# デバイスのオンボーディングと管理

ここでは、次の内容について説明します。



# インベントリへのデバイスの追加

Crossworkにデバイスを追加する方法はいくつかあります。それぞれに独自の前提条件があり、デバイスの追加を成功させるために必要です。デバイスが通信用とテレメトリ用に適切に設定されていることを確認します。ガイドラインと設定例については、「新しいデバイスのテレメトリの前提条件 （2 ページ）」と「Cisco NSO デバイスの設定例 （4 ページ）」を参照してください。

ほとんどのユーザーの優先順位、メソッド、およびそれらの前提条件は次のとおりです。

1. **Crosswork API を使用したデバイスのインポート**：これはすべての方法の中で最も時間がかからず、効率的ですが、プログラミングスキルとAPIの知識が必要です。詳細については、『Inventory Management APIs On Cisco Devnet』を参照してください。
2. **デバイスの CSV ファイルからデバイスをインポートする**：この方法は時間がかかる場合があります。この方法を最大限に活かすには、まず次の手順を実行する必要があります。
    - デバイスに関連付けるプロバイダーを作成します。「プロバイダの追加について」を参照してください。

- CSV ファイルにリストされているすべてのデバイスとプロバイダに対応するクレデンシャルプロファイルを作成します。「クレデンシャルプロファイルの作成」を参照してください。
- 新しいデバイスのグループ化に使用するタグを作成します。「タグの作成」を参照してください。
- Crosswork から CSV テンプレートファイルをダウンロードし、必要なすべてのデバイスを入力します。

3. **UI を使用したデバイスの追加**：この方法は、入力時にすべてのデータが検証されるため、3 つの方法の中で最もエラーが発生しにくい方法です。また、最も時間のかかる方法であり、一度に追加するデバイスが少ない場合にのみ適しています。適用するプロバイダー、クレデンシャルプロファイル、およびタグは事前に存在している必要があります。詳細については、「UI を使用したデバイスの追加 （4 ページ）」を参照してください。
4. **Cisco SR-PCE プロバイダからの自動オンボーディング**：この方法はかなり自動化されており、比較的簡単です。これらのデバイスに適用するデバイスとプロバイダのクレデンシャルプロファイルとタグは、事前に存在している必要があります。このソースからデバイスをオンボーディングした後、各デバイスを編集して、自動的に検出されないデバイス情報を追加する必要があります。詳細については、「Cisco SR-PCE プロバイダの追加」のプロバイダプロパティを参照してください。
5. **ゼロタッチプロビジョニングを使用した自動オンボーディング**：この方法は自動化されていますが、最初にデバイスエントリを作成し、インストールの DHCP サーバーを変更する必要があります。これらのデバイスに適用するデバイスとプロバイダのクレデンシャルプロファイルとタグは、事前に存在している必要があります。この方法を使用してデバイスをプロビジョニングおよびオンボーディングした後、各デバイスを編集して、自動的に提供されない情報を追加する必要があります。詳細については、「ゼロタッチプロビジョニング」を参照してください。

（注） Cisco Crosswork は、シングルスタック展開モードのみをサポートしています。デバイスは、IPv4 アドレスまたは IPv6 アドレスのいずれか（両方ではない）でオンボーディングできます。

Cisco Crosswork にオンボーディングされているデバイスが Cisco Crosswork Data Gateway インターフェイスと同じサブネット上にある場合、それらは Cisco Crosswork Data Gateway のサウスバウンドネットワーク上にある必要があります。これは、Cisco Crosswork Data Gateway が RPF チェックを実装しており、複数の NIC（2 NIC または 3 NIC）が展開されている、デバイスの送信元アドレスが管理ネットワークまたはノースバウンドネットワーク上にないためです。

# 新しいデバイスのテレメトリの前提条件

新しいデバイスをオンボーディングする前に、Cisco Crosswork でテレメトリデータを正常に収集および送信するようにデバイスを設定する必要があります。次の項では、SNMP、NETCONF、

SSH、Telnet などのいくつかのテレメトリオプションの設定例を示します。管理する予定のデバイスを設定するためのガイドとして使用します。

（注） SNMPv2 および SNMPv3（Auth/Priv）トラップがサポートされています。

### オンボーディング前のデバイス設定

次のコマンドは、正しい SNMPv2 と NETCONF の設定、および SSH と Telnet のレート制限を設定するオンボーディング前のデバイス設定の例を提供します。NETCONF 設定は、デバイスが MDT 対応の場合にのみ必要です。

警告 サービスヘルスモニタリング中に、IOS XR バージョン 7.8.1 以降のデバイスが重複した値で応答します。これにより、データ収集プロセスが中断され、インターフェイスのヘルスステータスを取得しようとすると、「フィードを取得できません（unable to acquire feed）」というエラーメッセージが表示されます。`snmp-server packetsize 4096` を使用して SNMP サーバーのパケットサイズを定義することで、この問題を回避できます。

```
logging console debugging
logging monitor debugging
telnet vrf default ipv4 server max-servers 100
telnet vrf default ipv6 server max-servers 100
crypto key generate rsa
 exec-timeout 0 0
 width 107
 length 37
 absolute-timeout 0
!
snmp-server community public RO
snmp-server community robot-demo2 RO
snmp-server ifindex persist
snmp-server packetsize 4096
ntp
 server <NTPServerIPAddress>
!
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
!
netconf agent tty
!
netconf-yang agent
 ssh
!
```

### SNMPv3 オンボーディング前のデバイス設定

SNMPv3 データ収集を有効にする場合は、前の項の SNMPv2 設定コマンドを繰り返し、次のコマンドを追加します。

```
snmp-server group grpauthpriv v3 priv notify v1default
snmp-server user <user-ID> grpauthpriv v3 auth md5 <password> priv aes 128 <password>
```

# Cisco NSO デバイスの設定例

Cisco Network Services Orchestrator（Cisco NSO）をプロバイダとして使用して Cisco Crosswork で管理するデバイスを設定する場合は、Cisco NSO デバイスの設定が次の例のガイドラインに従っていることを確認してください。

この例では、デバイス ID としてホスト名を使用する Cisco NSO 設定を示します。CSV ファイルを使用してデバイスをインポートする場合は、**ROBOT_PROVDEVKEY_HOST_NAME** を provider_node_key フィールドの列挙値として使用します。ここで使用する例のホスト名 **RouterFremont** は、CSV ファイル内のデバイスのホスト名と一致する必要があります。

```
configure
set devices device RouterFremont address 198.18.1.11 port 22
set devices device RouterSFO address 198.18.1.12 port 830
```

次に、リモート名とパスワードが「cisco」の「cisco」という認証グループを作成する例を示します。次に、「Router」で始まる名前のすべてのデバイスを、ned-id「cisco-iosxr-nc-6.6」を使用して「netconf」のデバイスタイプに設定します。最後に、名前が「Router」で始まるすべてのデバイスを「cisco」認証グループに割り当てます。環境に合うように次の設定を編集します。

```
set devices authgroups group cisco default-map remote-name cisco remote-password cisco
set devices device Router* device-type netconf ned-id cisco-iosxr-nc-6.6
set devices device Router* authgroup cisco
```

次の CLI コマンドは、SSH キーのロックを解除してすべてのデバイスから取得します。Cisco NSO は、各デバイスの現在の設定をアップロードして現在の設定を保存することでデバイスと同期します。次のコマンドを使用してデバイス、Cisco NSO、および Cisco Crosswork アプリケーションが共通の設定から開始されていることを確認することが重要です。

```
set devices device Router* state admin-state unlocked
request devices device Router* ssh fetch-host-keys
request devices device Router* sync-from
commit
```

# UI を使用したデバイスの追加

UI を使用してデバイスを 1 つずつ追加するには、次の手順に従います。通常の状況では、いくつかのデバイスを追加する場合にのみこの方法を使用します。

**ステップ 1** メインメニューから **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

**ステップ 2** ＋をクリックします。

**ステップ 3** 次の表に示すように、新しいデバイスの値を入力します。

**ステップ 4** [保存（Save）] をクリックします。すべての必須フィールドに入力するまで、[保存（Save）] ボタンは無効になります。

**ステップ 5** （オプション）デバイスをさらに追加するには、この手順を繰り返します。

**表 *1 : [*新しいデバイスの追加（***Add New Device***）*]* ウィンドウ（** =*必須）**

| フィールド | 説明 |
|---|---|
| *** 管理状態（Administration State）** | デバイスの管理状態。オプションは、次のとおりです。<br>• [管理対象外（UNMANAGED）] : Crosswork はデバイスをモニターしていません。<br>• [ダウン（DOWN）] : デバイスは管理されており、ダウンしています。<br>• [アップ（UP）] : デバイスは管理されており、稼働しています。 |
| *** 到達可能性チェック（Reachability Check）** | Crosswork がデバイスの到達可能性チェックを実行するかどうかを決定します。オプションは、次のとおりです。<br>• [有効（ENABLE）]（CSV では **`REACH_CHECK_ENABLE`**）：到達可能性を確認して UI の到達可能性状態を自動的に更新します。<br>• [無効（DISABLE）]（CSV では **`REACH_CHECK_DISABLE`**）：デバイスの到達可能性チェックは無効です。<br>常に [有効（ENABLE）] に設定することをお勧めします。[設定済みの状態（Configured State）] が [管理対象外（UNMANAGED）] とマークされている場合、このフィールドはオプションです。 |
| *** クレデンシャルプロファイル（Credential Profile）** | データ収集や設定変更のためにデバイスへのアクセスに使用するクレデンシャルプロファイルの名前。例：**`nso23`** または **`srpce123`**。<br>[設定済みの状態（Configured State）] が [管理対象外（UNMANAGED）] とマークされている場合、このフィールドはオプションです。 |
| **ホスト名（Host Name）** | デバイスのホスト名。 |
| **インベントリ ID（Inventory ID）** | デバイスのインベントリ ID 値。値には最大 128 文字の英数字を使用でき、ドット（.）、アンダースコア（「_」）、コロン（「:」）、またはハイフン（「-」）を含めることができます。その他の特殊文字は使用できません。<br>デバイスのホスト名か、またはインベントリ ID の簡単に識別できる名前を選択します。これは、デバイス名として使用されるインベントリ ID とデバイスを Crosswork に同期するために使用されます。 |
| **[ソフトウェア タイプ（Software Type）]** | デバイスのソフトウェアタイプ。 |

| フィールド | 説明 |
|---|---|
| **ソフトウェアバージョン（Software Version）** | デバイスのソフトウェア バージョン。 |
| **UUID** | デバイスの汎用一意識別子（UUID）。 |
| **シリアル番号（Serial Number）** | デバイスのシリアル番号。 |
| **MAC アドレス（MAC Address）** | デバイスの MAC アドレス。 |
| *** 機能（Capability）** | デバイスデータの収集を可能にし、デバイスに設定される機能。これは必須の機能であるため、少なくとも **SNMP** を選択する必要があります。**SNMP** が設定されていない場合、デバイスはオンボーディングされません。その他のオプションは、**YANG_MDT**、**YANG_CLI**、**TL1**、および**GNMI** です。選択する機能は、デバイスのソフトウェアタイプとバージョンによって異なります。<br>（注） MDT 機能を備えたデバイスの場合、この段階では YANG_MDT を選択しないでください。 |
| **タグ（Tag）** | 識別およびグループ化のためにデバイスに割り当てるために使用できるタグ。<br>デバイスタグを使用して、モニタリングのためにデバイスをグループ化し、デバイスの物理的な場所や管理者の電子メール ID など、他のユーザーにとって重要な可能性がある追加情報を提供します。 |
| **製品のタイプ（Product Type）** | デバイスの製品タイプ。 |
| **Syslog 形式（Syslog Format）** | デバイスから受信した syslog イベントの形式は、Syslog コレクタで解析する必要があります。次のオプションがあります。<br>• [不明（UNKNOWN）]：Syslog コレクタによる解析を行わない場合は、このオプションを選択します。Syslog 収集ジョブの出力には、デバイスから受信した syslog イベントが含まれます。<br>• [RFC5424]：デバイスから受信した syslog イベントを RFC5424 形式で解析するには、このオプションを選択します。<br>• [RFC3164]：デバイスから受信した syslog イベントを RFC3164 形式で解析するには、このオプションを選択します。<br>詳細については、「Syslog 収集ジョブの出力」の項を参照してください。 |
| **接続の詳細（Connectivity Details）** | |

| フィールド | 説明 |
|---|---|
| プロトコル（**Protocol**） | デバイスで使用する接続プロトコル。選択肢は、**SNMP**、**NETCONF**、**TELNET**、**HTTP**、**HTTPS**、**GNMI**、**TL1**、および **GRPC** です。<br>（注） [セキュア接続（Secure Connection）] スライダを切り替えて、選択した GNMI プロトコルを保護します。<br>このデバイスの接続プロトコルをさらに追加するには、[接続の詳細（Connectivity Details）] パネルの最初の行の末尾にある ＋ をクリックします。入力したプロトコルを削除するには、パネル内の該当する行の横にある × をクリックします。<br>同じプロトコルを複数セットなど、必要な数の接続の詳細のセットを入力できます。少なくとも **SSH** と **SNMP** の詳細は入力する必要があります。**SNMP** を設定しない場合、デバイスは追加されません。デバイスを管理する場合（または XR デバイスを管理している場合）、**NETCONF** の詳細を入力する必要があります。**TELNET** 接続はオプションです。 |
| ***IP アドレス/サブネットマスク（IP Address/Subnet Mask**） | デバイスの IP アドレス（IPv4 または IPv6）とサブネットマスクを入力します。<br>（注） 予期しない接続の問題が発生する可能性があるため、IP ネットワークに選択したサブネット（デバイスと接続先を含む）に重複するアドレス空間（サブネット/スーパーネット）がないことを確認してください。<br>（注） 同じ IP アドレスとサブネットマスクを持つ複数のプロトコルがある場合は、他のフィールドに詳細を自動入力するよう Crosswork に指示できます。 |
| ***ポート（Port**） | この接続プロトコルに使用するポート。各プロトコルはポートにマッピングされるため、選択したプロトコルに対応するポート番号を入力してください。各プロトコルの標準的なポート割り当ては次のとおりです。<br>• SSH：22<br>• SNMP：161<br>• NETCONF：830<br>• TELNET：23<br>• HTTP：80<br>• HTTPS：443<br>GNMI と GNMI_SECURE：ポート値は 57344 ー 57999 です。ここで入力するポート番号が、デバイスで設定されているポート番号と一致していることを確認します。 |
| タイムアウト（**Timeout**） | このプロトコルを使用した通信試行がタイムアウトするまでの経過時間（秒単位）。デフォルト値は 30 秒です。<br>NETCONF を使用する XE デバイスの場合、推奨される最小タイムアウト値は 90 秒です。その他のすべてのデバイスとプロトコルの場合、推奨される最小タイムアウト値は 60 秒です。 |

| フィールド | 説明 |
|---|---|
| **エンコード タイプ（Encoding Type）** | このフィールドは、**GNMI** プロトコルと **GNMI_SECURE** プロトコルにのみ適用されます。オプションは、**`PROTO`** と **`JSON IETF`** です。<br>デバイスの機能に基づいて、デバイスで一度にサポートされるエンコーディング形式は1つだけです。 |
| **暗号化** | このフィールドは、**SNMP** プロトコルにのみ適用されます。<br>ドロップダウンメニューから、デバイスでサポートされている関連する SNPMv3 プロトコルを選択します。デフォルト値は [なし（NONE）] です。<br>ドロップダウンメニューには、さまざまなキー長（128 ビット、192 ビット、256 ビット）に対する、カウンタモード（CTR）、Galois/カウンタモード（GCM）、および暗号ブロック連鎖モード（CBC）の Advanced Encryption Standard（AES）仕様がリストされます。 |
| SNMPトラップ無効化チェック（SNMP Disable Trap Check） | このチェックボックスは、プロトコルフィールドが **`SNMP`** に設定されている場合に表示されます。このチェックボックスを選択すると、ネットワークデバイスと Crosswork Data Gateway 間の SNMPv2 コミュニティストリング検証が無効になります。 |
| **ルーティング情報（Routing Info）** | |
| **ISIS システム ID（ISIS System ID）** | デバイスの IS-IS システムの ID。これは、IS-ISトポロジ内のルータを識別する ID で、SR-PCE 統合に必要です。 |
| **OSPF ルータ ID（OSPF Router ID）** | デバイスの OSPF ルータ の ID。これは、OSPFトポロジ内のルータを識別する ID で、SR-PCE 統合に必要です。 |
| *** TE ルータ ID（TE Router ID）** | 各 IGP のトラフィック エンジニアリング ルータ の ID。<br>（注） トポロジ内の L3 リンクを可視化するには、[TE ルータ ID（TE Router ID）] フィールドを入力して、デバイスを Cisco Crosswork にオンボーディングする必要があります。 |
| **IPv6 ルータ ID** | デバイスの IPv6 ルータ ID。このフィールドは構成可能なパラメータであり、Crosswork によって自動検出されることはありません。 |
| **ストリーミングテレメトリの設定（Streaming Telemetry Config）** | |
| **Vrf** | モデル駆動形テレメトリ（MDT）トラフィックがルーティングされる VRF の名前。 |
| **送信元インターフェイス（Source Interface）** | デバイスタイプのループバックの範囲。このフィールドは任意です。<br>（注） このフィールドは、デバイスが [ダウン（DOWN）] または [管理対象外（UNMANAGED）] の状態の場合にのみ編集できます。 |

| フィールド | 説明 |
|---|---|
| **MDT 設定の解除** | このチェックボックスを有効にすると、Crosswork が NSO 経由でテレメトリ構成をデバイスにプッシュするのをスキップします。この設定はデフォルトでは無効な状態になっています（Crosswork からデバイスに NSO を介してテレメトリ設定がプッシュされます）。<br>この設定を切り替えるには、デバイスが ADMIN DOWN 状態でなければなりません。設定を有効から無効に切り替える前に、アウトオブバンドの設定のセットアップをクリアする必要があります。 |
| **所在地（Location）**<br>ネットワークトポロジの地理的ビューに必要な [経度（Longitude）] と [緯度（Latitude）] を除き、ロケーションのすべてのフィールドはオプションです。 | |
| **経度（Longitude）、緯度（Latitude）** | 経度と緯度の値は、地理的マップがデバイスの正しい地理的位置と他のデバイスへのリンクを表示できるようにするために必要です。経度と緯度を 10 進数（DD）形式で入力します。 |
| **高度（Altitude）** | デバイスが設置されている高度（フィートまたはメートル）。たとえば、**123** です。 |
| **プロバイダとアクセス（Providers and Access）**<br>このデバイスにプロバイダを追加するには、[プロバイダとアクセス（Providers and Access）] パネルの最初の行の末尾にある ＋ をクリックします。入力したプロバイダを削除するには、パネル内のその行の横にある × をクリックします。 | |
| **プロバイダファミリ（Provider Family）** | トポロジの計算に使用するプロバイダタイプ。リストからプロバイダを選択します。 |
| **プロバイダー名（Provider Name）** | トポロジ計算に使用されるプロバイダタイプ。リストからプロバイダを選択します。<br>（注） Cisco NSO LSA 展開の場合、ユーザーは、デバイスを割り当てるリソースに面するサービス（RFS）ノードを選択できます。 |
| **クレデンシャル（Credential）** | プロバイダに使用するクレデンシャルプロファイル。このフィールドは読み取り専用で、選択したプロバイダーに基づいて自動的に入力されます。 |

# CSV ファイルからのインポートによるデバイスの追加

複数のデバイスを指定する CSV ファイルを作成し、Crosswork にインポートするには、次の手順を実行します。

CSV ファイルからデバイスをインポートすると、まだデータベースにないデバイスが追加され、デバイスレコード内のデータが、インポートされたデバイスのものと一致する [インベントリキータイプ（Inventory Key Type）] フィールド値で上書きされます（これは、システムによって設定され、インポートの影響を受けないUUID を除外します）。このため、インポート

する前に、すべての現在のデバイスのバックアップコピーをエクスポートすることをお勧めします。

**注目**

- CSV ファイルを使用して多数のデバイスをインポートしている間に、[TE ルータ ID（TE Router ID）] フィールドの値を入力する必要があります。
- Firefox ブラウザを使用して誤った CSV 値を持つ多数のデバイスをインポートすると、ウィンドウが使用できなくなることがあります。この場合は、新しいタブまたはウィンドウで Cisco Crosswork にログインし、正しい CSV 値でデバイスをオンボーディングします。
- Windows マシンで作成された CSV ファイルには、ファイルが期待どおりに処理されるように改行（「改行」文字でマーク）が含まれている必要があります。「復帰」オプションを使用して作成された改行は機能しません。

**ステップ 1** メインメニューから **[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択します。デフォルトでは、[ネットワークデバイス（Network Devices）] タブが表示されます。

**ステップ 2** をクリックして、[CSV ファイルのインポート（Import CSV File）] ダイアログボックスを開きます。

**ステップ 3** インポートするデバイス CSV ファイルをまだ作成していない場合：

a) [「Device Management template（*.csv）」サンプルファイルのダウンロード（Download sample 'Device Management template (* .csv)' file）] リンクをクリックし、CSV ファイルテンプレートをローカルストレージリソースに保存します。

b) 任意のツールを使用してテンプレートを開きます。ファイルに行を追加します（デバイスごとに 1 行）。

（注）
- 各デバイスの TE ルータ ID 値が入力されていることを確認します。この値は、SR-PCE から学習したトポロジ内のデバイスを一意に識別するために使用されます。各デバイスの有効な TE ルータ ID がない場合、トポロジは表示されません。
- デバイスのインポート後またはデバイスのオンボーディング後は、TE ルータ ID を変更しないでください。インポート後にデバイスの TE ルータ ID を変更する必要がある場合は、次の手順を実行します。
  1. デバイスを Crosswork から削除する必要があります。
  2. すべての SR-PCE プロバイダを削除する必要があります。
  3. 新しい TE ルータ ID を使用してデバイスを再度オンボーディングします。
  4. SR-PCE プロバイダを再度追加します。

同じフィールド内で複数のエントリを区切るには、セミコロンを使用します。それらのエントリ間に 2 つのセミコロンをスペースなしで使用することで、フィールドを空白のままにすることを示します。複数のエントリをセミコロンで区切る場合は、各フィールドに値を入力する順序が重要であることに注意してください。たとえば、[接続タイプ（Connectivity Type）] フィールドに **SSH;SNMP;NETCONF**

と入力し、[接続ポート（Connectivity Port）] フィールドに **22;161;830** と入力した場合、エントリの順序によって 2 つのフィールド間のマッピングが決定されます。

- SSH：ポート 22
- SNMP：ポート 161
- NETCONF：ポート 830

入力する必要があるフィールドと必須値のリストについては、UI を使用したデバイスの追加 （4 ページ）の [新しいデバイスの追加（Add New Device）] フィールドのテーブルを参照してください。

ファイルを保存する前にサンプルデータ行を必ず削除してください。削除しないと、必要なデータとともにインポートされます。インポート中は無視されるため、列ヘッダー行はそのままでかまいません。

c) 完了したら、新しい CSV ファイルを保存します。

**ステップ 4** [参照（Browse）] をクリックし、作成した CSV ファイルに移動した後、[開く（Open）] をクリックして選択します。

**ステップ 5** CSV ファイルを選択した状態で、[インポート（Import）] をクリックします。

（注） CSV ファイルを使用して UI 経由でデバイスまたはプロバイダをインポートする場合、ユーザーは操作が完了するまで待機する必要があります。操作の進行中に [インポート（Import）] ボタンをクリックすると、各デバイスまたはプロバイダのエントリの重複が発生します。

**ステップ 6** エラーを解決し、デバイスの到達可能性を確認します。

デバイスが最初にインポートされたときに、そのデバイスが到達不能または動作不能として表示されるのは正常です。ただし、30 分後に到達不能または動作不能と表示される場合は、調査が必要な問題がある可能性があります。調査するには、**[デバイス管理（Device Management）] > [ジョブ履歴（Job History）]** を選択し、[ステータス（Status）] 列に表示されるエラーアイコンをクリックします。一般的な問題として、関連付けられたクレデンシャルプロファイルに正しいクレデンシャルが含まれていないことが挙げられます。これをテストするには、サーバーで端末ウィンドウを開き、関連付けられているクレデンシャルプロファイルで指定されたプロトコルとクレデンシャルを使用してデバイスにアクセスします。

**ステップ 7** デバイスを正常にオンボーディングしたら、Cisco Crosswork Data Gateway インスタンスにそれらをマッピングする必要があります。

# CSV ファイルへのデバイス情報のエクスポート

デバイスリストをエクスポートすると、すべてのデバイス情報が CSV ファイルにエクスポートされます。デバイスリストのエクスポートは、システム内のすべてのデバイスのレコードを一度に保持するのに便利です。必要に応じて CSV ファイルを編集して再インポートし、既存のデバイスデータを上書きすることもできます。

エクスポートしたデバイス CSV ファイルには、各デバイスのクレデンシャルプロファイルの名前のみが含まれ、クレデンシャル自体は含まれません。

**ステップ 1** メインメニューから **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択します。デフォルトでは、[ネットワークデバイス（Network Devices）] タブが表示されます。

**ステップ 2** （オプション）必要に応じてデバイスリストをフィルタ処理します。

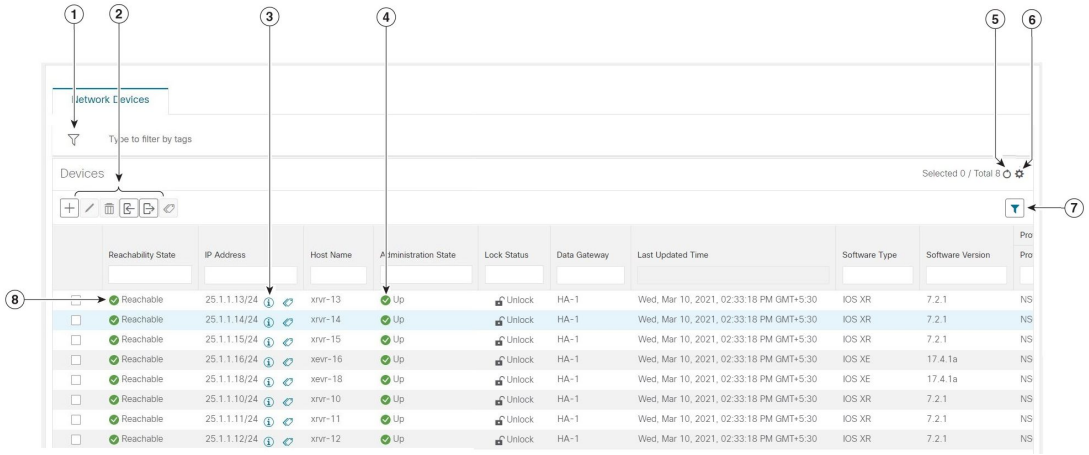
**ステップ 3** エクスポートするデバイスのチェックボックスをオンにします。すべてのデバイスをエクスポートするように選択するには、列の上部にあるチェックボックスをオンにします。

**ステップ 4** をクリックします。CSV ファイルを保存する際に使用するパスとファイル名を選択するか、またはすぐに開くかを確認するプロンプトがブラウザに表示されます。

# ネットワーク デバイスの管理

Cisco Crosswork の [ネットワークデバイス（Network Devices）] ウィンドウには、すべてのデバイスとそのステータスが統合されたリストが表示されます。[ネットワークデバイス（Network Devices）] ウィンドウを表示するには、**[デバイス管理（Device Management]** > **[ネットワークデバイス（Network Devices）]** を選択します。デフォルトでは、[ネットワークデバイス（Network Devices）] タブが表示されます。

**図 *1 : [ネットワークデバイス（Network Devices）] ウィンドウ***




| 項目 | 説明 |
|---|---|
| 1 | [タグによるフィルタ処理（Filter by tags）] フィールドでは、デバイスに適用されているタグでそれらのデバイスをフィルタ処理できます。検索しようとしているデバイスに適用されているタグの名前を入力します。 |

| 項目 | 説明 |
|---|---|
| 2 | 新しいデバイスをデバイスインベントリに追加するには、＋をクリックします。 |
| | 現在選択されているデバイスの情報を編集するには、✎をクリックします。。 |
| | 現在選択されているデバイスを削除するには、🗑をクリックします。 |
| | CSV ファイルを使用して、新しいデバイスをインポートし、既存のデバイスを更新するには、をクリックします。このアイコンをクリックして、CSV ファイルテンプレートをダウンロードすることもできます。テンプレートには、独自の CSV ファイルを作成するためのガイドとして使用できるサンプルデータが含まれています。 |
| | 選択したデバイスの情報を CSV ファイルにエクスポートするには、をクリックします。 |
| | 選択したデバイスに適用されているタグを変更するには、をクリックします。を参照してください。 |
| 3 | をクリックすると、[デバイスの詳細（Device Details）] ポップアップウィンドウが開き、選択したデバイスの重要な情報を表示できます。 |
| 4 | [管理状態（Administration State）] 列のアイコンは、デバイスが動作しているかどうかを示します。 |
| 5 | デバイスリストを更新するには、 をクリックします。 |
| 6 | デバイスリストに表示する列を選択するには、⚙をクリックします。 |
| 7 | デバイスリストの 1 つ以上の列にフィルタ条件を設定するには、をクリックします。 |
| | 設定したフィルタ条件をクリアするには、[フィルタのクリア（Clear Filter）] リンクをクリックします。 |
| 8 | [到達可能性状態（Reachability State）] 列のアイコンは、デバイスが到達可能かどうかを示します。 |

# デバイスの状態（Device State）

Cisco Crossworkは、使用するプロバイダーと管理対象デバイスの到達可能性状態、および到達可能な管理対象デバイスの動作状態およびNSO状態を計算します。次の表のアイコンを使用してこれらの状態を示します。

表 *2:* デバイス状態アイコン

| アイコン | 意味 |
|---|---|
| [到達可能性状態（Reachability State）] アイコンは、デバイスまたはプロバイダが到達可能かどうかを示 | |
|  | [到達可能（Reachable）]：設定されているすべてのプロトコルによってデバイスま |
|  | [到達可能性低下（Reachability Degraded）]：少なくとも 1 つのプロトコルでデバイスまたはプロバイダに設定されている他の 1 つ以上のプロトコルでは到達できませ |
|  | [到達不能（Unreachable）]：デバイスまたはプロバイダは、そのプロトコルに設定 |
|  | [到達可能性不明（Reachability Unknown）]：Cisco Crosswork は、デバイスが到達可断できません。デバイスが Cisco Crosswork データゲートウェイ（Cisco Crosswork 態になる可能性があります。 |
| [動作状態（Operational State）] アイコンは、デバイスが動作しているかどうかを示します。 | |
|  | デバイスは動作中であり、管理下にあります。すべての個別のプロトコルは「OK |
|  | デバイスが動作していません（「ダウン」）。デバイスがオペレータによって「管ンが使用されます。 |
|  | デバイスの動作状態または設定状態が不明です。 |
|  | デバイスの動作状態または設定状態が低下しています。 |
|  | デバイスの動作状態または設定状態がエラー状態です。到達して動作状態を計算しプしていないか、または到達不能です。アイコンの横に表示される円内の数字は、リストを表示するには、その数字をクリックします（エラーのアイコンバッジは、できません）。 |
|  | デバイスの動作状態は現在確認中です。 |
|  | デバイスは削除中です。 |
|  | デバイスは管理対象外です。 |
| [NSO状態（NSO State）] アイコンは、デバイスが Cisco NSO と同期されているかどうかを示します。<br>（注） デバイスのオンボーディング後の Cisco Crosswork と NSO 間の最初の同期では、デバイスの NSO がポリシーに基づいてデバイスを NSO と同期する必要があるかどうかを判断しておらず、初期生します。 | |
|  | デバイスは Cisco NSO と同期しています。 |
|  | デバイスが Cisco NSO と同期していません。 |

デバイスの到達可能性状態は次のように計算されます。

1. デバイスの設定状態（ユーザーによる設定）が[アップ（UP）]である限り、到達可能性は常にデバイスごとに計算されます。デバイスが管理上 [ダウン（DOWN）] または [管理対象外（UNMANAGED）] の場合は計算されません。
2. 到達可能性の状態は常に [到達可能（REACHABLE）]、[到達不能（UNREACHABLE）]、または [不明（UNKNOWN）] のいずれかです。
   - 少なくとも 1 つのプロトコルを介してデバイスへのルートが 1 つ以上あり、かつ、デバイスが検出可能な場合、到達可能性状態は [到達可能（REACHABLE）] です。
   - 1 つのプロトコルを介したデバイスへのルートがない場合、またはデバイスが応答しない場合、到達可能性状態は [到達不能（UNREACHABLE）] です。
   - デバイスが [管理対象外（UNMANAGED）] の場合、到達可能性状態は [不明（UNKNOWN）] です。

デバイスの動作状態は次のように計算されます。

1. （ユーザーが設定した）デバイスの動作状態が[アップ（UP）]である限り、動作状態は常に各デバイスに対して計算されます。デバイスが管理上 [ダウン（DOWN）] または [管理対象外（UNMANAGED）] の場合は計算されません。
2. 動作状態は常に [OK] または [エラー（ERROR）] です。
3. デバイスを管理上 OK の状態にするには、デバイスが到達可能で検出可能である必要があります。その他の到達可能性状態は [エラー（ERROR）] です。
4. XR デバイスまたは XE デバイスの場合のみ、管理上 OK の状態では、Crosswork ホストとデバイスクロック間のクロックドリフトの差がデフォルトの値（現在は 2 分）よりも小さいことも必要です。

（注） 一部のタイムゾーン設定では、実際にクロックドリフトが存在しない場合にクロックドリフトエラーが発生することがわかっています。この問題を回避するには、UTC 時間を使用するようにデバイスを設定します。

# タグによるネットワークデバイスのフィルタ処理

タグを作成して特定のデバイスに割り当てることで、デバイスの物理的な位置やその管理者の電子メール ID など、他のユーザーにとって重要な可能性のある追加情報を簡単に提供できます。また、タグを使用して、デバイスを一覧表示する任意のウィンドウで同じか、または類似するタグを持つデバイスを検索してグループ化することもできます。

タグでデバイスをフィルタ処理するには、次の手順を実行します。

**ステップ 1** メインメニューから **[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択します。

**ステップ 2** ユーザーインターフェイスの上部にある [入力してタグでフィルタ処理（Type to filter by tag）] バーに、タグ名のすべてまたは一部を入力します。

[入力してタグでフィルタ処理（Type to filter by Tags）] バーには、先行入力機能があります。入力を開始すると、これまでに入力したすべての文字に一致するタグのドロップダウンリストが表示されます。使用可能なすべてのタグをドロップダウンリストに表示するには、***** を入力します。

**ステップ 3** フィルタに追加するタグの名前を選択します。[入力してタグでフィルタ処理（Type to filter by tags）] フィルタバーにフィルタが表示されます。テーブルまたはマップには、そのタグを持つデバイスのみが表示されます。

**ステップ 4** 複数のタグでフィルタリングする場合は次の手順を実行します。

a) フィルタの一部として設定する追加タグごとに、手順 2 と 3 を繰り返します。

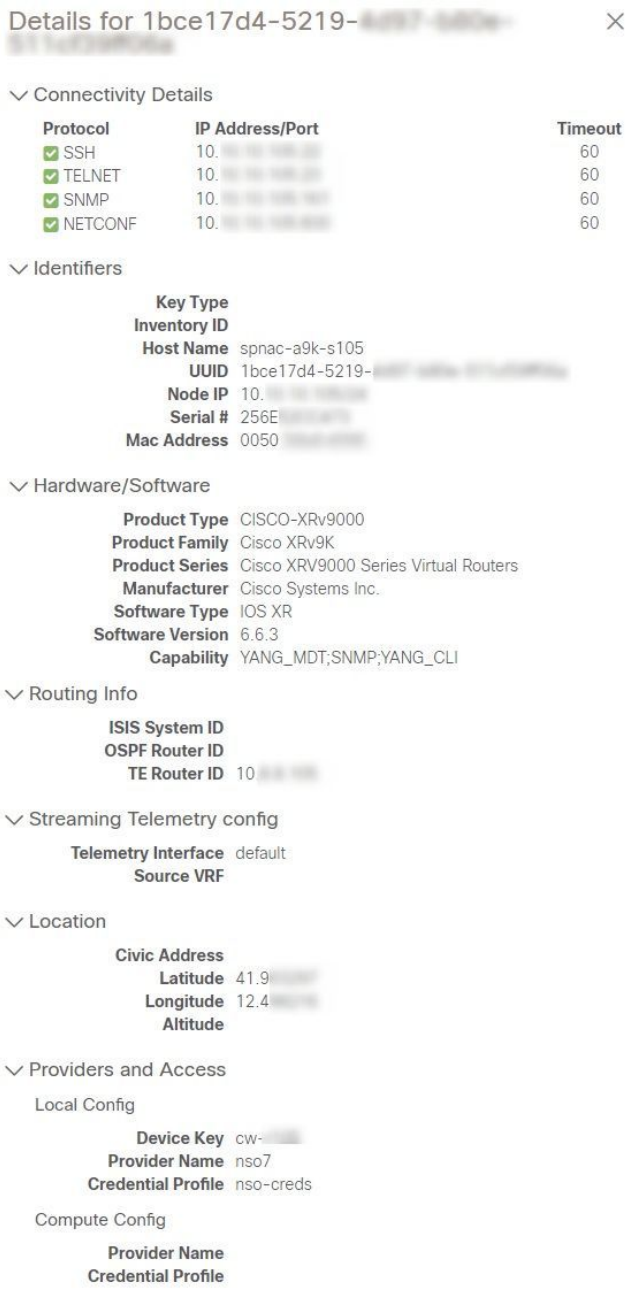
b) 必要なすべてのタグを選択したら、[フィルタの適用（Apply Filters）] をクリックします。テーブルまたはマップには、フィルタ内の**すべて**のタグに一致するタグを持つデバイスのみが表示されます。

**ステップ 5** すべてのタグフィルタをクリアするには、[フィルタのクリア（Clear Filters）] リンクをクリックします。複数のタグを含むフィルタからタグを削除するには、フィルタ内のそのタグの名前の横にある [X] アイコンをクリックします。

# デバイスの詳細情報の取得

**[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択し、[ネットワークデバイス（Network Devices）] タブにデバイスのリストを表示するたびに、リストされているデバイスの横にある をクリックすると、そのデバイスに関する詳細情報を取得できます。このアイコンをクリックすると、[デバイス名の詳細（Details for DeviceName）] ポップアップウィンドウが開きます。次に例を示します。

図 *2 : [*デバイス名の詳細（***Details for DeviceName***）*]* ウィンドウ




ポップアップウィンドウの上部にある [接続の詳細（Connectivity Details）] 領域を展開します（まだ展開していない場合）。この領域には、すべてのトランスポートタイプの到達可能性ステータスが表示されます。

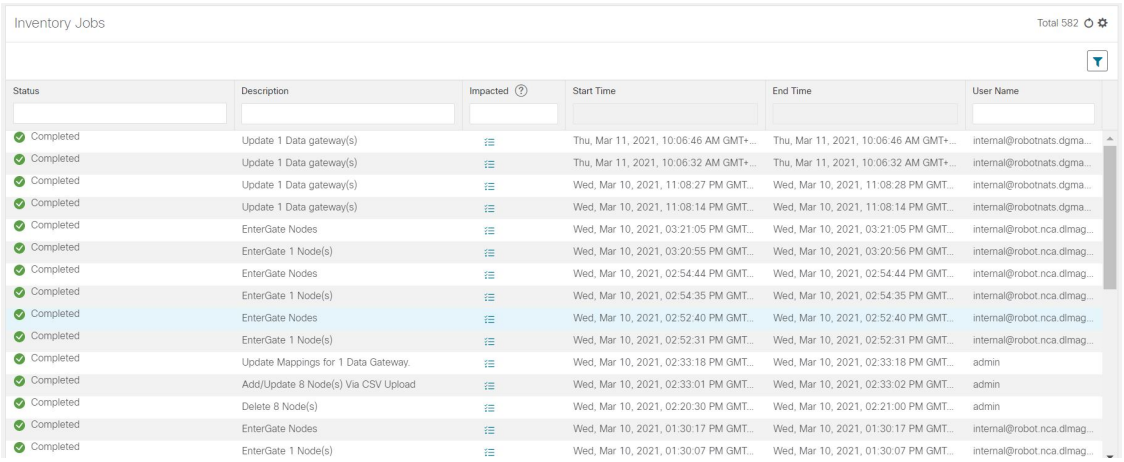
必要に応じて、ポップアップウィンドウの他の領域を展開したり、折りたたんだりします。× をクリックしてウィンドウを閉じます。

# デバイスのジョブ履歴の表示

Cisco Crossworkは、デバイス関連のジョブに関する情報を収集して保存します。作成、更新、および削除のすべてのアクティビティを追跡するには、次の手順を実行します。

**ステップ1** メインメニューから **[デバイス管理（Device Management）] > [インベントリジョブ（Inventory Jobs）]** を選択します。[インベントリジョブ（Inventory Jobs）] ウィンドウが開き、次のようなデバイス関連のすべてのジョブのログが表示されます。

**図 *3 : [インベントリジョブ（Inventory Jobs）] ウィンドウ***




ジョブは作成時刻の降順に表示されます。最新のジョブが最初に表示されます。テーブル内のデータをソートするには、列の見出しをクリックします。もう一度列の見出しをクリックすると、ソートの昇順と降順が切り替わります。

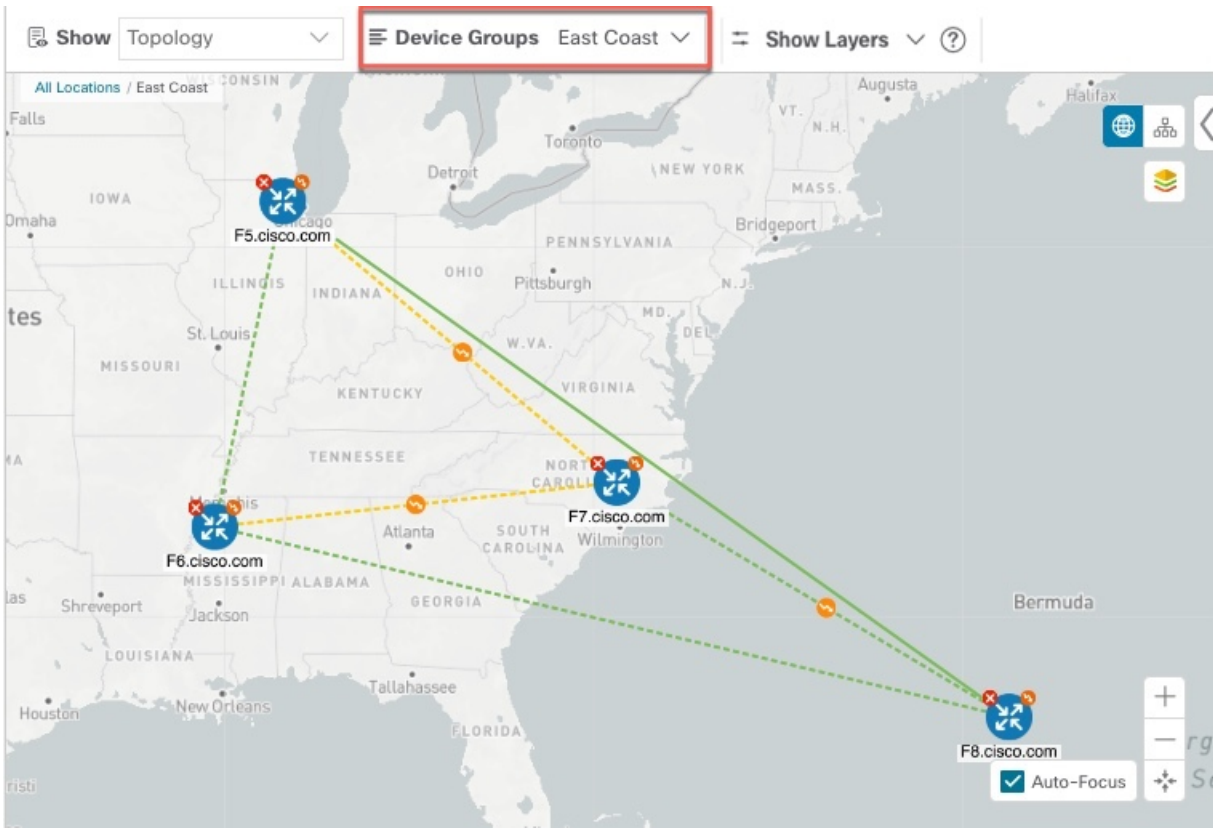
**ステップ2** [ステータス（Status）] 列には、完了、失敗、実行中、部分的、および警告の状態タイプが表示されます。失敗したジョブまたは部分的なジョブの場合に詳細を確認するには、エラーの横にある をクリックします。

（注） デバイスに到達できない場合でも、ステータスが [成功（Successful）] と表示される場合があります。表示されているジョブのステータスが正しいことを確認するには、デバイスのステータスも調べます（[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]）。

# デバイスグループを使用したトポロジビューのフィルタ処理

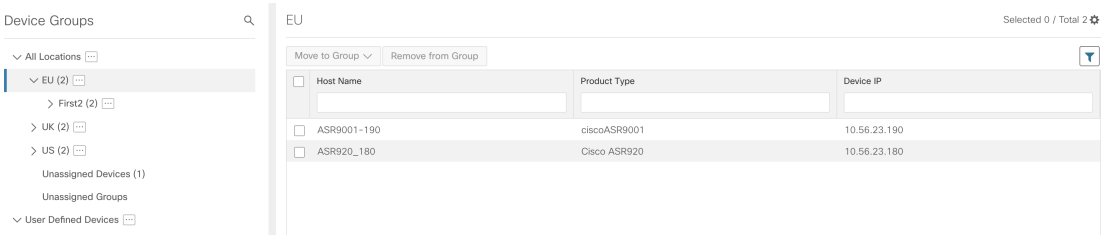
さまざまな目的でデバイスを識別、検索、およびグループ化するためにデバイスグループを作成できます。デバイスグループでは、そのデバイスグループに固有のデータを可視化して拡大できます。これにより、画面上の乱雑さが軽減され、最も重要なデータに集中できます。たとえば、次の図では、東海岸のデバイスグループが選択されており、トポロジマップに拡大表示されています。また、[デバイス（Devices）]テーブルには、東海岸のデバイスグループに属するデバイスのみが表示されていることに注意してください。

**図 *4:* トポロジマップでのデバイスグループの選択**




[デバイスグループ（Device Groups）] ウィンドウ（**[デバイス管理（Device Management）]** > **[グループ（Groups）]**）では、デバイスグループを作成および管理できます。デフォルトでは、すべてのデバイスが最初は [未割り当てデバイス（Unassigned Devices）] グループに表示されます。

図 *5:* デバイスグループセレクタ




# デバイスグループの作成と変更

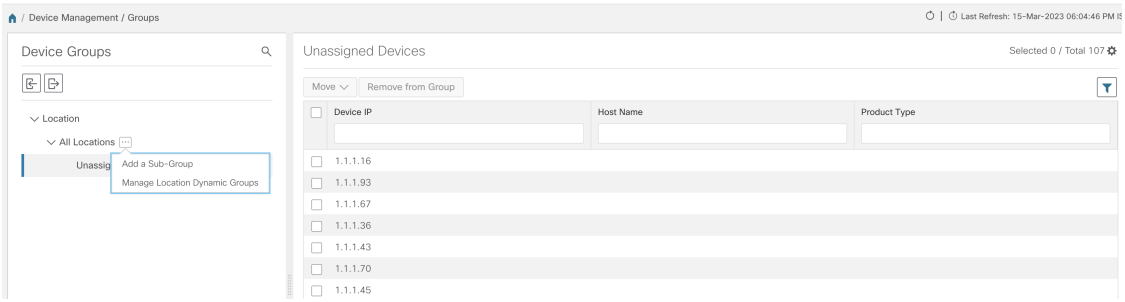
デバイスグループを作成し、そのグループにデバイスを割り当てることができます。ここで説明するように手動で行うことも、ダイナミック デバイス グループの有効化 （21 ページ）で説明するように自動で行うこともできます。デバイスは、1 つのデバイスグループにのみ属することができます。

**ステップ 1** メインメニューから **[デバイス管理（Device Management）]** > **[グループ（Groups）]** を選択します。

**ステップ 2** 新しいサブグループを追加するには、[すべての場所（All Locations）]の横にある をクリックします。[すべての場所（All Locations）] の下に新しいサブグループが追加されます。

**ステップ 3** グループにデバイスを追加するには、右側のペインの [未割り当てのデバイス（Unassigned Devices）] でデバイスを選択します。

**ステップ 4** [グループに移動（Move to Group）] ドロップダウンから、目的のグループを選択し、[移動（Move）] をクリックします。




**ステップ 5** グループから削除するには、[グループから削除（Remove from Group）] をクリックします。グループを削除すると、そのグループに属しているすべてのデバイスが [未割り当てデバイス（Unassigned Devices）] グループに移動します。また、グループを削除すると、そのグループのサブグループがすべて削除されます。

**ステップ 6** [保存（Save）] をクリックします。

# ダイナミック デバイス グループの有効化

デバイスホスト名で正規表現（regex）を使用して、デバイスグループを動的に作成し、未割り当てのデバイスをこれらのグループに自動的に追加するルールを作成できます。ルールに一致する新たに追加または検出されたデバイスは、適切なグループに配置されます。

ダイナミックルールは、すでにグループに属しているデバイスには適用されません。ルールで考慮されるようにするデバイスは、[未割り当てデバイス（Unassigned Devices）] に移動する必要があります。

### 始める前に

[ダイナミックグループ（Dynamic Groups）] ダイアログに示されている例に従うこともできますが、正規表現に精通していると有利です。

**ステップ 1** メインメニューから **[デバイス管理（Device Management）] > [グループ（Groups）]** を選択します。

**ステップ 2** [すべての場所（All Locations）] > [ロケーションダイナミックグループの管理（Manage Location Dynamic Groups）] の横にある をクリックします。

**ステップ 3** [他の詳細と例の表示（Show more details and examples）] をクリックして、必要な [ホスト名（Host Name）] フィールドと [グループ名（Group Name）] フィールドに入力します。

**ステップ 4** [未割り当てデバイス（Unassigned Devices）] グループに既存のデバイスがある場合は、[ルールのテスト（Test Rule）] をクリックして、作成されるグループ名のタイプのサンプリングを表示します。

**ステップ 5** [ルールの有効化（Enable Rule）] トグルをオンにして、ルールを有効にします。ルールが有効になると、システムは未割り当てのデバイスを 1 分おきに確認し、ルールに基づいてそれらを適切なグループに割り当てます。

**ステップ 6** [保存（Save）] をクリックします。

**ステップ 7** この方法で作成されたグループは、最初は [未割り当てグループ（Unassigned Groups）] の下に表示されます（ルールが初めて有効になったときに作成されます）。新たに作成したグループを必要なグループ階層に移動します。

**ステップ 8** 新しく作成した未割り当てグループを適切なグループに移動するには、次の手順を実行します。

a) すべてのロケーションの横にある をクリックし、[サブグループを追加（Add a Sub-Group）] をクリックします。
b) 新しいグループに詳細を入力して [作成（Create）] をクリックします。
c) 左ペインから未割り当てのデバイスをクリックします。
d) 右側のペインから、移動するデバイスを選択し、[グループに移動（Move to Group）] をクリックして適切なグループに移動します。

# デバイスの編集

デバイスの情報を更新するには、次の手順を実行します。

デバイスを編集する前に、変更するデバイスの CSV バックアップをエクスポートしておくことをお勧めします。

**ステップ 1** メインメニューから **[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択します。

**ステップ 2** （オプション）特定の列をフィルタ処理してデバイスのリストをフィルタ処理します。

**ステップ 3** 変更するデバイスのチェックボックスをオンにし、✎ をクリックします。

**ステップ 4** 必要に応じて、デバイスに設定されている値を編集します。

（注） ISIS システム ID や OSPF ルータ ID などのユーザー設定パラメータは、オンボードデバイスの Crosswork デバイス管理によって自動検出されません。デバイスを編集するときに、これらのフィールドが空白になる場合がありますが、同じデバイスのトポロジページにはパラメータが表示されます。

（注） 既存のフィールドに加えて、選択したデバイスに設定されているデータゲートウェイを表示することもできます。このフィールドは読み取り専用です。

**ステップ 5** [保存（Save）] をクリックします。[保存（Save）] ボタンは、すべての必須フィールドの入力が完了するまではグレー表示されます。

**ステップ 6** エラーを解決し、デバイスの到達可能性を確認します。

# デバイスの削除

次の手順を実行して、デバイスを削除します。

### 始める前に

- SR-PCE プロバイダーの [auto-onboard] プロパティを [管理（managed）] または [管理対象外（unmanaged）] オプションに設定した場合は、1 つ以上の SR-PCE の [自動オンボード（auto-onboard）] を [オフ（off）] に設定します。
- デバイスを削除する前に、デバイスが切断され、電源がオフになっていることを確認します。
- デバイス が MDT 機能を備えた Cisco NSO にマッピングされ、テレメトリ設定がプッシュされると、それらの設定はデバイスから削除されます。

- [自動オンボード（auto-onboard）] が [オフ（off）] に設定されていないためにまだ機能しており、ネットワークに接続されている場合、デバイスは削除時に管理対象外として再検出されます。

**ステップ 1** 削除するデバイスを含んでいるバックアップ CSV ファイルをエクスポートします。

**ステップ 2** メインメニューから **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択します。

**ステップ 3** （オプション）[デバイス（Devices）] ウィンドウで、[検索（Search）] フィールドにテキストを入力するか、または特定の列をフィルタ処理して、デバイスのリストをフィルタ処理します。

**ステップ 4** 削除するデバイスのチェックボックスをオンにします。

**ステップ 5** をクリックします。

**ステップ 6** 確認のダイアログボックスで [削除（Delete）] をクリックします。

# デバイスアラートの操作

Cisco Crosswork では、デバイスのアラームとイベントを「アラート」と呼んでいます。[デバイスアラーム（Device Alarms）] ウィンドウと [デバイスイベント（Device Events）] ウィンドウには、デバイスのすべてのアラートの統合されたリストが表示されます。各ウィンドウの [表示（Show）] オプションを使用して、[デバイスアラーム（Device Alarms）] ウィンドウと [デバイスイベント（Device Events）] ウィンドウを切り替えることができます。

[デバイスアラーム（Device Alarms）] ウィンドウを表示するには、**[アラート（Alerts）]** > **[デバイスアラーム（Device Alarms）]** を選択します。デフォルトでは、Crosswork は、下の最初の図に示すように、[表示（Show）] の選択が [アラーム（Alarms）] に設定された状態の [デバイスアラーム（Device Alarms）] ウィンドウを表示します。

[デバイスイベント（Device Events）] ウィンドウを表示するには、最初に **[アラート（Alerts）]** > **[デバイスアラーム（Device Alarms）]** を選択します。次に、[表示（Show）] の選択を [イベント（Events）] に変更します。Crosswork は、下の 2 番目の図に示すように、[デバイスイベント（Device Events）] ウィンドウを表示します。

図 *6 : [*デバイスアラーム（***Device Alarms***）*]* ウィンドウ

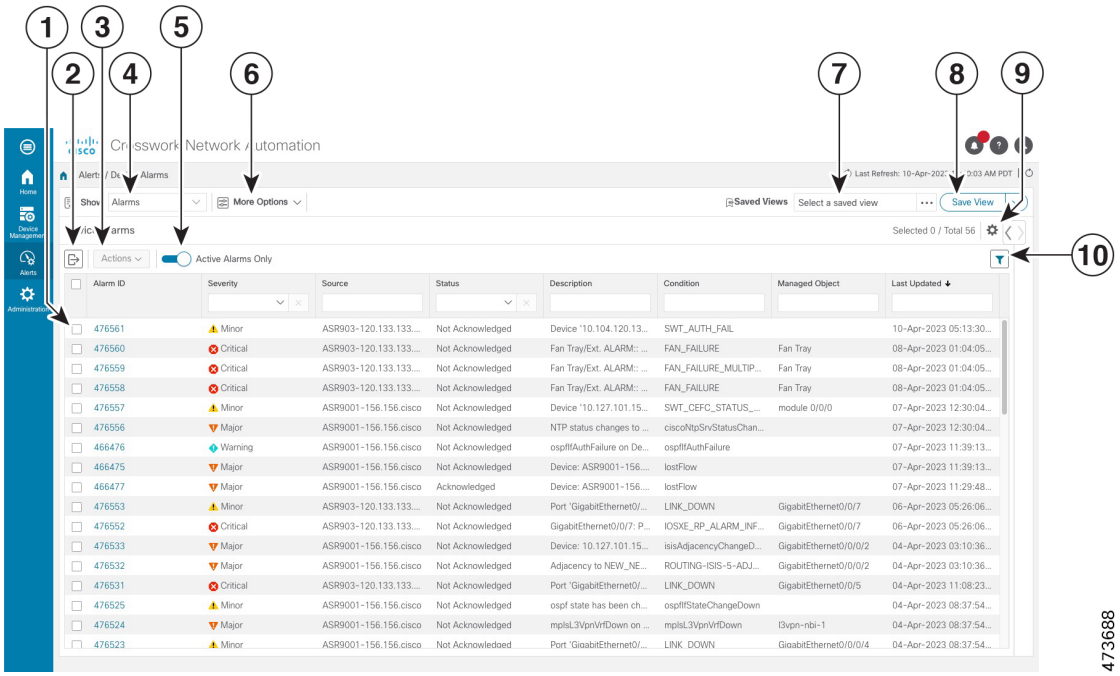
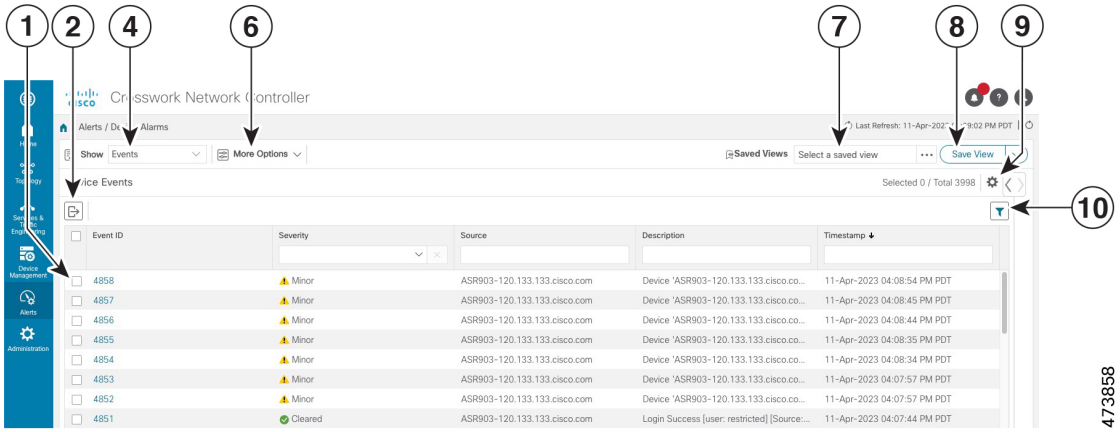



図 *7 : [*デバイスイベント（***Device Events***）*]* ウィンドウ



| 項目 | 説明 |
|---|---|
| 1 | [アラームID（Alarm ID）] または [イベントID（Event ID）] 列の横にある選択ボックスをクリックして、1 つ以上のアラートを選択します。<br><br>[アラームID（Alarm ID）] または [イベントID（Event ID）] 列の青色の ID リンクをクリックして、そのアラートの詳細を表示します。詳細については、アラートの詳細の表示 （27 ページ）を参照してください。<br><br>[デバイスアラーム（Device Alarms）] ウィンドウのみ：1 つ以上のアラームを選択すると、Crosswork は [アクション（Actions）] メニューを有効にし、選択したアラームの確認、クリア、または注釈付けを行うことができます。 |
| 2 |  アイコンをクリックして、ウィンドウに表示されているすべてのアラートの完全な情報をリストした PDF または CSV ファイルをエクスポートします。アイコンをクリックしたときに 1 つ以上のアラートが選択されている場合、ファイルには選択したアラートの情報のみが含まれます。詳細については、アラートのエクスポート （32 ページ） を参照してください。 |
| 3 | [デバイスアラーム（Device Alarms）] ウィンドウのみ：<br><br>[アクション（Actions）] ドロップダウンメニューをクリックして、現在選択されているアラームに対して次のアクションの 1 つ以上を実行します。<br><br>• [確認（Acknowledge）]：現在選択されているアラームを確認済みとしてマークします。詳細については、アラームの確認（Acknowledge Alarms） （28 ページ）を参照してください。<br><br>• [未確認（Unacknowledge）]：現在選択されているアラームのいずれかが確認されている場合、それらを未確認の状態に戻します。<br><br>• [クリア（Clear）]：現在選択されているすべてのアラームを [デバイスアラーム（Device Alarms）] ウィンドウから削除します。詳細については、アラームのクリア （29 ページ）を参照してください。<br><br>• [この状態のすべてをクリア（Clear all of this Condition）]：同じ状態の現在選択されているすべてのアラームを削除します。<br><br>• [メモ（Notes）]：現在選択されているすべてのアラームにテキストメモを追加できます。詳細については、アラームの注釈付け （30 ページ）を参照してください。<br><br>Crosswork は、[アラームID（Alarm ID）] 列の横にある選択ボックスを使用して 1 つ以上のアラームを選択するまで、[アクション（Actions）] メニューのみを有効にします。 |
| 4 | [デバイスアラーム（Device Alarms）] ウィンドウと [デバイスイベント（Device Events）] ウィンドウを切り替えます。 |

| 項目 | 説明 |
|---|---|
| 5 | [デバイスアラーム（Device Alarms）] ウィンドウのみ：<br>スライダを動かして、[すべてのアラーム（All Alarms）] または [アクティブなアラームのみ（Active Alarms only）] を表示するようにウィンドウを設定します。デフォルトは [アクティブなアラームのみ（Active Alarms only）] です。 |
| 6 | [その他のオプション（More Options）] をクリックして、すべてのアラートを表示するか、最新のアラートのみを表示するか、およびアラート表示を Crosswork データベースと同期する頻度を指定します。<br>[アラーム履歴（Alarm History）] または [イベント履歴（Event History）] チェックボックスをオフにすると、リストにはすべてのアラートが表示されます。<br>[自動同期（Auto Sync）] チェックボックスをオフにすると、Crosswork は同期を一時停止します。 |
| 7 | [保存されたビュー（Saved Views）] フィールドをクリックして、[ビューの保存（Save View）] ボタンを使用して作成した、以前に保存したビューを管理します。[保存されたビューの管理（Manage Saved Views）] ポップアップウィンドウでは、すべてのビューまたは保存したビューのみを表示、並べ替え、確認できます。詳細については、「保存されたアラートビューの操作 （30 ページ）」を参照してください。 |
| 8 | [ビューの保存（Save View）] ボタンをクリックして、現在のビューを保存します。Crosswork は、ビューを一意の名前で入力して保存するように求めます。 |
| 9 | アラートリストに表示する列を選択するには、⚙ をクリックします。 |
| 10 | ▼ をクリックして、アラートリストの上部にあるフローティング フィルタ フィールドの表示を切り替えます。リストの 1 つ以上の列にフィルタ条件を設定するには、これらのフィールドを使用します。<br>アイコンの横に表示される [適用したフィルタ（Filters Applied）] リンクをクリックして、設定したフィルタ条件をクリアします。 |

Crosswork では、生産要件に合わせてアラート設定をカスタマイズできます。詳細については、以下のトピックをクリックしてください。

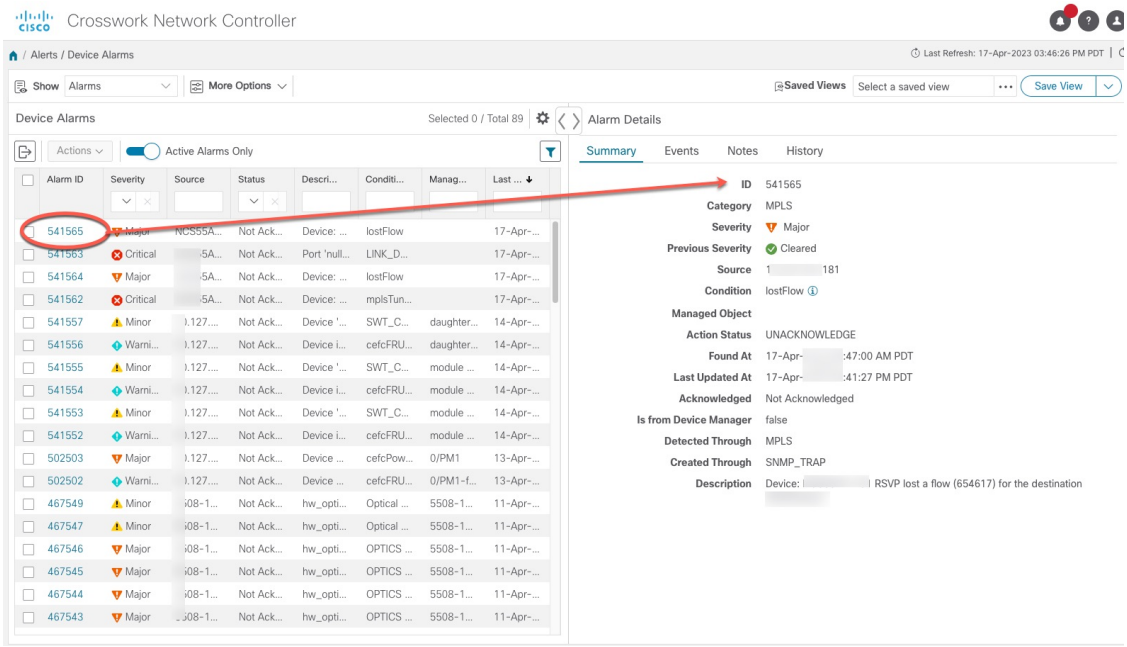
- アラートデバイスのカスタマイズ （33 ページ）
- アラームの自動クリアのカスタマイズ （33 ページ）
- アラームの説明テキストのカスタマイズ （34 ページ）
- アラートのクリーンアップのカスタマイズ （35 ページ）
- アラームの重大度のカスタマイズ （36 ページ）

# アラートの詳細の表示

**[アラート（Alerts）]** > **[デバイスアラート（Device Alerts）]** を選択して、アラームまたはイベントのリストを表示するときはいつでも、[アラームID（Alarm ID）] または [イベントID（Event ID）] 列でアラートの ID 番号をクリックして、そのアラートに関する詳細情報を取得できます。

例：**[アラート（Event ID）]** > **[デバイスアラート（Device Alerts）]** を選択して [デバイスアラーム（Device Alarms）] ウィンドウを表示し、[アラームID（Alarm ID）] 列の ID 番号をクリックすると、次の図に示すような [アラームの詳細（Alarm Details）] ウィンドウが開きます。

**図 *8 : [アラームの詳細（Alarm Details）] ウィンドウ：[概要（Summary）] タブ***



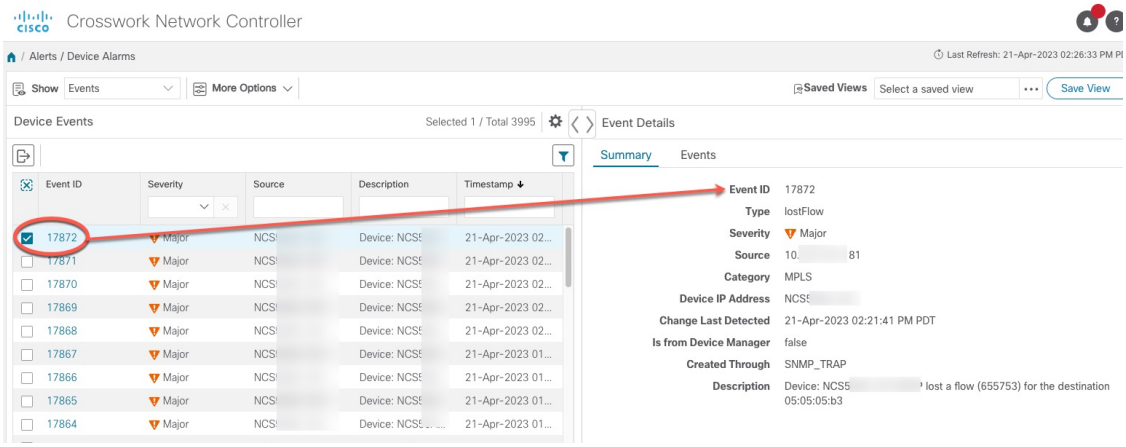

[概要（Summary）] タブがデフォルトであり、選択したアラームに関する基本情報が表示されます。

[アラームの詳細（Alarm Details）] ウィンドウを表示しているときに、次をクリックできます。

- は、[概要（Summary）] タブの [条件（Condition）] フィールドの横にあります。組織向けにカスタマイズされている場合は、条件の説明と、アラームをクリアするために組織が推奨するアクションが表示されます。
- [イベント（Events）] タブ。選択したアラームに関連するイベントが表示されます。
- [メモ（Notes）] タブ。自分や同僚がアラームに追加した注釈が表示されます。
- [履歴（History）] タブ。アラームがいつ、どのように発生して解決されたかに関する情報が表示されます。

イベントでも同じことができます。例：**[アラート（Alerts）]** > **[デバイスアラート（Device Alerts）]** を選択し、[表示（Show）] フィールドで [イベント（Events）] を選択すると、Crossworkは [デバイスイベント（Device Events）] ウィンドウを表示します。次に、[イベントID（Event ID）] 列のID番号をクリックすると、Crossworkは次のような [イベントの詳細（Event Details）] ウィンドウを表示します。

**図 *9*：*[*イベントの詳細（*Event Details*）*]*ウィンドウ：*[*概要（*Summary*）*]*タブ**




[イベントの詳細（Event Details）] ウィンドウの [概要（Summary）] タブがデフォルトであり、選択したイベントに関する基本情報が表示されます。

[イベントの詳細（Event Details）] ウィンドウを表示しているときに、[イベント（Events）] タブをクリックして、選択したイベントに関連付けられている他のイベントを表示できます。

# アラームの確認（Acknowledge Alarms）

次の手順に従って、デバイスアラームを確認するか、確認済みのアラームを未確認のステータスに戻します。**[アクション（Actions）]** > **[確認（Acknowledge）]** を選択する前にチェックボックスをオンにすることで、複数のアラームを同時に確認できます。

アラームを確認すると、アラームは永続的にクリアされますが、引き続き [デバイスアラーム（Device Alarms）] ウィンドウにリストされます。

**ステップ 1** メインメニューから **[デバイスアラート（Device Alerts）]** > **[デバイスアラーム（Device Alarms）]** を選択します。Crossworkは [デバイスアラーム（Device Alarms）] ウィンドウを表示します。

**ステップ 2** （オプション）列をフィルタリングするか、[アクティブなアラームのみ（Active Alarms Only）] スライダを変更するか、または⚙を使用して列を追加または削除することにより、アラームのリストをフィルタリングします。

**ステップ 3** （オプション）列をフィルタリングするか、または⚙を使用して列を追加または削除してから再度フィルタリングすることにより、アラームのリストをフィルタリングします。[その他のオプション（More Options）] ドロップダウンを使用して、現在のアラームのみを表示するかどうか、およびウィンドウが表示されたリ

ストを Crosswork データベースと同期する頻度を選択します。[アクティブなアラームのみ（Active Alarms Only）] スライダを動かして、すべてのアラームを表示します。

**ステップ 4** 確認するアラームの ID の横にあるチェックボックスをオンにします。

**ステップ 5** **[アクション（Actions）]** > **[確認（Acknowledge）]** を選択します。

**ステップ 6** [OK] をクリックして確認アクションを完了します。

**ステップ 7** 確認済みのアラームを未確認のステータスに戻すには、次の手順を実行します。

a) 確認済みのアラームの ID の隣にあるチェックボックスをオンにします。

b) **[アクション（Actions）]** > **[未確認（Unacknowledged）]** を選択します。Crosswork は、アラームステータスを未確認にリセットします。

# アラームのクリア

次の手順に従って、デバイスのアラームをクリアします。チェックボックスをオンにすることで、1 つまたは複数のアラームをクリアできます。同じアラーム状態（「lostFlow」や「mplsTunnelDown」など）を報告するすべてのアラームをクリアすることもできます。

アラームをクリアすると、[デバイスアラーム（Device Alarms）] ウィンドウからアラームが削除されますが、トリガーイベントが繰り返されると、アラームが再度生成されます。

**ステップ 1** メインメニューから **[デバイスアラート（Device Alerts）]** > **[デバイスアラーム（Device Alarms）]** を選択します。Crosswork は [デバイスアラーム（Device Alarms）] ウィンドウを表示します。

**ステップ 2** （オプション）列をフィルタリングするか、[アクティブなアラームのみ（Active Alarms Only）] スライダを変更してすべてのアラームを表示するか、または⚙を使用して列を追加または削除することにより、アラームのリストをフィルタリングします。[その他のオプション（More Options）] ドロップダウンを使用して、現在のアラームのみを表示するか、すべてのアラームを表示するか、およびウィンドウが表示されたリストを Crosswork データベースと同期する頻度を選択します。

**ステップ 3** クリアするアラームの ID の横にあるチェックボックスをオンにしてから、**[アクション（Actions）]** > **[クリア（Clear）]** を選択します。

**ステップ 4** [OK] をクリックしてクリアアクションを完了します。

**ステップ 5** 同じ条件を共有するすべてのアラームをクリアするには：

a) クリアする条件を共有する 1 つ以上のアラームの ID の横にあるチェックボックスをオンにします（異なる条件のアラームを選択できます）。

b) **[アクション（Actions）]** > **[この状態のすべてをクリア（Clear all of this Condition）]** を選択します。

c) [OK] をクリックして clear-all アクションを完了します。

# アラームの注釈付け

アラームメモは、同僚と情報を共有したり、自動監視で見逃した重要な情報を記録したりするのに便利な方法です。メモはアラームに永続的に添付され、アラームがデータベースから消去されるか、ユーザーによって削除されるまで取得できます。メモ作成者のユーザー ID は、メモとともに保存されます。

以下の手順に従って、デバイスアラームに注釈を付けます。メモの追加を選択する前にチェックボックスをオンにすることで、複数のアラームに同時に注釈を付けることができます。メモは、プレーンテキストのエントリのみをサポートします。

**ステップ 1** メインメニューから **[デバイスアラート（Device Alerts）]** > **[デバイスアラーム（Device Alarms）]** を選択します。Crosswork は [デバイスアラーム（Device Alarms）] ウィンドウを表示します。

**ステップ 2** （オプション）列をフィルタリングするか、[アクティブなアラームのみ（Active Alarms Only）] スライダを変更してすべてのアラームを表示するか、または⚙を使用して列を追加または削除することにより、アラームのリストをフィルタリングします。[その他のオプション（More Options）] ドロップダウンを使用して、現在のアラームのみを表示するか、すべてのアラームを表示するか、およびウィンドウが表示されたリストを Crosswork データベースと同期する頻度を選択します。

**ステップ 3** 注釈を付けるアラームの ID の横にあるチェックボックスをオンにします。

**ステップ 4** **[アクション（Actions）]** > **[メモ（Notes）]** を選択します。Crosswork に [注釈の追加（Add annotation）] ポップアップが表示されます。

**ステップ 5** 選択したアラームに追加するメモのテキストを入力します。

**ステップ 6** [追加（Add）] をクリックしてメモを追加します。

# 保存されたアラートビューの操作

[デバイスアラーム（Device Alarms）] ウィンドウと [デバイスイベント（Device Events）] ウィンドウのフィルタリングオプションを使用して、必要なアラートのみを表示できます。その後、このフィルタ処理された表示を保存されたビューとして保存できます。自分および他の Crosswork ユーザーは、数回クリックするだけで、保存されたビューをウィンドウに再度呼び出すことができます。

保存されたビューを再度呼び出したときに表示される個々のアラームとイベントは、ネットワークデバイスの現在の状態に応じて、最初にビューを保存したときに表示されるアラートと異なる場合があることに注意してください。

**ビューを必要なアラートにフィルタ処理するには**：

- ▼ をクリックして、[デバイスアラーム（Device Alarms）] または [デバイスイベント（Device Events）] リストの上部にあるフローティング フィルタ フィールドを切り替えます。次に、1 つ以上のフィールドで、アラートがリストに表示されるために一致する必要がある条件を入力または選択します。

- ⚙をクリックして、[デバイスアラーム（Device Alarms）] または [デバイスイベント（Device Events）] リストに表示される列を選択します。
- [デバイスアラーム（Device Alarms）] ウィンドウのみ：[アクティブなアラームのみ（Active Alarms Only）] スライダを左に移動してすべてのアラームの表示を有効にするか、右に移動してアクティブなアラームのみを表示します。

**現在のビューを新しい保存されたビューとして保存するには：**

1. 必要に応じて、現在のビューでアラートをフィルタ処理します。
2. 保存されたビューがすでに表示されている場合は、[保存されたビュー（Saved Views）] フィールドで保存されたビューの名前の横にある✕アイコンをクリックします。これを行わないと、現在保存されているビューが現在のビューで上書きされ、保存されたビューの名前を変更するように求められることはありません。
3. [Save View] をクリックします。
4. 新しい保存されたビューの一意の名前を入力します。
5. [保存（Save）] をクリックします。

**保存されたビューを表示するには：**

1. [保存されたビュー（Saved Views）] フィールドの横の⋯をクリックします。Crossworkに [保存されたビューの管理（Manage Saved Views）] ウィンドウが表示されます。
2. [マイビュー（My Views）] または [すべてのビュー（All Views）] タブをクリックするか、[並べ替え（Sort By）] メニューからオプションを選択するか、または🔍で検索フィールドに条件を入力して、表示する保存されたビューを見つけます。
3. 表示する保存されたビューの名前をクリックします。Crossworkはアラートリストを変更して、保存されたビューを表示します。

**現在保存されているビューを上書きするには：**

1. 上書きする保存されたビューを表示します。
2. 必要に応じて、アラートをフィルタ処理します。
3. [Save View] をクリックします。Crossworkは、保存されたビューを現在のビューで上書きします。

**保存されたビューを削除するには：**

1. [保存されたビュー（Saved Views）] フィールドの横の⋯をクリックします。Crossworkに [保存されたビューの管理（Manage Saved Views）] ウィンドウが表示されます。
2. [マイビュー（My Views）] または [すべてのビュー（All Views）] タブをクリックするか、[並べ替え（Sort By）] メニューからオプションを選択するか、または🔍で検索フィールドに条件を入力して、削除する保存されたビューを見つけます。

3. 削除する保存されたビューの名前の横にある をクリックします。Crossworkは、保存されたビューを削除します。

# アラートのエクスポート

次の手順に従って、オフラインストレージと分析のためにデバイスアラートをエクスポートします。

アラームをエクスポートするには、アラームを表示している必要があります。イベントをエクスポートする場合は、イベントを表示している必要があります。アラートをカンマ区切り値（CSV）またはPDFファイル形式にエクスポートすることを選択できます。

デフォルトでは、Crossworkは、[デバイスアラーム（Device Alarms）]または[デバイスイベント（Device Events）]リストに現在表示されているすべてのアラートをエクスポートします。 をクリックする前に、リストをフィルタリングするか、必要なアラートの横にあるチェックボックスを選択することにより、エクスポートされたファイルの内容を必要なアラートのみに制限できます。

**ステップ1** メインメニューから **[デバイスアラート（Device Alerts）]** > **[デバイスアラーム（Device Alarms）]** を選択します。Crossworkは[デバイスアラーム（Device Alarms）]ウィンドウを表示します。

アラームの代わりにイベントをエクスポートする場合：[表示（Show）]ドロップダウンで、[イベント（Events）]を選択します。

**ステップ2** （オプション）列をフィルタリングするか、または を使用して列を追加または削除してから再度フィルタリングすることにより、エクスポートするイベントのリストをフィルタリングします。[その他のオプション（More Options）]ドロップダウンを使用して、現在のアラートのみを表示するか、すべてのアラートを表示するか、およびウィンドウが表示されたリストをCrossworkデータベースと同期する頻度を選択します。アラームのみ：[アクティブなアラームのみ（Active Alarms Only）]スライダを動かします。エクスポートするアラートのみのIDの横にあるチェックボックスをオンにすることもできます。

アラームのみ：[アクティブなアラームのみ（Active Alarms Only）]スライダを動かします。エクスポートするアラートのIDの横にあるチェックボックスをオンにすることもできます。

**ステップ3** をクリックします。Crossworkは、エクスポートするアラートのタイプに適したエクスポート ポップアップ ウィンドウを表示します。

**ステップ4** [名前（Name）]フィールドに、宛先ファイルの名前を入力します（ファイル名の拡張子は含めないでください）。

**ステップ5** [フォーマット（Format）]ボタンを使用して、[CSV]または[PDF]を選択します。

**ステップ6** [OK]をクリックしてエクスポートを開始し、新しいファイルの保存場所を指定します。

# アラートデバイスのカスタマイズ

Crosswork を使用すると、アラートを受信する Cisco デバイスのセットをカスタマイズできます。

**ステップ 1** メインメニューから、**[管理（Administration）] > [システム設定（System Settings）] > [デバイスのアラーム設定（Device Alarm Settings）] > [デバイスのアラーム管理（Device Alarm Admin）] > [マネージャ設定（Manager Settings）] >** を選択します。Crosswork は、Crosswork がアラートを受信できるすべてのシスコデバイスのリストを含む [マネージャ設定（Manager Settings）] ウィンドウを表示します。

**ステップ 2** （オプション）[名前（Name）] および [ステータス（Status）] 列のフィルタフィールドでフィルタ処理して、デバイスのリストをフィルタ処理します。をクリックして、フィルタフィールドのオンとオフを切り替えることができます。

**ステップ 3** デバイスタイプからのアラートの受信を開始するには、デバイスタイプの名前の横に表示されるチェックボックスをクリックし、[有効にする（Enable）] をクリックします。

**ステップ 4** デバイスタイプからのアラートの受信を停止するには、デバイスタイプの名前の横に表示される選択チェックボックスをクリックし、[無効にする（Disable）] をクリックします。

**ステップ 5** 変更が完了したら、[保存（Save）] をクリックして適用します。

# アラームの自動クリアのカスタマイズ

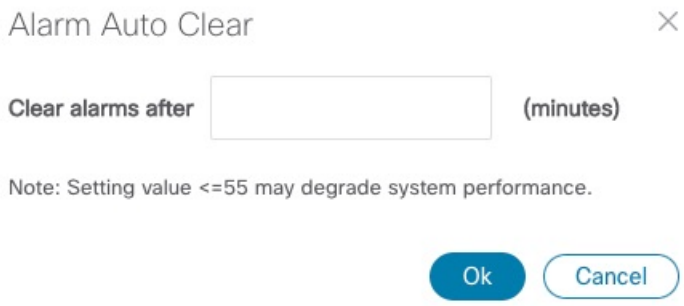
Crosswork を使用すると、アラームを自動的にクリアできるかどうか、およびアラームを自動的にクリアするまで何分待つかをカスタマイズできます。

**ステップ 1** メインメニューから、**[管理（Administration）] > [システム設定（System Settings）] > [デバイスのアラーム設定（Device Alarm Settings）] > [重大度および自動クリア（Severity and Auto Clear）]** を選択します。Crosswork は、[重大度および自動クリア（Severity and Auto Clear）] ウィンドウを表示し、すべての標準アラームタイプのリストを表示します。

**ステップ 2** （オプション）[名前（Name）]、[カテゴリ（Category）]、[重大度（Severity）]、および [自動クリア期間（Auto Clear Duration）] 列のフィルタフィールドの 1 つ以上で値を入力または選択して、アラームのリストをフィルタリングします。をクリックして、フィルタフィールドのオンとオフを切り替えることができます。

**ステップ 3** アラームが自動的にクリアされるまでの時間を割り当てるには、リスト内のアラーム名の隣に表示されるチェックボックスをクリックします。次に、[アラームの自動クリア（Alarm Auto Clear）] をクリックします。

**ステップ 4** [アラームの自動クリア（Alarm Auto Clear）] ウィンドウが表示されている状態で、[アラームをクリアする経過時間（Clear alarms after）] フィールドに、クリアするまでの待機時間を分単位で入力します。次に、[OK] をクリックします。




**ステップ 5** アラームが自動的にクリアされないようにするには、まずリストでアラームを選択してから、[アラームの自動クリアを元に戻す（Revert Alarm Auto Clear）] をクリックします。

**ステップ 6** 変更が完了したら、[保存（Save）] をクリックして適用します。

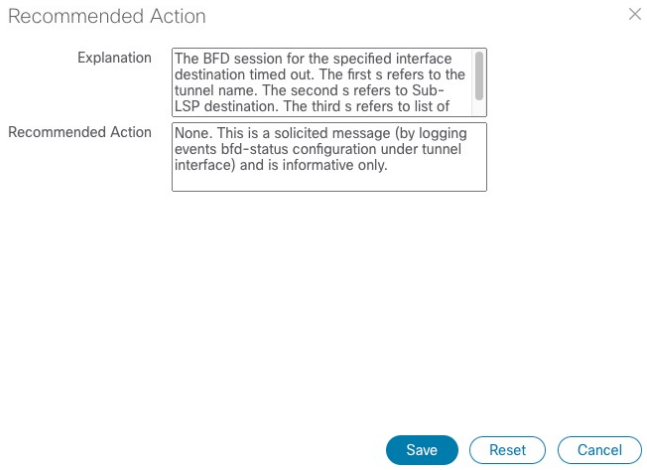
# アラームの説明テキストのカスタマイズ

Crosswork を使用すると、Crosswork データベース内の各アラームに使用できる、[説明（explanation）] および [推奨処置（Recommended Action）] の説明テキストをカスタマイズできます。自分または他のユーザーがこれらのテキストに変更を加えた場合、元のテキストを復元することを選択することもできます。

**ステップ 1** メインメニューから、**[管理（Administration）] > [システム設定（System Settings）] > [デバイスのアラーム設定（Device Alarm Settings）] > [重大度および自動クリア（Severity and Auto Clear）]** を選択します。Crosswork は、[重大度および自動クリア（Severity and Auto Clear）] ウィンドウを表示し、すべての標準アラームタイプのリストを表示します。

**ステップ 2** （オプション）[名前（Name）]、[カテゴリ（Category）]、[重大度（Severity）]、および [自動クリア期間（Auto Clear Duration）] 列のフィルタフィールドの 1 つ以上で値を入力または選択して、アラームのリストをフィルタリングします。をクリックして、フィルタフィールドのオンとオフを切り替えることができます。

**ステップ 3** アラームの説明テキストをカスタマイズするには、リスト内のアラーム名の隣に表示されているチェックボックスをクリックします。次に、[推奨処置（Recommended Action）] をクリックして、[推奨処置（Recommended Action）] ウィンドウを表示します。




**ステップ 4** [説明（Explanation）] および [推奨処置（Recommended Action）] フィールドをクリックし、必要なテキストを入力します。これらのフィールドに任意の形式のプレーン ASCII テキストを入力するか、すでにそこにあるテキストを編集できます。完了したら、[保存（Save）] をクリックします。

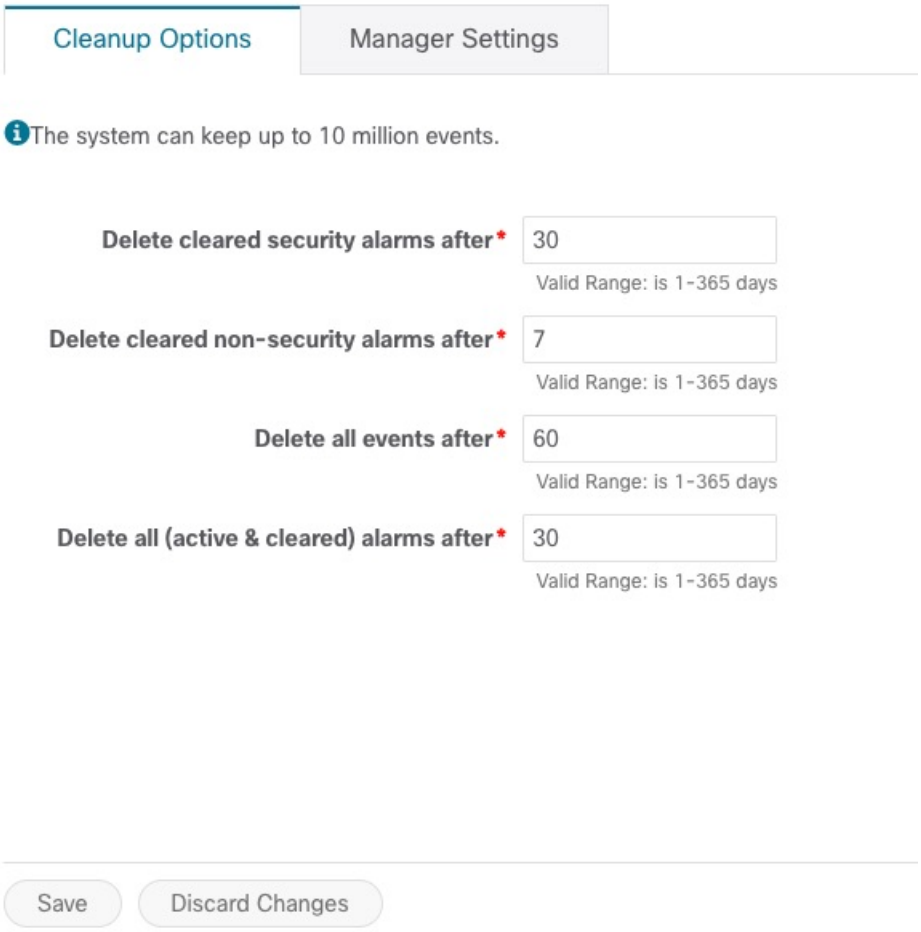
**ステップ 5** アラームの元の Crosswork 説明テキストに戻すには、最初にリストでアラームを選択し、[推奨処置（Recommended Action）] をクリックしてから [リセット（Reset）] をクリックします。完了したら、[保存（Save）] をクリックします。

# アラートのクリーンアップのカスタマイズ

Crosswork は、最大 1000 万のイベントを保存できます。その制限に達する前に、システムは自動的にイベントおよびアクティブまたはクリアされたアラームの削除を定期的なスケジュールで開始します。以下の手順に従って、スケジュールを表示およびカスタマイズできます。

**ステップ 1** メインメニューから、**[管理（Administration）] > [システム設定（System Settings）] > [デバイスのアラーム設定（Device Alarm Settings）] > [デバイスのアラーム管理（Device Alarm Admin）] > [クリーンアップオプション（Cleanup Options）]** を選択します。Crosswork は、[クリーンアップオプション（Cleanup Options）] ウィンドウを表示します。

図 *10* : アラートのクリーンアップオプション（***Alert Cleanup Options***）




**ステップ 2** 必要に応じて、アラートの種類ごとにクリーンアップスケジュールを変更します。スケジュールを変更するには、Crosswork が各種類のアラートを削除するまでの日数を入力します。有効な範囲は、1 日ー 365 日です。すべてのフィールドに入力が必要です。

**ステップ 3** 終了したら、[保存（Save）] をクリックして変更を適用します。

# アラームの重大度のカスタマイズ

Crosswork アラームデータベースをカスタマイズして、選択した重大度レベルを特定のアラームに割り当てることができます。

**ステップ 1** メインメニューから、**[管理（Administration）] > [システム設定（System Settings）] > [デバイスのアラーム設定（Device Alarm Settings）] > [重大度および自動クリア（Severity and Auto Clear）]**を選択します。Crosswork は、[重大度および自動クリア（Severity and AutoClear）] ウィンドウを表示し、すべての標準アラームタイプのリストを表示します。

**ステップ 2** （オプション）[名前（Name）]、[カテゴリ（Category）]、[重大度（Severity）]、および [自動クリア期間（Auto Clear Duration）] 列のフィルタフィールドの 1 つ以上で値を入力または選択して、アラームのリストをフィルタリングします。をクリックして、フィルタフィールドのオンとオフを切り替えることができます。

**ステップ 3** アラームの重大度をカスタマイズするには、リスト内のアラーム名の隣に表示されているチェックボックスをクリックします。次に、[重要度設定（Severity Configuration）] をクリックして、[重要度設定（Severity Configuration）] ページを表示します。


**ステップ 4** アラームに割り当てる重大度レベルをクリックします。次に、[OK] をクリックします。

**ステップ 5** 変更が完了したら、[保存（Save）] をクリックして適用します。

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。