



インベントリの管理

- [インベントリについて \(1 ページ\)](#)
- [インベントリと Cisco ISE の認証 \(2 ページ\)](#)
- [インベントリに関する情報の表示 \(3 ページ\)](#)
- [インベントリからのトポロジマップの起動 \(8 ページ\)](#)
- [Cisco DNA Center インベントリ内のデバイスのタイプ \(9 ページ\)](#)
- [デバイスのフィルタ \(24 ページ\)](#)
- [インベントリ内のデバイスの管理 \(26 ページ\)](#)
- [デバイスのロールの変更 \(インベントリ\) \(29 ページ\)](#)
- [デバイスの管理 IP アドレスの更新 \(30 ページ\)](#)
- [デバイスポーリング間隔の更新 \(31 ページ\)](#)
- [デバイス情報の再同期 \(32 ページ\)](#)
- [ネットワーク デバイスの削除 \(32 ページ\)](#)
- [コマンドランナーを起動 \(インベントリ\) \(33 ページ\)](#)
- [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 \(33 ページ\)](#)
- [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 \(34 ページ\)](#)
- [故障したデバイスの交換 \(37 ページ\)](#)
- [障害のあるアクセスポイントの交換 \(40 ページ\)](#)
- [Cisco DNA Center での RMA ワークフローの制限事項 \(42 ページ\)](#)

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6時間です。ただし、この間隔は、ネットワーク環境の必要性に応じて、最高 24 時間まで変更できます。詳細については、[デバイスポーリング間隔の更新 \(31 ページ\)](#) 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。

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
	<p>デバイスの名前。</p> <p>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。</p> <p>[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。</p> <ul style="list-style-type: none"> • [View Assurance 360] : 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する必要があります。 <p>• Interfaces</p> <ul style="list-style-type: none"> • [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。情報アイコンをクリックすると、ステータスの凡例が表示されます。 <p>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、VLAN、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。</p> <ul style="list-style-type: none"> • [VLANs] (スイッチとハブのみが対象) : VLAN のテーブルに、VLAN ID、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。[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。 • [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。 <ul style="list-style-type: none"> • [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。 • [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。 <p>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。</p> <ul style="list-style-type: none"> • [Power] : 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。 • [Fans] : 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。 • [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。

カラム	説明
	<ul style="list-style-type: none"> • [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。 <p>(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。</p>
IP Address	デバイスの IP アドレス。
Support Type	<p>以下に示すデバイスのサポートレベルが表示されます。</p> <ul style="list-style-type: none"> • [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。 • [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 Cisco 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。 • [Third Party] : デバイスパックは、顧客/ビジネスパートナーによって構築され、認定プロセスを通過しています。サードパーティ製デバイスは、ディスクバリ、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して修正を依頼する必要があります。
Reachability	<p>以下は、さまざまなステータスのリストです。</p> <ul style="list-style-type: none"> • [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。 • [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。 • [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。

カラム	説明
Manageability	<p>デバイスのステータスが次のように示されます。</p> <ul style="list-style-type: none"> • [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マウスの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、稼働している時間。
Device Role	<p>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。</p> <p>(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。</p> <p>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。</p> <ul style="list-style-type: none"> • Unknown • Access • Core • Distribution • Border Router
Site	<p>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。</p>


カラム	説明
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。
Last Sync Status	<p>デバイス最終検出のスキャン状態。</p> <ul style="list-style-type: none"> • [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。 • [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。 • [In Progress] : インベントリ収集が実行されています。

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。

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]**。

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、[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 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 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。 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。 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) 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 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	<ul style="list-style-type: none"> • [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。 <p>(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。</p>
Write	<ul style="list-style-type: none"> • [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。 <p>(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。</p>

[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。 <ul style="list-style-type: none"> • [noAuthNoPriv] : 認証または暗号化を提供しません。 • [AuthNoPriv] : 認証を提供しますが、暗号化は提供しません。 • [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。 <ul style="list-style-type: none"> • [SHA] : HMAC-SHA に基づく認証。 • [MD5] : HMAC-MD5 に基づく認証。

フィールド	説明
Auth Password	<p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> 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	<p>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。</p> <ul style="list-style-type: none"> [DES] : CBC DES-56 規格に基づく認証に DES 56-bit 暗号化を追加。 [AES128] : 暗号化の CBC モード AES。 [None] : プライバシー設定はありません。 <p>(注) DES 暗号化は廃止予定であり、将来のリリースでは削除されます。</p>
Privacy Password	<p>DES または 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。</p> <p>(注)</p> <ul style="list-style-type: none"> 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 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 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。「[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 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。 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。
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。 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。

フィールド	説明
Enable Password	<p>CLI で高い権限レベルに移るために使用するパスワード。</p> <p>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。</p> <p>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。</p>

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	<ul style="list-style-type: none"> • [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。 <p>(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。</p>
Write	<ul style="list-style-type: none"> • [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。 <p>(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。</p>

[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。 <ul style="list-style-type: none"> • [noAuthNoPriv] : 認証または暗号化を提供しません。 • [AuthNoPriv] : 認証を提供しますが、暗号化は提供しません。 • [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。 <ul style="list-style-type: none"> • [SHA] : HMAC-SHA に基づく認証。 • [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。 <p>(注)</p> <ul style="list-style-type: none"> • 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。（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。 <ul style="list-style-type: none"> • [DES] : CBC DES-56 規格に基づく認証に DES 56-bit 暗号化を追加。 • [AES128] : 暗号化の CBC モード AES。 • [None] : プライバシー設定はありません。 <p>(注) DES 暗号化は廃止予定であり、将来のリリースでは削除されます。</p>

フィールド	説明
Privacy Password	<p>DES または 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。</p> <p>(注)</p> <ul style="list-style-type: none"> 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 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。 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** (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。

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] > [Network Devices] > [Inventory]** の順に選択します。
インベントリのページには、ディスクカバリ 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。
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 14: *SNMPv2c* のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> [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。 <p>(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。</p>
Write	<ul style="list-style-type: none"> [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。 <p>(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。</p>

[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。

フィールド	説明
Mode	<p>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。</p> <ul style="list-style-type: none"> • [noAuthNoPriv] : 認証または暗号化を提供しません。 • [AuthNoPriv] : 認証を提供しますが、暗号化は提供しません。 • [AuthPriv] : 認証と暗号化の両方を提供します。
Auth Type	<p>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。</p> <ul style="list-style-type: none"> • [SHA] : HMAC-SHA に基づく認証。 • [MD5] : HMAC-MD5 に基づく認証。
Auth Password	<p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> • 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	<p>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。</p> <ul style="list-style-type: none"> • [DES] : CBC DES-56 規格に基づく認証に DES 56-bit 暗号化を追加。 • [AES128] : 暗号化の CBC モード AES。 • [None] : プライバシー設定はありません。 <p>(注) DES 暗号化は廃止予定であり、将来のリリースでは削除されます。</p>

フィールド	説明
Privacy Password	<p>DES または 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。</p> <p>(注)</p> <ul style="list-style-type: none"> 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 (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]。

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]。

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 [Add Device] ダイアログボックスの [Type] ドロップダウンリストで、[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] > [Network 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 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。

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] > [Network 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 [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 \(27 ページ\)](#)」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、デバイスファミリー、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、ディスクバリ 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せん。
- **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に変更されます。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 (DeviceName)] 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。

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] > [Network Devices] > [Inventory] の順に選択します。

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 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] > [Network 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 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] > [Network Devices] > [Inventory] の順に選択します。

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 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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [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。

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することができます。

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]。

インベントリのページには、ディスクバリ 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、tracert、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 クラスター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 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Provision] > [Network Devices] > [Inventory] の順に選択します。

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 [インポート (Import)] をクリックします。

デバイス設定のエクスポート

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。



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 [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 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] を選択してデバイスのログイン情報をエクスポートします。

[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。



(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。

ステップ 1 故障したデバイスを交換対象としてマークするには、次の手順を実行します。

- a) Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[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。
- b) 交換する故障したデバイスを選択します。
- c) [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。
- d) [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。

- e) [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。

- f) (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 Replace] ウィンドウで、[Now] をクリックしてデバイスの交換をただちに開始するか、[Later] をクリックして特定時間でのデバイスの交換をスケジュールします。

交換用デバイスがまだオンボードされていない場合、[Now] オプションは無効になります。[Later] をクリックして特定時間でのデバイスの交換をスケジュールすることは可能です。

- 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。
h) [Summary] ウィンドウで、次の手順を実行します。
1. 前の手順で選択したデバイスタイプ、故障したデバイス、または交換用デバイスを変更する場合は、[Edit] をクリックします。
2. [Replacement Device] で、[View] をクリックして、交換用デバイスの設定を確認します。
3. [置換 (Replace)] 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) 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。
• (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。

(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。

デバイスを交換対象としてマーキングする先行タスクと、デバイスを交換するタスクは、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** 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** 交換する障害のあ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] 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、[Mark] をクリックします。
- 成功したことを示す「Device(s) Marked for Replacement Successfully」というメッセージが表示されます。
- ステップ 5** [Replace Device] ウィンドウで、障害のあるデバイスと利用可能な交換用デバイスの詳細を確認します。
- ステップ 6** [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 7** [次へ (Next)] をクリックします。
- ステップ 8** [Replacement Summary] を確認し、[Next] をクリックします。
- ステップ 9** 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 10** 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 11** [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 12 [Marked for Replacement] ウィンドウで、[Refresh] をクリックしてから [Replacement History] をクリックして交換のステータスを確認します。
- ステップ 13 障害のあるデバイスが正常に交換されていれば、[Replacement History] ウィンドウの [Replace] 列に [Replaced] と表示されます。
- ステップ 14 (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、障害のある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。
 - ワイヤレスおよびワイヤレスコントローラが組み込まれたデバイス。
 - 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
- 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。また、RMA ワークフローでは、障害のあるデバイスを CSSM に登録したり、問題のあるデバイスライセンスを CSSM から削除したりはしません。

- 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。

- 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 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. So manually update the faulty device license on the replacement device and resync before proceeding.

- 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古い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。