インベントリの管理

• アクセスポイントのリブート （58 ページ）

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 （44 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、選択内容は新しい各ビューに保持されます。

[Focus] ドロップダウンリストから [Default] ビューを選択した場合、[Inventory] テーブルには、リストされたデバイスの [Device Name]、[IP Address]、[Device Family]、および [MAC Address] のみが表示されます。

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 500 のエントリを表示できます。

[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、新しい各ビューで同じ数のエントリが表示されます。

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。

メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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	デバイスの名前。 デバイス名をクリックすると、そのデバイスの詳細情報が表示されます。 （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	デバイスのサポートレベルが表示されます。
	• [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。
	• [Limited]：レガシーデバイス用のデバイスパックは、Cisco DNA Center の次の機能についてのみテストされています。
	  • 検出
	  • トポロジ
	  • デバイスの到達可能性
	  • 構成変更監査
	  • インベントリ
	  • ソフトウェアイメージ管理（ソフトウェアイメージは、cisco.com に記載の EOL デバイスでは利用できない場合があります。EOL デバイスには推奨されません。）
	  • テンプレート プロビジョニング（スイッチにのみ適用されます。）
	詳細については、『Cisco DNA Center Compatibility Matrix』を参照してください。
	• [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やバグを申請することはできません。
	• [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。 • [Reachable]：Cisco DNA Center から SNMP、HTTP（S）、および NETCONF ポーリングを使用してデバイスに到達できます。 • [Ping Reachable]：Cisco DNA Center から ICMP ポーリングを使用してデバイスに到達できます。SNMP、HTTP（S）、および NETCONF ポーリングでは到達できません。 • [Unreachable]：SNMP、HTTP（S）、NETCONF、ICMP のいずれのポーリングでもデバイスに到達できません。

カラム	説明
[EoX Status]	EoX スキャンのステータスが表示されます。 • [Success]：デバイスでの EoX アラートのスキャンに成功しました。 • [Not Scanned]：デバイスは EoX アラートについてスキャンされていません。 • [Scan Failed]：Cisco DNA Center でデバイスでの EoX アラートのスキャンに失敗しました。 • [Scanning]：Cisco DNA Center でデバイスでの EoX アラートのスキャンを実行しています。 [EoX Status] の横にある [i] アイコンにカーソルを合わせ、[Click here to accept] をクリックして、EoX スキャンを開始します。 正常にスキャンされたデバイスについては、[EoX Status] 列にアラートの数が表示されます（ある場合）。 アラートの数をクリックすると、アラートの詳細が表示されます。 slide-in pane で、[Hardware]、[Software]、および [Module] タブをクリックして、ハードウェア、ソフトウェア、およびモジュールの EoX アラートを表示します。
Manageability	デバイスのステータスが示されます。 • [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。 • [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。 • [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。
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の稼働時間。

カラム	説明
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。 （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。 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。
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、ネットワーク階層の概要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（Cisco Catalyst 4500 シリーズ スイッチなど）。
Resync Interval	デバイスのポーリング間隔。再同期間隔は、[Inventory] ウィンドウから **[Actions]** > **[Edit Device]** > **[Resync Interval]** の順に選択して設定します。再同期タイプを [Global] として設定するには、メインメニューから **[System]** > **[Settings]** の順に選択します。詳細については、『*Cisco DNA Center Administrator Guide*』を参照してください。
Last Sync Status	デバイス最終検出のスキャン状態。 • [Managed]：デバイスは完全に管理された状態です。 • [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。 • [Unreachable]：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。この状態は、定期的な収集が行われたときに発生します。 • [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クレデンシャルが変更された場合、この状態が表示されます。 • [In Progress]：インベントリ収集が実行されています。

カラム	説明
プロビジョニング ステータス	デバイスで試行された最後のプロビジョニング操作のステータスが示されます。過去のプロビジョニング操作のステータスを確認するには、[See Details] をクリックします。 • [Success]：デバイスでの最近の操作が成功しました。 • [Success] と警告アイコン：デバイスでの最近の操作は成功しましたが、過去のプロビジョニング操作による障害があるため、注意が必要です。 • [Failed]：デバイスでの最近の操作が失敗しました。 • [Failed] と警告アイコン：デバイスでの最近の操作が失敗しました。過去のプロビジョニング操作による障害があるため、注意が必要です。 • [Configuring]：デバイスは現在設定中です。 • [Pending]：システムは、進行中のプロビジョニング操作によってデバイスが影響を受けるかどうかを判断しようとしています。 • [Not Provisioned]：デバイスは一度もプロビジョニングされていません。 • [Out of Sync]：デバイスのネットワーク設定またはネットワークプロファイルが、最後のプロビジョニング操作の後に変更されました。
Credential Status	デバイスのクレデンシャルステータスが示されます。 • [Not Applied]：デバイスのクレデンシャルがデバイスに適用されていません。 • [Success]：デバイスのクレデンシャルがデバイスに正常に適用されました。 • [Failed]：デバイスのクレデンシャルがデバイスで失敗しました。 クレデンシャルの詳細を表示するには、[See Details] をクリックします。 [Credential Status] slide-in paneには、クレデンシャルの [Type]、[Name/Description]、[Status]、および [Details] が表示されます。 ステータスが [Failed] のデバイスの場合、[Actions] 列の省略記号アイコン（ *** ）の上にカーソルを置き、[Retry] または [Clear] を選択します。 • [Retry]：デバイスにクレデンシャルを適用します。 • [Clear]：デバイスのクレデンシャルをクリアします。
AP Ethernet Mac Address	AP イーサネット MAC アドレスに関する詳細を表示します。
AP CDP Neighbors	インベントリ リスト ウィンドウの AP に接続されているスイッチとポートに関する詳細が表示されます。このウィンドウには、接続されたアクセススイッチが Cisco DNA Center によって管理されている場合でも、AP CDP ネイバーに関する情報が表示されます。

インベントリ ユーザーインターフェイスの機能強化

Cisco DNA Center のインベントリ ユーザーインターフェイスの機能が強化され、これまでと同じ機能性を保ちながらフィルタとレイアウトがより使いやすくなりました。

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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Inventory]** の順に選択します。

[Inventory] ウィンドウがデフォルトで表示され、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 上部のメニューバーの場所オプションをクリックして、ネットワーク階層からサイト、ビルディング、またはフロアを選択してデバイスを管理します。

ステップ 3 **Inventory** ウィンドウの上部に表示されるデバイスファミリエリアを使用して、1 つ以上のデバイスファミリを選択します。

使用できるデバイスファミリは、[Routers]、[Switches]、[Wireless Controllers]、[Access Points]、[Sensors] です。

ステップ 4 [Focus] ドロップダウンリストを使用すると、[Inventory] 、[Default] 、[Software Image] 、[Provision] 、[Security] 、または [Device Replacement] に基づいてデバイスをフィルタ処理できます。

ステップ 5 [Device] テーブルの左隅にある分割バーを使用すると、テーブルの表示を調整できます。

ステップ 6 デバイスを絞り込むには、[DEVICE WORK ITEMS] 領域で、フィルタする条件を1 つ以上指定します。

ステップ 7 新たにデバイスをインベントリに追加するには[Add Device] をクリックします。詳細については、デバイスをサイトに追加するを参照してください。

ステップ 8 デバイスにタグを付けるには、[Tag] を使用します。詳細については、インベントリ内のデバイスの管理（32 ページ）を参照してください。

ステップ 9 [Action] ドロップダウンリストを使用すると、1 つ以上のデバイスでデバイスアクションを実行できます。

ステップ 10 動作のリストとそれぞれの内容は、[i] アイコンをクリックしてください。

ステップ 11 インベントリテーブルを編集またはカスタマイズするには、テーブルの右上隅にある歯車アイコンをクリックします。次のような操作を実行できます。

1. [Table Appearance] で、[Table Density] と[Table Striping] を設定します。
2. [Edit Table Columns] で、検出プロセスでインベントリテーブルに含めたいデバイス情報を選択します。
3. [Edit Custom Views] でビューの設定をカスタマイズできます。
4. [Apply] をクリックして変更を保存するか、[Reset All Settings] をクリックしてインベントリテーブルをデフォルト設定に戻します。

ステップ 12 デバイステーブルに更に詳細なフィルタ設定を行うには[Filter Devices] オプションを使います。詳細については、「デバイスのフィルタ」デバイスのフィルタ （31 ページ）を参照してください。

ステップ 13 右上隅にあるトグルボタンをクリックすると、[Dashboard] 、[Table] 、[Topology] 、[Map] の各ビュー間で切り替えることができます。

ステップ 14 過去のインベントリウィンドウを見るには [Go to old page] をクリックします。

ステップ 15 デバイステーブルの全てのデータをエクスポートするには、[Export] をクリックします。

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、デバイスに関する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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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] スライドインペインで、[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] フィールドに名前、[Field Description] フィールドに説明を入力します。

（注） お客様の IP アドレスやお客様のデバイス名など、[Device Details] ウィンドウ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 [保存（**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。これらのフィールドはテーブルに表示されます。

ステップ 6 （任意）ユーザー定義フィールドを編集するには、対応する編集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 （任意）ユーザー定義フィールドを削除するには、対応する削除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] ウィンドウで少なくとも 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 （10 ページ）』を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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から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 （任意） デバイスからユーザー定義フィールドを削除するには、対応する削除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 メニューアイコン（☰）をクリックして、[Provisioning] > [Network Devices] > [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* 互換性マトリクス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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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) グローバルログイン情報を使用するには、[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 クレデンシャルがない場合は、**[Network Settings]** > **[Device Credentials]**ウィンドウでグローバル CLI クレデンシャルを作成します。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) 特定のデバイスのログイン情報を設定するには、**[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
Name/Description	CLIクレデンシャルを説明する名前または語句。 CLI の認証が失敗した場合、Cisco DNA Center は、認証プロセスを 300 秒（5 分）間再試行してから、[CLI Authentication Failed] のステータスでデバイスをインベントリに移動します。
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。 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。 （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。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。 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。 （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) グローバルログイン情報を使用するには、[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 クレデンシャルがない場合は、**[Network Settings]** > **[Device Credentials]**ウィンドウでグローバル SNMP クレデンシャルを作成します。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。 • [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。 （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。 • [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。 （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。 • [Authentication and Privacy]：認証と暗号化の両方を行います。 • [Authentication, No Privacy]：認証は行いますが、暗号化は行いません。 • [No Authentication, No Privacy]：認証も暗号化も行いません。
Auth. Type	使用する認証タイプ（[Mode] として [Authentication and Privacy] または [Authentication, No Privacy] 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。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5 (not recommended)]：HMAC-MD5 に基づく認証。

フィールド	説明
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。 （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。 • 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。（[Mode] として [Authentication and Privacy] を選択した場合に有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。 （注） • 検出機能とインベントリ機能の使用は、プライバシータイプ CISCOAES192 および CISCOAES256 のみでサポートされています。アシュアランス 機能はサポートされていません。 • プライバシー タイプ AES128 は、検出、インベントリ、およびアシュアランスでサポートされています。
プライバシー パスワード（**Privacy Password**）	暗号化の標準規格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。 （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。 • 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　[SNMP Retries and Timeout] エリアがまだ展開されていない場合は展開し、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	Cisco DNA Centerが SNMP を使用してネットワークデバイスとの通信を試行する回数。
[Timeout (in Seconds)]	再試行の時間間隔（秒単位）。

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]** ウィンドウでグローバル 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 : HTTPS* クレデンシャル

フィールド	説明
[Type]	設定している HTTPS クレデンシャルのタイプを指定します。有効なタイプは、[Read] または [Write] です。
Read	最大 10 つの HTTPS 読み取りクレデンシャルを設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [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。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

フィールド	説明
Write	最大 10 つの HTTPS 書き込みクレデンシャルを設定できます。 • [Name/Description]：追加している HTTPS ログイン情報の名前または説明。 • [Username]：HTTPS 接続の認証に使用される名前です。 • [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。 • [Port]：HTTPS トラフィックに使用される TCP/UDP ポートの番号です。デフォルトはポート番号 443（HTTPS の既知のポート）です。 パスワードは 7 ～ 128 文字で指定します。次から少なくとも 1 つずつ使用する必要があります。 • 小文字の英字（a ～ z） • 大文字の英字（A ～ Z） • 数字（0 ～ 9） • 特殊文字（: # _ * ?）– パスワードにスペースや山カッコ（<>）は使用できません。一部の Cisco IOS XE デバイスでは、疑問符（?）を使用できないので注意してください。

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。

（注）　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。

表 *7 : NETCONF* 設定

フィールド	説明
Port	デバイスのポート。次のいずれかのポートを使用できます。 • ポート 830（デフォルト） • デバイスで使用可能なその他のポート • Cisco DNA Center で構成するカスタムポート。（デバイス可制御性が有効になっている場合にのみ、カスタムポートを使用できます詳細については、*Cisco DNA Center* 管理者ガイド の「Device Controllability」の項を参照してください NETCONF の認証が失敗した場合、Cisco DNA Center は、認証プロセスを 300 秒（5 分）間再試行してから、[NETCONF port not given] のステータスでデバイスをインベントリに移動します。

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 （任意） [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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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 *8 : 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。 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。 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。 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。 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 *9 : 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。 • [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。 （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。

フィールド	説明
Write	• [Name/Description]：追加している SNMPv2c 設定の名前または説明。 • [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。 （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 *10 : 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。 • [Authentication and Privacy]：認証と暗号化の両方を行います。 • [Authentication, No Privacy]：認証は行いますが、暗号化は行いません。 • [No Authentication, No Privacy]：認証も暗号化も行いません。
Auth. Type	使用する認証タイプ（[Mode] として [Authentication and Privacy] または [Authentication, No Privacy] 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。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5 (not recommended)]：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。 （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。 • 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
Privacy Type	プライバシー タイプ。（[Mode] として [Authentication and Privacy] を選択した場合に有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。 （注） • 検出機能とインベントリ機能の使用は、プライバシータイプ CISCOAES192 および CISCOAES256 のみでサポートされています。アシュアランス 機能はサポートされていません。 • プライバシー タイプ AES128 は、検出、インベントリ、およびアシュアランスでサポートされています。
プライバシーパスワード（**Privacy Password**）	暗号化の標準規格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。 （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。 • 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の再試行回数とタイムアウト（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 *11 : 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 *12 : 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。 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。 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 （任意） [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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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。

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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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]** ウィンドウで作成します。グローバル HTTPS 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 : 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]** ウィンドウで作成します。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 *14 : 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。 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。 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。 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。 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 *15 : 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。 • [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。 （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。 • [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。 （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 *16 : 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。 • [Authentication and Privacy]：認証と暗号化の両方を行います。 • [Authentication, No Privacy]：認証は行いますが、暗号化は行いません。 • [No Authentication, No Privacy]：認証も暗号化も行いません。
Auth. Type	使用する認証タイプ（[Mode] として [Authentication and Privacy] または [Authentication, No Privacy] 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。 • [SHA]：HMAC-SHA に基づく認証。 • [MD5 (not recommended)]：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。 （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。 • 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
Privacy Type	プライバシー タイプ。（[Mode] として [Authentication and Privacy] を選択した場合に有効になります）。次のいずれかのプライバシー タイプを選択します。 • [AES128]：暗号化の 128 ビット CBC モード AES。 • **CISCOAES192**：シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • **CISCOAES256**：シスコのデバイス上での暗号化の 256 ビット CBC モード AES。 （注） • 検出機能とインベントリ機能の使用は、プライバシータイプ CISCOAES192 および CISCOAES256 のみでサポートされています。アシュアランス 機能はサポートされていません。 • プライバシー タイプ AES128 は、検出、インベントリ、およびアシュアランスでサポートされています。
プライバシーパスワード（**Privacy Password**）	暗号化の標準規格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。 （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。 • 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 （任意） [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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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] スライドインペインの [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 （任意） [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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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。

ステップ 4 [Edit Device] スライドインペインで、[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 メニューアイコン（≡）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

ステップ 2 **[Filter devices]** をクリックします。

- [Quick Filter]：このフィルタでは、デバイスの詳細を取得できます。

- [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 （任意） 必要に応じて、さらにフィルタ処理を追加します。

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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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。

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。

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、[Save] をクリックします。

ステップ 6 （任意） 複数のデバイスを選択して同じ場所に追加する場合は、最初のデバイスで [Apply to All] チェックボックスをオンにして残りのデバイスに同じ場所を割り当て、[Next] をクリックします。

ステップ 7 [Application and Endpoint Visibility is enabled on all applicable devices.Check this to skip enabling it on all devices] チェックボックスをオンにします。

（注） [Application and Endpoint Visibility] の有効化は、コントローラベースのアプリケーション認識（CBAR）の有効化または展開解除されたアプリケーション可視性サービス（AVS）がサポートされないデバイスについてはデフォルトでスキップされます。

ステップ 8 サマリ設定を確認し、[Next] をクリックします。

ステップ 9 [Task Name] フィールドに、任意のタスク名を入力します。

ステップ 10 デバイスを今すぐ（[Now]）サイトに割り当てるか、後でスケジュールするかを選択します。

ステップ 11 [**Assign**] をクリックします。

ステップ 12 CLI 構成をプレビューするには、[Generate Configuration Preview] オプションボタンをクリックして、次の手順を実行します。

1. [Task Name] フィールドに任意のタスク名を入力し、[Preview] をクリックします。

   後で、作成した構成のプレビューを使用して、選択したデバイスに展開できます。

2. [Task Submitted] ダイアログボックスで、[Work Items] リンクをクリックします。

   （注） このダイアログボックスは表示されてから数秒で表示されなくなります。[Work Items] ウィンドウに移動するには、メニューアイコン（☰）をクリックして、**[Activities]**>**[Work Items]** を選択します。

3. [Work Items] ウィンドウで、設定プレビュー要求を送信した CLI プレビュータスクをクリックします。

4. CLI 設定の詳細を表示し、[Deploy] をクリックします。

5. 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。

6. 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

7. 確認ウィンドウで [Yes] をクリックします。

   （注） CLI タスクは、[Work Items] ウィンドウで完了済みとしてマークされます。このタスクの CLI 設定は表示することはできますが、再度展開することはできません。

ステップ 13 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。

[Inventory] ウィンドウで、デバイスにタグを追加したり、デバイスからタグを削除したりできます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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] 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。「ルールを使用してデバイスにタグ付けする （34 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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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] 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。

[Create New Tag] ウィンドウが表示されます。

[Total Devices Tagged Count] の下にある [Manually Added] フィールドは、選択されたデバイスの数を示します。

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：[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：既存の条件の横にある追加アイコン (+) 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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

[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、**[Tag]** 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 [Manage Tags] をクリックします。

[All Tags] スライドインペインが表示されます。

ステップ 4 編集するタグの横にある鉛筆アイコンをクリックします。

ステップ 5 タグを変更し、[Save] をクリックします。

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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

ステップ 2 デバイスを選択しないで、**[Tag]** > **[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 プロンプトで [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。

デバイスの REP リングを構成する

Resilient Ethernet Protocol（REP）はネットワークループの制御、リンク障害の処理、コンバージェンス時間の改善を実現します。

（注） REP リングの制約事項：

リングのインターフェイスを介してのみ接続するルートノードを選択しないでください。

始める前に

- デバイスがオンボーディングされており、到達可能な状態であることを確認します。
- REP リングの終端となっているデバイスとそのインターフェイスを特定します。
- リングの一部であるすべてのインターフェイスが「switchport mode trunk」を使用して構成されていることを確認します。

ステップ 1 メニューアイコン（≡）をクリックして、[Workflows] > [Configure REP Ring (Non-Fabric)] の順に選択します。

または、[Inventory] サイトトポロジ表示に移動して、REP リングを作成するデバイスノードを選択し、[REP Rings] タブで [Create REP Ring] をクリックすることもできます。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Select a root device] ウィンドウで、ルートデバイスを選択します。

（注） デバイスは到達可能な状態であり、アップストリーム接続が確立されている必要があります。

ステップ 4 [Select adjacent devices connected to root device] ウィンドウで、リングの一部であり、ルートデバイスに接続されている隣接デバイスを 1 つ選択します。

ステップ 5 [Select adjacent devices connected to root device] ウィンドウで、同じリングの一部であり、ルートデバイスに接続されている他の隣接デバイスを選択します。

同じリングの一部であり、ルートデバイスに直に接続されている 2 つのデバイスを選択する必要があります。

ステップ 6 ルートデバイスと選択した隣接デバイスを確認（[Review]） して編集（[Edit]） します。

ステップ 7 REP リングの設定を開始するには、[Provision] をクリックします。

[REP Ring Configuration Status] ウィンドウで、設定の進捗状況の詳細なステータスを確認できます。

ステップ 8 [REP Ring Summary] ウィンドウに、作成された REP リングの詳細情報が、検出されたデバイスとともに表示されます。

ステップ 9 REP リングの作成後、成功メッセージが表示されます。

ステップ 10 REP リングの作成を確認するには、[Inventory] ウィンドウのトポロジビューに移動し、リングの一部であるデバイスをクリックします。スライドインペインの [REP Rings] タブで、そのデバイスに存在するすべての REP リングのリストを確認できます。

リスト内の REP リング名をクリックすると、リングに存在するデバイス、リングに接続する各デバイスのポートなど、その REP リングの詳細情報が表示されます。

ポート グループの作成

属性またはルールに基づいてポートをグループ化できます。

ステップ 1 メニューアイコン（≡）をクリックして、**[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 新しいポートタグを作成するには、[Tag] をクリックし、[Create New Tag] を選択します。

[Create New Tag] slide-in paneが表示されます。

ステップ 3 [Tag Name] フィールドに、タグ名を入力します。[Description] フィールドに、タグの説明を追加します。

（注） [WAN] タグは予約済みのタグ名です。WAN タグは自動生成されるため、*WAN* という名前の新しいポートタグは作成できません。

ステップ 4 [Tag Rule] 領域で、[Port] タブをクリックします。

ステップ 5 [Device Scope] 領域で、ドロップダウンリストをクリックし、デバイスの [Location] または [Tag Name] を選択して、フィルタを定義します。

ステップ 6 ポートにタグを付けるためのルールを追加するには、アイコンをクリックします。ポートステータス、速度、タグ名、動作ステータス、および説明に基づいてポートにタグを付けることができます。ブール演算子（AND、OR）を使用して条件を追加できます。

条件を削除するには、削除アイコンをクリックします。

ステップ 7 条件が設定されると、ペインの左下隅に条件に一致するポートのリンクが表示されます。

リンクをクリックしてポートを表示します。[Matching Ports] slide-in paneで、ポートが属するデバイスとポート名を表示できます。

ステップ 8 [Save] をクリックします。

ポートへのタグの割り当て

ポートにタグを手動で割り当てることができます。たとえば、システムで生成された **WAN** タグをポートに手動で割り当てることができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Inventory]** の順に選択します。

ステップ 2 [Inventory] ウィンドウで、デバイス名をクリックし、[View Device Details] を選択します。

ステップ 3 左ペインで [Interfaces] を展開し、[Ethernet Ports] をクリックします。

ステップ 4 ウィンドウの右上隅で、テーブルビューに切り替えます。

ステップ 5 タグ付けするポート（1 つまたは複数）を選択し、[Tag] をクリックします。

ステップ 6 適切なタグを選択します。

ステップ 7 [Apply] をクリックします。

ポート利用情報

ポートが最後に受信した入力と最後に送信した出力を確認できます。

ステップ 1 メニューアイコン（☰）をクリックして、[Provision] [Inventory]

ステップ 2 デバイス名をクリックします。

[Device Details] ウィンドウが表示されます。

ステップ 3 左ペインで [Ethernet Ports] を選択します。

ステップ 4 ポートをクリックしてその詳細を表示します。

ポートの詳細ウィンドウでは、ポートが受信した最後の入力（[Last Input]）と、ポートが送信した最後の出力（[Last Output]）のタイムスタンプを表示できます。

デバイスのメンテナンスモード

デバイスのメンテナンスのスケジュール

Cisco DNA Center で 1 つ以上のデバイスをメンテナンスモードにすることができます。デバイスがメンテナンスモードになっている場合、Cisco DNA Center ではデバイスに関連付けられているテレメトリデータは処理されません。故障したデバイスをメンテナンスモードにすることで、デバイスからの不要なアラートの受信を回避できます。

（注） メンテナンスモードのデバイスからは情報を収集できません。また、設定やポーリング操作はできません。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

ステップ 2 メンテナンスをスケジュール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]** > **[Schedule Maintenance]** の順に選択します。

[Schedule Maintenance] スライドインペインが表示されます。

ステップ 4 [Reason For Maintenance] フィールドに、デバイスをメンテナンスモードにする理由を入力します。

デフォルトでは、Cisco DNA Center が理由を追加し、ユーザーがそれを変更できます。

ステップ 5 [Define Maintenance Window] 領域で、次の手順を実行します。

a) メンテナンスの開始日時を選択します。

b) メンテナンスの終了日時を選択します。

c) または、[Days/Hours] をクリックして、メンテナンスの日数と時間を入力します。

注：メンテナンスの繰り返しを選択するには、[Days/Hours] オプションを選択します。

ステップ 6 [Maintenance Recurrence] 領域で、[None]、[Daily]、または [Weekly] をクリックします。

- [None]：メンテナンスは繰り返されません。
- [Daily]：[Run at Interval（Days）] フィールドに間隔を日単位で入力します。
- [Weekly]:[Run at Interval（Weeks）] フィールドに間隔を週単位で入力します。

ステップ 7 繰り返しに [Daily] または [Weekly] を選択した場合は、[Set Schedule End]チェックボックスをオンにします。

ステップ 8 [End Date] または [End After (Occurrences)] をクリックします。

- [End Date]：メンテナンスを終了する月、日付、年を入力します。
- [End After (Occurrences)]：メンテナンスを終了するまでの回数を入力します。

ステップ 9 [Maintenance Time Zone] 領域で、メンテナンスのタイムゾーンを選択します。

ステップ 10 [送信（Submit）] をクリックします。

デバイスのメンテナンススケジュールの管理

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

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

[Manage Maintenance] スライドインペインが表示されます。[Status] 列には、メンテナンススケジュールの現在のステータスが表示されます。

ステップ 3 [Search] または [Filter] アイコンをクリックして、メンテナンススケジュールを検索またはフィルタします。

ステップ 4 [Actions] 列で、[Edit] アイコンをクリックして、メンテナンススケジュールを編集します。

（注） 進行中のメンテナンススケジュールの場合、メンテナンスの終了時間のみを延長できます。

ステップ 5 [Actions] 列で、[Delete] アイコンをクリックして、メンテナンススケジュールを削除します。

（注） 進行中のメンテナンススケジュールは削除できません。

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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory Insights]** の順に選択します。

[Inventory Insights] ウィンドウが表示されます。

ステップ 2 [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 3 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 4 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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory Insights]** の順に選択します。

[Inventory Insights] ウィンドウが表示されます。

ステップ 2 [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 3 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。

ステップ 4 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。

システムビーコンの管理

システムビーコンを使用して、Cisco DNA Center インベントリ内のスイッチを強調表示できます。

システムビーコンは、次のデバイスで有効にできます。

- Cisco Catalyst 9200 シリーズ スイッチ
- Cisco Catalyst 9300 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ イーサネット スタッカブル スイッチ

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

ステップ 2 ビーコンを有効または無効にするデバイスを選択します。

（注）
- 一度に最大 5 台のスタンドアロンデバイスでビーコンを有効にできます。
- スタックされたデバイスでビーコンを有効にするには、一度に 1 つのデバイスのみを選択する必要があります。スタックされたデバイスでは、1 つ以上のスタックメンバーでビーコンを有効にすることができます。

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

ステップ 4 [Manage System Beacon] スライドインペインで、[System Beacon State] の下の [Enabled] オプションボタンをクリックし、[Apply] をクリックして、選択したデバイスでビーコンを有効にします。

システムビーコンが有効になると、インベントリのデバイス名の横に青いビーコンアイコン（  ）が表示されます。

ステップ 5 （任意） スタックされたデバイスを選択した場合は、[Manage System Beacon] スライドインペインで次の手順を実行します。

a) ビーコンを有効にするスタックメンバーに対応する [Update System Beacon Status?] チェックボックスをオンにします。
b) [System Beacon State] で、[Enabled] オプションボタンをクリックします。
c) [Apply] をクリックします。

ステップ 6 （任意） 選択したデバイスでビーコンを無効にするには、[Manage System Beacon] スライドインペインで次の手順を実行します。

a) [System Beacon State] で、[Disabled] オプションボタンをクリックします。
b) [Apply] をクリックします。

または、[Inventory] ウィンドウで、デバイス名の横にある青いビーコンアイコン（  ）にカーソルを合わせ、[Disable] をクリックします。

デバイスのロールの変更（インベントリ）

検出プロセス中に、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 *17*：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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

ステップ 2 デバイスロールを更新するには、[Edit Device] スライドインペインで次の手順を実行します。

a) ロールを変更するデバイスを選択します。

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

c) **[ロール（Role）]** タブをクリックし、**[デバイスロール（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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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] スライドインペインが表示されます。

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 メニューアイコン（≡）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

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] slide-in pane で、[Resync Interval] をクリックします。

ステップ 5 再同期タイプを選択します。

（注）
- 再同期タイプをグローバルとして設定するには、**[System]** > **[Settings]**の順に移動します。
- 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 [Resync Interval (in Mins)] フィールドで、連続するポーリングサイクル間の時間間隔（分単位）を入力します。

ステップ 7 [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 メニューアイコン（≡）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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、**[More]** > **[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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 2 [Actions] ドロップダウンリストから、**[More]** > **[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] ウィンドウに移動し、**[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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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 **[インポート (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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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。

デバイスの構成ドリフトの表示

デバイスで行った構成の変更は、内部 Cisco DNA Center サーバーに保存されます。外部 Cisco DNA Center からデバイスに加えられた構成の変更に関する詳細情報を表示できます。

ステップ 1 メニューアイコン（☰）をクリックして、[Provision] > [Inventory] の順に選択します。

ステップ 2 デバイス名をクリックします。そのデバイスに関する詳細情報が表示されます。

ステップ 3 [View Device Details] をクリックします。[Device Details] ウィンドウが表示されます。

ステップ 4 左ペインで、[Config Drift] をクリックします。

[Configuration Changes] ウィンドウには、保存された構成ドリフトの数が表示されます。これには、ラベル付きの設定と構成ドリフトバージョンが含まれます。

ステップ 5 [Change History] タブを展開して、次の詳細を表示します。

a) [Config drift date range]：[Start Date] と [End date] をクリックして、構成ドリフトを表示する日付範囲を選択します。デフォルトでは、開始日と終了日は、過去 15 日間の構成ドリフトを表示するように設定されています。

b) [Config drift timeline graph]：選択した日付範囲の構成ドリフトを表示します。デフォルトでは、過去 15 日間の構成ドリフトがタイムライングラフに表示されます。

タイムライングラフには、次の詳細が表示されます。

- [In-band Config Drift]：Cisco DNA Center によって行われた設定変更は、タイムライングラフに青いバブルとして表示されます。
- [Out-of-band Config Drift]：Cisco DNA Center の外で行われた設定変更は、タイムライングラフに紫色のバブルとして表示されます。
- [Labeled Config]：ラベル付きで Cisco DNA Center にアーカイブされた設定バージョンは、タイムライングラフにオレンジ色のバブルとして表示されます。詳細については、構成ドリフトのラベル付け （52 ページ）を参照してください。

c) [Config Drift Version]：下矢印をクリックして、使用可能なすべての構成ドリフトバージョンを表示します。

d) [Running Config]：タイムライングラフの構成ドリフトをクリックします。比較が [Running Config] タブに表示されます。設定バージョン間の違いは、見やすくするために異なる色でマークされています。

構成ドリフトのラベル付け

将来の参照のために、時系列グラフで構成ドリフトにラベルを付けることができます。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Inventory]** の順に選択します。

ステップ 2 デバイス名をクリックします。そのデバイスに関する詳細情報が表示されます。

ステップ 3 [View Device Details] をクリックします。[Device Details] ウィンドウが表示されます。

ステップ 4 左ペインで、[Config Drift] をクリックします。[Configuration Changes] ウィンドウが表示されます。

ステップ 5 ラベルを付ける時系列グラフの構成ドリフトを選択します。選択した構成ドリフトのタイムスタンプは、時系列グラフの下の [Config Drift Version] に表示されます。

ステップ 6 選択した構成ドリフトバージョンに対応する [Label Config] をクリックします。

ステップ 7 [Label Configuration] ウィンドウで、設定バージョンの名前を入力します。ラベル設定のプレフィックスは CCA_ に固定されています。

（注） 設定バージョン名に特殊文字を使用しないでください。

ステップ 8 [Save] をクリックします。ラベル付きの構成ドリフトは、時系列グラフでオレンジ色で表示されます。

ラベル付けされた設定バージョンの数が選択した範囲より大きい場合は、保存される構成ドリフトの合計数を変更します。保存する構成ドリフトの数を設定する方法の詳細については、*Cisco DNA Center* 管理者ガイドの「Configure Device Configuration Backup Settings」のセクションを参照してください。

ステップ 9 ラベルを削除するには、ラベル付きの設定バージョンを選択し、[Remove label] をクリックします。

故障したデバイスの交換

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できます。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。シスコのスイッチスタック（ハードウェアスタッキング）の場合、メンバースイッチの交換のために Cisco DNA Center で

別の手順に従う必要はありません。これはアクティブスイッチにより処理されます。メンバースイッチは、ソフトウェアイメージと設定を提供することで、アクティブスイッチにより交換されます。フルスタック交換は Cisco DNA Center によって処理されます。

（注） デバイス交換ワークフローを使用して、故障したデバイスを交換することもできます。詳細については、デバイスの交換ワークフローを参照してください。

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。
- スイッチスタックの交換の場合、故障したデバイスと交換用デバイスのスタックの数が同一であることが必要です。

ステップ 1 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

a) 交換する故障したデバイスを選択します。

b) [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。

c) [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、PnP でデバイスを Cisco DNA Center にオンボードするために、交換用デバイスに IP アドレスを割り当てるために必要です。この DHCP サーバーは、故障したデバイスが正常に交換されると削除されます。

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。

d) [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。

e) （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 2 （任意） デバイスを交換するには、次の手順を実行します。

a) 交換するデバイスを選択し、**[Actions]** > **[Replace Device]** を選択します。
b) [Choose Replace Device] ウィンドウで、[Unclaimed] タブまたは [Managed] タブから交換用デバイスを選択します。

[Unclaimed] タブには、PnP によってオンボードされたデバイスが表示されます。[Managed] タブには、インベントリまたは検出プロセスによってオンボードされたデバイスが表示されます。

c) （任意） 交換用デバイスがまだオンボードされていない場合は、次の手順を実行します。

1. [Choose Replace Device] ウィンドウで、[Add Device] をクリックします。
2. [Add New Device] ウィンドウで、デバイスのシリアル番号（[Serial Number]）を入力し、[Add New Device] をクリックします。

または

1. [Choose Replace Device] ウィンドウで、[Sync with Smart Account] をクリックします。
2. [Sync with Smart Account] ウィンドウで、[Sync] をクリックします。

d) [Next] をクリックします。
e) [Schedule Replacement] ウィンドウで、デバイスの交換をすぐに開始するか（開始する場合は [Now] をクリックします）、後でスケジュールするかを選択します。
f) [Review] をクリックして、選択したデバイスタイプ、故障したデバイスの詳細情報、および交換用デバイスの詳細情報を確認します。
g) [Next] をクリックして [Summary] ウィンドウで詳細情報を確認します。

[Summary] ウィンドウで、設定を確認します。

h) 変更するには、[編集（Edit）] をクリックします。
i) [Click Monitor Replacement Status] をクリックして [Provision] ウィンドウの [Mark for Replacement] ビューに移動します。
j) [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。

- デバイス交換の準備状況チェックを実行します。
- （PnP）交換用デバイスを請求します。
- 交換用デバイスにソフトウェアイメージを配信してアクティブ化します。
- ライセンスを展開する。
- VLAN 構成をプロビジョニングします。
- スタートアップ構成をプロビジョニングします。
- 交換用デバイスをリロードします。
- 交換用デバイスの到達可能性を確認します。
- 交換用デバイスに SNMPv3 ログイン情報を展開します。
- 交換用デバイスを同期します。

- 故障したデバイスを CSSM から削除します。
- 交換用デバイスを CSSM に追加します。
- PKI 証明書を失効化して作成します。
- Cisco ISE を更新します。
- 障害のあるデバイスを削除します。

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

k) 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。

l) [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。

[Main Inventory] ウィンドウには、新しい交換用デバイスの詳細情報が表示されます。

（注） デバイスを交換対象としてマーキングするのと、デバイスを交換するのは、異なるタイミングで実行できます。

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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[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。

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 （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。

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
  - シスコ ワイヤレス コントローラについて
  - シャーシベース Nexus 7700 シリーズ スイッチ
  - スイッチスタック（SVL スタッキング）
- RMA は、外部 SCEP ブローカ PKI 証明書を使用するデバイスをサポートします。RMA ワークフロー中に、交換デバイス用に PKI 証明書が作成および認証されます。交換した障害のあるデバイスの PKI 証明書は、証明書サーバーから手動で削除する必要があります。
- 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、拡張ノードおよびファブリック内の AP を除く、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）。
- ネイバーデバイスがファブリックの一部でない場合、ファブリックエッジの交換ではネイバーデバイスの DHCP サーバー設定はサポートされていません。中間ノードは Cisco SD-Access ファブリックの一部ではないため、オプション 43 の DHCP サーバーはプッシュされません。
- 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、Cisco SSM から障害のあるデバイスの登録が解除され、交換用デバイスが Cisco SSM 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 は、ファブリックネットワークでの交換デバイスの PnP オンボーディングをサポートします。ただし、次の場合を除きます。
  - 障害のあるデバイスが複数のインターフェイスを使用してアップリンクデバイスに接続されている。
  - 重複プールを使用したローカルエリアネットワーク（LAN）自動化。
- 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。

アクセスポイントのリブート

AP の再起動機能を使用すると、トラブルシューティングとメンテナンスのために 1 つ以上の AP を再起動できます。

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 メニューアイコン（☰）をクリックして、**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。

ステップ 2 再起動する 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、**[Inventory]** > **[Reboot Device]** を選択します。

ステップ 4 [Reboot Device] スライドインペインで、AP を今すぐ再起動する（[Now]）か、後で再起動するようにスケジュールするかを選択します。

ステップ 5 [Selected Devices] を展開して、再起動 AP の AP 名とフロアの詳細を表示します。

ステップ 6 [Reboot] をクリックします。

選択した AP を再起動するタスクが シスコ ワイヤレス コントローラで開始されると、「Reboot Initiated Successfully」というメッセージが表示されます。

ステップ 7 [Task Submitted] ダイアログボックスで、[Task] リンクをクリックします。

このダイアログボックスは表示されてから数秒で表示されなくなります。タスクに移動するには、メニューアイコン（☰）をクリックし、**[Activities]** > **[Tasks]** の順に選択します。

ステップ 8 タスク名をクリックして、再起動の開始ステータスを表示します。

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。