インベントリの管理

インベントリについて

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

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、最大 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（23 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、その後、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。

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 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] 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 : Inventory*

カラム	説明
Device Name	デバイスの名前。 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。 • [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]：**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。 （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。 • [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 ウィンドウが表示されます。360 を開くには、アシュアランス アプリケーションをインストールしている必要があります。 （注） 赤で表示されているデバイス名は、インベントリがデバイスをポーリングしておらず、30 分を超える期間にわたってその情報を更新していないことを意味しています。
IP Address	デバイスの IP アドレス

カラム	説明
Support Type	以下に示すデバイスのサポートレベルが表示されます。 • [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、検出、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	以下は、さまざまなステータスのリストです。 • [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。 （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。 • [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。 （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。
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。

カラム	説明
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、稼働している期間。
Device Role	スキャン プロセス中に、検出された各デバイスに割り当てられているロール。デバイス ロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。Cisco DNA Center でデバイス ロールを特定できない場合、デバイス ロールは不明に設定されます。 （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。次のデバイス ロールを使用できます。 • **不明** • **アクセス** • **[Core]** • **[Distribution]** • **[Border Router]**
Site	デバイスに割り当てられているサイト。デバイスがどのサイトにも割り当てられていない場合は、[Assign] をクリックします。[Choose a Site] をクリックし、階層からサイトを選択して [Save] をクリックします。詳細については、About Network Hierarchy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。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。

カラム	説明
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 のホームページで、[Provisioning] > [Inventory] をクリックします。

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。

（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。

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 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、[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。

（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 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	• 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 ストリング 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 ストリング。 （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 *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。 • noAuthNoPriv：認証または暗号化を提供しません。 • AuthNoPriv：認証は提供しますが、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。 • 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	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。（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。 • DES：CBC DES-56 規格に基づく認証に DES 56-bit（DES-56）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	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。 （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 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。

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 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	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 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	• 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 ストリング 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 ストリング。 （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。

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。

フィールド	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。 • noAuthNoPriv：認証または暗号化を提供しません。 • AuthNoPriv：認証は提供しますが、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。 • 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） • 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。 • DES：CBC DES-56 規格に基づく認証に DES 56-bit（DES-56）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	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。 （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。
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が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。

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 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 [HTTP(S)] エリアを展開して（まだ展開されていない場合）、次のフィールドを入力します。

- **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 12 [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 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 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 *10 : SNMPv2c* のクレデンシャル

フィールド	説明
Read	• 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 ストリング 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 ストリング。 （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 *11 : 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	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。 • noAuthNoPriv：認証または暗号化を提供しません。 • AuthNoPriv：認証は提供しますが、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。 • 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） • 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。 • DES：CBC DES-56 規格に基づく認証に DES 56-bit（DES-56）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	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。 （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 [CLI] エリアを展開し、次のフィールドを設定します。

表 *12 : 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。デフォルトでは、[SSH2] が選択され、変更することはできません。
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 9 [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 ダッシュボードのログイン情報を更新できます。選択したデバイスに対しては、この更新された設定が、グローバル設定やジョブ固有の設定よりも優先されます。

始める前に

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

ステップ 1 Cisco DNA Center 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 *13 :* 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	ボーダー ルータ
階層 3	コア
階層 4	配信
階層 5	アクセス
階層 6	不明

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、[Device Role] 列の鉛筆アイコンをクリックし、[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、[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 [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
- プロトコル

- 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 [一括インポート（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。

[エクスポート] 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 [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。

Export Device Credentials

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。

[エクスポート] 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。

故障したデバイスの交換

障害のあるデバイスを、デバイスインベントリにある交換用デバイスと交換できます。

始める前に

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

ステップ 1 Cisco DNA Center 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。

ステップ 2 交換する故障した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]** > **[Device Replacement]** > **[Mark Device for Replacement]** を選択します。

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

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

交換用としてマークされたデバイスのリストが表示されます。

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

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

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

ステップ 9 [Replace Device] ページで、[Available Replacement Devices] エリアの下にあるデバイスを選択します。

ステップ 10 **[次へ (Next)]** をクリックします。

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

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

RMA ワークフローが開始されます。

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

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

- 交換用デバイスにソフトウェアイメージを配布しています。
- デバイスのソフトウェアイメージをアクティブ化しています。

  （注） 交換用デバイスの上位デバイスが故障したデバイスの上位デバイスと異なる場合、交換用デバイスにプッシュされたソフトウェアイメージには互換性がないことがあります。その場合、交換用デバイスのイメージのアクティブ化は ROM モニタ（ROMmon）モードになります。

- ライセンスの展開
- VLAN とスタートアップ コンフィギュレーションのプロビジョニング
- デバイスをリロードする
- 到達可能性のチェック
- Cisco ISE を使用した認証 Cisco ISE
- PKI 証明書の取り消し
- 故障したデバイスの削除
- 交換用デバイスの同期

Cisco DNA Center での RMA ワークフローの制限事項 Cisco DNA Center

- 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。
- 交換用デバイスのスーパバイザエンジンが障害のあるデバイスと異なる場合、交換用デバイスにプッシュされたソフトウェアイメージは互換性がない可能性があります。その場合、交換用デバイスのイメージのアクティブ化は ROM モニタ（ROMmon）モードになります。

- RMA は、LAN の自動化によってプロビジョニングされたすべてのスイッチ、ルータ、SDA デバイス、およびデバイスの交換をサポートします（スタック構成のスイッチ、Nexus スイッチ、アクセスポイント、デュアル スーパーバイザ エンジンを備えたデバイス、ワイヤレスコントローラを除く）。

（注） SDA デバイスの場合、SDA ネットワークには DHCP サーバがなく、PnP を介してデバイスを追加できないため、交換用デバイスを Cisco DNA Center に手動で追加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。
- 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 から削除したりはされません。
  - 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（たとえば、レガシーまたはネットワーク）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。

    「故障した一部のデバイスに *DNA* ライセンスがありません。（*Some of the faulty devices don't have a DNA license.*）交換用デバイスに、障害のあるデバイスで有効になっていたのと同じレガシーライセンスがあることを確認してください。（*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* はレガシーライセンスの展開をサポートしていません。（*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。（*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。最新のアーカイブ後に古いデバイスに何らかの設定変更が加えられた場合、交換用デバイスの設定が最新では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。