



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)
- [Cisco DNA Center インベントリ内のデバイスのタイプ](#) (7 ページ)
- [デバイスのフィルタ](#) (17 ページ)
- [デバイスのロールの変更 \(インベントリ\)](#) (18 ページ)
- [デバイスの管理 IP アドレスの更新](#) (19 ページ)
- [デバイスの再同期間隔の更新](#) (20 ページ)
- [デバイス情報の再同期](#) (21 ページ)
- [ネットワーク デバイスの削除](#) (21 ページ)
- [コマンドランナーを起動 \(インベントリ\)](#) (22 ページ)
- [CSV ファイルを使用してデバイス設定をインポート/エクスポートします。](#) (22 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。

インベントリ機能デバイスの可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行うこともできます（これらの設定がまだデバイスに存在しない場合）。デバイスの制御性については、[Cisco Digital Network Architecture Center 管理者ガイド](#)を参照してください。

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。デフォルトの最小間隔は 25 分です。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、「[デバイスの再同期間隔の更新 \(20 ページ\)](#)」を参照してください。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。アクティブだった期間が 1 日未満のデバイスのみ表示されます。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。平均すると、500 台のデバイスのポーリングには約 20 分かかります。

Cisco DNA Center 1.3 以降、[Inventory] 機能は [Provision] ページとマージされます。

Cisco DNA Center 1.2.x から Cisco DNA Center 1.3 にアップグレードした場合は、Cisco DNA Center のホームページから [Inventory] ツールを選択します。[Provision Devices] ページに移動するように要求するメッセージが表示されます。[Provision Devices] ページで、[Actions] > [Inventory] を選択して、インベントリ機能を表示および実行します。

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。このように、デバイスをプロビジョニングする場合、Cisco DNA Center はユーザが定義した Cisco ISE サーバ情報を使用してデバイスを設定します。また、Cisco DNA Center は Cisco ISE サーバ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 シリーズのデバイスを認証する場合は、netconf ユーザの権限を提供するように 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 サーバのダウンによって予定通りにデバイスが Cisco ISE サーバ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。監査ログを使用して、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を実行できます。Cisco DNA Center の監査ログの詳細については、『[Cisco Digital Network Architecture Center 管理者ガイド](#)』を参照してください。

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。この使用例については、『[Cisco Digital Network Architecture Center 管理者ガイド](#)』を参照してください。

インベントリに関する情報の表示

[インベントリ (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。[Config] カラムを除く、すべてのカラムではソートをサポートします。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。

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。

Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。

[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。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	<p>デバイスの名前。</p> <p>名前をクリックすると、ダイアログボックスが開き、次の情報が表示されます。</p> <ul style="list-style-type: none">• [Details] : デバイス名、デバイスタイプ、IP アドレス、シリアル番号、ソフトウェアイメージなどの詳細が表示されます。• [Configuration] : 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。 show running-config <p>(注) 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">• [Interface] : デバイスのインターフェイスの [Interface Name]、[MAC Address]、および [Status] が表示されます。• [Stack] : MAC アドレス、ロール、状態、プライオリティが表示されます。• [Run Commands] : デバイスで CLI コマンドを実行するためのコマンドランナーを開きます。• [View 360] : 360 ページを表示します。360 を開くには、アシュアランス アプリケーションをインストールしている必要があります。 <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。

カラム	説明
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">• [Connecting] : Cisco DNA Center がデバイスに接続しています。• [Reachable] : Cisco DNA Center がデバイスに接続されており、CLI を使用して Cisco コマンドを実行できます。 <p>(注) 失敗は、Cisco DNA Center がデバイスに接続されていますが、CLI を使用して Cisco コマンドを実行できなかったことを示します。この状態は通常、デバイスがシスコデバイスではないことを示します。</p> <ul style="list-style-type: none">• [Authentication Failed] : Cisco DNA Center がデバイスに接続されていますが、デバイスのタイプを判別できません。• [Unreachable] : Cisco DNA Center がデバイスに接続できません。 <p>(注) デバイスに接続できないのは、ディスカバリジョブにクレデンシャルが存在しないか、ディスカバリジョブに誤ったクレデンシャルが存在するためである場合があります。これに該当する疑いがある場合は、新しいディスカバリジョブを実行し、デバイスの正しいクレデンシャルを指定します。</p>
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。

カラム	説明
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"> • 不明 • アクセス • [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>
Last Updated	<p>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。</p>
Device Family	<p>ルータ、スイッチとハブ、ワイヤレスコントローラなど、関連するデバイスのグループ。</p>
Device Series	<p>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）。</p>
Resync Interval	<p>デバイスのポーリング間隔。この間隔は、[設定 (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 Digital Network Architecture Center 管理者ガイドを参照してください。</p>

カラム	説明
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。

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。



(注) サポート対象デバイスの完全なリストについては、[Cisco Digital Network Architecture Center のサポート対象デバイス](#)ドキュメントを参照してください。

- **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。

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。

- ステップ 1** Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。
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** **[Add Device]** をクリックします。
- ステップ 3** **[タイプ (Type)]** ドロップダウン リストから、**[ネットワークデバイス (Network Device)]** を選択します。
- ステップ 4** **[デバイスの IP/名前 (Device IP / 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** 表示されていない場合は、**[SNMP]** エリアを展開します。
- ステップ 6** **[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 2: *SNMPv2c* のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • [名前/説明 (Name/Description)] : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティ スtring 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"> • [名前/説明 (Name/Description)] : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティ スtring。 <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 3: 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 : 認証または暗号を提供しません。• AuthNoPriv : 認証を提供しますが、暗号は提供しません。• AuthPriv : 認証と暗号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。 (注) <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 : プライバシー設定なし。

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 7 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 4: *SNMP Properties*

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 8 まだ展開されていない場合は [CLI] エリアを展開し、次のフィールドを設定します。

表 5: *CLI* クレデンシャル

フィールド	説明
Protocol	<p>Cisco DNA Center とリモート デバイスとの通信を有効にするネットワーク プロトコル。有効な値は SSH2 または Telnet です。</p> <p>NETCONF ポートを設定する場合は（次の手順を参照）、ネットワーク プロトコルとして SSH2 を選択する必要があります。</p>
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もう一度入力します。 (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もう一度入力します。 (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 9** 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 10** [追加 (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 ホームページで、[プロビジョニング (Provision)] をクリックします。
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** 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** まだ展開されていない場合は、[SNMP] エリアを展開します。
- ステップ 6** [バージョン (Version)] フィールドから、SNMP バージョン ([V2C] または [V3]) を選択します。

(注) SNMP 資格情報と CLI クレデンシャルの両方が一緒に更新されるため、両方のクレデンシャルを提供することをお勧めします。SNMP 資格情報のみが提供された場合、Cisco DNA Center は SNMP 資格情報のみを保存し、CLI クレデンシャルは更新されません。

ステップ 7 [V2C] または [V3] のいずれを選択したかに応じて、次の表に説明されているように、その他のフィールドに情報を入力します。

表 6: *SNMPv2c* のクレデンシャル

フィールド	説明
Read	<ul style="list-style-type: none"> • [名前/説明 (Name/Description)] : 追加する SNMP v2c 設定の名前または説明。 • Read コミュニティ : デバイス上の SNMP 情報を表示するためにのみ使用される read-only コミュニティ スtring 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"> • [名前/説明 (Name/Description)] : 追加する SNMP v2c 設定の名前または説明。 • Write コミュニティ : デバイス上の SNMP 情報を変更するために使用される write コミュニティ スtring。 <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>

表 7: *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	<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 : 認証または暗号を提供しません。 • AuthNoPriv : 認証を提供しますが、暗号は提供しません。 • AuthPriv : 認証と暗号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。

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 : プライバシー設定なし。
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 [SNMP Retries and Timeout] エリアがまだ展開されていなければ展開し、次のフィールドに入力します。

表 8 : *SNMP Properties*

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。

フィールド	説明
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 [CLI] エリアがまだ展開されていなければ展開し、次のフィールドに入力します。

(注) SNMP と CLI の両方のクレデンシャルと一緒に更新されるため、どちらのクレデンシャルも提供する必要があります。SNMP 資格情報のみが提供された場合、Cisco DNA Center は SNMP 資格情報のみを保存します。CLI クレデンシャルは更新されません。

表 9: CLI クレデンシャル

フィールド	説明
Protocol	Cisco DNA Center とリモート デバイスとの通信を有効にするネットワーク プロトコル。有効な値は SSH2 または Telnet です。 NETCONF ポートを設定する場合は（次の手順を参照）、ネットワーク プロトコルとして SSH2 を選択する必要があります。
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もう一度入力します。 (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もう一度入力します。 (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 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 [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 ホームページで、**[プロビジョニング (Provision)]** をクリックします。

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 **[Add Device]** をクリックします。

ステップ 3 **[タイプ (Type)]** ドロップダウンリストから、**[計算デバイス (Compute Device)]** を選択します。

ステップ 4 **[デバイスの IP/名前 (Device IP/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 表示されていない場合は **[HTTP(S)]** エリアを展開し、次のフィールドを設定します。

- **ユーザ名** : HTTPS 接続の認証に使用される名前。
- **パスワード** : HTTPS 接続の認証に使用されるパスワード。
- **ポート** : HTTPS トラフィックで使用される TCP/UDP ポートの数。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 **[追加 (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 ホームページで、**[プロビジョニング (Provision)]** をクリックします。

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 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 [ユーザ名 (Username)] および [パスワード (Password)] フィールドに、ユーザ名とパスワードを入力します。

ステップ7 [ポート (Port)] フィールドにポート番号を入力します。

ステップ8 [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 ホームページで、[プロビジョニング (Provision)] をクリックします。

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 [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 キー/パスワード (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。

Cisco DNA Center Cisco DNA Center は、Meraki ダッシュボードからインベントリデータを収集して、情報を表示します。

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 ホームページで、[プロビジョニング (Provision)] をクリックします。

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 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、[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 キー/パスワード (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 [ポート (Port)] フィールドにポート番号を入力します。
- ステップ8 [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 ホームページで、[プロビジョニング (Provision)] をクリックします。
- 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 [Filter] をクリックします。
- 次のフィルタが表示されます。

- Tag
- Device Name
- IP Address
- Device Family
- Site
- MAC Address
- Reachability
- Device Role
- Image Version
- Up Time
- Last Sync Status
- Resync Interval

- Serial Number
- Device Series
- Platform

ステップ 3 選択したフィルタフィールドに適切な値を入力します。たとえば、[デバイス名（Device Name）] フィルタには、デバイスの名前を入力します。

Cisco DNA Center では、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。

また、これらのフィルタではワイルドカード（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を含む値を入力できます。

ステップ 4 [Apply] をクリックして情報をフィルタ処理します。

[Device Type] と [Reachability] のクイックフィルタを使用して、デバイスをフィルタ処理することもできます。さらに、左側のペインに表示されている任意のサイトをクリックして、デバイスに割り当てられているサイトに基づいてデバイスをフィルタ処理できます。

[デバイス（Devices）] テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

（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。

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 10: 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（構成不可）
階層 2	[Border Router]
階層 3	コア
階層 4	Distribution
階層 5	アクセス

トポロジの位置	デバイスロール
階層 6	不明 (Unknown)

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 ホームページで、**[プロビジョニング (Provision)]** をクリックします。

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 ロールを変更するデバイスを見つけて、**[デバイスのロール (Device Role)]** カラムの鉛筆アイコンをクリックし、**[デバイスロールの更新 (Update Device Role)]** ダイアログボックスからロールを選択します。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、**[デバイスの編集 (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。
- **[アクション (Actions)]** > **[インベントリ (Inventory)]** > **[デバイスの編集 (Edit Device)]** の順に選択します。
- **[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 Cisco DNA Center ホームページで、**[プロビジョニング (Provision)]** をクリックします。

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 更新するデバイスを選択します。

ステップ 3 [アクション (Actions)] ドロップダウンリストから、[インベントリ (Inventory)] > [デバイスの編集 (Edit Device)] の順に選択します。

[デバイスの編集 (Edit Device)] ダイアログボックスが表示されます。

ステップ 4 [IPの管理 (MANAGEMENT IP)] タブをクリックし、[デバイス IP/DNS 名 (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。

デバイスの再同期間隔の更新

[インベントリ (Inventory)] ウィンドウから、次の方法でデバイスの再同期を設定できます。

- 特定のデバイスのカスタム再同期間隔を有効にして、設定できます。
- すべてのデバイスに設定されている事前設定されたグローバル再同期間隔を有効にすることができます (この設定は、[設定 (Settings)] > [システム設定 (System Settings)] > [設定 (Settings)] > [ネットワーク再同期間隔 (Network Resync Interval)] ウィンドウで設定されます)。
- 再同期を無効にすることができます。

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 ホームページで、[プロビジョニング (Provision)] をクリックします。

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 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 [Resync Interval] タブで、デバイスに設定する再同期オプションのタイプに対応するオプションボタンをクリックします。有効な選択肢は[カスタム (Custom)]、[グローバル (Global)]、および[無効化 (Disable)] です。

ステップ5 [カスタム (Custom)] を選択した場合は、[再同期間隔 (分単位)] 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。有効な値は、25 ~ 1,440 分 (24 時間) です。

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、再同期間隔の設定に関わらず、直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 ホームページで、[プロビジョニング (Provision)] をクリックします。

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 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] をクリックして、アクションを確認します。

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。

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。

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 ホームページで、[プロビジョニング (Provision)] をクリックします。

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 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 [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）

[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 Digital Network Architecture Center 管理者ガイド](#)を参照してください。

ステップ1 Cisco DNA Center ホームページで、[プロビジョニング（Provision）] をクリックします。

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 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] を選択します。

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。

CSVファイルを使用してデバイス設定をインポート/エクスポートします。

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を行うことができません。

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

レディ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tring
- SNMP 書き込みコミュニティ スtring
- 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tring
- SNMP 書き込みコミュニティ スtring
- SNMP 再試行値
- SNMP タイムアウト値
- Protocol
- CLI ユーザ名
- 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 ホームページで、**[プロビジョニング (Provision)]** をクリックします。

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

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

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

ステップ 4 **[Import]** をクリックします。

デバイス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 ホームページで、**[プロビジョニング (Provision)]** をクリックします。

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 特定のデバイスのみの設定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] 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、**[Data]** オプションボタンをクリックします。

ステップ5 CSV ファイルに含めるデータの横にあるチェックボックスをオンにします。

ステップ6 [Export] をクリックします。

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

デバイスのクレデンシャルのエクスポート

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



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

ステップ1 Cisco DNA Center ホームページで、[プロビジョニング (Provision)] をクリックします。

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 [エクスポートタイプの選択 (Select Export Type)] で、[クレデンシャル (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、エクスポートした CSV ファイルに、最初の SSH キー、最初の SSH キーアルゴリズム、現在の SSH キー、現在の SSH キーアルゴリズムなどの情報を含めます。

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。

