Cisco Crosswork Hierarchical Controller 7.0

アドミニストレーション ガイド

2023 年 4 月

はじめに

このドキュメントは、Cisco Crosswork Hierarchical Controller プラットフォーム、バージョン 7.0 の構成に関する管理ガイドです。インストールの詳細については、『*Cisco Crosswork Hierarchical Controller Installation Guide*』を参照してください。

このドキュメントでは、次の項目を説明しています。

- セキュリティアーキテクチャ
- セキュリティと管理
- Notification Manager を含むシステムの正常性
- データベースのバックアップと復元
- HA クラスタ管理
- デバイス管理（ログイン情報、アダプタ、管理対象デバイス）
- モデル設定（地域、タグ、イベント）
- リンク管理

セキュリティアーキテクチャ

このセクションでは、Cisco Crosswork Hierarchical Controller が高度に保護され、リスクや脆弱性なしで安全に展開できるようにするためにシスコが使用する、セキュリティ アーキテクチャ、機能セット、構成、プラクティスに関する情報を提供します。シスコは、業界で一般的に許容されている開発とプラクティスに継続的に従い、Cisco Crosswork Hierarchical Controller を更新することで常に反映させています。

このセクションでは、カテゴリ別の機能セット、リスクを軽減するための構成、サポートされている標準、開発と展開のプロセスについて詳しく説明します。Cisco Crosswork Hierarchical Controller のセキュリティでは、各論理要素が異なるセキュリティを提供するレイヤードアーキテクチャに基づいており、各セキュリティステップは次のステップの前提条件です。たとえば、ユーザー認可は、すでに認証されているユーザーに対してのみ行われます。

NGINX Web サーバーは、Cisco Crosswork Hierarchical Controller がインストールされているデバイスの外部からアクセスできる唯一のコンポーネントです。HTTP および SQL 接続はローカルインターフェイスにバインドされた内部接続であり、Cisco Crosswork Hierarchical Controller がインストールされているデバイスの外部からはアクセスできません。さらに、各論理要素は Docker コンテナ内で実行されます。つまり、各ボックスはサンドボックス化されており、許可されている明示的な接続を除き、他のボックスやオペレーティング システムにはアクセスできません。

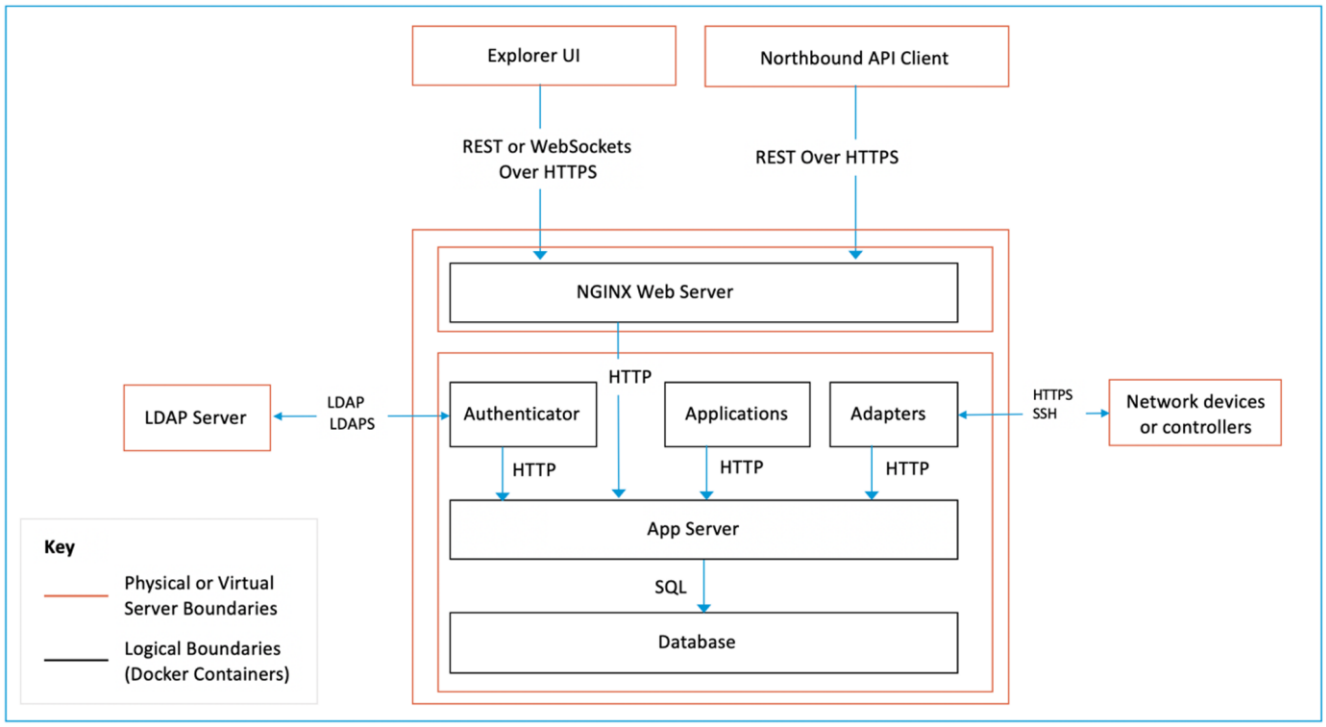


図 1.
Cisco Crosswork Hierarchical Controller のセキュリティアーキテクチャ

アーキテクチャの概要

NGINX Web サーバー

Cisco Crosswork Hierarchical Controller は、NGINX Web サーバーの背後に展開されたアプリケーションサーバーで実行されます。NGINX Web サーバーはリバースプロキシサーバーとして構成され、Cisco Crosswork Hierarchical Controller アプリケーションサーバーへのすべてのリクエストを傍受し、セキュリティ攻撃に対する防御の最前線として機能します。

NGINX Web サーバーは、ポート 443 で HTTPS パケットのみを許可します。HTTP トラフィックはリバースプロキシによって排除され、HTTPS にリダイレクトされるため、HTTP トラフィックが Cisco Crosswork Hierarchical Controller アプリケーションサーバーにすることはありません。

NGINX Web サーバーは、NGINX の ngx_http_auth_request_module を使用して、Cisco Crosswork Hierarchical Controller オーセンティケーターへのクライアントの認可を実行します。

認証フレームワーク

Cisco Crosswork Hierarchical Controller の認証フレームワークは、包括的な一連の認証戦略をサポートする認証ミドルウェアである Passport です。

パスワードの保存

ローカル認証の場合、パスワードは、一方向の関数である安全なソルト付きパスワードハッシュを使用してデータベースに保存されます。ソルトは、パスワードをハッシュ化する関数へのインプットとして使用されるランダムなデータであり、辞書攻撃を防ぎます。これにより、パスワード ファイルが侵害された場合でもパスワードが保護されるため、セキュリティが大幅に向上します。

使用されるハッシュ関数は、Blowfish 暗号を基盤とする bcrypt です。レインボーテーブル攻撃から保護するためのソルトの追加に加えて、bcrypt は、Cisco Crosswork Hierarchical Controller が計算能力の高い総当たり攻撃に対する耐性を維持できるようにする適応機能です。

コンテナ

Cisco Crosswork Hierarchical Controller は、Docker コンテナを使用して、アプリケーションとアプリケーションサーバーのプロセスを展開および実行します。高レベルのデータベースセキュリティを維持するために、コンテナは 2 つの別々のネットワークに展開されます。アプリケーションサーバーとデータベースは 1 つのネットワークに展開され、残りのすべてのコンテナは別のネットワークに展開されます。そのため、アプリケーションサーバーのみがデータベースにアクセスできます。

コンテナのデバッグ レベルは、最初は **INFO** に設定されています。

データベース

Cisco Crosswork Hierarchical Controller は、データベースに Postgres を使用します。データベースへのアクセスは、ユーザーごとに暗号化されたパスワードによって制限されます。ネットワーク要素の詳細やユーザーのログイン情報などの機密データのテーブルは、すべて暗号化されます。

暗号化には AES256 を使用します。

ユーザーアクセスと認証

Cisco Crosswork Hierarchical Controller は、外部 LDAP サーバと通信することで、または Cisco Crosswork Hierarchical Controller で定義されたユーザに対してはローカルに通信することでユーザを認証します。

システムにアクセスする各ユーザーは、一意に認証されます。

各ユーザーは、同時に複数のセッションを開くことができます。

Cisco Crosswork Hierarchical Controller のユーザーはプラットフォームリソースのみにアクセスでき、プラットフォームから基盤となる OS へアクセスすることはできません。

ホスト OS と Cisco Crosswork Hierarchical Controller プラットフォームのアクセス管理は、個別に管理されます。

ユーザー グループ

ユーザーグループは LDAP サーバーで定義でき、アクセス許可時に Cisco Crosswork Hierarchical Controller に渡されます。これらのグループは、ユーザーロールにマッピングされます（詳細については、「認証」を参照してください）。

ローカル ユーザ（Local Users）

Cisco Crosswork Hierarchical Controller では、ローカルユーザーを作成できます。

ベストプラクティスとして、ローカル定義のユーザーは管理者ユーザーのみに限定することが推奨されます。

パスワードポリシーの設定

ローカルユーザーに強制されるパスワードの強度は有効または無効にすることができ、1 ~ 5（弱いから強い）のスコアで設定できます。指定されたパスワードは、選択されたスコアに応じた複雑さを保証するために、いくつかのディクショナリおよび一般的なパスワードリストに対してチェックされます。

二要素認証

二要素認証は現在、デフォルトパッケージには含まれていません。ただし、必要に応じてプロフェッショナルサービスとして追加できます。

LDAP サーバーとの通信

LDAP アプリケーションプロトコルは、分散型ディレクトリ情報サービスにアクセスして維持するための、ベンダーに依存しないオープンな業界標準です。LDAP 認証は、通信が暗号化されたトランスポート接続を介して行われることを除けば同様です。

管理者のオプション

管理者はログインバナーを設定できます。

管理者は、アクティブなユーザーをブロックおよびブロック解除し、アイドルセッションの有効期限を設定できます。

SAML

複数の Crosswork プラットフォーム アプリケーションで同じ SAML サーバーが使用されている場合、ユーザーは 1 回ログインするだけで済みます。その後、再度ログインすることなく、他の Crosswork プラットフォーム アプリケーションを使用できます。SAML サーバーはお客様のサーバーです（Crosswork Hierarchical Controller プラットフォームの一部ではありません）。

ユーザーのロックアウトポリシー

設定可能な回数のログインに失敗すると、ユーザーはブロックされます。ブロック期間は短い期間から始まり、ログインに失敗するたびに長くなります。

デフォルトのログイン試行回数は 8 回です。

この期間中、ユーザーの IP アドレスからのログイン試行は処理されません。

認証フロー

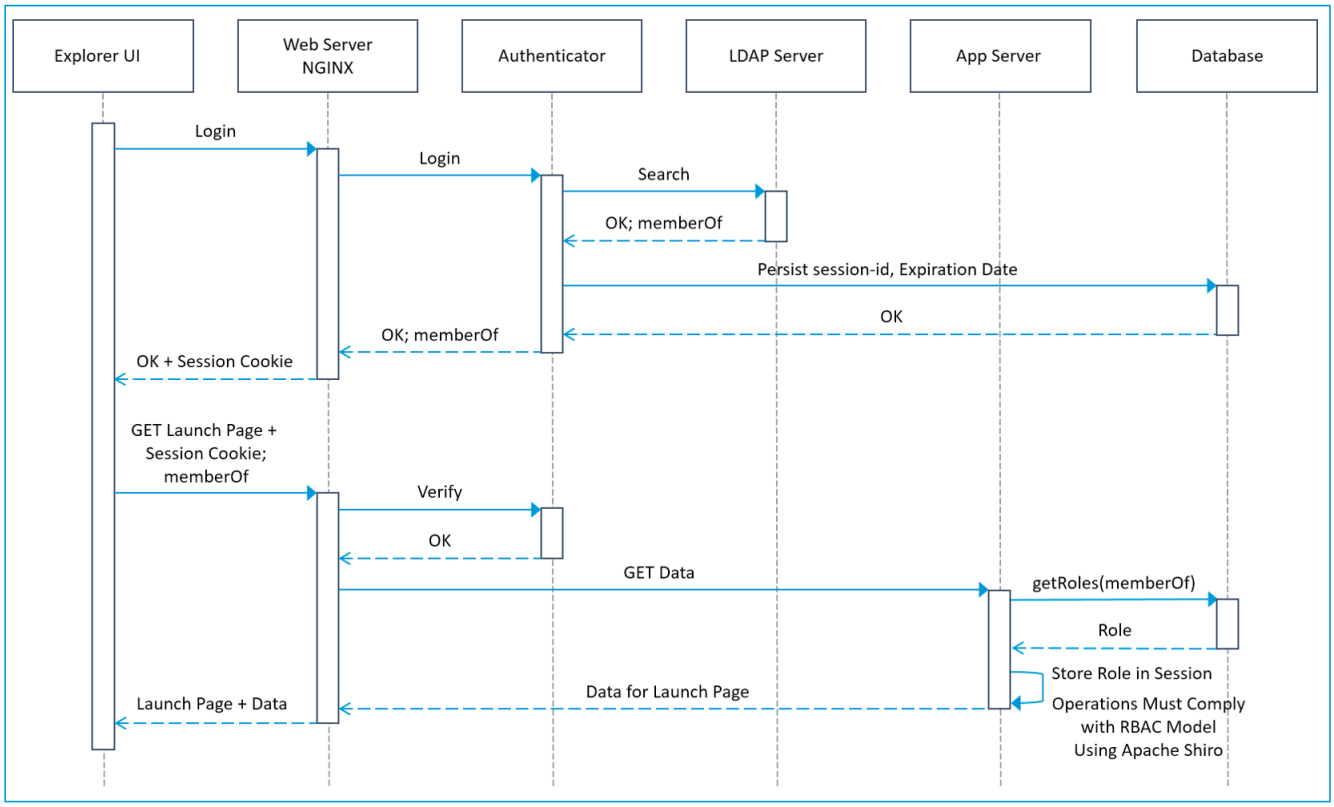


図 2.
Cisco Crosswork Hierarchical Controller の認証フロー

Cisco Crosswork Hierarchical Controller は、ロールベース アクセス コントロール（RBAC）をサポートします。これにより、各ユーザー（ローカルに定義されたユーザーまたは LDAP ユーザー）を個別にロールに割り当てることができます。次の Cisco Crosswork Hierarchical Controller ロールを使用できます。

Cisco Crosswork Hierarchical Controller のロール	権限
読み取り専用	Cisco Crosswork Hierarchical Controller Explorer UI への読み取り専用アクセス。
ユーザ	Cisco Crosswork Hierarchical Controller Explorer UI およびすべてのアプリケーションへのアクセス。一部はネットワークを変更可能。
管理者	構成とすべてのユーザーに対する完全な管理権限。 構成 UI、Cisco Crosswork Hierarchical Controller Explorer UI、およびすべてのアプリケーションへのアクセス。
サポート	ユーザーロールと同じ権限だが、シスコサポートチーム用の Cisco Crosswork Hierarchical Controller 診断ツールへのアクセス権が追加される。

ユーザーへのロールの割り当て

Cisco Crosswork Hierarchical Controller の管理者は、Cisco Crosswork Hierarchical Controller が LDAP サーバーに接続してクエリを実行するために使用する、バインド DN とパスワードを提供します。管理者は、検索ベース、検索フィルタ、および LDAP グループと Cisco Crosswork Hierarchical Controller ロール間のマッピングも構成します。このマッピングポリシーは、Cisco Crosswork Hierarchical Controller Explorer UI にログインできるユーザーと、そのロールを特定します。検索ベースと検索フィルタ基準の両方を満たすすべてのユーザーは、グループに割り当てられたロール（アクセス権限）でログインすることが許可されます。ユーザーが Cisco Crosswork Hierarchical Controller ロールにマッピングされているグループのメンバーでない場合、ログインの試行は拒否されます。

Cisco Crosswork Hierarchical Controller の管理者は、LDAP によって処理されないローカルユーザーにもロールを割り当てます。ローカルユーザーと LDAP サーバーへのアクセスの両方を無効にして、認証と認可にいずれか一方の方法を使用できるようにできます。

VM とコンテナへのアクセス

VM レベル

Cisco Crosswork Hierarchical Controller は、適切な OS バージョンと HW リソースが割り当てられた任意の VM でホストされる Docker コンテナにインストールされた、複数のマイクロ サービスにインストールされます。

VM OS レベルでのアクセス制限は運用者の責任で行なってください。

ホスト OS を介した Cisco Crosswork Hierarchical Controller への通信には、暗号化されたプロトコル（UI/NBI には HTTPS/WS 保護、ホスト OS を介した高度な管理には SSH）が使用されます。

以下に列挙するように、Cisco Crosswork Hierarchical Controller には VM で次の特定のポートのみを開きます。

方向	ポート	説明
着信	TCP 22	SSH リモート管理
	TCP 80	UI アクセス用の HTTP（HTTPS へのリダイレクト）
	TCP 443	UI アクセス用の HTTPS
発信	TCP+ 22	ルータへの NETCONF

方向	ポート	説明
	UDP 161	ルーターおよび/または ONE への SNMP
	TCP 389	LDAP（アクティブディレクトリを使用している場合）
	TCP 636	LDAPS（アクティブディレクトリを使用している場合）
	顧客固有（Customer Specific）	SDN コントローラにアクセスするための HTTP
	顧客固有（Customer Specific）	SDN コントローラにアクセスするための HTTPS

VM および NGINX サーバーへのアクセスは、初期インストール時に特定の IP アドレスとポート（ホワイトリスト）に制限できます。

コンテナ

Cisco Crosswork Hierarchical Controller はコンテナに Alpine OS を使用し、1 つのポートのみを使用して localhost をリッスンします。

ノースバウンド インターフェイスでの HTTP アクセス

Cisco Crosswork Hierarchical Controller の管理インターフェイスは、保護されたインターフェイスを使用します。GUI と NBI 両方のアプリケーションレベル管理に向けた管理インターフェイスで、HTTPS /Secure WebSocket が使用されます。

Cisco Crosswork Hierarchical Controller UI および Web サービスへの Web アクセス（REST コマンド）は、SSL および X509 バージョン 3 の証明書で保護されます。

URL には、ユーザーのログイン情報やデバイスの機密情報は含まれません。

サウスバウンド インターフェイスでのアクセス

Cisco Crosswork Hierarchical Controller と NE/NMS 間のすべての制御トラフィックは暗号化されます。

これは、暗号化されたインターフェイスを提供する NE/NMS の機能に依存します。ベストプラクティスのポリシーとして、シスコは NE/NMS が提供する最も安全なインターフェイス/プロトコルを選択します。

監査証跡ログ（アカウンティング）

アプリケーションでのすべてのユーザーのログイン/ログアウトおよび操作アクティビティは監査され、ログに記録され、外部システムにエクスポートできます。監査ログには、ユーザー名、ホスト名、時刻、操作、特定の情報、結果が含まれます。

イベントと通知

システムイベントは Cisco Crosswork Hierarchical Controller DB に保存され、SHQL コマンドを介してアクセスできます。次の機能が含まれています。

- ログイン/ログアウトセッション
- アプリケーション アクティビティ
- ネットワークインベントリとトポロジの更新

イベントは、カテゴリに応じて複数の宛先に SYSLOG として送信できます。

EU データ保護指令

ネットワークコントローラである Cisco Crosswork Hierarchical Controller はネットワークデータを処理しますが、EU データ保護指令で規定される GDPR で定義されている「自然人」に関連したデータは処理しません。さらに、サポート チケットに対処する場合、シスコは最大でもデータ処理者であり、サービスプロバイダーのお客様は引き続き Cisco Crosswork Hierarchical Controller を利用するデータ管理者、データ処理者です。「自然人」に関連する個人データは取り扱いません。

開発セキュリティ手順

Cisco の継続的インテグレーションによるビルドプロセスでは、セキュリティチェックを含む静的チェックを実行します。静的分析は、セキュリティ警告などの重大度の高い警告がある場合、ビルドの続行を許可しません。継続的インテグレーションプロセスでは、統合テストの目的で自動的に展開される Cisco Crosswork Hierarchical Controller のインスタンスに対する Web サーバースキャナも実行されます。

OWASP[1] によって参照されるセキュリティツールは、FindBugs、Find Security Bugs プラグイン、および SSL 構成を検証する Test-ssl です。

- FindBugs は、静的分析を使用して Java コードのバグパターンを検出するオープンソースツールです。潜在的なエラーはランク付けされているため、開発者は起こりうる影響や重大度を容易に理解できます。FindBugs が使用する主な手法の 1 つは、ソースコードを既知の疑わしいプログラミングプラクティスに構文的に一致させることです。
- Find Security Bugs は、Java Web アプリケーションのセキュリティ監査用の FindBugs プラグインです。200 を超える固有のシグネチャを持つ 86 の異なる脆弱性タイプを検出できます。OWASP トップ 10 および CWE2 の参照とともに、各バグパターンについて広範な参照が提供されます。
- Test-ssl は、TLS/SSL 暗号のサポート、プロトコル、最近の暗号化の欠陥などについて、任意のポートでサーバーのサービスをチェックするコマンドラインツールです。

セキュリティパッチ更新ポリシー

シスコは、Cisco Crosswork Hierarchical Controller ソフトウェアおよびその展開コンポーネントによって使用されるすべてのソフトウェアライブラリとイメージがセキュリティの脅威から完全に保護され、サービス プロバイダー ネットワーク内の他のシステムに対するマルウェアやウイルスのリスクを発生させないことを保証する責任があります。

Cisco Crosswork Hierarchical Controller ソフトウェア保護へのプロアクティブな取り組み

このコミットメントを果たし、この記述に準拠するために、シスコは本書に記載する必要な手順を実行します。手順は設計段階、新しいコンポーネントを選択して使用前に認定するとき、そのようなコンポーネントにアップグレードが必要なとき、およびセキュリティパッチがプロアクティブにリリースされるときに実行されます。これらのテストでは、Clair を使用してコンテナの脆弱性をチェックします。

---

[1] OWASP（Open Web Application Security Project）は、Web アプリケーションのセキュリティに重点を置いた組織です。その取り組みの 1 つは、上位 10 の脆弱性のリストを公開することです。

[2] CWE（Common Weakness Enumeration）は、統一された、測定可能なソフトウェアの弱点情報を提供する国際組織です。

新しいソフトウェアコンポーネントの認定

Cisco Crosswork Hierarchical Controller、コンテナ化されたホスト、データベース、オペレーティングシステムによるソフトウェアライブラリまたはイメージの使用は、使用前に、選択過程の一環としてシスコによるセキュリティ認証の対象となります。

認証プロセスでは、公式の通知をレビューし、次の条件を満たしていることをテストで確認します。

- ウェルノウンポートである。
- すべての通信が認証付きの安全なプロトコル（SSH、HTTPS、TLS v1.2/1.3、SFTP）によって行われている。
- スーパーユーザーまたは管理者権限の使用がない。
- API へのアクセスに認証が必要。
- 内部でプロセス間に認可が実施されている。
- パスワードルールが適用される。
- セキュリティテストの結果が公開されている。

シスコは常に、最高のセキュリティレベルを備えたソフトウェアライブラリと製品を優先しています。代替ソフトウェアがない場合は、使用を制限して慎重に使用し、このソフトウェアによって引き起こされる可能性のある潜在的なリスクについてリリースノートで通知します。

プロアクティブなパッチ更新ポリシー

シスコは使用中の、または Cisco Crosswork Hierarchical Controller と相互作用する、関連するオープンソース ソフトウェア ライブラリおよびエンタープライズ ソフトウェア製品を継続的に追跡します。必要に応じて、完全なリストをシスコから取得できます。

追跡の目的は、セキュリティホールに関連するパッチの更新またはアラート、またはこのソフトウェアによってユーザーにもたらされる脅威があるかどうかを把握することです。

シスコのエキスパートは、Cisco Crosswork Hierarchical Controller で使用する潜在的なリスクを調査し、重大度と実行するアクションを決定します。緊急度に基づいて、以下を実行することが決定されます。

- アラートがある場合 – 導入しているすべてのお客様に公式の情報通知を生成します。このような通知によって、シスコが状況を認識しており、パッチのリリースによる問題の解決に取り組んでいることをお客様に知らせます。復旧が計画されていない場合、シスコはコンポーネントの交換を検討する場合があります。
- パッチがリリースされたとき – パッチによって修復された脅威が Cisco Crosswork Hierarchical Controller ユーザーに影響を与えることが判明した場合です。シスコはパッチ更新のプロセスを開始します。このプロセスには以下が含まれます。1) R&D ラボでのパッチへのアップグレード、2) セキュリティおよび Cisco Crosswork Hierarchical Controller の機能に害を与えない円滑な動作を確認するための適切な品質テスト、3) すべての Cisco Crosswork Hierarchical Controller ユーザーへの正式な通知としてのパッチのリリース。パッチ更新に関する正式な通知は、その重大度に応じて、電子的または直接提供されます。

リアクティブなパッチ更新ポリシー
非常にまれなケースですが、Cisco Crosswork Hierarchical Controller ユーザーがセキュリティ上の脅威を発見し、シスコに警告することがあります。

シスコは、報告された脅威がソフトウェアと環境に与える影響を直ちに評価し、評価することに全力を尽くしています。シスコは結果をお客様と共有し、被害を避けるために必要な措置を講じます。この手順では、Cisco Crosswork Hierarchical Controller のパッチ更新が必要な場合があります。この場合、シスコは、ユーザーによるセキュリティパッチを使用した独立アップグレードが許可されているかどうかをユーザーに通知します。

テスト
Cisco Crosswork Hierarchical Controller のソフトウェアコンポーネントのセキュリティパッチはテストされ、機能に影響がないことが確認されます。結果として制限が発生する場合は、パッチリリースノートで報告されます。

承認
テストの結果およびソフトウェアの安定性と品質に対するリスクの評価に基づいて、パッチ配信は担当のセキュリティおよび IT チームによってレビューされ、現場チームがインストールを続行することが承認されます。承認は配信の正式な手順であり、パスのリリースノートに承認者の名前が記載されます。

配信
セキュリティおよびその他の目的のためのパッチの配信後、シスコからすべてのユーザへの正式な通知が出されます。セキュリティパッチが宣言され、適切なドキュメントとともにリリースされ、無料であり、特定のメンテナンス契約に関連付けられていないことが伝達されます。

メンテナンス契約に従ってシスコによる継続的なサポートを受けるために、また Cisco Crosswork Hierarchical Controller の新しいバージョンにアップグレードするために、最新のセキュリティパッチへのアップグレードが必須であることに注意してください。

セキュリティと管理

証明書のインストール

有効な証明書の取得は、2 段階のプロセスです。まず、証明書リクエスト（CSR）を生成します。次に、このファイルを CA（お客様の IT チーム）が使用して、サーバーにインストールする信頼できる証明書（PEM/CRT）を生成します。

CSR を生成する前に、展開されたシステムの正確な URL が必要です（例: cisco.corp.com）。これは、証明書の共通名（CN）です。

CSR を生成するには、次の手順を実行します。

1. Cisco Crosswork Hierarchical Controller サーバーのコマンドラインにアクセスします（通常は SSH を使用）
2. root としてログインしていることを確認します。別のユーザーとしてログインしている場合は、次を実行します。

   ```
   sudo su -
   ```

3. CSR 用のフォルダを作成します。

   ```
   mkdir /usr/local/etc/sedona/ssl
   ```

4. 作成したフォルダへのパスを変更します。

```
cd /usr/local/etc/sedona/ssl
```

5. 新しい DH パラメータファイルを生成します（これには数分かかる場合があります）。

```
openssl dhparam -out dhparam.pem 2048
```

証明書のインストール方法

1. CA から受け取った PEM ファイルを次の場所にコピーします。

```
/usr/local/etc/sedona/ssl/new_certificate.pem
```

2. システムを再起動します。

```
sedo system restart
```

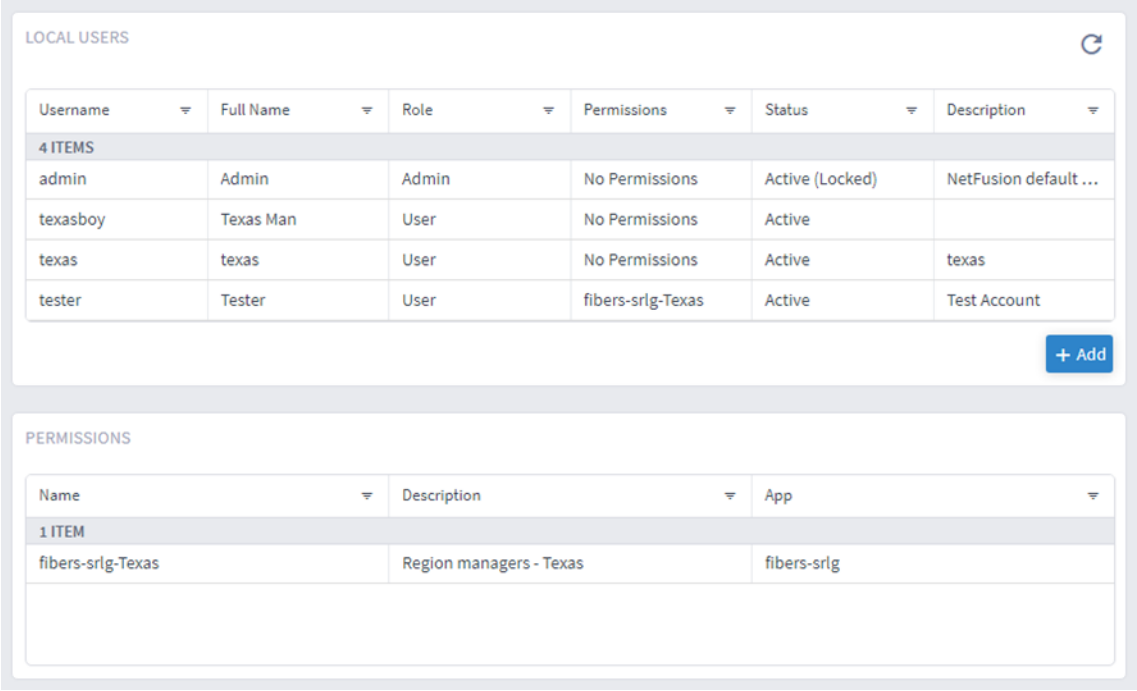
ユーザー管理

Crosswork Hierarchical Controller はローカルユーザーの作成とメンテナンス、および Active Directory（LDAP）サーバーとの統合をサポートします。ローカルユーザーを作成し、ロールと権限を割り当てることができます。管理者は、ローカルユーザーのパスワードに対するパスワード複雑性のルール（OWASP）を選択することもできます。スコアレベルを選択することにより、パスワードの長さと文字構成が適用されます。

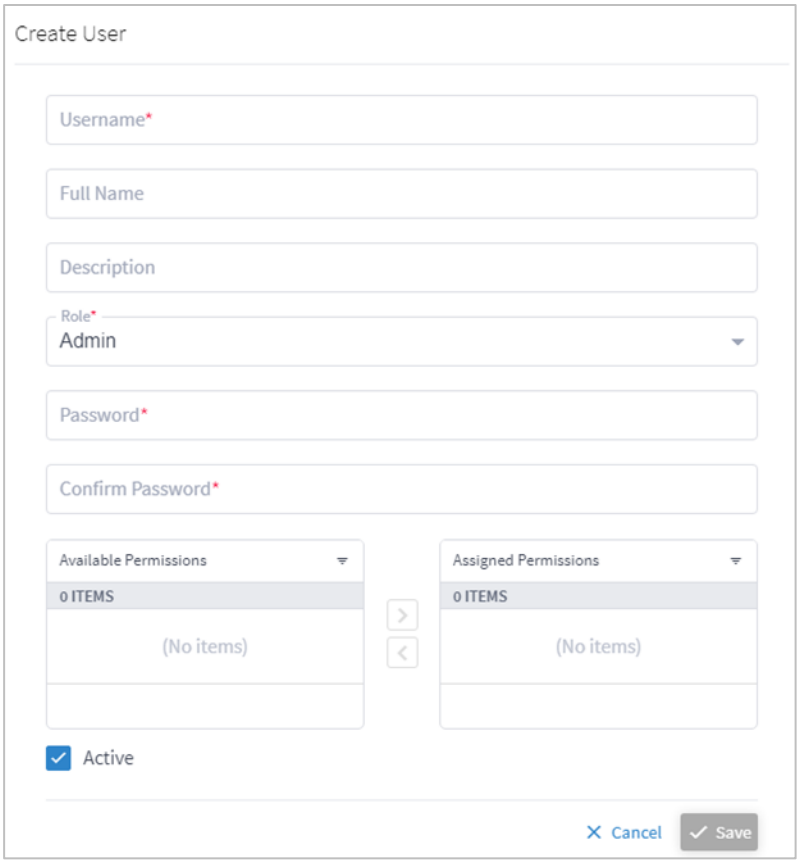
Crosswork Hierarchical Controller のロール	権限
読み取り専用（ReadOnly）	Crosswork Hierarchical Controller Explorer UI への読み取り専用アクセス。
ユーザ	Crosswork Hierarchical Controller Explorer UI およびすべてのアプリケーションへのアクセス。一部はネットワークを変更可能。
Admin	構成とすべてのユーザーに対する完全な管理権限。 構成 UI、Crosswork Hierarchical Controller Explorer UI、およびすべてのアプリケーションへのアクセス。
サポート	ユーザーロールと同じ権限だが、シスコサポートチーム用の Crosswork Hierarchical Controller 診断ツールへのアクセス権が追加される。

ユーザーを追加/編集するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[設定（Settings）] を選択します。
2. [セキュリティ設定（Security Settings）] をクリックします。



3. [ローカルユーザー（LOCAL USERS）] で、[追加（Add）] をクリックするか、既存のユーザーをクリックします。



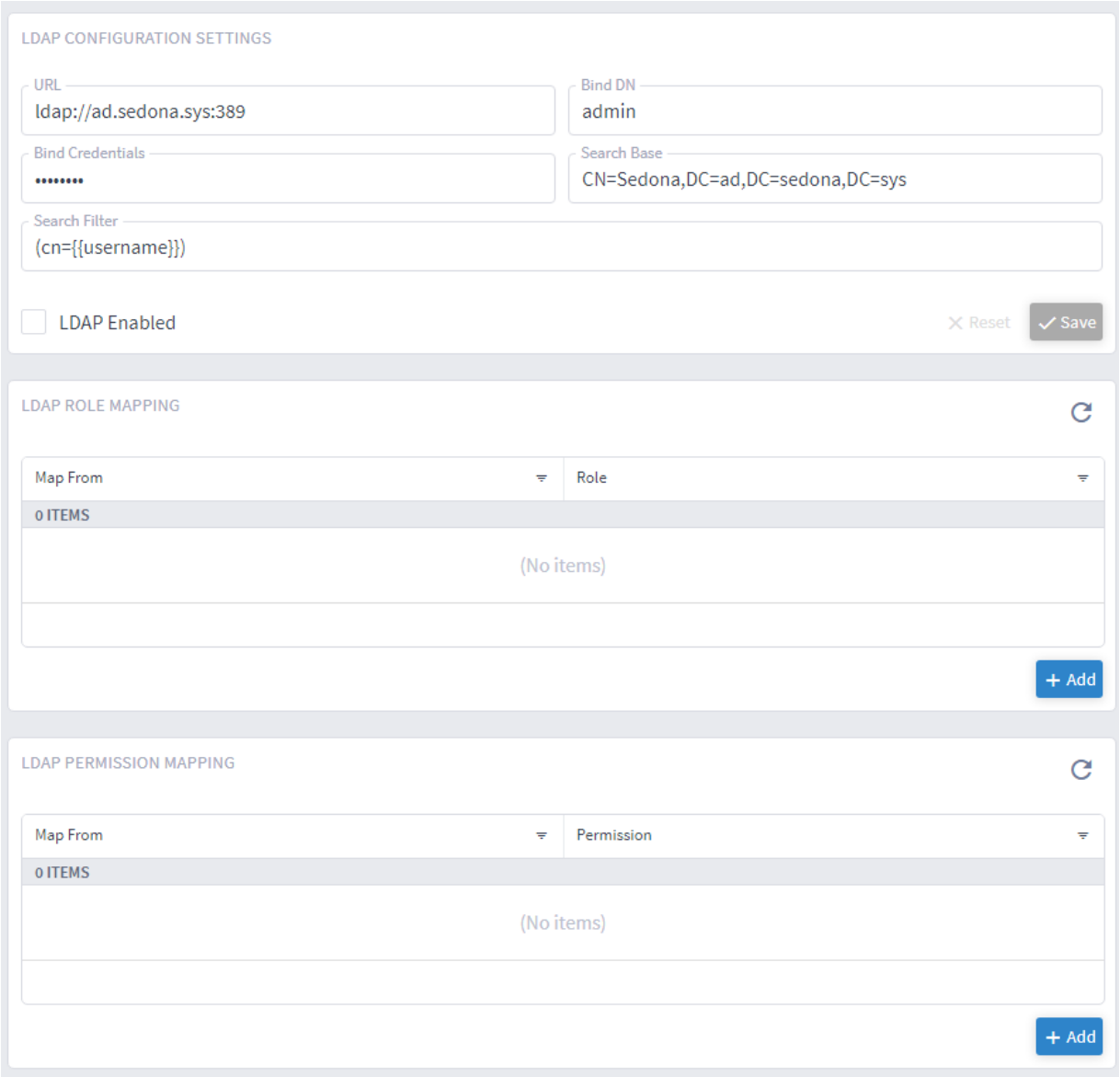
4. フィールドに入力し、必要な権限を割り当てます。
5. [保存（Save）] をクリックします。

Active Directory

Crosswork Hierarchical Controller は、LDAP サーバー経由でユーザーを認証できます。

LDAP サーバーを構成するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[設定（Settings）] を選択します。
2. [セキュリティ設定（Security Settings）] をクリックします。



3. [アクティブディレクトリ（ACTIVE DIRECTORY (LDAP)）] 設定を構成します。
4. [保存（Save）] をクリックします。

SAML

Crosswork Hierarchical Controller では、サービスプロバイダーモードで SAML サーバーを使用してシングルサインオン（SSO）できます。

SSO を使用している場合、Crosswork Hierarchical Controller からログアウトしても、SAML サーバーからはログアウトされません。これは、同じ SAML サーバーログインを使用する他のアプリケーションで引き続き作

業できることを意味し、SAML セッションがアクティブなときに HCO を再起動した場合、再度ログインする必要はありません。

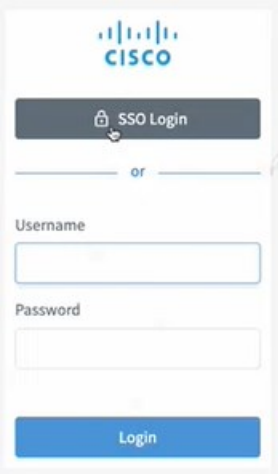
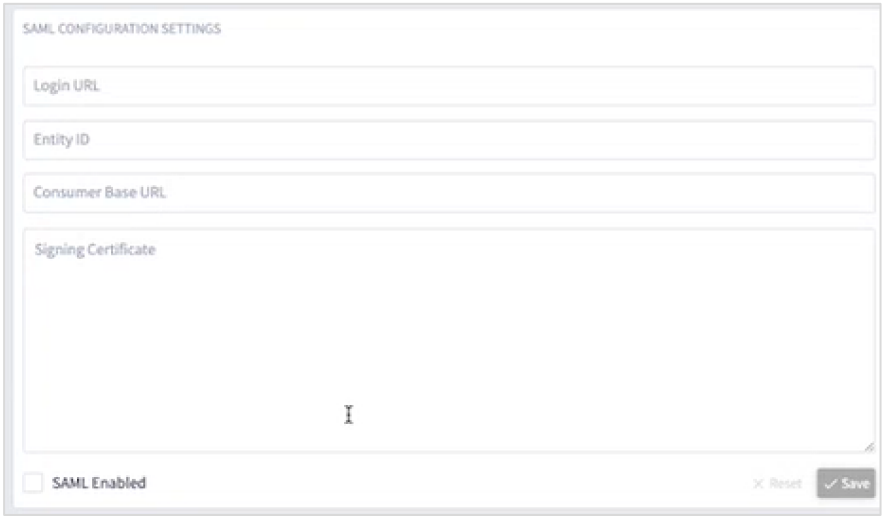


図 3.
Cisco Crosswork Hierarchical Controller SSO ログインまたは Crosswork Hierarchical Controller ログイン

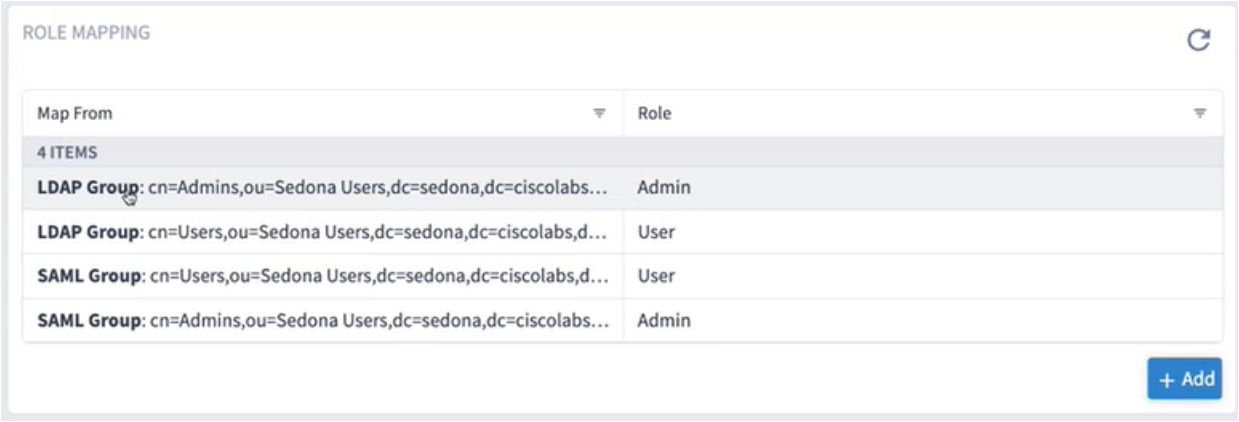
SAML を設定するには、次の手順を実行します。

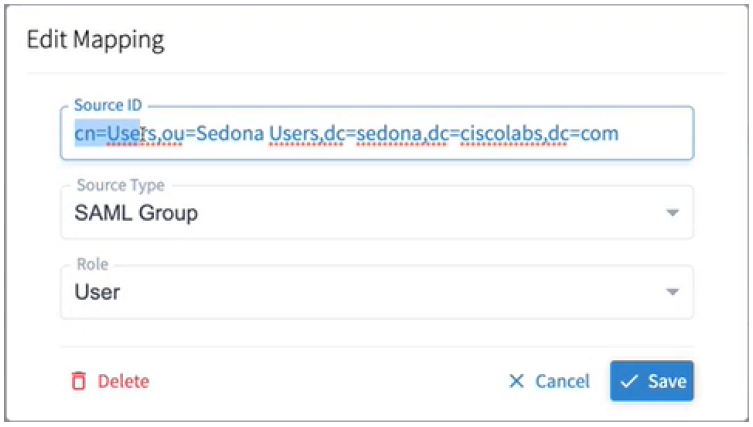
1. Crosswork Hierarchical Controller のアプリケーションバーで、[設定（Settings）] を選択します。
2. [セキュリティ設定（Security Settings）] をクリックします。



3. [SAML 構成設定（SAML CONFIGURATION SETTINGS）] を設定します。
   - [ログイン URL（Login URL）] : SAML サーバーの URL。
   - [エンティティ ID（Entity ID）] : SAML エンティティのグローバルに一意の名前。
   - [コンシューマーベース URL（Consumer Base URL）] : ユーザーがログインしたときにユーザーをリダイレクトする URL、つまり HCO インスタンス。
   - [署名証明書（Signing Certificate）] : SAML サーバーでの認証に使用される証明書。
4. [SAML が有効（SAML Enabled）] を選択します。

5. [保存（Save）] をクリックします。
6. [ロールマッピング（ROLE MAPPING）] で、[ユーザー（User）] ロールと [管理者（Admin）] ロールの [SAML グループ（SAML Group）] ロールを設定します。





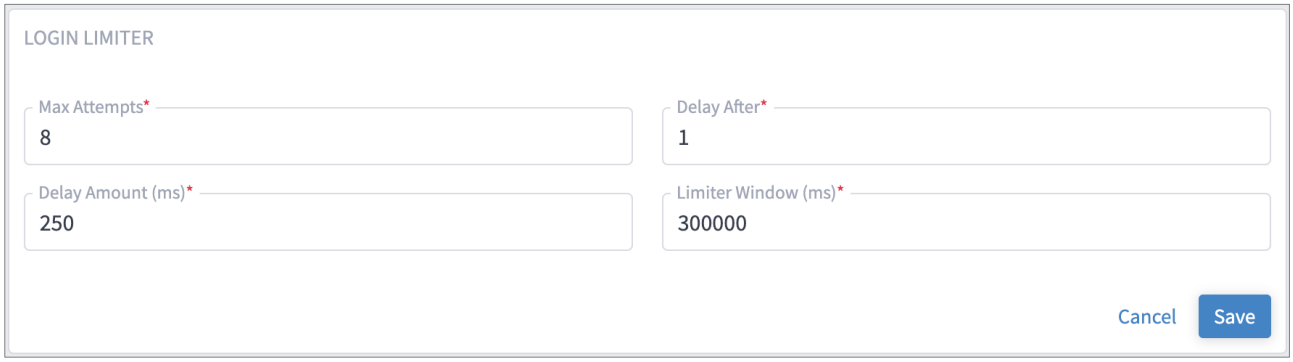
7. [保存（Save）] をクリックします。

ログイン制限

サービス拒否や総当たり攻撃を避けるために、ユーザーによるログインの試行回数を制限できます。

ログイン制限を構成するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[設定（Settings）] を選択します。
2. [セキュリティ設定（Security Settings）] をクリックします。



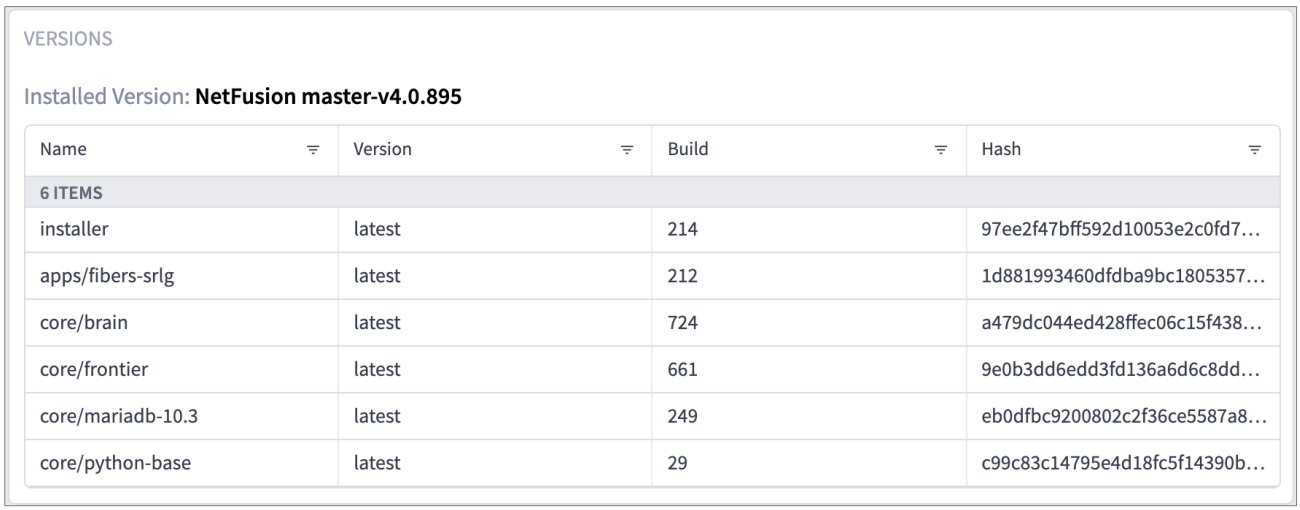
3. [ログイン制限（LOGIN LIMITER）] 設定を構成します。
    - [最大試行回数（Max Attempts）]： 最大ログイン試行回数。
    - [この回数後に遅延（Delay After）]：遅延処理が適用されるまでのログイン試行失敗の回数。
    - [遅延時間（ミリ秒）（Delay Amount (ms)）]：次のログイン試行が許可されるまでの時間（ミリ秒）。
    - [制限時間（ミリ秒）]：最大試行回数を超えた後、ログインが許可されない時間。通常は 300000 ミリ秒または 5 分に設定します。
4. [保存（Save）] をクリックします。

システムの状態

システム情報の表示

システム情報を表示するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[設定（Settings）] を選択します。



2. [システム情報（System Info）] の [バージョン（VERSIONS）] テーブルにインストールされているパッケージとそのビルド番号が表示されます。

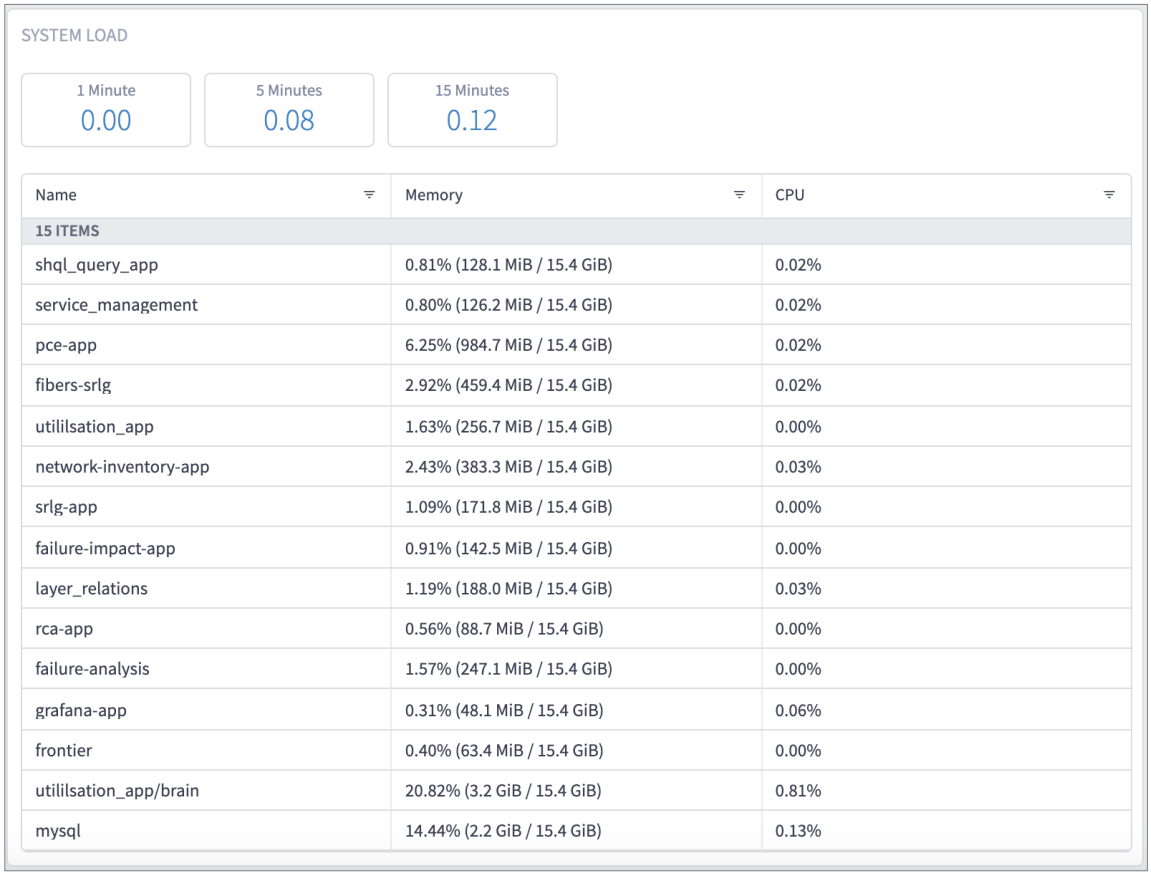
システムの CPU 負荷の表示

Crosswork Hierarchical Controller プラットフォームのパフォーマンスを追跡し、UI でシステムの CPU 負荷とディスク使用量を確認して、パフォーマンスの低下を引き起こしたり、特定の機能をブロックしたりする可能性のあるサービスを分離できます。

システム負荷を表示するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[設定（Settings）] を選択します。
2. [システム情報（System Info）] では、[システム負荷（SYSTEM LOAD）] 情報はデフォルトで 2 分ごとに更新されます。
    - 3 つの長方形の値は、過去 1 分、5 分、および 15 分に Crosswork Hierarchical Controller によって使用された CPU のパーセンテージ（サーバー負荷平均）を示します。

- 列には、各 Crosswork Hierarchical Controller プロセスによって現在使用されているメモリと CPU の割合が表示されます。



Name	Memory	CPU
15 ITEMS		
shql_query_app	0.81% (128.1 MiB / 15.4 GiB)	0.02%
service_management	0.80% (126.2 MiB / 15.4 GiB)	0.02%
pce-app	6.25% (984.7 MiB / 15.4 GiB)	0.02%
fibers-srlg	2.92% (459.4 MiB / 15.4 GiB)	0.02%
utililsation_app	1.63% (256.7 MiB / 15.4 GiB)	0.00%
network-inventory-app	2.43% (383.3 MiB / 15.4 GiB)	0.03%
srlg-app	1.09% (171.8 MiB / 15.4 GiB)	0.00%
failure-impact-app	0.91% (142.5 MiB / 15.4 GiB)	0.00%
layer_relations	1.19% (188.0 MiB / 15.4 GiB)	0.03%
rca-app	0.56% (88.7 MiB / 15.4 GiB)	0.00%
failure-analysis	1.57% (247.1 MiB / 15.4 GiB)	0.00%
grafana-app	0.31% (48.1 MiB / 15.4 GiB)	0.06%
frontier	0.40% (63.4 MiB / 15.4 GiB)	0.00%
utililsation_app/brain	20.82% (3.2 GiB / 15.4 GiB)	0.81%
mysql	14.44% (2.2 GiB / 15.4 GiB)	0.13%

3. 別の間隔を構成するには、次のコマンドを実行します。

   ```
   sedo config set monitor.load_average.rate.secs [VALUE]
   ```

4. 画面を更新して変更を確認します。
5. 負荷平均しきい値（これを超えた場合は Syslog 通知が生成される）を設定するには、次のコマンドを実行します。

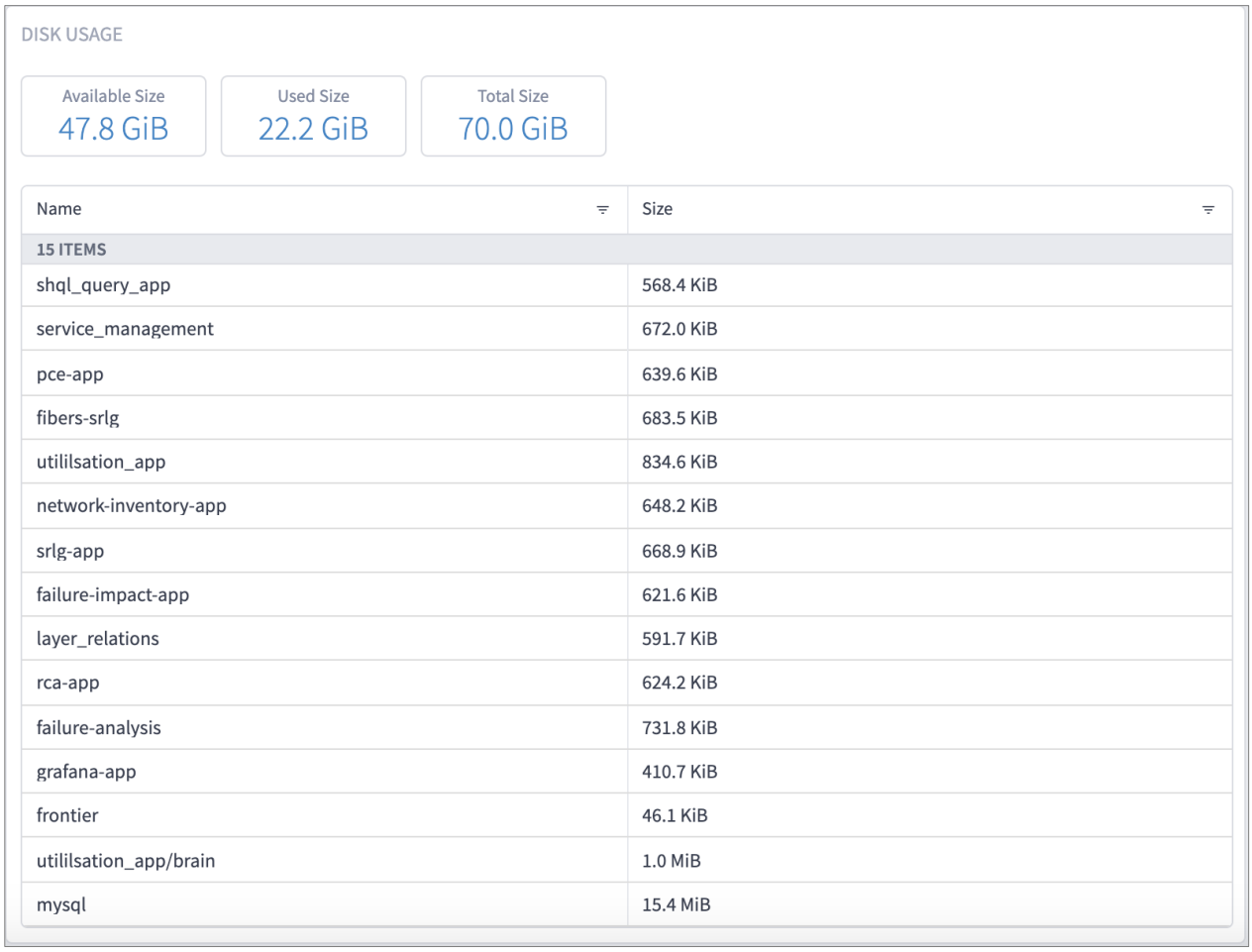
   ```
   sedo config set monitor.load_average.threshold [VALUE]
   ```

   推奨されるしきい値は、コアの数に 0.8 を掛けた値です。

ディスク使用率の表示

ディスク使用率を表示するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[設定（Settings）] を選択します。
2. [システム情報（System Info）] では、[ディスク使用率（DISK USAGE）] 情報はデフォルトで 1 時間ごとに更新されます。
   - 3 つの長方形の値は、現在のパーティションの使用可能ディスク容量な、使用されているディスク容量、合計のディスク容量を示します。
   - [サイズ（Size）] 列には、各 Crosswork Hierarchical Controller アプリケーション コンテナのサイズが表示されます（アプリケーション データを除く）。



3. 別の間隔を構成するには、次のコマンドを実行します。

   ```
   sedo config set monitor.diskspace.rate.secs [VALUE]
   ```

4. 画面を更新して変更を確認します。

5. ディスク容量のしきい値（これを超えた場合は Syslog 通知が生成される）を設定するには、次のコマンドを実行します。

   ```
   sedo config set monitor.diskspace.threshold.secs [VALUE]
   ```

   推奨されるしきい値は 80% です。

Syslog 通知

Crosswork Hierarchical Controller は、セキュリティおよびモニタリングイベントに関する Syslog 通知を複数の宛先に送信できます。

バージョン 7.0 以降、新しい Notification Manager を使用すると、SMTP を介してイベントを Syslog サーバーおよび/または Pulsar サーバーに送信できることに留意してください。

これらのイベントのカテゴリは次のとおりです。

- [すべて（All）] - セキュリティおよびモニタリング
- [セキュリティ（Security）]：すべてのログインおよびログアウトイベント
- [モニタリング（Monitoring）]：ディスク容量のしきい値、負荷平均のしきい値
- [カスタム（Custom）]：カスタムカテゴリのイベント

Crosswork Hierarchical Controller は、次のファシリティコードを含む 3 種類のメッセージを送信します。

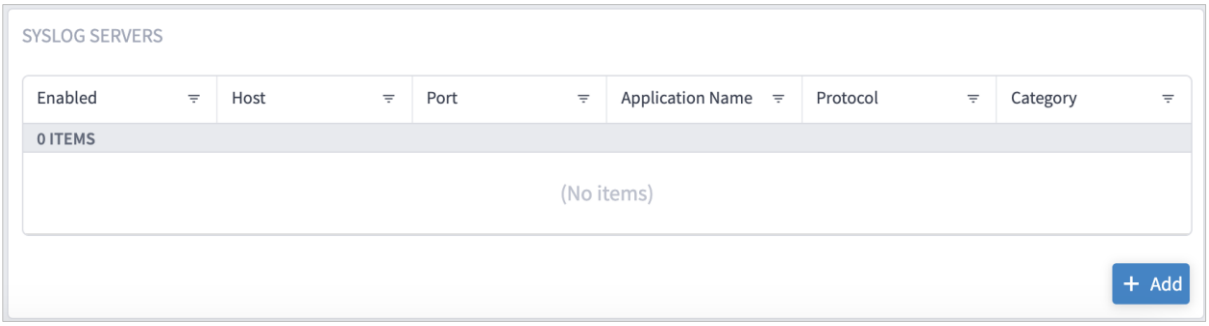
- **AUTH (4)：**/var/log/security メッセージ用。
- **LOGAUDIT (13)：**監査メッセージ用（ログイン、ログアウトなど）。
- **[USER (1)]：**他のすべてのメッセージ用。

Crosswork Hierarchical Controller は、次の場合にデバイスマネージャの Syslog イベントを送信します。

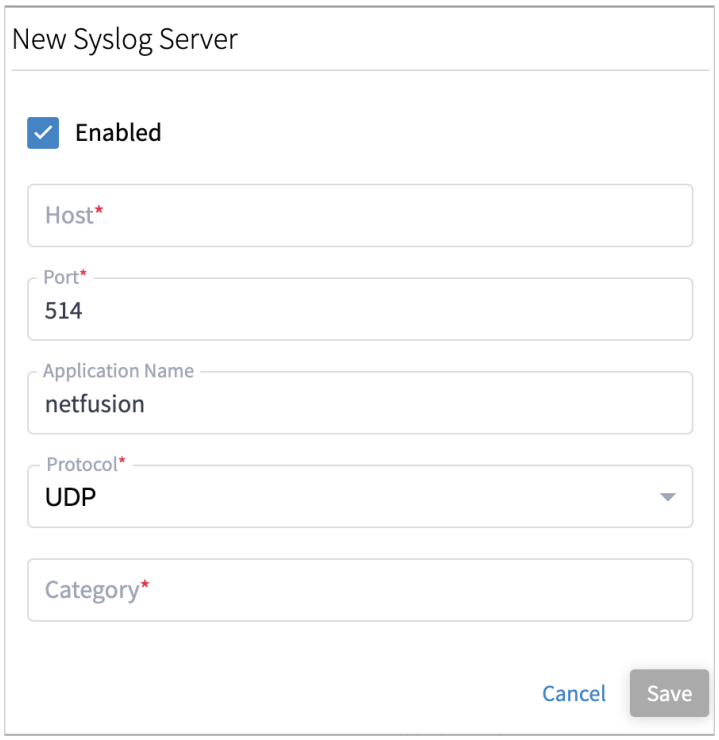
- デバイスの到達可能性状態の変更
- アダプタによるファイル解析の失敗
- アダプタがコントローラへの接続に失敗した場合。たとえば、認証の失敗または TCP 接続の失敗。

新規 Syslog サーバを追加するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[設定（Settings）] を選択します。
2. [セキュリティ設定（Security Settings）] をクリックします。



3. [Syslog サーバー（SYSLOG SERVERS）] で [追加（Add）] をクリックします。



4. 次の手順を実行します。
    - Host
    - [ポート（Port）]：514 または 601
    - [アプリケーション名（Application Name）]：フリーテキスト
    - [プロトコル（Protocol）]：TCP または UDP
    - [カテゴリ（Category）]：[すべて（All）]、[モニタリング（Monitoring）]、[セキュリティ（Security）]、[カスタム（Custom）]
5. [カスタム（Custom）] を選択した場合は、カスタムカテゴリを入力します。
6. [保存（Save）] をクリックします。

Notification Manager

イベントは、SMTP 経由で Syslog サーバーおよび/または Pulsar サーバーに送信できます。

通知を送信するための複数のルールを指定できます。たとえば、あるルールではユーザーがログインした監査イベント、別のルールではデバッグ計算イベントで通知を送信します。

次のイベントもサポートされます。

- ノード間の切り替え、アクティブノードの詳細と理由。
- スタンバイノードが応答していない。
- ウィットネスノードが応答していない。
- DB 同期に失敗した。

また、いくつかのストリームを追加して、SMTP 経由でさまざまなイベントを Syslog サーバーと Pulsar サーバーに送信することもできます。

最大 100 のイベントがキューに入れられて送信されます。キューに 100 を超えるイベントがある場合、最も古いメッセージが破棄されます。

SMTP 経由でのイベントの送信

通知でイベント情報（event.severity や event.subType など）を送信できます。

イベントを SMTP に送信するには、次の手順を実行します。

1. Cisco Crosswork Hierarchical Controller サーバーのコマンドラインにアクセスします（通常は SSH を使用）
2. root としてログインしていることを確認します。別のユーザーとしてログインしている場合は、次を実行します。

   ```
   sudo su -
   ```

3. SMTP 経由での **USER_LOGGED_IN** 監査イベントの電子メール送信を設定するには、次のコマンドを実行します。

   ```
   sedo apps state set notification-manager-app config global '
   {
      "pollIntervalSec":60,
      "upstreams":{
         "email-1":{
            "type":"smtp",
            "host":"host",
            "port":1025,
            "username":"username",
            "password":"password",
            "from":"from",
            "to":[
               "emailto"
            ],
            "subject":"HCO Event {{ event.severity }}",
            "template":"This is an urgent email about {{ event.subType }}"
         }
      },
      "rules":{
         "rule1":{
            "filter":{
               "severity":"Audit",
               "type":"Audit",
               "subType":"USER_LOGGED_IN",
               "data":{
                  "msg":"User"
               }
   ```

```
            },
            "upstream":"email-1",
            "maxRequestsPerInterval":5,
            "intervalSec":60
        }
    }
}'
```

Syslog サーバーへのイベントの送信

Syslog サーバーにイベントを送信するには、次の手順を実行します。

1. Cisco Crosswork Hierarchical Controller サーバーのコマンドラインにアクセスします（通常は SSH を使用）
2. root としてログインしていることを確認します。別のユーザーとしてログインしている場合は、次を実行します。

   ```
   sudo su -
   ```

3. Syslog サーバーへの **USER_LOGGED_IN** 監査イベントの電子メール送信を設定するには、次のコマンドを実行します。

   ```
   sedo apps state set notification-manager-app config global '{
       "pollIntervalSec": 60,
       "upstreams": {
           "syslog-1": {
               "type": "syslog",
               "host": "host",
               "port": 514,
               "protocol": "udp",
               "appName": "appName",
               "template": "This is an urgent message about {{ event.subType }}",
           }
       },
       "rules": {
           "rule1": {
               "filter": {
                   "severity": "Audit",
                   "type": "Audit",
                   "subType": "USER_LOGGED_IN",
                   "data": {"msg": "User"},
               },
               "upstream": "syslog-1",
               "maxRequestsPerInterval": 5,
               "intervalSec": 60,
           }
   ```

```
    },
}'
```

Pulsar サーバーへのイベントの送信

送信には証明書の使用が必要です。

Pulsar サーバーにイベントを送信するには、次の手順を実行します。

1. Cisco Crosswork Hierarchical Controller サーバーのコマンドラインにアクセスします（通常は SSH を使用）
2. root としてログインしていることを確認します。別のユーザーとしてログインしている場合は、次を実行します。

   ```
   sudo su -
   ```

3. Pulsar サーバーへの **USER_LOGGED_IN** 監査イベントの電子メール送信を設定するには、次のコマンドを実行します。

   ```
   sedo apps state set notification-manager-app config global '{
       "pollIntervalSec": 60,
       "upstreams": {
           "pulsar-1": {
               "type": "pulsar",
               "server": "pulsar+ssl://host:6651",
               "topic": "topic",
               "publicKey": "publiccert",
               "privateKey": "privatekey",
               "ca": "cacert",
               "template": "This is an urgent message about {{ event.subType }}",
           }
       },
       "rules": {
           "rule1": {
               "filter": {
                   "severity": "Audit",
                   "type": "Audit",
                   "subType": "USER_LOGGED_IN",
                   "data": {"msg": "User"},
               },
               "upstream": "pulsar-1",
               "maxRequestsPerInterval": 5,
               "intervalSec": 60,
           }
       },
   }'
   ```

複数のストリームへのイベントの送信

通知でイベント情報（event.severity や event.subType など）を送信できます。

複数のストリームにイベントを送信するには、次の手順を実行します。

1. Cisco Crosswork Hierarchical Controller サーバーのコマンドラインにアクセスします（通常は SSH を使用）
2. root としてログインしていることを確認します。別のユーザーとしてログインしている場合は、次を実行します。

   ```
   sudo su -
   ```

3. 複数のストリームの送信を設定するには、次のコマンドを実行します。

```
sedo apps state set notification-manager-app config global '{
    "pollIntervalSec": 60,
    "upstreams": {
        "email-1": {
            "type": "smtp",
            "host": "host",
            "port": 1025,
            "username": "username",
            "password": "password",
            "from": from,
            "to": [emailto],
            "subject": "HCO Event {{ event.severity }}",
            "template": "This is an urgent email about {{ event.subType }}",
        },
        "syslog-2": {
            "type": "syslog",
            "host": "host",
            "port": 514,
            "protocol": "udp",
            "appName": "appName",
            "template": "This is an urgent email about {{ event.subType }}",
        },
        "pulsar-3": {
            "type": "pulsar",
            "server": "pulsar+ssl://host:6651",
            "topic": "topic",
            "publicKey": "publiccert",
            "privateKey": "privatekey",
            "ca": "cacert",
            "template": "This is an urgent message about {{ event.subType }}",
        },
    },
```

```
    "rules": {
        "rule1": {
            "filter": {
                "severity": "Audit",
                "type": "Audit",
                "subType": "USER_LOGGED_IN",
                "data": {"msg": "User"},
            },
            "upstream": "email-1",
            "maxRequestsPerInterval": 5,
            "intervalSec": 60,
        },
        "rule2": {
            "filter": {
                "severity": "Audit",
                "type": "Audit",
                "subType": "USER_LOGGED_IN",
                "data": {"msg": "User"},
            },
            "upstream": "syslog-2",
            "maxRequestsPerInterval": 5,
            "intervalSec": 60,
        },
        "rule3": {
            "filter": {
                "severity": "Audit",
                "type": "Audit",
                "subType": "USER_LOGGED_IN",
                "data": {"msg": "User"},
            },
            "upstream": "pulsar-3",
            "maxRequestsPerInterval": 5,
            "intervalSec": 60,
        },
    },
}'
```

Crosswork Hierarchical Controller データベースのバックアップと復元

定期的な Crosswork Hierarchical Controller DB バックアップ

- バックアップは毎日自動的に実行されます。
- 日次バックアップには、前日からの変更のみが含まれます。これらの差分バックアップは、1 週間後に期限切れになります。
- 完全バックアップは、週に 1 回自動的に実行されます。完全バックアップは一定期間の後に期限切れになります。この期間はデフォルトでは 1 年に設定されています。

バックアップコマンド

```
sedo backup [-h] COMMAND ...
```

位置引数:

```
COMMAND
Create create a backup
list   list available backups
export export a backup to file
delete delete backups
```

任意因数:

```
-h, --helpshow this help message and exit
```

手動の Crosswork Hierarchical Controller DB バックアップ

データベースを手動でバックアップし、この完全なバックアップ ファイルを使用して Crosswork Hierarchical Controller データベースを復元したり、新しいインスタンスにコピーしたりできます。

DB をバックアップするには以下を実行します。

- 次のコマンドを使用して、データベースをバックアップします。

```
sedo backup create [-h] [--omit-stats] [-f] [FILENAME]
```

位置引数:

```
FILENAMEspecify filename (default: netfusion-backup-<version>-<timestamp>.tar.gz)
```

任意因数:

```
-h, --help   show this help message and exit
--omit-stats omit the operational statistics table (not for production use!)
-f, --force  do not prompt for confirmation
```

バックアップファイル名にはバージョンと日付が含まれます。

Crosswork Hierarchical Controller DB の復元

復元する場合、Crosswork Hierarchical Controller ユーザーは最新の完全バックアップと差分バックアップを使用して復元します。これは、復元コマンドを使用すると自動的に行われます。

DB を復元するには以下を実行します。

- データベースを復元するには、次のコマンドを使用します。

```
sedo system restore [-h] (--backup-id BACKUP_ID | --filename FILENAME) [--no-verify]
[-f]
```

任意因数:

```
-h, --help            show this help message and exit
--backup-id BACKUP_ID restore backup by this ID
--filename FILENAME   restore from this backup filename
--no-verify           do not verify backup file integrity
-f, --force           do not prompt for confirmation
```

Crosswork Hierarchical Controller DB バックアップの一覧表示

バックアップは次のように作成されます。

- 完全バックアップは毎週日曜日に作成されます（デフォルトでは有効期限が 1 年）
- 差分バックアップは、日曜日を除いて毎日作成されます（有効期限は 7 日後）。

したがって、通常、完全バックアップの間に 6 つのデルタバックアップが表示されます。

さらに、以下の場合に完全バックアップが作成されます（有効期限は 7 日後）。

- マシンが最初にインストールされたとき。
- Crosswork Hierarchical Controller またはマシン全体が再起動された場合（月曜日から土曜日）。

バックアップを一覧表示するには以下を実行します。

- 使用するコマンドは、次のとおりです。

```
sedo backup list[-h]
```

任意因数:

```
-h, --help show this help message and exit
```

```
+----+--------+-----------------------+--------+-----------------------+----------+----------+
|    | ID     | Timestamp             | Type   | Expires               | Status   | Size     |
+====+========+=======================+========+=======================+==========+==========+
|  1 | QP80G0 | 2021-02-28 04:00:04+00 | FULL   | 2022-02-28 04:00:04+00 | OK       | 75.2 MiB |
+----+--------+-----------------------+--------+-----------------------+----------+----------+
|  2 | QP65S0 | 2021-02-27 04:00:01+00 | DELTA  | 2021-03-06 04:00:01+00 | OK       | 2.4 MiB  |
+----+--------+-----------------------+--------+-----------------------+----------+----------+
|  3 | QP4B40 | 2021-02-26 04:00:04+00 | DELTA  | 2021-03-05 04:00:04+00 | OK       | 45.9 MiB |
+----+--------+-----------------------+--------+-----------------------+----------+----------+
|  4 | QP2GG0 | 2021-02-25 04:00:03+00 | DELTA  | 2021-03-04 04:00:03+00 | OK       | 44.3 MiB |
+----+--------+-----------------------+--------+-----------------------+----------+----------+
|  5 | QP0LS0 | 2021-02-24 04:00:00+00 | DELTA  | 2021-03-03 04:00:00+00 | OK       | 1.5 MiB  |
+----+--------+-----------------------+--------+-----------------------+----------+----------+
|  6 | QOYR40 | 2021-02-23 04:00:03+00 | FULL   | 2021-03-02 04:00:03+00 | OK       | 39.7 MiB |
+----+--------+-----------------------+--------+-----------------------+----------+----------+
```

バックアップの削除

特定の期間のバックアップを削除できます。単一のバックアップを削除するには、FROM_ID を TO_ID と同じ値に設定します。

完全バックアップを削除すると、後続の差分バックアップも削除されます。

バックアップを削除するには以下を実行します。

- 使用するコマンドは、次のとおりです。

  ```
  sedo backup delete [-h] [-f] FROM_ID TO_ID
  ```

  位置引数:

  ```
  FROM_ID delete backups starting from this backup ID inclusive
  TO_ID   delete backups up to this backup ID inclusive
  ```

  任意因数:

  ```
  -h, --help  show this help message and exit
  -f, --force do not prompt for confirmation
  ```

バックアップのエクスポート

バックアップをファイルにエクスポートできます。

バックアップをエクスポートするには以下を実行します。

- 使用するコマンドは、次のとおりです。

  ```
  sedo backup export [-h] BACKUP_ID [FILENAME]
  ```

  位置引数:

  ```
  BACKUP_ID export backup of this ID
  FILENAME  specify filename (default: netfusion-backup-<version>-<timestamp>.tar.gz)
  ```

  任意因数:

  ```
  -h, --help show this help message and exit
  ```

履歴削除

データベース内の履歴を削除できます。

クリーナーのしきい値のデフォルトは 365 日です。これは、クリーナーの実行時に 365 日より古い履歴が削除されることを意味します（毎晩 00:30）。

履歴のしきい値を設定するには、次の手順を実行します。

- 履歴を削除するには、次のコマンドを使用します。

  ```
  sedo history [-h] [cleaner-threshold]
  ```

  位置引数:

  ```
      cleaner-threshold    after how many days the history should be deleted
  ```

  任意因数:

  ```
      -h, --help      show this help message and exit
  ```

履歴のデフラグ

データベースをデフラグできます。履歴のクリーナーしきい値を更新した場合は、これを実行します。

データベースをデフラグするには、次の手順を実行します。

- データベースをデフラグするには、次のコマンドを使用します。

  ```
  sedo history defrag [-h]
  ```

  任意因数:

  ```
      -h, --help      show this help message and exit
  ```

クリーナーのしきい値を変更する場合は、次回のクリーニングで新しい設定を使用する前に、デフラグコマンドを実行する必要があります。たとえば、30 日前よりも前の履歴を削除するには、次のコマンドを実行します。

```
sedo history cleaner-threshold set P30D
sedo history defrag
```

HA クラスタ管理

HA クラスタの構成解除

HA クラスターを構成解除するには、以下の順序でノードを HA クラスタから切断します。

- スタンバイ（Standby）
- ウィットネス
- アクティブ（リーダー）

デフォルトでは、アンインストールするとアプリケーションは無効になります。アプリケーションをアクティブノードに保持し、単一のノードで実行を続けることができます。

HA クラスタの構成を解除するには以下を実行します。

1. スタンバイノードで次のコマンドを実行します。

   ```
   sedo ha reset-node
   ```

2. 現在のノード（スタンバイ）を HA クラスタから切断することを確認するには、次のように入力します。

   対応

3. 手順を繰り返してウィットネスノードを切断します。
4. リーダー（アクティブ）ノードを切断し、アプリケーションの実行を続けるには、次のコマンドを実行します。

   ```
   sedo ha reset-node -keep-apps
   ```

5. クラスタのステータスを確認するには、次のコマンドを実行します。

   ```
   sedo ha state
   ```

   このノードはクラスタの一部ではありません。

HA クラスタのアップグレード

HA をアップグレードするには、HA クラスタの構成を解除し、ノードをアップグレードしてからクラスタを再構成します。

HA クラスタをアップグレードするには以下を実行します。

1. クラスタの構成を解除します。「HA クラスタの構成解除」を参照してください。
2. 各ノードをアップグレードします。
3. クラスタを設定します。『*Cisco Crosswork Hierarchical Controller Installation Guide*』[英語] を参照してください。

HA クラスタの復元

必要なバックアップを使用してクラスタを復元します。

注：同じバージョンからのバックアップのみを復元してください。

HA クラスタを復元するには以下を実行します。

1. クラスタの構成を解除します。「HA クラスタの構成解除」を参照してください。
2. 必要な（インスタンスの 1 つからの）バックアップを使用して 1 つのノードを復元します。このノードのデータベースがクラスタの基礎になります。
3. この復元されたノードからクラスタを構成します。『*Cisco Crosswork Hierarchical Controller Installation Guide*』[英語] を参照してください。

HA ステータスの確認

ステータスコマンドは、IPsec トンネル、etcd ノード、およびデータベースクラスタ情報を返します。

HA クラスタのステータスを確認するには以下を実行します。

- 次のコマンドを実行して、HA クラスタのステータスを確認します。

  ```
  sedo ha state
  ```

  ノードは IPsec トンネルのフル メッシュを介して接続されており、etcd ツールを使用した永続的なクラスタ構成に向けた分散型データストアを使用しています。

Device Management

用語

用語	定義
アダプタ	Crosswork Hierarchical Controller がデバイスまたはマネージャに接続し、ネットワークモデルに必要な情報を収集してデバイスを設定するために使用するソフトウェア。
デバイス	光ネットワーク要素、ルータ、またはマイクロ波デバイス。
Device Manager	展開されたアダプタを管理する Crosswork Hierarchical Controller アプリケーション。
NMS	Network Management System（ネットワーク管理システム）。複数の光ネットワーク要素またはルータを管理する。
SDN コントローラ	複数のルータまたは光ネットワーク要素を管理するソフトウェア。

デバイス管理について

オペレータにとって重要なニーズは、ネットワークの検出と、ネットワークデバイスのモニタリングおよび管理です。これを達成する方法はネットワークアダプタを構成し、CLI、SNMP、REST などのさまざまなテクノロジーを使用して、直接または管理システム（EMS、NMS、SDN コントローラ）を介してネットワークデバイスのグループをモニタリングすることです。

デバイスマネージャは非常に重要な Crosswork Hierarchical Controller アプリケーションであり、Crosswork Hierarchical Controller のサウスバンドアダプタを管理します。これにより、デバイスの追加と管理、デバイスのアダプタへの割り当ての管理、アダプタの健全性、デバイス到達可能性や検出ステータスのモニタリングが可能になります。

デバイスマネージャを使用すると、ネットワークを検出し、接続をモニタリングし、接続障害が発生した場合にトラブルシューティングを実行できます。

デバイスマネージャのサービスは、UI と API の両方で使用できます。

到達可能性と検出を正確に反映するために、デバイス マネージャ アプリケーションはアダプタごと、および情報タイプ（インベントリ、トポロジ、統計）ごとにデバイス検出ステータスを提供します。3D Explorer では、デバイスの**到達可能性ステータス**は、すべての情報タイプのステータスを反映する集約ステータスです。

Crosswork Hierarchical Controller は、次の場合に Syslog イベントを送信します。

- デバイスの到達可能性状態の変更
- アダプタによるファイル解析の失敗
- アダプタがコントローラへの接続に失敗した場合。たとえば、認証の失敗または TCP 接続の失敗。

資格情報

アダプタを使用する場合は、クレデンシャルを使用する必要があります。これらは、デバイスがアダプタに割り当てられる際の認証に使用されます。同じクレデンシャルが複数のアダプタで共有される場合があります。したがって、再利用のために「テンプレート」のクレデンシャルを作成できます。使用しやすいように、意味のある名前を入力してください。

クレデンシャルを追加、編集、削除できます。

クレデンシャルは次のいずれかになります。

- SSH ユーザーとパスワード
- SSH 公開キー
- HTTP
- SNMP コミュニティ
- SFTP

クレデンシャルの追加
クレデンシャルを追加できます。

クレデンシャルを追加するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] を選択します。
2. [クレデンシャル（Credentials）] タブをクリックします。
3. [新しいクレデンシャルの追加（Add New Credentials）] をクリックします。
4. [名前（Name）] を入力して [タイプ（Type）] を選択します。
5. 必要なクレデンシャルを入力します。
6. [クレデンシャルの追加（Add Credentials）] をクリックします。

クレデンシャルの削除
クレデンシャルを削除できます。

クレデンシャルを削除するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] を選択します。
2. [クレデンシャル（Credentials）] タブをクリックします。
3. 必要なクレデンシャルを選択します。
4. [選択したクレデンシャルを削除（Delete Selected Credentials）] をクリックします。確認メッセージが表示されます。
5. [確認（Confirm）] をクリックします。

アダプタ

アダプタタイプはシスコによってインストールされます。アダプタタイプは特定のプロトコルを使用して、特定の範囲の情報がデバイスグループまたはネットワークマネージャから取得されるように、またはそこで構成されるように管理します。1 つのアダプタタイプは、1 つのマネージャにのみ接続されます（EPN-M インスタンスなど）。

アダプタはアダプタタイプのインスタンスであり、Crosswork Hierarchical Controller がデバイスまたはマネージャに接続し、ネットワークモデルに必要な情報を収集してデバイスを設定するために使用します。

デバイスマネージャは、展開されあたアダプタ、アダプタとマネージャへのデバイスの割り当て、および運用のライフサイクルを通じたアダプタとデバイス両方のステータスを管理します。デバイスおよび/またはマネージャに接続するように設定されたアダプタは、定期的にポーリングして、デバイスおよび/または NMS が到達可能で検出済みであることを確認します。

（注） リンクの検出状態は Explorer とネットワーク インベントリ アプリケーションで報告されます (デバイス マネージャ内ではありません)。

デバイスまたはマネージャは、1 つまたは複数のアダプタに関連付けることができます。これは、デバイスを複数のアダプタに関連付けることにより、同じデバイスのさまざまなタイプの情報をモニタリングできることを意味します。

デバイスまたはマネージャにアクセスするすべてのアダプタは同じ IP アドレスまたはホスト名を使用しますが、クレデンシャルは異なる場合があります。

Crosswork Hierarchical Controller は、次の場合に Syslog イベントを送信します。

- アダプタによるファイル解析の失敗
- アダプタがコントローラへの接続に失敗した場合。たとえば、**認証の失敗**または **TCP 接続の失敗**。

アダプタのステータスの値

デバイスマネージャの [アダプタ（Adapters）] テーブルでは、アダプタに割り当てられたデバイス（およびアダプタに割り当てられたすべてのデバイスの総合）に以下の値が表示されます。

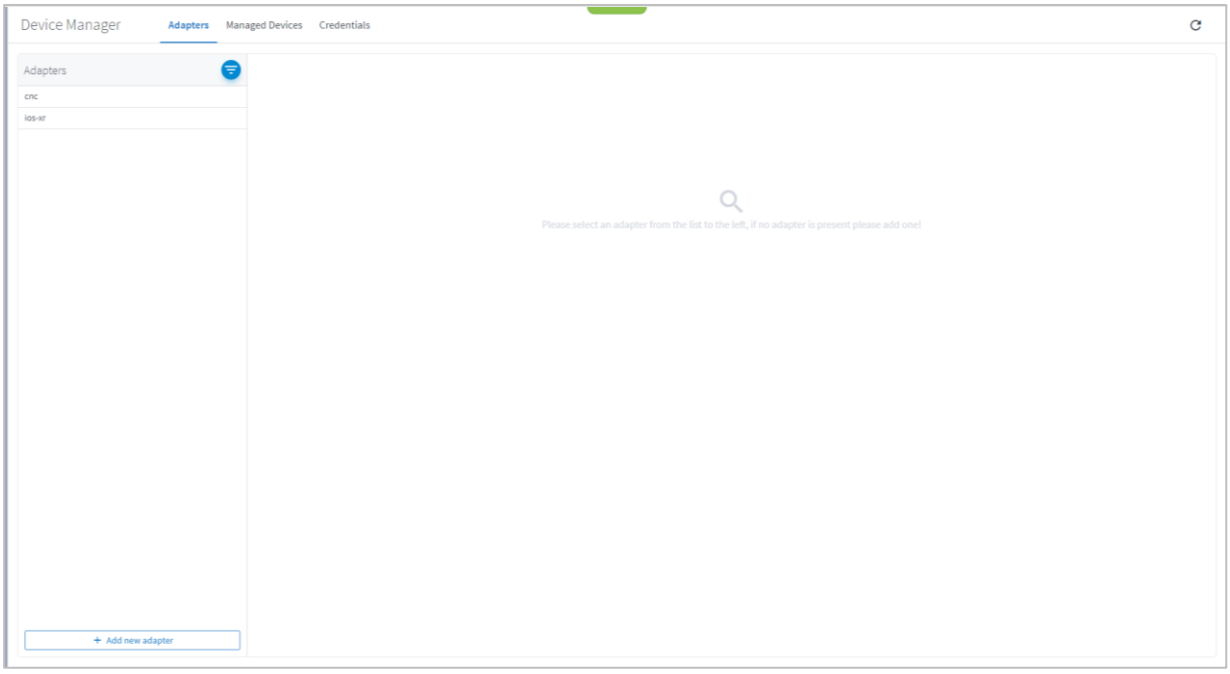
	情報の種類		
有効な値	**インベントリ**	**トポロジ**	**統計**
OK	特定の種類の情報を収集するアダプタがデバイスの NMS システムまたはデバイス自体に正常に到達し、デバイスデータを検出した場合。		
ERROR	特定の種類の情報を収集しているアダプタがデバイスに到達したものの、必要な情報を収集できなかった場合（クレデンシャルが正しくない、コマンドタイプエラー、データが存在しないなど）。		
UNREACHABLE	特定の種類の情報を収集するアダプタがデバイスに到達できなかった場合。通常は接続の問題が原因です。		
WARNING	該当なし	該当なし	統計情報を収集するアダプタが一部のデバイスポートのデータを取得できなかった場合。
UNKNOWN	アダプタによってステータスが報告されなかった場合。これは、内部通信エラーが原因です。サポートに問い合わせてください。		

アダプタを表示する

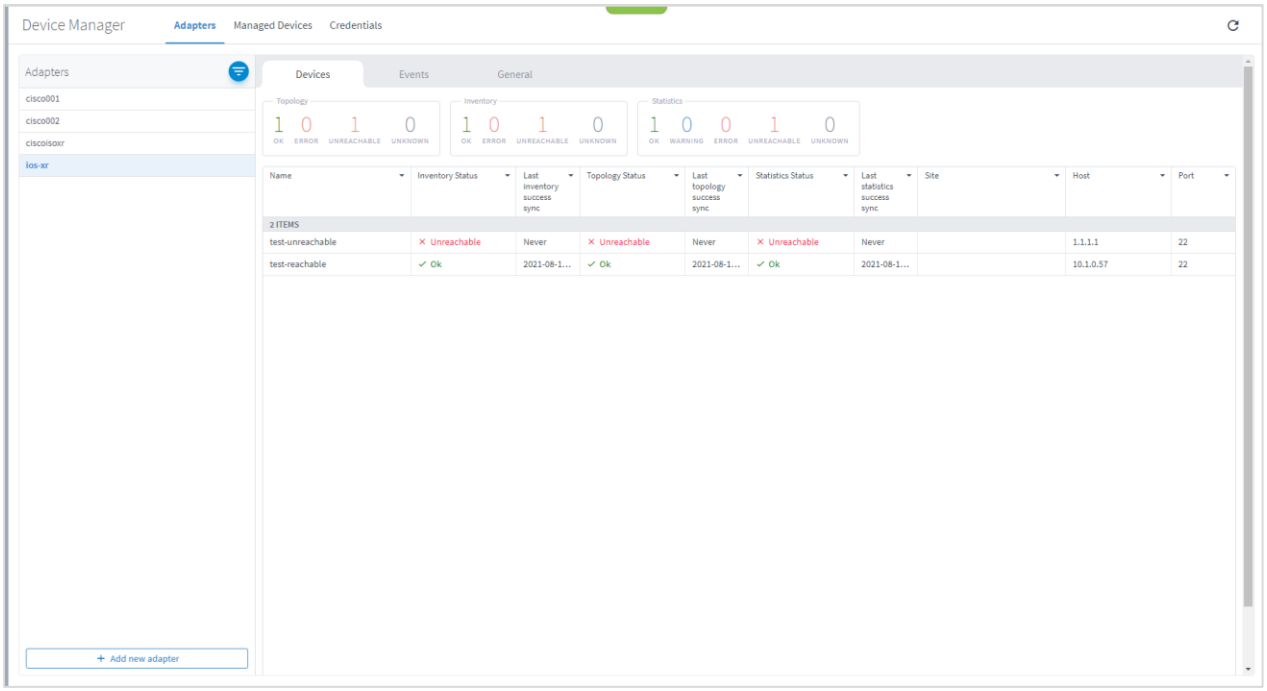
アダプタのリストを表示し、各アダプタに割り当てられたデバイスのリストと、デバイスのインベントリ、トポロジ、統計ステータス、およびアダプタで発生したイベントを表示できます。

アダプタを表示するには以下を実行します

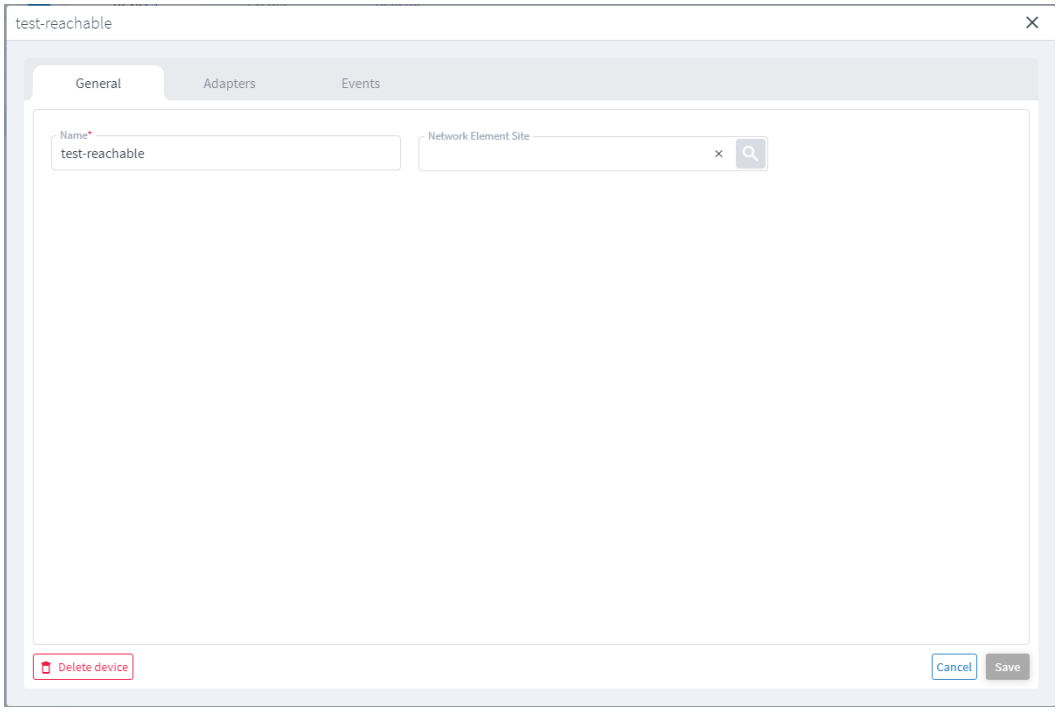
1. アプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] > [アダプタ（Adapters）] を選択します。[アダプタ（Adapters）] ペインにアダプタのリストが表示されます。



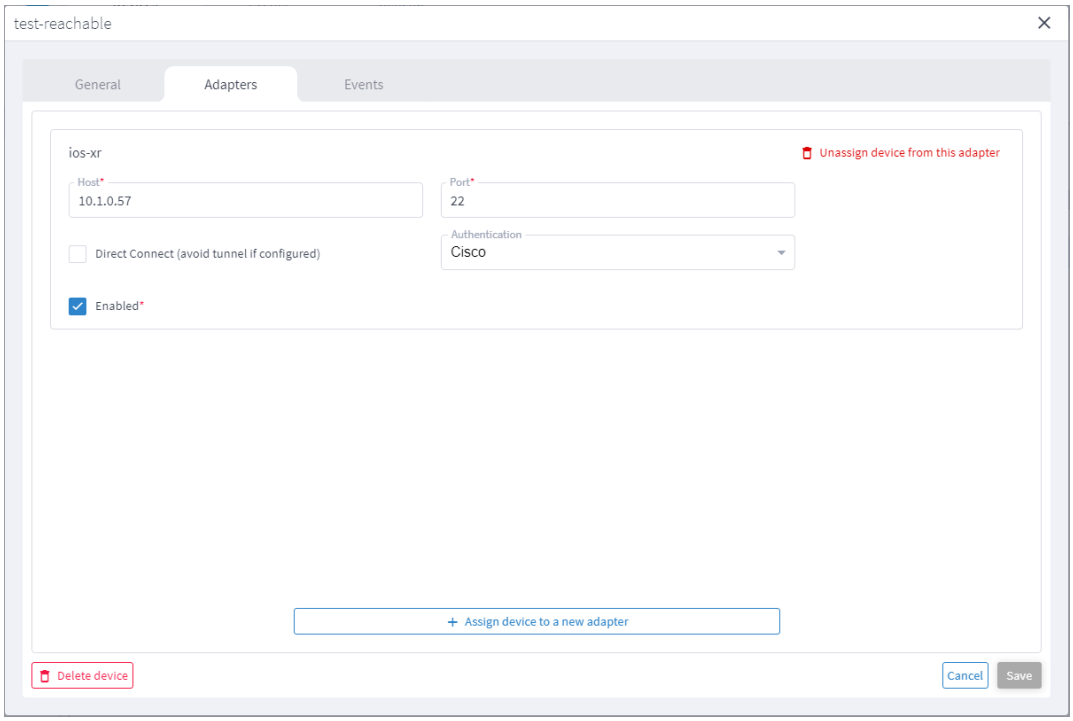
2. 必要なアダプタを選択します。[トポロジ（Topology）]、[インベントリ（Inventory）]、[統計（Statistics）] について、ステータスが [OK]、[エラー（ERROR）]、[到達不能（UNREACHABLE）]、[不明（UNKNOWN）] になっているデバイスの数の概要が表示されます。また、割り当てられたデバイスのリストと、デバイスごとの次の情報も表示されます。
    - 名前
    - トポロジのステータス（Topology Status）
    - 最後に成功したトポロジの同期（Last topology success sync）
    - インベントリ ステータス
    - 最後に成功したインベントリの同期（Last inventory success sync）
    - 統計のステータス（Statistics Status）
    - 最後に成功した統計の同期（Last statistics success sync）
    - サイト（Site）
    - ホスト（Host）
    - ポート（Port）



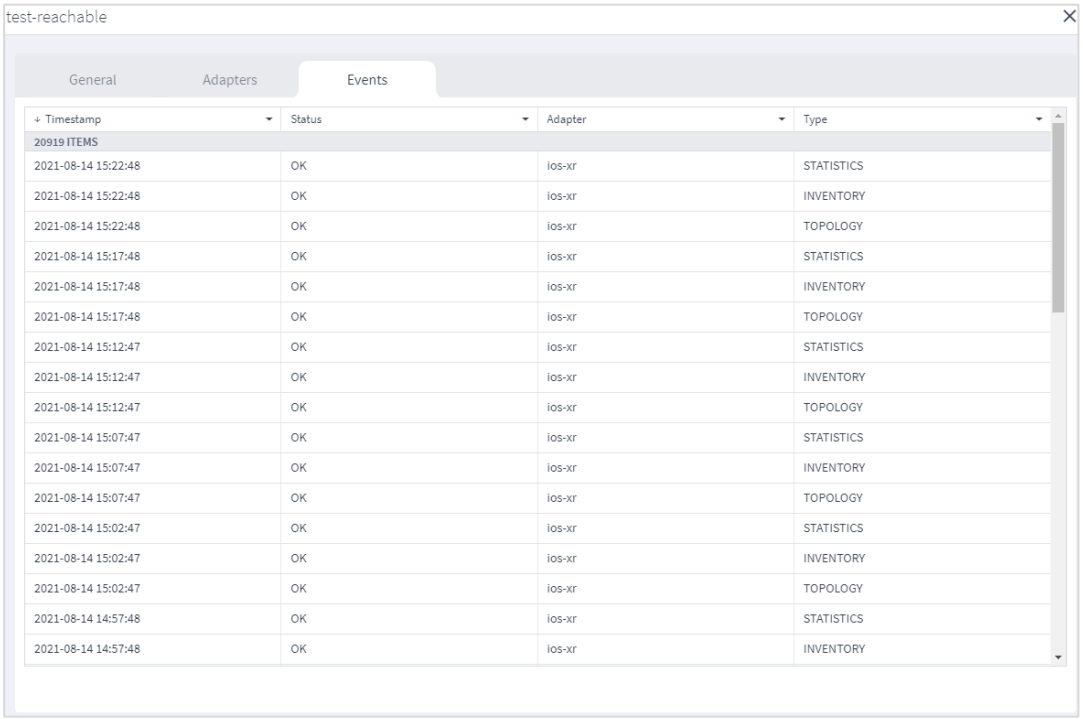
3. デバイス名にカーソルを合わせてマップ内のデバイスを表示し、[Explorer で開く（Open in Explorer）] をクリックして Explorer でデバイスを開きます（または、デバイスを直接クリックして Explorer でデバイスを表示します）。
4. デバイスの詳細を表示するには、任意の列をクリックします（[名前（Name）] 列を除く、）。



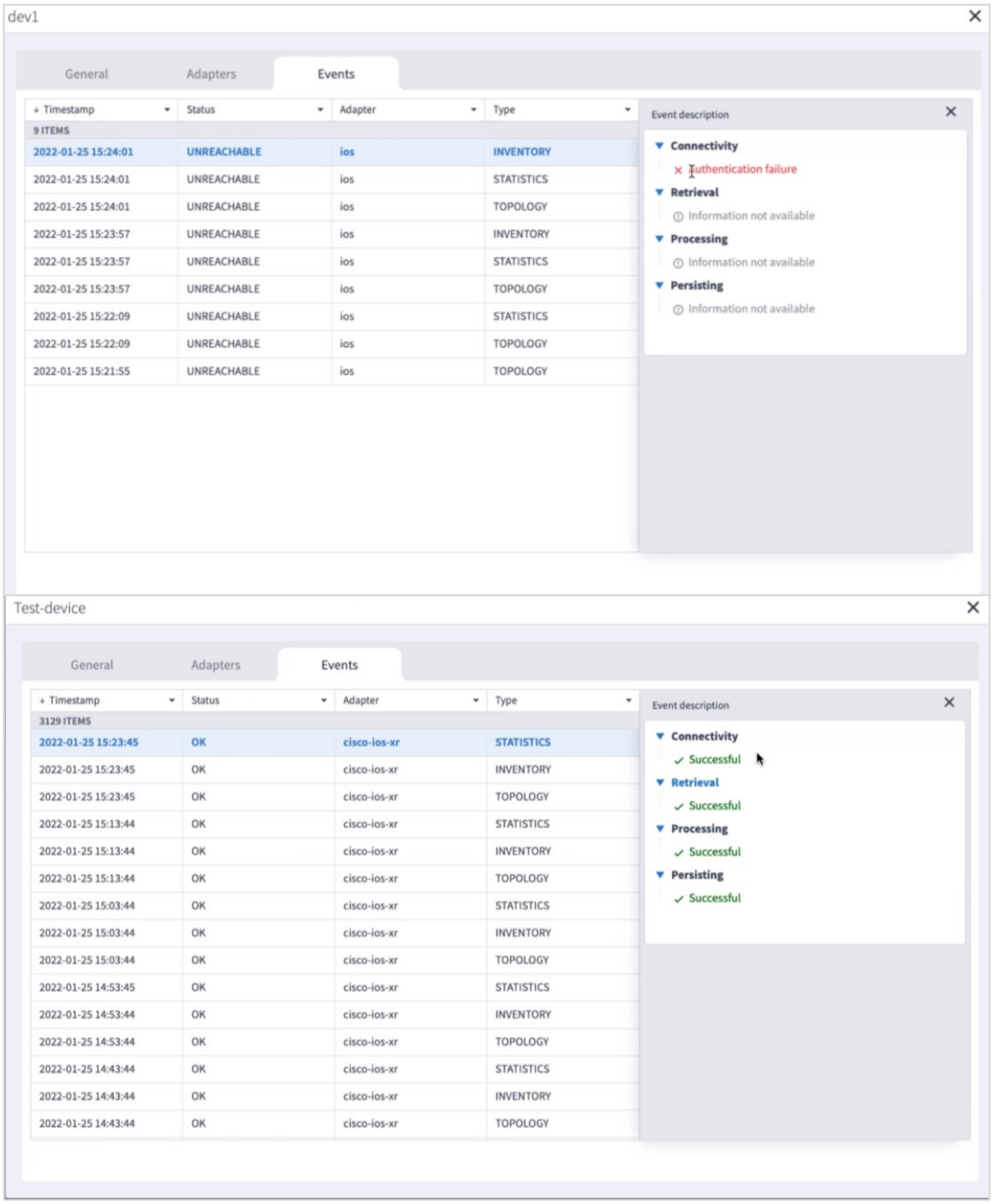
5. デバイスのアダプタを表示するには、[アダプタ（Adapters）] タブを選択します。



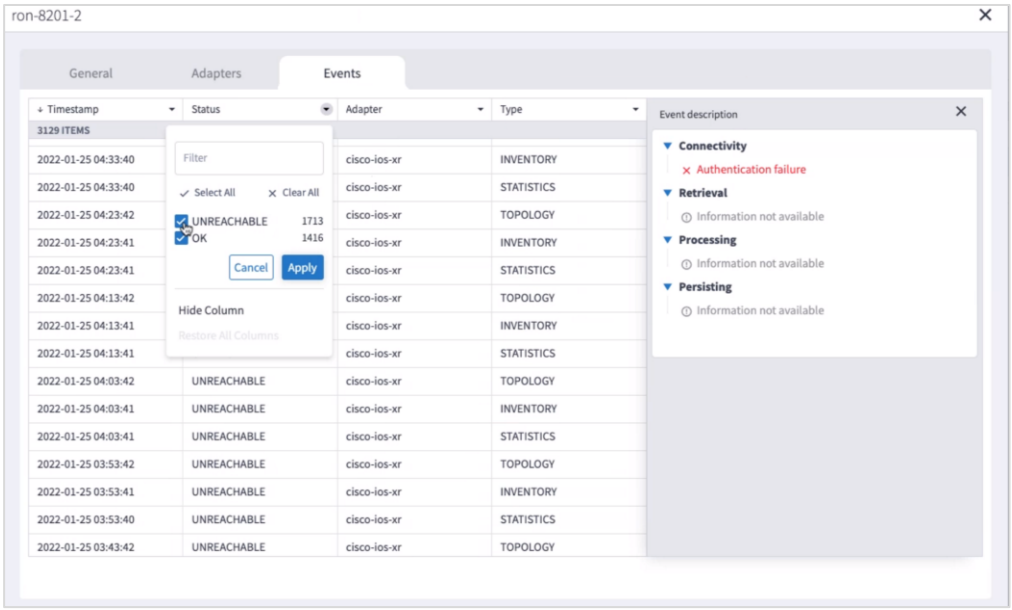
6. デバイスのイベントを表示するには、[イベント（Events）] タブを選択します。



7. さらに詳細を表示するには、任意のイベントをクリックします。



8. クリックして、イベントのステータスでフィルタ処理します。



Edit Device

デバイスを編集して Explorer でネットワーク要素を選択したり、デバイスをアダプタに割り当てたり、アダプタからデバイスの割り当てを解除したりできます。

デバイスを編集するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] を選択します。
2. 必要なアダプタを選択します。
3. [管理対象デバイス（Managed Devices）] タブを選択します。
4. 必要なデバイス行をクリックします（[名前（Name）] 列のリンクではありません）。
5. [全般（General）] タブの [ネットワーク要素のサイト（Network Element Site）] をクリックして、Explorer でネットワーク要素を選択します。

アダプタの編集

アダプタの構成を編集してアダプタを有効または無効にし、ロギングレベルとポーリングサイクルを設定し、各ポーリングサイクルでポーリングする同時ルータ数を指定し、必要な収集パラメータを選択できます。また、アダプタの固有パラメータを編集することもできます。デバイスをアダプタに追加する、またはアダプタから削除するには、「管理対象デバイス」をご覧ください。

アダプタを編集するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] を選択します。[アダプタ（Adapters）] ペインにアダプタのリストが表示されます。
2. 必要なアダプタを選択します。
3. [General] タブをクリックします。
4. 次のオプションを設定します。
    - [有効（Enabled）]：アダプタが有効か無効か。

- [ロギングレベル（Logging Level）]：ロギングレベル（[情報（Info）]、[重要（Critical）]、[エラー（Error）]、[警告（Warning）]、[デバッグ（Debug）]）。デフォルトは [情報（Info）] です。
- [ポーリングサイクル（秒）（Polling Cycle (sec)）]：ポーリング間隔（秒）
- [収集される同時ルータの数（Number of concurrent routers collected）]：ポーリング サイクルで同時にポーリングできるネットワーク要素の数。
- [プロビジョニングサポートの有効化（Enable provisioning support）]：プロビジョニングサポートを有効にするかどうか。たとえば、プロビジョニングが有効になっている場合は新しいトンネルまたはサービスを作成します。

5. [SSH 設定パラメータ（SSH CONFIGURATION PARAMETERS）] を設定します（SSH を使用するように設定されたアダプタの場合）。
   - [トンネルの有効化（Enable Tunnel）]：トンネルを有効にします。
   - [トンネルホスト（Tunnel Host）]：トンネルのホスト。
   - [トンネルポート（Tunnel Port）]：トンネルのポート。
   - [トンネルのクレデンシャルキー（Tunnel Credentials Key）]：トンネル
   - [ルータ接続タイムアウト（Router Connect timeout）]：ルータ接続のタイムアウト。
   - [ルータコマンドタイムアウト（Router Command timeout）]：ルータコマンドのタイムアウト。
6. **ファイルブリンガのパラメータ**を構成します。
   - [ファイルブリンガの有効化（Enable File Bringer）]：これにより、アダプタのモジュールがリモートファイルサーバーから Crosswork Hierarchical Controller にファイルを転送できるようになります。
   - [ファイルサーバーの場所（File Server Location）]：ファイルサーバーの場所（形式は *http/sftp://<ip>:port/<path>*）。
   - [ファイルの種類（File Type）]：CSV、JSON など。
   - **認証**
   - [バックアップ ファイル サーバーの場所（Backup File Server Location）]：バックアップ ファイル サーバーの場所（形式は *http/sftp://<ip>:port/<path>*）。
   - **Backup_server_authentication**
7. **NetFusion 収集サイクルファイル**を設定します。
   - [NetFusion サイクルモードの有効化（Enable NetFusion Cycles mode）]：定期的にファイルを取得するかどうか。
   - [サイクルディレクトリの場所（Cycle Directories Location）]：Crosswork Hierarchical Controller で受信したファイルを保存する場所。
8. 他のアダプタ固有のパラメータがあれば構成します。
9. **収集パラメータ**（すべての IP アダプタに共通）を設定します。
   - [トポロジ収集の有効化（Enable Topology Collection）]

- [IGP IS-IS 収集の有効化（Enable IGP IS-IS Collection）]
- [IGP OSPF 収集の有効化（Enable IGP OSPF Collection）]
- [インターフェイス統計収集の有効化（Enable Interface Stats Collection）]
- [VRF 収集の有効化（Enable VRF Collection）]
- [LLDP 収集の有効化（Enable LLDP Collection）]
- [MLPS トンネル収集の有効化（Enable MLPS Tunnels Collection）]
- [LSP 統計収集の有効化（Enable LSP Stats Collection）]
- [SNMP 収集の有効化（Enable SNMP Collection）]
- [IGP IS-IS 優先順位（IGP IS-IS Priority）]
- [IGP IS-IS シードルータのみを収集（Collect only IGP IS-IS seed routers）]
- [ループバック IP の管理 IP としての使用を許可（Allow to use loopback IP as management IP）]
- [RSVP 収集の有効化（Enable RSVP Collection）]
- [オプティクスおよびコヒーレント DSP の収集を有効化（Enable collection of optics and coherent DSP）]
- [セグメントルーティング収集の有効化（Enable Segment Routing Collection）]

10. [保存（Save）] をクリックします。

アダプタの追加

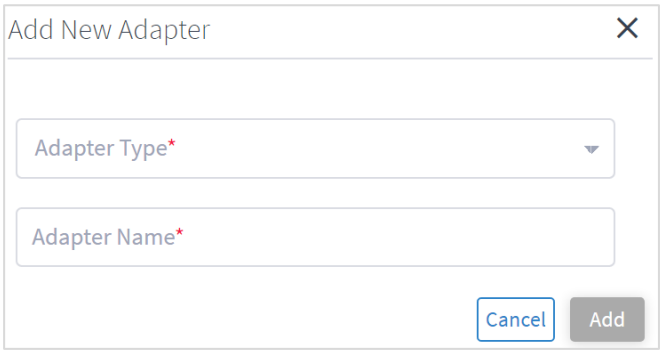
アダプタは、アダプタタイプのインスタンスです。通常、アダプタタイプは Crosswork Hierarchical Controller に事前にインストールされています（アダプタタイプは、Crosswork Hierarchical Controller プラットフォームのインストールに影響を与えることなく追加することもできます）。

任意のアダプタ固有パラメータを構成することもできます（これらはプロジェクトごとに追加されます）。

デバイスをアダプタに追加する、またはアダプタから削除するには、「管理対象デバイス」をご覧ください。

アダプタを追加するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] を選択します。[アダプタ（Adapters）] ペインにアダプタのリストが表示されます。
2. [新規アダプタの追加（Add new adapter）] をクリックします。



3. アダプタの詳細を入力します。
    - [アダプタタイプ（Adapter Type）]：Crosswork Hierarchical Controller に現在インストールされている使用可能なアダプタタイプのリストからアダプタタイプを選択します。
    - [アダプタ名（Adapter Name）]：このアダプタタイプ インスタンスの一意のユーザー定義名（同じアダプタタイプのインスタンスが複数存在する場合があります）。
4. [追加（Add）] をクリックします。
5. アダプタを構成するには、[アダプタ（Adapter）] ペインでアダプタを選択します。
6. [General] タブをクリックします。
7. 次のオプションを設定します。
    - [有効（Enabled）]：アダプタが有効か無効か。
    - [ロギングレベル（Logging Level）]：ロギングレベル（[情報（Info）]、[重要（Critical）]、[エラー（Error）]、[警告（Warning）]、[デバッグ（Debug）]）。デフォルトは [情報（Info）] です。
    - [ポーリングサイクル（秒）（Polling Cycle (sec)）]：ポーリング間隔（秒）
    - [収集される同時ルータの数（Number of concurrent routers collected）]：ポーリング サイクルで同時にポーリングできるネットワーク要素の数。
    - [プロビジョニングサポートの有効化（Enable provisioning support）]：プロビジョニングサポートを有効にするかどうか。たとえば、プロビジョニングが有効になっている場合は新しいトンネルまたはサービスを作成します。
8. [SSH 設定パラメータ（SSH CONFIGURATION PARAMETERS）] を設定します（SSH を使用するように設定されたアダプタの場合）。
    - [トンネルの有効化（Enable Tunnel）]
    - [トンネルホスト（Tunnel Host）]
    - トンネル ポート
    - [トンネルのクレデンシャルキー（Tunnel Credentials Key）]
    - [ルータ接続タイムアウト（Router Connect timeout）]
    - [ルータコマンドタイムアウト（Router Command timeout）]
9. **ファイルブリンガのパラメータ**を構成します。
    - [ファイルブリンガの有効化（Enable File Bringer）]：これにより、アダプタのモジュールがリモートファイルサーバーから Crosswork Hierarchical Controller にファイルを転送できるようになります。
    - [ファイルサーバーの場所（File Server Location）]：ファイルサーバーの場所（形式は http/sftp://<ip>:port/）<path>。
    - [ファイルの種類（File Type）]：CSV、JSON など。
    - **認証**

10. **NetFusion 収集サイクルファイル**を構成します。
    - [NetFusion サイクルモードの有効化（Enable NetFusion Cycles mode）]：定期的にファイルを取得するかどうか。
    - [サイクルディレクトリの場所（Cycle Directories Location）]：Crosswork Hierarchical Controller で受信したファイルを保存する場所。
11. 他のアダプタ固有のパラメータがあれば構成します。
12. **収集パラメータ**（すべての IP アダプタに共通）を設定します。
    - [トポロジ収集の有効化（Enable Topology Collection）]
    - [IGP IS-IS 収集の有効化（Enable IGP IS-IS Collection）]
    - [IGP OSPF 収集の有効化（Enable IGP OSPF Collection）]
    - [インターフェイス統計収集の有効化（Enable Interface Stats Collection）]
    - [VRF 収集の有効化（Enable VRF Collection）]
    - [LLDP 収集の有効化（Enable LLDP Collection）]
    - [MLPS トンネル収集の有効化（Enable MLPS Tunnels Collection）]
    - [LSP 統計収集の有効化（Enable LSP Stats Collection）]
    - [SNMP 収集の有効化（Enable SNMP Collection）]
    - [IGP IS-IS 優先順位（IGP IS-IS Priority）]
    - [IGP IS-IS シードルータのみを収集（Collect only IGP IS-IS seed routers）]
    - [ループバック IP の管理 IP としての使用を許可（Allow to use loopback IP as management IP）]
    - [RSVP 収集の有効化（Enable RSVP Collection）]
    - [オプティクスおよびコヒーレント DSP の収集を有効化（Enable collection of optics and coherent DSP）]
    - [セグメントルーティング収集の有効化（Enable Segment Routing Collection）]
13. [保存（Save）] をクリックします。
14. アダプタにデバイスを割り当てます。「デバイスの割り当て」を参照してください。

アダプタの削除

アダプタを削除するには以下を実行します。

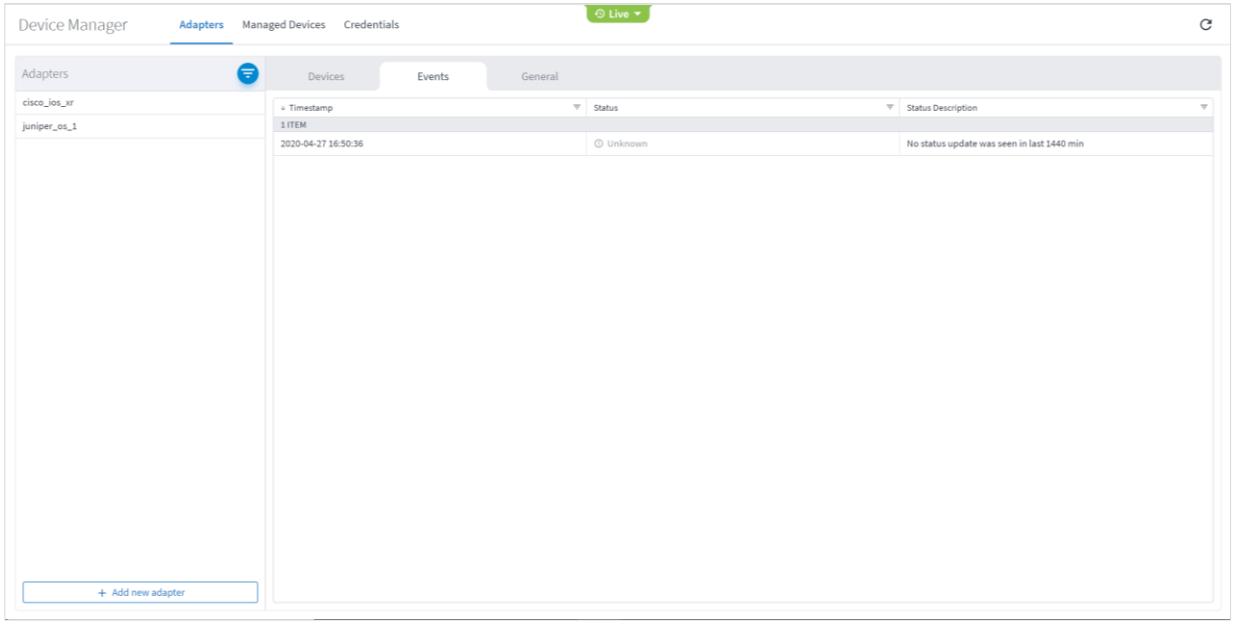
1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] を選択します。[アダプタ（Adapters）] ペインにアダプタのリストが表示されます。
2. アダプタを選択します。
3. [全般（General）] タブを選択します。
4. [アダプタの削除（Delete Adapter）] をクリックします。確認メッセージが表示されます。
5. [確認（Confirm）] をクリックします。アダプタが削除されます。

アダプタイベントの表示

特定のアダプタのユーザ主導およびシステム主導のイベントを表示できます。アダプタタイプによって異なります。

アダプタイベントを表示するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] を選択します。[アダプタ（Adapters）] ペインにアダプタのリストが表示されます。
2. 必要なアダプタをクリックして選択します。
3. [イベント（Events）] タブをクリックします。



4. イベントテーブルの詳細
    - タイムスタンプ
    - ステータス
    - ステータスの説明

管理対象デバイス

デバイスマネージャの [管理対象デバイス（Managed Device）] テーブルでは、デバイスごと（およびアダプタに割り当てられたすべてのデバイスの総合）に以下のステータスが表示されます。

	情報の種類		
有効な値	**インベントリ**	**トポロジ**	**統計**
OK	特定の種類の情報を収集するアダプタがデバイスの NMS システムまたはデバイス自体に正常に到達し、デバイスデータを検出した場合。		
ERROR	特定の種類の情報を収集しているアダプタがデバイスに到達したものの、必要な情報を収集できなかった場合（クレデンシャルが正しくない、コマンドタイプエラー、データが存在しないなど）。		

	情報の種類		
有効な値	インベントリ	トポロジ	統計
UNREACHABLE	特定の種類の情報を収集するアダプタがデバイスに到達できなかった場合。通常は接続の問題が原因です。		
WARNING	該当なし	該当なし	統計情報を収集するアダプタが一部のデバイスポートのデータを取得できなかった場合。
UNKNOWN	アダプタによってステータスが報告されなかった場合。これは、内部通信エラーが原因です。サポートに問い合わせてください。		

Crosswork Hierarchical Controller は、デバイスの到達可能性のステータスが変更された場合に Syslog イベントを送信します。

デバイスを追加してアダプタに割り当てることができます。

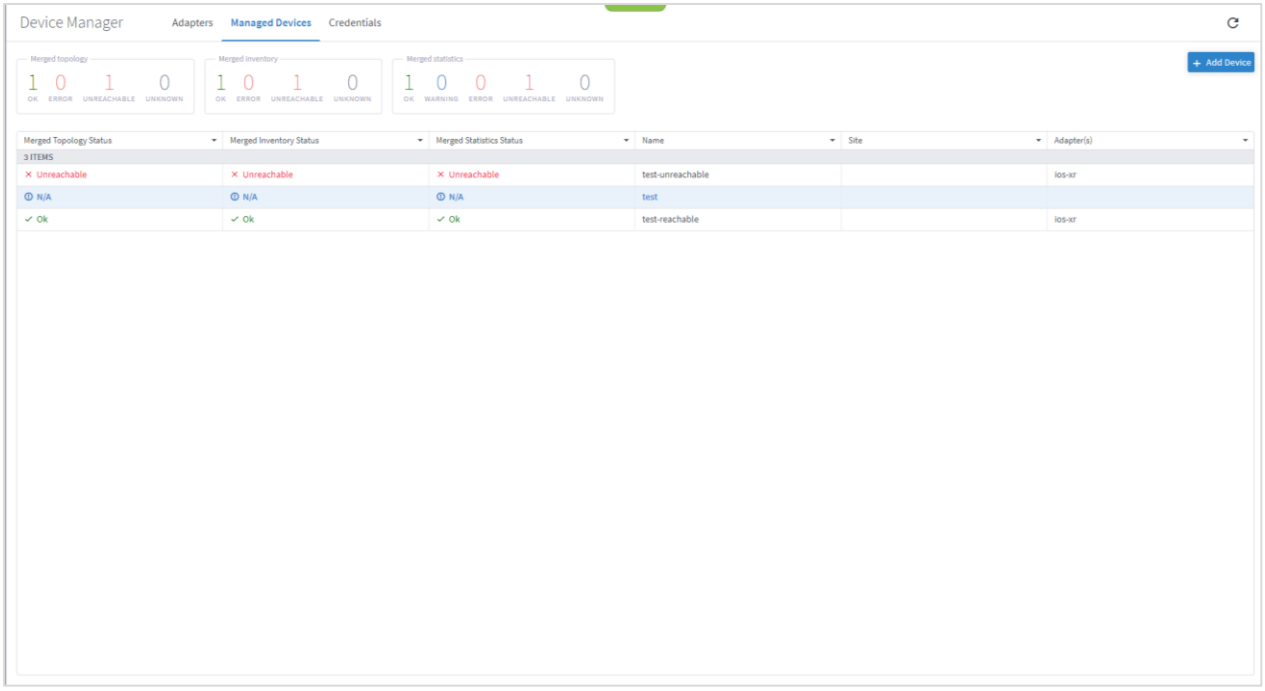
デバイスの追加とアダプタへの割り当て

デバイスを追加し、1 つ以上のアダプタに割り当てることができます。

デバイスをアダプタに割り当てる前に、必要なクレデンシャルを追加したことを確認してください。「クレデンシャル」を参照してください。

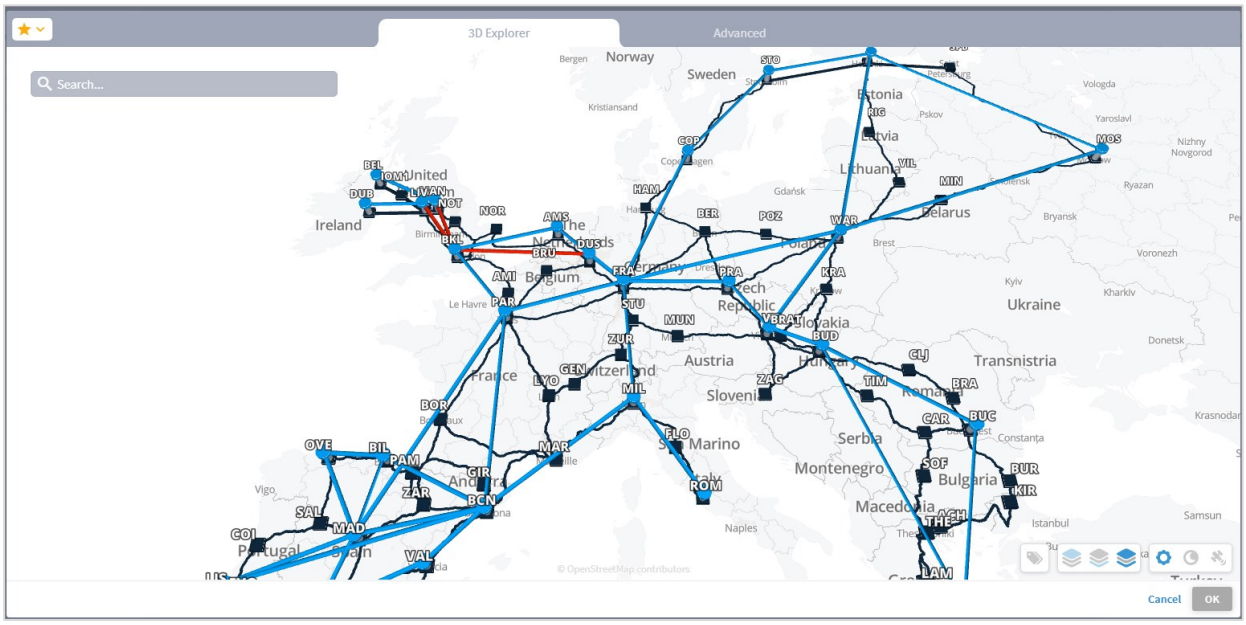
デバイスを追加するには、次の手順を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] を選択します。[アダプタ（Adapters）] ペインにアダプタのリストが表示されます。
2. [管理対象デバイス（Managed Devices）] タブを選択します。

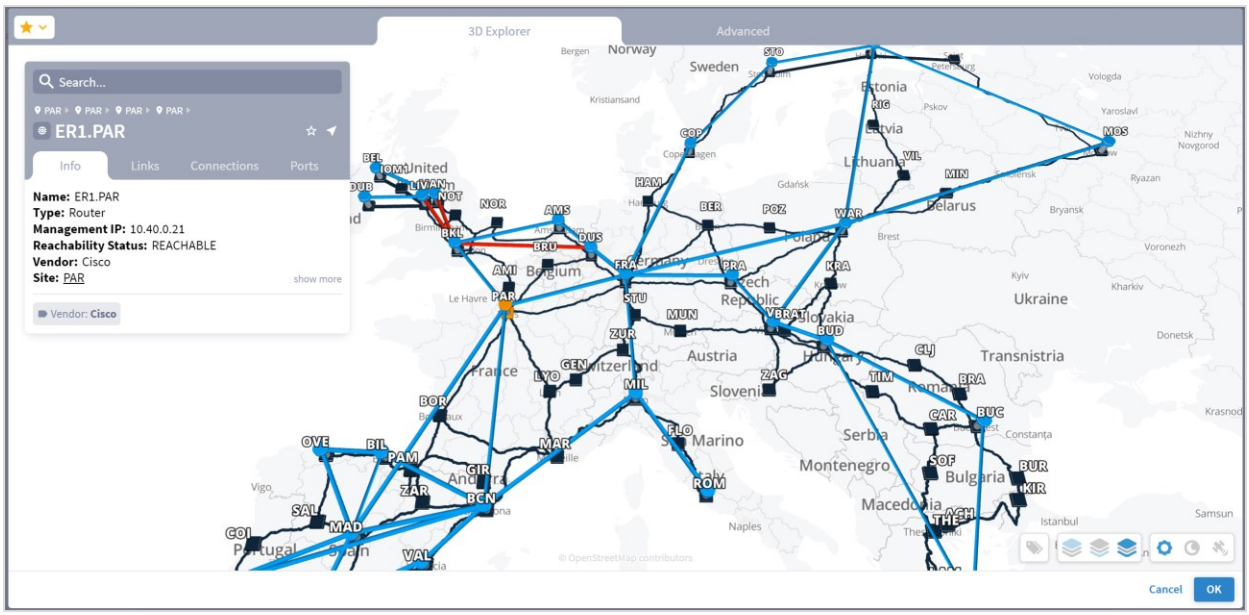


3. [Add Device] をクリックします。
4. [全般（General）] タブで、[名前（Name）]を入力します。

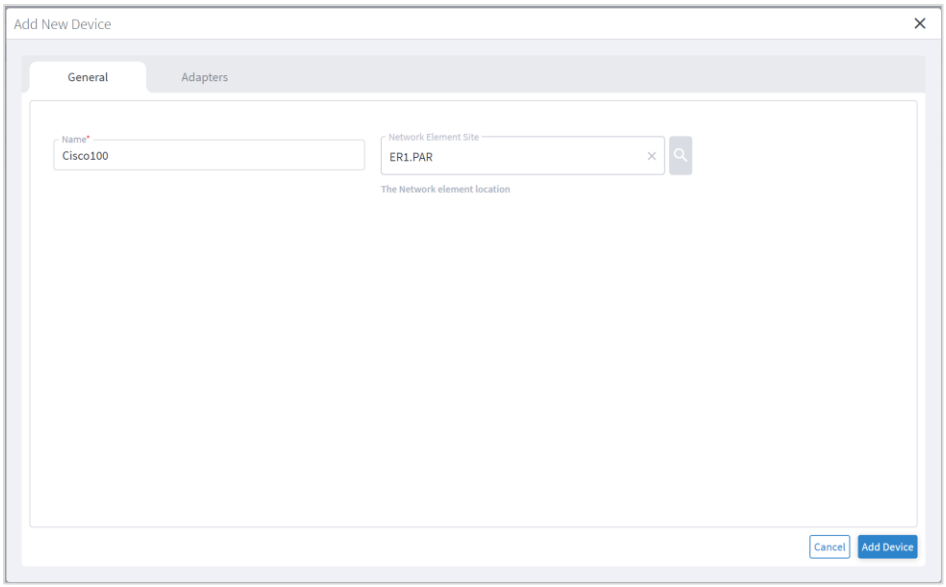
5. （オプション）[ネットワーク要素のサイト（Network Element Site）] で、デバイスがあるサイトをクリックして選択します。



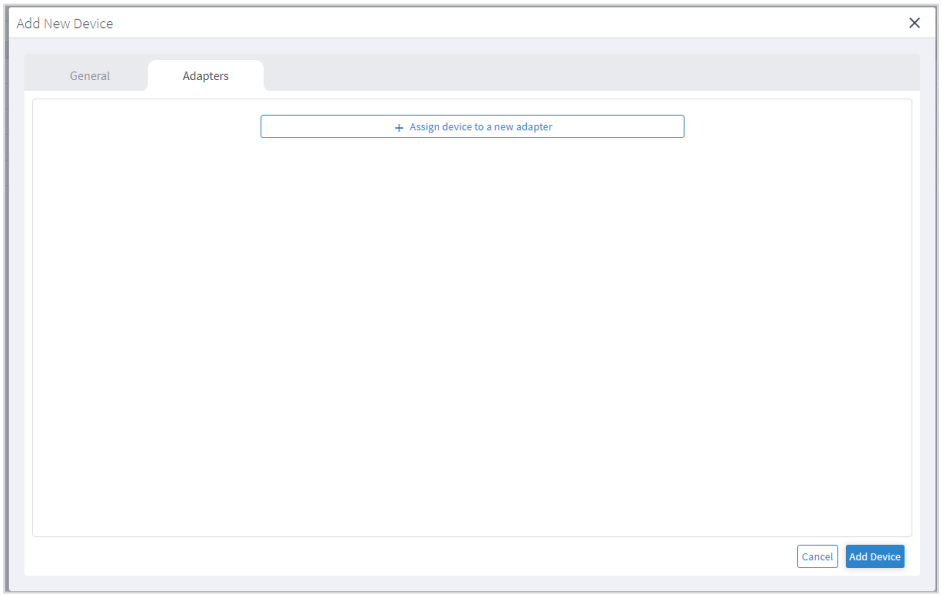
6. ネットワーク要素を選択します。



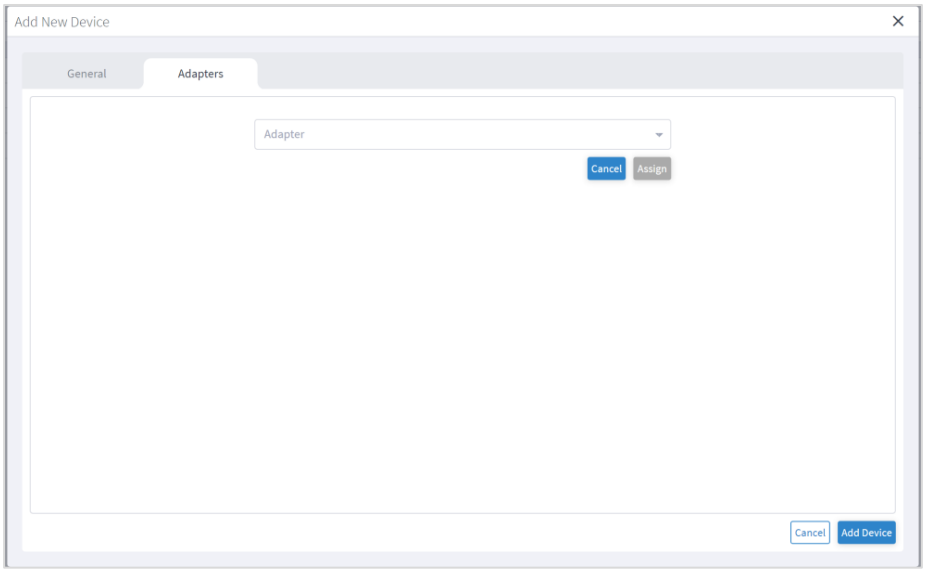
7. [OK] をクリックします。



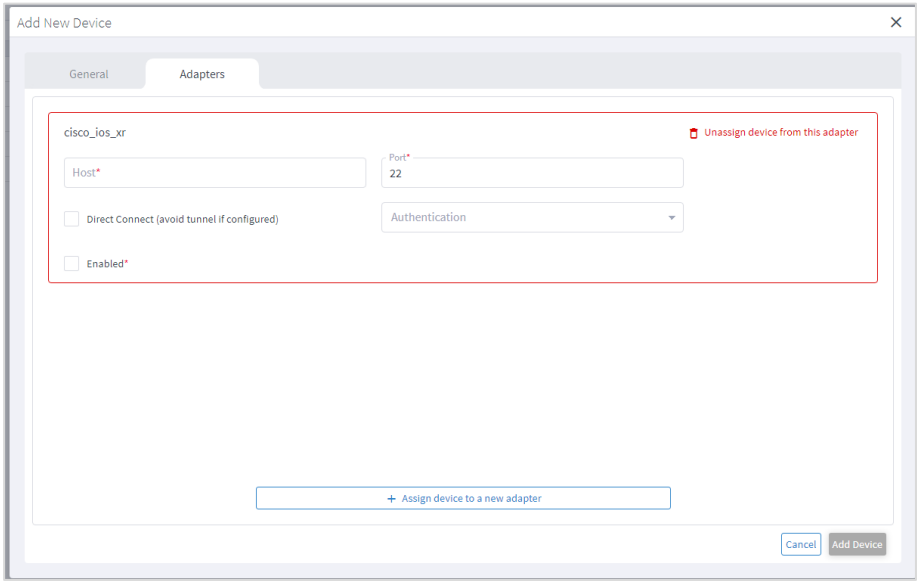
8. [アダプタ（Adapter）] タブを選択します。



9. [デバイスの新しいアダプタへの割り当て（Assign device to a new adapter）] をクリックします。



10. 割り当て先のアダプタを選択し、[割り当て（Assign）] をクリックします。



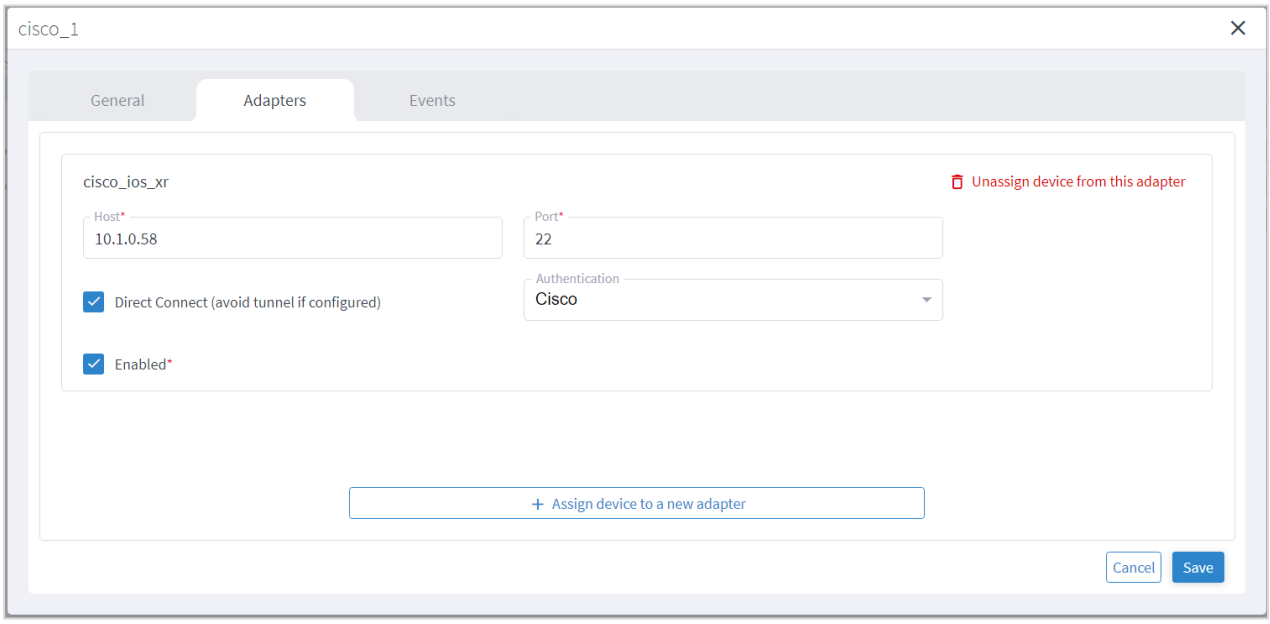
11. アダプタの詳細を入力します。
    - **ホスト（Host）**
    - **ポート（Port）**
    - **直接接続（Direct Connect）**（設定されている場合はトンネルを避けます）
    - **認証（Authentication）**（これがログイン情報です）
    - **[有効（Enabled）]**
12. [保存（Save）] をクリックします。
13. 必要な数のアダプタについて、手順を繰り返します。
14. [Add Device] をクリックします。

デバイスのアダプタへの割り当て

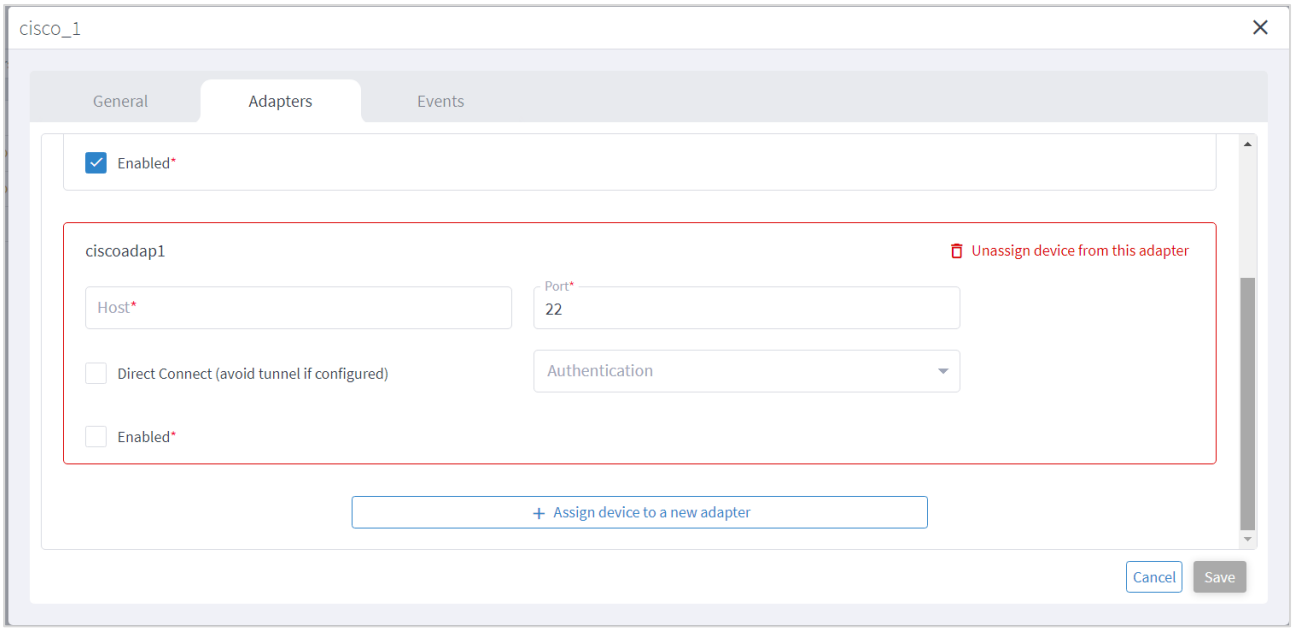
デバイスを 1 つ以上のアダプタに割り当てることができます。

デバイスを割り当てるには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] を選択します。
2. [管理対象デバイス（Managed Devices）] タブを選択します。
3. 必要なデバイス行をクリックします（[名前（Name）] 列のリンクではありません）。
4. [アダプタ（Adapter）] タブを選択します。



5. [デバイスの新しいアダプタへの割り当て（Assign device to a new adapter）] をクリックします。
6. アダプタを選択し、[割り当て（Assign）] をクリックします。



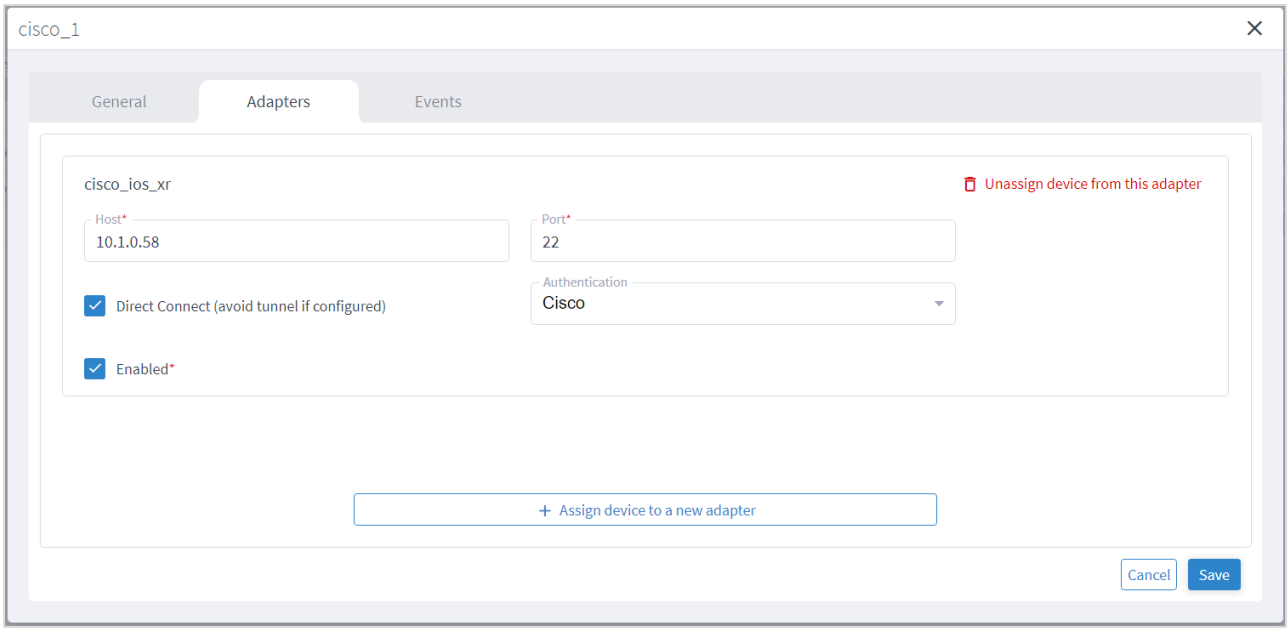
7. 次の手順を実行します。
   - **ホスト（Host）**
   - **ポート（Port）**
   - **直接接続（Direct Connect）**（設定されている場合はトンネルを避けます）
   - **認証（Authentication）**（これがクレデンシャルです）
   - **[有効（Enabled）]**
8. [保存（Save）] をクリックします。

デバイスの割り当て解除

アダプタからデバイスの割り当てを解除できます。デバイスはアダプターから削除されますが、モデルには残ります。

アダプタからデバイスの割り当てを（デバイスから）解除するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] を選択します。
2. [管理対象デバイス（Managed Devices）] タブを選択します。
3. 必要なデバイス行をクリックします（[名前（Name）] 列のリンクではありません）。
4. [アダプタ（Adapter）] タブを選択します。



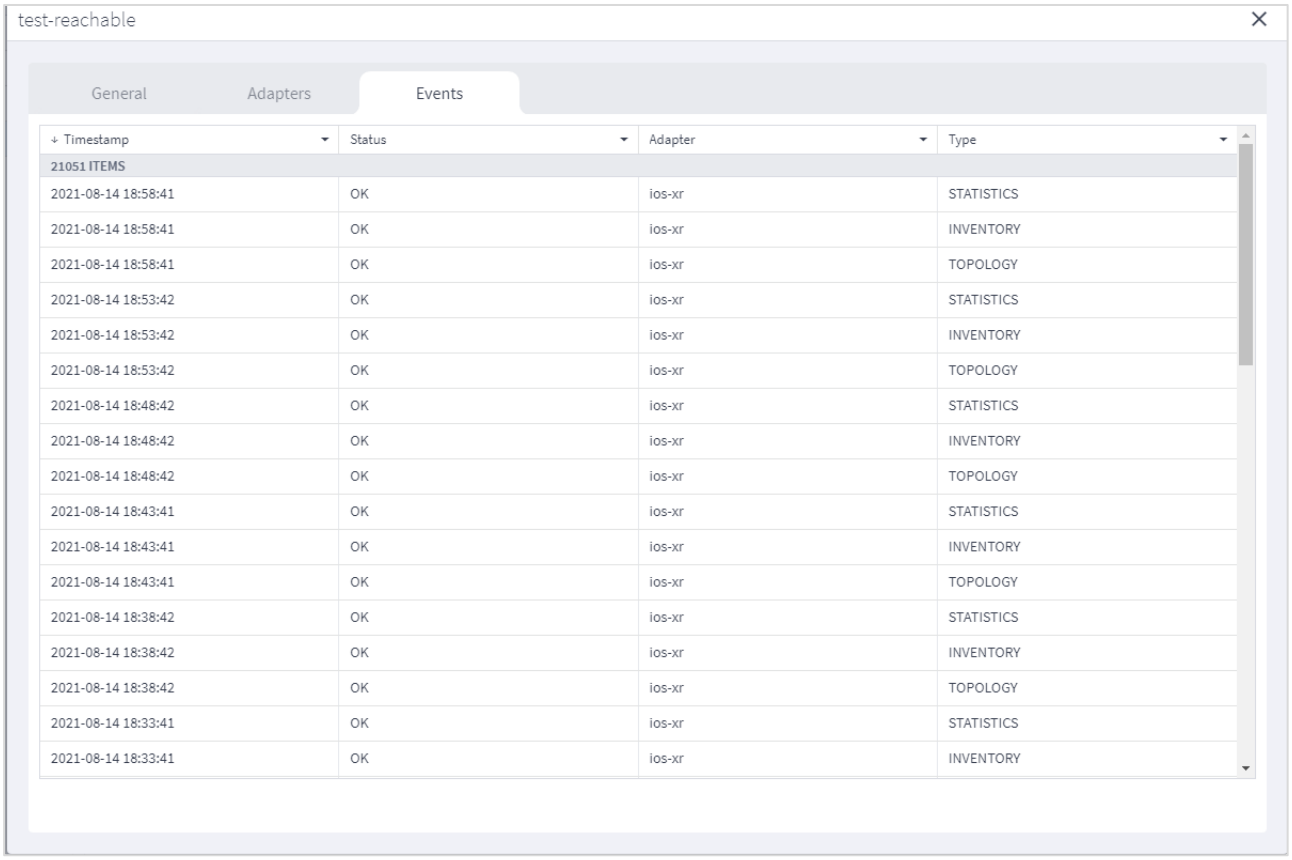
5. [このアダプタからデバイスを割り当てを解除（Unassign device from this adapter）] をクリックします。
6. [保存（Save）] をクリックします。

デバイスイベントの表示

デバイスのイベントを表示できます。アダプタは定期的にデバイスをポーリングします。

デバイスイベントを表示するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] を選択します。
2. [管理対象デバイス（Managed Devices）] タブを選択します。
3. 必要なデバイス行をクリックします（[名前（Name）] 列のリンクではありません）。
4. [イベント（Events）] タブをクリックします。

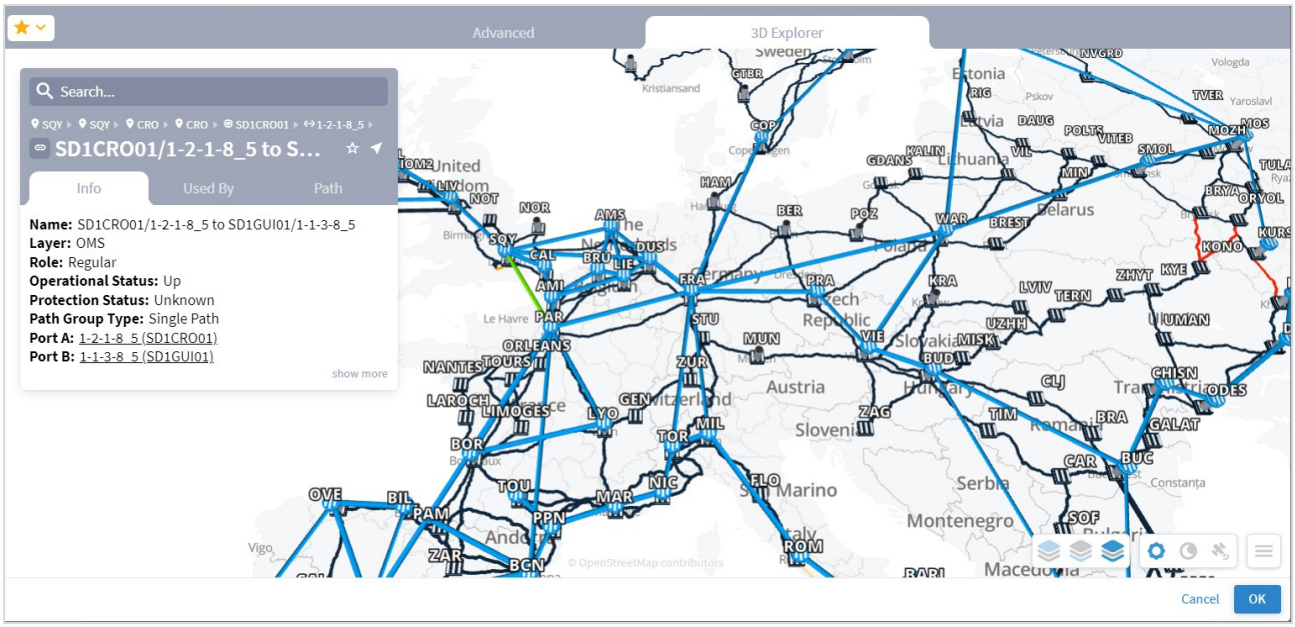


Edit Device

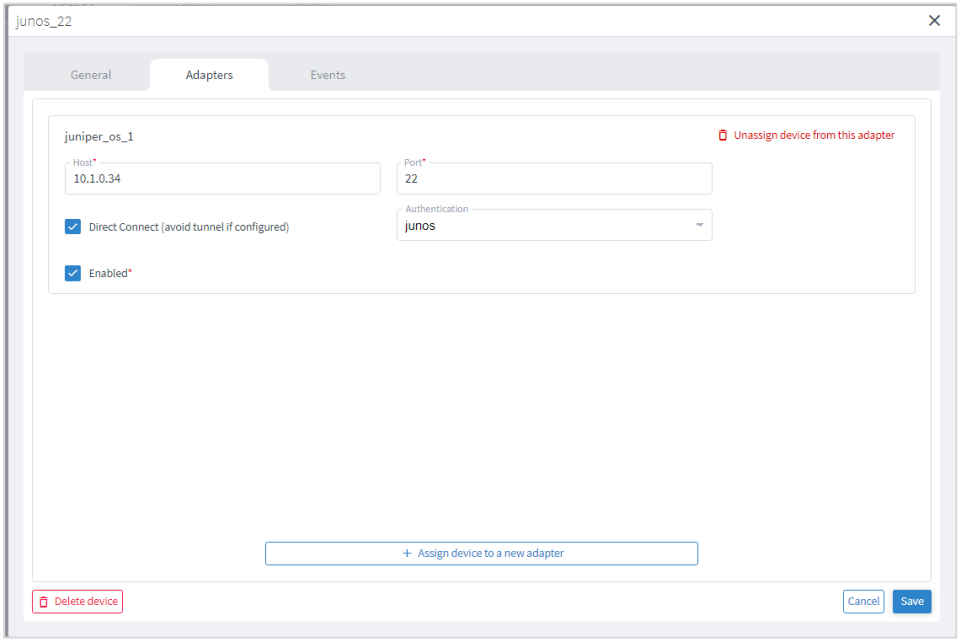
デバイスを編集して Explorer でネットワーク要素を選択したり、デバイスをアダプタに割り当てたり、アダプタからデバイスの割り当てを解除したりできます。

デバイスを編集するには以下を実行します。

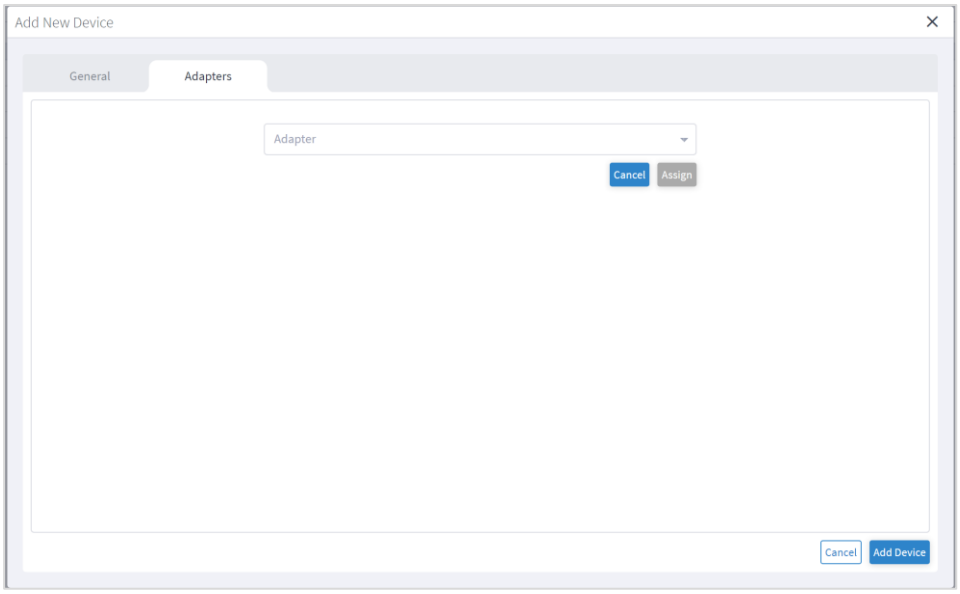
1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] を選択します。
2. 必要なアダプタを選択します。
3. [管理対象デバイス（Managed Devices）] タブを選択します。
4. 必要なデバイス行をクリックします（[名前（Name）] 列のリンクではありません）。
5. [全般（General）] タブの [ネットワーク要素のサイト（Network Element Site）] をクリックして、Explorer でネットワーク要素を選択します。
6. [3D Explorer] タブを選択します。
7. ネットワーク要素を選択します。



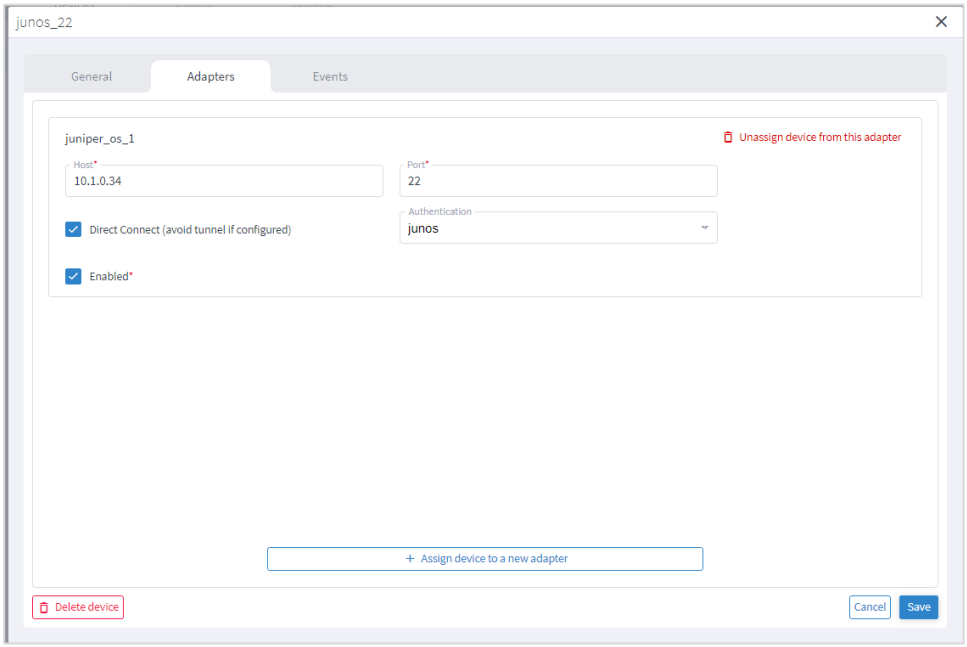
8. [OK] をクリックします。
9. [アダプタ（Adapter）] タブを選択します。



10. アダプタからデバイスの割り当てを解除するには、[このアダプタからデバイスの割り当てを解除（Unassign device from the adapter）] をクリックします。
11. デバイスをアダプタに割り当てるには、[デバイスの新しいアダプタへの割り当て（Assign device to a new adapter）] をクリックします。



12. 割り当て先のアダプタを選択し、[割り当て（Assign）] をクリックします。



13. アダプタの詳細を入力します。
    - **ホスト（Host）**
    - **ポート（Port）**
    - **直接接続（Direct Connect）**（設定されている場合はトンネルを避けます）
    - **認証（Authentication）**（これがログイン情報です）
    - **[有効（Enabled）]**
14. [保存（Save）] をクリックします。

デバイスの削除

デバイスを削除して、アダプタから割り当てを解除できます。この場合はデバイスがモデルから削除されます。

または、デバイスをモデルに保持し、デバイスの割り当てのみを解除する場合は、「デバイスの割り当て解除」を参照してください。

デバイスを削除する手順は、次のとおりです。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [デバイスマネージャ（Device Manager）] を選択します。
2. 必要なアダプタを選択します。
3. [管理対象デバイス（Managed Devices）] タブを選択します。
4. 必要なデバイス行をクリックします（[名前（Name）] 列のリンクではありません）。
5. [デバイスの削除（Delete device）] をクリックします。確認メッセージが表示されます。
6. [確認（Confirm）] をクリックしてデバイスを削除し、すべてのアダプタから割り当てを解除して、デバイスをモデルから削除します。

モデル設定

ネットワークモデルには地域（ネットワークサイトが配置されている地理的エリア）が含まれ、サイト（ネットワーク内の論理グループ）はモデル内で定義されます。さらに、リソースにテキストラベルのタグを付けることができ、さまざまなアプリケーションでのフィルタ処理に使用できます。

地域とサイトの詳細については、『*Cisco Crosswork Hierarchical Controller Network Visualization Guide*』を参照してください。

リージョン

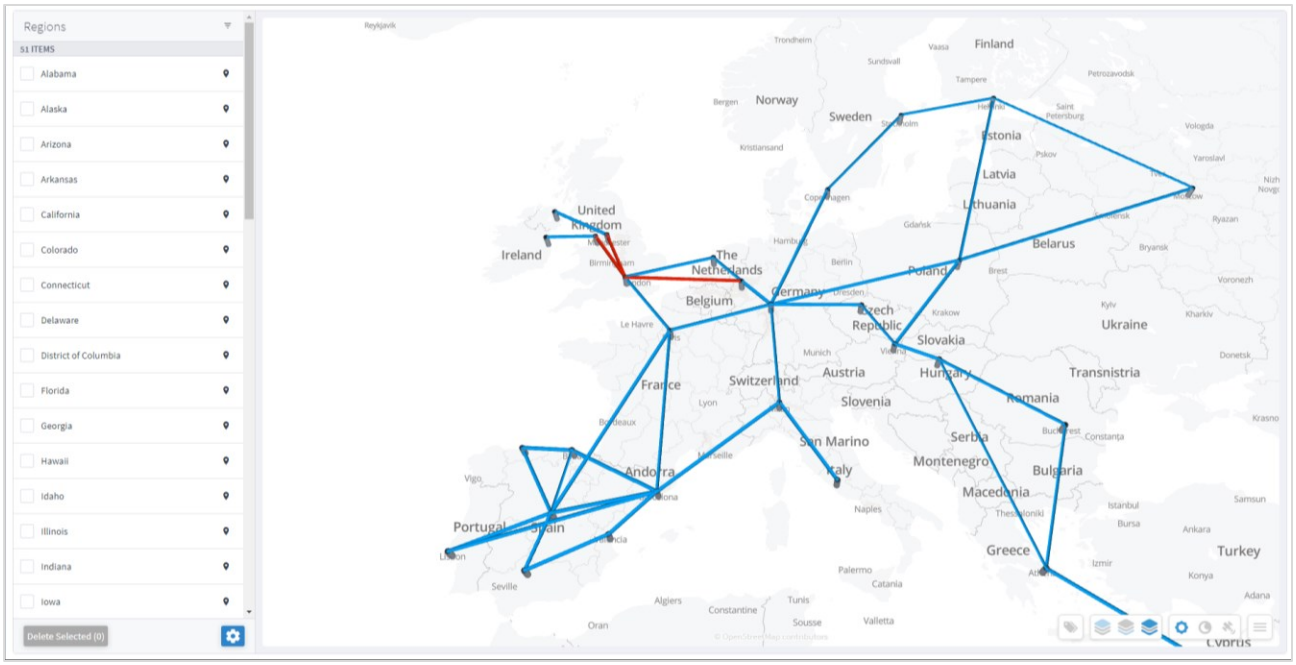
リージョンは、ネットワークサイトが配置されている地理的エリアです。モデル設定アプリケーションを使用すると、リージョンの表示とフィルタ処理、リージョンの削除、リージョンのエクスポートおよびインポートを実行できます。通常、シスコはお客様と協力してモデルにリージョンを設定します。

リージョンの表示

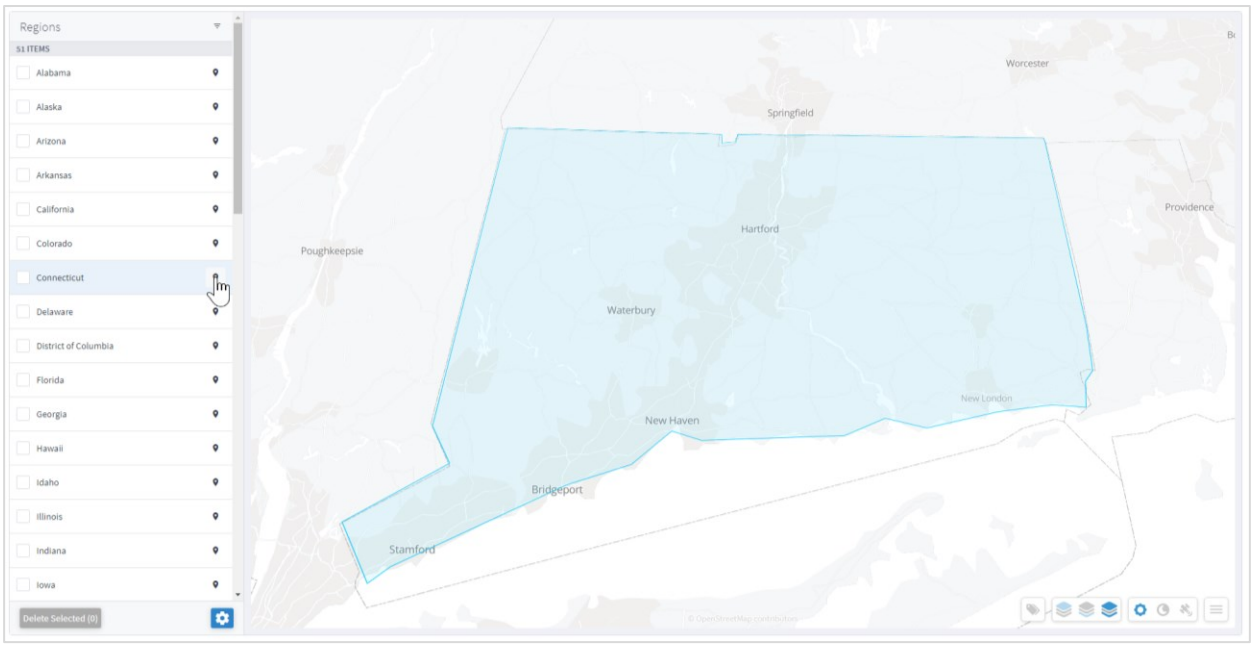
[モデル設定（Model Settings）] でリージョンを表示できます。

モデル設定でリージョンを表示するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。
2. [リージョン（Regions）] タブを選択します。



3. リージョンを表示するには、[リージョン（Regions）] で必要なリージョンの（例：コネチカット）の横をクリックします。選択したリージョンにマップが移動します。リージョンの概要が表示されます。

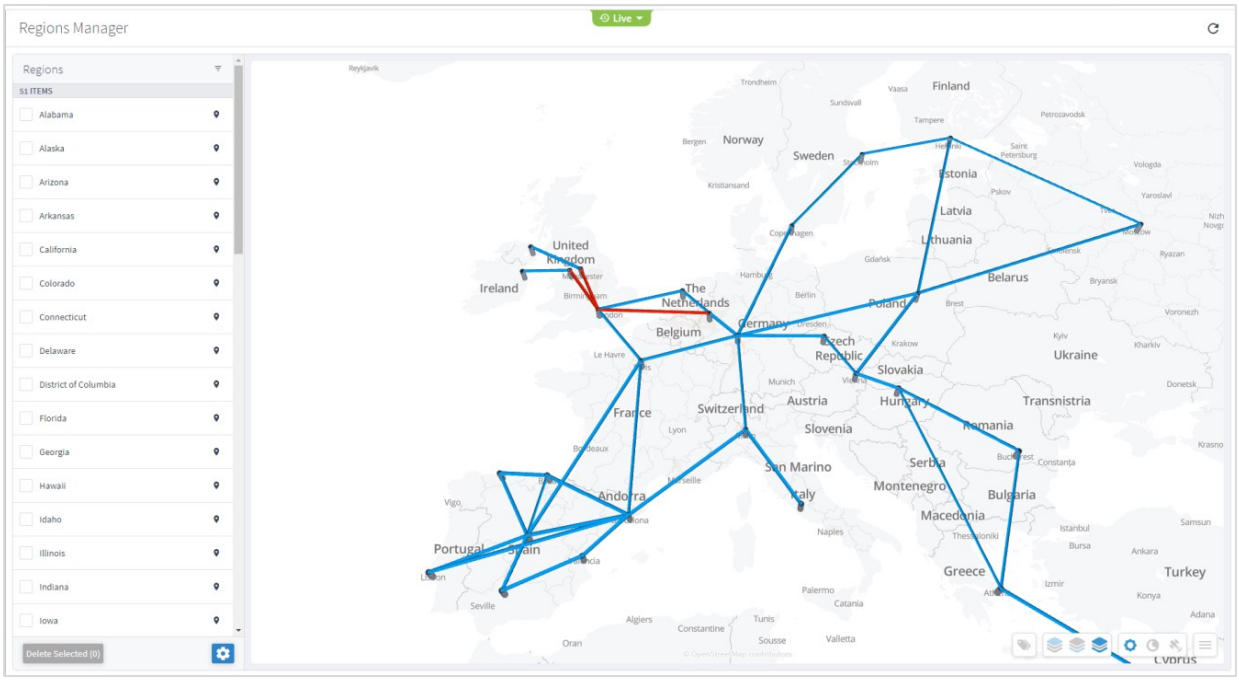


リージョンのフィルタ処理

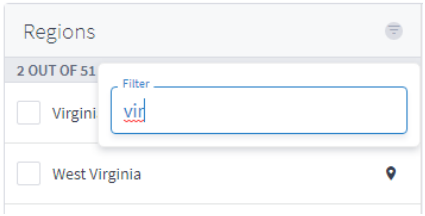
リージョンをフィルタ処理できます。

リージョンをフィルタ処理するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。
2. [リージョン（Regions）] タブを選択します。



3. リージョンをフィルタ処理するには、 をクリックしてフィルタ条件を入力します（大文字と小文字は区別されません）。



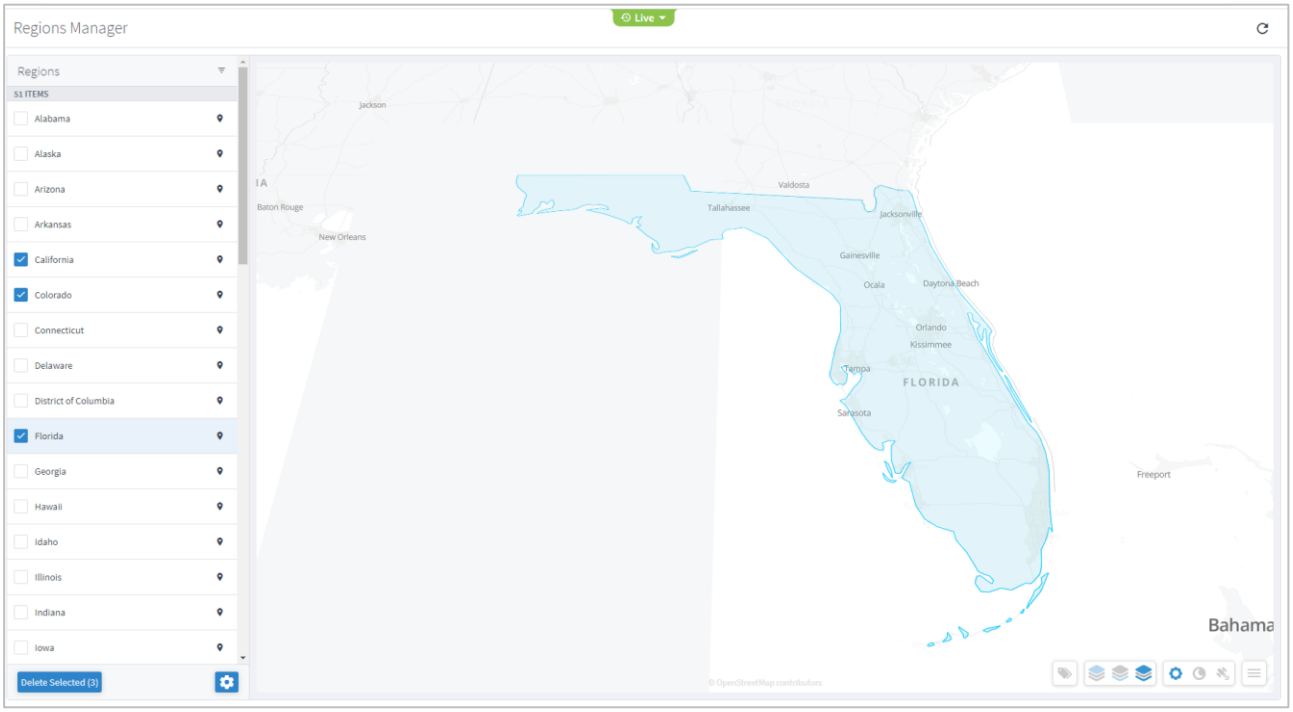
リージョンの削除

リージョンマネージャでリージョンを削除できます。

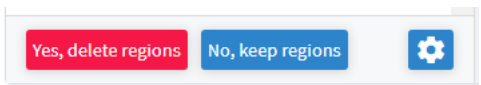
リージョンマネージャーでリージョンを削除するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。
2. [リージョン（Regions）] タブを選択します。

3. [リージョン（Regions）] で、1 つ以上のリージョンを選択します。



4. [選択項目の削除（Delete Selected）] をクリックします。



5. リージョンを削除するには、[はい、リージョンを削除します（Yes, delete regions）] をクリックします。

リージョンのエクスポートおよびインポート

通常、シスコはお客様と協力してモデルにリージョンを設定します。リージョンは、http://geojson.io/ で公開されている標準に従って設定され、GeoJSON または Region POJO でエクスポートまたはインポートできます。

次の形式でリージョンをインポート（およびエクスポート）できます。

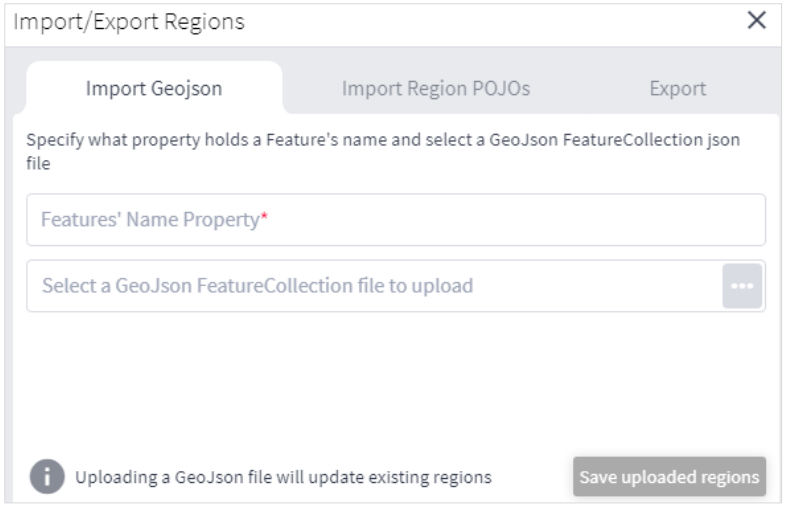
- GeoJSON
- Region POJO

リージョンの有効なジオメトリタイプは次のとおりです。

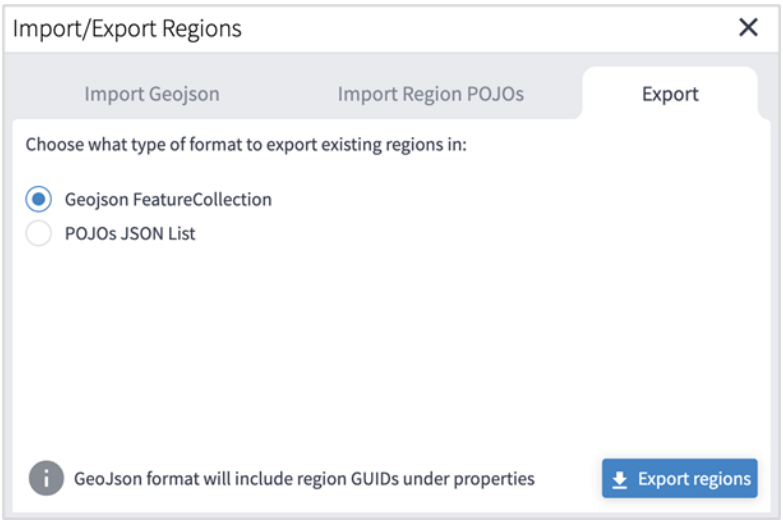
- Point
- LineString
- Polygon
- MultiPoint
- MultiLineString
- マルチポリゴン

リージョンをエクスポートするには以下を実行します。

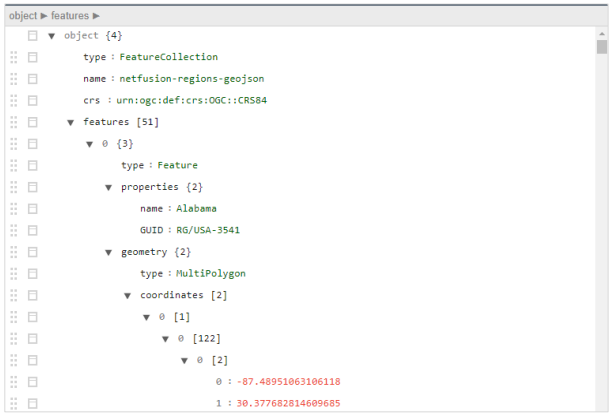
1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。
2. [リージョン（Regions）] タブを選択します。
3. [リージョン（Regions）] で、 をクリックします。



4. [リージョン（Regions）] でエクスポートするには、[エクスポート（Export）] タブを選択します。



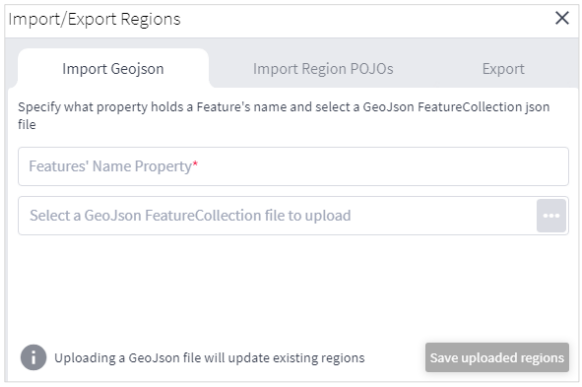
5. 必要な形式を選択してから、[リージョンのエクスポート（Export regions）] をクリックします。 JSON ファイルがダウンロードされます。
6. （オプション）JSON フォーマッタを使用してコンテンツを確認します。



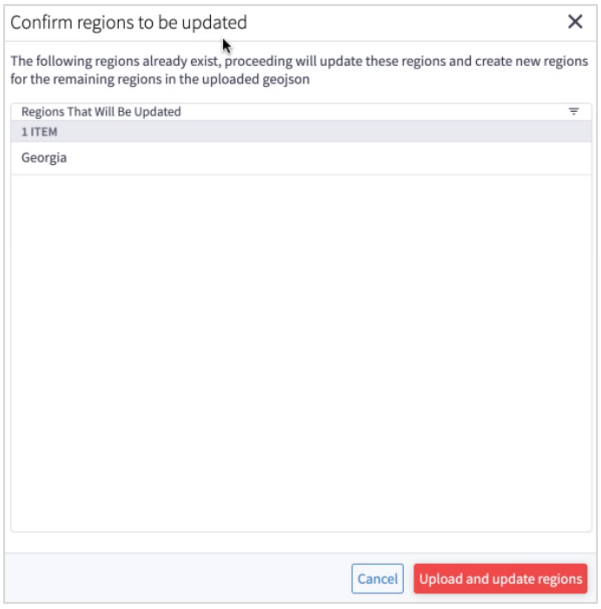
リージョンをインポートするには以下を実行します。

1. （オプション 1）**GeoJSON** 形式のインポートファイルを準備します。
    - 正しい形式でファイルを簡単に作成するには、現在のリージョンを必要な形式でエクスポートしてからファイルを編集します。
    - GeoJSON インポートファイルは、単一の **Feature** GeoJSON ファイルではなく、**FeatureCollection** GeoJSON ファイルである必要があります。
    - GeoJSON インポートファイルには、ファイルをインポートするときに指定されるリージョン名のプロパティが必要です。
    - GeoJSON インポートファイルには、各リージョンの GUID が含まれる場合があります。GUID が指定されていない場合、リージョンマネージャは GeoJSON 機能の GUID を生成します。GUID が指定されている場合、リージョンマネージャはそれを使用し、その GUID を持つリージョンが既に存在する場合は更新されます。
    - 同じリージョン名（および含まれている場合は GUID）を使用できるのは 1 度のみです。
    - リージョン名の大文字と小文字は区別されません。
    - GUID または名前が同じリージョンが既に存在する場合、ファイルをインポートすると、続行するとリージョンが更新されることを通知するメッセージが表示されます。
2. （オプション 2）Region POJO 形式のインポートファイルを準備します。
    - 正しい形式でファイルを簡単に作成するには、現在のリージョンを必要な形式でエクスポートしてからファイルを編集します。
    - RegionPOJO インポートファイルの形式は固定で、リージョン名のプロパティは **name** です。ファイルをインポートする際、このプロパティを指定する必要はありません。
    - RegionPOJO インポートファイルには、プロパティとしてリージョン GUID が含まれている必要があります。
    - 同じリージョン名と GUID を使用できるのは 1 度のみです。
    - リージョン名の大文字と小文字は区別されません。
    - GUID または名前が同じリージョンが既に存在する場合、ファイルをインポートすると、続行するとリージョンが更新されることを通知するメッセージが表示されます。
3. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。
4. [リージョン（Regions）] タブを選択します。

5. [リージョン（Regions）] で、 をクリックします。



6. GeoJSON 形式でリージョンをインポートするには以下を実行します。
   - リージョン名を含むプロパティを入力します。通常、これは name です。
   - アップロードするファイルを選択します。
7. Region POJO 形式でリージョンをインポートするには以下を実行します。
   - [Region POJO のインポート（Import Region POJOs）] タブを選択します。
   - アップロードするファイルを選択します。
8. [アップロードされたリージョンを保存（Save uploaded regions）] をクリックします。JSON ファイルが処理されます。
9. 既存のリージョンに更新がある場合、更新されるリージョンのリストが表示されます。続行するには、[リージョンのアップロードと更新（Upload and update regions）] をクリックします。



リージョン API

通常、シスコのセールスエンジニアがモデルにリージョンとオーバーレイを設定します。リージョンは、http://geojson.io/ で公開されている標準に従って設定されます。リージョンの定義を返すように、モデルにクエリを実行できます。これにより、リージョンの GUID、名前、座標、ジオメトリタイプが返されます。リージョンの有効なジオメトリタイプは、Point、LineString、Polygon、MultiPoint、MultiLineString、MultiPolygon です。

Crosswork Hierarchical Controller では、デバイスはサイトに接続されています。サイトには地理的な座標（緯度、経度）があります。サイトは 1 つ以上のリージョンにある場合があります。

オーバーラップは、アフリカの国々など、複数のリージョンをグループ化するために使用されます。

次の目的で使用できる API がいくつかあります。

- リージョンの定義を取得する。
- 1 つ以上のリージョンのサイトを取得する。
- オーバーレイにリージョンを追加する。
- オーバーレイのサイトを取得する。

いくつか例を以下に示します。

- RG/1 リージョンの定義を返すには、次の GET コマンドを実行します。

  ```
  curl -skL -u admin:admin -H 'Content-Type: application/json'
  https://$SERVER/api/v2/config/regions/RG/1 | jq
  ```

- エストニアとギリシャのリージョンにあるサイトを返すには以下を実行します。

  ```
  curl -skL -u admin:admin -H 'Content-Type: application/json'
  https://$SERVER/api/v2/config/regions/RG/1 | jq
  ```

- エストニアとギリシャのリージョンにあるサイトを返すには以下を実行します。

  ```
  curl -skL -u admin:admin -H 'Content-Type: text/plain'  -d 'region[.name in
  ("Estonia", "Greece")] | site' https://$server/api/v2/shql
  ```

- エストニアとギリシャのリージョンを overlay_europe のオーバーラップに追加するには以下を実行します。

  ```
  curl -X PUT -skL -u admin:admin -H 'Content-Type: application/json' -d '{"guid":
  "RG/116", "overlay": "overlay_europe"}' https://$SERVER/api/v2/config/regions/RG/116
  ```

  ```
  curl -X PUT -skL -u admin:admin -H 'Content-Type: application/json' -d '{"guid":
  "RG/154", "overlay": "overlay_europe"}' https://$SERVER/api/v2/config/regions/RG/154
  ```

- overlay_europe オーバーレイのサイトを返すには以下を実行します。

  https://$SERVER/api/v2/config/regions/RG/154

  ```
  curl -skL -u admin:admin -H 'Content-Type: text/plain' -d 'region[.overlay =
  "overlay_europe"] | site' https://$SERVER/api/v2/shql | jq | grep -c name
  ```

  リージョンとオーバーレイを SHQL で使用して、モデルをクエリできます。リンクまたはサイトを使用して、モデルを下に遷移できます。

  特定のリージョン内のすべてのリンクを返すには（SHQL を使用）、次のコマンドを実行します。

  ```
  region[.name = "France"] | link
  ```

サイト

サイトは、ネットワーク内の論理グループです。モデル設定アプリケーションを使用すると、サイトの表示とフィルタ処理、サイトの削除、サイトのエクスポートおよびインポートを実行できます。通常、シスコはお客様と協力してモデルにサイトを設定します。

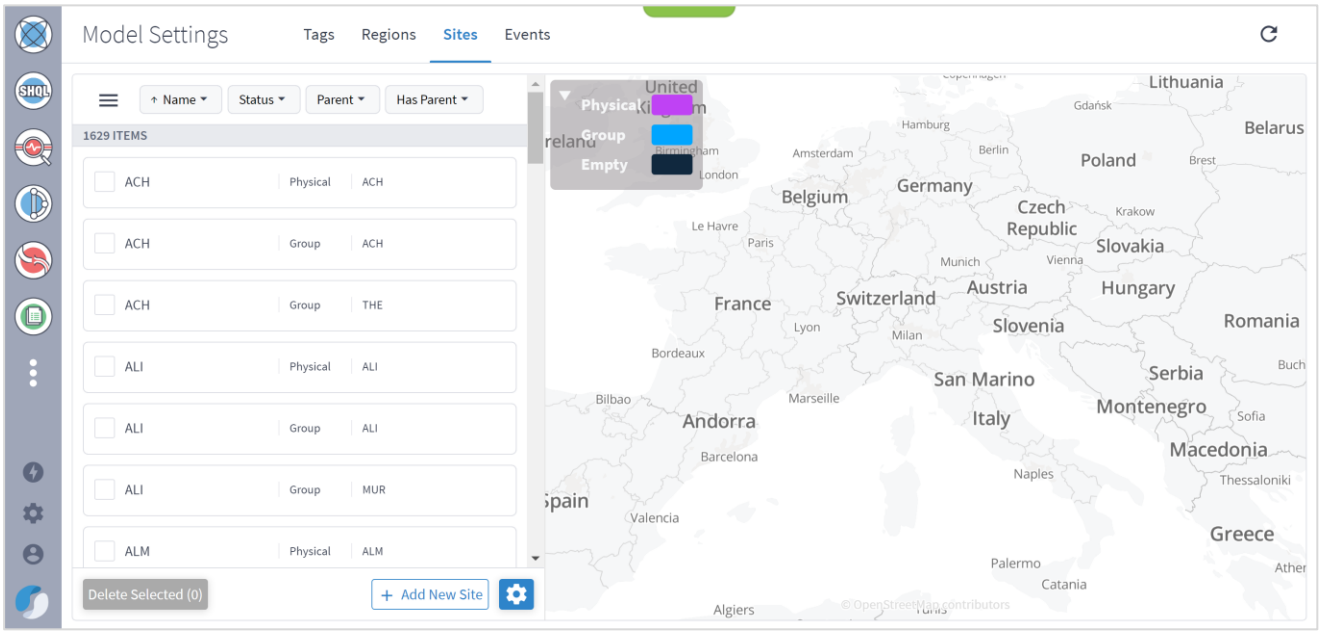
サイト内の物理オブジェクトは親オブジェクトによってグループ化することができ、さらに次のレベルの親オブジェクトによってグループ化し、これを続けることができます。唯一の制限は、すべてのサイトが同じ数のレベルを持つ必要があることです。

サイトの表示

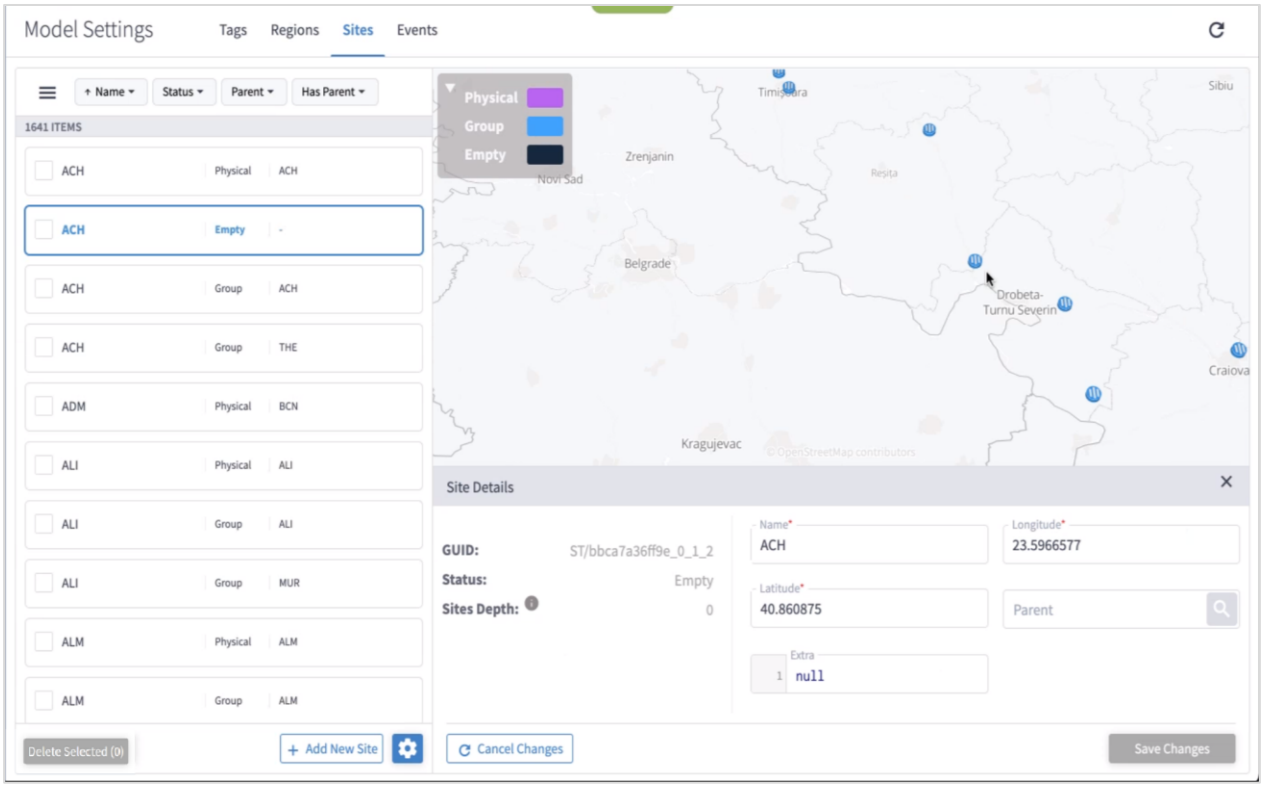
[モデル設定（Model Settings）] でサイトを表示できます。

モデル設定でサイトを表示するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。]
2. [サイト（Site）] タブをクリックします。



3. サイトアイテムを表示するには、[サイト（Site）] で必要なサイトアイテムをクリックします。選択したサイトアイテムにマップが移動します。

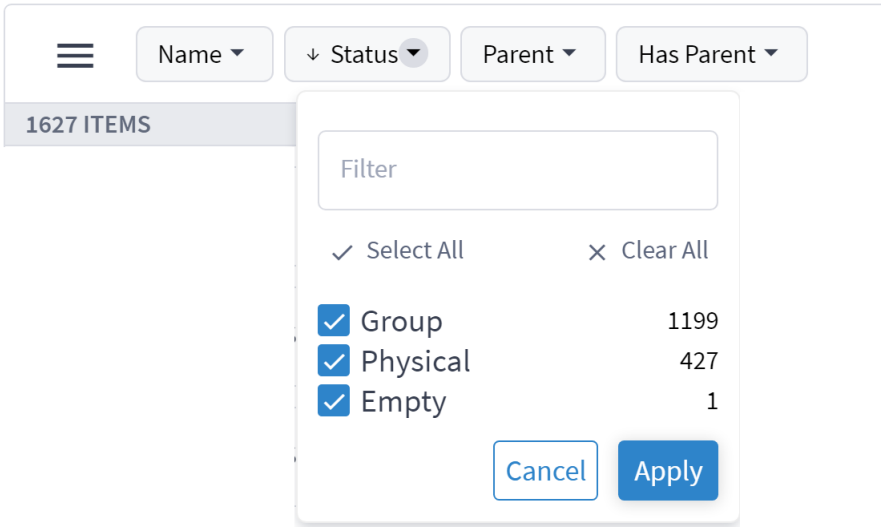


サイトのフィルタ処理

名前、ステータス、親、または親を持つサイトでサイトをフィルタ処理できます。

サイトをフィルタ処理するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーション バーで、[サービス] > [モデル設定（Model Settings）] を選択します。
2. [サイト（Site）] タブをクリックします。
3. サイトをフィルタ処理するには、フィルタ基準をクリックして選択するか、入力します（大文字と小文字は区別されません）。

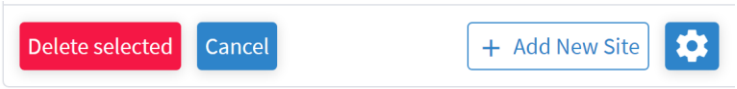


サイトの削除

サイトマネージャでサイトを削除できます。

サイトマネージャでサイトを削除するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。
2. [サイト（Site）] タブを選択します。
3. [サイト（Site）] で 1 つ以上のサイトを選択します。
4. [選択項目の削除（Delete Selected）] をクリックします。確認が表示されます。
5. 削除するには、[選択項目の削除（Delete Selected）] をクリックします。

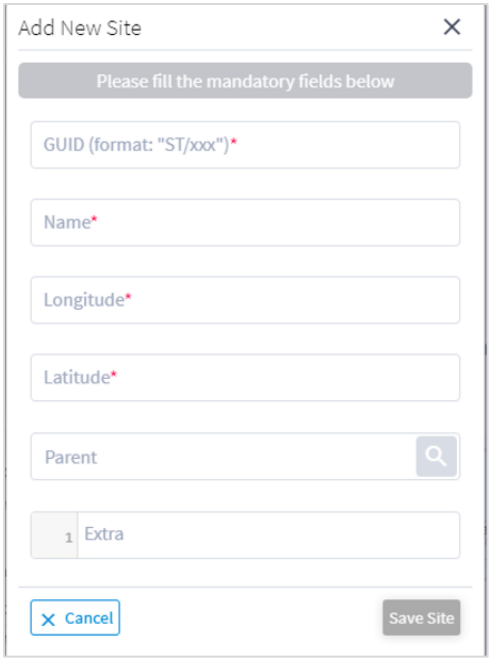


サイトの追加

サイトマネージャでサイトを追加できます。

サイトマネージャでサイトを追加するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。
2. [サイト（Site）] タブを選択します。
3. [新規サイトの追加（Add New Site）] をクリックします。



4. サイトの詳細を入力します。例：**ST/London**。
5. [サイトの保存（Save Site）] をクリックします。

サイトのエクスポートとインポート

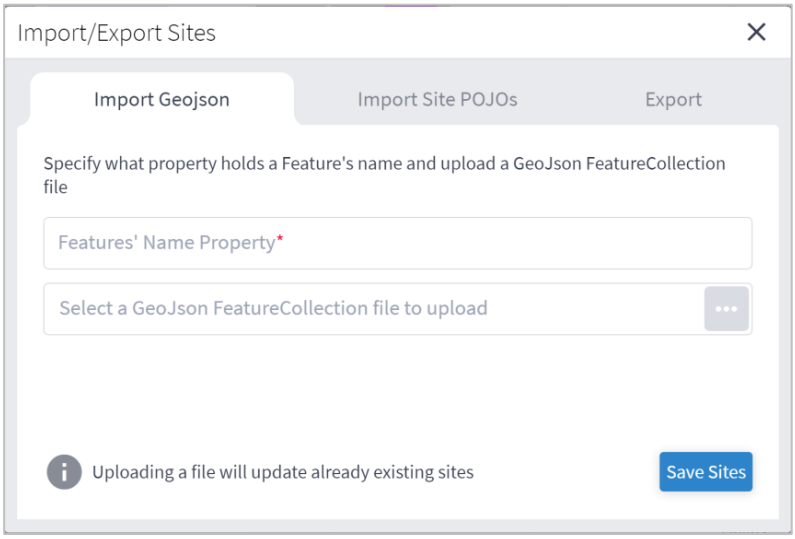
通常、シスコはお客様と協力してモデルにサイトを設定します。サイトは、http://geojson.io/ で公開されている標準に従って設定され、GeoJSON または Site POJO でエクスポートまたはインポートできます。

次の形式でサイトをインポート（およびエクスポート）できます。

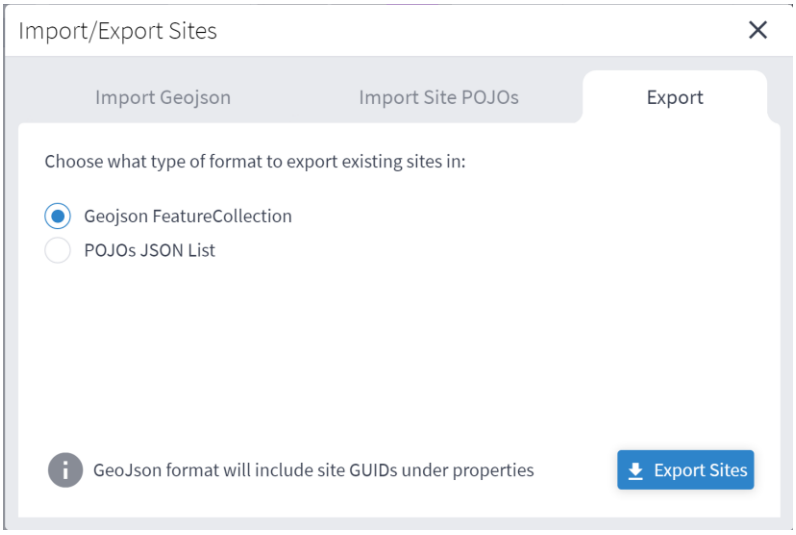
- GeoJSON
- Site POJO

サイトをエクスポートするには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。
2. [サイト（Site）] タブをクリックします。
3. [サイト（Site）] で、 をクリックします。



4. [サイト（SIte）] でエクスポートするには、[エクスポート（Export）] タブを選択します。



5. 必要な形式を選択してから、[サイトのエクスポート（Export sites）] をクリックします。 **netfusion-sites-geojson.json** ファイルがダウンロードされます。

6. （オプション）JSON フォーマッタを使用してコンテンツを確認します。

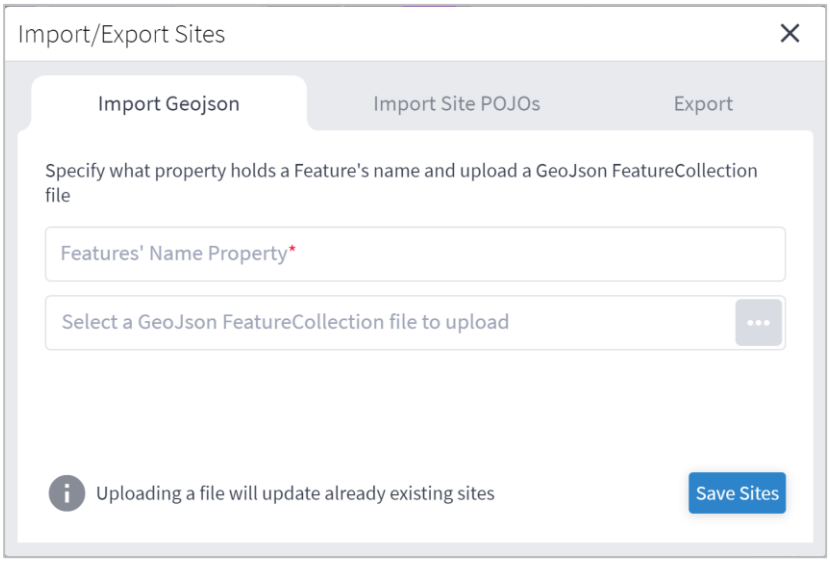
```
{
  "site": [
    {
      "guid": "ST/001ca9f0dc37",
      "latitude": 51.5105384,
      "longitude": -0.5950406,
      "name": "SLO",
      "parent": {
        "guid": "ST/001ca9f0dc37_0"
      },
      "extra": null
    },
    {
      "guid": "ST/001ca9f0dc37_0",
      "latitude": 51.5105384,
      "longitude": -0.5950406,
      "name": "SLO",
      "parent": {
        "guid": "ST/2971737bd3ba_0_1"
      },
      "extra": null
    },
    {
      "guid": "ST/002d237f16fb8c65",
      "latitude": 37.9020842,
      "longitude": -6.5648524,
      "name": "ILA-SD1EVO01-SD1SEV01-1",
      "parent": {
        "guid": "ST/002d237f16fb8c65_0"
      },
      "extra": null
    },
    {
      "guid": "ST/002d237f16fb8c65_0",
      "latitude": 37.9020842,
      "longitude": -6.5648524,
      "name": "ILA-SD1EVO01-SD1SEV01-1",
```

サイトをインポートするには以下を実行します。

1. （オプション 1）**GeoJSON** 形式のインポートファイルを準備します。
   - 正しい形式でファイルを簡単に作成するには、現在のサイトを必要な形式でエクスポートしてからファイルを編集します。
   - GeoJSON インポートファイルは、単一の Feature GeoJSON ファイルではなく、**FeatureCollection** GeoJSON ファイルである必要があります。
   - GeoJSON インポートファイルには、ファイルをインポートするときに指定されるサイト名プロパティが必要です。
   - GeoJSON インポートファイルには、各サイトの GUID が含まれる場合があります。GUID が指定されていない場合、サイトマネージャは GeoJSON 機能の GUID を生成します。GUID が指定されている場合、サイトマネージャはそれを使用し、その GUID を持つサイトが既に存在する場合は更新されます。
   - 同じサイト名（および含まれている場合は GUID）を使用できるのは 1 度のみです。

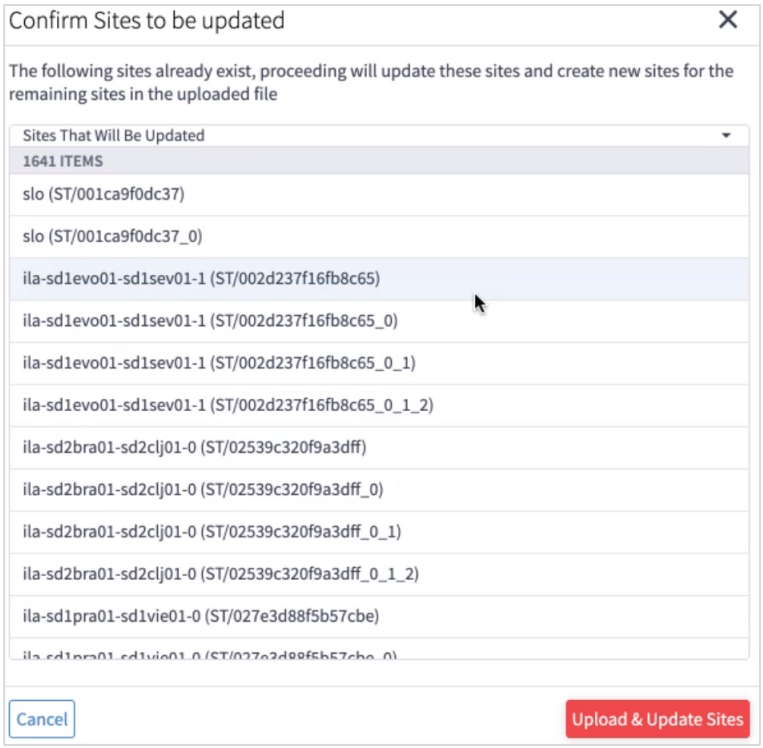
- サイト名の大文字と小文字は区別されません。
- GUID または名前が同じサイトが既に存在する場合、ファイルをインポートすると、続行するとサイトが更新されることを通知するメッセージが表示されます。

2. （オプション 2）Site POJO 形式のインポートファイルを準備します。
   - 正しい形式でファイルを簡単に作成するには、現在のサイトを必要な形式でエクスポートしてからファイルを編集します。
   - SitePOJO インポートファイルの形式は固定で、サイト名のプロパティは name です。ファイルをインポートする際、このプロパティを指定する必要はありません。
   - SitePOJO インポートファイルには、プロパティとしてサイト GUID が含まれている必要があります。
   - 同じサイト名と GUID を使用できるのは 1 度のみです。
   - サイト名の大文字と小文字は区別されません。
   - GUID または名前が同じサイトが既に存在する場合、ファイルをインポートすると、続行するとサイトが更新されることを通知するメッセージが表示されます。
3. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。
4. [サイト（Site）] タブをクリックします。
5. [サイト（Site）] で、 をクリックします。



6. GeoJSON 形式でサイトをインポートするには以下を実行します。
   - サイト名を含むプロパティを入力します。通常、これは name です。
   - アップロードするファイルを選択します。

7. Site POJO 形式でサイトをインポートするには以下を実行します。
    - [Site POJO のインポート（Import Site POJOs）] タブを選択します。
    - アップロードするファイルを選択します。
8. [アップロードされたサイトを保存（Save uploaded sites）] をクリックします。JSON ファイルが処理されます。
9. 既存のサイトに更新がある場合、更新されるサイトのリストが表示されます。続行するには、[サイトのアップロードと更新（Upload and Update Sites）] をクリックします。



タグ

リソースには、テキストラベルでタグを付けることができます（「キー：値のペアを使用）モデル設定アプリケーションで（またはタグ API を使用して）タグを表示、追加、削除できます。

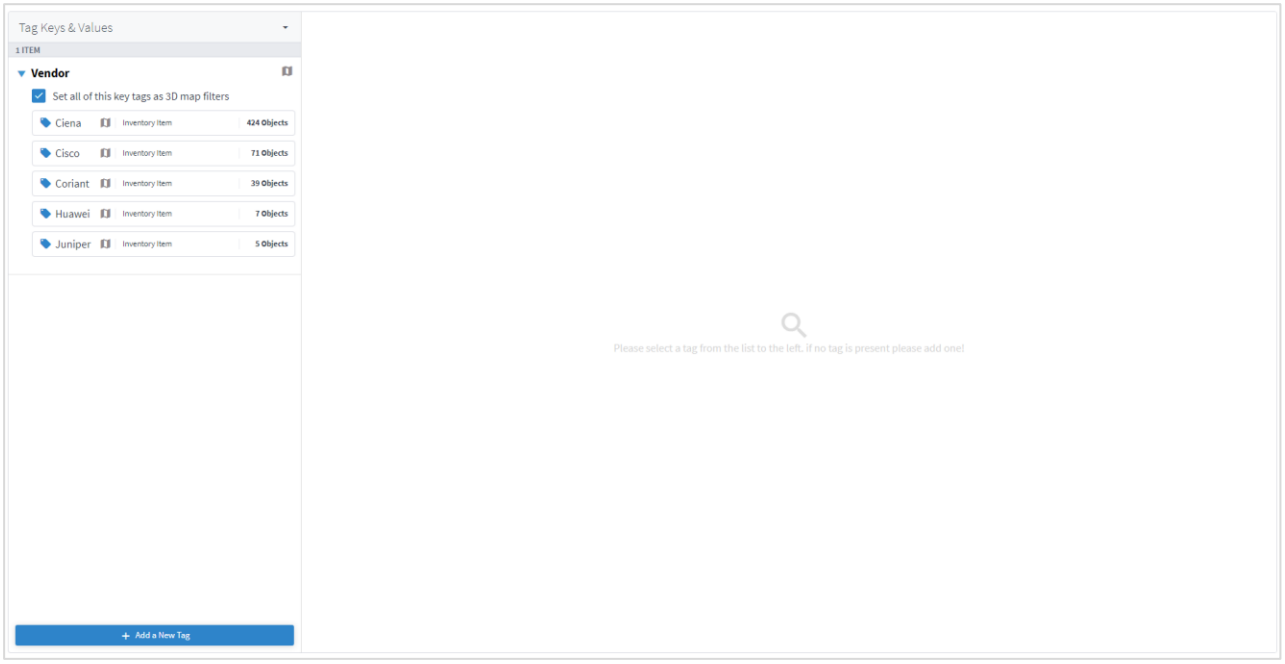
タグは次のように使用できます。

- たとえば Explorer では、リンクタグで 3D マップをフィルタ処理できます。これはマップに表示されるリンク（論理、OMS）に適用され、マップフィルタとして使用するタグを選択できます。
- ネットワーク インベントリ アプリケーションでは、タグを列として表示できます。
- パス最適化アプリケーションでは、タグを付けたリンクにテストを実行し、タグを付けたリンクをパスから除外できます。
- ネットワーク脆弱性アプリケーションでは、タグを付けたルータにテストを実行できます。
- 根本原因分析アプリケーションでは、タグで結果をフィルタ処理できます。

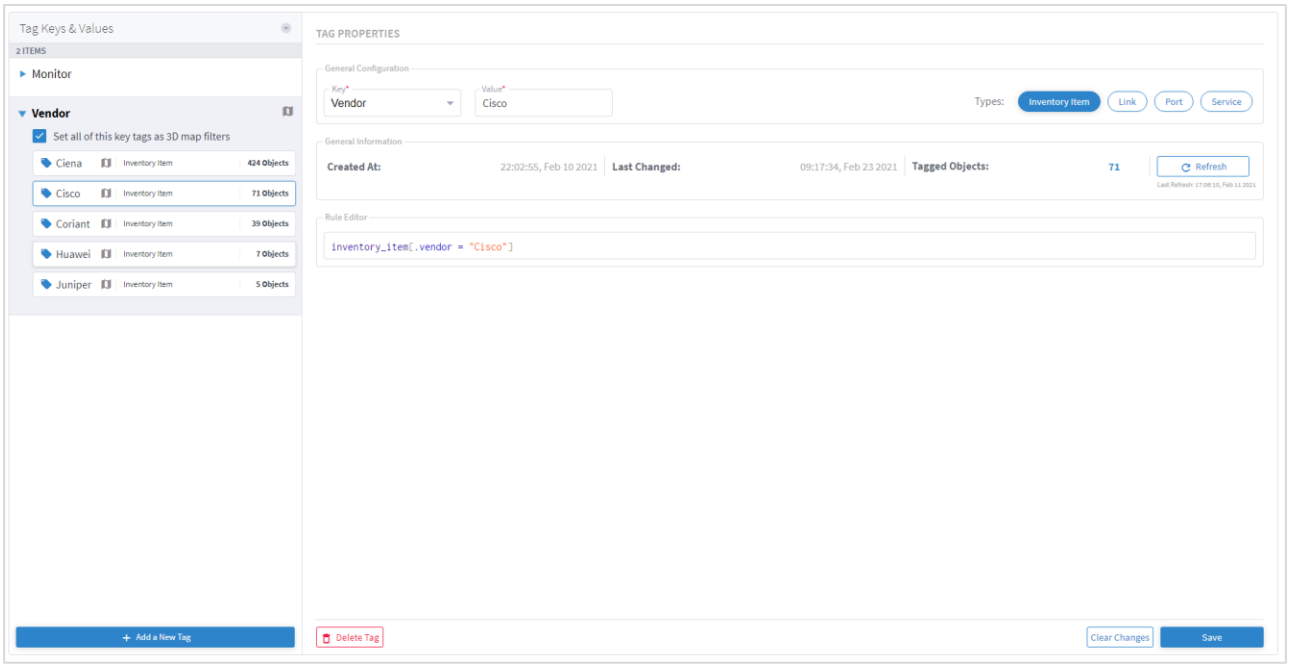
タグの表示

モデル設定でタグを表示するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。
2. [タグ（Tag）] タブを選択します。



3. タグを表示するには、タグキーを展開して値を選択します（たとえば、[ベンダー（Vendor）] を展開します）。

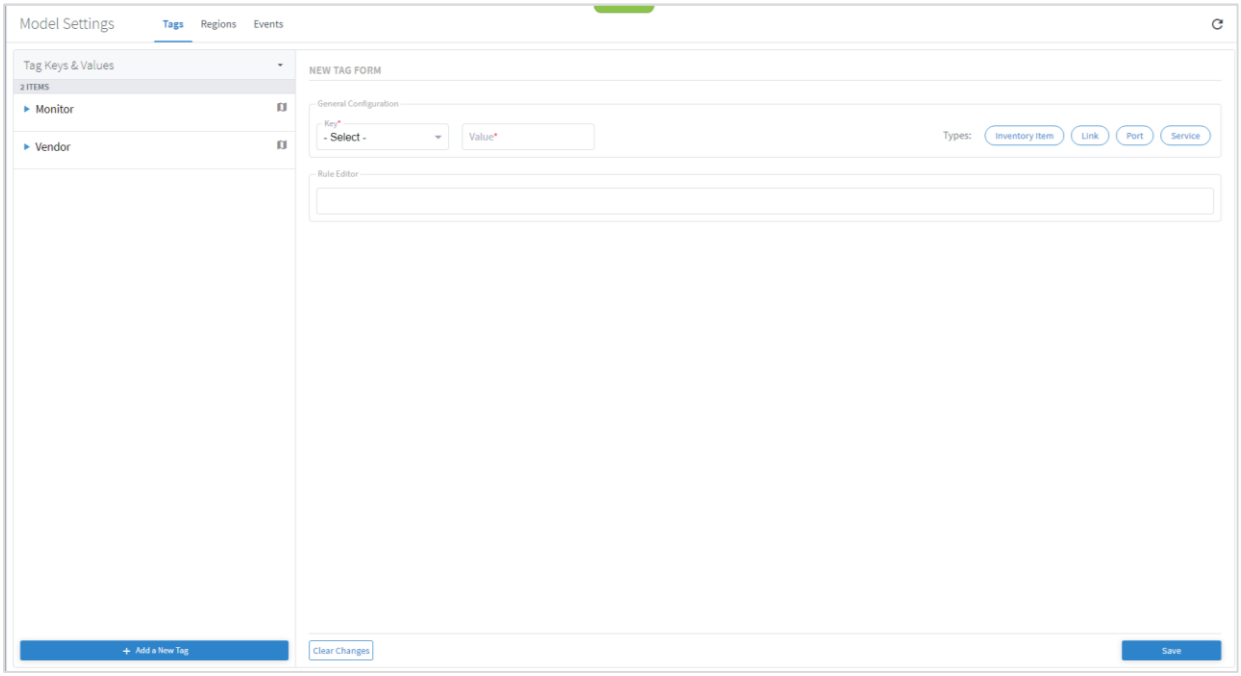


[タグの追加（Add Tags）]

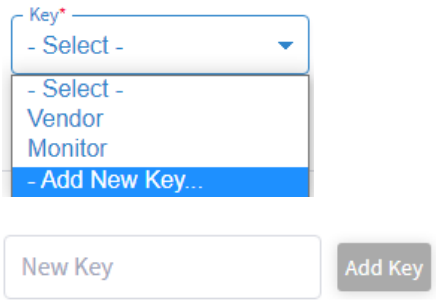
既存のタグに新しい値を追加するか、新しいタグを追加できます。

モデル設定でタグを追加するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。
2. [タグ（Tag）] タブを選択します。
3. [新規タグの追加（Add a New Tag）] をクリックします。

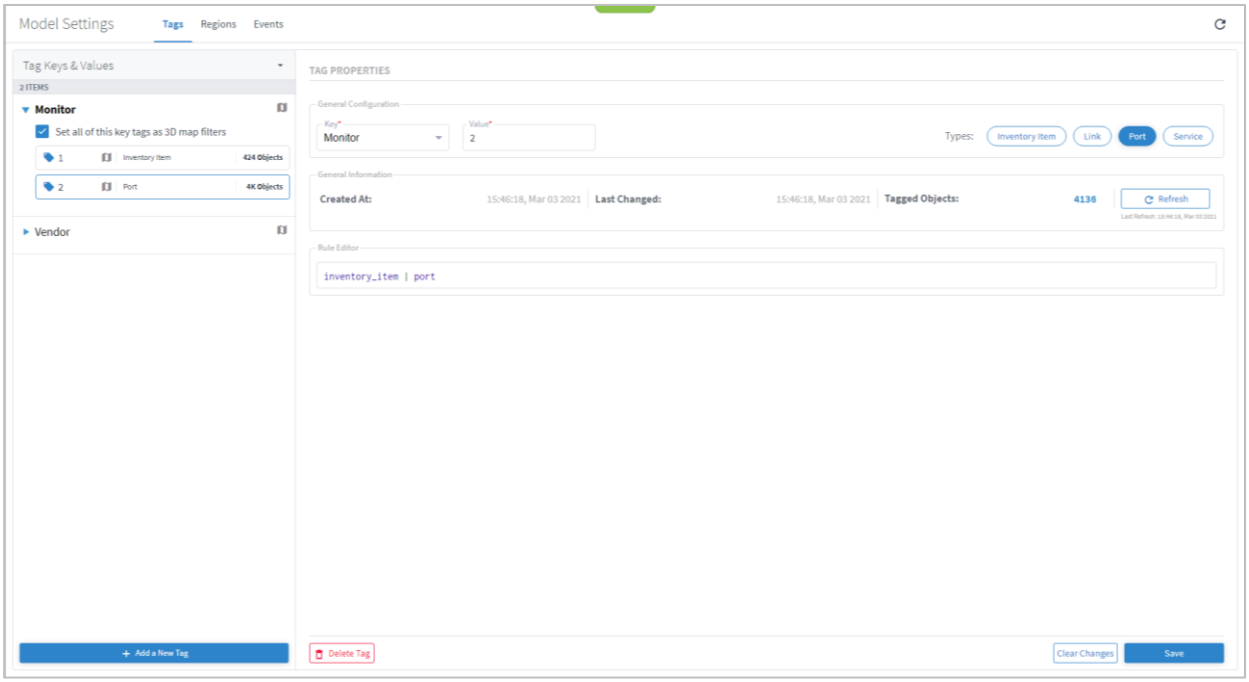


4. 新しいキーを追加するには、[キー（Key）] ドロップダウンから [新規キーの追加（Add New Key）] を選択します。



5. キー名を入力し、[キーの追加（Add Key）] をクリックします。
6. 既存のキーに新しい値を追加するには、[キー（Key）] ドロップダウンから既存のキーを選択し、新しい [値（Value）] を入力します。

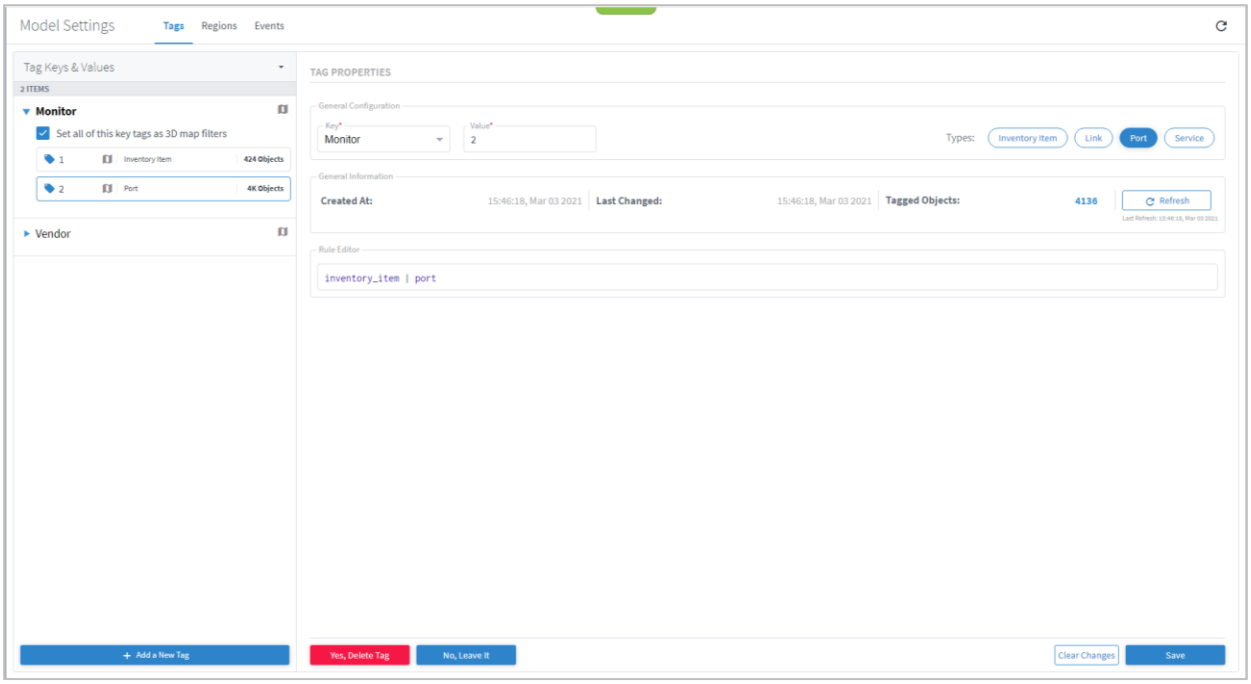
7. [ルールエディタ（Rule Editor）] で、キーと値を適用するために必要なリソースを選択します。たとえば、[インベントリアイテム|ポート（inventory_item | port）] を選択し、[保存（Save）] をクリックします。キーのエントリが追加され、タグが付けられているオブジェクトの数を確認できます。



タグの削除

モデル設定でタグを削除するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。
2. [タグ（Tag）] タブを選択します。
3. 必要なタグキーを展開し、タグ値を選択します。
4. [タグを削除（Delete Tag）]をクリックします。



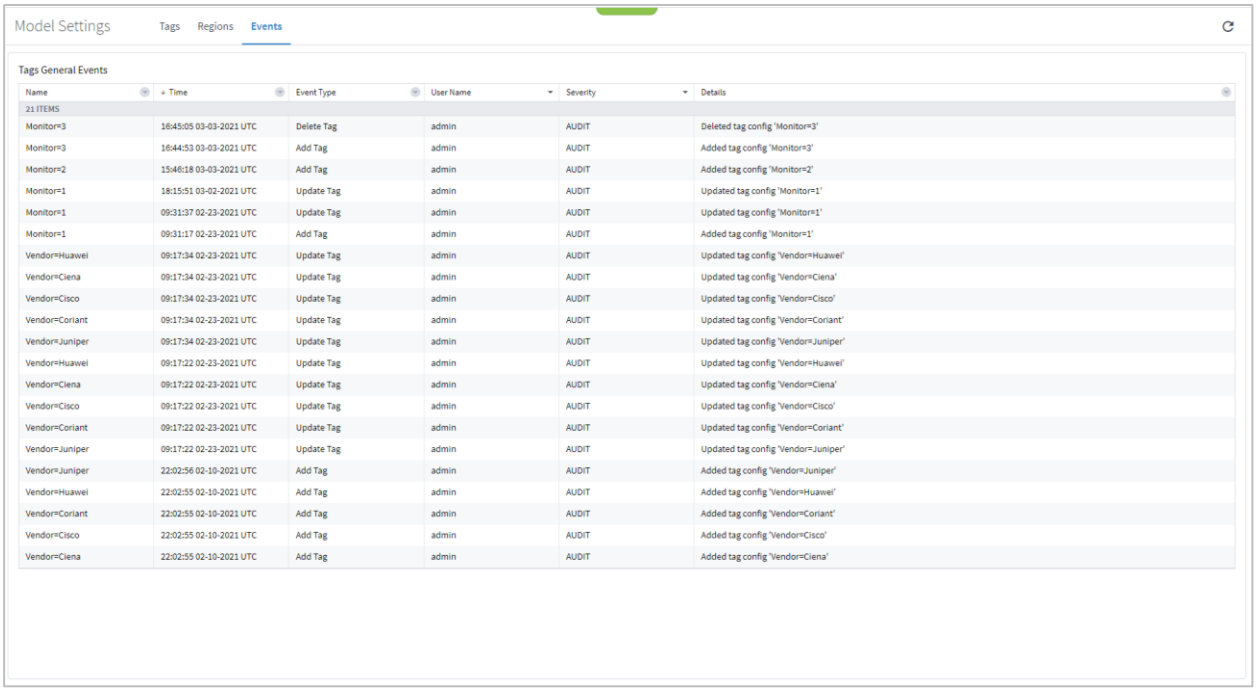
5. [はい、タグを削除します（Yes, Delete Tag）] をクリックします。

タグのイベントの表示

タグの追加、更新、削除イベントのリストを表示できます。

モデル設定でタグイベントを表示するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーションバーで、[サービス（Services）] > [モデル設定（Model Settings）] を選択します。
2. [イベント（Events）] タブをクリックします。



タグ API

タグは、API または SHQL によっても追加または変更できます。

タグでデバイスを取得

SHQL アプリケーションを使用してタグでデバイスを取得できます。

- ベンダータグが Ciena に設定されているすべてのデバイスを返すには以下を実行します（SHQL を使用）。

```
inventory[.tags.Vendor has ("Ciena")]
```

デバイスへのタグの追加

タグを作成し、タグ API を使用して、値を付けたタグをデバイス（または複数のデバイス）に割り当てることができます。この API は、パラメータとして SHQL ルールを使用します。SHQL ルールによって返されるすべてのデバイスは、指定された値でタグ付けされます。たとえば、これによってベンダータグが作成され、ベンダーが Ciena であるすべてのインベントリアイテムに Ciena の値が割り当てられます。

```
 POST "https://$SERVER/api/v2/config/tags" -H 'Content-Type: application/json' -d
"{
     \"category\": \"Vendor\",
     \"value\": \"Ciena\",
     \"rules\": [
          \"inventory_item[.vendor = Error! Hyperlink reference not valid. "
  }"
```

パラメータ	説明
category	ベンダーなどのタグ カテゴリ。
value	デバイスにタグを付けるための値（Ciena など）。
ルール	適用する SHQL ルール。ルールは必ずアイテムを返す必要があります。 ルールでは、地域、タグ、サイト、インベントリを使用します。

たとえば、特定のリージョンのすべてのデバイスを返すクエリを使用して、デバイスにタグを追加できます。

```
 POST  "https://$SERVER/api/v2/config/tags" -H 'Content-Type: application/json' -
d "{
      \"category\": \"Region\",
      \"value\": \"RG_2\",
      \"rules\": [
           \"region[.guid = \\\"RG/2\\\"] | site | inventory\"
      ]
  }"
```

タグの削除

タグを削除できます。

```
DELETE "https://$SERVER/api/v2/config/tags/Vendor=Ciena"
```

管理対象デバイス

デバイスマネージャの [管理対象デバイス（Managed Device）] テーブルでは、デバイスごと（およびアダプタに割り当てられたすべてのデバイスの総合）に以下のステータスが表示されます。

	情報の種類		
有効な値	インベントリ	トポロジ	統計
OK	特定の種類の情報を収集するアダプタがデバイスの NMS システムまたはデバイス自体に正常に到達し、デバイスデータを検出した場合。		
ERROR	特定の種類の情報を収集しているアダプタがデバイスに到達したものの、必要な情報を収集できなかった場合（クレデンシャルが正しくない、コマンドタイプエラー、データが存在しないなど）。		
UNREACHABLE	特定の種類の情報を収集するアダプタがデバイスに到達できなかった場合。通常は接続の問題が原因です。		
WARNING	該当なし	該当なし	統計情報を収集するアダプタが一部のデバイスポートのデータを取得できなかった場合。
UNKNOWN	アダプタによってステータスが報告されなかった場合。これは、内部通信エラーが原因です。サポートに問い合わせてください。		

Crosswork Hierarchical Controller は、デバイスの到達可能性のステータスが変更された場合に Syslog イベントを送信します。

デバイスを追加してアダプタに割り当てることができます。

リンク管理

Link Manager アプリケーションを使用すると、IP から光ネットワークへのインターリンク（またはクロスリンク）を手動で追加および検証できます。または、アプリケーションでユーザーが追加したリンクは Crosswork Hierarchical Controller ネットワークモデルにマージされます。

イーサネットおよび NMC クロスリンクを手動で追加できます。

- イーサネットリンク - IP から光
- NMC リンク - マックスポンダまたはトランスポンダから ROADM

以下の場合に IP リンクが検証されます。

- リンクが追加されたとき、またはリンクのステータスが変更されたとき
- 定期的（構成されたサイクルタイムごと）
- ユーザーが手動で実行

注：イーサネットリンクを対象とするリンク検証は、リンクポートで受信した PM カウンタを分析することによって実行できます。

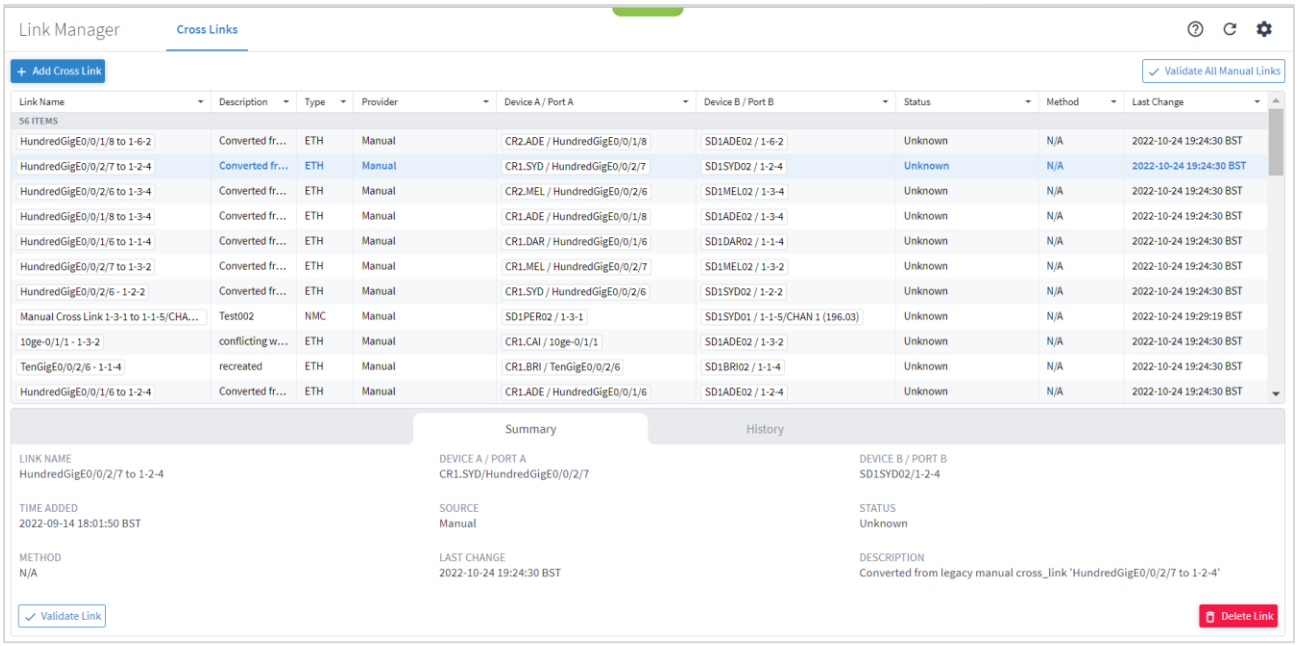
バージョン 7.0 以降、NMC リンクを検証できます。

クロスリンク情報の表示

クロスリンクを選択して、概要情報を表示できます。[プロバイダー（Provider）] 列はクロスリンクが手動で追加されたかネットワークによって検出されたかを示し、[ステータス（Status）] はクロスリンクが [不明（Unknown）]（手動またはアダプタによって追加され、まだ検証されていない）、[検証済み（Validated）]、または [可能性が低い（Unlikely）]（検証に失敗し、別の検証済みクロスリンクと一致しない）のいずれであるかを示します。

クロスリンク情報を表示するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーション バーで、[リンクマネージャ（Link Manager）] を選択します。
2. クロスリンクをクリックします。

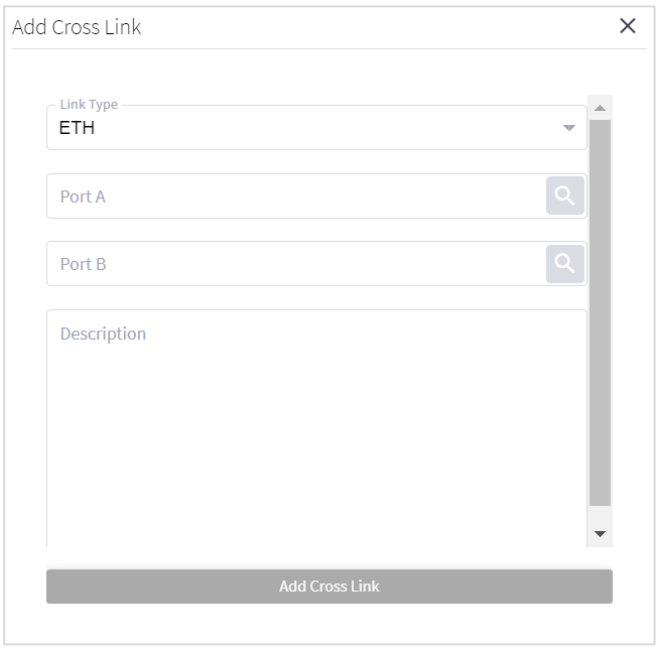


クロスリンクを追加

イーサネットまたは NMC クロスリンクを追加できます。

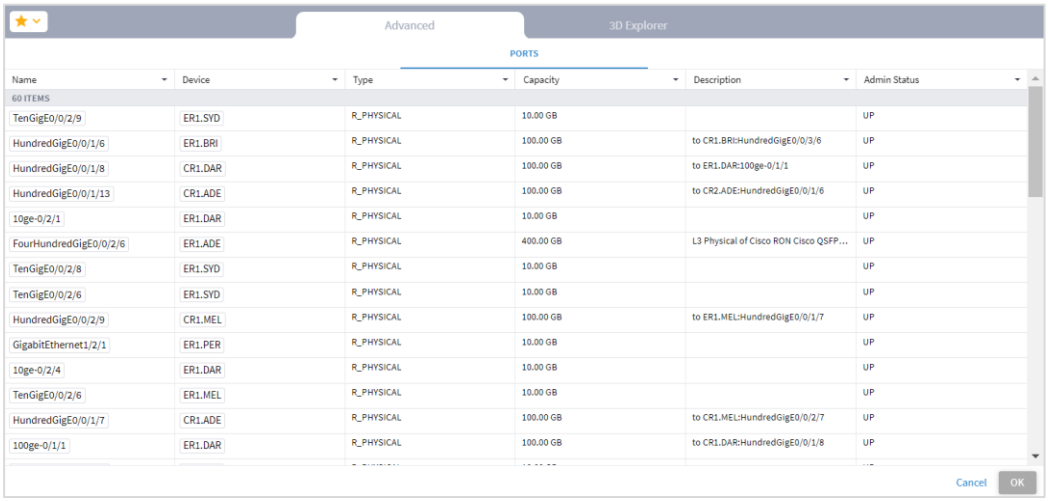
クロスリンクを追加するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーション バーで、[リンクマネージャ（Link Manager）] を選択します。
2. [クロスリンクの追加（Add Cross Link）] をクリックします。



3. リンクを追加するには、[リンクタイプ（Link Type）] で [ETH] または [NMC] を選択します。

4. [ポート A（Port A）] および [ポート B（Port B）] については、 をクリックします。[ポート（Port）] タブでポートを選択するか、[3D Explorer] タブをクリックしてポートを選択します。[OK] をクリックします。
NMC クロスリンクの場合



（注） 3D Explorer の詳細については、『*Cisco Crosswork Hierarchical Controller Network Visualization Guide*』を参照してください。

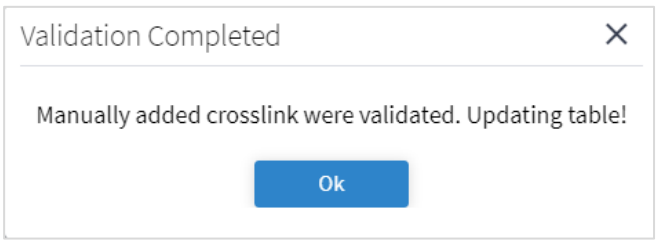
5. [説明（Description）] を追加します。
6. [クロスリンクの追加（Add Cross Link）] をクリックします。

すべての手動クロスリンクの検証

すべての手動クロス リンクを検証できます。イーサネットリンクの場合、手動で追加されたクロスリンクとネットワークから検出されたクロスリンクの間に競合が発生している場合、手動で追加されたリンクは Cisco Crosswork Hierarchical Controller ネットワークモデルから削除されます。このようなリンクは別のテーブルに残り、リンク マネージャ アプリケーションで表示できます。これにより、削除済みとしてマークされたすべてのクロスリンクも削除されます。

手動クロスリンクを検証するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーション バーで、[リンクマネージャ（Link Manager）] を選択します。
2. [すべての手動リンクを検証（Validate all Manual Links）] をクリックします。[ステータス（Status）] が更新されます。



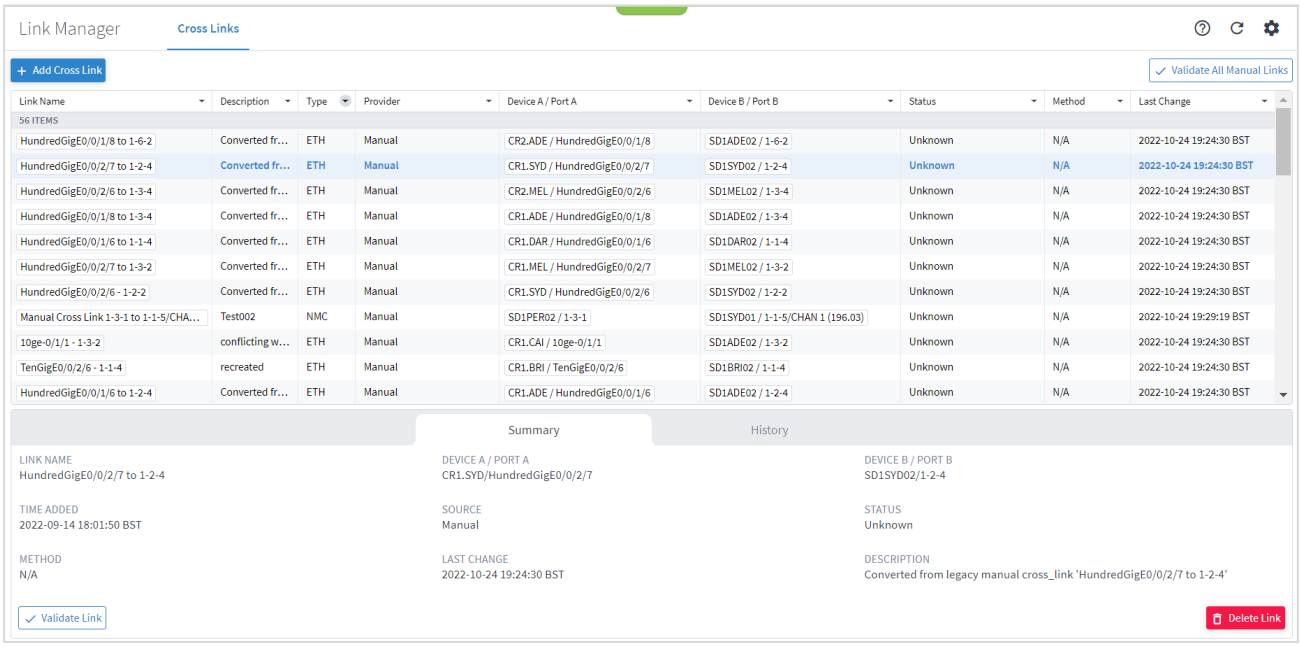
3. [OK] をクリックします。

1 つの手動クロスリンクの検証

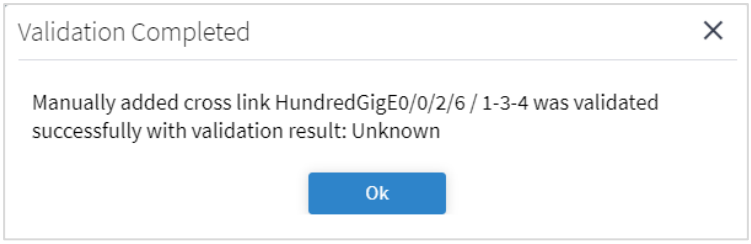
1 つの手動クロスリンクを検証できます。バージョン 6.0 では、イーサネットリンクのみを検証できます。

1 つの手動クロスリンクを検証するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーション バーで、[リンクマネージャ（Link Manager）] を選択します。
2. 必要な手動リンクを選択します。



3. 下部のペインで、[リンクの検証（Validate Link）] をクリックします。



4. [OK] をクリックします。

NMC リンクの検証

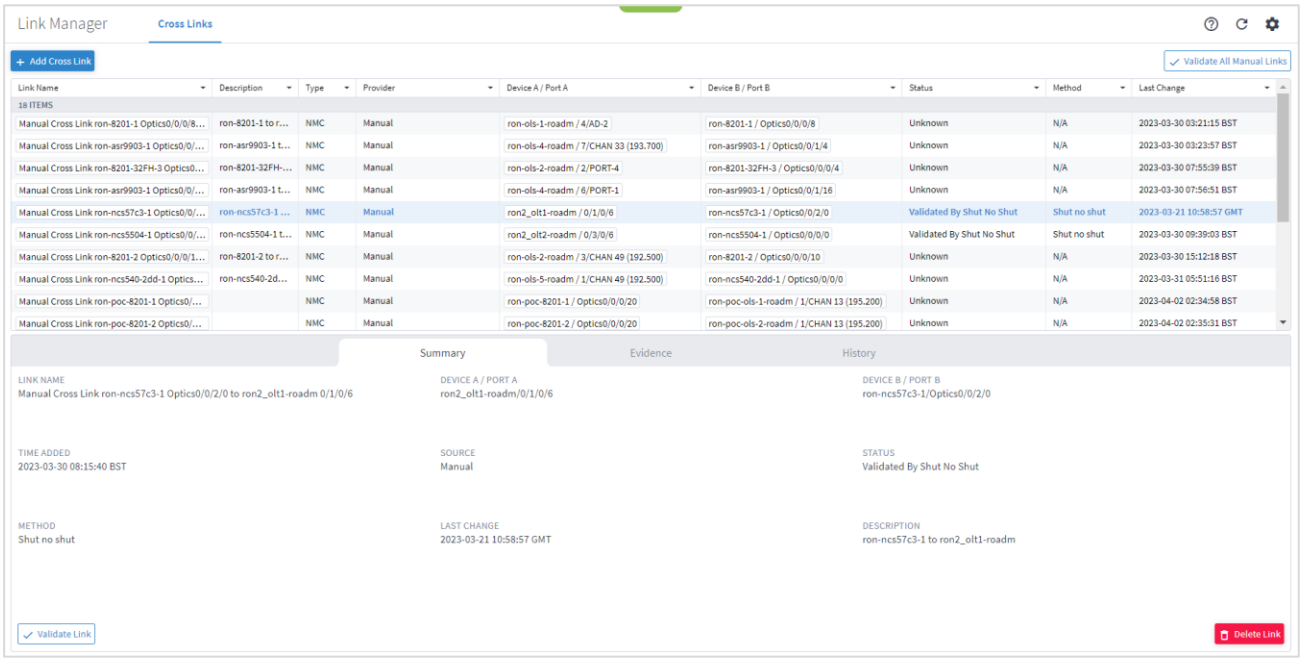
バージョン 7.0 以降、NMC リンク、つまり、トランスポンダ/マックスポンダから ROADM へのリンクを検証できます。この検証により、オプティカルコントローラの電力ステータスが切り替わり、対応するアド/ドロップポートの ONC コントローラから収集されたライブ光電力に関連付けられます。

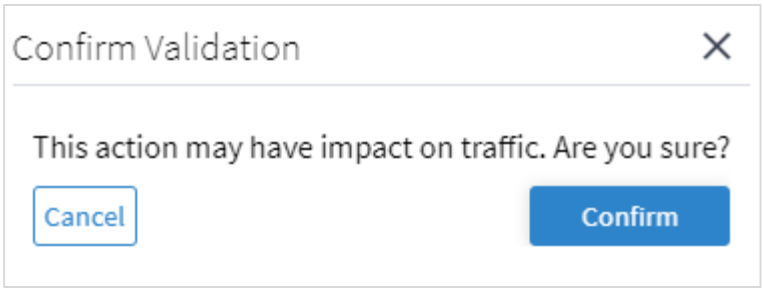
（注） この動作には数分かかる場合があり、その間はトラフィックが中断されます。

NMC リンクを検証するには、次の手順を実行します。

1. Crosswork Hierarchical Controller のアプリケーション バーで、[リンクマネージャ（Link Manager）] を選択します。
2. いずれかの NMC クロスリンクをクリックします。

3. [概要（Summary）] タブで、[リンクの検証（Validate Link）] をクリックします。この操作はトラフィックに影響を与える可能性があります。

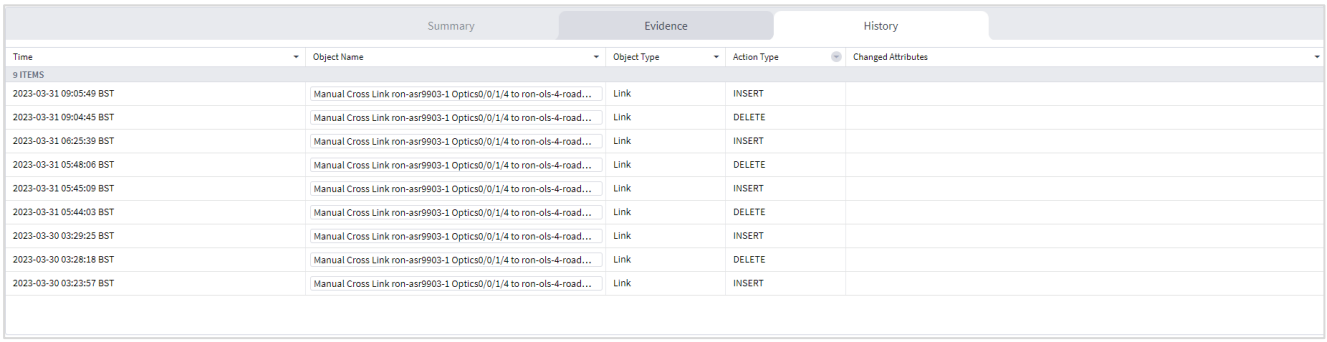




4. [確認（Confirm）] をクリックします。

5. リンクの検証結果を表示するには、[証拠（Evidence）] タブをクリックします。青い線は設定された ZR ポート値を時間の経過とともに示しており、赤い線は光ポートからの読み取り値を示しています。グラフ内の任意のポイントにカーソルを合わせると、実際の値が表示されます。-50 dBm はゼロ出力を示します。シャットダウン後、読み取りが開始されるまでの最初の待機期間があります。この期間は、検証が開始されるとフラットな線で示されます。リンクの [ステータス（Status）] が [不明（Unknown）] から [開閉により検証済み（Validated By Shut No Shut）] に変わります。

6. リンクの履歴を表示するには、[履歴（History）] タブを選択します。[アクションタイプ（Action Type）] は、リンクがいつ挿入、削除、または更新されたかを示します。

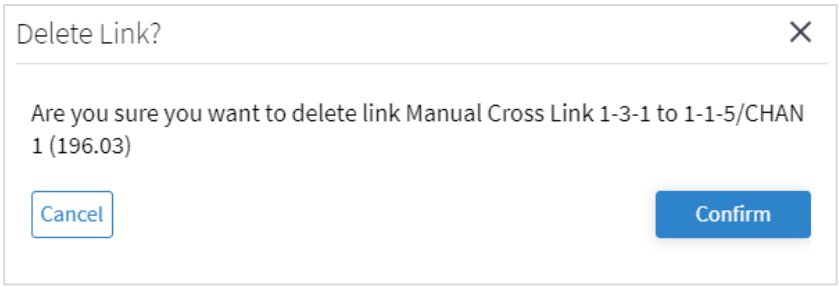


クロスリンクの削除

手動クロスリンクを削除できます。クロスリンクは削除済みとしてマークされ、次の検証の実行時に削除されます。

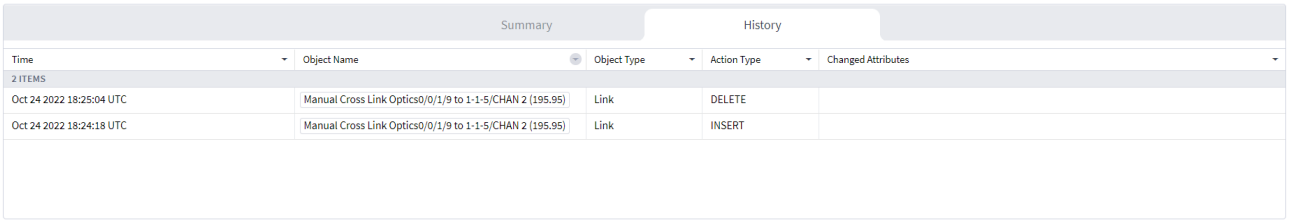
手動クロスリンクを削除するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーション バーで、[リンクマネージャ（Link Manager）] を選択します。
2. 必要な手動リンクを選択します。
3. 下部のペインで、[リンクの削除（Delete Link）] をクリックします。



4. [確認（Confirm）] をクリックします。

5. [OK] をクリックします。
6. 削除されたクロスリンクを選択し、[履歴（History）] タブをクリックして **DELETE** アクションを表示します。



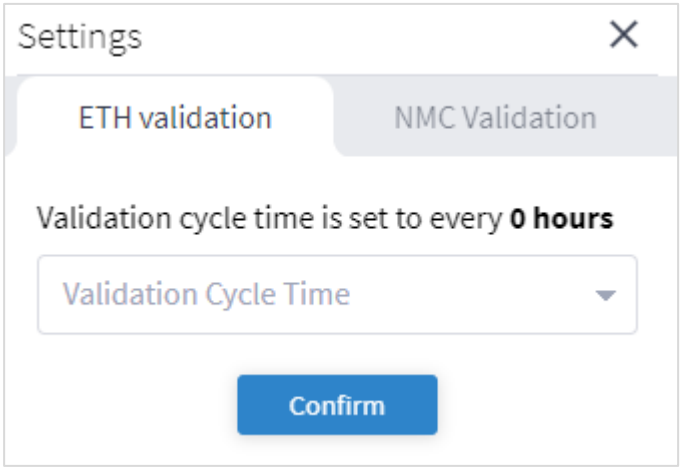
リンクは次の検証の実行時に削除されます。

ETH 検証サイクルタイムの設定

検証サイクルタイムを設定できます。

検証サイクル時間を設定するには以下を実行します。

1. Crosswork Hierarchical Controller のアプリケーション バーで、[リンクマネージャ（Link Manager）] を選択します。
2. ⚙ をクリックします。



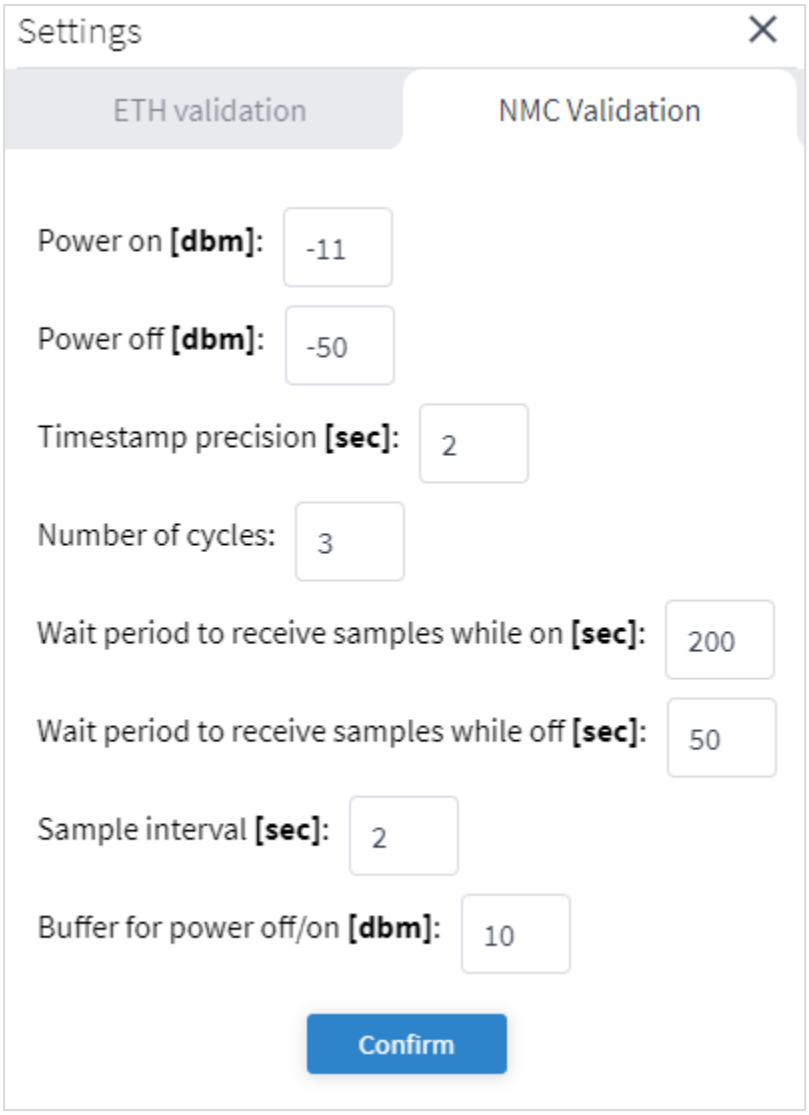
3. [ETH 検証（ETH validation）] タブで、[検証サイクルタイム（Validation Cycle Time）] を選択します。
4. [確認（Confirm）] をクリックします。

NMC 検証設定の設定

検証設定を設定できます。

検証設定を設定するには、次の手順を実行します。

1. Crosswork Hierarchical Controller のアプリケーション バーで、[リンクマネージャ（Link Manager）] を選択します。
2. ⚙ をクリックします。
3. [NMC 検証（NMC Validation）] タブを選択します。



4. 設定を指定します。
5. [確認（Confirm）] をクリックします。

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。