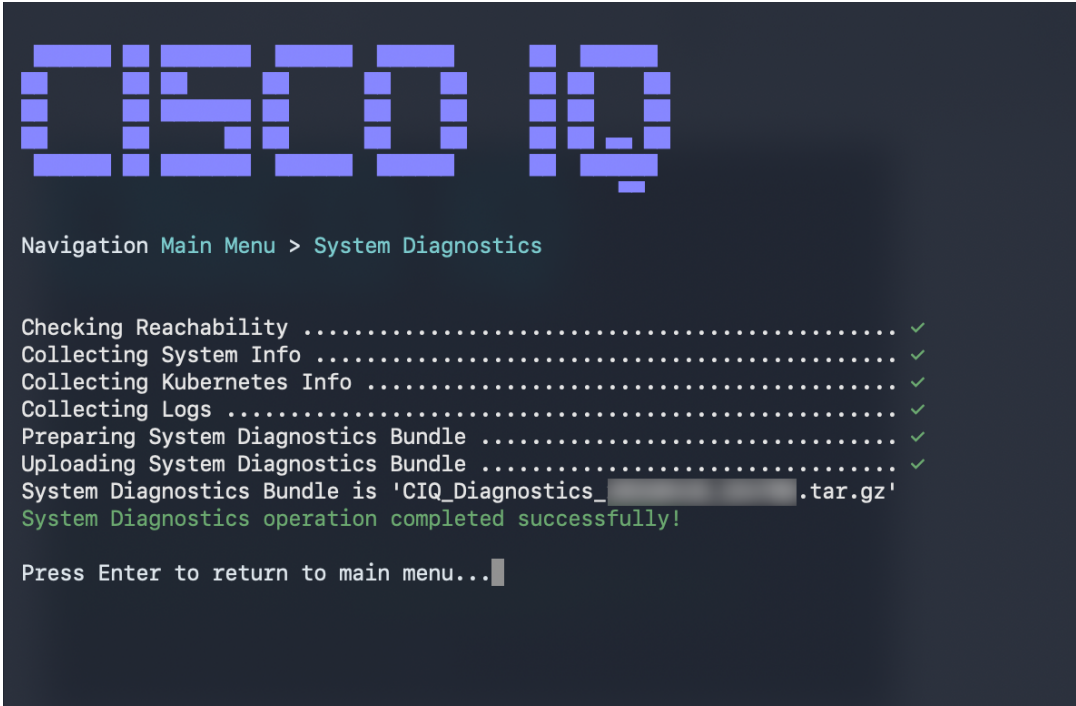
PROTOCOL SELECTION
[1] SCP (Secure Copy Protocol) - Default
[2] SFTP (SSH File Transfer Protocol)

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

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

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。

A screenshot of a terminal window with a dark background and light blue text. At the top, there is a large, stylized logo made of small squares. Below the logo, the text "Navigation Main Menu > System Diagnostics" is displayed. A list of diagnostic steps follows, each with a green checkmark at the end: "Checking Reachability", "Collecting System Info", "Collecting Kubernetes Info", "Collecting Logs", "Preparing System Diagnostics Bundle", and "Uploading System Diagnostics Bundle". Below this list, a message states "System Diagnostics Bundle is 'CIQ_Diagnostics_XXXXXXXXXX.tar.gz'" where XXXXXXXXXX is a placeholder for a unique identifier. The final line of the list is "System Diagnostics operation completed successfully!". At the bottom, a prompt says "Press Enter to return to main menu..." followed by a cursor.

```
Navigation Main Menu > System Diagnostics

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

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

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

。

サポートモジュール

Cisco IQ SaaSからVAおよびモジュール固有のサポートケースを作成できます。このサポートモジュールは、Cisco IQ SaaSで利用でき、サポートケースの統合ビューを提供します。サポート案件リストビューのフィルタリング、並べ替え、カスタマイズを行うことができ、アクセス権のあるオープンなサポート案件とクローズしたサポート案件の両方を表示できます。Cisco IQ SaaSのサポートモジュールの詳細については、『[Cisco IQ SaaS Getting Started Guide](#)』を参照してください。



注: Cisco IQ VAをご利用のお客様は、Cisco IQ SaaSサポートモジュールのほとんどの機能をご利用いただけます。これには、Cisco IQ VAとそのモジュールに関連するTechnical Assistance Center(TAC)のケースを開いたり、製品ケースを作成して管理したりする機能が含まれます。

サポートケースの作成

Cisco IQ SaaSでは、VAとモジュール固有のケースを作成できます。ケースを作成するには、次の手順に従います。

1. [Cisco IQ\(SaaS\)](#)にログインします。
2. Helpアイコン> Report an Issueの順にクリックします。Report an Issueウィンドウが開きます。

Report an Issue

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

Issue type

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

Issue description

Describe what happened.

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

Preferred contact method

☐ Telephone ☐ Email ☐ Virtual space via Webex

Include recipients (optional)

Select or add email addresses

Select or enter email addresses to include.

Cancel

Submit

問題の報告

3. 必要な詳細情報を入力します。
4. [Submit] をクリックします。

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。