# インベントリの管理



# インベントリについて

インベントリ機能は、ホストの IP アドレス、MAC アドレス、およびそのデータベース内のデバイスに関するネットワーク アタッチメント ポイントなどの詳細を取得して保存します。

また、インベントリ機能は、デバイスの制御性機能と連携して、デバイスに必要なネットワーク設定を構成することもできます（ネットワーク設定がデバイスにまだ存在しない場合）。

インベントリは、必要に応じて次のプロトコルを使用します。

- リンク層検出プロトコル（LLDP）
- IP デバイス トラッキング（IPDT）またはスイッチ統合セキュリティ機能（SISF）（IPDT または SISF をデバイス上で有効にする必要があります）。
- LLDP Media Endpoint Discovery （このプロトコルは IP フォンや一部のサーバーの検出に使用されます）。
- ネットワーク設定プロトコル（NETCONF）デバイスのリストについては、ディスカバリの前提条件 を参照してください。

初期検出後、Cisco DNA Center は定期的にデバイスをポーリングすることでインベントリを維持します。デフォルトの間隔は 24 時間ごとです。ただし、この間隔は、ネットワーク環境の必要性に応じて変更できます。詳細については、デバイスポーリング間隔の更新 （37ページ）を参照してください。また、デバイスの設定変更によって SNMP トラップがトリガーされ、次にデバイスの再同期がトリガーされます。ポーリングはデバイス、リンク、ホスト、およびインターフェイスごとに実行されます。アクティブ状態が 1 日未満のデバイスのみが表示されます。これによって、古いデバイス データが表示されないようにします。500 個のデバイスのポーリングに約 20 分かかります。

# インベントリと Cisco ISE の認証

Cisco ISE には、Cisco DNA Center で次の 2 つの異なる使用例があります。

- ネットワークでデバイス認証に Cisco ISE を使用する場合、Cisco DNA Center で Cisco ISE を設定する必要があります。これにより、Cisco DNA Center でデバイスをプロビジョニングする際に、ユーザーが定義した Cisco ISE サーバー情報を使用してデバイスが設定されます。また、Cisco DNA Center は Cisco ISE サーバーでデバイスを設定し、後に続くデバイスの更新プログラムについても伝えます。Cisco DNA Center での Cisco ISE の設定については、グローバル ネットワーク サーバーの設定を参照してください。

（注） Cisco ISE を使用して Cisco Catalyst 9800 シリーズ デバイスを認証する場合は、NETCONF ユーザーに権限が提供されるように Cisco ISE を設定する必要があります。

ネットワーク障害や Cisco ISE サーバーのダウンによって予定通りにデバイスが Cisco ISE サーバーで設定または更新されていない場合、Cisco DNA Center は一定の待機期間が経過した後に自動的に操作を再試行します。ただし、入力の検証エラーとして Cisco ISE から拒否されていることが障害の原因である場合、Cisco DNA Center は操作を再試行しません。

Cisco DNA Center が Cisco ISE サーバーでデバイスを設定および更新する場合、トランザクションは Cisco DNA Center の監査ログでキャプチャされます。Cisco DNA Center や Cisco ISE インベントリに関する問題のトラブルシューティングに監査ログを役立てることができます。

デバイスのプロビジョニング後、Cisco DNA Center は Cisco ISE でデバイスを認証します。Cisco ISE に到達できない（RADIUS 応答がない）場合、デバイスはローカルのログイン クレデンシャルを使用します。Cisco ISE に到達できるが Cisco ISE にデバイスが存在しない場合や、そのクレデンシャルが Cisco DNA Center で設定されたクレデンシャルと一致しない場合、デバイスはローカルのログイン クレデンシャルを使用するためにフォールバックしません。代わりに、部分的な収集状態になります。

この状態を回避するには、Cisco DNA Center を使用してデバイスをプロビジョニングする前に、必ず Cisco DNA Center で使用しているのと同じデバイス クレデンシャルで Cisco ISE のデバイスを設定します。また、有効なディスカバリ クレデンシャルを設定したことも確認してください。詳細については、ディスカバリ クレデンシャルを参照してください。

- 必要に応じて、Cisco ISE を使用してデバイス グループにアクセス制御を実行できます。

# インベントリに関する情報の表示

[Inventory] テーブルには、検出された各デバイスの情報が表示されます。列ヘッダーをクリックすると、行が昇順にソートされます。列ヘッダーをもう一度クリックすると、行が降順にソートされます。

テーブルで表示または非表示にする列を選択するには、 をクリックします。列の選択はセッション間では保持されない点に注意してください。

デバイスの選択は、ビュー間で保持されます。デバイスを選択し、[Focus] ドロップダウンリストから別のビューを選択すると、選択内容は新しいビューに保持されます。

デフォルトでは、[Inventory] テーブルに 25 のエントリが表示されます。追加のエントリを表示するには、[Show More] をクリックします。[Inventory] テーブルには最大 200 のエントリを表示できます。

[Inventory] テーブルに表示されるエントリの数は、ビュー間で保持されます。[Inventory] テーブルに 25 を超えるエントリがあり、[Focus] ドロップダウンリストから別のビューを選択した場合、同じ数のエントリが新しいビューで保持されます。

### 始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

---

[Provision]Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します > [Inventory] の順に選択します。

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。次の表に、使用できる情報を記載します。

表 *1:* インベントリ

| カラム | 説明 |
| --- | --- |
| **Device Name** | |

| カラム | 説明 |
| --- | --- |
| | デバイスの名前。<br><br>デバイス名をクリックすると、デバイスの次の詳細が表示されます。<br><br>[Details]：デバイス名、到達可能性ステータス、管理性ステータス、IP アドレス、デバイスモデル、ロール、稼働時間、サイトなどの詳細が表示されます。<br><br>• [View Assurance 360]：[Assurance 360] ウィンドウが表示されます。360 を開くには、アシュアランス アプリケーションをインストールしている必要があります。<br><br>• **Interfaces**<br><br>• [Ethernet Ports]（すべてのデバイスが対象）：イーサネットポートの動作ステータスと管理ステータスが表示されます。<br><br>Cisco Catalyst 4000 シリーズ、6000 シリーズ、および 9000 シリーズ スイッチとアグリゲーション サービス ルータ（ASR）1000 シリーズ ルータの場合、ポートビューにはラインカードとスーパーバイザカードの詳細が表示されます（使用可能な場合）。<br><br>ラインカードには、プラットフォーム、アドレス、シリアル番号、ロール、およびスタックメンバー番号の詳細が含まれます。スーパーバイザカードには、部品番号、シリアル番号、スイッチ番号、およびスロット番号の詳細が含まれます。<br><br>[Ports] テーブルには、動作ステータス、管理ステータス、タイプ、MAC アドレス、PoE ステータス、速度、および MTU が表示されます。このテーブルには、次のタイプの VLAN の ID も表示されます。<br><br>• 製造時提供のデフォルト VLAN の VLAN ID<br><br>• 設定されたデフォルト VLAN の VLAN ID<br><br>• 設定された VLAN の VLAN ID<br><br>Cisco Catalyst 2000、3000、および 9000 シリーズ スイッチの場合は、ポートビューでポートをクリックするか、[Ports] テーブルのポート名をクリックして、ポートの最大割り当て電力、割り当て電力、および消費電力の詳細を表示します。<br><br>• [VLANs]（スイッチとハブのみが対象）：VLAN のテーブルに、動作ステータス、管理ステータス、VLAN タイプ、および IP アドレスが表示されます。このテーブルには、次のタイプの VLAN の ID も表示されます。<br><br>• 製造時提供のデフォルト VLAN の VLAN ID<br><br>• 設定されたデフォルト VLAN の VLAN ID<br><br>• 設定された VLAN の VLAN ID |

| カラム | 説明 |
|---|---|
| | [Search] や [Filter] のオプションをクリックして、目的の VLAN の詳細を表示できます。<br>• [Virtual Ports]（ワイヤレスデバイス、コントローラ、ルータのみが対象）：ポートのテーブルに、動作ステータス、管理ステータス、タイプ、MAC アドレス、PoE ステータス、速度、および MTU が表示されます。[Search] や [Filter] のオプションをクリックして、目的のポートの詳細を表示できます。<br>• [Hardware and Software]：デバイスのハードウェアとソフトウェアの詳細が表示されます。<br>• [Configuration]：**show running-config** コマンドの出力で表示される内容に似た詳細な設定情報が表示されます。<br>この機能は、アクセスポイント(AP)とワイヤレス コントローラにはサポートされていません。したがって、これらのデバイスタイプの場合は設定データは返されません。<br>• [Power]：デバイスに割り当てられている電力、消費電力、および残りの電力に関する詳細が表示されます。[Power Supplies] テーブルに、動作ステータス、シリアル番号、およびベンダー機器タイプの詳細が表示されます。<br>• [Fans]：ファンの動作ステータス、シリアル番号、およびベンダー機器タイプが表示されます。<br>• [User Defined Fields]：デバイスに関連付けられているユーザー定義フィールドが表示されます。<br>• [Config Drift]：構成の変更を表示し、同じデバイスの任意の 2 つのバージョンを選択して、各バージョンの実行中の構成データを比較できます。<br>（注） 実行中の構成データは、ワイヤレスコントローラやレガシーコントローラなどのデバイスではサポートされません。<br>• [Wireless Info]：プライマリとセカンダリの管理対象ロケーションが表示されます。<br>• [Mobility]：モビリティグループ名、RF グループ名、仮想 IP、およびモビリティ MAC アドレスが表示されます。<br>（注） 赤で表示されているデバイス名は、インベントリがデバイスをポーリングしておらず、30 分を超える期間にわたってその情報を更新していないことを意味しています。 |
| **IP Address** | デバイスの IP アドレス。 |

| カラム | 説明 |
| --- | --- |
| **Support Type** | 以下に示すデバイスのサポートレベルが表示されます。<br>• [Supported]：Cisco DNA Center のすべてのアプリケーションに対してデバイスパックがテスト済みです。これらのデバイスのいずれかの Cisco DNA Center 機能が動作しない場合は、サービスリクエストを開くことができます。<br>• [Unsupported]：Cisco DNA Center でテストおよび認定されていない他のすべてのシスコデバイスとサードパーティ製デバイス。これらのデバイスについて、Cisco DNA Center でさまざまな機能をベストエフォートとして試すことができます。ただし、Cisco DNA Center の機能が期待どおりに動作しない場合 、サービスリクエストまたはバグを発生させることは求められていません。<br>• [Third Party]：デバイスパックは、お客様またはビジネスパートナーによって構築され、認定プロセスを経ています。サードパーティ製デバイスは、ディスカバリ、インベントリ、トポロジなどの基本自動化機能をサポートします。Cisco TAC は、これらのデバイスの初期レベルのサポートを提供します。ただし、デバイスパックに問題がある場合は、ビジネスパートナーに連絡する必要があります。 |
| **Reachability** | 以下は、さまざまなステータスのリストです。<br>• [Reachable]：Cisco DNA Center から SNMP、HTTP（S）、および NETCONF ポーリングメカニズムを使用してデバイスに到達できます。<br>• [Ping Reachable]：Cisco DNA Center から ICMP ポーリングメカニズムを使用してデバイスに到達できます。SNMP、HTTP（S）、および Netconf ポーリングメカニズムでは到達できません。<br>• [Unreachable]：SNMP、HTTP（S）、Netconf、および ICMP のいずれのポーリングメカニズムでもデバイスに到達できません。 |
| **Manageability** | デバイスのステータスが次のように示されます。<br>• [Managed] と緑色のチェックアイコン：デバイスに到達可能で、完全に管理されています。<br>• [Managed] とオレンジ色のエラーアイコン：デバイスは管理されていますが、到達不能、認証失敗、Netconf ポートがない、内部エラーなど、何らかのエラーがあります。エラーメッセージにカーソルを合わせると、エラーおよび影響を受けるアプリケーションに関する詳細が表示されます。<br>• [Unmanaged]：デバイスの接続の問題が原因でデバイスに到達できず、インベントリ情報が収集されていません。 |
| **MAC Address** | デバイスの MAC アドレス。 |

| カラム | 説明 |
|---|---|
| **Image Version** | デバイスで現在実行されている Cisco IOS ソフトウェア。 |
| **Platform** | シスコ製品の部品番号。 |
| **Serial Number** | シスコ デバイスのシリアル番号。 |
| **Uptime** | デバイスが起動してから、稼働している時間。 |
| **Device Role** | スキャン プロセス中に、検出された各デバイスに割り当てられているロール。デバイス ロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。Cisco DNA Center でデバイス ロールを特定できない場合、デバイス ロールは不明に設定されます。<br>（注） デバイス ロールを手動で変更すると、割り当ては静的のままになります。 Cisco DNA Center は、後続のデバイスの再同期中に変更が検知されたとしても、デバイス ロールは更新されません。<br>必要に応じて、このカラムのドロップダウン リストを使用して、割り当てられたデバイス ロールを変更することができます。次のデバイス ロールを使用できます。<br>• **Unknown**<br>• Access<br>• Core<br>• **Distribution**<br>• **Border Router** |
| **Site** | デバイスに割り当てられているサイト。デバイスがどのサイトにも割り当てられていない場合は、[Assign] をクリックします。[Choose a site] をクリックし、階層からサイトを選択して [Save] をクリックします。詳細については、ネットワーク階層についてを参照してください。 |
| **Last Updated** | Cisco DNA Center がデバイスをスキャンし、デバイスに関する新しい情報でデータベースを更新した最新の日付と時刻。 |
| **Device Family** | ルータ、スイッチ、ハブ、またはワイヤレスコントローラなどの関連するデバイスのグループ。 |
| **Device Series** | デバイスのシリーズ番号（たとえば、Cisco Catalyst 4500 シリーズスイッチ）。 |
| **Resync Interval** | デバイスのポーリング間隔。この間隔は、[Settings] でグローバルに設定するか、またはインベントリ内の特定のデバイスに対して設定できます。詳細については、「Cisco DNA Center 管理者ガイド」を参照してください。 |

| カラム | 説明 |
|---|---|
| **Last Sync Status** | デバイス最終検出のスキャン状態。<br>• [Managed]：デバイスは完全に管理された状態です。<br>• [Partial Collection Failure]：デバイスは部分的に収集された状態で、すべてのインベントリ情報は収集されていません。障害の追加情報を表示するには、[Information]（i）アイコンにマウスを合わせます。<br>• [Unreachable]：デバイスの接続問題のため、デバイスに到達できず、インベントリ情報は収集されませんでした。この状態は、定期的な収集が行われたときに発生します。<br>• [Wrong Credentials]：デバイスをインベントリに追加した後にデバイスのログイン情報が変更された場合、この状態が表示されます。<br>• [In Progress]：インベントリ収集が実行されています。 |

# ユーザー定義フィールドの管理

ユーザー定義フィールドは、Cisco DNA Center で作成して任意のデバイスに割り当てることができるカスタムラベルです。これらのラベルを使用すると、デバイスの詳細のページにデバイスのより多くの詳細情報を表示できます。ユーザー定義フィールドを表示するには、そのフィールドをデバイスに割り当て、それに値を追加する必要があります。

## ユーザー定義フィールドの作成

Cisco DNA Center では、ユーザー定義フィールドを作成し、任意のデバイスに割り当てることができます。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** [Actions] ドロップダウンリストから、**[Provision]** > **[Inventory]** > **[Manage User Defined Fields]** の順に選択します。

**ステップ 3** [Manage User Defined Fields] ダイアログボックスで、[Create New Field] をクリックします。

**ステップ 4** [Create New Field] ダイアログボックスで、[Field Name] フィールドと [Field Description] フィールドにユーザー定義フィールドの名前と説明を入力します。

（注） お客様の IP アドレスやお客様のデバイス名など、[Device Details] ページにまだ表示されていないデバイスの詳細をユーザー定義フィールドに追加できます。

**ステップ 5** [Save] をクリックします。

同様に、追加のユーザー定義フィールドを作成できます。ユーザー定義フィールドはテーブルに表示されます。

**ステップ 6** ユーザー定義フィールドを編集する場合は、対応する [Edit] アイコンをクリックして必要な変更を行い、[Save] をクリックします。

**ステップ 7** ユーザー定義フィールドを削除する場合は、対応する [delete] アイコンをクリックし、後続の警告メッセージで [Yes] をクリックします。

# デバイスへのユーザー定義フィールドの追加

**始める前に**

[Manage User Defined Fields] ページで少なくとも 1 つのユーザー定義フィールドを作成しておく必要があります。「ユーザー定義フィールドの作成 （9 ページ）」を参照してください

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** ユーザー定義フィールドを追加するデバイスの名前をクリックします。

**ステップ 3** 左側のペインで、[User Defined Fields] をクリックします。

**ステップ 4** [Add] をクリックします。

**ステップ 5** [Field Name] ドロップダウンリストでユーザー定義フィールドを選択し、[Value] フィールドにその値を入力します。

たとえば、お客様の IP アドレスのユーザー定義フィールドを作成した場合、[Field Name] ドロップダウンリストでそのフィールドを選択し、[Value] フィールドにお客様の IP アドレスを入力します。

**ステップ 6** デバイスからユーザー定義フィールドを削除する場合は、対応する [Delete] アイコンをクリックします。

**ステップ 7** [Save] をクリックします。

# インベントリからのトポロジマップの起動

[Inventory] ウィンドウから、検出されたデバイスのトポロジマップを起動できます。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します[Provision] > [Inventory] の順に選択します。

**ステップ 2** トグルボタン  を使用して、トポロジマップビューとインベントリビューを切り替えます。トポロジマップビューには、デバイスのトポロジとプロビジョニングステータスが表示されます。各ノードをクリックすると、デバイスの詳細が表示されます。トポロジマップの詳細については、「トポロジについて」を参照してください。

（注） トポロジマップビューを折りたたむには [Collapse all] を、展開するには [expand all] をクリックします。

# Cisco DNA Center インベントリ内のデバイスのタイプ

デバイスは、2 つの方法（検出されるか手動で追加される）のいずれかでインベントリに表示されます。Cisco DNA Center インベントリは、次のタイプのデバイスをサポートしています。

- **ネットワークデバイス**：サポート対象のネットワークデバイスには、シスコルータ、スイッチ、およびワイヤレスコントローラ（WLC）やアクセスポイント（AP）などのワイヤレスデバイスが含まれます。
- **計算デバイス**：サポート対象の計算デバイスには、Cisco Unified Computing System（UCS）、シスコ エンタープライズ ネットワーク機能仮想化インフラストラクチャ ソフトウェア（NFVIS）を実行しているデバイス、その他のデータセンターデバイスが含まれます。
- **Meraki ダッシュボード**：Cisco Meraki 製品を管理するためのシスコクラウド管理プラットフォームのダッシュボード。
- Firepower Management Center（FMC）：シスコのネットワーク セキュリティ ソリューションを管理するための Firepower Threat Defense（FTD）デバイスを介した完全かつ統合された管理を提供します。

サポート対象デバイスの完全なリストについては、「Cisco DNA Center Supported Devices」を参照してください。

# ネットワークデバイスの管理

## ネットワーク デバイスを追加

ネットワーク デバイスは、インベントリに手動で追加できます。

### 始める前に

ネットワークデバイスを設定していることを確認します。詳細については、「ディスカバリの前提条件」を参照してください。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** [Add Device] をクリックします。

**ステップ 3** [Type] ドロップダウン リストから、[Network Device] を選択します。

**ステップ 4** [Device IP / DNS Name] フィールドで、デバイスの IP アドレスまたは名前を入力します。

（注） デバイスで HSRP プロトコルを使用している場合は、仮想 IP アドレスではなく、プライマリ IP アドレスを入力する必要があります。

**ステップ 5** [CLI] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されているグローバル CLI クレデンシャルを使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能なグローバル CLI ログイン情報がない場合は、[Network Settings] > [Device Credentials] ページでグローバル CLI ログイン情報を作成します。「グローバル CLI クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *2 : CLI* クレデンシャル

| フィールド | 説明 |
|---|---|
| **Username** | ネットワーク内のデバイスの CLI にログインするために使用する名前。 |
| **Password** | ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。<br>セキュリティ上の理由から、確認のためにパスワードを再入力します。<br>（注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |
| **Enable Password** | CLI で高い権限レベルに移るために使用するパスワード。<br>セキュリティ上の理由から、有効なパスワードを再入力します。<br>（注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

**ステップ 6** [SNMP] 領域がまだ表示されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている SNMP グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能なグローバル SNMP ログイン情報がない場合は、[Network Settings] > [Device Credentials] ページでグローバル SNMP ログイン情報を作成します。「グローバル SNMPv2c クレデンシャルの設定」および「グローバル SNMPv3 クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次の手順を実行します。

**ステップ 7** [Version] ドロップダウンリストから、[V2C]（SNMP バージョン 2c）または [V3]（SNMP バージョン 3）を選択します。

[V2C] を選択した場合、次のフィールドを設定します。

表 *3 : SNMPv2c* のクレデンシャル

| フィールド | 説明 |
|---|---|
| **Read** | • [Name/Description]：追加している SNMPv2c 設定の名前または説明。<br>• [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。<br>（注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |
| **Write** | • [Name/Description]：追加している SNMPv2c 設定の名前または説明。<br>• [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。<br>（注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

[V3] を選択した場合、次のフィールドを設定します。

表 *4 : SNMPv3* のクレデンシャル

| フィールド | 説明 |
|---|---|
| **Name/Description** | 追加した SNMPv3 設定の名前または説明。 |
| **Username** | SNMPv3 設定に関連付けられている名前。 |
| **Mode** | SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。<br>• [noAuthNoPriv]：認証または暗号化を提供しません。<br>• [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。<br>• [AuthPriv]：認証と暗号化の両方を提供します。 |

| フィールド | 説明 |
|---|---|
| **Auth Type** | 使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。<br>• [SHA]：HMAC-SHA に基づく認証。<br>• [MD5]：HMAC-MD5 に基づく認証。 |
| **Auth Password** | SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。<br>（注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。<br>• パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |
| **Privacy Type** | プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。<br>• [AES128]：暗号化の CBC モード AES。<br>• [None]：プライバシー設定はありません。 |
| **Privacy Password** | AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。<br>（注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。<br>• パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

**ステップ 8** まだ展開されていない場合は [SNMP RETRIES AND TIMEOUT] エリアを展開し、次のフィールドを設定します。

表 *5 : SNMP* のプロパティ

| フィールド | 説明 |
|---|---|
| **Retries** | デバイスへ接続可能な試行回数。有効な値は 1 ～ 3 です。デフォルトは 3 です。 |
| **Timeout** | タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Cisco DNA Center が待機する秒数。有効な値は、5 秒間隔で 1 ～ 300 秒です。デフォルトは 5 秒です。 |

**ステップ 9** [HTTP(S)] 領域がまだ表示されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている HTTP（HTTPS）グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能なグローバル HTTP（HTTPS）ログイン情報がない場合は、[Network Settings] > [Device Credentials] ページでグローバル HTTP（HTTPS）ログイン情報を作成します。「HTTPS グローバルログイン情報の設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *6 : HTTP*（*S*）

| フィールド | 説明 |
|---|---|
| **Username** | ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用する名前。 |
| **Password** | ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用するパスワード。<br>セキュリティ上の理由から、確認のためにパスワードを再入力します。<br>（注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |
| **Port** | 必要な HTTP（HTTPS）ポート番号を指定します。 |

**ステップ 10** まだ展開されていない場合は **NETCONF** 領域を展開し、**ポート** フィールドを設定します。

NETCONF では、CLI プロトコルとして SSH を設定し、SSH クレデンシャルを定義することが必要です。

**ステップ 11** Cisco DNA Center とリモートデバイスとの通信を可能にするいずれかのネットワークプロトコルの [Protocol] オプションボタンを選択します。有効な値は **SSH2** または **Telnet** です。

**ステップ 12** （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

SNMP 書き込みログイン情報を除くすべてのログイン情報が検証されます。

**ステップ 13** [Add] をクリックします。

## ネットワーク デバイス クレデンシャルの更新

選択したネットワーク デバイスのディスカバリ クレデンシャルを更新することができます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

### 始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

この手順を実行するには、管理者（ROLE_ADMIN）またはポリシー管理者（ROLE_POLICY_ADMIN）権限、および適切な RBAC スコープが必要です。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** 更新するネットワーク デバイスを選択します。

**ステップ 3** **[Actions]** ドロップダウンリストから **[Inventory]** > **[Edit Device]** の順に選択します。

**ステップ 4** [Edit Device] ダイアログボックスで、[Type] ドロップダウンフィールドから [Network Device] を選択します（まだ選択していない場合）。

**ステップ 5** [CLI] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されているグローバル CLI クレデンシャルを使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な CLI グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル CLI クレデンシャルの設定」を参照してください。

b) [Edit device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *7: CLI* クレデンシャル

| フィールド | 説明 |
|---|---|
| **Username** | ネットワーク内のデバイスの CLI にログインするために使用する名前。 |
| **Password** | ネットワーク内のデバイスの CLI にログインするために使用されるパスワード。<br>セキュリティ上の理由から、確認のためにパスワードを再入力します。<br>パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

| フィールド | 説明 |
|---|---|
| **Enable Password** | CLI で高い権限レベルに移るために使用するパスワード。<br>セキュリティ上の理由から、有効なパスワードを再入力します。<br>パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

**ステップ 6** [SNMP] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている SNMP グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な SNMP グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル SNMPv2c ログイン情報の設定」および「グローバル SNMPv3 ログイン情報の設定」を参照してください。

b) [Edit device specific credential] オプションボタンをクリックし、次の手順を実行します。

**ステップ 7** [Version] ドロップダウンリストから、[V2C]（SNMP バージョン 2c）または [V3]（SNMP バージョン 3）を選択します。

[V2C] を選択した場合、次のフィールドを設定します。

表 *8 : SNMPv2c* のクレデンシャル

| フィールド | 説明 |
|---|---|
| **Read** | • [Name/Description]：追加している SNMPv2c 設定の名前または説明。<br>• [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。<br>（注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |
| **Write** | • [Name/Description]：追加している SNMPv2c 設定の名前または説明。<br>• [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。<br>（注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

[V3] を選択した場合、次のフィールドを設定します。

表 *9 : SNMPv3* のクレデンシャル

| フィールド | 説明 |
|---|---|
| **Name/Description** | 追加した SNMPv3 設定の名前または説明。 |
| **Username** | SNMPv3 設定に関連付けられている名前。 |
| **Mode** | SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。<br>• [noAuthNoPriv]：認証または暗号化を提供しません。<br>• [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。<br>• [AuthPriv]：認証と暗号化の両方を提供します。 |
| **Auth Type** | 使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。<br>• [SHA]：HMAC-SHA に基づく認証。<br>• [MD5]：HMAC-MD5 に基づく認証。 |
| **Auth Password** | SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。<br>（注） • 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。<br>• パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |
| **Privacy Type** | プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。<br>• [AES128]：暗号化の CBC モード AES。<br>• [None]：プライバシー設定はありません。 |

| フィールド | 説明 |
|---|---|
| **Privacy Password** | AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。<br>（注）<br>• 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。<br>• パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

**ステップ 8** まだ展開されていない場合は [SNMP RETRIES AND TIMEOUT] エリアを展開し、次のフィールドを設定します。

表 *10 : SNMP* のプロパティ

| フィールド | 説明 |
|---|---|
| **Retries** | デバイスへ接続可能な試行回数。有効な値は 1 ～ 3 です。デフォルトは 3 です。 |
| **Timeout** | タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Cisco DNA Center が待機する秒数。有効な値は、5 秒間隔で 1 ～ 300 秒です。デフォルトは 5 秒です。 |

**ステップ 9** [HTTP(S)] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている HTTP（HTTPS）グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な HTTP（HTTPS）グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「HTTPS グローバルログイン情報の設定」を参照してください。

b) [Edit device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *11 : HTTP*（*S*）

| フィールド | 説明 |
|---|---|
| **Username** | ネットワーク内のデバイスの HTTP（HTTPS）にログインするために使用する名前。 |

| フィールド | 説明 |
|---|---|
| **Password** | ネットワーク内のデバイスのHTTP（HTTPS）にログインするために使用するパスワード。<br>セキュリティ上の理由から、確認のためにパスワードを再入力します。<br>パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |
| **Port** | 必要なHTTP（HTTPS）ポート番号を指定します。 |

**ステップ10** まだ展開されていない場合は **NETCONF** 領域を展開し、**ポート** フィールドを設定します。

NETCONFでは、CLIプロトコルとしてSSHを設定し、SSHクレデンシャルを定義することが必要です。

**ステップ11** Cisco DNA Centerとリモートデバイスとの通信を可能にするいずれかのネットワークプロトコルの[Protocol]オプションボタンを選択します。有効な値は **SSH2** または **Telnet** です。

**ステップ12** （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Centerにより、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色のXマークが表示されます。

ログイン情報を更新する対象として複数のデバイスを選択した場合、[Validation] ボタンは無効になります。

**ステップ13** [更新（Update）] をクリックします。

## ネットワークデバイスのセキュリティフォーカス

Cisco DNA Centerのセキュリティフォーカスにより、デバイスでの信頼できるチェックの結果を表示できます。

使用しているシスコのデバイスが正規の製品であり、セキュリティ侵害を受けたり物理的に変更されたりしていないことを確認するために実行されるセキュリティチェックはわずかしかありません。

デバイスアイデンティティ検証の一環として、次のチェックが実行されます。

- セキュアな固有デバイス識別子（SUDI）証明書チェーンの検証。
- デバイスのSUDI証明書応答の署名検証。
- SUDI証明書による製品ID検証。
- SUDI証明書によるシリアル番号検証。

これらのチェックは、次の状況でトリガーされます。

- Cisco DNA Centerでインベントリが収集されるたび。

- デバイスの設定を変更するとき。
- デバイスでイメージをアップグレードするとき。

次の CLI コマンドを使用して、デバイスアイデンティティ検証チェックを実行します。

```
show platform sudi certificate sign nonce ${randomNonceValue}
```

## 整合性検証チェックの実行

この手順では、整合性検証チェックのステータスを確認する方法について説明します。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** [Inventory] ドロップダウンメニューから [Security] を選択します。

**ステップ 3** テーブルに示されているデバイスの詳細情報を確認します。

**ステップ 4** テーブルをカスタマイズするには、テーブルの端にある縦に並んだ 3 つのドットをクリックし、[Add] または [Delete] を選択します。
[Integrity Verification] 列に結果が表示されます。

**ステップ 5** デバイスの [Integrity Verification] 列にステータスとして [Failed] と表示されている場合は、情報アイコンをクリックして理由を表示します。

整合性検証のステータスは次のとおりです。

- [Passed]：デバイスの整合性検証に合格しました。
- [Failed]：デバイスの整合性検証に合格しませんでした。
- [Unverified]：検証を実行できませんでした。
- [Not Available]：このバージョンのデバイスまたはソフトウェアイメージが検証をサポートしていません。

# 計算デバイスの管理

## 計算デバイスの追加

計算デバイスは、インベントリに手動で追加できます。計算デバイスには、Cisco Unified Computing System（UCS）などのデバイス、Cisco Enterprise ネットワーク機能の仮想化インフラストラクチャ ソフトウェア（NFVIS）を実行しているデバイス、およびその他のデータセンター デバイスが含まれます。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Inventory]**。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** [Add Device] をクリックします。

**ステップ 3** [Type] ドロップダウン リストから、[Compute Device] を選択します。

**ステップ 4** [Device IP / DNS Name] フィールドで、デバイスの IP アドレスまたは名前を入力します。

**ステップ 5** [HTTP(S)] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている HTTP（HTTPS）グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な HTTP（HTTPS）グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「HTTPS グローバルログイン情報の設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *12 : HTTP*（*S*）

| フィールド | 説明 |
|---|---|
| **Username** | HTTPS 接続の認証に使用される名前。 |
| **Password** | HTTPS 接続の認証に使用されるパスワード。 |
| **Port** | HTTPS トラフィックに使用される TCP/UDP ポートの番号。デフォルトはポート番号 443（HTTPS の既知のポート）です。 |

**ステップ 6** [CLI] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されているグローバル CLI クレデンシャルを使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な CLI グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル CLI クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次のフィールドを設定します。

表 *13 : CLI* クレデンシャル

| フィールド | 説明 |
|---|---|
| **Username** | ネットワーク内のデバイスの CLI にログインするために使用する名前。 |

| フィールド | 説明 |
|---|---|
| **Password** | ネットワーク内のデバイスのCLIにログインするために使用されるパスワード。<br>セキュリティ上の理由から、確認のためにパスワードを再入力します。<br>パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |
| **Enable Password** | CLI で高い権限レベルに移るために使用するパスワード。<br>セキュリティ上の理由から、有効なパスワードを再入力します。<br>パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

**ステップ 7** [SNMP] 領域がまだ展開されていない場合は展開し、次のいずれかを実行します。

a) すでに作成されている SNMP グローバルログイン情報を使用する場合は、[Select global credential] オプションボタンをクリックします。

（注） 使用可能な SNMP グローバルログイン情報がない場合は、**[Network Settings]** > **[Device Credentials]** ページで作成します。「グローバル SNMPv2c クレデンシャルの設定」および「グローバル SNMPv3 クレデンシャルの設定」を参照してください。

b) [Add device specific credential] オプションボタンをクリックし、次の手順を実行します。

**ステップ 8** [Version] ドロップダウンリストから、[V2C]（SNMP バージョン 2c）または [V3]（SNMP バージョン 3）を選択します。

[V2C] を選択した場合、次のフィールドを設定します。

表 *14 : SNMPv2c* のクレデンシャル

| フィールド | 説明 |
|---|---|
| **Read** | • [Name/Description]：追加している SNMPv2c 設定の名前または説明。<br>• [Read Community]：デバイスに SNMP 情報を表示する目的のみに使用される読み取り専用のコミュニティ文字列パスワード。<br>（注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |
| **Write** | • [Name/Description]：追加している SNMPv2c 設定の名前または説明。<br>• [Write Community]：デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティ文字列。<br>（注） パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

[V3] を選択した場合、次のフィールドを設定します。

表 *15 : SNMPv3* のクレデンシャル

| フィールド | 説明 |
|---|---|
| **Name/Description** | 追加した SNMPv3 設定の名前または説明。 |
| **Username** | SNMPv3 設定に関連付けられている名前。 |
| **Mode** | SNMP メッセージを必要とするセキュリティ レベル。次のいずれかのモードを選択します。<br>• [noAuthNoPriv]：認証または暗号化を提供しません。<br>• [AuthNoPriv]：認証を提供しますが、暗号化は提供しません。<br>• [AuthPriv]：認証と暗号化の両方を提供します。 |
| **Auth Type** | 使用する認証タイプ（認証モードとして [AuthPriv] または [AuthNoPriv] を選択した場合に有効になります）。次のいずれかの認証タイプを選択します。<br>• [SHA]：HMAC-SHA に基づく認証。<br>• [MD5]：HMAC-MD5 に基づく認証。 |
| **Auth Password** | SNMPv3 を使用するデバイスから情報にアクセスする際に使用する SNMPv3 パスワード。これらのパスワード（またはパスフレーズ）は、8 文字以上にする必要があります。<br>（注）<br>• 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。<br>• パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |
| **Privacy Type** | プライバシー タイプ。（認証モードとして [AuthPriv] を選択すると有効になります）。次のいずれかのプライバシー タイプを選択します。<br>• [AES128]：暗号化の CBC モード AES。<br>• [None]：プライバシー設定はありません。 |

| フィールド | 説明 |
|---|---|
| **Privacy Password** | AES128 暗号化をサポートしているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。<br>（注）<br>• 一部のシスコ ワイヤレス コントローラでは、パスワード（あるいはパスフレーズ）は少なくとも 12 文字以上である必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。<br>• パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。 |

**ステップ 9** （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

SNMP 書き込みログイン情報を除くすべてのログイン情報が検証されます。

**ステップ 10** [Add] をクリックします。

## 計算デバイス クレデンシャルの更新

選択した計算デバイスのディスカバリ クレデンシャルを更新することができます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

### 始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** 更新するデバイスを選択します。

**ステップ 3** [Actions] ドロップダウンリストから **[Inventory]** > **[Edit Device]** の順に選択します。

**ステップ 4** [Edit Device] ダイアログボックスの [Type] ドロップダウンリストで、[Compute Device] を選択します。

**ステップ 5** まだ展開されていない場合は、[HTTP（S）] エリアを展開します。

**ステップ 6** [Username] および [Password] フィールドに、ユーザー名とパスワードを入力します。

**ステップ 7** [Port] フィールドにポート番号を入力します。

**ステップ 8** （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイス ログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ログイン情報を更新する対象として複数のデバイスを選択した場合、[Validation] ボタンは無効になります。

**ステップ 9** [更新（Update）] をクリックします。

# Meraki ダッシュ ボードの管理

## Meraki ダッシュボードの統合

Meraki ダッシュボードと Cisco DNA Center を統合できます。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** [Add Device] をクリックします。

**ステップ 3** [デバイスの追加（Add Device）] ダイアログボックスの [タイプ（Type）] ドロップダウンリストで、[Meraki ダッシュボード（Meraki Dashboard）] を選択します。

**ステップ 4** まだ展開されていない場合は、[HTTP（S）] エリアを展開します。

**ステップ 5** [API Key/Password] フィールドで、API キーとパスワードのログイン情報を入力し、[Get Organization details] リンクをクリックします。

**ステップ 6** [Organization] ドロップダウンリストから組織のオプションを選択するか、組織名を検索します。

**ステップ 7** （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイス ログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

**ステップ 8** [Add] をクリックします。

選択した組織のみで Cisco Meraki ダッシュボードとデバイスの収集が開始されます。

## Meraki ダッシュボード クレデンシャルの更新

選択したデバイスの Meraki ダッシュボードログイン情報を更新することができます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** 更新するデバイスを選択します。

**ステップ 3** [Actions] ドロップダウンリストから **[Inventory]** > **[Edit Device]** の順に選択します。

**ステップ 4** [Edit Device] ダイアログボックスの [Type] ドロップダウンリストから、[Meraki Dashboard] を選択します。

**ステップ 5** まだ展開されていない場合は、[HTTP（S）] エリアを展開します。

**ステップ 6** [API Key / Password] フィールドで、Meraki ダッシュボードへのアクセスに使用する API キーとパスワードのクレデンシャルを入力します。

**ステップ 7** [Port] フィールドにポート番号を入力します。

**ステップ 8** （オプション）[Credentials] の横にある [Validate] をクリックします。Cisco DNA Center により、デバイスログイン情報が検証され、有効なログイン情報には緑色のチェックマーク、無効なログイン情報には赤色の X マークが表示されます。

ログイン情報を更新する対象として複数のデバイスを選択した場合、[Validation] ボタンは無効になります。

**ステップ 9** [更新（Update）] をクリックします。

# Firepower Management Center の管理

## Firepower Management Center の統合

Firepower Management Center（FMC）を Cisco DNA Center と統合できます。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]** の順に選択します。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** [Add Device] をクリックします。

**ステップ 3** [Add Device] ダイアログボックスの [Type] ドロップダウンリストで、[Firepower Management Center] を選択します。

**ステップ 4** [Device IP / DNS Name] フィールドで、デバイスの IP アドレスまたは名前を入力します。

**ステップ 5** [HTTP(S)] エリアを展開します（まだ展開していない場合）。

[Add device specific credential] オプションボタンは、デフォルトで選択されています。

**ステップ 6** 次の情報を入力します。

a) [Username]：HTTPS 接続の認証に使用される名前です。
b) [Password]：HTTPS 接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
c) [Port]：HTTPS トラフィックで使用される TCP/UDP ポートの番号です。デフォルトのポート番号は 443 です。

**ステップ 7** [Add] をクリックします。

（注） インベントリに FMC を追加すると、FMC によって管理される Firepower Threat Defense（FTD）デバイスもインベントリに自動的に追加されます。

## Firepower Management Center のログイン情報の更新

Cisco DNA Center では Firepower Management Center（FMC）のログイン情報を更新できます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

### 始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** 更新する FMC デバイスを選択します。

（注） FMC によって管理されている Firepower Threat Defense（FTD）デバイスを更新、編集、または削除することはできません。インベントリ内の FMC を介して FTD デバイスを管理する必要があります。

**ステップ 3** **[Actions]** ドロップダウンリストから **[Inventory]** > **[Edit Device]** の順に選択します。

[Edit Device] ダイアログボックスが表示されます。

**ステップ 4** [Credentials] をクリックします。

**ステップ 5** [HTTP(S)] エリアを展開します（まだ展開していない場合）。

[Add device specific credential] オプションボタンは、デフォルトで選択されています。

**ステップ 6** 次の情報を入力します。

a) [Username]：HTTPS 接続の認証に使用される名前です。

b) [Password]：HTTPS接続の認証に使用されるパスワードです。パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

c) [Port]：HTTPS トラフィックで使用される TCP/UDP ポートの番号です。デフォルトのポート番号は 443 です。

**ステップ 7** [Management IP] をクリックし、[Device IP/DNS Name] フィールドにデバイスの IP アドレスまたは名前を入力します。

**ステップ 8** [Resync Interval] をクリックし、再同期間隔タイプを選択します。

- [Custom]：再同期間隔を分単位で入力できます。有効な範囲は 25 ～ 1,440 分（24 時間）です。
- [Global]：デフォルトでは、再同期間隔は 1,440 分（24 時間）に設定されます。
- [Disable]：再同期間隔が無効になるかゼロに設定されます。

**ステップ 9** [Role] をクリックし、[Device Role] ドロップダウンリストからロールを選択します。

**ステップ 10** [更新（Update）] をクリックします。

# デバイスのフィルタ

（注） フィルタを削除または変更するには、[リセット（Reset）] をクリックします。

**始める前に**

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** [Filter] をクリックします。

次のタイプのフィルタを使用できます。

- クイック フィルタ
- 拡張フィルタ
- 最近のフィルタ

[Quick Filter]：このフィルタでは、次の項目に基づいてデバイスの詳細を取得できます。

- **Device Family**
- **Device Role**

- **Last Sync Status**
- **Provision Status**
- **Credential Status**
- **OS Updated Status**
- **Image Needs Update**
- **Image Pre Check Status**
- **Support Type**

[Advanced Filters]：このフィルタでは、[Contains]、[Starts With]、[Ends With]、[Equals]、[Does not contains] などの演算子と正規表現を使用してフィルタ基準を設定し、その条件に基づいてデバイスの詳細を絞り込むことができます。たとえば、ドロップダウンリストからフィルタパターン（テーブル列名ごと）と演算子を選択できます。さらに、使用可能なデータに基づいてフィルタ基準の値を入力する必要があります。

[Recent Filters]：このフィルタでは、最近使用したフィルタが表示されます。フィルタ基準を保存するには、[RECENT] から [SAVED] にフィルタをドラッグアンドドロップします。

**ステップ 3** 選択したフィルタのフィールドに適切な値を入力します。たとえば、[Device Name] フィルタであれば、デバイスの名前を入力します。

Cisco DNA Center その他のフィールドに値を入力すると、オートコンプリート値が提示されます。推奨されるいずれかの値を選択するか、または値の入力を終了します。

これらのフィルタにワイルドカード（アスタリスク）を使用することもできます。たとえば、文字列値の先頭、末尾、または中間にアスタリスクがある値を入力できます。その後、Enter を押します。

**ステップ 4** [Apply] をクリックして情報をフィルタします。

[Devices] テーブルに表示されるデータは、フィルタ選択に従って自動的に更新されます。

（注） フィルタごとに複数のフィルタ タイプと複数の値を使用できます。

**ステップ 5** （オプション）必要に応じて、フィルタを追加します。

フィルタを削除するには、対応するフィルタ値の横にある [x] アイコンをクリックします。

# インベントリ内のデバイスの管理

ここでは、[Inventory] ウィンドウを使用して、サイトにデバイスを割り当て、デバイスタグを管理する方法について説明します。

# デバイスをサイトに追加する

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックし、**[Provision]** > **[Inventory]** の順に選択します。
[Inventory] ウィンドウには、**ディスカバリ**プロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** サイトに割り当て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 3** [Actions] メニューから、**[Provision]** > **[Assign Device to Site]** を選択します。
[Assign Device to Site] スライドインペインが表示されます。

**ステップ 4** [Assign Device To Site] スライドインペインで、デバイスの  アイコンの横にあるリンクをクリックします。
[Choose a floor] スライドイン ペインが表示されます。

**ステップ 5** [Choose a floor] スライドインペインで、デバイスに割り当てるフロアを選択します。

**ステップ 6** [Save] をクリックします。

**ステップ 7** （任意） 複数のデバイスを選択して同じ場所に追加した場合は、最初のデバイスで [Apply to All] チェックボックスをオンにすると、残りのデバイスに同じ場所を割り当てることができます。

**ステップ 8** [**Assign**] をクリックします。

**ステップ 9** サイトにデバイスを割り当てるときにデバイスの可制御性が有効になっていると、ワークフローが自動的にトリガーされ、サイトからデバイスにデバイス設定がプッシュされます。
[Focus] ドロップダウンリストから [Provision] を選択し、[Provision Status] 列の [See Details] をクリックします。デバイスの可制御性を有効にしている場合、デバイスにプッシュされる設定が別のウィンドウに表示されます。

# デバイスのタグ付け

デバイス タグは属性またはルールに基づいてデバイスをグループ化することができます。単一のデバイスに複数のタグを設定できます。同様に、複数のデバイスに適用できる単一のタグもあります。

[プロビジョン（Provision）]ウィンドウのデバイスに対してタグを追加したり、削除できます。

**ステップ 1** Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、[Provision] を選択します。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** タグを適用するデバイスの横にあるチェックボックスをオンにして、[Tag Device] をクリックします。

**ステップ 3** [タグ名（Tag Name）] フィールドにタグ名を入力します。

- 新しいタグを作成している場合は、[ 新規タグの作成（Create New Tag） ] をクリックします。ルールを使用して新規タグを作成することもできます。詳細については、「ルールを使用してデバイスにタグ付けする （32 ページ）」を参照してください。
- 既存のタグを使用する場合は、一覧からタグを選択して、[Apply] をクリックします。

タグを適用するデバイス名の下に、タグ アイコンとタグ名が表示されます。

**ステップ 4** デバイスからタグを削除するには、以下のいずれか 1 つを行います。

- Click **Create New Tag**, unselect all tags, and then click **APply**.
- タグアイコンまたはタグ名にカーソルを合わせて、[X] をクリックし、デバイスからタグの関連付けを解除します。

# ルールを使用してデバイスにタグ付けする

ルールを定義するタグに基づいてデバイスをグループ化することができます。ルールを定義するとき、Cisco DNA Center は指定したルールと一致するすべてのデバイスにタグを適用します。ルールはデバイス名、デバイスファミリ、デバイスシリーズ、IP アドレス、ロケーション、またはバージョンに基づくことができます。

**ステップ 1** Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、[Provision] を選択します。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** タグを適用するデバイスの隣のチェックボックスをオンにして、**[ デバイスのタグ付け（Tag Device） ]** をクリックします。

**ステップ 3** [ タグ名（Tag Name） ] フィールドにタグ名を入力し、[ ルールによる新規タグの作成（Create New Tag with Rule） ] をクリックします。

[ 新規 VRF の作成（Create New VRF） ] ウィンドウが表示されます。

[ タグ付きデバイスの合計数（Total Devices Tagged Count） ] の下の [ 手動で追加（Manually Added） ] フィールドは、ステップ 2 で選択されたデバイスの合計数を示します。

**ステップ 4** [ 条件の追加（Add Condition） ] をクリックして、ルールに必要なフィールドに記入します。

[ 一致するデバイス（Matching Devices） ] の数は、この条件に一致するデバイスの数に応じて、自動的に変更されます。

追加条件を作成するためには、次の 2 つのオプションがあります。

- *And* 条件— [ 条件の追加（Add Condition） ] リンクをクリックします。**And** が条件の上に表示されます。
- *Or* 条件—既存の条件の隣の追加アイコン (+) をクリックします。**Or** は条件の隣に表示されます。

必要に応じていくつでも条件を追加できます。ルールを変更すると、指定したルールに一致するインベントリのデバイス数を反映して一致するデバイス数が変更されます。デバイス数でクリックして、ルールと一致するデバイスを表示できます。

**ステップ 5** [ 保存（Save） ] をクリックして、定義されたルールと共にタグを保存します。

タグを適用するデバイス名の下に、タグ アイコンとタグ名が表示されます。

デバイスがインベントリに追加されると、定義したruleと一致する場合、タグは自動的にデバイスに適用されます。

# デバイスタグの編集

以前に作成したデバイスタグを編集できます。

**ステップ 1** Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、[Provision] を選択します。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

[ デバイス名（Device Name） ] 列のデバイス名の下に以前に作成したデバイスタグがありある場合はそれがリスト表示されます。

**ステップ 2** デバイスを選択しないで、 [ デバイスのタグ付け（Tag Device） ] をクリックします。

以前に作成されたタグがリストされます。

**ステップ 3** 編集するタグをマウスオーバーして、タグ名の隣の鉛筆アイコンをクリックします。

代わりに、**[Tag Device]** > **[View All Tags]** の順に選択してから、編集するタグの横にある鉛筆アイコンをクリックすることもできます。

**ステップ 4** タグを変更し、 [ 保存（Save） ] をクリックして変更を保存します。

# タグの削除

デバイスタグまたはテンプレートタグは、デバイスまたはテンプレートに関連付けられていない場合にのみ削除できます。

### 始める前に

デバイスに（ルールを使用して）静的または動的に関連付けられているタグを削除します。

テンプレートに関連付けられているタグを削除します。

**ステップ 1** Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、[Provision] を選択します。

デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** デバイスを選択しないで、**[Tag Device]** > **[Manage Tags]** の順に選択します。

**ステップ 3** 削除するタグにマウスカーソルを合わせてから、タグ名の横にある削除アイコンをクリックします。

**ステップ 4** 警告メッセージが表示されたら、[Yes] をクリックします。

タグがデバイスまたはテンプレートに関連付けられている場合は、エラーメッセージが生成されます。デバイスまたはテンプレートに関連付けられているタグを除去し、タグを削除します。

# インベントリインサイト

[Inventory Insights] ウィンドウには、他の直接接続されたデバイスと設定が一致しないデバイスが表示されます。また、Cisco DNA Center のベストプラクティスの推奨事項と比較して、誤って設定されたデバイスも表示されます。Cisco DNA Center では、次のインサイトと推奨されるアクションが提供されます。

- 速度/デュプレックス設定の不一致
- VLAN の不一致

## 速度/デュプレックス設定の不一致

Cisco DNA Center には、相互に接続されているが、デバイスリンクの両端で異なる速度とデュプレックス値が設定されているデバイスが表示されます。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** [Focus] ドロップダウンリストから [Inventory Insights] を選択します。

[Inventory Insights] ウィンドウが表示されます。

**ステップ 3** [Speed/Duplex settings mismatch] をクリックして、デバイスで実行できる推奨アクションを確認します。

推奨アクションが右側のペインに表示されます。

**ステップ 4** インスタンスの番号をクリックして、不一致を確認します。

[Speed/Duplex settings mismatch] ウィンドウでは、速度とデュプレックスの不一致が強調表示されます。

**ステップ 5** 推奨アクションに従って、デバイス設定に必要な変更を加えます。

## VLAN の不一致

Cisco DNA Center には、相互に接続されているが、デバイスリンクの両端で異なる VLAN が設定されているデバイスが表示されます。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** [Focus] ドロップダウンリストから [Inventory Insights] を選択します。

[Inventory Insights] ウィンドウが表示されます。

**ステップ 3** [VLAN Mismatch] をクリックして、デバイスで実行できる推奨アクションを確認します。

推奨アクションが右側のペインに表示されます。

**ステップ 4** インスタンスの番号をクリックして、不一致を確認します。

[VLAN Mismatch] ウィンドウに、許可された VLAN とネイティブ VLAN の不一致が強調表示されます。

**ステップ 5** 推奨アクションに従って、デバイス設定に必要な変更を加えます。

# デバイスのロールの変更（インベントリ）

ディスカバリ プロセスに、Cisco DNA Center は検出された各デバイスにロールを割り当てます。デバイスのロールは、デバイスを特定してグループ化するためと、トポロジツールでネットワーク トポロジ マップのデバイスの配置を決定するために使用されます。最上位の層は、インターネットです。最下層のデバイスは、次のロールのいずれかに割り当てられます。

**表 *16*：デバイスのロールとトポロジの位置**

| トポロジの位置 | デバイス ロール |
|---|---|
| 階層 1 | インターネット（設定不可） |
| 階層 2 | [Border Router] |
| 階層 3 | コア |
| 階層 4 | Distribution |
| 階層 5 | アクセス |
| 階層 6 | 不明（Unknown） |

（注） **アクセス**ロールをデバイスに割り当てると、IP デバイストラッキング（IPDT）が設定されるか、サイトの IPDT 設定に基づいてデバイスから削除されます。

**始める前に**

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** Locate the device whose role you want to change, click the pencil icon under the **Device Role** column, and choose a role from the **Update Device Role** dialog box. 有効な選択肢は、[Unknown] 、[Access] 、[Core] 、[Distribution] 、または [Border Router] です。

デバイスロールは次の手順で、[Edit Device] ダイアログボックスでも更新できます。

- ロールを変更するデバイスを選択します。
- **[Actions]** > **[Inventory]** > **[Edit Device]** の順に選択します。
- **[Role]** タブをクリックし、**[Device Role]** ドロップダウンリストから適切なロールを選択します。

（注） デバイス ロールを手動で変更すると、割り当ては静的のままになります。 Cisco DNA Center は、後続のデバイスの再同期中に変更が検知されたとしても、デバイス ロールは更新されません。

# デバイスの管理 IP アドレスの更新

デバイスの管理 IP アドレスを更新することができます。

（注） 複数のデバイスを同時に更新することはできません。また、Meraki デバイスの管理 IP アドレスは更新できません。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** 更新するデバイスを選択します。

**ステップ 3** **[Actions]** ドロップダウンリストから **[Inventory]** > **[Edit Device]** の順に選択します。

[Edit Device] ダイアログボックスが表示されます。

**ステップ 4** **[Management IP]** タブをクリックし、**[Device IP/DNS Name]** フィールドに新しい管理 IP アドレスを入力します。

（注） 新しい管理 IP アドレスが Cisco DNA Center から到達可能であり、デバイス クレデンシャルが正しいことを確認します。そうでない場合、デバイスが管理対象外状態になる可能性があります。

### 次のタスク

デバイスを再プロビジョニングして、送信元インターフェイスの設定を更新します。

# デバイスポーリング間隔の更新

**[System]** > **[Settings]** > **[Network Resync Interval]** の順に選択すると、グローバルレベルですべてのデバイスのポーリング間隔を更新できます。また、[Device Inventory] を選択すると、デバイスレベルで特定のデバイスのポーリング間隔を更新できます。[Network Resync Interval] を使用してポーリング間隔を設定すると、その値が [Device Inventory] ポーリング間隔値よりも優先されます。

デバイスにポーリングさせない場合は、ポーリングを無効にできます。

### 始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

**ステップ 2** 更新するデバイスを選択します。

**ステップ 3** [Update Polling Interval] をクリックします

**ステップ 4** [Update Resync Interval] ダイアログボックスの [Status] フィールドで、[Enabled] をクリックしてポーリングを有効にするか、[Disabled] をクリックしてポーリングを無効にします。

**ステップ 5** [Polling Time] フィールドには、継続的なポーリングサイクルの間隔（分単位）を入力します。有効な値は、25 ～ 1,440 分（24 時間）です。

（注） デバイス固有のポーリング時間は、グローバルなポーリング時間より優先されます。デバイス固有のポーリング時間を設定した後でグローバルなポーリング時間を変更した場合、Cisco DNA Center は引き続きデバイス固有のポーリング時間を使用します。

**ステップ 6** [更新（Update）] をクリックします。

# デバイス情報の再同期

選択したデバイスのデバイス情報は、再同期間隔の構成にかかわらず、ただちに再同期できます。同時に最大 40 台のデバイスを再同期することができます。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** 関連する情報を収集するデバイスを選択します。

**ステップ 3** [Actions] ドロップダウンリストから [Inventory] > [Resync Device] の順に選択します。 >

**ステップ 4** [OK] をクリックします。

# ネットワーク デバイスの削除

デバイスがまだサイトに追加されていない場合に限り、Cisco DNA Center データベースからデバイスを削除できます。

インベントリからワイヤレスセンサーを削除すると、センサーは工場出荷時のデフォルト状態にリセットされるため、再接続すると現在の構成が採用されます。

### 始める前に

この手順を実行するには、管理者（ROLE_ADMIN）権限、およびすべてのデバイスへのアクセス権（[RBAC Scope] を [ALL] に設定）が必要です。

**ステップ 1** [Provision]Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します > [Inventory] の順に選択します。
[Inventory] ウィンドウには、**ディスカバリ**プロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** 削除するデバイスの横にあるチェックボックスをオンにします。

（注） さらにチェック ボックスをオンにして複数のデバイスを選択できますが、リストの上部にあるチェック ボックスをクリックしてすべてのデバイスを選択できます。

**ステップ 3** [Actions] ドロップダウンリストから [Inventory] > [Delete Device] > の順に選択します。

**ステップ 4** [Warning] ウィンドウで、[Config Clean-Up] チェックボックスをオンにして、選択したデバイスからネットワーク設定およびテレメトリ設定を削除します。

**ステップ 5** [OK] をクリックして、アクションを確認します。

# コマンド ランナーを起動（インベントリ）

[Inventory] ウィンドウで選択したデバイスのコマンド ランナー アプリケーションを起動できます。

### 始める前に

コマンド ランナー アプリケーションをインストールします。詳細については、Cisco DNA Center 管理者ガイドを参照してください。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** コマンドを実行するデバイスを選択します。

**ステップ 3** [Actions] ドロップダウンリストから、**[Others]** > **[Launch Command Runner]** の順に選択します。

実行可能なコマンドの詳細、およびこれらのコマンドの実行方法については、デバイスの診断コマンドを実行を参照してください。

# Run コマンドを使用したデバイスの到達可能性の問題のトラブルシューティング

[Inventory] ウィンドウから [Run Commands] ウィンドウを起動し、ping、traceroute、snmpget などのプラットフォームコマンドを実行して、デバイス到達可能性の問題をトラブルシューティングできます。

（注） Cisco DNA Center クラスタでプラットフォームコマンドを直接実行する場合は、[Run Commands] を起動する前にデバイスを選択しないでください。そうしないと、プラットフォームではなくそのデバイスに対してコマンドが実行されます。

### 始める前に

コマンド ランナー アプリケーションをインストールします。詳細については、Cisco DNA Center 管理者ガイドを参照してください。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

**ステップ 2** [Actions] ドロップダウンリストから、**[Others]** > **[Run Commands]** の順に選択します。

**man** を入力すると、現在サポートされているコマンドおよびショートカットのリストをいつでも取得できます。

# CSVファイルを使用したデバイス設定のインポート/エクスポート

### CSV ファイルのインポート

CSV ファイルを使用して、別のソースから Cisco DNA Center にデバイスの設定やサイトをインポートできます。サンプルテンプレートをダウンロードする場合は、[Provision Devices] ページに移動し、**[Actions]** > **[Inventory]** > **[Import Inventory]** を選択します。[Download Template] をクリックして、サンプル CSV ファイルテンプレートをダウンロードします。

CSV ファイルを使用してデバイスまたはサイト設定をインポートする場合、Cisco DNA Center がデバイスをどれだけ管理できるのかはCSV ファイルに指定する情報に依存します。CLI ユーザー名、パスワード、およびイネーブルパスワードの値を指定しない場合、Cisco DNA Center の機能が制限され、デバイス設定の変更、デバイス ソフトウェア イメージの更新、および他の重要な機能の実行ができません。

CSV ファイルでクレデンシャル プロファイルを指定し、対応するクレデンシャルをデバイスのセットに適用できます。クレデンシャル プロファイルを指定して、CSV ファイルに手動で値も入力する場合、手動入力されたクレデンシャルが優先され、デバイスは手動入力されたクレデンシャルとクレデンシャル プロファイルの組み合わせに基づいて管理されます。たとえば、手動で入力した SNMP ログイン情報に加えて、SNMP および SSH または Telnet のログイン情報を含むログイン情報プロファイルが CSV ファイルに含まれている場合、デバイスは手動で入力された SNMP ログイン情報とログイン情報プロファイル内の SSH または Telnet ログイン情報に基づいて管理されます。Telnet は非推奨です。

（注） また、指定したプロトコルに対応するフィールドにも値を入力する必要があります。たとえば、SNMPv3 を指定した場合、SNMPv3 のユーザー名や認証パスワードなど、サンプルの CSV ファイルの SNMPV3 フィールドに値を指定する必要があります。

Cisco DNA Center の部分的なインベントリ収集の場合は、CSV ファイルに次の値を指定する必要があります。

- デバイスの IP アドレス

- SNMP バージョン
- SNMP 読み取り専用コミュニティ ストリング
- SNMP 書き込みコミュニティ ストリング
- SNMP 再試行値
- SNMP タイムアウト値

Cisco DNA Center の完全なインベントリ収集では、CSV ファイルに以下の値を提供する必要があります。

- デバイスの IP アドレス
- SNMP バージョン
- SNMP 読み取り専用コミュニティ ストリング
- SNMP 書き込みコミュニティ ストリング
- SNMP 再試行値
- SNMP タイムアウト値
- Protocol
- CLI ユーザー名
- CLI パスワード
- CLI イネーブル パスワード
- CLI タイムアウト値

### CSV ファイル エクスポート

Cisco DNA Center では、すべてまたは選択したデバイスを含む CSV ファイルをインベントリに作成できます。このファイルを作成するには、ファイルに含まれる設定データを保護するパスワードを入力する必要があります。

# CSV ファイルからのデバイス設定のインポート

CSV ファイルからデバイス設定をインポートできます。

**ステップ 1** [Provision] > [Devices] > [Inventory]。Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します> >

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** [Actions] ドロップダウンリストから、[Inventory] > [Import Inventory] > を選択してデバイスのログイン情報をインポートします。

**ステップ 3** [Bulk Import] ダイアログボックスのボックスエリアに CSV ファイルをドラッグアンドドロップするか、点線のボックスエリアをクリックして CSV ファイルを参照します。

**ステップ 4** **[Import]** をクリックします。

# デバイスデータのエクスポート

選択したデバイスに関する特定のデータを CSV ファイルにエクスポートできます。CSV ファイルは圧縮されます。[Export] をクリックして、フィルタ処理されたデバイスまたはすべてのデバイスのデータをエクスポートします。

⚠

**注意** CSV ファイルにはエクスポートされたデバイスに関する機密情報が含まれているため、取り扱いには注意してください。特別な権限を持つユーザーのみがデバイスのエクスポートを行うことを確認します。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

インベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** 特定のデバイスのみの構成情報をエクスポートするには、含めるデバイスの横にあるチェックボックスをオンにします。すべてのデバイスを含めるには、デバイスリストの最上部にあるチェックボックスをオンにします。

**ステップ 3** [Actions] ドロップダウンリストから、[Inventory] > [Export Inventory] > を選択してデバイス設定をエクスポートします。

[Export Inventory] ダイアログボックスが表示されます。

**ステップ 4** **[パスワード（Password）]** フィールドに、エクスポートされた CSV ファイルを暗号化するために使用するパスワードを入力します。

（注） エクスポートしたファイルを開くには、パスワードが必要です。

**ステップ 5** 確認のために暗号化パスワードをもう一度入力します。

**ステップ 6** [Include SSH key information] チェックボックスをオンにして、最初の SSH 鍵、最初の SSH 鍵アルゴリズム、現在の SSH 鍵、現在の SSH 鍵アルゴリズムなどの情報をエクスポートした CSV ファイルに追加します。

**ステップ 7** [Export] をクリックします。

（注） ブラウザの設定によっては、圧縮したファイルを保存したり、開くことができます。

# デバイスのクレデンシャルのエクスポート

デバイスのクレデンシャル CSV ファイルにエクスポートできます。不要なアクセスからファイルを保護するために、パスワードを設定する必要があります。ファイルを開くことができるように、受信者にパスワードを提供する必要があります。

⚠

**注意** CSV ファイルにはエクスポートされたデバイスのすべてのクレデンシャルがリストされているため、取り扱いには注意してください。特別な権限を持つユーザーのみがデバイスのエクスポートを行うことを確認します。

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** CSV ファイルに含めるデバイスの横にあるチェックボックスをオンにします。すべてのデバイスを含めるには、リストの最上部にあるチェックボックスをオンにします。

**ステップ 3** [Actions] ドロップダウンリストから **[Inventory]** > **[Export Inventory]** を選択します。

[Export] ダイアログボックスが表示されます。

**ステップ 4** [Select Export Type] で、[Credentials] オプションボタンをクリックします。

**ステップ 5** [Include SSH key information] チェックボックスをオンにして、最初の SSH 鍵、最初の SSH 鍵アルゴリズム、現在の SSH 鍵、現在の SSH 鍵アルゴリズムなどの情報をエクスポートした CSV ファイルに追加します。

**ステップ 6** **[パスワード（Password）]** フィールドに、エクスポートされた CSV ファイルを暗号化するために使用するパスワードを入力します。

（注） エクスポートしたファイルを開くには、パスワードが必要です。

**ステップ 7** 暗号化パスワードを確認し、[エクスポート（Export）] をクリックします。

（注） ブラウザの設定によっては、圧縮したファイルを保存したり、開くことができます。

# 故障したデバイスの交換

ネットワーク内で障害が発生したデバイスを交換することは、デバイスのライフサイクル管理の重要な部分です。Cisco DNA Center の返品許可（RMA）ワークフローにより、障害が発生したデバイスを迅速に交換する手順を容易に自動化できるため、生産性が向上し、運用コストが減少します。RMA では、ルータ、スイッチ、および AP を共通のワークフローに従って交換できます。

ルータおよびスイッチで RMA ワークフローを使用すると、ソフトウェアイメージ、構成、およびライセンスが、障害が発生したデバイスから交換用デバイスに復元されます。ワイヤレス AP の場合、交換用デバイスは同じサイトに割り当てられ、プライマリワイヤレス LAN コントローラ、RF プロファイル、および AP グループ設定でプロビジョニングされ、障害が発生した AP と同じ Cisco DNA Center のフロアマップの場所に配置されます。

### 始める前に

- 故障したデバイスのソフトウェア イメージ バージョンをイメージリポジトリにインポートしてから、交換するデバイスにマークを付ける必要があります。
- 故障したデバイスは到達不能な状態になっている必要があります。
- 交換用デバイスがプラグアンドプレイ（PnP）で Cisco DNA Center をオンボードしている場合は、故障したデバイスをユーザー定義のサイトに割り当てる必要があります。
- RMA ワークフローのトリガー中は、交換用デバイスがプロビジョニング状態であってはなりません。

---

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ウィンドウには、検出プロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** 交換する故障したデバイスを選択します。

（注） RMA は、障害のある SMU およびパッケージの交換をサポートします。

**ステップ 3** [Actions] ドロップダウンリストから、**[Inventory]** > **[Device Replacement]** > **[Mark Device for Replacement]** を選択します。

**ステップ 4** [Mark For Replacement] ウィンドウで、[Mark] をクリックします。

（注） ファブリックデバイスのシームレスな交換を実現するために、DHCP サーバーがネイバーデバイスで設定されます。これは IP アドレスを割り当てるために必要であり、障害のあるデバイスが正常に交換されると除外されます。

障害のあるデバイスからの最新の構成変更は、RMA ワークフロー中に交換後のデバイスにプッシュされます。

**ステップ 5** [Inventory] ドロップダウンリストから、[Marked for Replacement] を選択します。

交換用としてマークされたデバイスのリストが表示されます。

**ステップ 6** （任意） デバイスを交換しない場合は、デバイスを選択して、**[Actions]** > **[Unmark for Replacement]** を選択します。

**ステップ 7** 交換するデバイスを選択し、**[Actions]** > **[Replace Device]** を選択します。

**ステップ 8** [Replace Device] ウィンドウで、[Start] をクリックします。

**ステップ 9** [Replace Device] ウィンドウで、[Available Replacement Devices] 領域の下にあるデバイスを選択します。

**ステップ 10** **[次へ (Next)]** をクリックします。

**ステップ 11** [Replacement Summary] を確認し、[Next] をクリックします。

**ステップ 12** デバイスを今すぐ交換するか、後で交換を行うようスケジュールするかを選択し、[Submit] をクリックします。

RMA ワークフローが開始されます。

**ステップ 13** [Monitor Replacement Status] をクリックして、[Provision] ページに移動します。

**ステップ 14** 交換用デバイスの [Replace Status] をクリックすると、次のように RMA ワークフローの進捗状況が表示されます。

- 交換用デバイスにソフトウェアイメージを配布します。
- デバイスのソフトウェアイメージをアクティブ化します。
- ライセンスを展開する。
- ネイバーデバイスで DHCP サーバーを作成します。
- VLAN とスタートアップ構成をプロビジョニングします。
- デバイスのリロード。
- 到達可能性をチェックします。
- 交換用デバイスに SNMPv3 ログイン情報を展開します。
- Cisco ISE に対して認証します。
- PKI 証明書を失効化します。
- 障害のあるデバイスを削除します。
- 交換用デバイスを同期します。
- ネイバーデバイスから DHCP サーバーを削除します。
- RMA ワークフローにより、CSSM から障害のあるデバイスの登録が解除されます。
- RMA ワークフローにより、交換デバイスが CSSM に登録されます。

ワークフローが完了すると、[Replace Status] が [Replaced] に更新されます。

**ステップ 15** エラーメッセージが表示された場合は、エラーリンクをクリックします。

**ステップ 16** [Retry] をクリックして、故障したデバイスと交換用デバイスの同じ組み合わせを使用してワークフローを再トリガーします。

（注） [Main Inventory] ウィンドウには、故障したデバイスと交換した新しいデバイスの詳細情報が表示されます。

# 障害のあるアクセスポイントの交換

AP の RMA 機能を使用して、障害のある AP をデバイスインベントリに登録されている交換用 AP に交換できます。

### 始める前に

- AP の返品許可（RMA）機能では、同等の交換のみをサポートしています。モデル番号と PID が障害のある AP と同じ交換用 AP を用意する必要があります。
- 交換用 AP を障害のある AP と同じ シスコ ワイヤレス コントローラに接続しておく必要があります。
- ワイヤレスコントローラとして機能する Cisco Mobility Express AP は、交換用 AP の候補ではありません。
- 障害のある AP のソフトウェア イメージ バージョンをイメージリポジトリにインポートしてから、交換用デバイスにマークを付ける必要があります。
- 交換用デバイスがプラグアンドプレイ（PnP）で Cisco DNA Center をオンボードしている場合は、故障したデバイスをユーザー定義のサイトに割り当てる必要があります。
- RMA ワークフローのトリガー中は、交換用 AP がプロビジョニング状態であってはなりません。
- 故障したデバイスは到達不能な状態になっている必要があります。

---

**ステップ 1** Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Devices]** > **[Inventory]**。

[Inventory] ページには、ディスカバリプロセス中に収集されたデバイス情報が表示されます。

**ステップ 2** 交換する故障した AP のチェックボックスをオンにします。

**ステップ 3** [Actions] ドロップダウンリストから、**[Device Replacement]** > **[Mark Device for Replacement]** の順に選択します。

**ステップ 4** [Mark For Replacement] ウィンドウで、障害のあるデバイス名の横にあるオプションボタンをクリックします。

**ステップ 5** [Actions] ドロップダウンリストから、**[Replace Device]** を選択します。

**ステップ 6** [Replace Device] ウィンドウで、[Start] をクリックします。

**ステップ 7** [Available Replacement Devices] テーブルで、交換用デバイスの名前の横にあるオプションボタンをクリックします。

**ステップ 8** **[次へ (Next)]** をクリックします。

**ステップ 9** [Replacement Summary] を確認し、[Next] をクリックします。

**ステップ 10** [Schedule Replacement] ウィンドウで、デバイスを今すぐ交換するか、後で交換を行うようスケジュールするかを選択し、[Submit] をクリックします。

RMA ワークフローが開始されます。

**ステップ 11** 交換ステータスをモニターするには、[What's Next] で [Monitor Replacement Status] をクリックします。

[Mark For Replacement] ウィンドウに、交換用としてマークされているデバイスのリストが表示されます。

[Replace Status] 列で交換のステータスを確認します。当初は [In-Progress] と表示されます。

**ステップ 12** [Replace Status] 列の [In-Progress] をクリックします。

[Replace Status] タブには、デバイス交換の一環として Cisco DNA Center で実行されるさまざまな手順が表示されます。

**ステップ 13** [Marked for Replacement] ウィンドウで、[Refresh] をクリックしてから [Replace Status] をクリックして交換ステータスを確認します。

故障した AP の交換が失敗すると、[Replace Status] 列にエラーメッセージとともに失敗した理由が表示されます。

故障した AP を別の新しい AP に交換するか、AP RMA 再試行機能を使用して失敗した交換を再試行できます。

**ステップ 14** 失敗した交換を再試行するには、デバイス名の [Replace Status] 列のエラーメッセージをクリックします。

**ステップ 15** [Retry] をクリックします。

**ステップ 16** [Marked for Replacement] ウィンドウで、[Replace Status] 列の [In-Progress] をクリックします。

故障した AP が正常に交換されると、[Replace Status] タブに成功と表示されます。

**ステップ 17** 故障したデバイスが正常に交換されると、[Replacement History] ウィンドウの [Replace Status] に [Replaced] と表示されます。

**ステップ 18** （オプション）デバイスを交換しない場合は、デバイスを選択し、**[Actions]** > **[Unmark for Replacement]** の順に選択します。

# Cisco DNA Center での RMA ワークフローの制限事項

- RMA は、類似デバイスの交換のみサポートしています。たとえば Cisco Catalyst 3650 スイッチは、別の Cisco Catalyst 3650 スイッチとのみ交換できます。また、故障したデバイスと交換用デバイスのプラットフォーム ID も同じである必要があります。
- RMA は、以下を除くすべてのスイッチ、ルータ、および Cisco SD-Access デバイスの交換をサポートします。
  - ワイヤレスコントローラが組み込まれたデバイス
  - ワイヤレスコントローラ（WLC）
  - ファブリック イン ア ボックス
  - クラシックおよびポリシー拡張ノード

- シードデバイス（LAN 自動化プライマリおよびピアデバイス）など、LAN 自動化によって検出および設定されたデバイス
- Catalyst 9400、Catalyst 9600、Catalyst 4500e、Catalyst 6500、Catalyst 6800、Nexus 7700 シリーズ スイッチなど、シャーシベースのスイッチ
- スイッチスタック（ハードウェアスタッキングおよび SVL スタッキング）
- シングルおよびデュアル スーパーバイザ エンジンを搭載したデバイス
- サードパーティの証明書を持つデバイス
- 外部 SCEP ブローカ PKI 証明書を持つデバイス

- RMA ワークフローでは、次の場合にのみデバイスの交換が可能です。
  - 障害のあるデバイスと交換用デバイスの両方に同じ拡張カードが搭載されている。
  - 両方のデバイスのポート数が拡張カードによって変わらない。
  - 障害のあるデバイスは、Cisco DNA Center によって静的 IP で管理されます（RMA は、Cisco DNA Center によって DHCP IP で管理されるデバイスではサポートされません）。
- 交換用デバイスが、障害のあるデバイスが接続されていたポートと同じポートに接続されていることを確認してください。
- Cisco DNA Center レガシーライセンスの導入はサポートされていません。

  RMA ワークフローにより、CSSM から故障したデバイスの登録が解除され、交換用デバイスが CSSM に登録されます。
  - 障害のあるデバイスにインストールされているソフトウェアイメージが Cisco IOS XE 16.8 よりも前のバージョンの場合、[License Details] ウィンドウにはネットワークと機能のライセンスの詳細が表示されず、警告メッセージも表示されません。そのため、障害のあるデバイスに設定されているレガシー ネットワーク ライセンスを確認し、交換用デバイスに同じレガシー ネットワーク ライセンスを手動で適用する必要があります。
  - 故障したデバイスにインストールされているソフトウェアイメージが Cisco IOS XE 16.8 以降の場合は、[License Details] ウィンドウにネットワークライセンスの詳細（**レガシー**、**ネットワーク**など）と機能ライセンス（IP Base、IP Service、LAN Base など）が表示されます。障害のあるデバイスを交換対象としてマークしている際に、次の警告メッセージが表示されます。

    ```
    Some of the faulty devices don't have a Cisco DNA license. Please
    ensure your replacement device has the same Legacy license of
    the faulty device enabled.
    ```
  - 交換用デバイスと障害のあるデバイスのレガシー ネットワーク ライセンスが一致しない場合は、ライセンスの展開中に次のエラーメッセージが表示されます。

Cisco DNA Center doesn't support legacy license deployment. そのため、交換用デバイスで障害のあるデバイスのライセンスを手動で更新し、再同期してから続行してください。

- Cisco DNA Center 障害のあるデバイスのアーカイブに保存されている実行中コンフィギュレーションと VLAN 設定を交換用デバイスにプロビジョニングします。最新のアーカイブの後に障害のあるデバイスで何らかの構成変更が発生した場合、交換用デバイスに最新の構成が反映されない可能性があります。
- 交換用デバイスが PnP DHCP 機能によってオンボードされる場合は、リロードのたびにデバイスが同じ IP アドレスを取得し、DHCP のリースタイムアウトが 2 時間を超えていることを確認してください。

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。