Cisco IQ入門ガイド

はじめに

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

このドキュメントでは、Cisco IQとそのアプリケーションの概要について説明します。 詳細は、『Cisco IQリリースノート』または『Cisco IQに関するFAQ』を参照してください。

オンボーディング

前提条件

Cisco IQを使用する前に、次の前提条件が満たされていることを確認してください。

サポートされるブラウザ

Cisco IQは、次のブラウザの最新の安定したリリースでサポートされています。

- Google Chrome
- Microsoft Edge
- Apple Safari
- Mozilla Firefox

注：サポート対象は現行のブラウザバージョンに限定され、古いバージョンでは完全な機能が提供されない場合や、新しいアップデートのリリースに伴ってサポートされない場合があります。

Ciscoアカウント

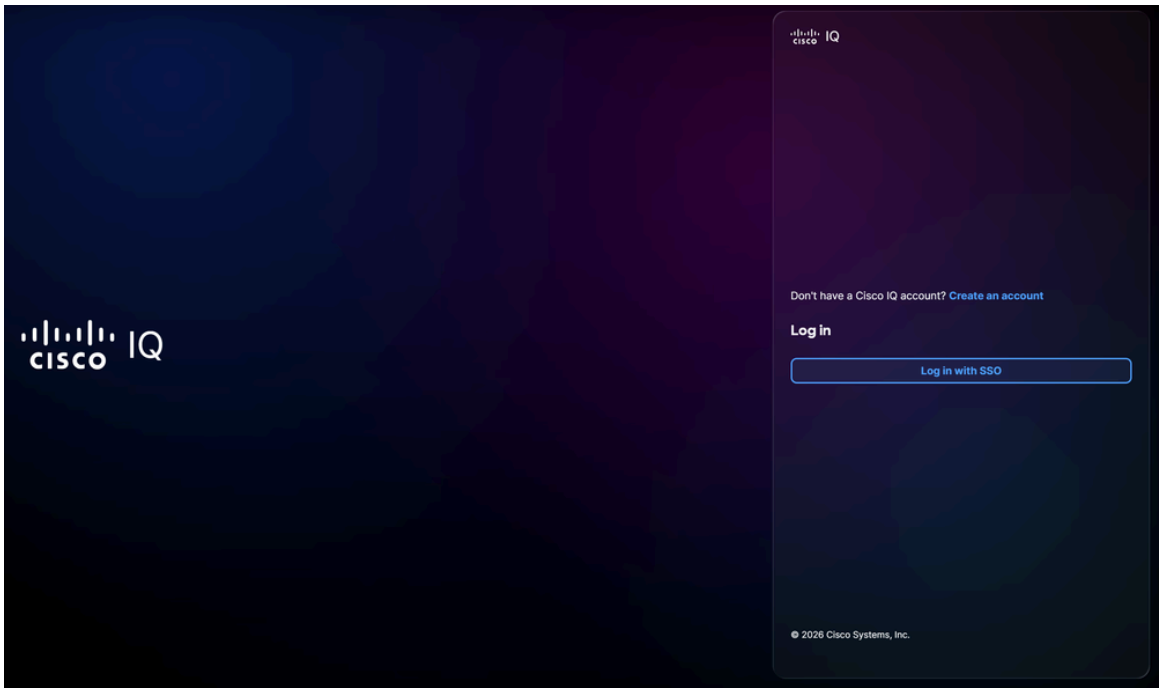
Cisco IQにアクセスするには、Cisco.comのアカウントが必要です。シスコのアカウントの詳細については、ログインおよびアカウントのヘルプを参照してください。

アカウントの作成

新しいCisco IQアカウントの作成

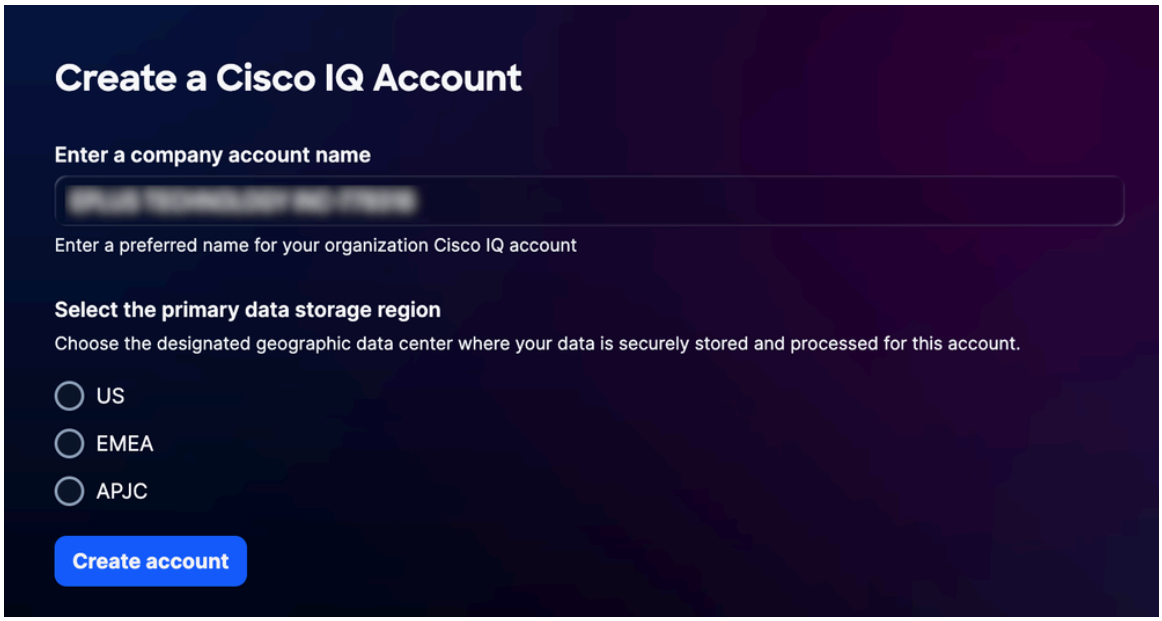
新しいCisco IQアカウントを作成するには：

1. Cisco IQに移動します。Cisco Log inページが表示されます。



Cisco IQログイン

2. Create an accountをクリックします。
3. EmailフィールドにCisco Connection Online(CCO)IDクレデンシャルを入力します。
4. [Next] をクリックします。
5. パスワードを入力します。
6. Verifyをクリックします。Create a Cisco IQ Accountページが表示されます。



Cisco IQアカウントの作成

7. Enter a company account nameフィールドに、組織のCisco IQアカウントに使用する一意の名前を入力します。
8. プライマリ・データ・ストレージ・リージョンを選択します。
9. Create accountをクリックします。Cisco IQ Launchpadにリダイレクトされます。

CX CloudアカウントのCisco IQへの移行

注：既存のCX CloudアカウントをCisco IQに移行できるのは、アカウント管理者だけです。

既存のCX Cloudアカウントをお持ちの場合は、既存のCX CloudデータをCisco IQに移行できます。次のデータは、既存のCX Cloudアカウントから自動的に移行されます。

- ユーザおよびユーザグループ（パートナーユーザおよびグループを除く）
- 契約
- Intersight、Webex、Software-Defined Wide Area Network(SD-WAN)、Merakiのクラウドデータソースの追加

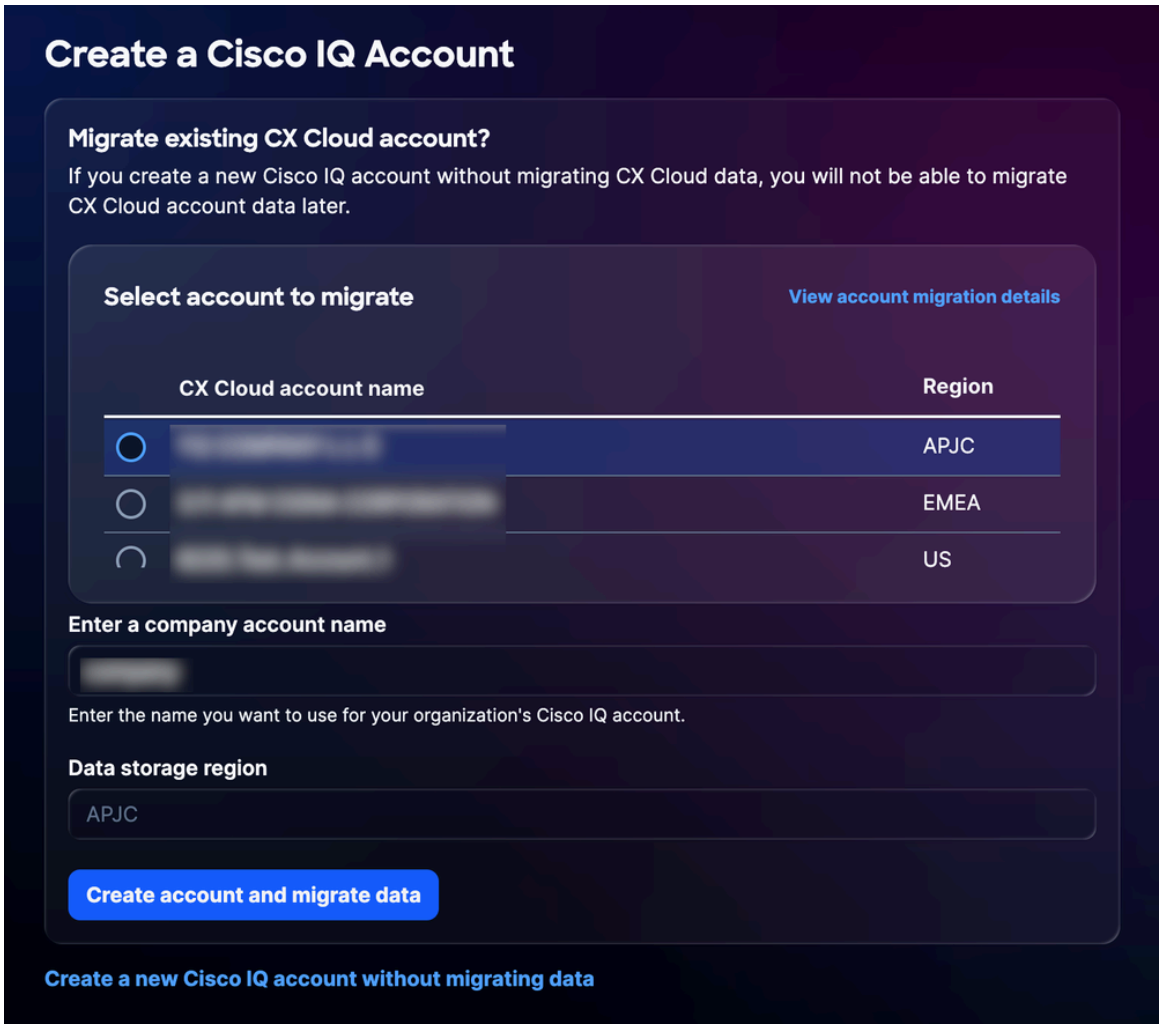
注：スムーズな移行を保証し、Cisco IQのパーソナライズされた予測的でプロアクティブなAIを活用したインテリジェンスからより正確な洞察を得るために、移行前にCX Cloudアカウントデータの検証と整理を検討してください。

警告:CX Cloudデータを移行せずに新しいCisco IQアカウントを作成した場合、後でCX Cloudアカウントデータを移行することはできません。

注:一度に移行できるCX Cloudアカウントは1つだけです。追加のアカウントを移行する必要がある場合は、このセクションで説明する手順を繰り返します。

既存のCX Cloudアカウントを移行するには

1. Cisco IQに移動します。Cisco Log inページが表示されます。
2. Create an accountをクリックします。
3. EmailフィールドにCisco Connection Online(CCO)IDクレデンシャルを入力します。
4. [Next] をクリックします。
5. パスワードを入力します。
6. Verifyをクリックします。Create a Cisco IQ Accountページが表示されます。



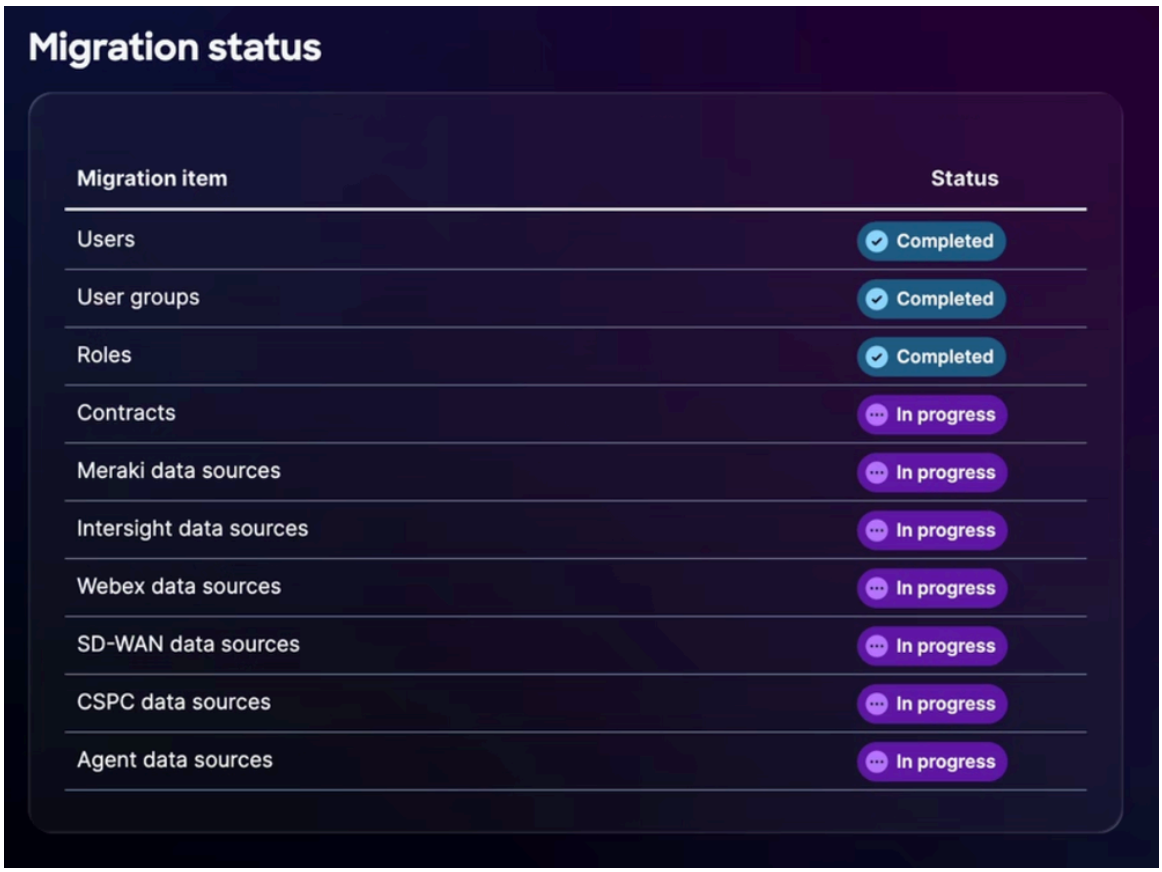
CX Cloudアカウントの選択

7. データの移行元のCX Cloudアカウントを選択します。
8. 組織のCisco IQアカウントに使用する一意の名前を入力します。

> 注：元のアカウントのデータストレージ領域は自動入力され、Cisco IQ企業アカウントに移行されます。データストレージ領域を変更するには、新しいCisco IQ企業アカウントを作成する必要があります。

9. Create account and migrate dataをクリックします。Migration Statusページが表示されます。

   Migration Statusページには、Cisco IQに移行されるデータの完了ステータスが表示されます。次のステータスを使用できます。



移行ステータス

   - 進行中：データは移行中です
   - 完了：移行が完了しました
   - Unable to Migrate：データ移行が不完全で、Cisco IQがデータを移行できない

   データを移行できない場合は、手動でデータを新しいCisco IQ企業アカウントに移行する必要があります。Cisco IQにデータを追加する方法の詳細については、システム設定を参照してください。

10. 移行プロセスが完了したら、Continueをクリックします。Cisco IQ Launchpadにリダイレク

トされます。

既存のアカウントへのログイン

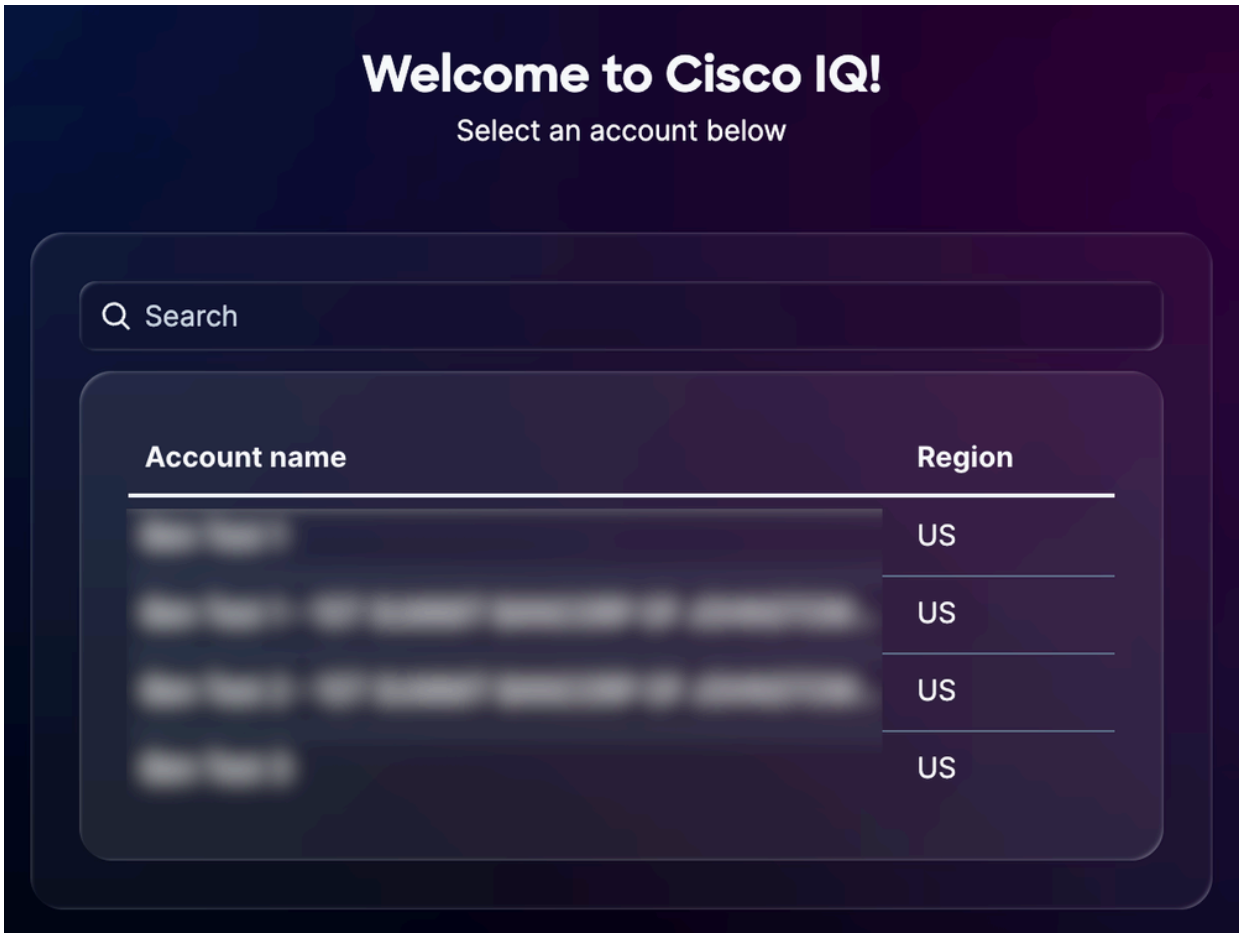
> 注：既存のCisco IQアカウントをお持ちで会社のアカウントに追加されていないお客様は、会社のアカウント管理者に連絡して、アカウントへのアクセスをリクエストする必要があります。

既存のアカウントにログインするには、次の手順を実行します。

1. Cisco IQに移動します。Cisco Log inページが表示されます。
2. Log in with SSOをクリックします。
3. EmailフィールドにCCO IDクレデンシャルを入力します。
4. [Next] をクリックします。
5. パスワードを入力します。
6. Verifyをクリックします。

アカウントを1つ持っている場合は、Cisco IQ Launchpadにリダイレクトされます。

複数のアカウントをお持ちの場合は、「Cisco IQへようこそ」ページにリダイレクトされます。



アカウント名の選択

はじめに

> ✎ 注：作業を開始する前に、Cisco IQに完全にオンボーディングされていることを確認してください。詳細は、『オンボーディング』を参照してください。

サポート階層

Cisco IQサポート階層レベルは、Cisco IQ内で利用可能なアクセスと機能を定義し、サポートとプロフェッショナルサービスのエクスペリエンスを強化するように設計されています。これらのレベルは、お客様の有効なシスコサポート契約に関連付けられており、AIに基づく洞察やトラブルシューティングから、資産や契約管理まで、どの機能やツールを利用できるかを決定します。レベルを理解することで、契約上の権利へのコンプライアンスを維持しながら、Cisco IQの機能を最大限に活用できます。次の表に、各レベルで利用可能なCisco IQ機能の概要を示します。

> ✎ 注：機能はサポート階層レベル全体で累積されます。上位レベルには、下位レベルのすべての機能が含まれます。

	基本レベル	標準レベル	シグニチャレベル
	所有している資産を把握	運用の復元力を優先する	優れた運用効率の促進
完全なランドスケープの明瞭さ	次の機能を使用して、シスコのすべての資産とサブコンポーネントを動的かつ確実に追跡します。 • 資産インベントリ • サポート終了(EOL)レポート • サービス契約レポート • サポート終了日(LDOS)ダッシュボード	次の機能を使用して、ネットワークのパフォーマンスを分析し、リソースの割り当て先を決定します。これにより、インフラストラクチャへの投資に関して、十分な情報に基づいた意思決定が可能になります。 • EOLに関する洞察[1] • サービス契約の分析[1] • LDOS分析[1] • 資産の重要度に関する洞察[1] • 資産のタギング	
予防的な復元力	次の機能を使用して、環境内の潜在的なリスクを特定して対処するのに役立つ重要な通知を可視化できます。 • セキュリティアドバイザリレポート • Field Noticeレポート	Cisco IQは、資産リスクを関連付けることによってデータを洞察に変えます。これにより、最も重要なセキュリティリスクを特定し、優先順位を付けることができます。 • セキュリティアドバイザリの洞察[1] • セキュリティ強化の洞察[1] • フィールド通知の考察[1] • 設定に関する洞察[1]	次の機能は、セキュリティポスチャを改善し、環境内の設定を最適化するのに役立つ実用的な推奨事項を提供します。 • 推奨設定[1] • セキュリティ強化の推奨事項[1]
迅速な解決	次の機能を使用して、サポート・リクエストを管	次の機能を使用してケースの傾向と効率性メトリック	

	理し、解決ステータスを1か所で追跡し、問題を迅速に解決できます。 • 事例管理 • セルフサービスのトラブルシューティング[1]	を追跡し、継続的な運用改善を示します。Cisco IQは、コンテキスト認識型の解決アシスタントを提供し、アクティブな問題の解決と、根本的な根本原因の調査を支援します。 • ケースインサイト[1]	

[1] Cisco IQ Link、Intersight、Meraki、SD-WAN Manager、およびWebEx Control Hub経由のデバイスとテレメトリ接続をサポートします。

基本機能

Basicサポート層では、信頼性の高い事後対処的なサポートを通じて、基本的な制御を行うことができます。たとえば、製品サポートの専門家へのアクセス、セルフサービスによるトラブルシューティング、一元的なケース管理などが可能です。完全な可視性を確保するために、Cisco IQは資産テレメトリ、契約情報、およびサポート履歴を統合し、資産ライフサイクル、セキュリティアドバイザリ、およびField Noticeの包括的なビューを提供します。さらに、Cisco Uから入手可能な基本的な学習リソースにアクセスすることで、技術的な専門知識を強化できます。

次の表に、Basicサポート階層で使用可能な機能の概要を示します。

機能	説明
資産インベントリ	Asset Inventoryでは、ハードウェア製品、モデル番号とシリアル番号、OSのバージョン、設置場所、サービス契約の詳細について、最新のリストと豊富なビジュアライゼーションが提供されます。また、Technical Assistance Center(TAC)ケース、契約更新、テレメトリなどに基づいて「最後の信号」でフィルタリングする方法も提供します。この信号は、シスコが資産がアクティブであることを認識している時間です。
EOLレポート	EOLレポートは、販売終了からLDOSまでのEOLマイルストーンに近いか、そのマイルストーンを達成しているか、そのマイルストーンを過ぎているハードウェアおよびソフトウェアの最新リストと豊富なビジュアライゼーションを提供し、ライフサイクルおよびテクノロジーの更新プランニングを可能にします。
サービス契約レポート	サービス契約レポートは、契約対象および契約対象外の資産に関する最新のリストと豊富なビジュアライゼーションを提供します。

LDOSダッシュボード	LDOSダッシュボードは、LDOSマイルストーンの一元化されたビューを提供します。これにより、ハードウェアまたはソフトウェアがサポート終了に達する前に、資産計画と予算予測を改善し、運用リスクを軽減できます。
セキュリティ アドバイザリ	セキュリティアドバイザリは、リスクを検出し、リスクの重大度と重要度に基づいて脆弱性の優先順位を付け、重大な脅威の軽減を促進する経営陣レベルの洞察を提供する自動化されたソリューションを提供します。これにより、進化する脅威に対する企業の復元力が強化されます。
Field Notice	Field Noticeは、セキュリティに関連しない製品の問題を検出し、影響の重大度と重要度に基づいて問題の優先順位を付け、経営陣レベルの洞察を提供して運用上の重大な問題の解決を迅速化することで、企業の復元力を強化し、最適なパフォーマンスを維持する自動化されたソリューションを提供します。
事例管理	Case Managementには、ケース数、ステータス、重大度、ケースに関連付けられた返品許可(RMA)など、Cisco TACケースの最新リストが記載されています。 また、TACケースを(クロス起動からSupport Case Manager(SCM)へ)オープンし、ケース情報を迅速に更新して解決を容易にする機能も提供します。
セルフサービスのトラブルシューティング[1]	セルフサービストラブルシューティングでは、Cisco IQ AI Assistantを使用して問題を即座に解決できます。このインタラクティブなツールは、シスコの検証済みナレッジベースから直接、コンテキスト認識型のリアルタイムなトラブルシューティングとエキスパートによる推奨事項を提供します。これにより、サポートケースをオープンすることなく問題を解決できます。

[1] Cisco IQ Link、Intersight、Meraki、SD-WAN Manager、およびWebEx Control Hub経由のデバイスとテレメトリ接続をサポートします。

標準機能

Standardサポート階層では、ソリューションレベルの問題に対する一元的なトリアージと、必要なテクニカルエキスパートと連携する専任のケースオーナーを提供することで、運用効率を向上させます。資産データをビジネスの重要性と関連付けるAIを活用したインサイトを使用してリスクをプロアクティブに軽減し、インベントリ、セキュリティ、および構成の評価を明確に可視化できます。さらに、シスコUで提供されているパーソナライズされたラーニングパスを通じて、チームの専門知識を特定のビジネスニーズに合わせることも可能です。

次の表に、Standardサポート階層で使用可能な機能の概要を示します。

機能	説明
EOLに関する洞察[1]	EOL Insightsは、EOLマイルストーンに関するインテリジェントなクエリ、サマリー、可視化、およびレポートを提供し、ライフサイクルとテクノロジー更新の計画に関してパーソナライズされた優先順位付けを可能にします。
サービス契約の分析[1]	サービスカバレッジの分析では、サービスカバレッジの詳細と更新マイルストーンを視覚化して分析し、カバレッジ更新と更新計画のパーソナライズされた優先順位付けを可能にします。
資産のタギング	資産タグを使用すると、資産タグを使用してビジネスニーズに従ってインベントリを整理できます。これにより、ハードウェアおよびソフトウェア資産を、部門、場所、またはプロジェクトごとにキーと値のペアとして柔軟に編成できます。
LDOS分析[1]	LDOS Insightsは、LDOSのマイルストーンを超えているか、それに近づいている資産の可視化と分析を提供し、ライフサイクルとテクノロジー更新の計画をパーソナライズされた優先順位に基づいて優先順位付けします。
資産の重要度に関する洞察[1]	資産の重要度インサイトを使用すると、ネットワークにおける資産の役割とその相対的な重要性を評価および特定し、リスク軽減活動の優先順位付けや運用回復力の向上を実現できます。
セキュリティアドバイザリの洞察[1]	セキュリティアドバイザリインサイトは、セキュリティアドバイザリの影響を受ける資産のインテリジェントなクエリ、集約、可視化、およびレポートを提供し、リスクとセキュリティインシデント対応のパーソナライズされた優先順位付けを可能にします。
セキュリティ強化の洞察[1]	セキュリティ強化インサイトは、デバイス構成を評価し、影響の重大度と重要度に基づいてセキュリティ強化のギャップを特定し、重要な強化対策の実装を加速するためのエグゼクティブレベルのインサイトを提供する自動化ソリューションを提供します。これにより、企業の耐障害性が強化され、進化する脅威に対する攻撃対象領域が縮小されると同時に、リスクのある資産に対するインテリジェントなクエリ、サマリー、可視化、およびレポートを通じて、セキュリティ態勢の改善によるパーソナライズされた優先順位付けが可能になります。

フィールド通知の考察[1]	Field Notice Insightsは、Field Noticeの影響を受ける資産に関するインテリジェントなクエリ、サマリー、可視化、およびレポート機能を提供し、リスクと既知の問題への対応に関してパーソナライズされた優先順位付けを可能にします。
設定に関する洞察[1]	Configuration Insightsは、現場で実証済みの専門知識に基づいて、シスコが推奨するベストプラクティスに照らしてデバイス構成を評価する自動化ソリューションを提供します。影響を受ける資産のインテリジェントなクエリー、集約、可視化、およびレポート機能により、パーソナライズされた優先順位付けが可能になり、重要な構成ギャップの修復が迅速化されるため、インフラストラクチャの復元力が強化され、ネットワーク全体の運用リスクが軽減されます。
ケースインサイト[1]	Case Insightsは、Cisco TACケースに関するインテリジェントなクエリ、集約、可視化、およびレポートを提供し、運用効率のパーソナライズされたモニタリングを可能にします。

[1] Cisco IQ Link、Intersight、Meraki、SD-WAN Manager、およびWebEx Control Hub経由のデバイスとテレメトリ接続をサポートします。

シグニチャ機能

Signatureサポート層は、Standardサポート層を基盤として構築されており、定義された復旧サービスレベル契約を通じて運用実績を向上させ、お客様固有の環境に精通した専門のエキスパートチームにアクセスできます。この階層は、運用に影響が及ぶ前に中断を防ぐことに重点を置いており、予防的なセキュリティ強化、体系的な根本原因の排除、エキスパート主導の継続的な資産分析を提供します。さらに、高度なCisco U.認定トレーニングと仮想プラクティスラボを利用して、高度な技術的能力を身につけることができます。

次の表に、シグニチャサポート層で使用可能な機能の概要を示します。

機能	説明
推奨設定[1]	Configuration Recommendationは、潜在的な設定の誤りと不整合に対処するための実用的な推奨事項を提供します。
セキュリティ強化の推奨事項[1]	セキュリティ強化の推奨事項では、失敗した各強化チェックに固有の一般的な推奨事項を提供する自動化ソリューションが提供され、基盤となるセキュリティ問題に明確かつ簡潔に対処します。

[1] Cisco IQ Link、Intersight、Meraki、SD-WAN Manager、およびWebEx Control Hub経由のデバイスとテレメトリ接続をサポートします。

管理者向けのスタートガイド

新しく作成または移行したCisco IQアカウントに初めてログインすると、ようこそページにはじめにの行程が表示されます。移行したデータを使用してアカウントを作成したか、使用しなかったかによって、作業の開始は異なります。

注:Get Startedジャーニーのエクスペリエンスは、ロールベースアクセスコントロール(RBAC)権限によって異なります。

作成による新規アカウント

新しく作成したアカウントのGet Startedジャーニーでは、Cisco IQ環境の設定とCisco IQの調査に必要な初期初期初期初期登録手順を説明します。

シスコクラウド製品の接続

注：この手順を完了するには、少なくとも1つのクラウド製品を接続する必要があります。

シスコのクラウド製品データをCisco IQに接続することは、強力でパーソナライズされた機能の使用を開始する最速の方法です。データ接続をセットアップした後、カスタマイズされたインサイトを数分で受け取ることができます。

シスコのクラウド製品を接続するには、「データコネクタ」を参照してください。

サービス契約のリンク

注：この手順を完了するには、1つ以上のサービス契約をリンクする必要があります。

契約をリンクすることで、異なるチームメンバーに関連付けられた契約のデータを統合し、テレメトリを介してインベントリに関連付けられていない資産を組み込むことができるため、サポート契約を一元的に可視化して、更新に関する予想外の事態を防ぐことができます。

サービス契約をリンクするには、「サービス契約」を参照してください。

オンプレミスデバイスの接続

注：この手順を完了するには、Cisco IQ Linkを最低1つ登録する必要があります。

オンプレミスデバイスとの通信を確立するには、Cisco IQ Linkを設定する必要があります。Cisco IQ Linkは、シスコのクラウドプラットフォームでは管理されていないオンプレミスデバイスにCisco IQの全機能を提供します。Cisco IQ Linkは、データセンターに仮想マシン(VM)としてインストールし、Cisco IQアカウントにリンクすることができます。

オンプレミスデバイスを接続するには、「データコネクタ」を参照してください。

ユーザー・アクセスの管理

注：この手順を完了するには、2人以上のユーザを追加する必要があります。

Cisco IQのシンプルなアクセス制御機能は、小規模なチームでも大規模な組織でも使用できるように設計されています。ユーザを追加し、グループおよび個人に管理者ロールまたは表示専用ロールを割り当てることができます。

ユーザを追加して権限を割り当てるには、「ユーザ」を参照してください。

Cisco IQの確認

利用可能なCisco IQの機能とアプリケーションを確認します。次のような機能があります。

- スタートパッド：アプリケーションへのアクセス、新機能の検出、ダッシュボードの作成
- 資産申請：詳細は、「資産申請」を参照してください。
- 評価アプリケーション：詳細は、『評価アプリケーション』を参照してください
- Support Application：詳細は、『Support Application』を参照してください
- Cisco IQ AI Assistant：詳細は、『AI Assistant』を参照してください
- システム設定：アカウント設定の管理、ユーザーへのアクセス許可、データ接続の構成、アカウントのアクティビティとログの表示を行います。詳細については、「システム設定」を参照してください

移行による新規アカウント

新しいCisco IQアカウントが移行によって作成された場合、以前のアカウントの情報はすでに使用可能です。その結果、新しく移行されたアカウントのGet Startedプロセスは、以下に詳述する移行のレビューに限定されます。

移行の確認

移行を確認するには、次の手順に従います。

- Home > System Settings > Service Contractsで、契約が正常に移行されたことを確認します。
- Home > System Settings > Data Connectorsで、必要なデータ接続がすべて正しく設定されていることを確認します。
- 正常に移行されたユーザデータを確認し、移行されたユーザのアカウントをHome > System Settings > Identity & Access > Usersでアクティブにすることにより、そのユーザにアクセス権を付与します。
- Home > Assets > Inventoryで、アセットが正常に移行されたことを確認します。

一般ユーザ向けのスタートガイド

Cisco IQアカウントに初めてログインすると、ようこそページにはじめにの行程が表示されます。このガイドでは、Cisco IQの機能と一般的なワークフローについて説明します。

注:Get Started Journeyのエクスペリエンスは、RBACの権限によって異なります。

Cisco IQの確認

利用可能なCisco IQの機能とアプリケーションを確認します。次のような機能があります。

- スタートパッド：アプリケーションへのアクセス、新機能の検出、ダッシュボードの作成
- 資産申請：詳細は、「資産申請」を参照してください。
- 評価アプリケーション：詳細は、『評価アプリケーション』を参照してください
- Support Application：詳細は、『Support Application』を参照してください
- Cisco IQ AI Assistant：詳細は、『AI Assistant』を参照してください

最初のAIレポートの生成

Cisco IQのAIを活用した分析機能は、特定のビジネスニーズに合わせてカスタマイズ可能な、選択した資産に基づいてカスタマイズ可能な対象を絞ったレポートを生成します。

最初のAIレポートの生成の詳細については、「アセットアプリケーション」を参照してください。

Cisco IQ AI Assistantへの質問

Get Startedプロセスの最後のステップは、どこからでもCisco IQ AI Assistantを起動して、資産、ケース、またはアセスメントについて質問することです。

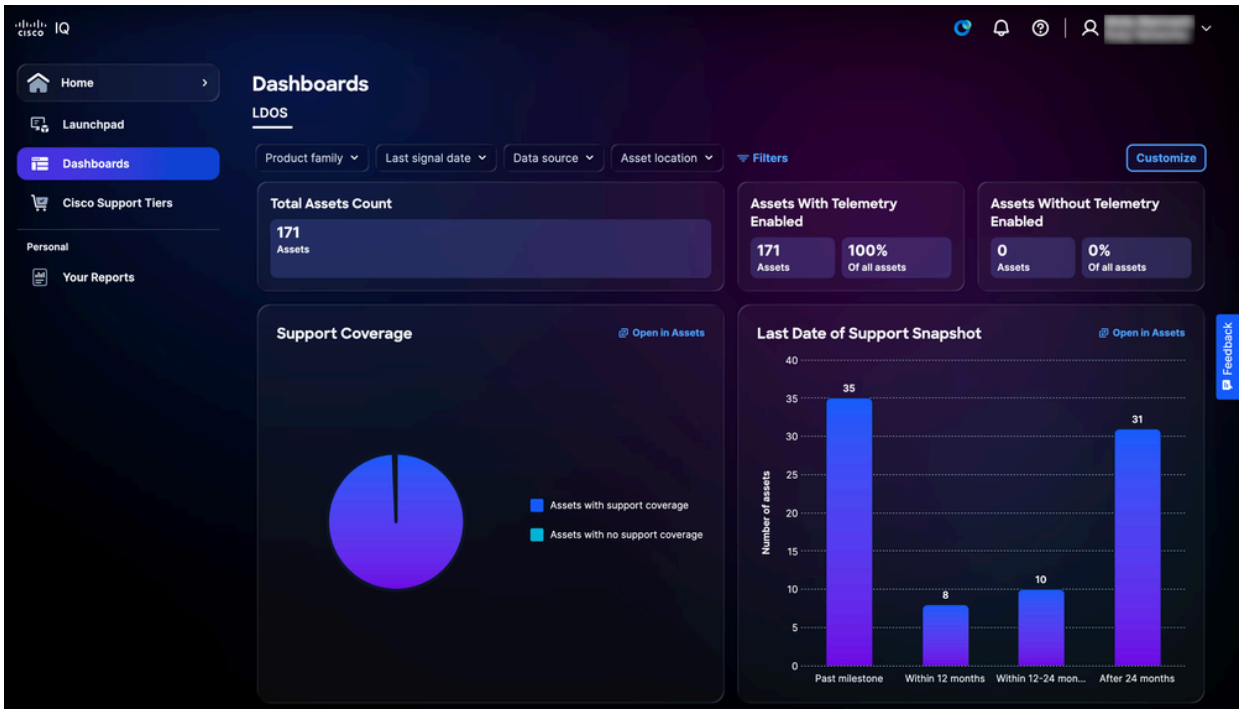
Cisco IQ AI Assistantの使用方法の詳細については、AI Assistantを参照してください。

[ダッシュボード（Dashboards）]

Dashboardsタブには、Cisco IQで使用可能な次のダッシュボードが表示されます。

LDOSダッシュボード

LDOSダッシュボードでは、LDOSメトリックに関する包括的で詳細な洞察が提供されます。これにより、顧客の可視性が高まり、ユーザがリスクをプロアクティブに管理できるようになり、情報に基づいた効率的な意思決定がサポートされます。



LDOSダッシュボード

LDOSダッシュボード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Filtersをクリックして、使用可能なフィルタオプションのリストからフィルタを選択します。

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。

注：ユーザのロールと権限に応じて、異なるフィルタを使用できます。

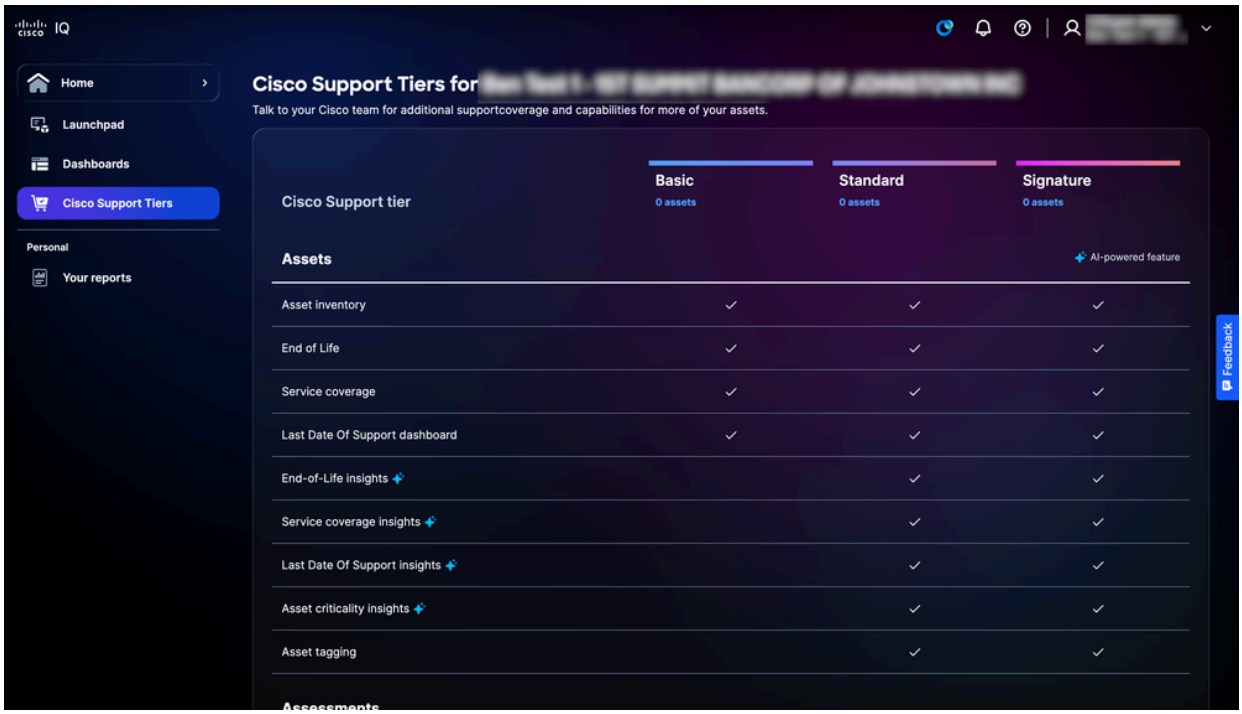
LDOSダッシュボードの詳細の表示

Open in Assetsをクリックすると、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。

シスコのサポート階層

「Cisco Support Tiers」ページには、購入したサポート階層で使用できる機能の概要と、リンクされたサポート契約に関連するアセットの数が表示されるので、含まれているサポート機能を簡単に理解し、その機能を管理および確認するための措置を講じることができます。サポート層の

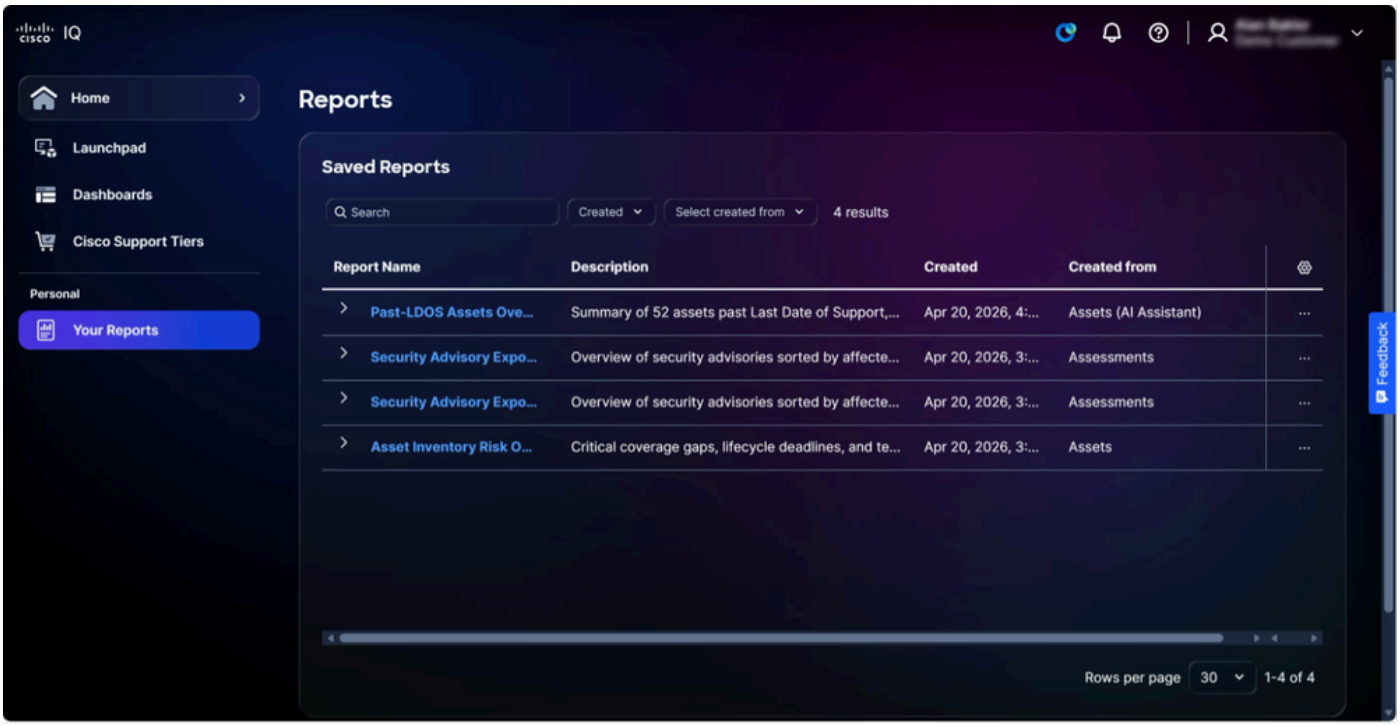
機能の詳細については、「サポート層」を参照してください。



シスコのサポート階層

レポート

レポート機能を使用すると、AIで生成されたインサイトをパーソナライズされたYour Reportsリストに保存することで、Cisco IQ全体で一元化して管理し、自分のデータに迅速かつ安全にアクセスできるようにします。



レポート

System Settings

System Settingsメニューに移動するには、Home > System Settingsの順に選択します。Account Detailsページが表示されます。

注：システム設定は、アカウント管理者のみが使用できます。

アカウントの詳細

システム設定機能により、管理、アクセス制御、およびデータ割り当てが容易になり、アカウント管理者は包括的な可視性とアクセスを確保できます。アカウントの詳細ページを表示すると、詳細セクションに次の情報が表示されます。

- アカウント名（Account Name）
- 勘定タイプ
- データストレージ領域
- ユーザ
- 作成日

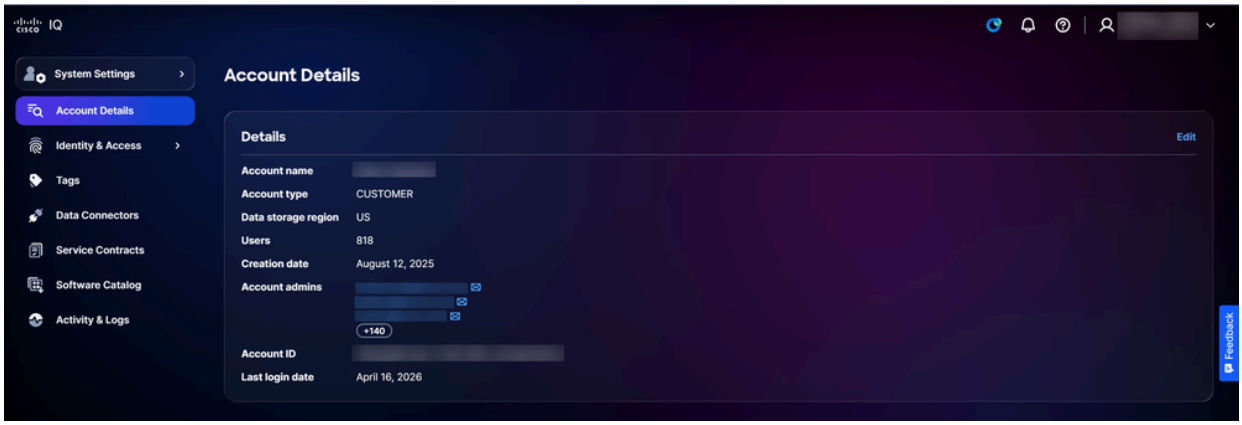
- アカウント管理者
- account id
- 最終ログイン日

アカウント名の編集

Account Detailsページで変更できるのは、アカウント名だけです。

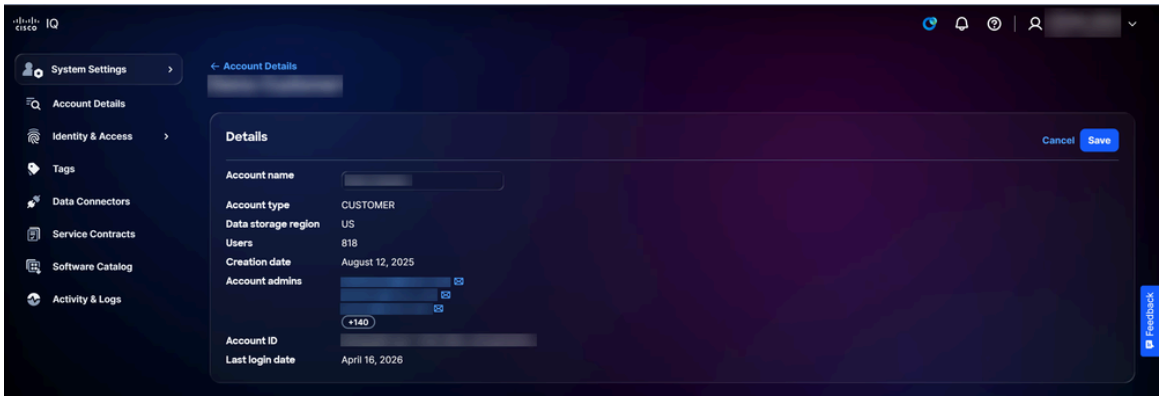
注:データストレージ領域などのフィールドを変更するには、新しい会社アカウントを作成する必要があります。

アカウント名を編集するには：



アカウントの詳細

1. [Edit] をクリックします。



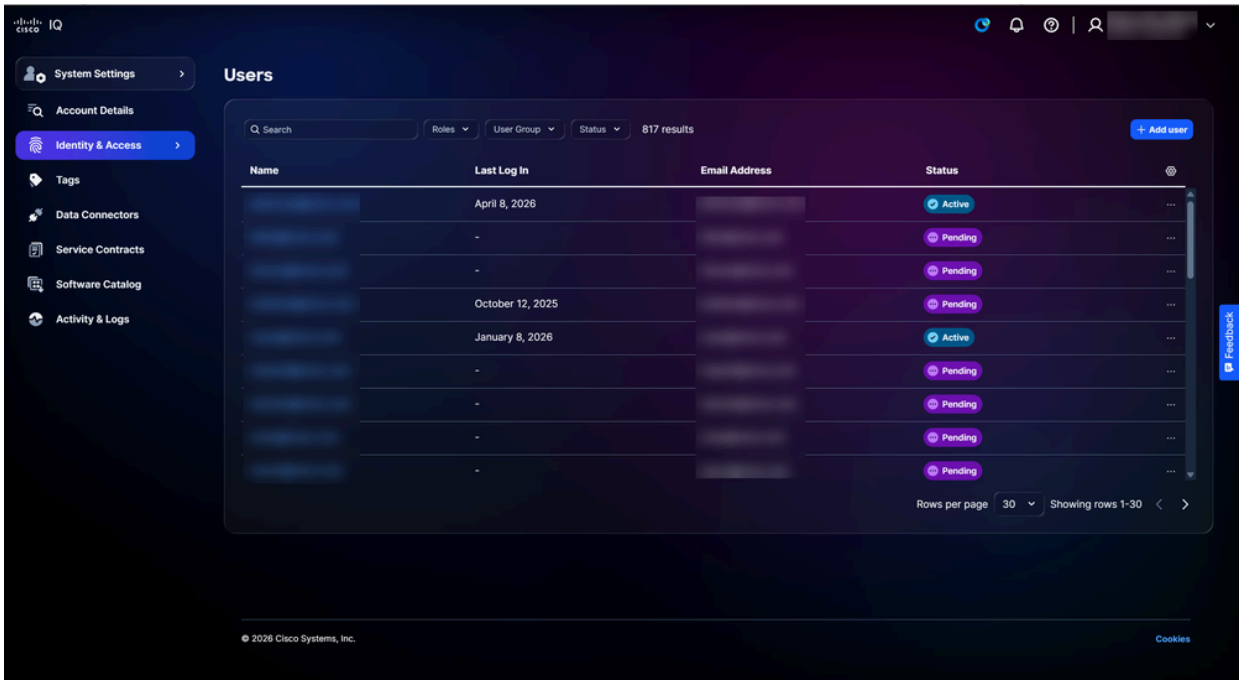
アカウント名の編集

2. アカウント名を修正します。

3. [Save] をクリックします。

ユーザ

ユーザアカウントの作成、変更、削除はUsersページで行います。Usersページに移動するには、System Settings > Identity & Access > Usersの順に選択します。Usersページが表示されます。



ユーザ

検索とフィルタを使用して、ページ上部のフィールドを使用してリストを絞り込むことができます。

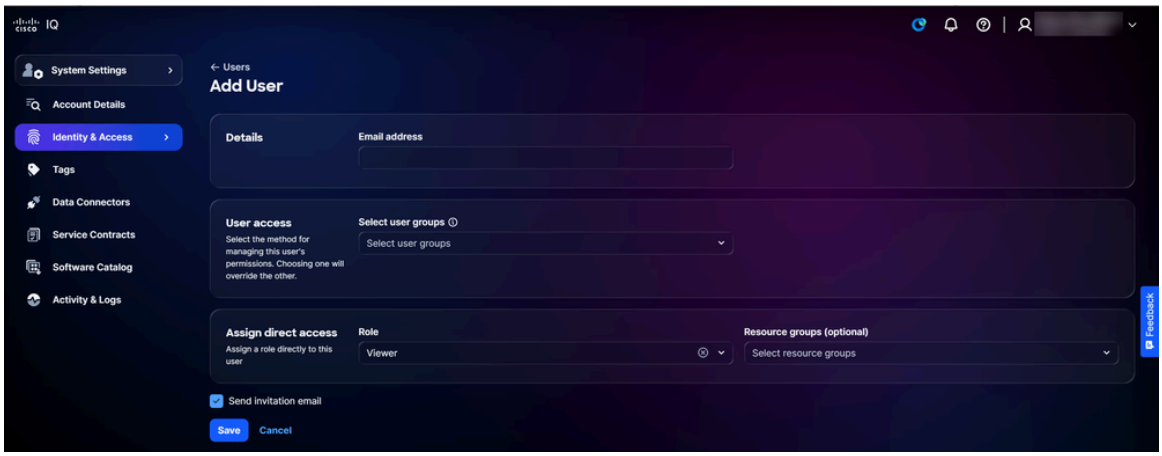
新規ユーザの追加

新しいユーザを追加するには、次の手順を実行します。

注：新しいユーザを追加できるのは、アカウント管理者またはその他の権限のあるユーザだけです。

---

1. Usersページで、Add User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

2. 電子メールアドレスを入力します。
3. 必要に応じて、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。
4. ドロップダウンリストからロールを選択します。

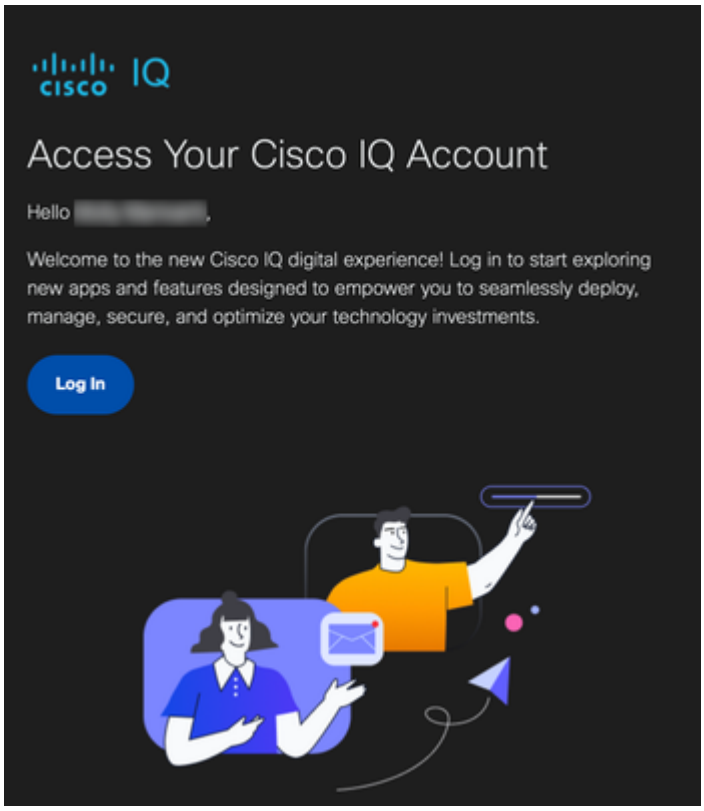
> 注：ユーザは、ロールを持つ1つ以上のユーザグループに属しているか、1つ以上のロールが割り当てられている必要があります。

5. 必要に応じて、ドロップダウンリストからリソースグループを選択します。

> 注：選択したロールの「リソースグループ」ドロップダウンリストのみが表示されます。

6. Send invitation emailチェックボックスにチェックマークが付いていることを確認します。
7. [Save] をクリックします。Usersページに確認が表示されます。

ユーザは、アカウント管理者から招待された後に電子メールを受信します。

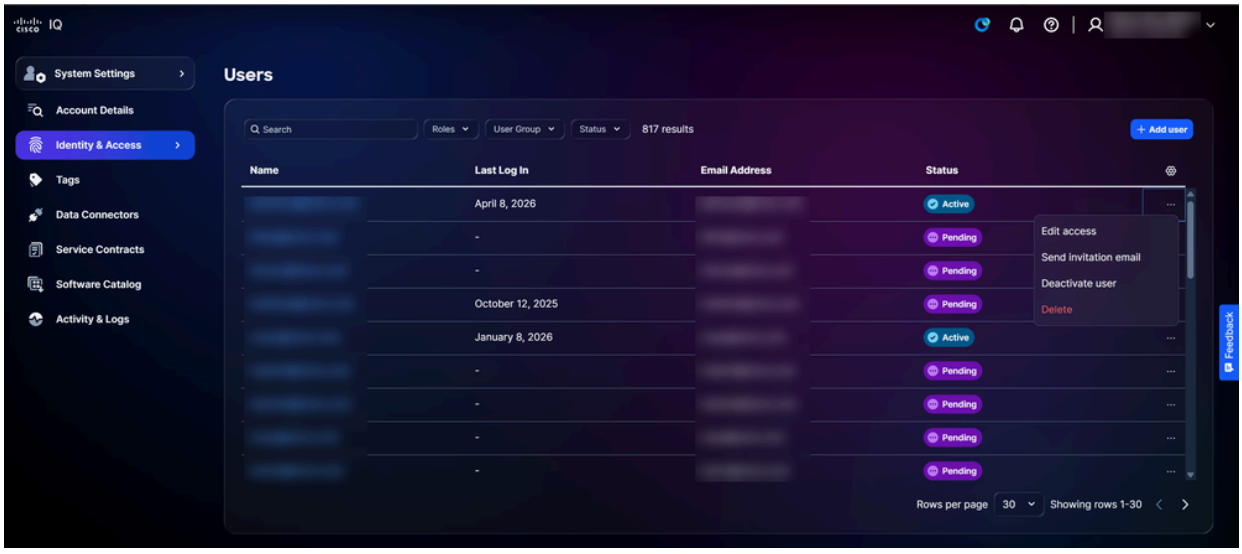


電子メールによる招待

招待されたユーザは、電子メールでLog Inをクリックしてアカウントにログインできます。ログイン後、ユーザのステータスがActiveになります。

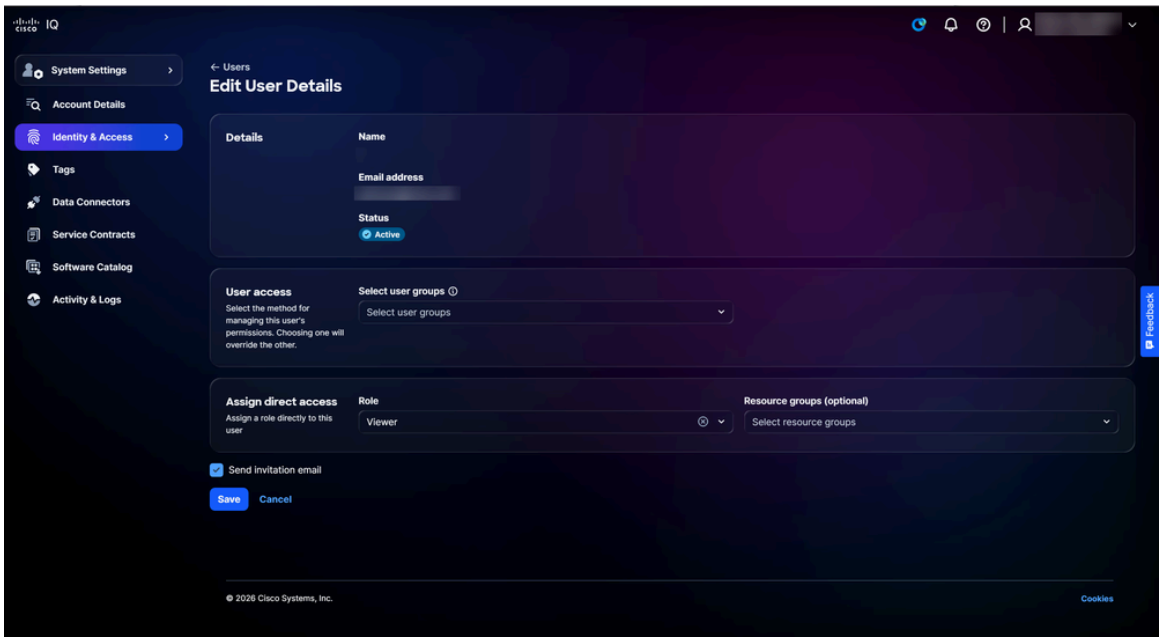
ユーザーアクセスの編集

ユーザーアカウントのユーザーグループ、役割、またはリソースグループを編集するには、次の手順に従います。



アクセス権の編集

1. Usersページの目的のユーザから、More Optionsアイコン> Edit accessを選択します。Edit User Detailsページが表示されます。



ユーザーの詳細の編集

2. 目的のユーザグループ、ロール、およびリソースグループを編集します。

> 注:リソースグループは、選択したロールについてのみ表示されます。

3. [Save] をクリックします。

招待メールの送信

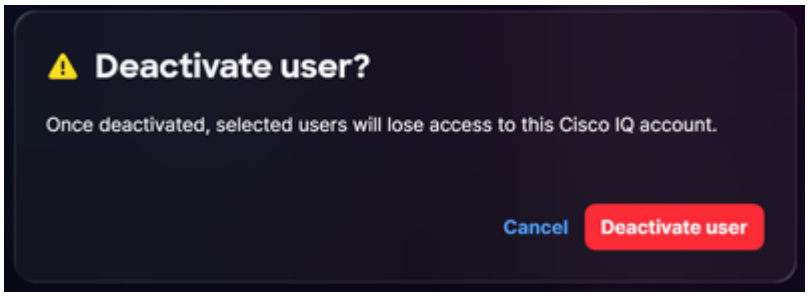
既存のユーザアカウントに招待メールを送信するには、次の手順を実行します。

1. Usersページに移動します。
2. 目的のユーザから、More Optionsアイコン> Send invitation emailを選択します。確認が表示されます。

ユーザの非アクティブ化

ユーザーアカウントを非アクティブ化するには、次の手順に従います。

1. Usersページの目的のユーザから、More Optionsアイコン> Deactivate userを選択します。Deactivate userウィンドウが開きます。



ユーザーの非アクティブ化の確認

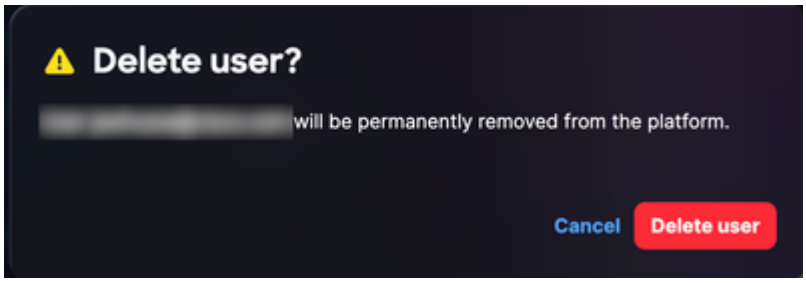
2. Deactivate userをクリックして確定します。確認が表示されます。

ユーザの削除

⚠ 警告：ユーザーの削除は元に戻せません。

ユーザを削除するには、次の手順を実行します。

1. Usersページの目的のユーザから、More Optionsアイコン> Deleteを選択します。Delete userウィンドウが開きます。



ユーザーの削除の確認

2. Delete userをクリックします。ユーザが削除されます。

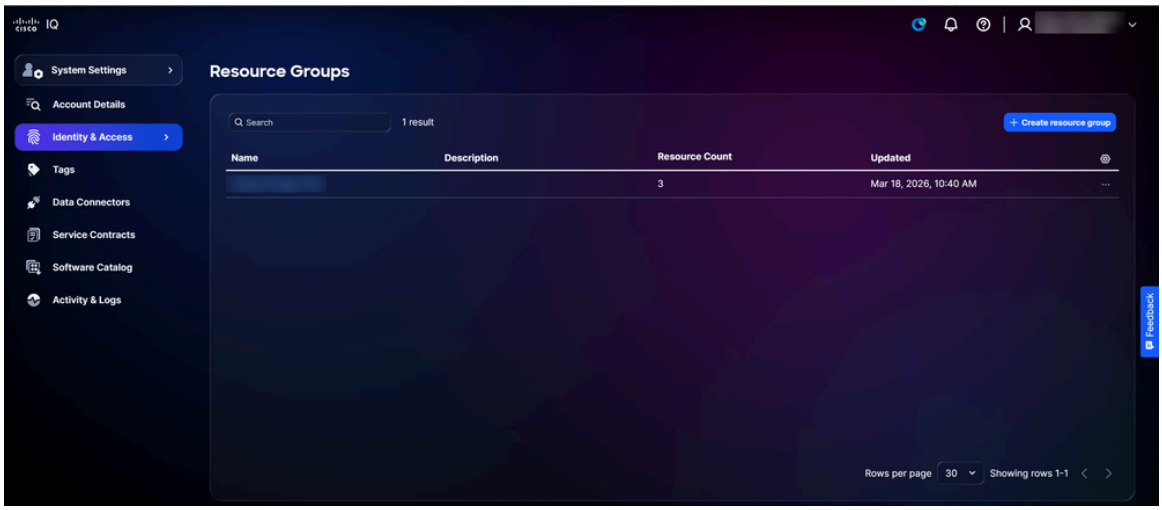
リソースグループ

リソースグループは、タイプと属性に基づいてリソースを指定する動的なコレクションです。リソースグループを設定すると、グループの条件を満たすリソースへのロールのデータアクセスを制限できます。リソースは、複数のリソースグループに属することができます。アカウント管理者は、リソースグループを作成、編集、および削除できます。

リソースグループを表示するには

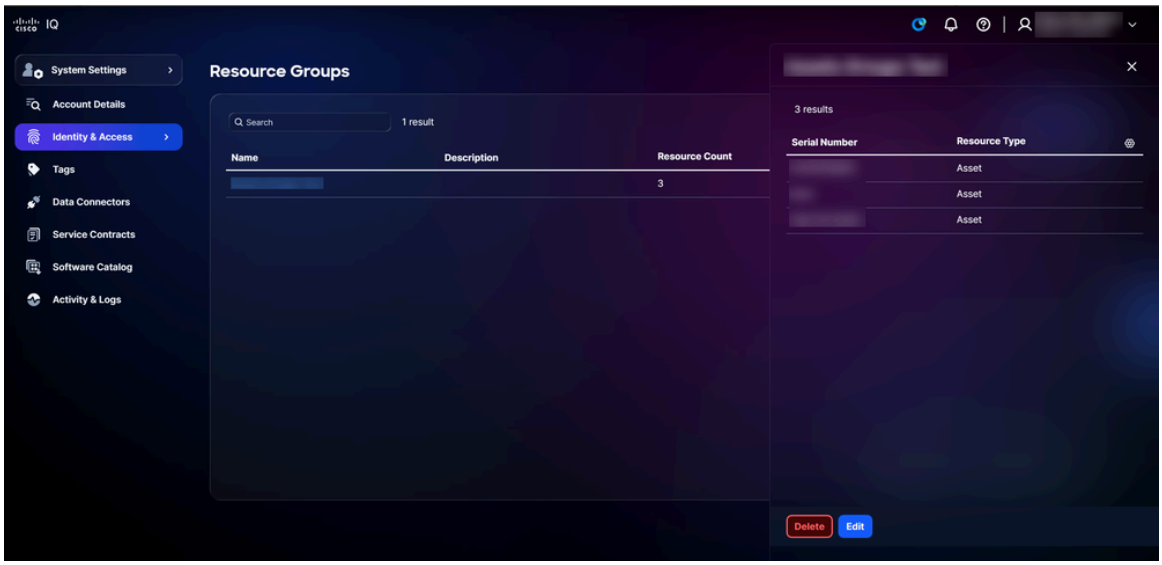
1. System Settings > Identity & Access > Resource Groupsの順に選択します。Resource

Groupsページが表示されます。



リソースグループ

2. SearchフィールドとFilterフィールドを使用して、リストを絞り込みます。
3. リソースグループ名をクリックすると、その詳細が表示されます。

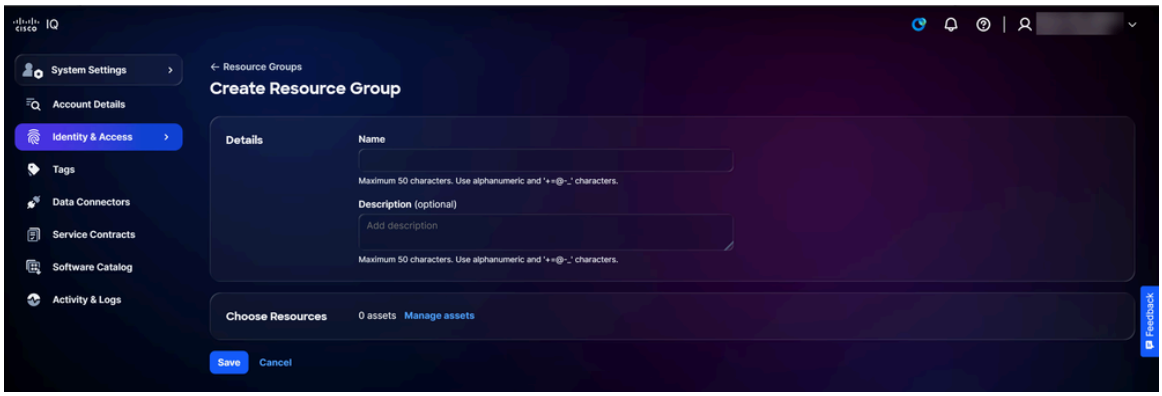


リソースグループの詳細

リソースグループの作成

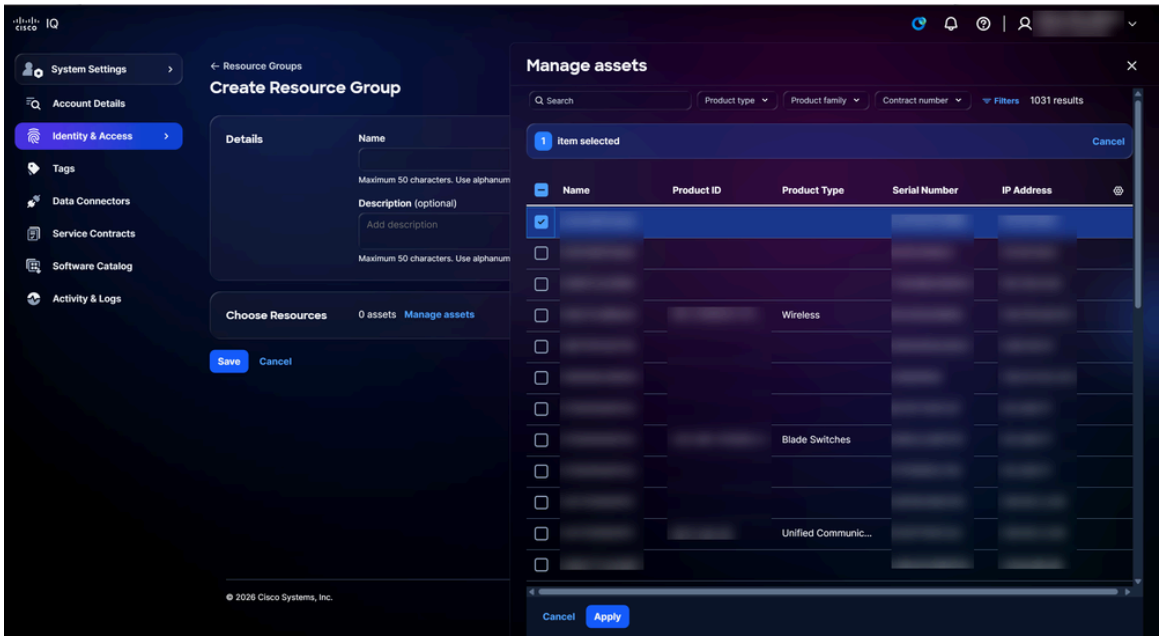
新しいリソースグループを作成するには

1. Resource Groupsページで、Create resource groupをクリックします。Create Resource Groupページが表示されます。



リソースグループの作成

2. リソースグループの名前を入力します
3. 必要に応じて、「摘要」を入力します。
4. Manage assetsをクリックします。アセットの管理ウィンドウが開きます。

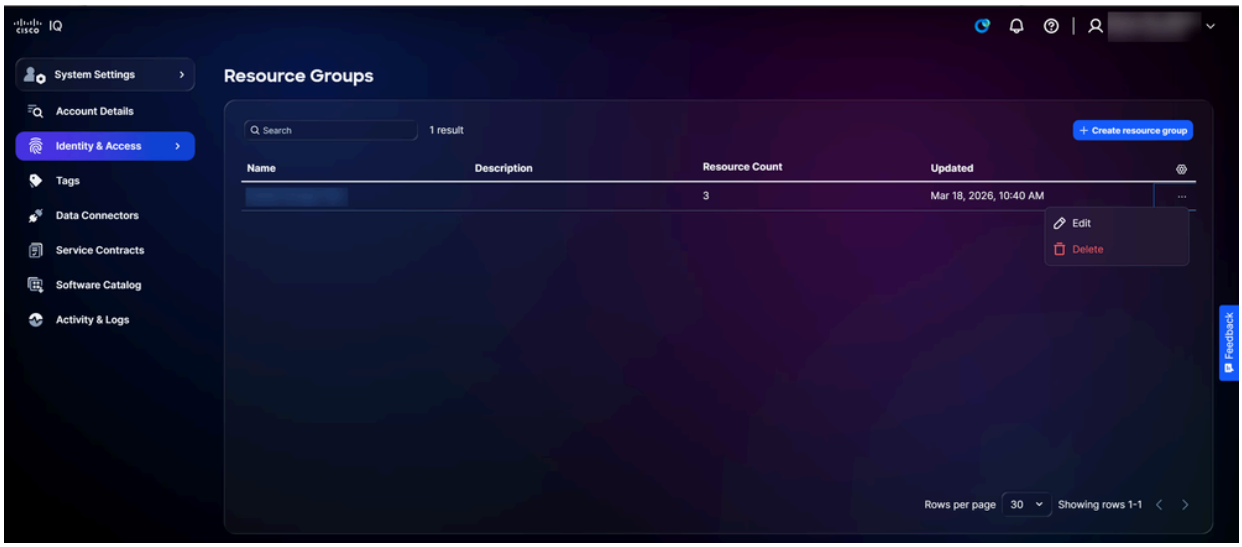


資産の管理

5. 必要なアセットのチェックボックスをオンにします。
6. [APPLY] をクリックします。
7. [Save] をクリックします。

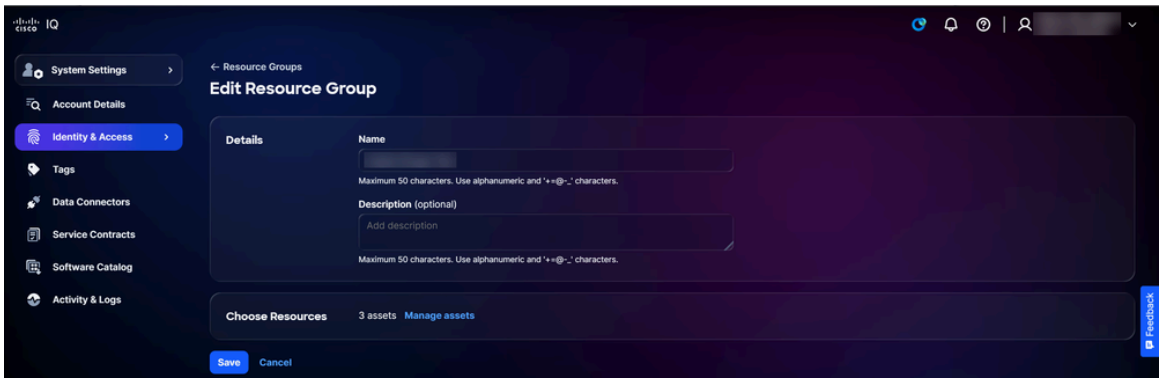
リソースグループの編集

リソースグループを編集するには



編集

1. Resource Groupsページのレコードから、More Optionsアイコン> Editを選択します。Edit Resource Groupページが表示されます。



リソースグループの編集

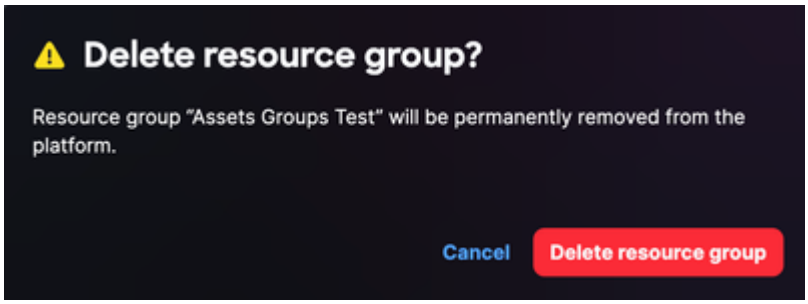
2. 必要に応じて、リソースグループ属性を編集します。
3. [Save] をクリックします。

リソースグループの削除

⚠ 警告：リソースグループの削除は元に戻せません。

リソースグループを削除するには

1. Resource Groupsページのレコードから、More Optionsアイコン> Deleteを選択します。「リソースグループの削除」ウィンドウが開きます。



リソースグループの削除

2. Delete resource groupをクリックします。リソースグループが削除されます。

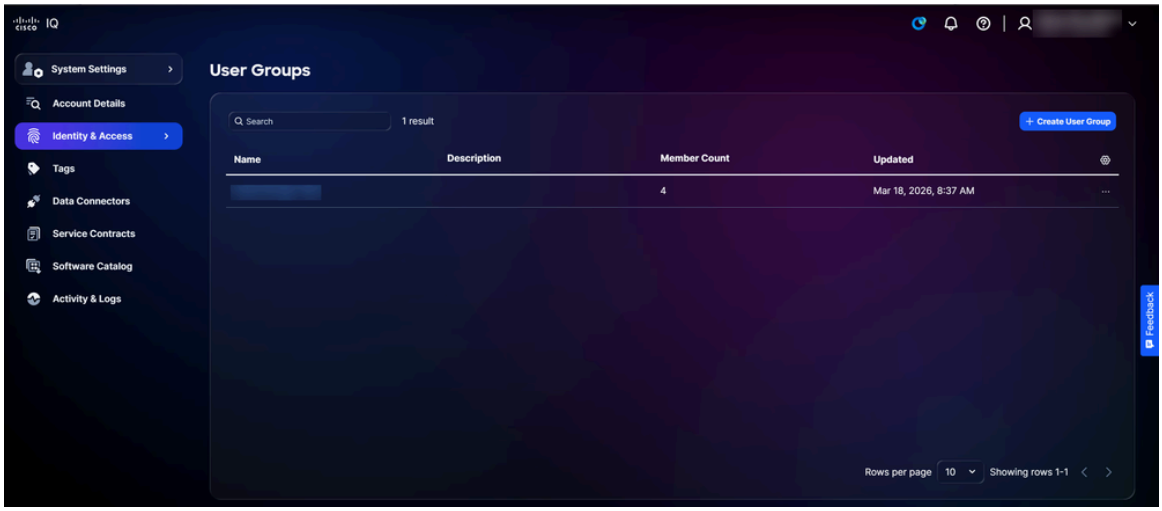
ユーザーグループ

ユーザーグループを作成、編集、および削除することで、アカウント全体でユーザーを効果的に制御できます。

注：デフォルトでは、Cisco IQのすべてのアカウントに「All account users」ユーザグループが存在し、このユーザグループを削除または編集することはできません。常に、特定のタイプのすべてのアカウントユーザが含まれます。その目的は、アカウントのすべてのユーザにロールを適用することです。

ユーザー・グループを表示するには、次の手順に従います。

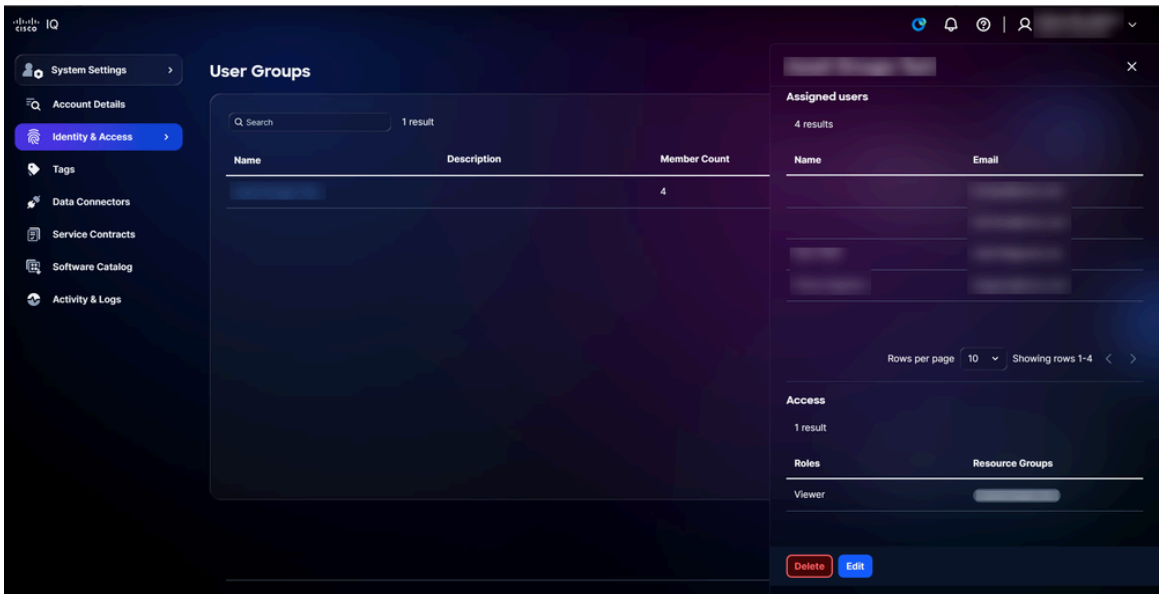
1. System Settings > Identity & Access > User Groupsの順に選択します。User Groupsページが表示されます。



ユーザーグループ

2. SearchフィールドとFilterフィールドを使用して、リストを絞り込みます。

3. ユーザグループ名をクリックすると、詳細が表示されます。

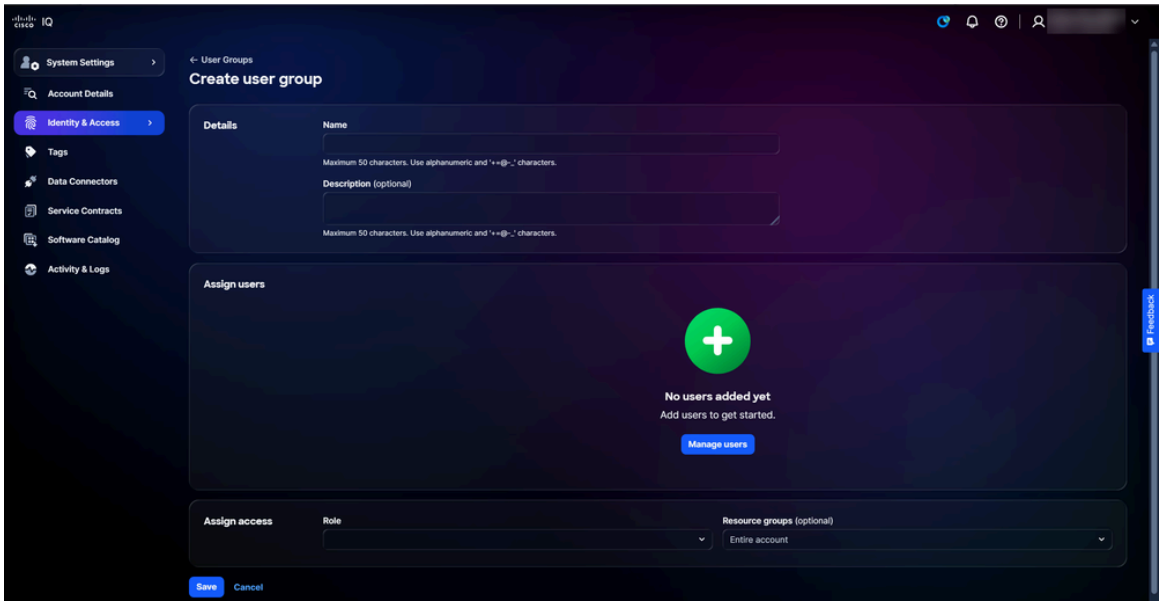


ユーザグループの詳細

ユーザグループの作成

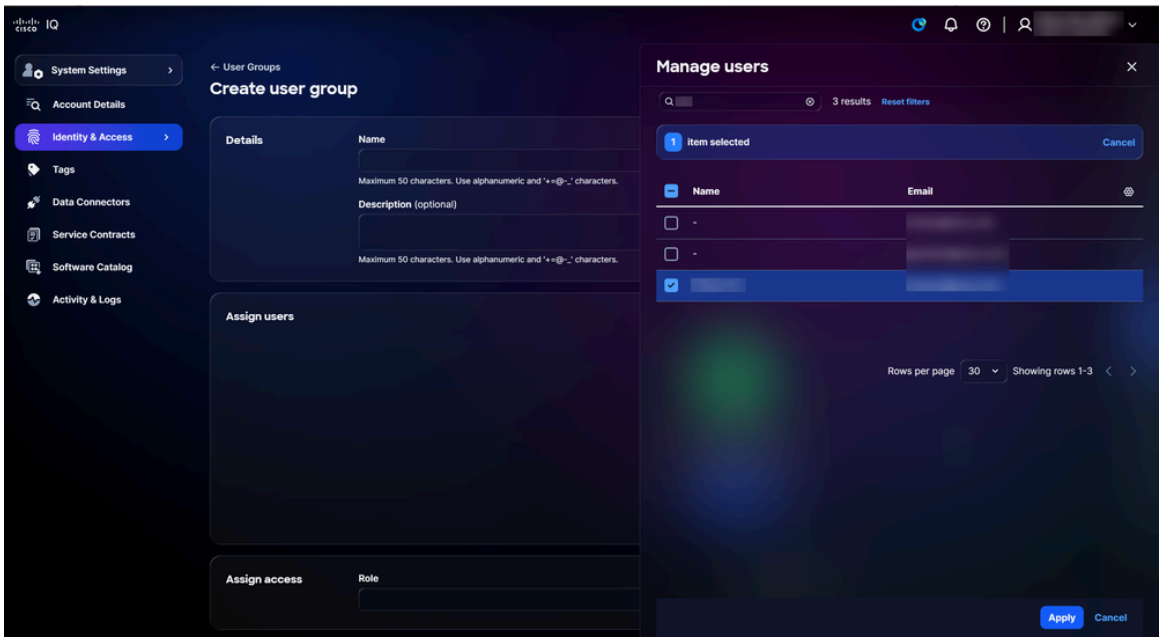
新しいユーザー・グループを作成するには、次の手順に従います。

1. 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

2. ユーザグループの名前を入力します。
3. 必要に応じて、「摘要」を入力します。
4. Manage usersをクリックします。Manage usersウィンドウが開きます。



ユーザーの管理

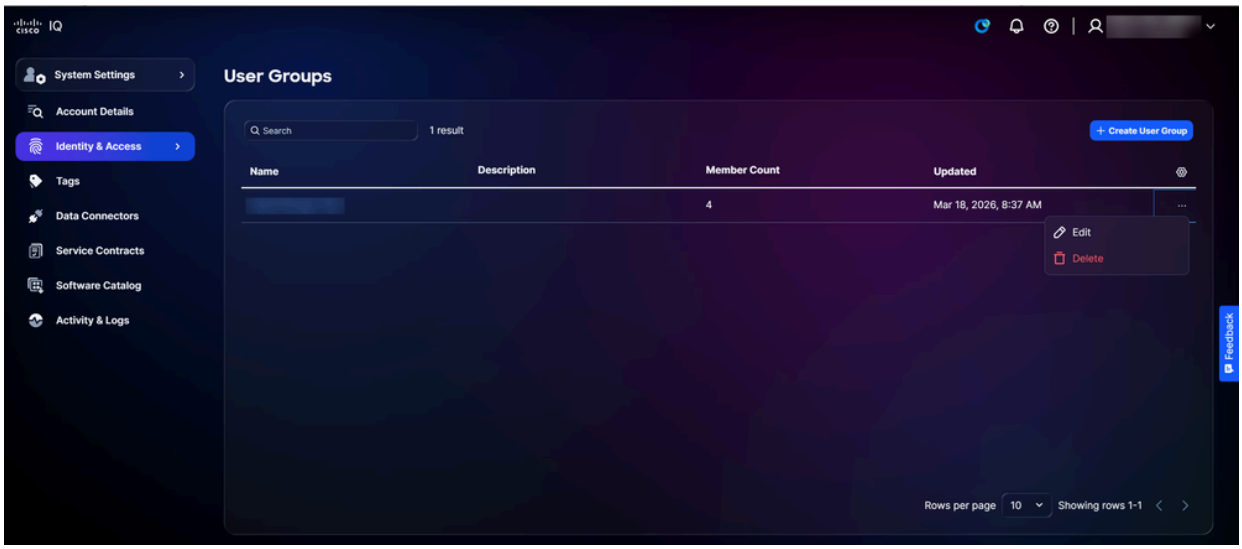
5. 該当するユーザのチェックボックスをオンにします。
6. [APPLY] をクリックします。
7. ドロップダウンリストからロールを選択します。
8. 必要に応じて、ドロップダウンリストからリソースグループを選択します。

> 注：リソースグループを追加すると、ユーザグループがアクセスできるリソースが制限されます。ロールが割り当てられているが、リソースグループが選択されていない場合、そのロールはアカウント内のロールに関連するすべてのリソースに適用されます。

9. [Save] をクリックします。新しいユーザグループが「ユーザグループ」テーブルに表示されます。

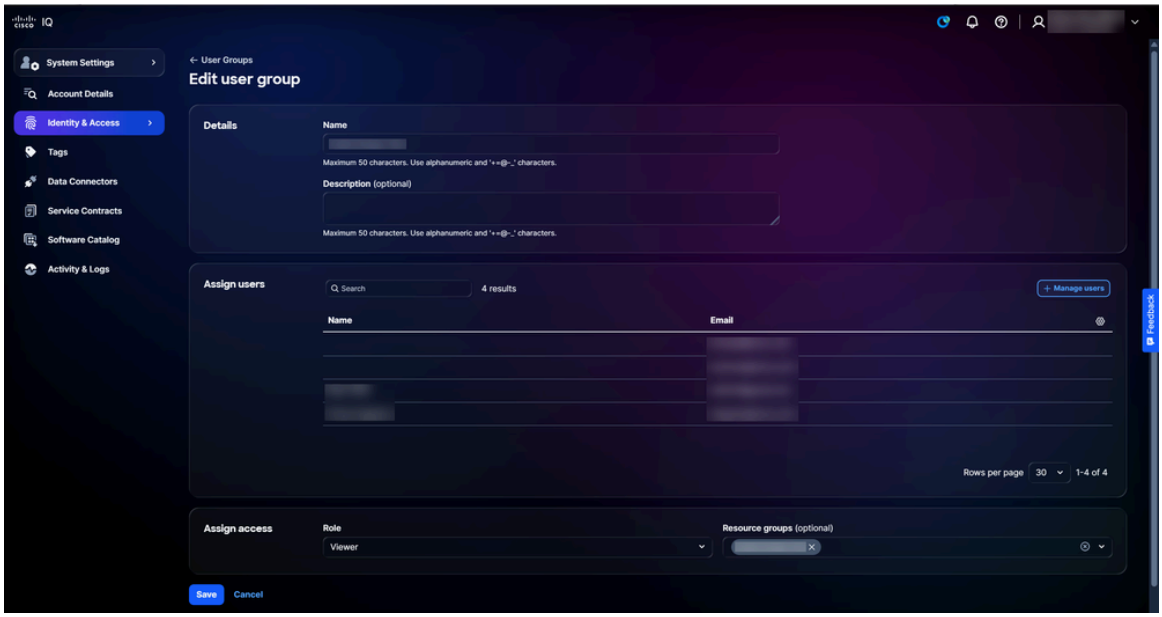
ユーザグループの編集

ユーザー・グループを編集するには、次の手順に従います。



編集

1. User Groupsページのレコードから、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

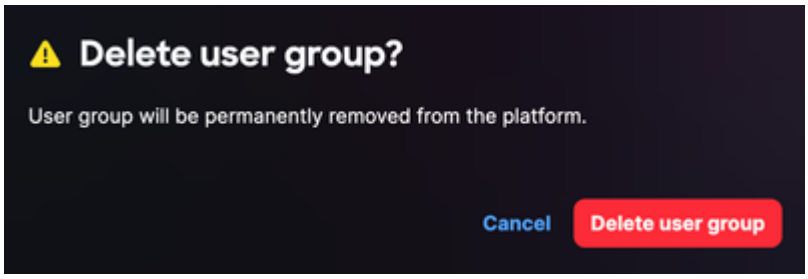
2. 必要に応じて、ユーザグループ属性を編集します。
3. [Save] をクリックします。

ユーザグループの削除

⚠ 警告：ユーザーグループの削除は元に戻せません。

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ページのレコードから、More Optionsアイコン> Deleteを選択します。Delete user groupウィンドウが開きます。



ユーザグループの削除

2. Delete user groupsをクリックします。ユーザグループが削除されます。

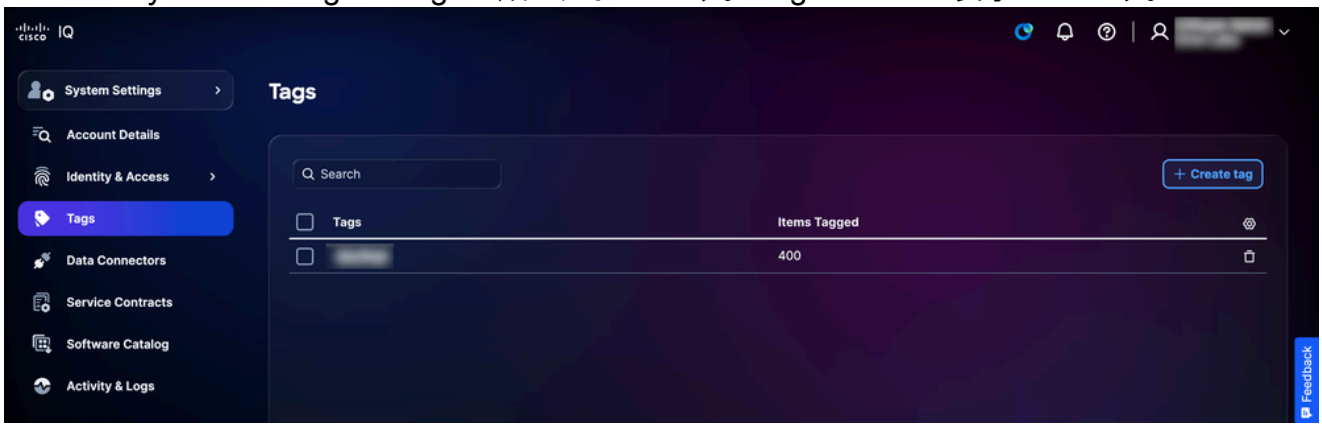
タグ

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、キーと値のペアのことで、たとえばEnvironment:ProdやLabel:Campusのように定義します。アカウント管理者は、タグを作成および削除したり、リソースグループにユーザーを割り当てたりして、デバイスに資産タグを割り当てることができます。リソースグループへのユーザーの割り当てについての詳細は、「リソースグループ」を参照してください。

資産タグの作成

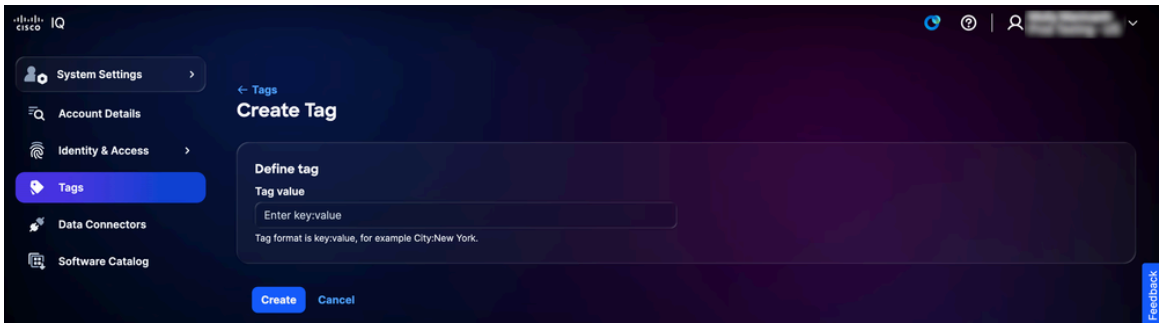
タグを作成するには：

1. Home > System Settings > Tagsの順に選択します。Tagsページが表示されます。



タグ

2. Create tagをクリックします。Create tagページが表示されます。



タグの作成

3. Enter key:valueフィールドにタグの値を入力します。

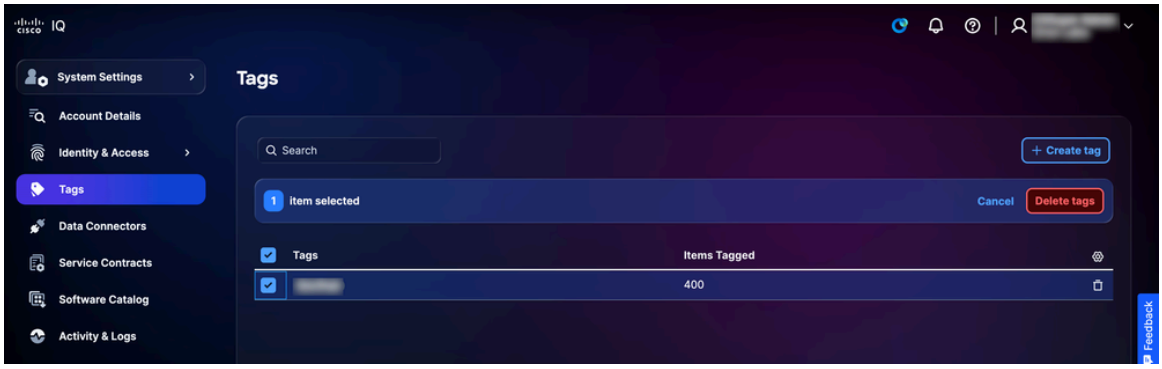
> 注：タグ名は`key:value`形式です(例：`City:NYC`)。

4. [Create] をクリックします。新しいタグが「タグ」ページのタグリストに表示されます。

資産タグの削除

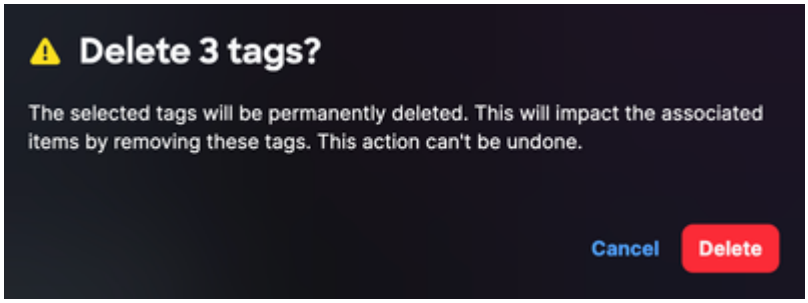
タグを削除するには

1. Home > System Settings > Tagsの順に選択します。Tagsページが表示されます。



タグ

2. 削除するタグのチェックボックスをオンにします。
3. タグの削除をクリックします。確認が表示されます。



タグの削除

4. Deleteをクリックして確定します。

データコネクタ

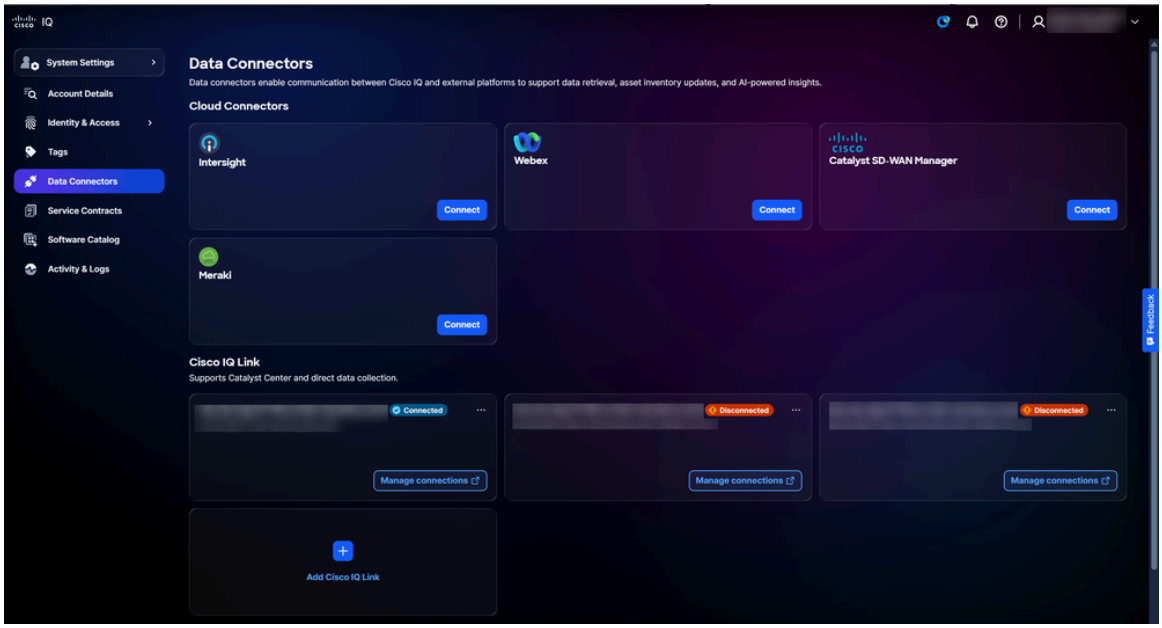
Cisco IQは、データコネクタを多層データ取り込みアプローチの一部として使用し、ネットワークに関する包括的な洞察を提供します。データコネクタは、ネットワーク上の資産からテレメトリを収集し、Cisco IQが適切な洞察と信頼できる専門知識を提供できるようにします。

クラウドコネクタの追加

シスコのクラウド製品データをCisco IQに接続することは、強力でパーソナライズされた機能の使用を開始する最速の方法です。Intersight®、Meraki Dashboard、SD-WAN Manager、Webex® Control Hubの製品コントローラへのデータ接続を設定した後、数分でカスタマイズされたインサイトを受け取ることができます。

シスコクラウド製品を接続するには、次の手順を実行します。

1. System Settings > Data Connectorsの順に選択します。データコネクタページが表示されます。

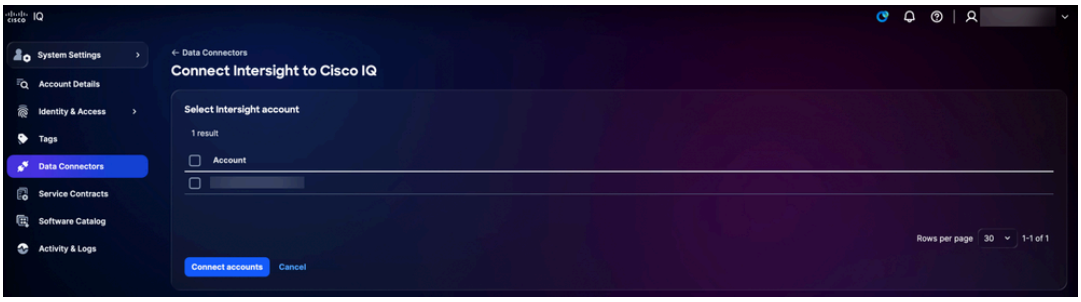


クラウドコネクタ

2. 目的のクラウドコネクタでConnectをクリックします。

3. 選択したクラウドコネクタについて、次の手順を実行します。

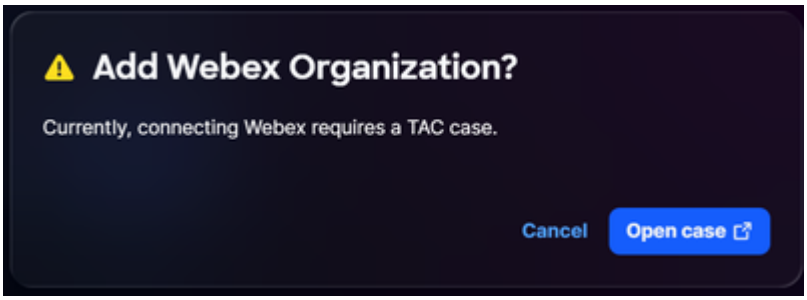
- Intersight



Intersightの接続

1. 該当するアカウントのチェックボックスをオンにします。
2. Connect accountsをクリックします。データコネクタのページにリダイレクトされ、確認が表示されます。

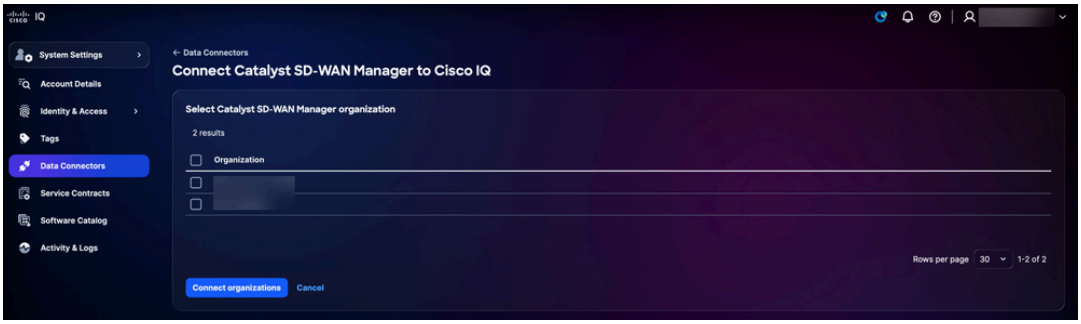
- Webex



Webexの接続

1. Add Webex Organizationウィンドウで、Open caseをクリックします。SCMにリダイレクトされます。
2. SCMでサポートケースを作成します。

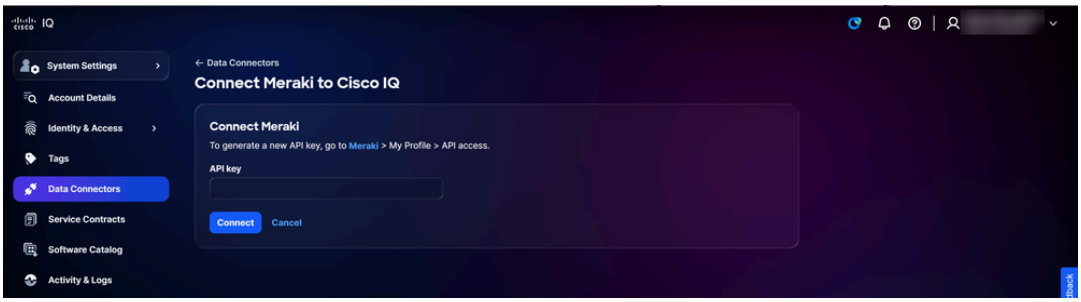
- Catalyst SD-WAN Manager



Catalyst SD-WAN Managerの接続

1. 目的の組織のチェックボックスをオンにします。
2. Connect organizationsをクリックします。データコネクタのページにリダイレクトされ、確認が表示されます。

- Meraki



Merakiの接続

1. 画面の指示に従います。
2. APIキーを入力します。
3. [Connect] をクリックします。データコネクタのページにリダイレクトされ、確認が表示されます。

Cisco IQ Linkインスタンスの追加

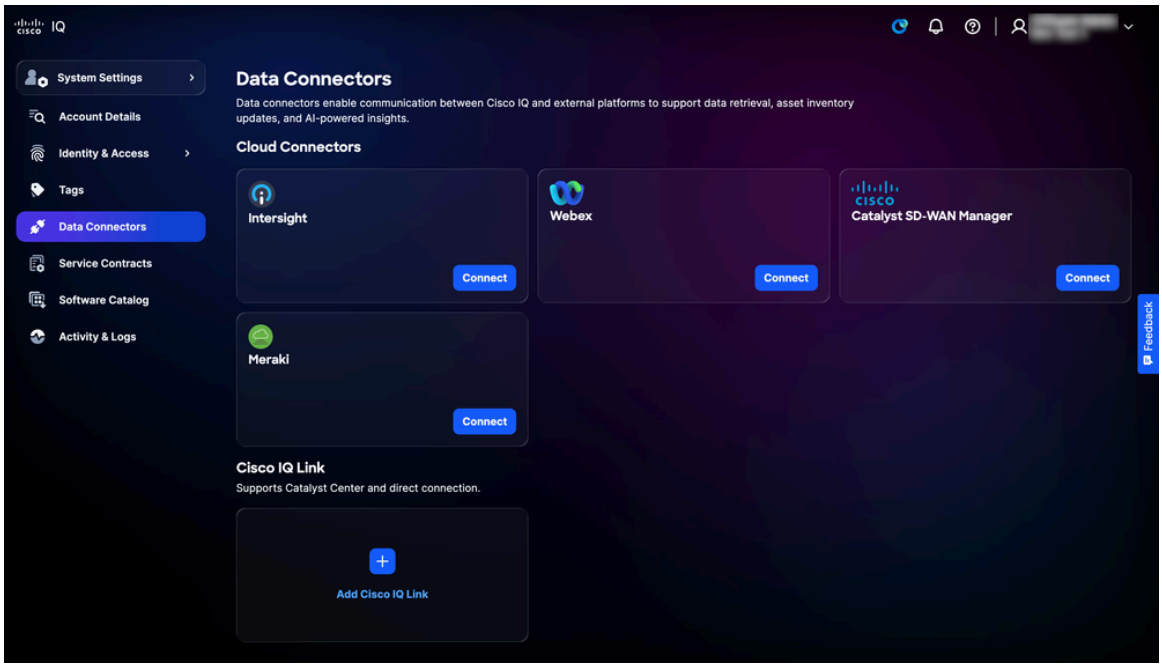
Cisco IQ Linkは、Cisco IQのオンプレミスコンポーネントで、ハードウェアとソフトウェアのライフサイクルやインベントリレポートなど、より豊富でインテリジェントな情報を提供します。以前のコレクタを仮想マシン(VM)にインストールした単一のコネクタに統合し、デバイスから詳細なテレメトリデータを収集します。

Cisco IQ Linkは、オンプレミスネットワーク内に導入され、自動デバイス検出とテレメトリ収集を実行します。Cisco IQ Linkは、Catalyst Centerとの直接接続と統合をサポートしています。また、移行を通じてアカウントを作成した場合は、CXエージェントまたはCSPCを利用してテレメトリに接続できます。

注：クラウドマネージドコントローラでは、必要なデータにシスコクラウドから直接アクセスできるため、Cisco IQ Linkは不要です。

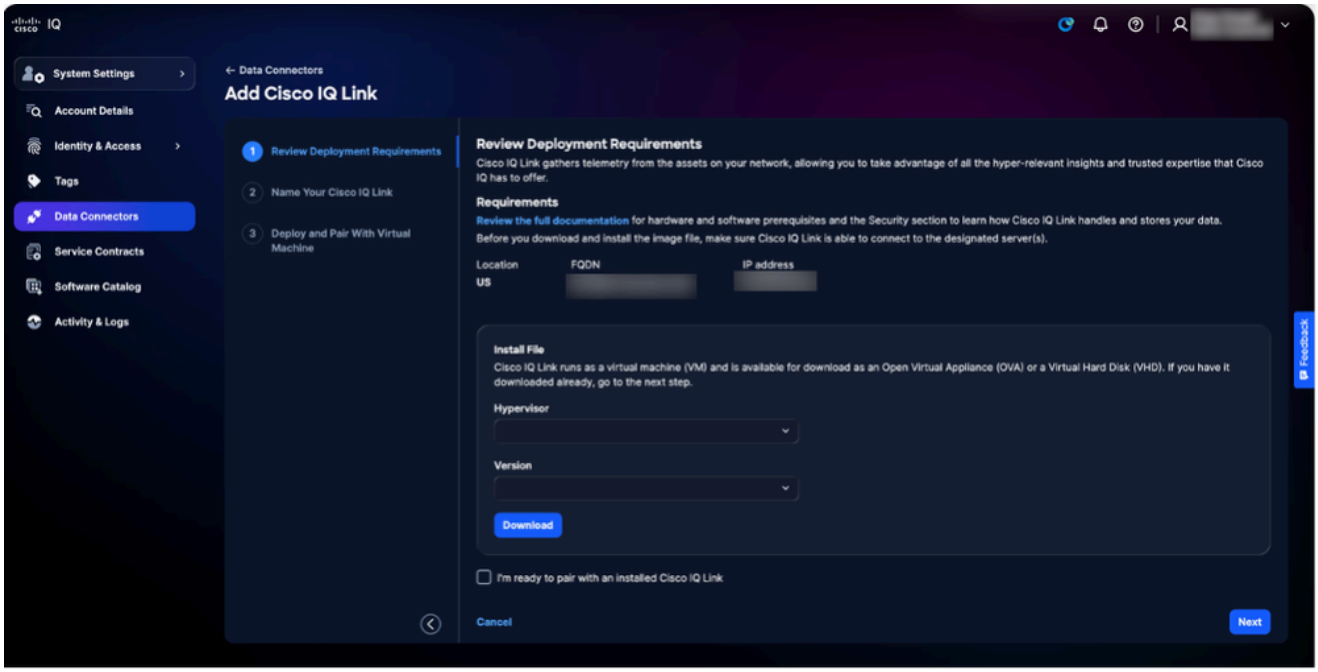
Cisco IQ LinkインスタンスをCisco IQに追加するには：

1. データコネクタページに移動します。



Cisco IQ Linkの追加

2. Add Cisco IQ Linkをクリックします。



OVAまたはVHDのダウンロード

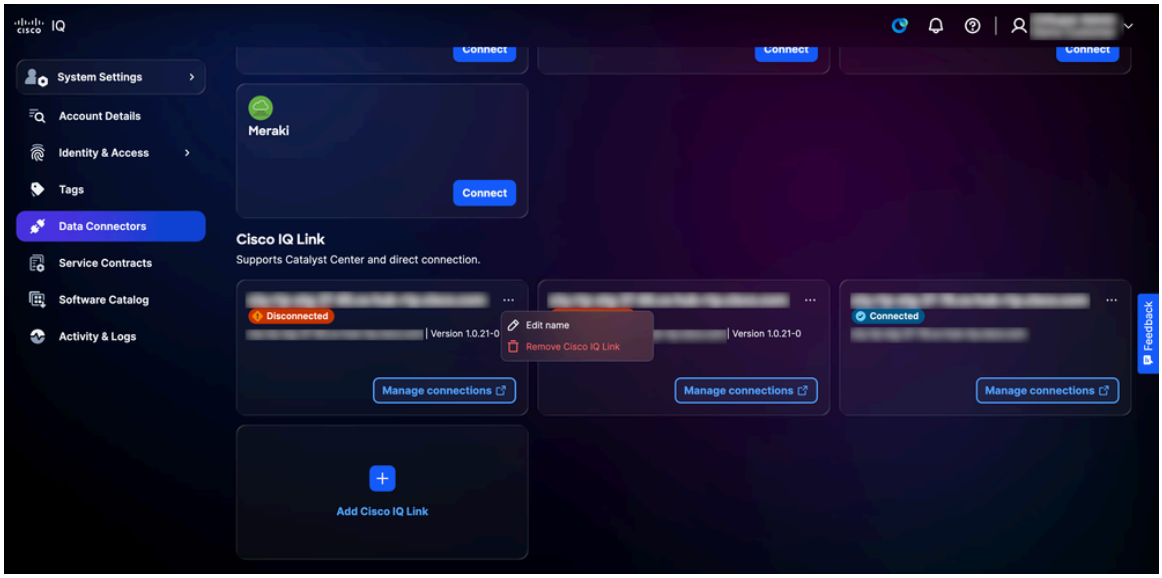
3. Open Virtual Appliance(OVA)または仮想ハードディスク(VHD)をダウンロードします。
    1. ドロップダウンリストからハイパーバイザを選択します。
    2. ドロップダウンリストからバージョンを選択します。
    3. [Download] をクリックします。
4. Review the full documentationをクリックして、Cisco IQ Link Getting Started Guideにアクセスします。このドキュメントでは、前の手順でダウンロードしたファイルを使用して

Cisco IQ Linkをインストールする手順を包括的に説明します。Cisco IQとCisco IQ Linkインターフェイス間で必要なすべての遷移を含む、完全な導入ワークフローをカバーし、ペアリングと設定を完了します。

Cisco IQ Linkインスタンス名の編集

Cisco IQ Linkインスタンス名を編集するには：

1. データコネクタページで、目的のCisco IQ Linkインスタンスに移動します。



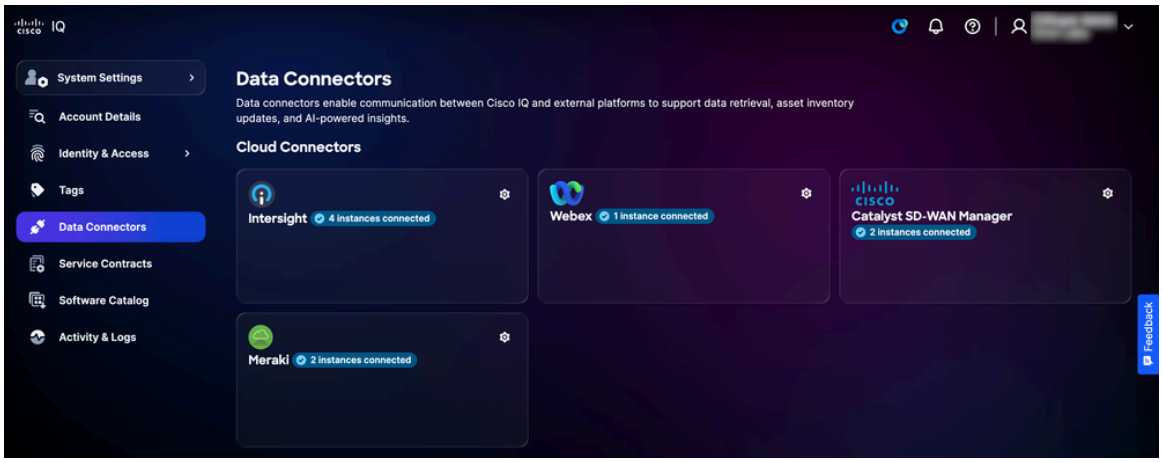
名前の編集

2. More Optionsアイコン> Edit nameを選択します。
3. 必要に応じて名前を編集します。
4. [Update] をクリックします。

クラウドコネクタからの接続アカウントの削除

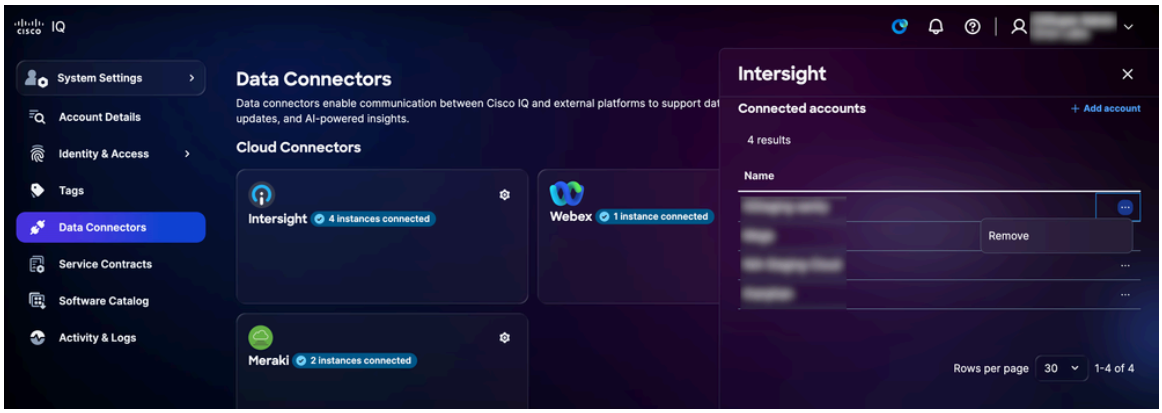
接続されているアカウントをクラウドコネクタから削除するには、次の手順を実行します。

1. Data Connectorsページで、目的のクラウドコネクタに移動します。



クラウドコネクタの設定

2. Settingsアイコンをクリックします。Connected accountsウィンドウが開きます。



Cloud Connector接続アカウントの削除

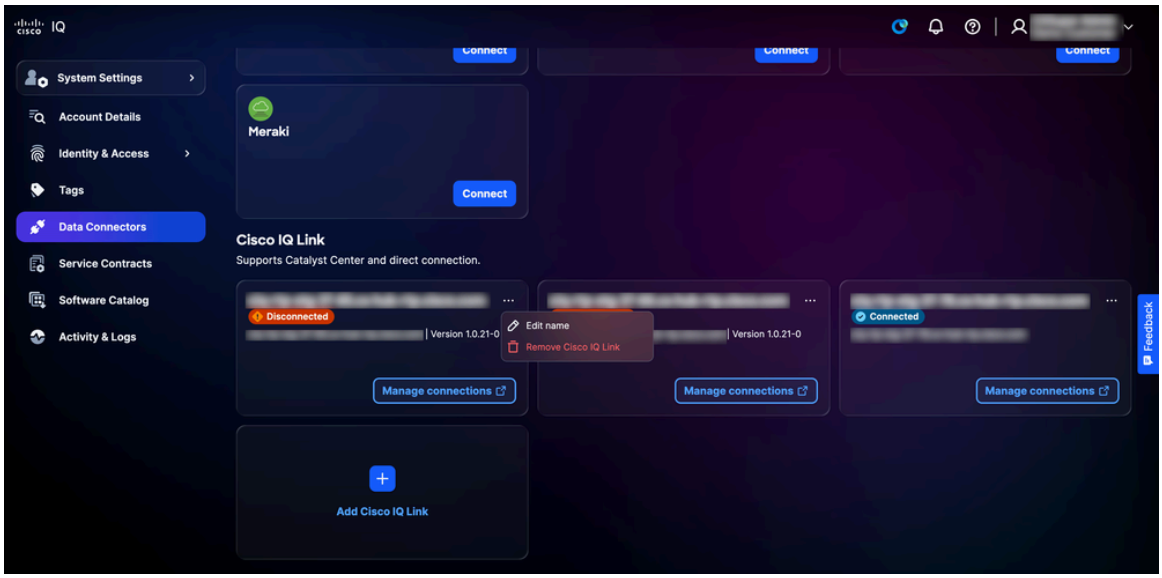
3. 目的のアカウントから、More Optionsアイコン> Removeを選択します。確認が表示されます。

4. Removeをクリックして確定します。

Cisco IQ Linkインスタンスの削除

データコネクタからCisco IQ Linkインスタンスを削除するには：

1. データコネクタページで、目的のCisco IQ Linkインスタンスに移動します。



Cisco IQ Linkの削除

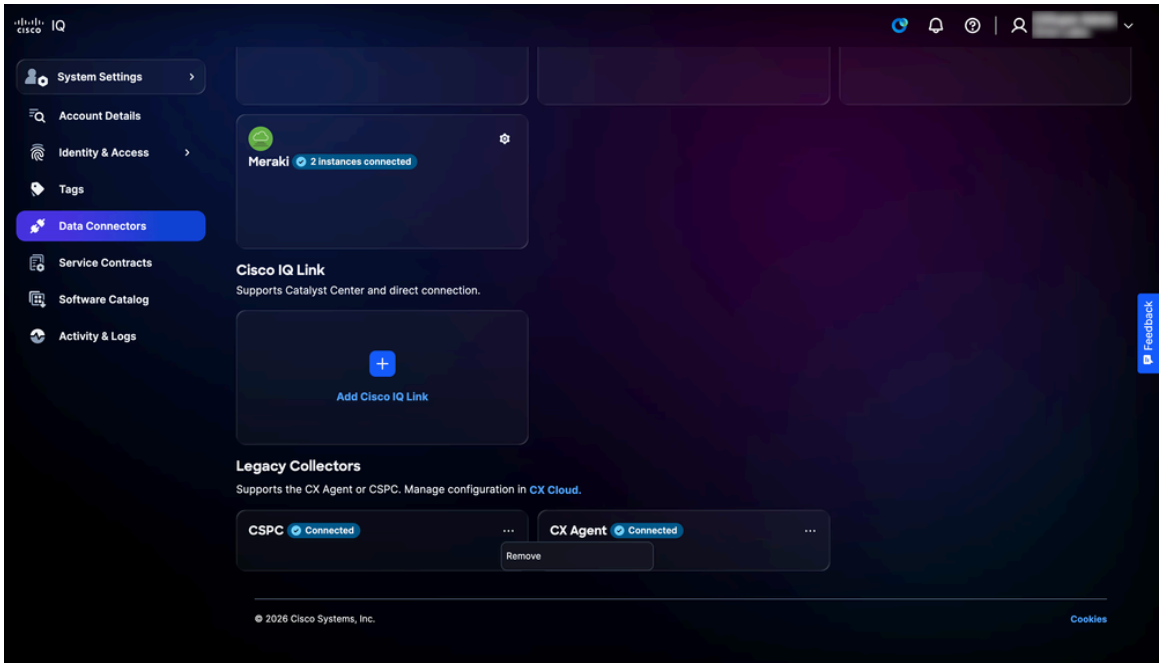
2. More Optionsアイコン> Remove Cisco IQ Linkの順に選択します。確認が表示されます。
3. Open caseをクリックしてサポートケースを開き、Cisco IQ Linkを削除します。

レガシコレクタの削除

注：従来のコレクタは、CX Cloudから移行されたアカウントにのみ表示されます。

接続されているレガシコネクタを削除するには、次の手順に従います。

1. データコネクタページで、目的のレガシーコレクタに移動します。



レガシコレクタのリンク解除

2. More Optionsアイコン> Removeの順に選択します。確認が表示されます。
3. Open caseをクリックしてサポートケースを開き、レガシーコレクタを削除します。

サービス契約

契約をリンクすることで、異なるチームメンバーに関連付けられた契約のデータを統合し、テレメトリ経由でインベントリに接続されていないデバイスを組み込むことができるため、サポート対象範囲の可視性が一元化され、更新に関する予想外の事態を回避できます。契約をリンクするには、サポートケースをオープンするために使用する契約番号が必要です。

注：契約番号のサポートについては、パートナーまたはシスコの営業担当者にお問い合わせください。

サービス契約の主な利点は次のとおりです。

- 組織のサポート対象範囲の一元化されたビューの作成
- 更新を数ヵ月前から行える、カスタマイズ可能なダッシュボード
- テレメトリまたは工アギャップ環境の一部に接続されていない資産を含めるためのインベントリの可視性の拡張

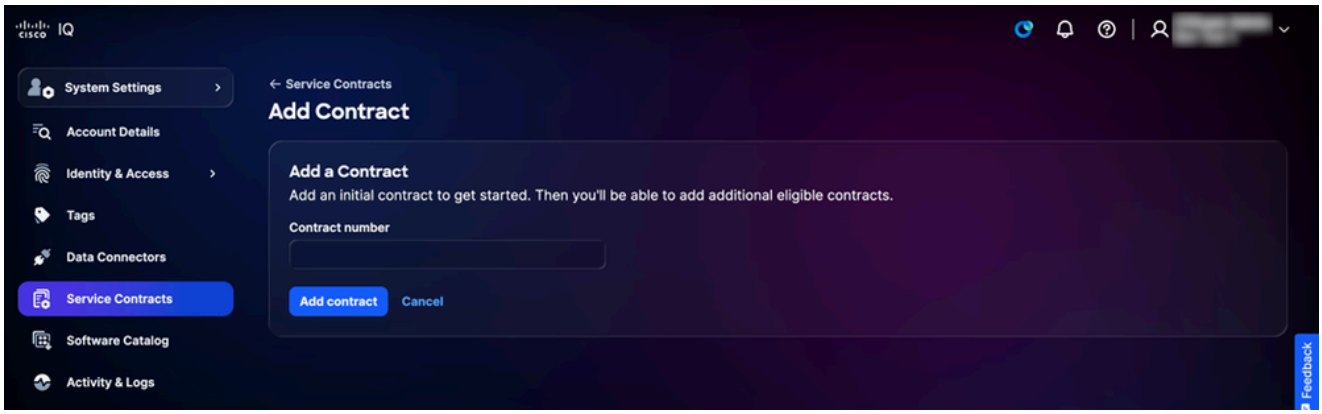
契約のリンク

Service Contractsページから契約をリンクするには、次の手順に従います。 

契約の追加

1. Add contractをクリックします。Add Contractページが表示されます。

注：最初の契約をアカウントに追加した後で、追加の契約を追加できます。



契約番号の入力

2. 契約番号を入力します。
3. Add contractをクリックします。契約がアカウントに追加されます。

ソフトウェアカタログ

ソフトウェアカタログには、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。

ソフトウェアカタログにアクセスするには、Home > System Settings > Software Catalogの順に選択します。Software Catalogページが表示されます。このページでは、使用可能なソフトウェアインスタンスがリンクコレクタの可用性カードとして表示されます。各リンクコレクタの可用性カードには、ソフトウェアインスタンスの名前、説明、パブリッシャ、およびバージョンが表示されます。

ソフトウェア・インスタンスの詳細の表示

ソフトウェアインスタンスのリリースノートを表示するには、Detailsをクリックします。ウィンドウが開き、インスタンスの最新のリリースノートが表示されます。以前のリリースノートを表示するには、ドロップダウンリストからリリースバージョンを選択します。

新しいソフトウェアインスタンスのパッケージのインストール

インストーラをダウンロードして新しいインスタンスを作成するには：

1. 目的のリンクコレクタ可用性カードから、ダウンロードオプション> インストールパッケージの順に選択します。「パッケージをインストール」ウィンドウが開きます。

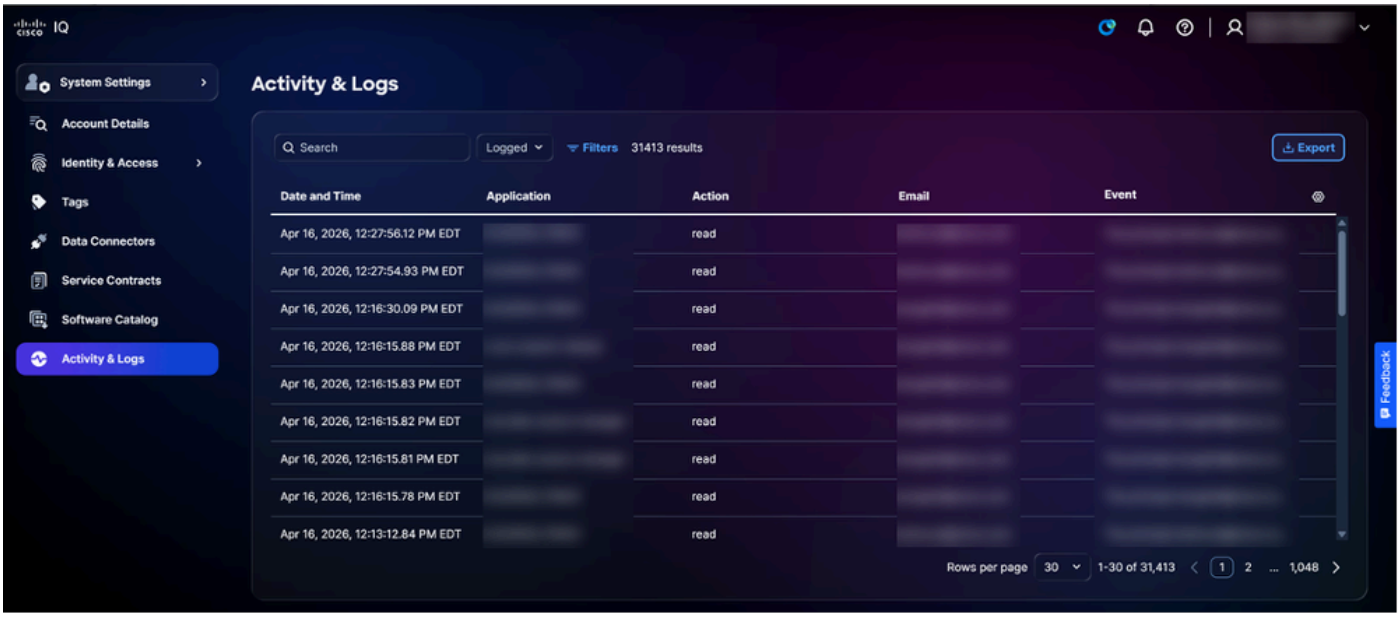
2. ドロップダウンリストから、次のハイパーバイザオプションのいずれかを選択します。
    - ESXi:VMware ESXi用
    - Hyper-V:Microsoft Hyper-V向け
    - KVM:Linuxカーネルベース仮想マシン(KVM)用
3. ドロップダウンリストからバージョンを選択します。
4. Downloadをクリックして、ファイルをローカルに保存します。

> 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。

5. ファイルをデータセンターに導入します。詳細については、『Cisco IQ Link Getting Started Guide』を参照してください。

アクティビティとログ

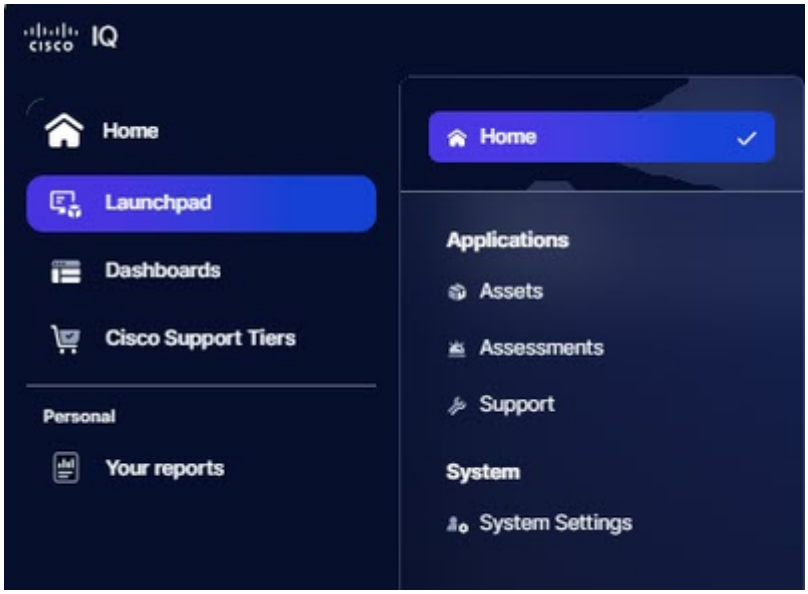
アクティビティとログサービスは、Cisco IQ全体にわたるすべてのユーザアクションとシステムイベントの追跡を一元化し、コンプライアンス、トラブルシューティング、モニタリングに対応します。認証イベント、許可決定、リソースアクセス、設定変更、および管理アクションに関する不変の監査レコードを、ユーザID、タイムスタンプ、送信元IPアドレス、および影響を受けるリソースを含む詳細なコンテキストとともにキャプチャします。アクティビティとログは、保存ポリシーを適用し、時間範囲検索、ユーザーベースのフィルタ、およびリソース固有のアクティビティの追跡をサポートすることで、監査イベントの柔軟なクエリとフィルタリングを可能にします。



アクティビティとログ

資産アプリケーション

Assetsアプリケーションは、シスコの資産に対する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の他のアプリケーション（評価アプリケーションなど）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。



ホームメニュー

コア概念

アセットアプリケーションは、次のコアコンセプト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。
- 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いて、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。

Assetsアプリケーションへのアクセス

Cisco IQでアセット管理機能にアクセスするには、Homeメニュー> Assetsの順に選択します。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。


Assets
Overview
Inventory
Service Contracts
End of Life
Overview
Product family
Last signal date
Data source
Asset location
Filters
Ask AI
Customize
Total Assets
168
Assets
Covered assets
58
Covered
97%
of all assets
Uncovered assets
2
Uncovered
3%
of all assets
Assets Covered by Service Contracts
View details
Number of Assets
Support Tier
Basic
Standard
Signature
No support
8
37
123
Last Date of Support Snapshot
View details
Number of Assets
Past milestone
Within 12 months
Within 12-24 mon...
After 24 months
37
8
9
31
Key Asset Metrics
Assets with telemetry
168
with telemetry
100%
of all assets
Assets without telemetry
0
without telemetry
0%
of all assets
Assets With Critical or High Security Advisories
View details
85%
Of the 168 assets with telemetry enabled, 142 have critical or high Security Advisories
Assets by Criticality
View details
18 assets can be evaluated for criticality.
Number of Assets
Criticality
High
Critical
10
8
Asset Breakdown
Top 5 Product Families
View details
Cisco Catalyst 9...
Cisco 4000 Serie...
Cisco Catalyst 9...
Cisco Catalyst 9...
Cisco Catalyst 9...
30
30
16
13
7
Number of Assets
Top 5 Install-at Locations
View details
SANTA CLARA,CA,U...
60
Number of Assets
Top 5 Software Versions
View details
IOS-XE 16.12.4
IOS-XE 16.6.6
IOS-XE 16.6.4
IOS-XE 16.8.1a
IOS-XE 16.6.2
21
11
10
8
8
Number of Assets
Top 5 Asset Roles
View details
18 assets can be evaluated for roles.
Access
Wireless LAN Con...
Core
8
5
5
Number of Assets
© 2026 Cisco Systems, Inc.
Cookies

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
- 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
- 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
    - テレメトリ付き資産：テレメトリが有効な資産の総数と割合
    - テレメトリのない資産：テレメトリが有効になっていない資産の総数と割合
    - 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：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。

注：使用できるフィルタは、ロールと権限によって異なります。

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アプリケーションの新機能である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、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。

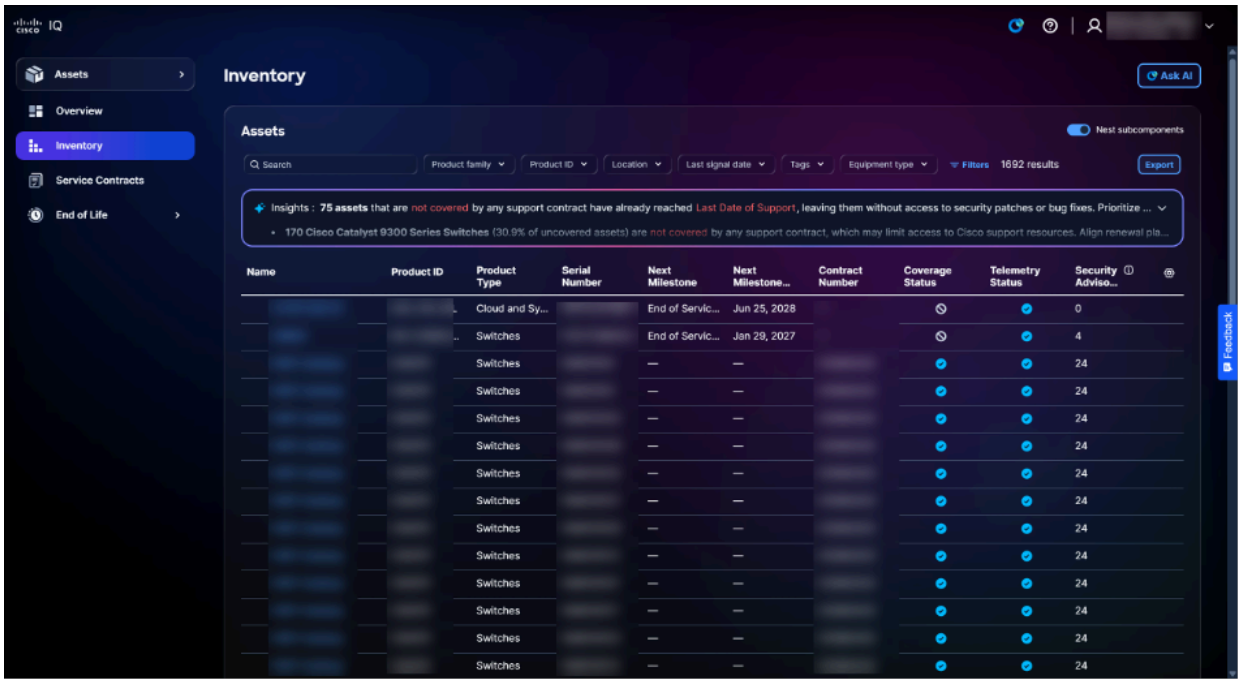
注：Asset Criticality Insightsは、アクティブなテレメトリ接続があるStandardまたはSignatureレベルの資産でのみ利用できます。ダッシュボード内でこれらのインサイトを読み込むために、資産が構成要件を満たしていることを確認してください。

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ー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。

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。

注：使用できるフィルタは、ロールと権限によって異なります。

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、『共通アプリケーション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

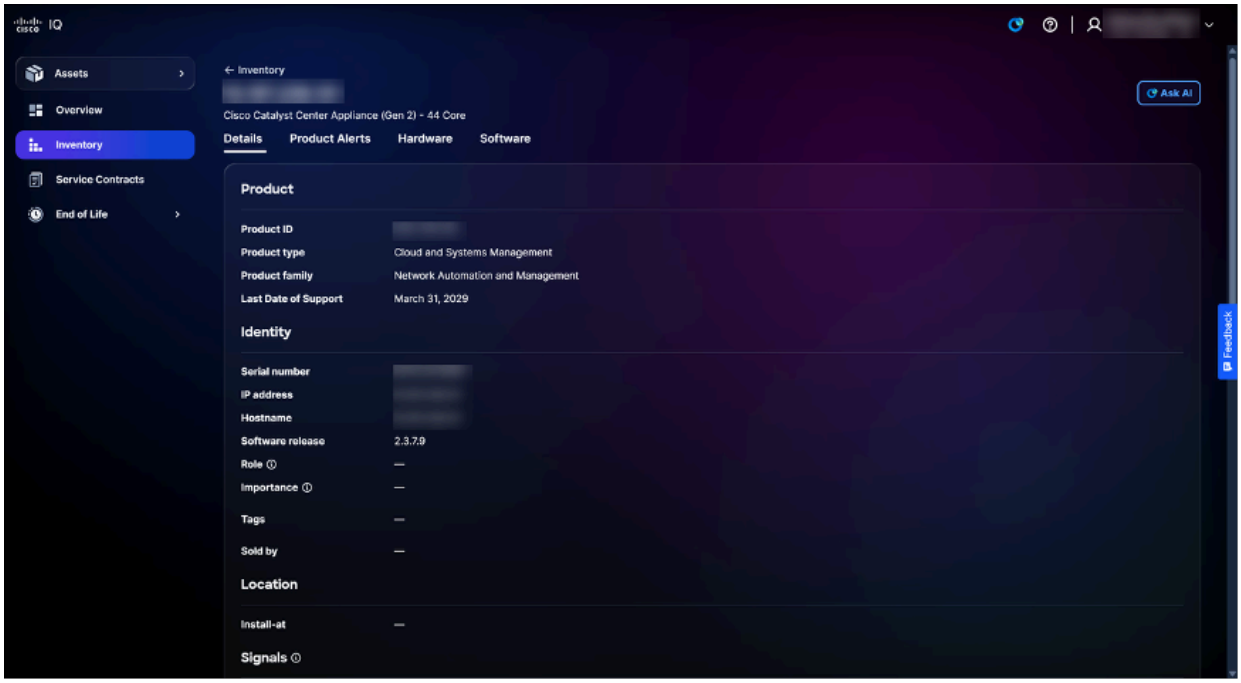
Exportをクリックして、フィルタリングされたインベントリリストを.xlsまたは.csv形式で保存し

ます。詳細は、『共通アプリケーション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。



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、キーと値のペアのことで、たとえばEnvironment:ProdやLabel:Campusのように定義します。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。

資産タグの作成および削除

アセットタグの作成と削除の詳細については、システム設定の「タグ」を参照してください。

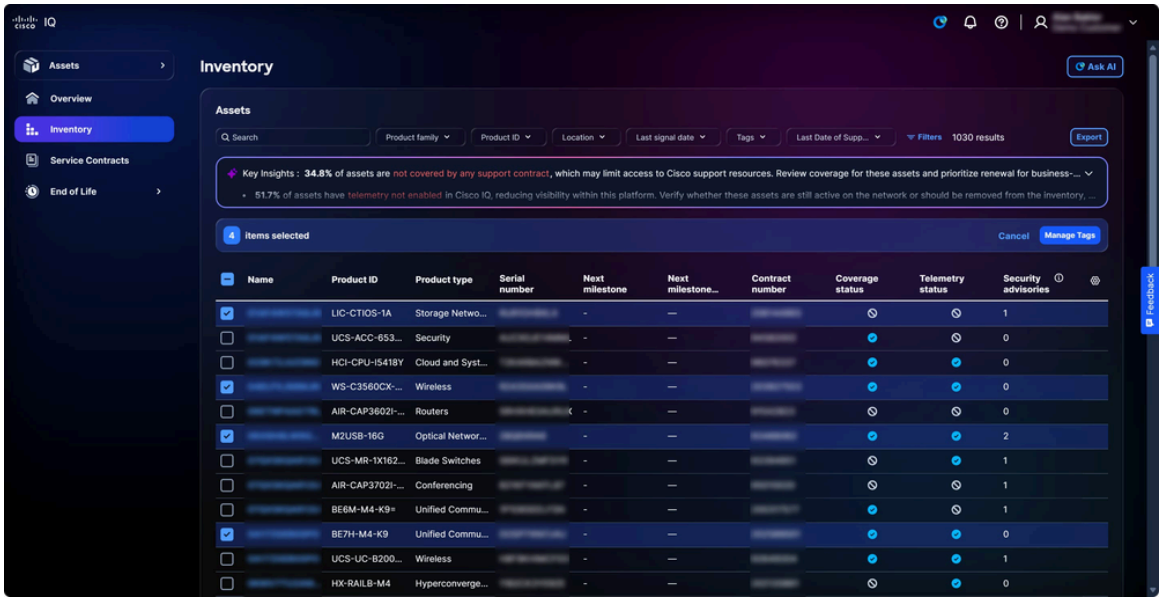
注：タグを作成および削除できるのは、アカウント管理者だけです。

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：

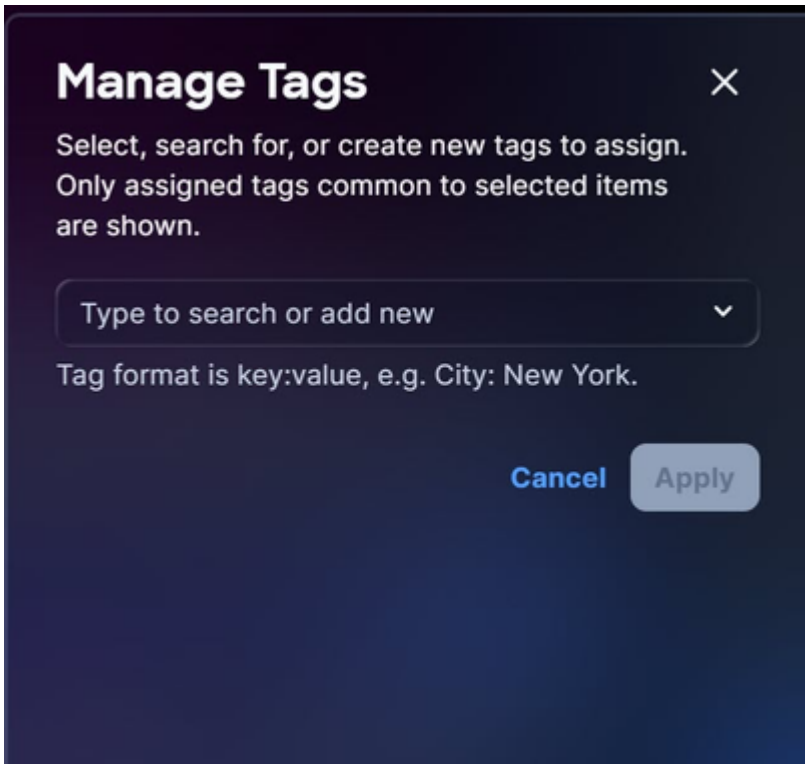
1. Assets > Inventoryの順に移動します。



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。

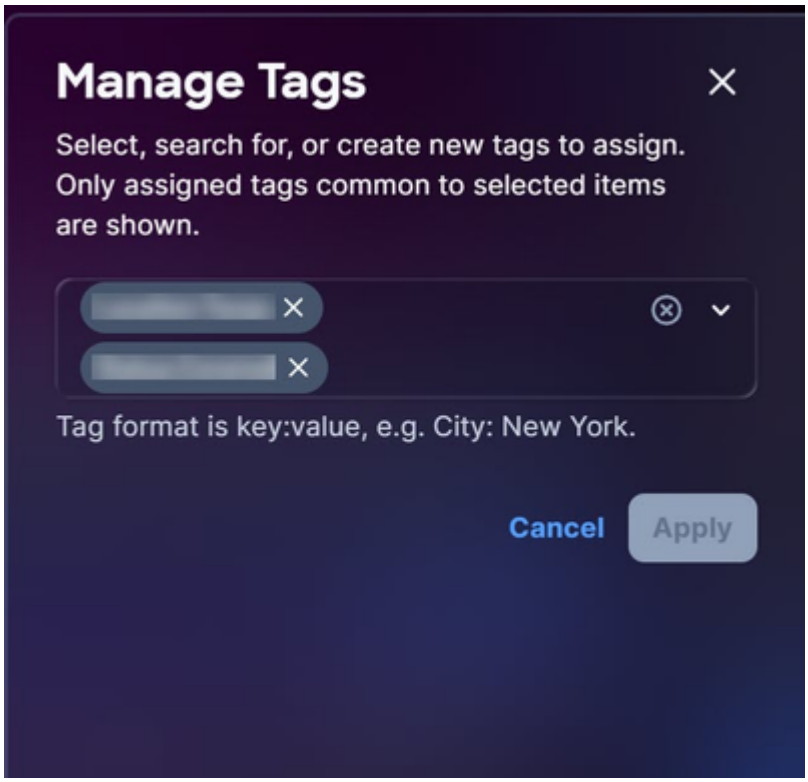
> 注：タグはkey:value形式です(例：City:NYC)。

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。Manageタグウィンドウが開きます。



タグの削除

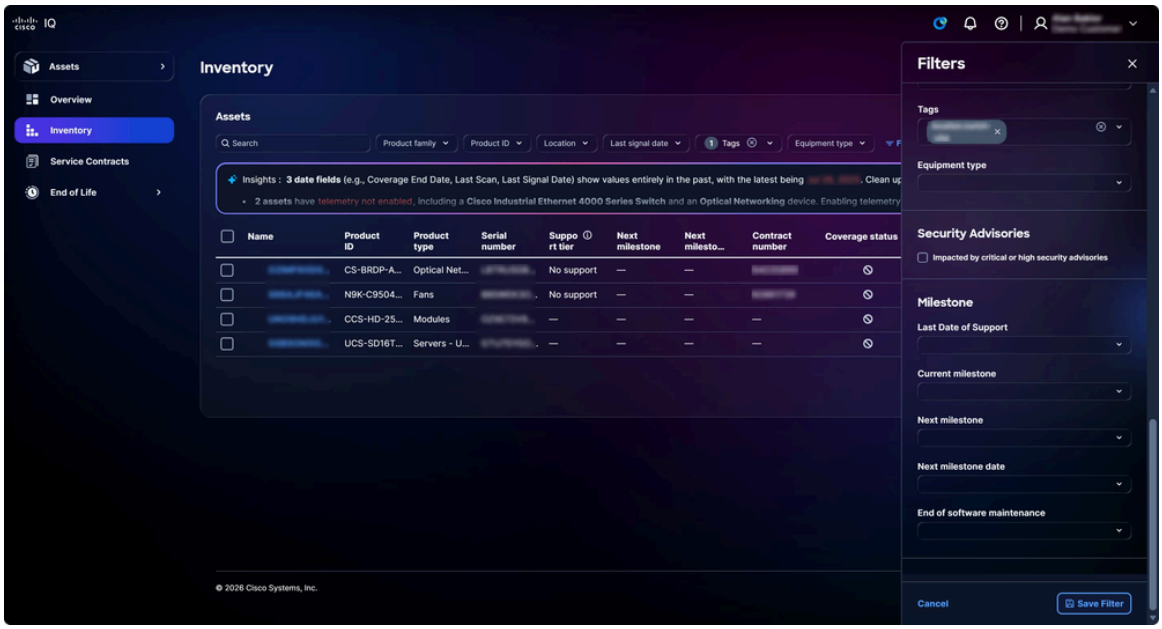
4. 任意のタグのXをクリックして、選択から削除します。
5. [APPLY] をクリックします。

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。

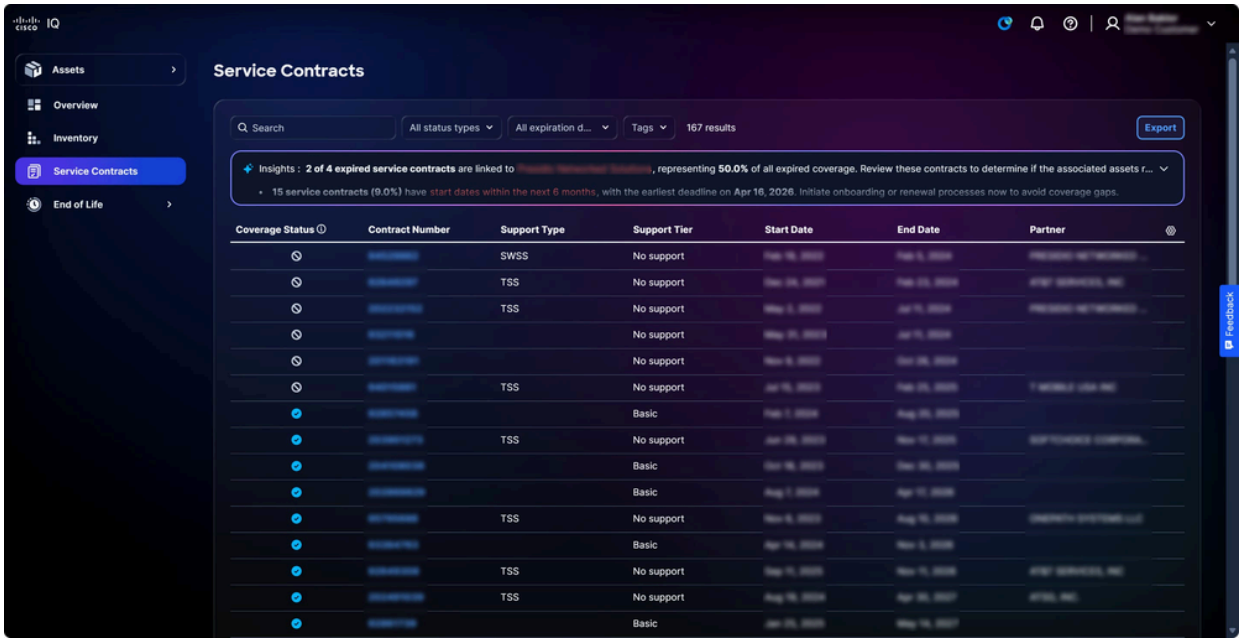


タグをフィルタとして使用

3. 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

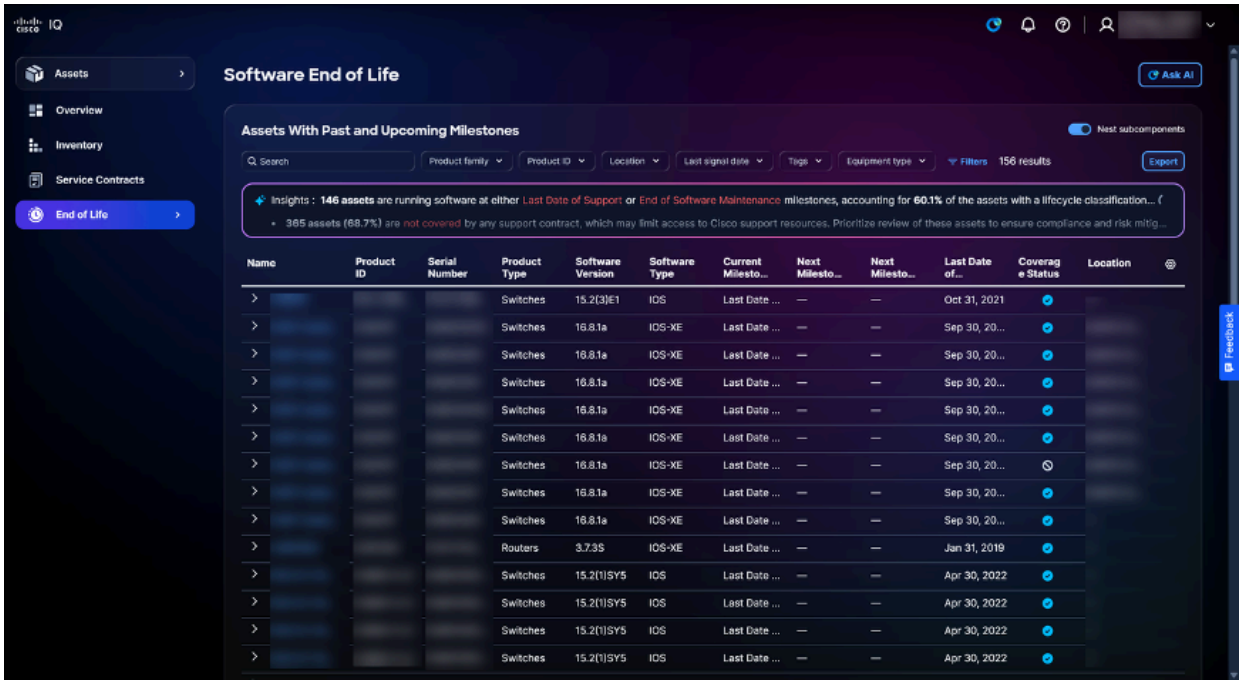
ドロップダウンリストからフィルタを選択して、リストビューをフィルタリングできます。Searchフィールドに契約番号を入力して、サービス契約を検索することもできます。

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、『共通アプリケーション機能での情報のエクスポート』を参照してください。

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ページでアセットをクリックすると、Inventoryページの関連するアセット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、『共通アプリケーション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、『共通アプリケーション機能での情報のエクスポート』を参照してください。

評価アプリケーション

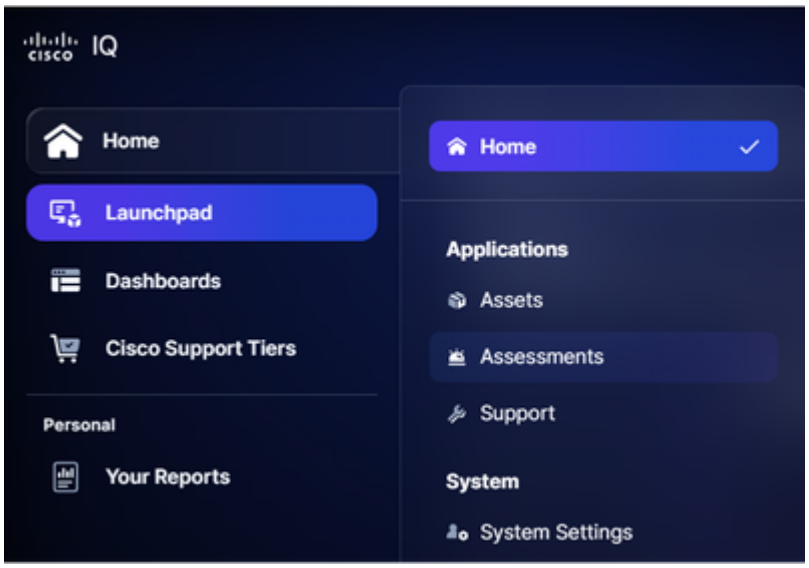
評価アプリケーションは、評価フレームワークを提供します。これにより、ユーザは、セキュリティ、安定性、キャパシティ、コンプライアンス、およびエージングに関連するリスクをプロアクティブに調査して軽減し、ネットワークの安全性、安定性、および信頼性を維持できます。

コア概念

評価アプリケーションは、次の基本概念に基づいて構築されています。

- 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

評価アプリケーションへのアクセス



評価

Cisco IQ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、Homeメニュー> Assessmentsの順に選択します。「評価の概要」ページが表示されます。

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

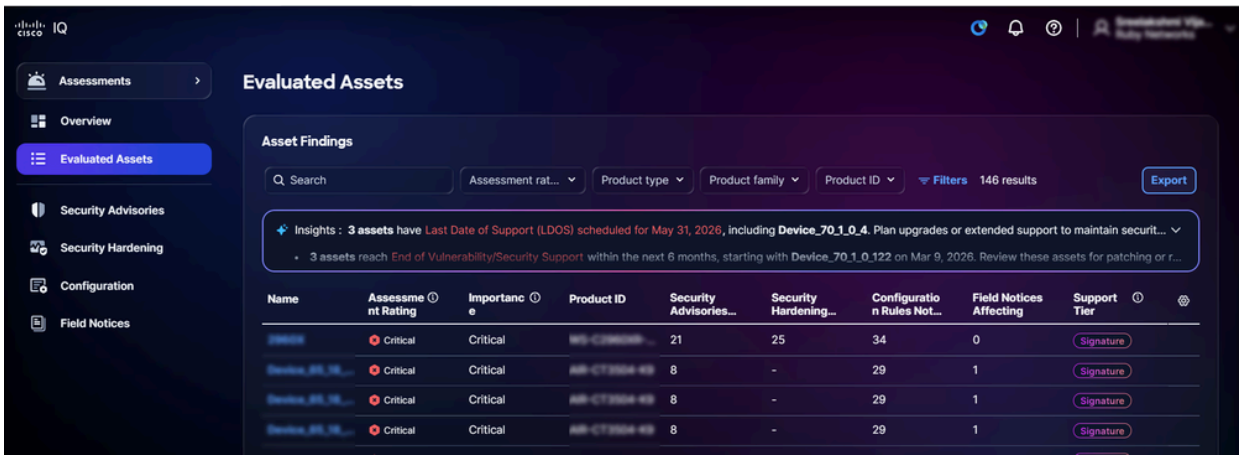
ダッシュボードには、次の情報が表示されます。

- 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。
- 合格しなかった資産に関するセキュリティ強化ルール：セキュリティ強化ルールに合格しなかった資産を、重大度（高、中、低、情報）別に分類して表示します
- 合格しなかった資産の構成ルール：構成コンプライアンスルールに失敗した資産を、重大、高、中、低、および情報の重大度別に分類して表示します
- Field Notice Assessments:Field Noticeの評価を、Critical、High、Medium、Noの各重大度に分類して表示します。

注：お客様は、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など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。



資産別の結果

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。

注：使用できるフィルタは、ロールと権限によって異なります。

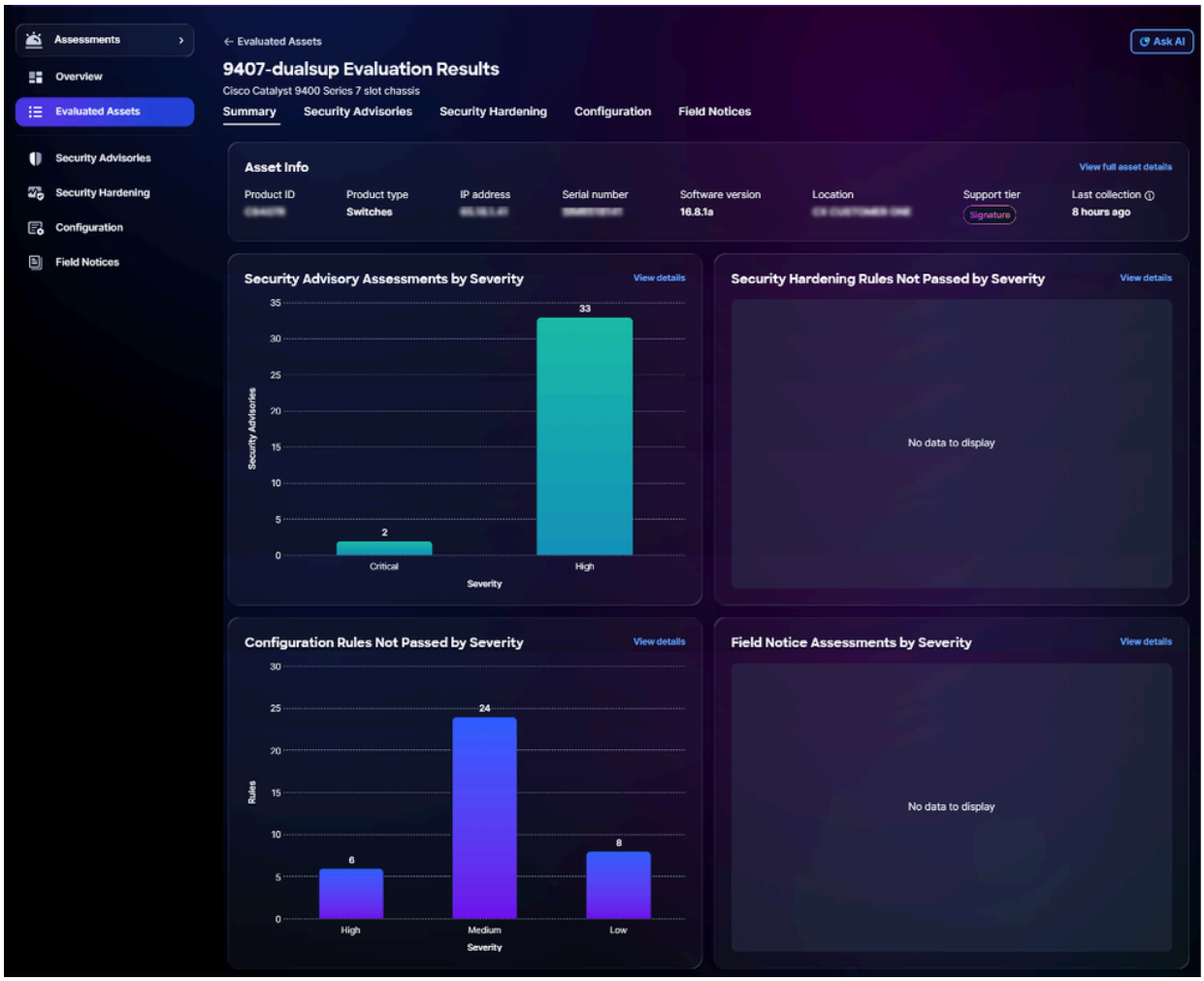
アセット別の結果のエクスポート

Finding by Assetリストビューをエクスポートするには、Exportをクリックします。エクスポートの詳細については、「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

資産別結果の詳細を表示するには、資産をクリックします。次のタブには、選択したアセットの詳細が表示されます。

- サマリー: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、およびField Noticeを含む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
- 設定:設定に失敗したアセットのベストプラクティスルールのリストを提供します。
- 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

タイルのView Detailsをクリックすると、ページはアプリケーション内の該当する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。

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フィルタリングビューの検索

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：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。

注：使用できるフィルタは、ロールと権限によって異なります。

注：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。エクスポートの詳細については、「情報のエクスポート」を参照してください。

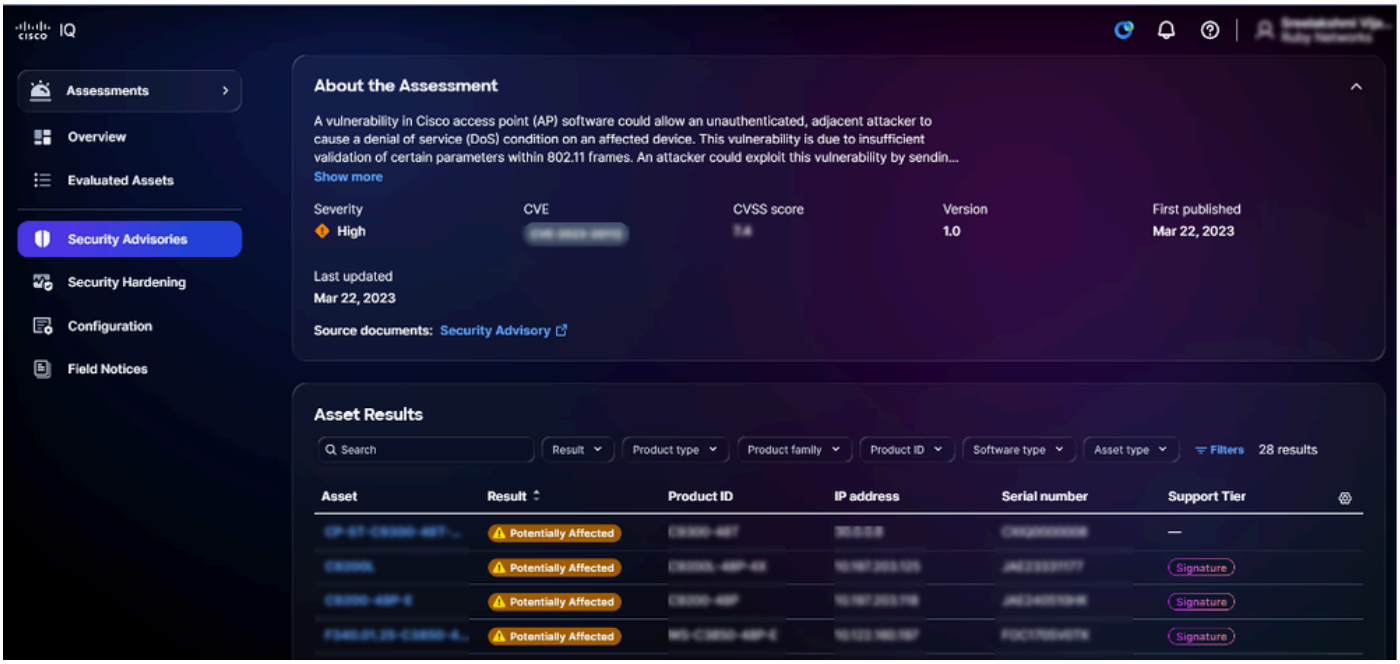
セキュリティアドバイザリアセスメントの詳細の表示

アセスメントの詳細を表示するには、アドバイザリをクリックします。この詳細ページには、

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。



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

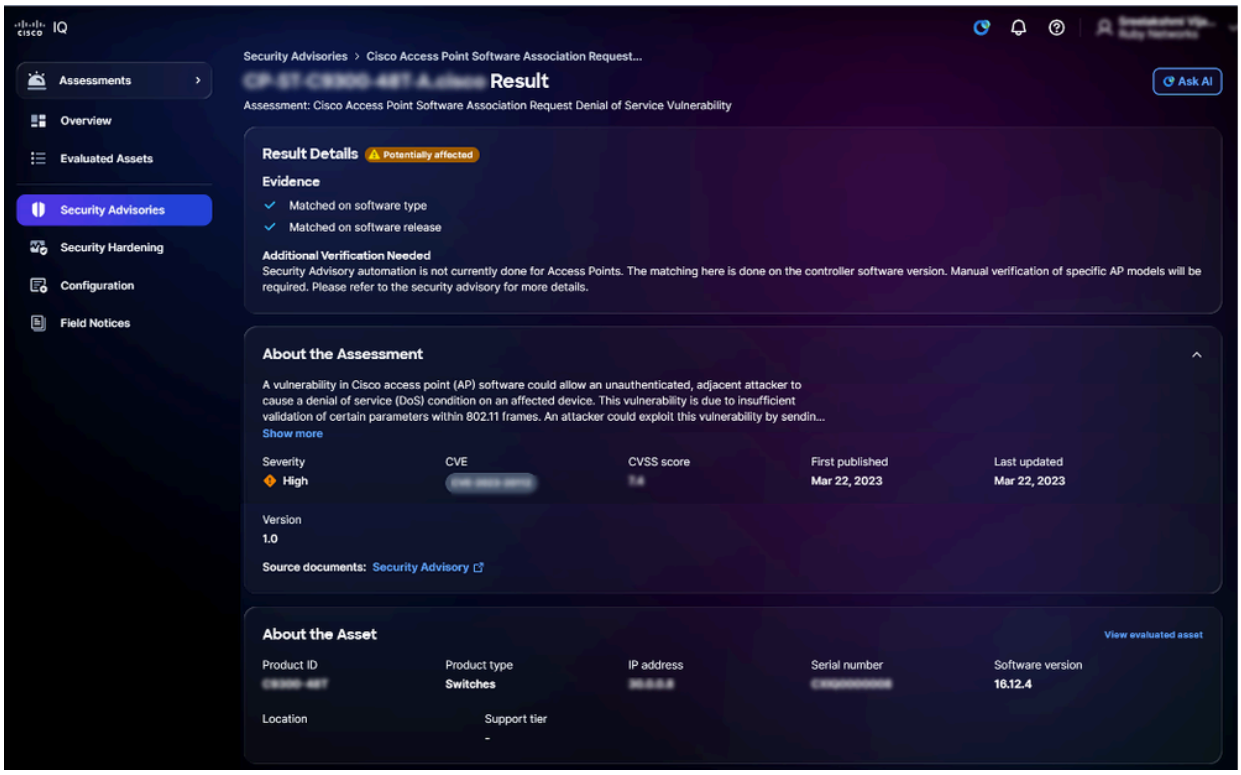
リストビューをフィルタリングするには、ドロップダウンリストからフィルタを選択するか、Filtersをクリックして、使用可能なフィルタのリストからオプションを選択します。Searchフィールドにアセット名を入力して、アセットを検索することもできます。

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。

注：使用できるフィルタは、ロールと権限によって異なります。

資産査定結果の表示

評価結果の詳細を表示するには、「資産評価結果」テーブルの資産をクリックします。評価結果の詳細ページが表示されます。



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。エクスポートの詳細については、「情報のエクスポート」を参照してください。

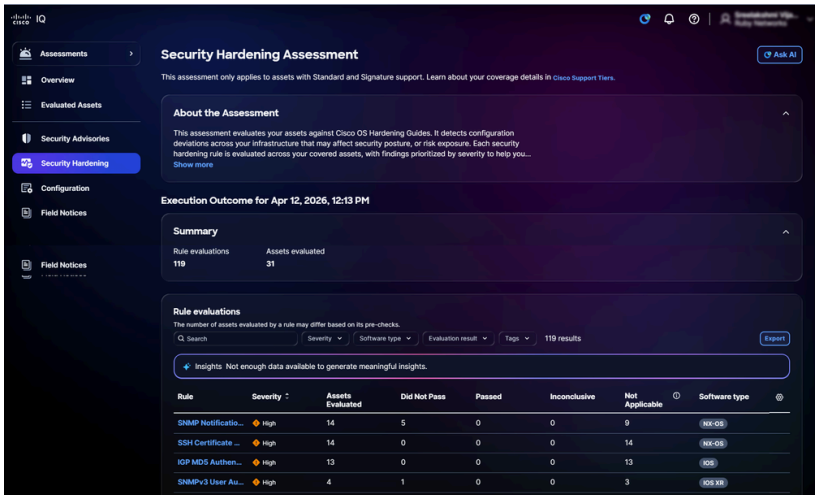
セキュリティの強化

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、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ベストプラクティスとの一貫性のある整合性を維持できます。コンプライアンスモニタリングを一元化し、強化プロセスを簡素化することで、アプリケーションはセキュリティ管理を事後対応型のタスクから予防的なデータ駆動型の戦略に変え、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：セキュリティ強化評価は、標準またはシグニチャのサポート階層を持つ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

セキュリティの強化の詳細を表示するには、評価をクリックします。「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。



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 Summary:ルール評価および含まれる資産の合計数を含む、資産評価結果の要約を提供します。
- 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

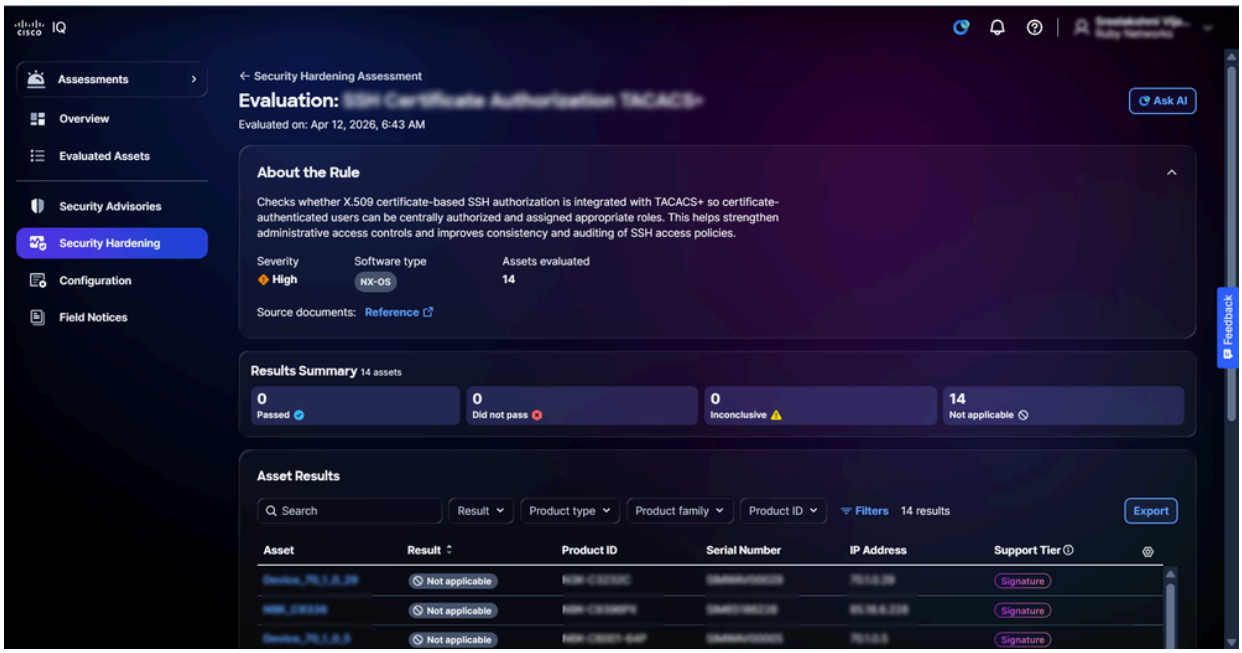
リストビューをフィルタリングするには、ドロップダウンリストからフィルタを選択するか、Filtersをクリックして、使用可能なフィルタのリストからオプションを選択します。Searchフィールドにルール名を入力して、ルールを検索することもできます。

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。

注：使用できるフィルタは、ロールと権限によって異なります。

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。



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。
- アセットの結果：アセットのリストが表示され、アセット、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が示されます。

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。

注：使用できるフィルタは、ロールと権限によって異なります。

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。エクスポートの詳細については、「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。

注：使用できるフィルタは、ロールと権限によって異なります。

セキュリティ強化の資産結果の表示

資産結果の詳細を表示するには、「資産結果」で資産をクリックします。資産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。

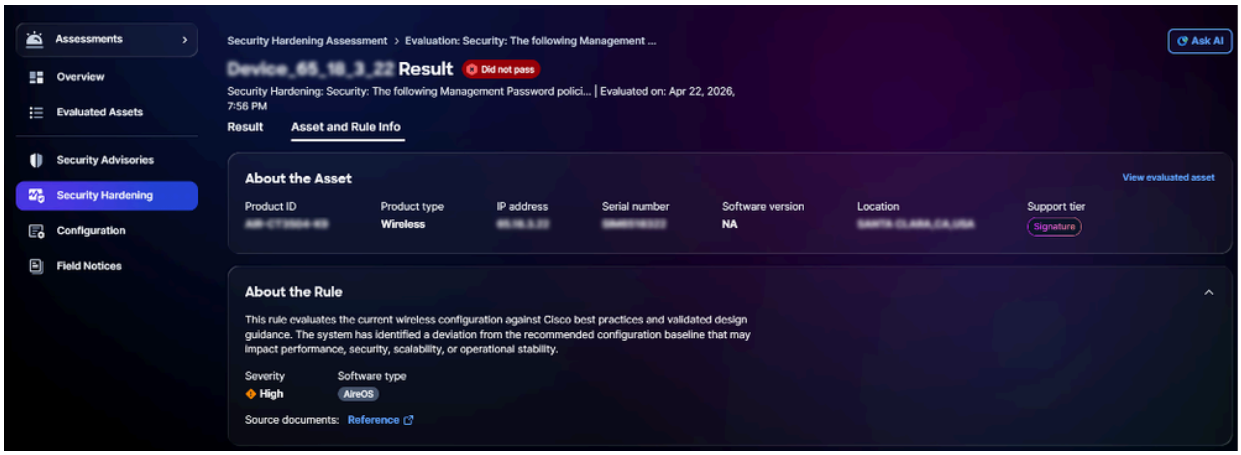
- 標準層
    - 詳細の検索：評価中に特定された構成の逸脱に関する情報と、証拠ログを提供します。
    - 推奨事項：結果に対処し、設定の一貫性を確保するためのガイダンスを提供します。

セキュリティ強化のシグニチャ層

- 署名階層
  - 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：設定の一貫性を確保するためのコードスニペットとともに、デバイスレベルの実用的な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。



資産とルールの情報

- 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

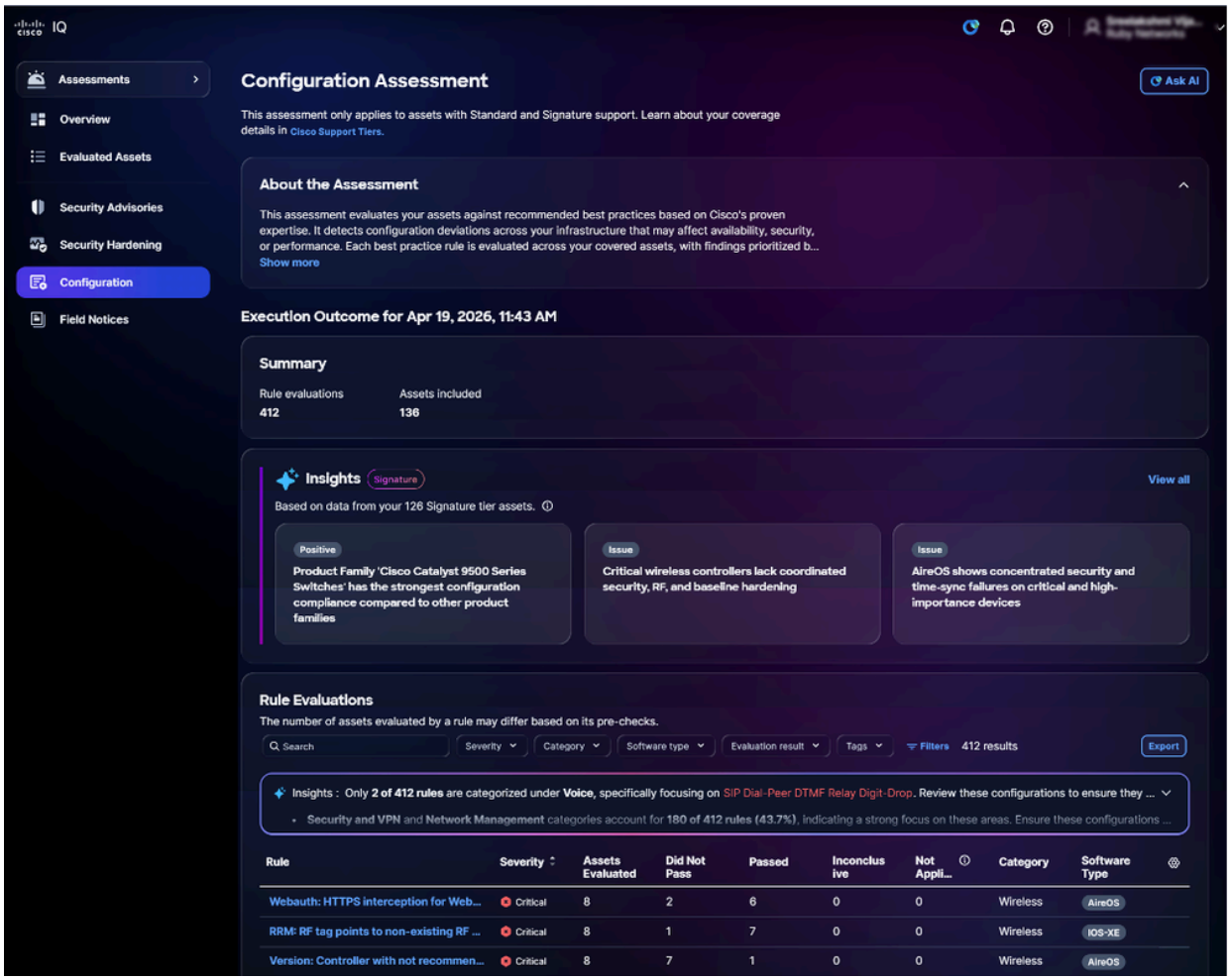
コンフィギュレーション

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、対象の資産全体にわたって評価され、結果は重大度に応じて優先順位が付けられ、設定の一貫性、復元力の強化、運用リスクの軽減が確実に行われます。

注：設定評価は、サポート階層がStandardまたはSignatureの資産に対してのみ利用できます。

構成評価の表示

設定に関するその他の詳細を表示するには、アセスメントをクリックします。Configuration Assessmentページには、次の情報が表示されます。

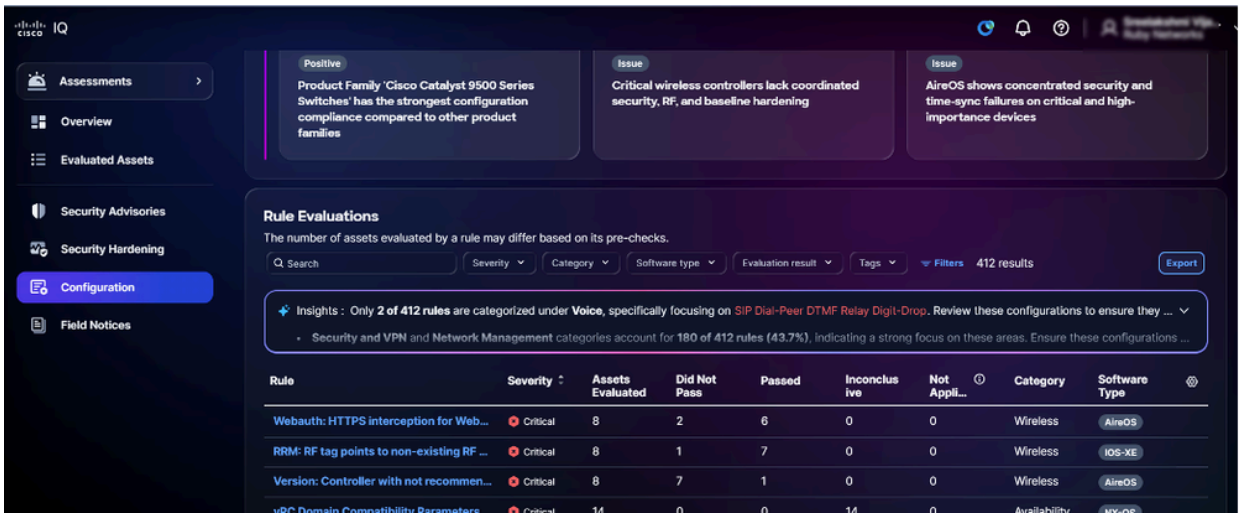


構成の評価

- 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指定します
- ソフトウェアタイプ：ルールを適用す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



ルールの評価

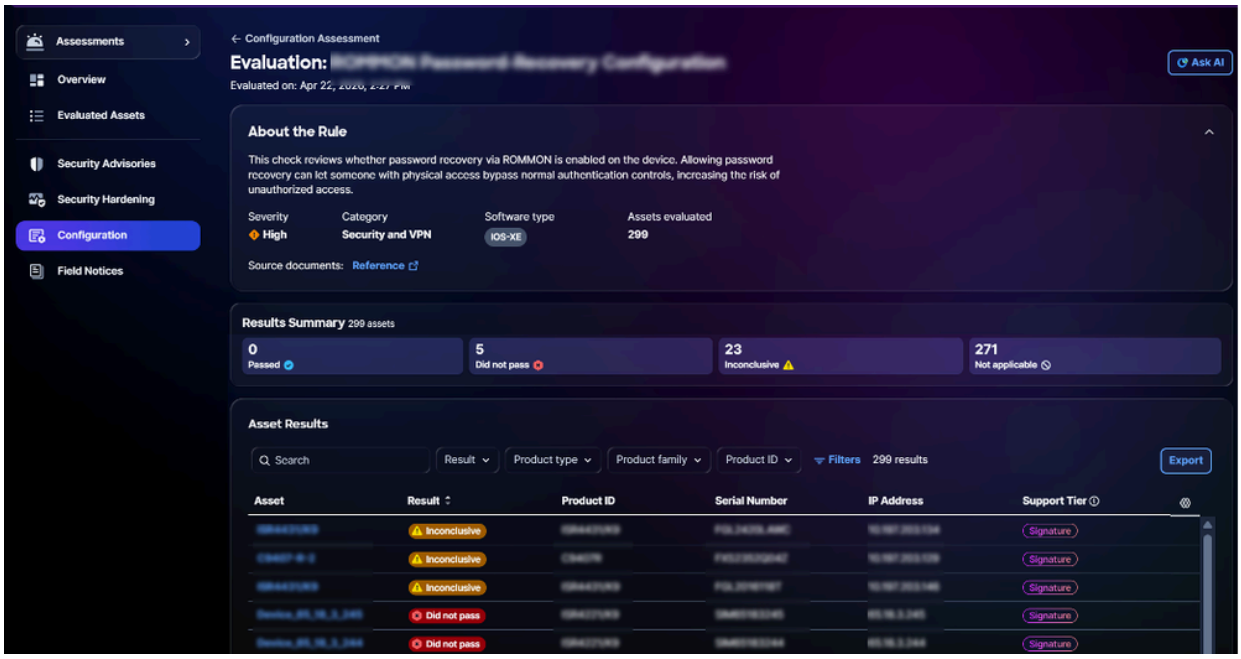
リストビューをフィルタリングするには、ドロップダウンリストからフィルタを選択するか、Filtersをクリックして、使用可能なフィルタのリストからオプションを選択します。Searchフィールドにルール名を入力して、ルールを検索することもできます。

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。

注：使用できるフィルタは、ロールと権限によって異なります。

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。



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。

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。エクスポートの詳細については、「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。

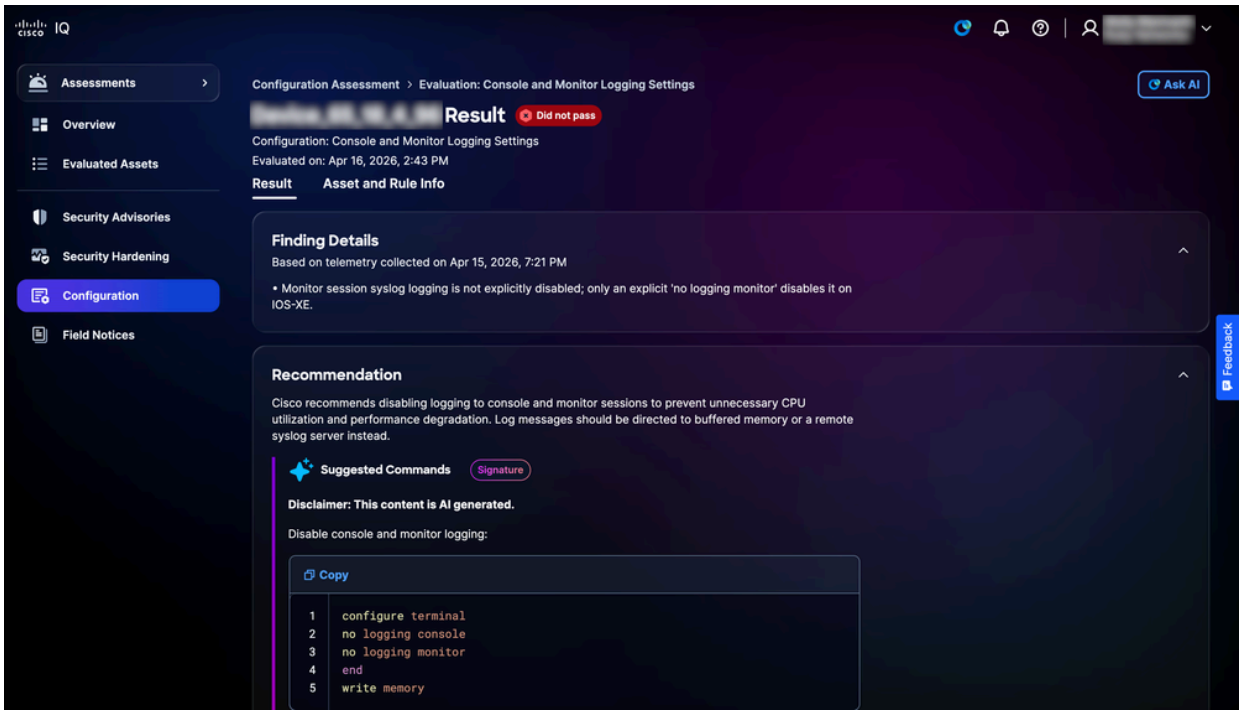
注：使用できるフィルタは、ロールと権限によって異なります。

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。

資産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。

- 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。

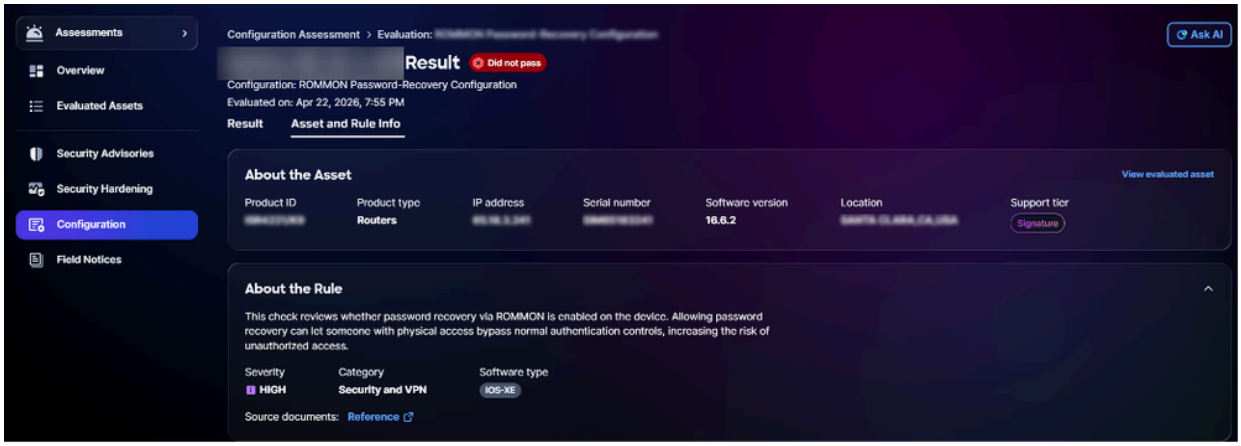


構成シグネチャ層

- 署名階層
  - 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に、コードスニペットを使用してデバイスレベルの実用的な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。



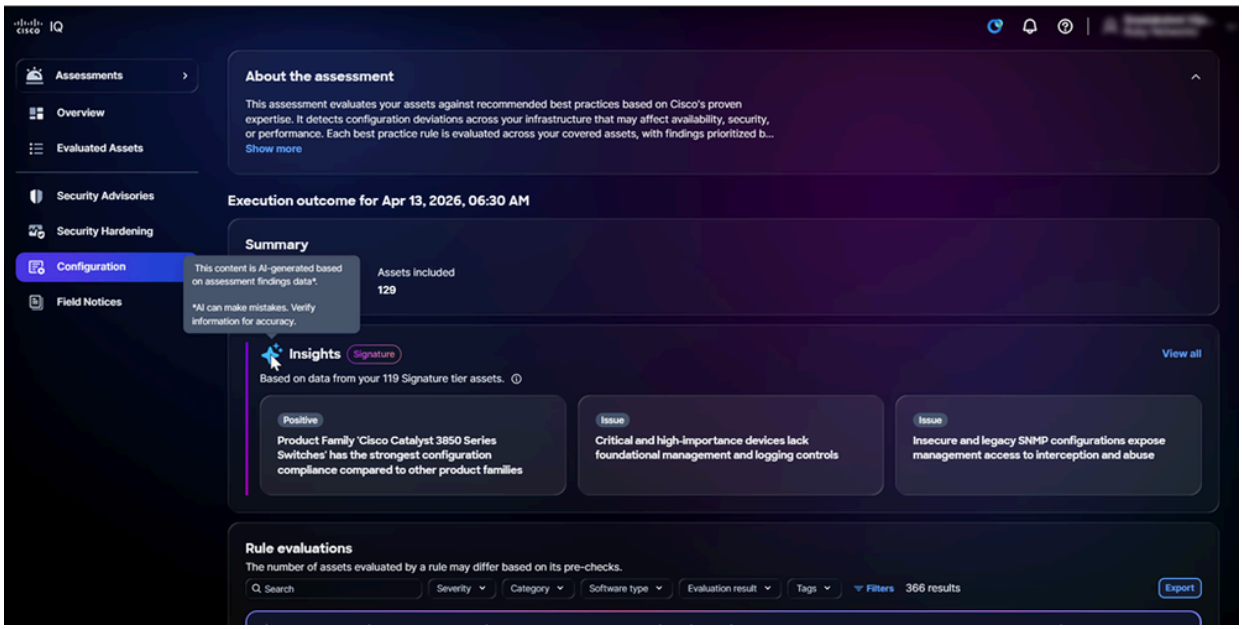
資産とルールの情報

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

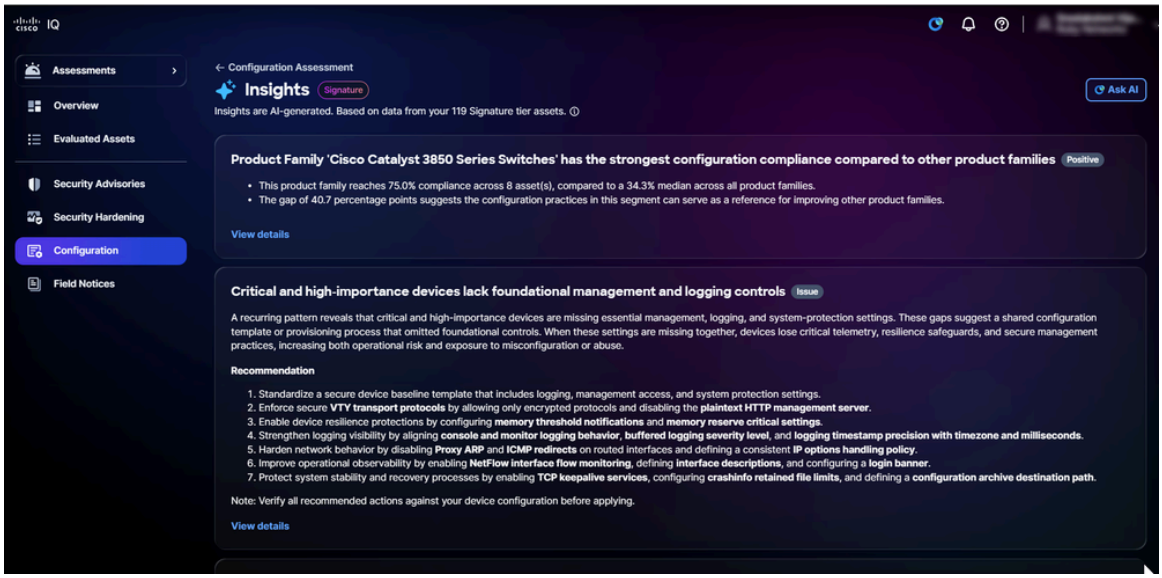
インサイトはAIによって生成され、アセスメントデータを優先順位付けされたキーカードに統合するインテリジェントなダッシュボードとして機能し、複数の結果にわたって重要な構成の違いを強調します。これらの緊急分野に焦点を当てることで、最も影響の大きいインフラストラクチャリスクに効率的に対処できます。また、ベストプラクティスに従ってインフラストラクチャが実行されている領域を特定することで、長所を強調します。



考察

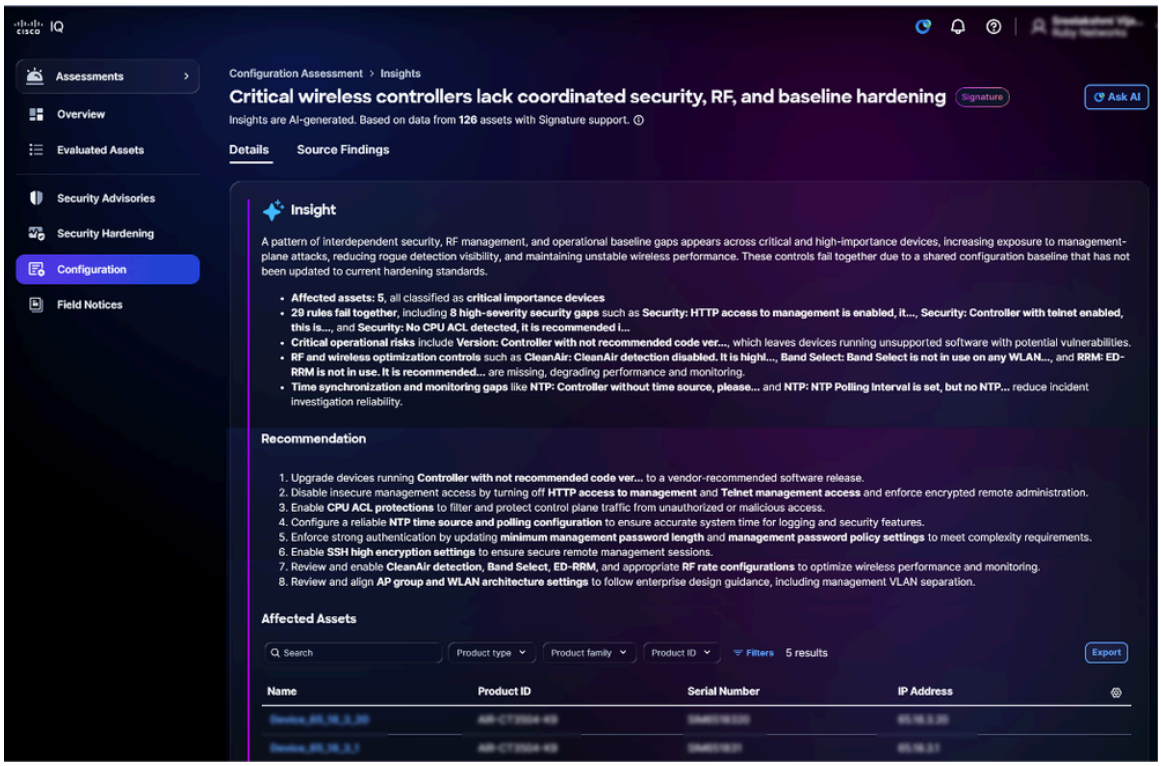
インサイトの詳細を表示するには：

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

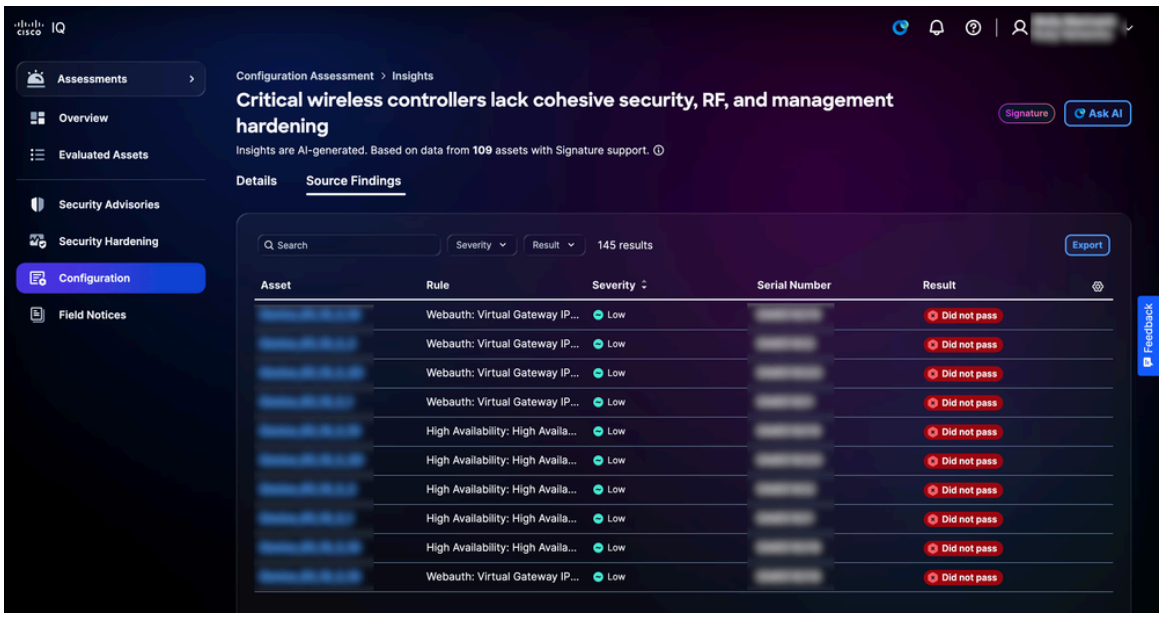
2. View detailsをクリックします。「インサイト」詳細ページが表示され、次の情報が表示されます。任意のカードをクリックして詳細ページを開くこともできます。



インサイトの詳細

- 洞察：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提供します。
- 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。



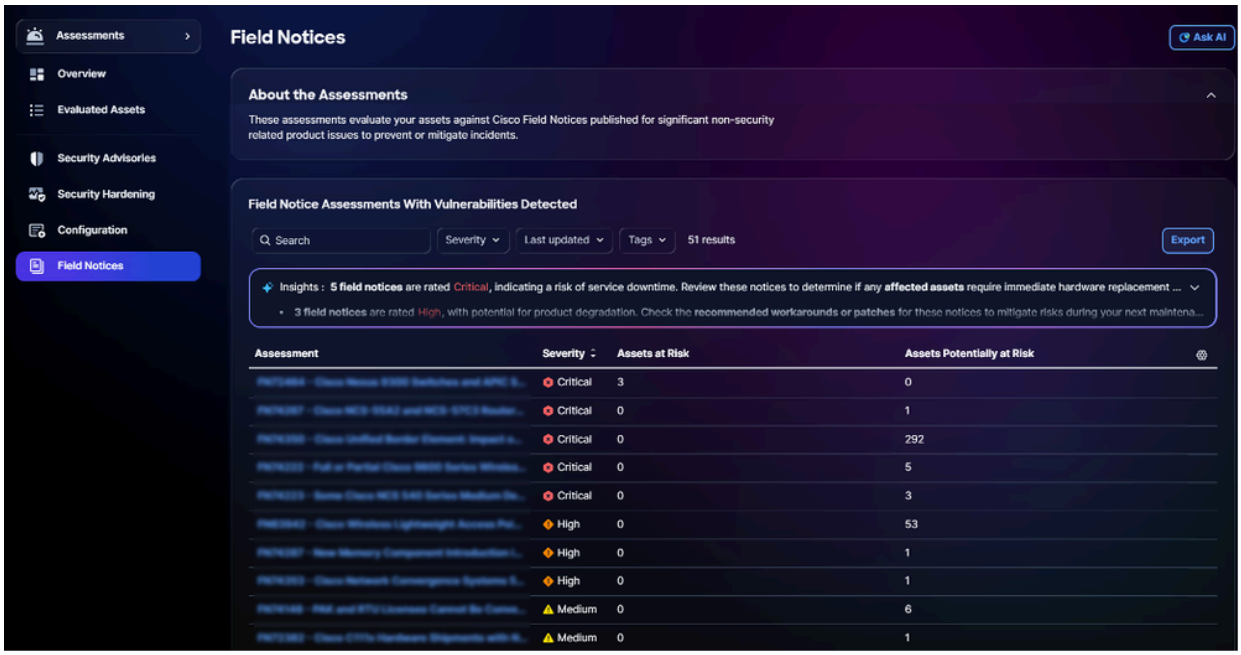
ソースの結果

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の問題を特定し、その影響の重大度と重要度に基づいてそれらを分類することで、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

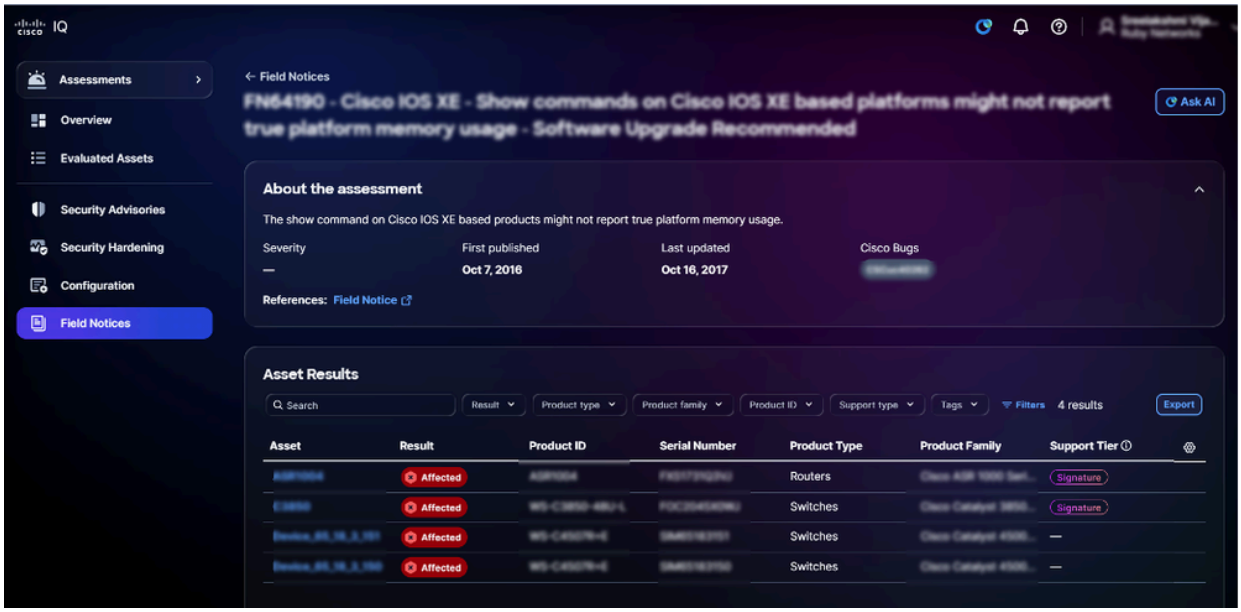
Field Noticeのビューの検索とフィルタリング

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。次のアセットアセスメント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 Assessments with Vulnerabilities Detected：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。

注：使用できるフィルタは、ロールと権限によって異なります。

Field Noticeのアセスメント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。エクスポートの詳細については、「情報のエクスポート」を参照してください。

Field Noticeのアセスメント資産結果の表示

アセスメント資産結果の詳細を表示するには、資産評価結果から資産をクリックします。アセスメント資産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。

サポートアプリケーション

サポートアプリケーションでは、カスタマーサポートケースの統合ビューが提供されます。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のサポートアプリケーションにアクセスするには、ホーム > サポートの順に選択します。Support Overviewページが表示されます。

サポートの概要

サポートの概要

サポートの概要ページは、次の情報を含むインタラクティブなグラフのダッシュボードです。

- 重大度別オープン・ケース:S1からS4までの重大度別に分類された過去90日間のオープン・ケースすべて
- ケース・ステータス別オープン・ケース：過去90日間にオープンされたすべてのケースが、ケース・ステータス別に分類されます。
- ステータス別RMA：ステータス別に分類された過去90日間のすべてのRMA
- 重大度別クローズ・ケース：重大度別に分類された過去90日間のクローズ・ケースの合計数

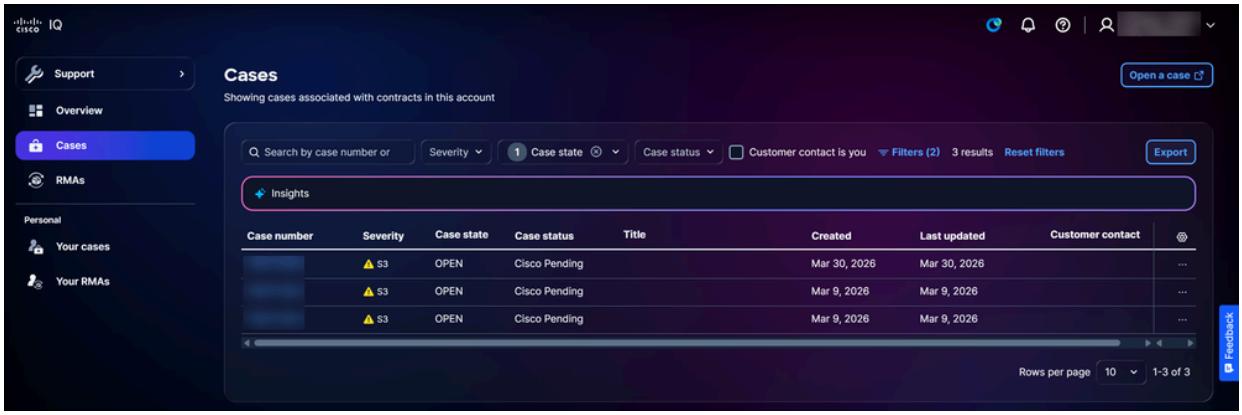
サポート案件の詳細の表示

View detailsをクリックすると、ページがアカウントのCasesページにリダイレクトされます。概要ページのグラフのバーをクリックすると、該当するフィルタが適用されているアカウントのケースページにページがリダイレクトされます。たとえば、重大度別オープンケースのグラフでS1重大度バーをクリックすると、アカウントのケースページにリダイレクトされ、ケースステータスが「オープン」、重大度が「S1」に設定されます。詳細は、『サービスリクエスト』を参照してください。

ケース

アカウントケース

左側のパネルでCasesをクリックして、Casesページに移動します。



ケース

Casesページには、Cisco IQアカウントの契約に関連するすべてのケースをまとめたリストが表

示されます。このリストに表示されるカラムを設定するには、Settingsアイコンをクリックして、必要なカラムのチェックボックスをオンにし、Applyをクリックします。Case number、Severity、Case state、Case status、Title、およびCreatedの各列は常に表示され、選択解除することはできません。

利用可能なアクション

Casesページでは、次のアクションを実行できます。

- ケースを開く:Open a caseをクリックしてSCMをクロス起動し、ケースを作成します。
- データのエクスポート：ダッシュボードに現在表示されているすべてのデータをCSVファイルとしてダウンロードするには、エクスポートをクリックします
- ケース詳細の表示：ケース番号またはテーブル行をクリックして、ケースの詳細ビューを開きます(詳細については、「ケースの詳細ビュー」を参照してください)。
- ケースのクローズ：オープン· ケースの「その他オプション」アイコン> 「ケースのクローズ」を選択して「ケースのクローズ」ウィンドウをオープンします。このウィンドウで、クローズする理由を指定してケースをクローズできます
- ケースの再オープン：クローズしたケースの「その他オプション」アイコン> 「ケースの再オープン」を選択して「ケースの再オープン」ウィンドウをオープンします。このウィンドウで、再オープンの理由を指定してケースをオープンできます

注：終了した症例は、終了から14日以内に再開できる。

ケースのビューのフィルタ

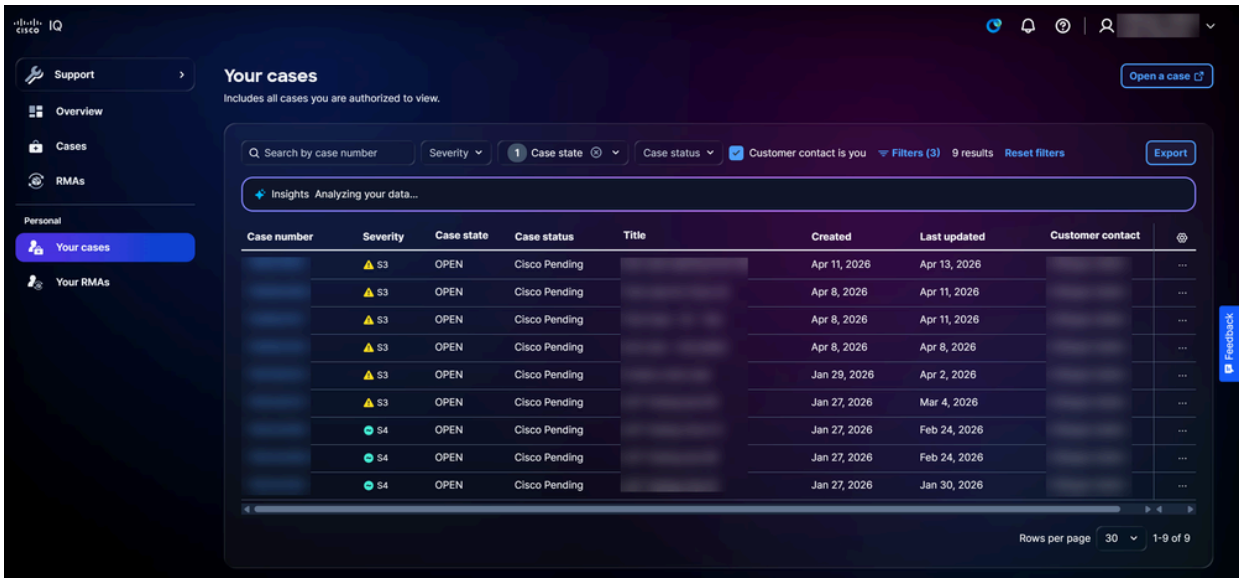
ドロップダウンリストからフィルタを選択するか、[お客様の連絡先]チェックボックスをオンにすることで、リストビューにフィルタを適用できます。必要に応じて、Filtersをクリックし、使用可能なフィルタオプションのリストから選択します。フィルタと選択は、セッションとログインを通じて保持され、ダッシュボードをパーソナライズします。適用されるデフォルトのフィルタは次のとおりです。

- ケースの状態：オープン
- 作成日:90日以内に作成

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。

ケース

左側のパネルからYour Casesをクリックして、Your Casesページに移動します。



ケース

Your Casesページには、表示および管理する権限を持つケースの統合リストが表示されます。このリストに表示されるカラムを設定するには、Settingsアイコンをクリックして、必要なカラムのチェックボックスをオンにし、Applyをクリックします。Case number、Severity、Case state、Case status、Title、およびCreatedの各列は常に表示され、選択解除することはできません。

利用可能なアクション

「サービスリクエスト」ページでは、以下のアクションを実行できます。

- ケースを開く:ケースを開く: [ケースを開く]をクリックしてSCMを相互起動し、ケースを作成します
- データのエクスポート：ダッシュボードに現在表示されているすべてのデータをCSVファイルとしてダウンロードするには、エクスポートをクリックします
- ケース詳細の表示：ケース番号またはテーブル行をクリックして、ケースの詳細ビューを開きます(詳細については、「ケースの詳細ビュー」を参照してください)。
- ケースのクローズ：オープン・ケースの「その他オプション」アイコン> 「ケースのクローズ」を選択して「ケースのクローズ」ウィンドウをオープンします。このウィンドウで、クローズする理由を指定してケースをクローズできます
- ケースの再オープン：クローズしたケースの「その他オプション」アイコン> 「ケースの再

オープン」を選択して「ケースの再オープン」ウィンドウをオープンします。このウィンドウで、再オープンの理由を指定してケースをオープンできます

注：終了した症例は、終了から14日以内に再開できる。

ケースのビューのフィルタ

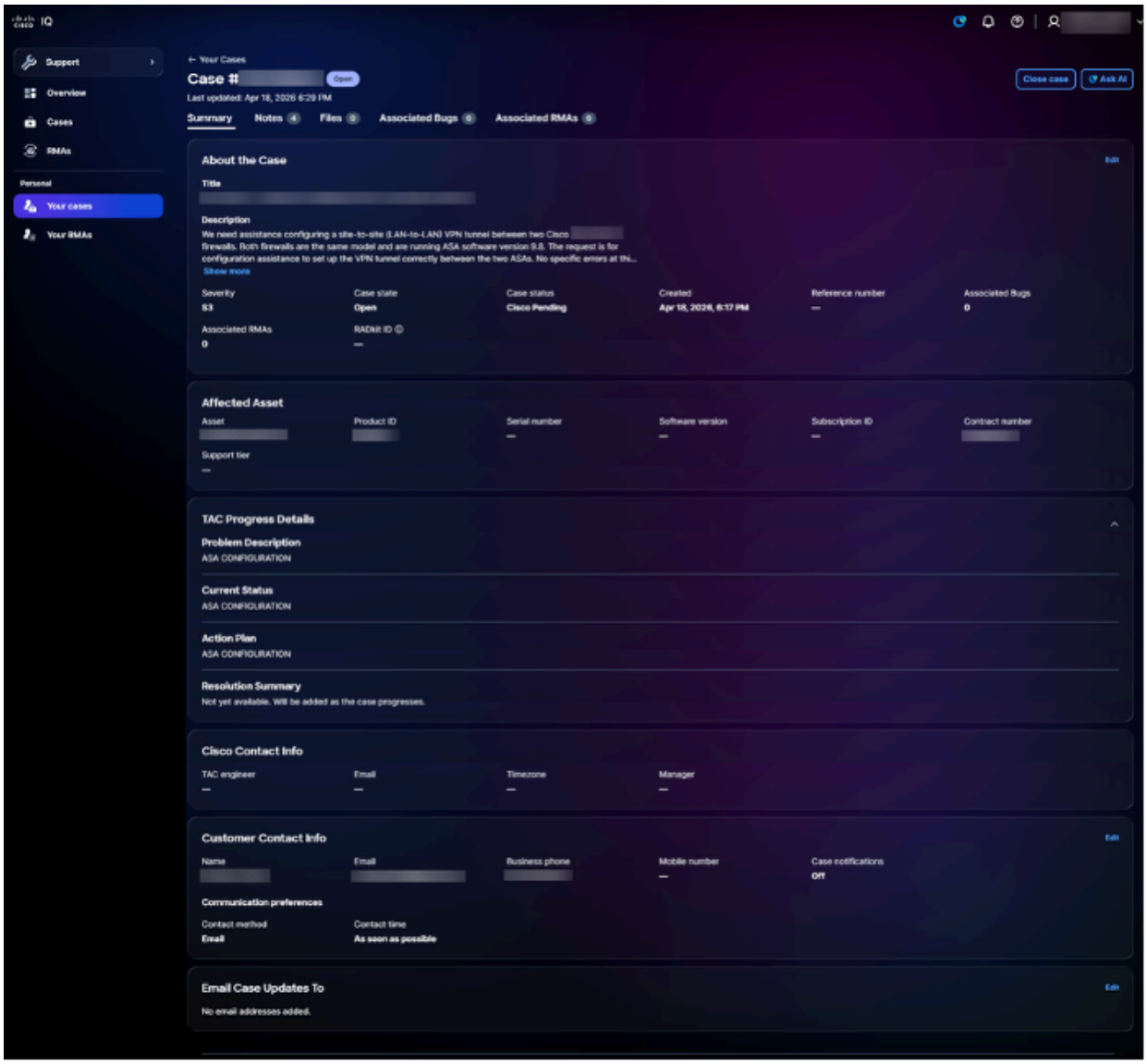
ドロップダウンリストからフィルタを選択するか、[お客様の連絡先]チェックボックスをオンにすることで、リストビューにフィルタを適用できます。必要に応じて、Filtersをクリックし、使用可能なフィルタオプションのリストから選択します。フィルタと選択は、セッションとログインを通じて保持され、ダッシュボードをパーソナライズします。適用されるデフォルトのフィルタは次のとおりです。

- ケースの状態：オープン
- Customer contact is youチェックボックス
- 作成日:90日以内に作成

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。

ケースの詳細ビュー

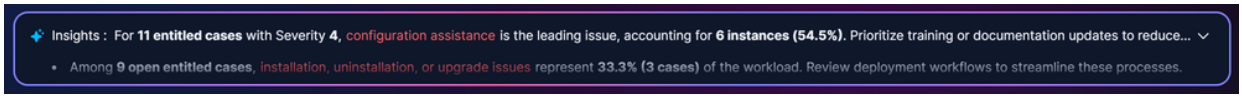
ケースの詳細を表示するには、リストからケースをクリックします。



サポート案件の詳細ビュー

サポート・リクエストの詳細ビューが表示され、サポート・リクエストの一元的なビューが提供されます。このビューでは、ケース情報、影響を受ける資産情報を確認し、TACの進行状況を追跡し、使用可能なケース・アクションにアクセスできます。実行できるアクションには、「ケースを再オープン」をクリックしてクローズしたケースを再オープンする、「ケースをクローズ」をクリックしてオープンしたケースをクローズする、および「AIに問い合わせる」をクリックしてケースのコンテキストでAIアシスタントを起動するなどがあります。使用可能なタブについては、以下のセクションで説明します。

注:AIによって生成されたフィールドには、該当する場合にアスタリスクのアイコンが付いています。

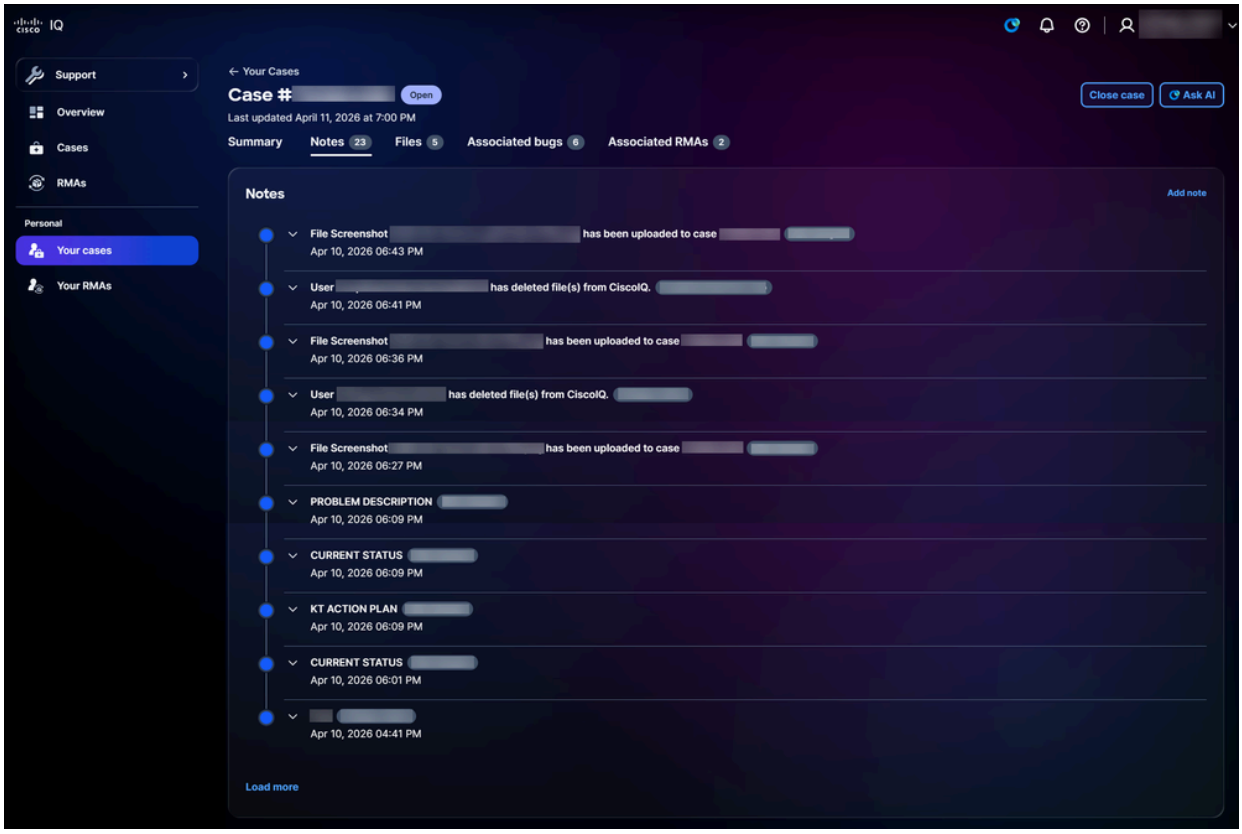


星アイコン

要約

Summaryタブには、主なサポート案件の情報が表示されます。個々のサポート案件の現在の状態、コンテキスト、進捗状況をすばやく把握できます。ケースの詳細と影響を受ける資産を確認し、TAC進捗状況の詳細からケースのライフサイクルを監視し、連絡先情報を変更し、ケースの更新通知を受信する電子メールアドレスを指定できます。編集できるのは選択したフィールドだけです。

注意事項



注意事項

Notesタブをクリックすると、Notesページが開きます。お客様またはシスコのエンジニアが送信したかどうかにかかわらず、ケースに関連するすべてのメモを表示できます。

新しいノートを追加するには、次の手順に従います。

⚠ 警告：メモを削除できません。

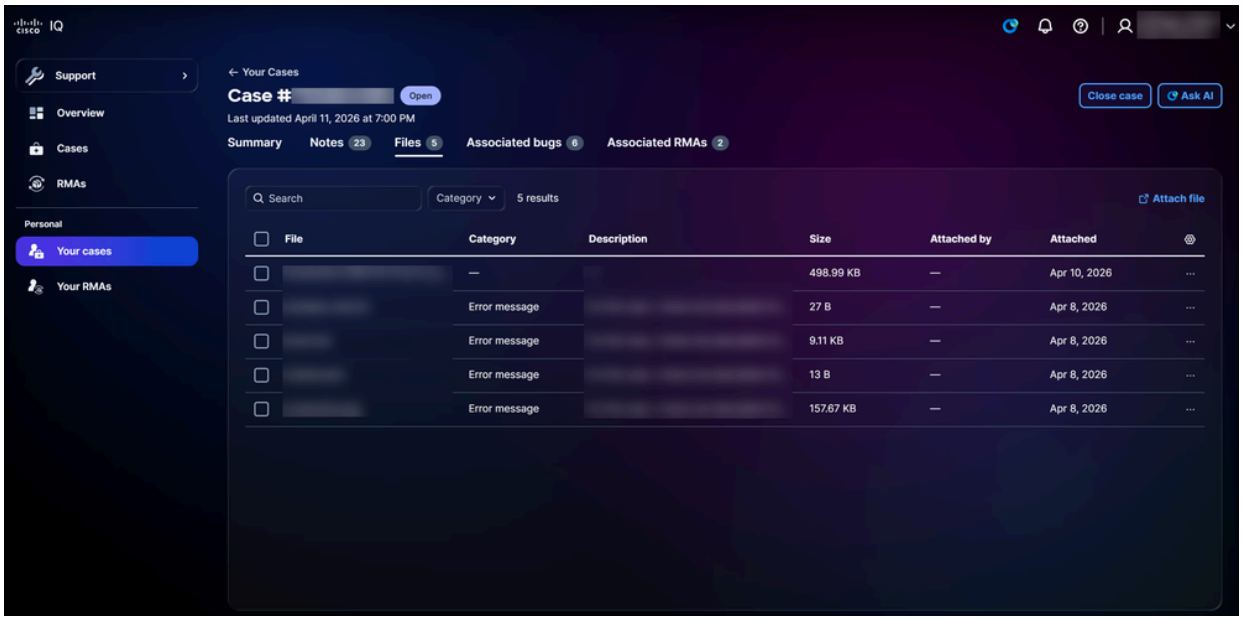
---

1. Add noteをクリックします。Add noteウィンドウが開きます。
2. タイトルを入力します。

3. 詳細を入力します。

4. [Add] をクリックします。

ファイル



ファイル

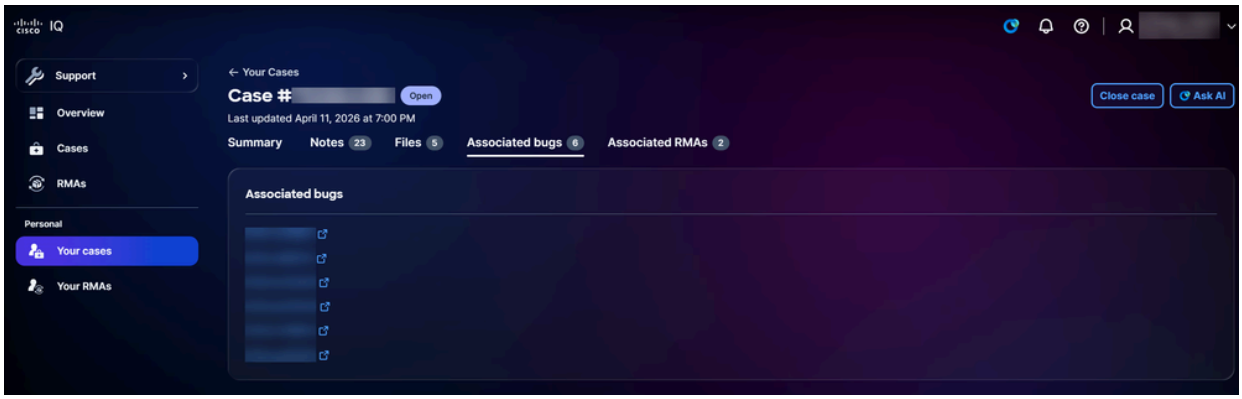
Filesタブをクリックすると、Filesページが開きます。ケースのファイルの名前、サイズ、日付を表示したり、ファイルを追加または削除したりできます。Categoryドロップダウンリストからオプションを選択して、ファイルをフィルタリングします。必要に応じて、Filtersをクリックし、使用可能なフィルタオプションから選択します。また、Settingsアイコンをクリックし、目的のカラムのチェックボックスをオンにして、Applyをクリックすると、リストに表示されるカラムを設定できます。

ファイルを追加するには、Attach fileをクリックします。ケースのファイルをアップロードできるSCMにリダイレクトされます。

ファイルを削除するには、削除するファイルのチェックボックスをオンにして、Deleteをクリックします。ファイルの削除ウィンドウが開きます。Delete file(s)をクリックします。

注：ファイルのダウンロードはサポートされていません。

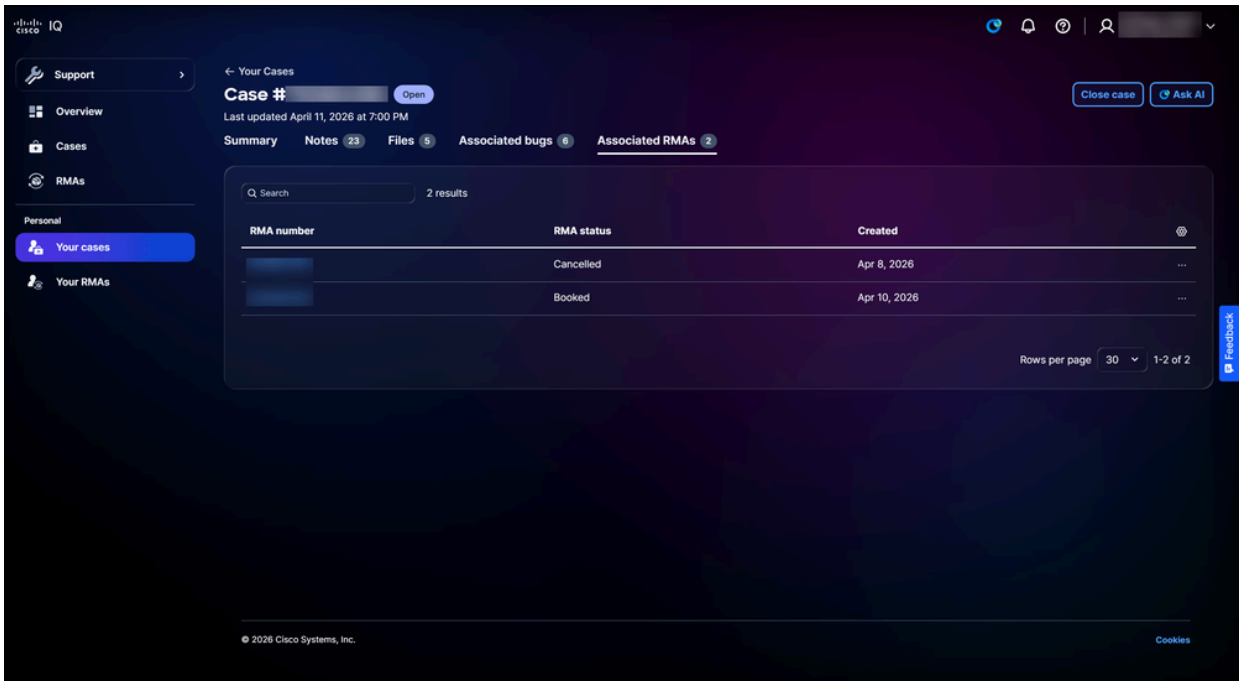
関連するバグ



関連するバグ

Associated bugsタブをクリックすると、Associated bugsページが開きます。バグIDをクリックすると、Cisco.comのBug Search Toolでバグの詳細情報をクロス起動できます。

関連するRMA



関連するRMA

Associated RMAsタブをクリックすると、Associated RMAsページが開きます。このリストに表示されるカラムを設定するには、Settingsアイコンをクリックして、必要なカラムのチェックボックスをオンにし、Applyをクリックします。関連するRMAページでは、次のアクションを実行できます。

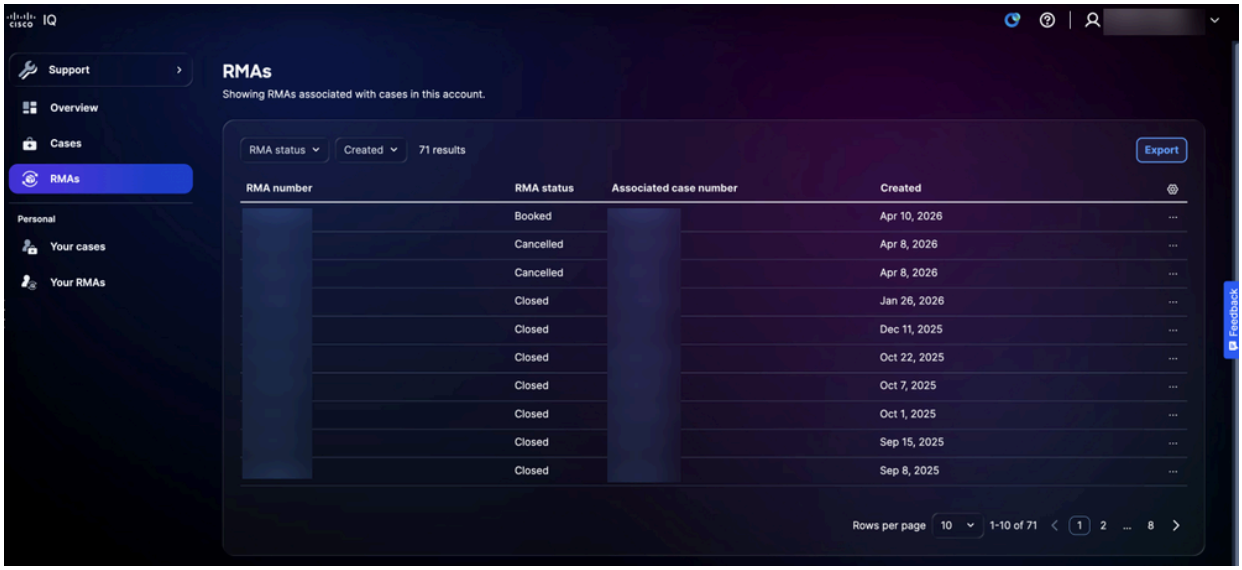
- ケースを閉じる: 「ケースを閉じる」をクリックして「ケースを閉じる」ウィンドウを開きます。このウィンドウで、終了の理由を指定してケースを閉じることができます
- RMA詳細の表示:RMA番号またはテーブル行をクリックして、RMAの詳細ビューを開きます

(詳細は、「RMA詳細ビュー」を参照してください)。

- Contact Cisco Logistics：行のMore Optionsアイコンを選択> Contact Cisco logisticsをクリックして、Cisco Logistics Teamに連絡してください。

RMA

アカウントRMA



RMAリスト

左側のパネルでRMAsをクリックして、RMAsページに移動します。RMAページには、Cisco IQアカウントのケースに関連付けられたすべてのRMAの一覧表が表示されます。このリストに表示されるカラムを設定するには、Settingsアイコンをクリックして、必要なカラムのチェックボックスをオンにし、Applyをクリックします。

利用可能なアクション

RMAページでは、次のアクションを実行できます。

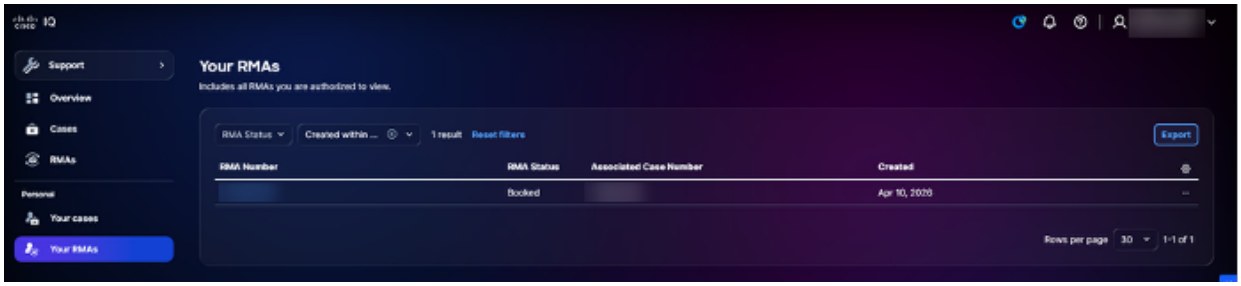
- データのエクスポート：現在CSVファイルとして表示されているすべてのデータをダウンロードするには、エクスポートをクリックします
- RMA詳細の表示:RMA番号またはテーブル行をクリックして、RMAの詳細ビューを開きます(詳細は、「RMA詳細ビュー」を参照してください)。
- Contact Cisco Logistics：行のMore Optionsアイコンを選択> Contact Cisco logisticsをクリックして、Cisco Logistics Teamに連絡してください。

アカウントRMAのビューのフィルタリング

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。

RMA

左側のパネルからYour RMAsをクリックして、Your RMAsページに移動します。



RMA

「Your RMAs」ページに、表示および管理に必要な資格を持つRMAの一覧が表示されます。このリストに表示されるカラムを設定するには、Settingsアイコンをクリックして、必要なカラムのチェックボックスをオンにし、Applyをクリックします。

利用可能なアクション

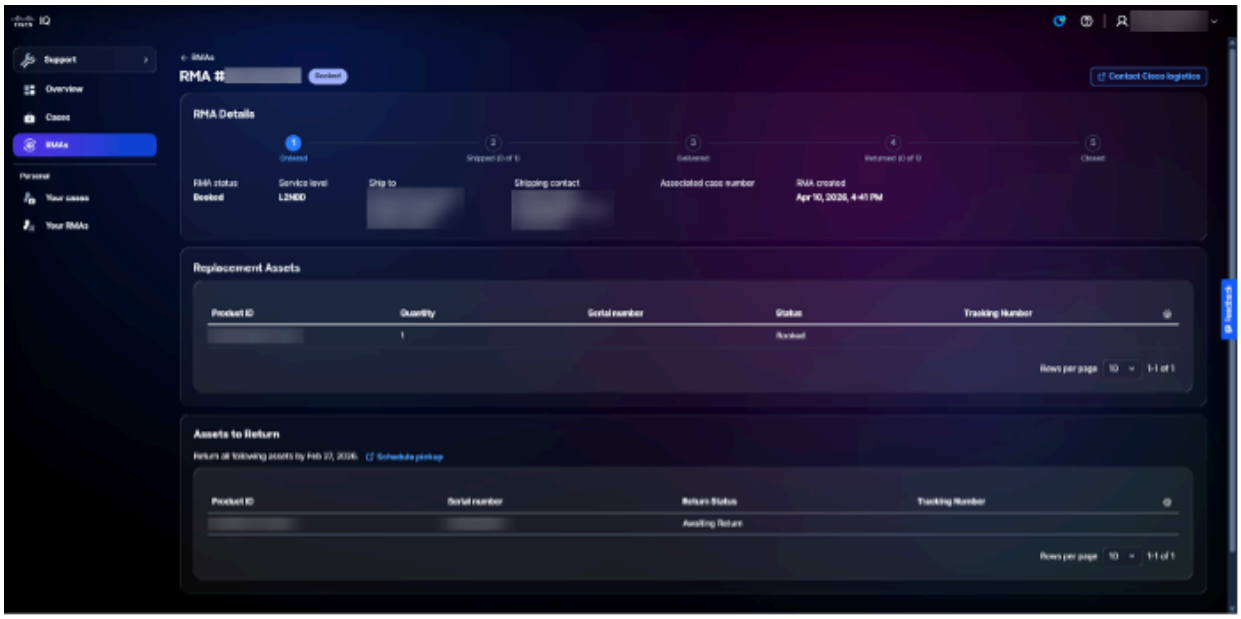
RMAページから次のアクションを実行できます。

- データのエクスポート：現在CSVファイルとして表示されているすべてのデータをダウンロードするには、エクスポートをクリックします
- RMA詳細の表示:RMA番号またはテーブル行をクリックして、RMAの詳細ビューを開きます(詳細は、「RMA詳細ビュー」を参照してください)。
- Contact Cisco Logistics：行のMore Optionsアイコンを選択> Contact Cisco logisticsをクリックして、Cisco Logistics Teamに連絡してください。

RMAのビューのフィルタリング

Createdドロップダウンリストからオプションを選択して、リストビューをフィルタリングできます。

RMAの詳細ビュー



RMA詳細ビュー

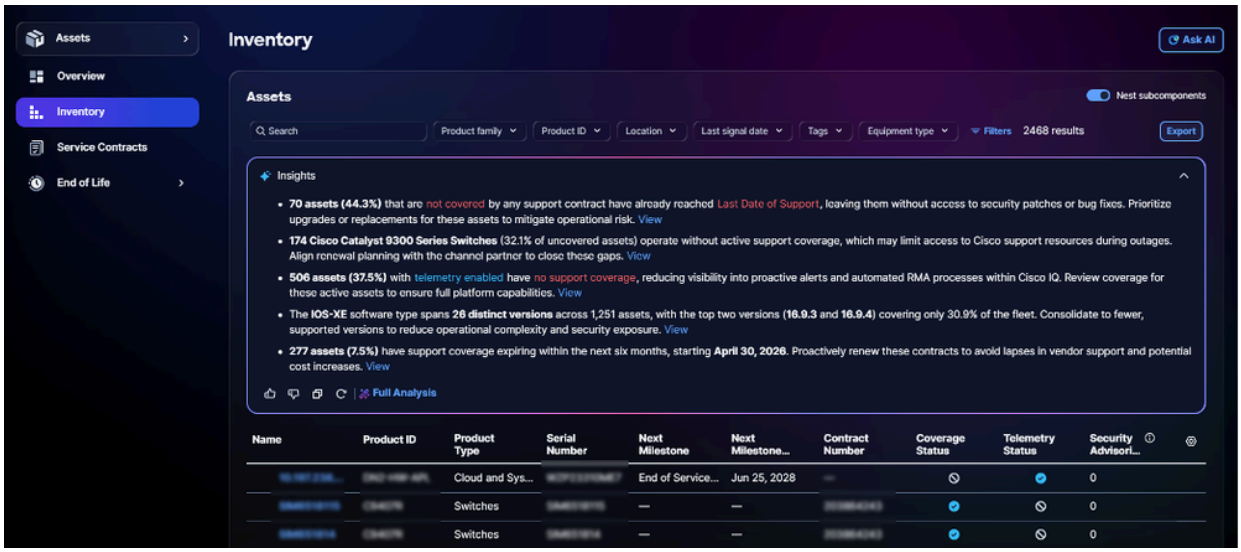
RMAの詳細ビューにはRMAの一元化されたビューが表示され、RMA情報の確認、進行状況の追跡、および使用可能なRMA処理へのアクセスが可能になります。利用可能なアクションには、シスコロジスティクスチームへの連絡、追跡番号へのアクセス、資産の受け取りのスケジュールなどがあります。

共通のアプリケーション機能

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。

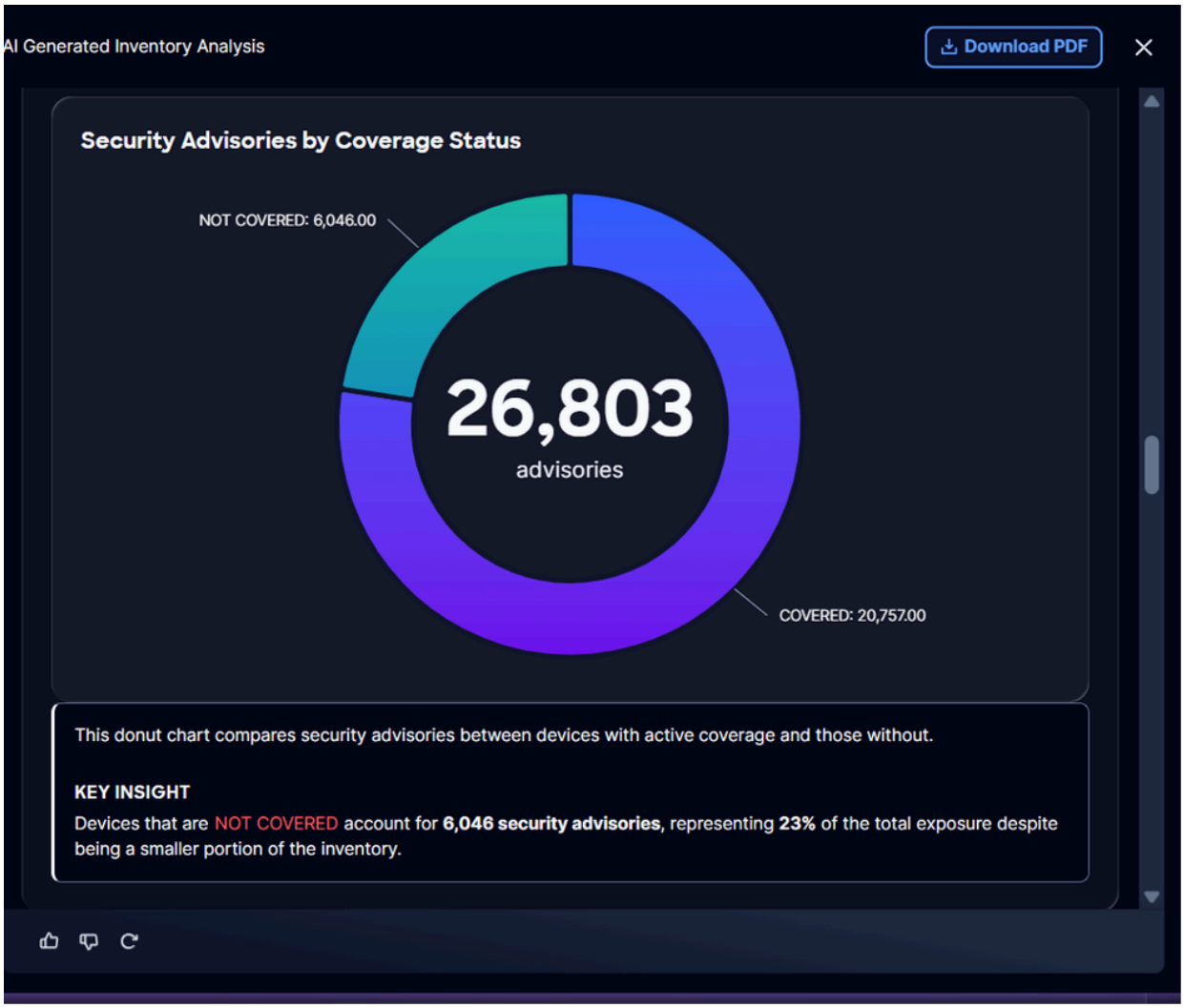
✎ 注：分析機能は、選択したページでのみ使用できます。



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



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。

- 記録や共同作業のために分析のオフラインコピーを保存するには、PDFのダウンロードをクリックします

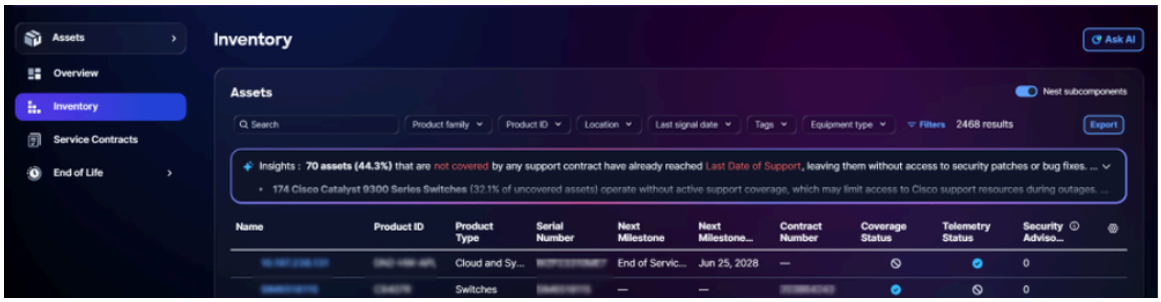
情報のエクスポート

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。

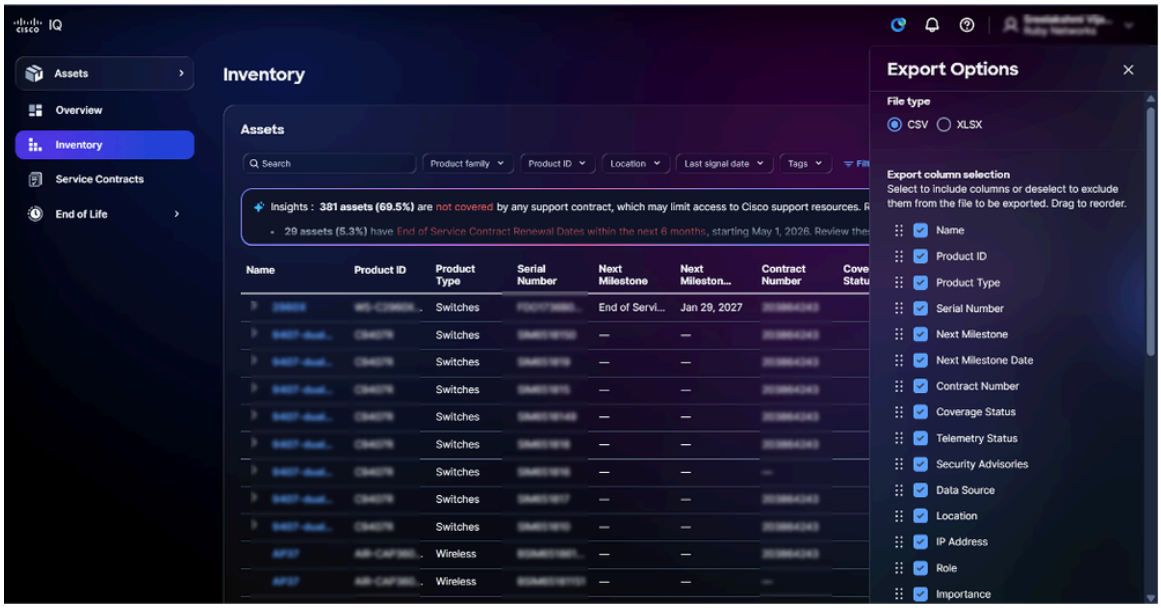
ページから情報をエクスポートするには、次の手順に従います。

1. ページに移動します。



Assetsアプリケーション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。

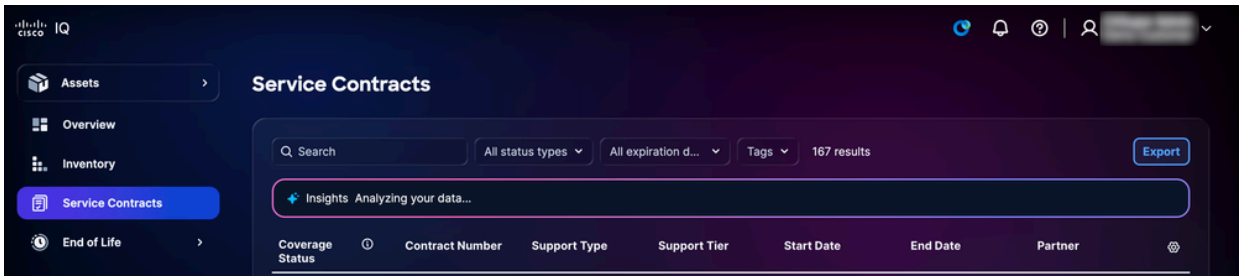


エクスポートオプション

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。

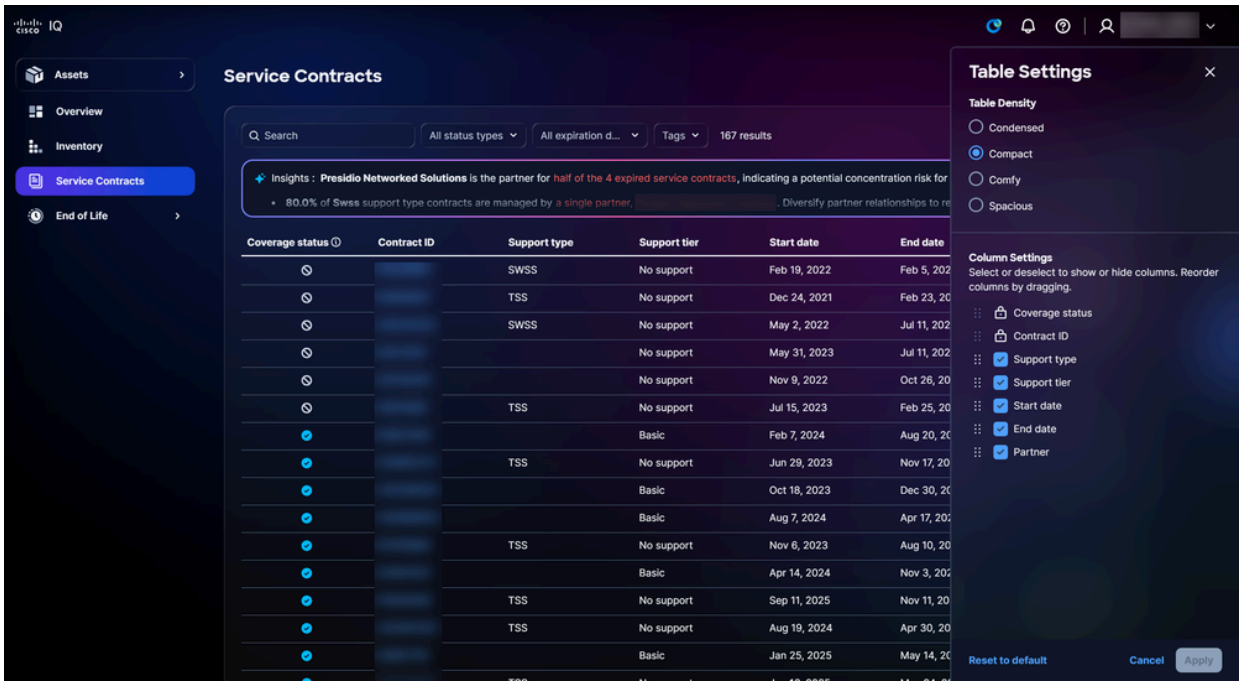
テーブルの設定

テーブル設定を構成して、異なるアプリケーション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。

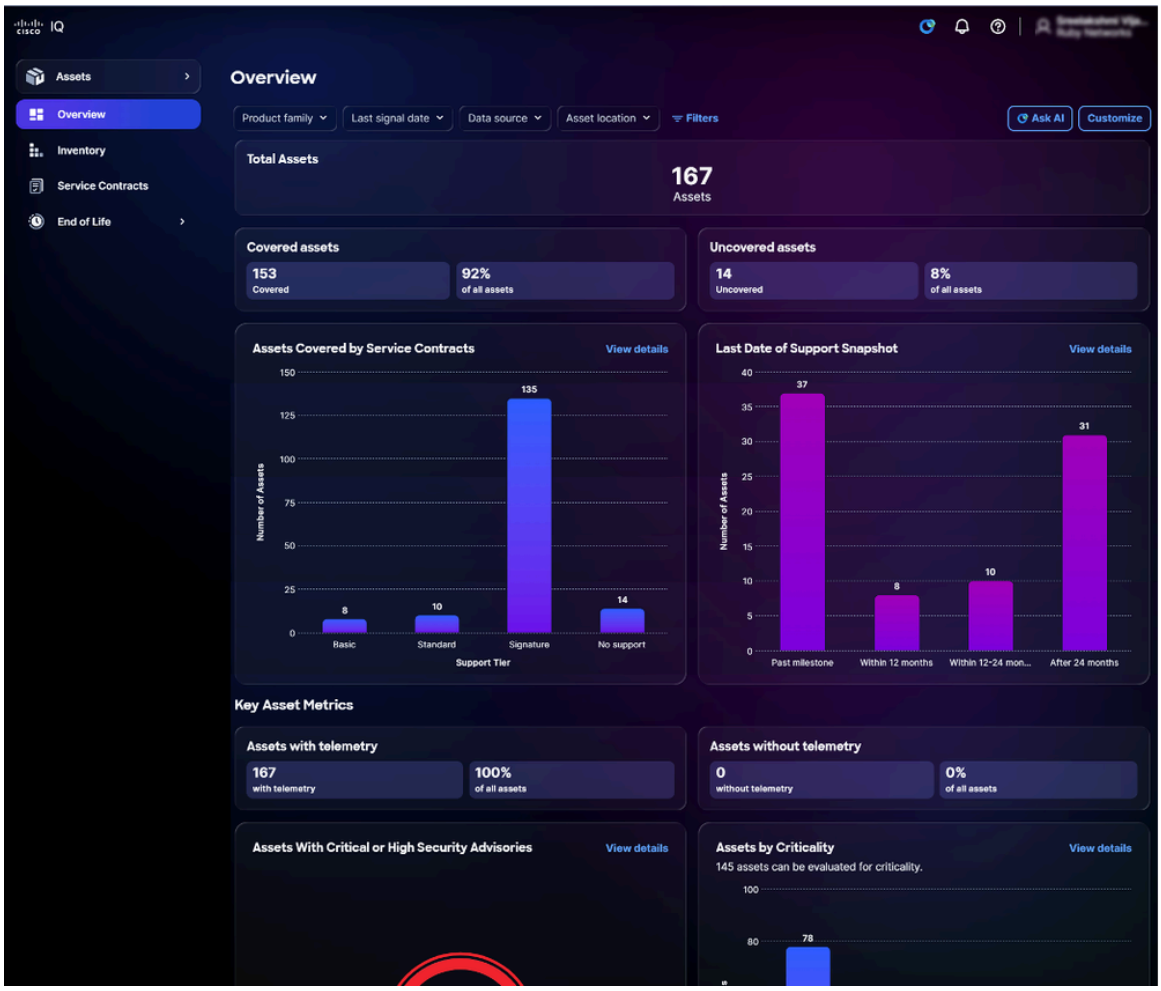
ダッシュボードのカスタマイズ

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。

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。

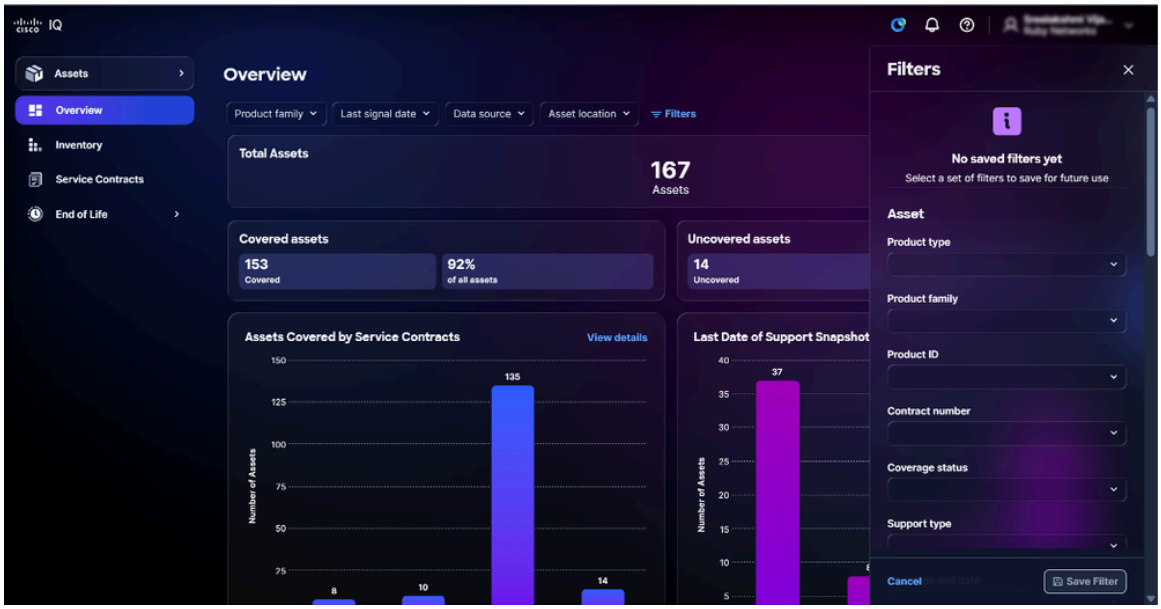
フィルタのカスタマイズ

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

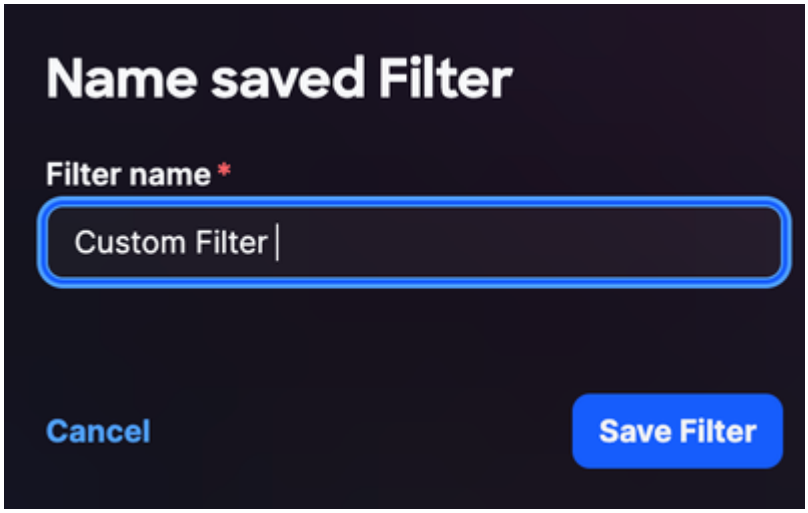
カスタムフィルタを作成するには、次の手順を実行します。

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。Name saved Filterウィンドウが開きます。



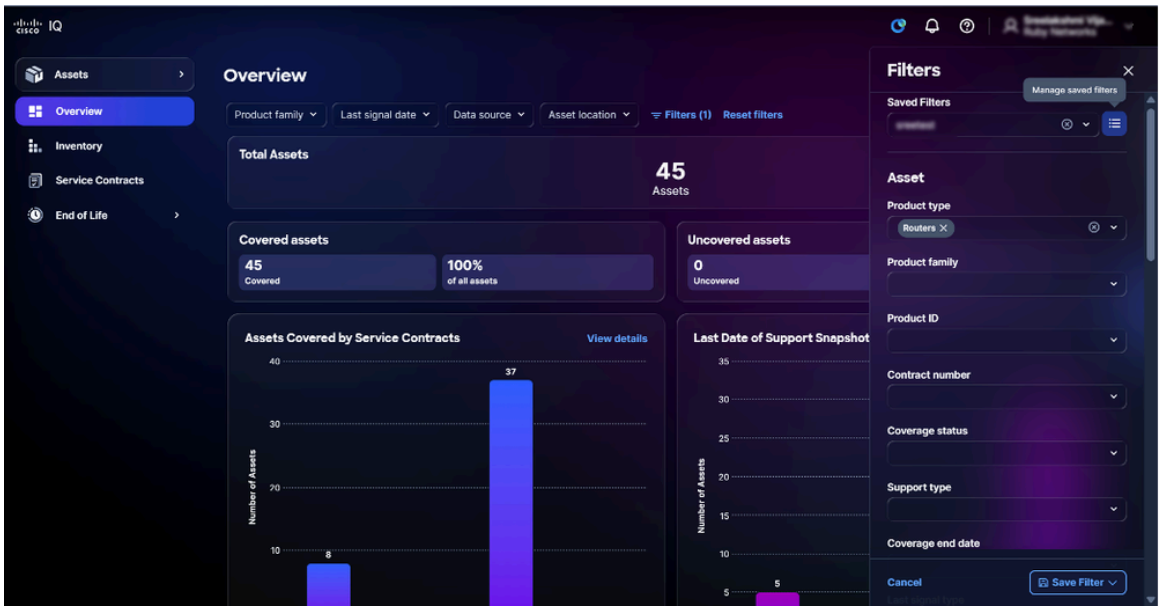
フィルタ名

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。

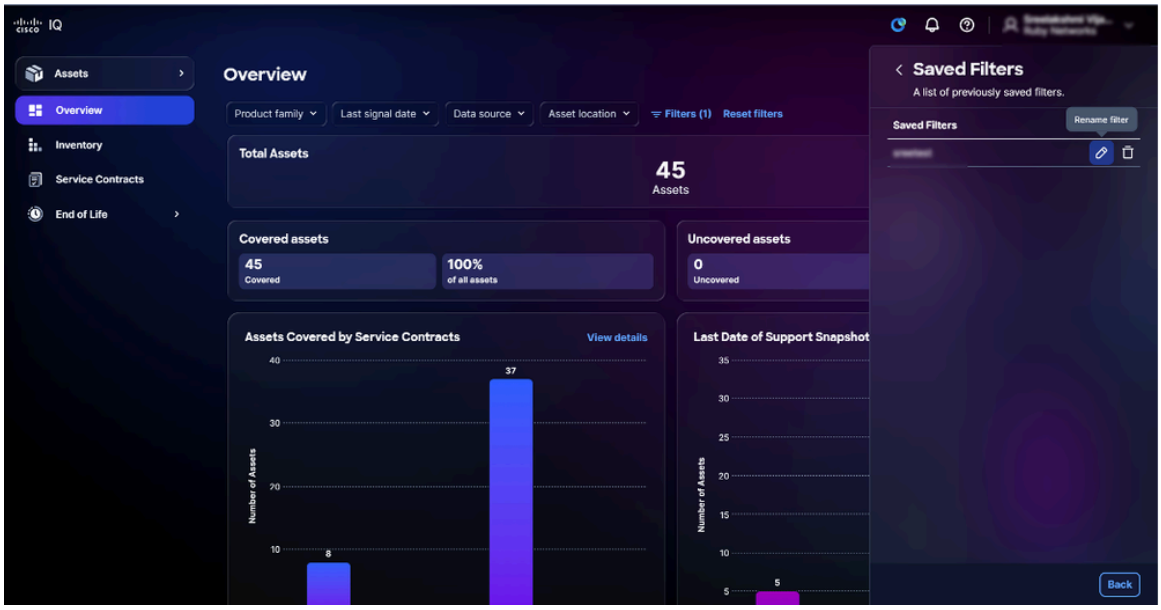
1. Filtersをクリックします。



保存済みフィルタの管理

2. 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。



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。

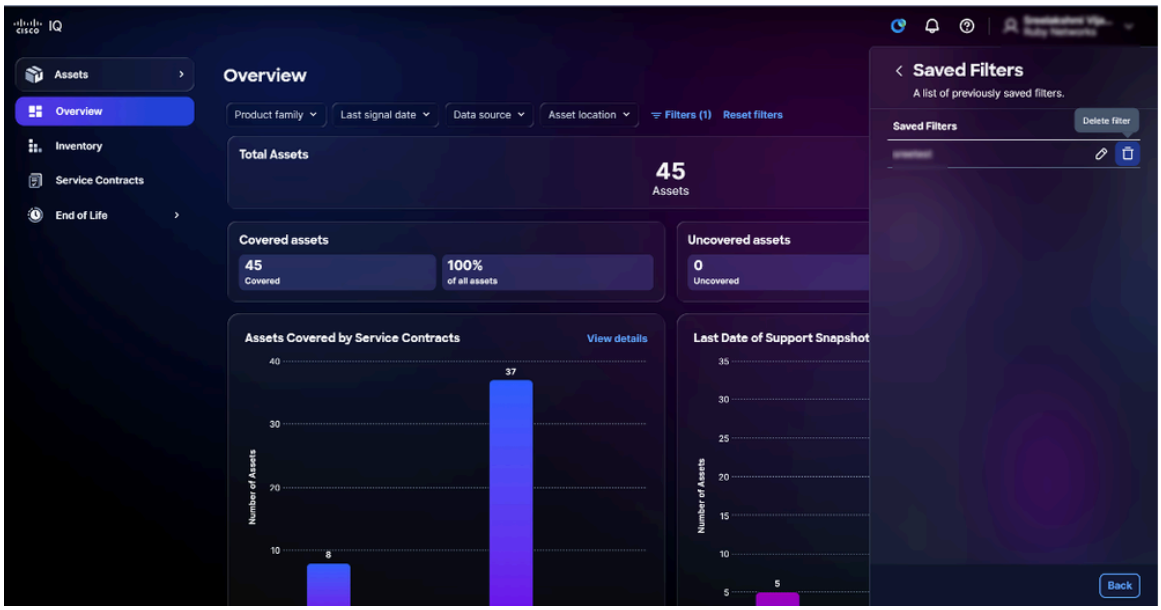
フィルタの削除

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。
5. Yes, deleteをクリックして確定します。

AIアシスタント

概要

Cisco IQ AI Assistantは、生データを実用的な洞察、推奨事項、およびガイド付きアクションに変換することで、Cisco IQの理解と利用を向上させることを目的としています。既存のツールと統合して、個々のデータソースを活用し、複数のデータストリームにわたってインテリジェンスを統合して、リアルタイムの提案を行います。状況に応じた情報に基づいた事前対応型の意思決定を可能にし、顧客エンゲージメントと成功のためのプロセスを合理化することで、Cisco IQ AI Assistantは運用成果を最適化し、Cisco IQのユーザエクスペリエンスを向上させます。

Cisco IQ AI Assistantには次の機能があります。

- 堅牢なエッジケース処理：透過的な説明と明確な指示を受け取り、シームレスなサポートエクスペリエンスと高いユーザ満足度を確保します。
- ストリーミング機能：生成された応答の表示
- 拡張されたコンテキストデータ：動的なコンテキストにより、アプリケーション、ページ、およびセッション間のシームレスな対話が可能になります。
- サポート・リクエスト管理サポート:「サポート・リクエスト」リスト・ビューに表示され

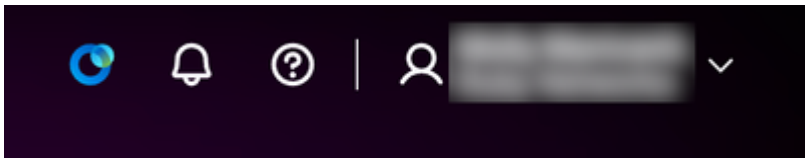
るサポート・リクエストの作成、表示および管理

- 資産インベントリ管理：組織の資産またはリソースの追跡、管理、およびレポートの生成
- 資産の重要度：ネットワーク内での役割と重要性に基づいて、リスク軽減活動の対象となる資産の優先順位を設定します。
- リスクの評価と管理：組織の資産に関連する潜在的リスクを評価および管理します。
- セキュリティの強化：サポート対象デバイスに対するお客様のデバイス実行コンフィギュレーションを、関連するシスコおよびCybersecurity and Infrastructure Security Agency(CISA)の強化ガイドラインと比較します。
- 設定：お客様のデバイス実行コンフィギュレーションを推奨されるベストプラクティスに照らし合わせて評価し、設定の不整合を特定して実行可能な推奨事項を提供します。

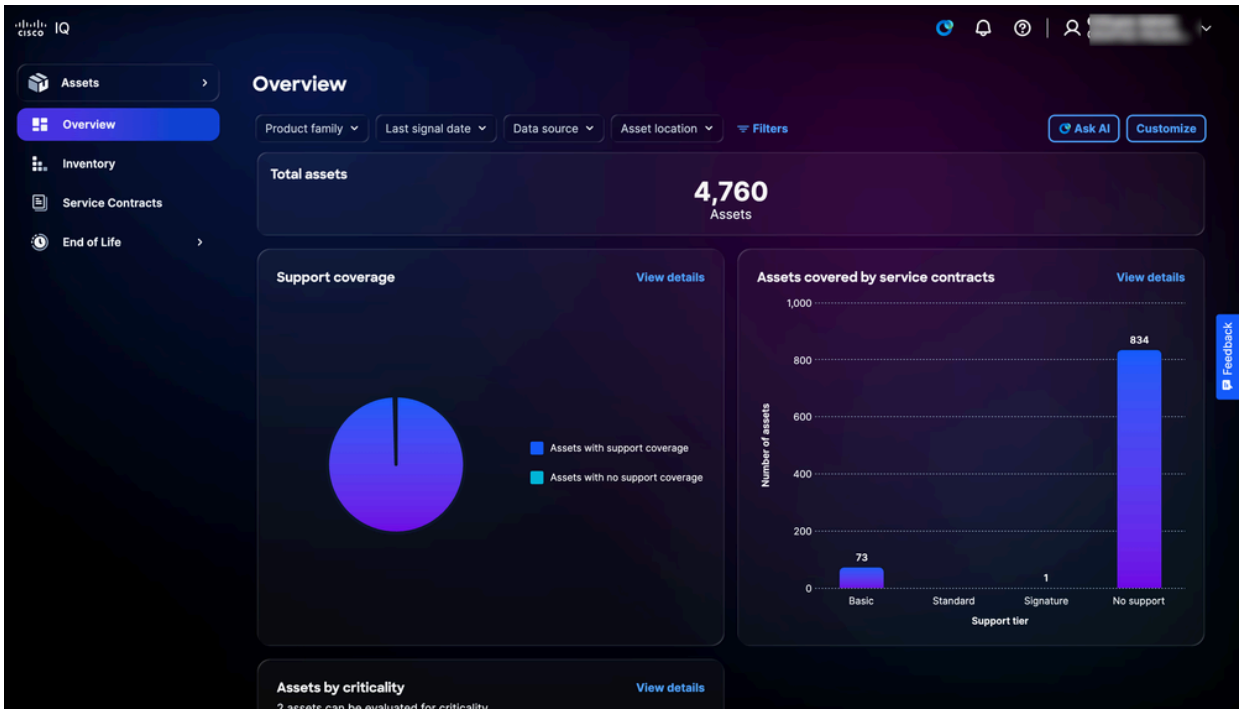
注:Cisco IQ AI Assistantは、Cisco IQ内のどこからでも起動できます。すべてのユーザが利用できますが、提供される機能はサポート層レベル（Basic、Standard、またはSignature）によって異なります。

Cisco IQ AI Assistantへのアクセス

Cisco IQ AI Assistantを使用するには：



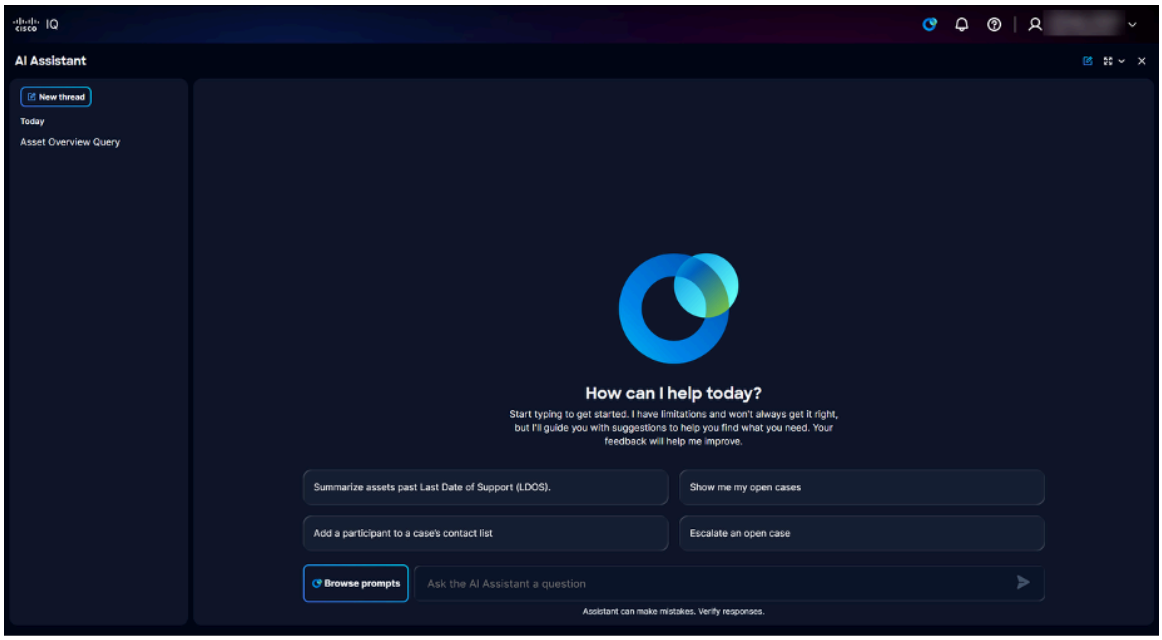
AIアシスタントアイコン



AIに聞く

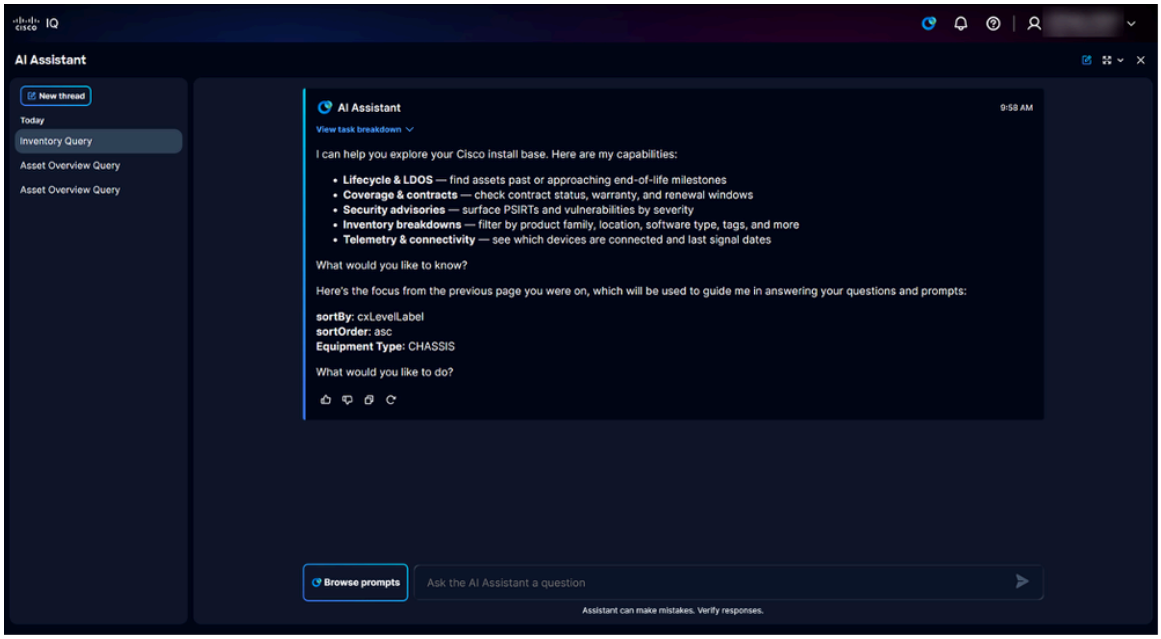
1. AI Assistantアイコンをクリックするか、Ask AIをクリックして、Cisco IQ AI Assistantを起動します。

注:Cisco IQ AI Assistantには、これら2つのオプションをクリックすることで、Cisco IQ内のどこからでもアクセスできます。ユーザが起動する特定のページのデータとコンテキストを利用して、関連性の高い洞察と推奨事項を提供します。お客様の現在のタスクを理解することで、パーソナライズされたガイダンス、トラブルシューティング手順、および効率性の向上を実現します。



ランディングページ

注：新しいプロンプトを入力するか、あらかじめ作成されたプロンプトのライブラリを参照できます。



アプリケーションコンテキストを含むランディングページ

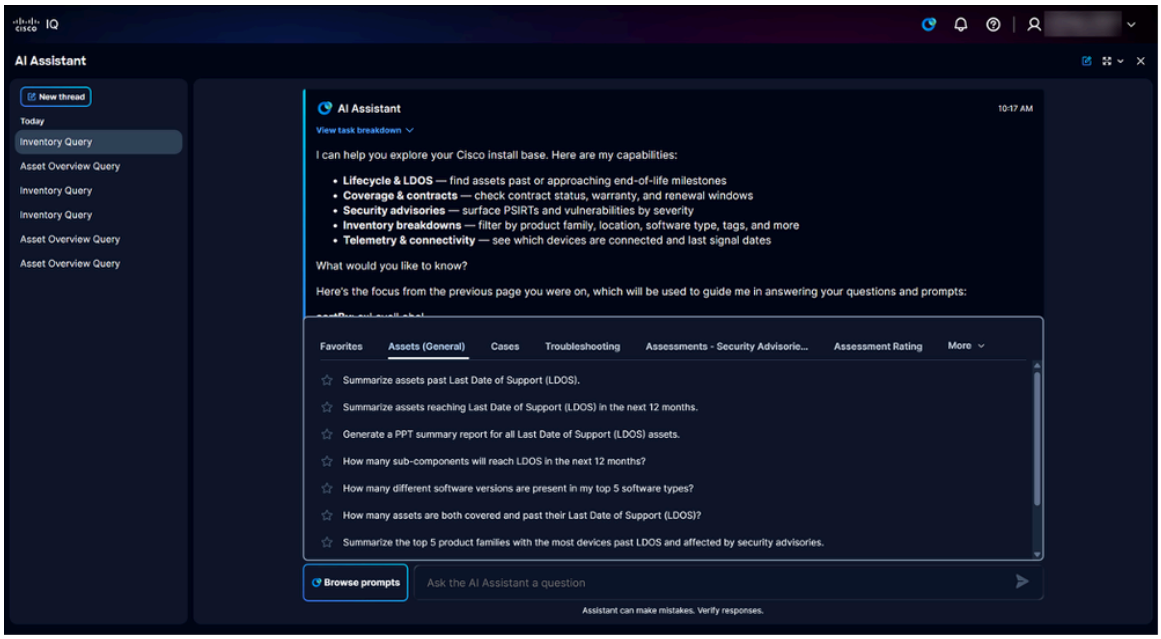
注：デフォルトでは、Cisco IQ AI Assistantのビューは全画面に設定されています。新しいビューを選択すると、Cisco IQ AI Assistantは以前に選択したビューを保持します。

Cisco IQ AI Assistantには、次の使用可能なオプションが表示されます。

- 以前のスレッド：30日間のプロンプト履歴を提供
- プロンプトの参照：プロンプトライブラリを開きます。プロンプトライブラリで使用可能なすべての質問のリストについては、「付録A:Cisco IQ AI Assistantのプロンプト」を参照してください
- AI Assistantに質問フィールドを入力する：テキストフィールドを使用してAI Assistantに質問します。完全な説明文を使用して、より適切な回答を得ます。

2. 次のいずれかの方法を使用して、プロンプトを選択します。

- 「AIアシスタントに質問」フィールドに1つ以上のキーワードを入力してプロンプトを検索し、プロンプトをクリックします
- 説明文と完全な文を使用した自由形式の質問をAI Assistantに質問フィールドに入力します



プロンプトライブラリ

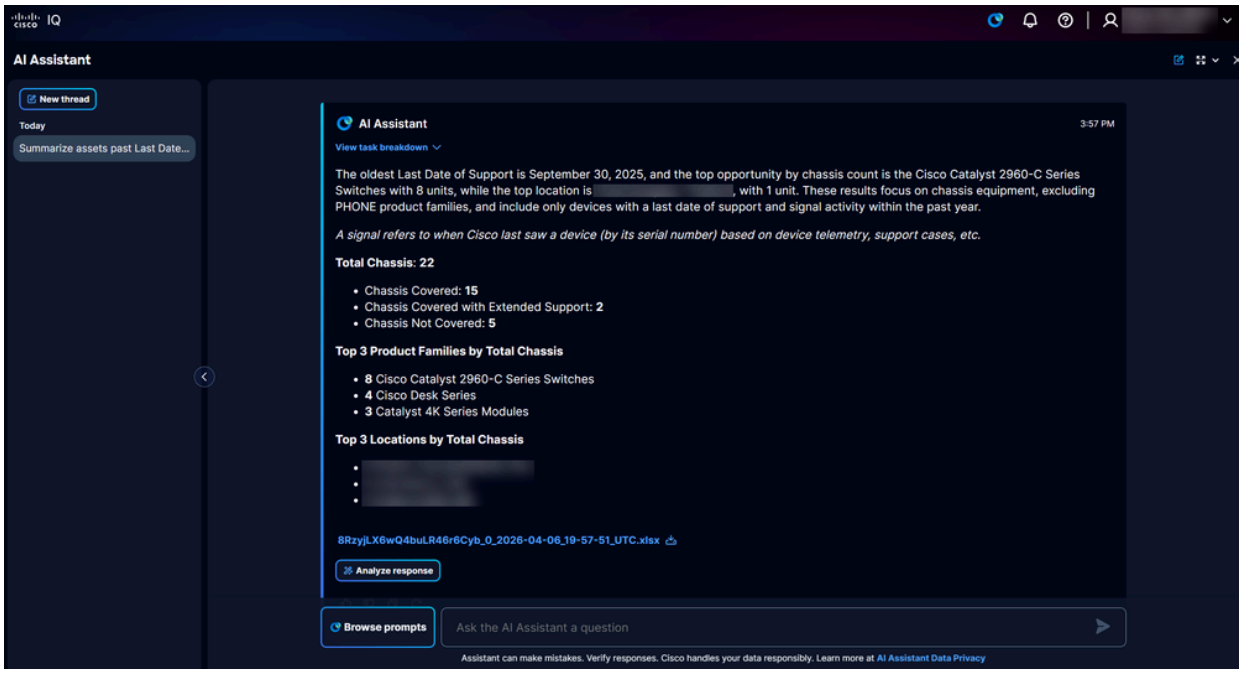
- Browse Promptsをクリックしてプロンプトライブラリを開き、次のプロンプトカテゴリタブのいずれかを選択します。
    - Assets(General):LDOSおよび一般的なインベントリクエリーを含む、資産ライフサイクルに関連するプロンプト
    - ケース：ケースの表示、更新、エスカレーション、終了などのケース管理アクションをサポートするためのプロンプト。これにより、シスコサポートエンジニアによる効率的な追跡と接続が可能
    - Troubleshooting：エラーsyslogメッセージまたは設定に関する質問を支援するプロンプト
    - 評価 – セキュリティアドバイザリ：全体的なネットワークセキュリティポスチャの評価、重大な脆弱性の特定、および重大度の高いセキュリティの脅威または設定の脆弱性の影響を受ける特定の資産のリストに関するプロンプト
    - 資産重要度：ネットワーク内での役割と重要性に基づいて、リスク軽減活動の資産の優先順位付けに関連するプロンプト
    - Assessments - Configuration(評価 – 構成)：構成の評価結果の要約、推奨ベストプラクティスに対する構成の逸脱の特定、および実行可能な推奨事項の生成に関連するプロンプト
    - 評価 – セキュリティの強化：推奨されるセキュリティベースライン設定の特定、デバイスを強化するためのベストプラクティス、シスコネットワークインフラストラクチャを保護するための手順に関する情報を提供します。

3. プロンプトをクリックします。応答が生成されます。

AI Assistantの拡張コンテキストデータ

Cisco IQ AI Assistantは、コンテキストを動的にし、アプリケーション、ページ、セッション間のシームレスなインタラクションを可能にします。これにより、すべての回答でコンテキストデータを活用し、質問に合わせて関連性の高い回答を提供できます。

LDOSの集約と優先順位付け



LDOSレポート

LDOSの集約と優先順位付け機能により、ネットワーク資産に関連するリスクを迅速に特定して対処できます。この機能は、予想されるネットワークの役割とセキュリティ脆弱性のステータスによって資産を分類し、脆弱性の修復を可能にして、サービス全体の品質を向上させます。

主な利点

LDOSの集約と優先順位付け機能の主な利点は次のとおりです。

- 優先順位付けされたリスクビュー
- 運用インパクト分析
- 実用的な洞察

この機能の一部として、ユーザインターフェイスまたはLDOSインサイトの表示時に、事前シー

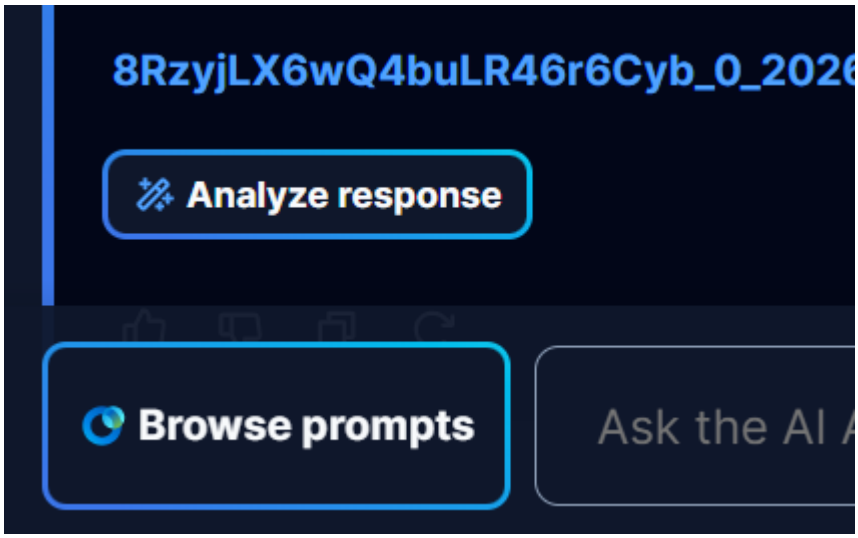
ド済み質問の限定されたセット（「*」でマーク）を表示できます。

レポート

LDOSレポートの生成

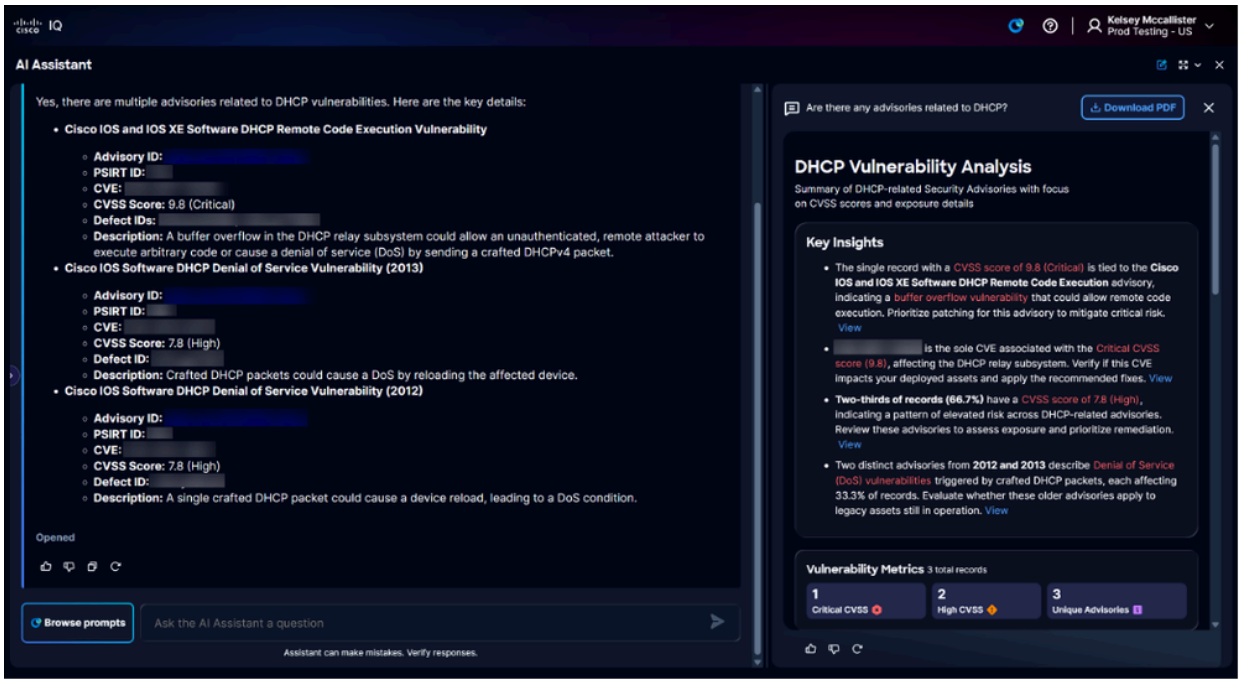
AIによって生成され、キュレーションされたLDOSレポートは、LDOSに接近または通過した資産の概要を提供します。このレポートでは、更新オプションが強調表示されるほか、セキュリティアドバイザリと脆弱性が特定されるため、ネットワークのリスク状況を迅速に把握するのに役立ちます。

応答の分析



応答の分析

Analyze Responseをクリックすると、データを要約し、グラフ、ダッシュボード、チャートなどのさまざまな可視化を生成するAI駆動型のサマリーが表示され、有益な情報が提供されます。



AIサマリー

AI駆動サマリーには、レポートをPDFとしてダウンロードするための「PDFのダウンロード」ボタンが含まれています。

LDOS集約およびレポート生成のデータソース

LDOSの集約および優先順位付け機能では、次の主要なデータソースが利用されます。

- インストールベースの資産と契約
- テレメトリ資産および契約
- CX信号データ
- ハードウェアおよびソフトウェア資産のEOLマイルストーン

Cisco IQ AI Assistantのトラブルシューティング

Cisco IQを使用すると、Cisco IQ AI Assistantでデバイスの問題を個別に解決できます。シスコ認定のトラブルシューティングツールと実績のあるナレッジベースを基盤とするこの直感的でインタラクティブなアシスタントは、コンテキストに応じた推奨事項をリアルタイムで提供します。

日常のトラブルシューティングシナリオに対応するように設計されており、ネットワークエンジニアがシスコ製品の問題を調査し、症状を確認し、実用的な次のステップを特定できるように支援します。エラーメッセージ、syslog、ソフトウェア不具合、リリースガイダンス、設定に関す

る質問などの技術的な詳細を解釈します。課題に即座に対応することで、サポートケースをオープンすることなく問題を解決し、最適なパフォーマンスを維持して時間を節約できます。

ベスト プラクティス

Cisco IQ AI Assistantをトラブルシューティングに使用する場合は、次のベストプラクティスに従ってください。

- 最初のメッセージには、プラットフォーム、製品ファミリ、およびソフトウェアのバージョンをできるだけ具体的に記載してください

注：アセットからCisco IQ AI Assistantを起動すると、すでにこの情報が表示されます。

- 正確なエラー、アラーム、またはsyslogテキストを、言い換える代わりに貼り付けます
- アップグレード、設定の更新、トポロジの変更など、問題が発生する前の変更点を説明する
- 問題が1台のデバイス、1つのサイト、または複数のユーザに影響するかどうかなど、影響を明確に共有します。

ケース

サポート・リクエスト管理機能を使用すると、ユーザーはセルフ・サービスを通じてサポート・リクエストを管理でき、ビジネス・アプリケーションとサービスが迅速にリストアされます。この機能は、ケースを効率的に管理し、サポートを合理化するのに役立ちます。Case Managementについての詳細は、『サポートアプリケーション』を参照してください。

Cases Managementを使用すると、ユーザーはサポート・リクエストを1か所ですばやく表示および管理できます。サポート・リクエストのステータスの確認、更新の確認、進行状況の確認、次のステップに関する情報の確認が可能なため、問題の管理とサポートの迅速な受け取りが容易になります。

付録A:Cisco IQ AI Assistantのプロンプト

この付録では、Cisco IQ AI Assistantで使用できるプロンプトの詳細な概要を説明します。この概要は、問題のテーマ別に箇条書きで構成されています。

注：使用可能なプロンプトを参照するには、プロンプトライブラリで入力に基づいてオプシ

ョンを絞り込みながら関連する候補を選択するか、独自のカスタムプロンプトを送信します。Cisco IQ AI Assistantは、自然言語入力に依存し、ドロップダウンメニューなどの入力フォームを含まないため、シームレスなユーザエクスペリエンスを実現します。

Assets (General)タブでは、次のプロンプトが表示されます。

- サポート終了日(LDOS)を過ぎた資産を要約します。
- 今後12ヵ月以内にサポート終了日(LDOS)に達する資産を要約します。
- すべてのサポート終了日(LDOS)資産に関するPPTサマリーレポートを生成します。
- 今後12ヵ月でLDOSに到達するサブコンポーネントはいくつありますか。
- 上位5つのソフトウェアタイプには、何種類の異なるソフトウェアバージョンがありますか。
- サポート対象の資産とサポート終了日(LDOS)を過ぎた資産の両方はいくつありますか。
- LDOSを過ぎ、セキュリティアドバイザリの影響を受けるデバイスの数が最も多い上位5つの製品ファミリをまとめます。
- LDOSを過ぎており、セキュリティアドバイザリの影響を受けるカードとモジュールを要約します。
- 親シャーシより前にサポート終了マイルストーンに達しているサブコンポーネントはいくつありますか。

Casesタブでは、次のプロンプトが表示されます。

- 未処理のサポート案件を表示する
- ケースの要約
- RMAステータスの表示
- バグのステータスを表示する
- 事例の最新情報を教えてください
- サポート案件に対する最新の更新と保留中のアクション項目を指定します
- 開いているケースを閉じる
- ケースの連絡先リストへの参加者の追加
- ケースに関するWebexスペース通信の作成
- 担当のエンジニアに連絡してください
- 未解決のサポート案件の重大度レベルを上げる
- 未解決のケースのエスカレーション
- ケースの新しいエンジニアをリクエストする
- オープン· ケースのキューの再作成
- サポート案件にメモを追加する

Troubleshooting タブでは、次のプロンプトが表示されます。

- Syslogエラー[Error]のトラブルシューティングを行い、根本原因を特定するにはどうすれば

よいのですか。
- 設定の問題のトラブルシューティングを行い、[ABCD]の根本原因を特定するにはどうすればよいのですか。
- 製品ID [ABCD]の[XYZ]を設定するにはどうすればよいですか。

Assessments - Security Advisoriesタブでは、次のプロンプトが表示されます。

- DHCPに関連するアドバイザリはありますか。
- salt typhoonに関連するwebUIの権限昇格の脆弱性を確認するためのセキュリティアドバイザリはありますか。
- HTTPを有効にする前に、HTTPの有効化に関連する既知のセキュリティアドバイザリや脆弱性を確認できますか。
- ネットワーク内に脆弱性を含むセキュリティアドバイザリはいくつありますか。
- セキュリティアドバイザリに対して脆弱なデバイスはいくつありますか。

Asset Criticalityタブでは、次のプロンプトが表示されます。

- 職務別および重要度別の最も重要な資産
- セキュリティアドバイザリの影響を受けるコアデバイスはいくつありますか。
- 今後12ヵ月以内に契約期限が切れる重要なデバイスと重要度の高いデバイスを要約する
- 役割と重要度に基づいて、更新するLDOS資産に優先順位を付けます。
- 役割と重要度に基づいて、契約対象外または契約対象外の資産を優先的に更新します。
- 契約対象の資産の役割と重要性に基づいて、契約更新の期限切れ契約に優先順位を付けます。
- 影響を受ける資産の重大度、役割、重要性に基づいて、PSIRTの脆弱性に優先順位を付けます。

Assessments - Configurationタブでは、次のプロンプトが表示されます。

- 最近の設定評価の概要を教えてください。
- 評価された設定のベストプラクティスルールの数と、少なくとも1つのアセットがパスしなかった数を答えてください。
- ネットワーク全体で最も一般的な設定の違いは何ですか。
- 構成のベストプラクティスとの相違が最も多いシスコ製品ファミリはどれか？
- 評価された資産の数と、合格しなかった割合を答えてください。
- 設定のベストプラクティスと最も異なるカテゴリはどれか？
- ネットワークに最も大きなリスクをもたらす設定の変更と、推奨される修正措置は何ですか。
- 重大度が高い構成と重要な構成の偏差の最大値を持つ資産はどれですか。推奨される修正措置は何か？

- 重要度の高い構成の相違の資産重要度ごとの内訳を表示します
- 構成のベストプラクティスルールの詳細（重大度、カテゴリ、およびソフトウェアタイプ別の偏差）を表示します。

「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。

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。