デバイスの追加と整理

どのデバイス ソフトウェア バージョンが Cisco EPN Manager によってサポートされているか。

すべてのデバイスは、認定されたデバイス ソフトウェア バージョンを実行している必要があります。ただし、特定のデバイスは最小のデバイス ソフトウェア バージョンを実行している必要があります。デバイス ソフトウェア バージョンを確認する方法については、次の表の手順に従ってください。

Cisco EPN Manager によって、未認定のデバイス ソフトウェア バージョンがデバイスで実行されていることが報告される場合があります。未認定のデバイス ソフトウェア バージョンを実行しているデバイスを Cisco EPN Manager がどのように管理するかについては違いに気付かないことになる可能性があります。管理方法は、デバイス ソフトウェア バージョンに基本的な変更（XML インターフェイス、SNMP コマンド、MIB、CLI コマンドなどに対する変更）が含まれているかどうかによって異なります。Cisco EPN Manager はデバイス ソフトウェア バー

ジョンを認識しても、新しいモジュールなどのデバイス NE を完全にサポートできない場合があります。

この情報を見つけるには、次の手順を実行します。	手順
認定されたすべてのデバイス ソフトウェア バージョンの一覧	『Cisco Evolved Programmable Network Manager のサポート対象デバイス』を参照してください。
	[ヘルプ（Help）] > **[サポートされるデバイス（Supported Devices）]** を選択し、[ソフトウェアバージョン（Software Version）] 列の [i] にカーソルを合わせるとポップアップが表示されます。
管理対象デバイスが未認定のデバイス ソフトウェア バージョンを実行している場合	**[モニタ（Monitor）]** > **[管理対象要素（Managed Elements）]** > **[ネットワークデバイス（Network Devices）]** を選択し、デバイスを見つけて [最後のインベントリ収集（Last Inventory Collection）] 列の [i] にカーソルを合わせます。[未認定のソフトウェアバージョン（Uncertified Software Version）] がポップアップ表示されるかどうかを確認します。
	デバイスの [デバイスの詳細（Device Details）] ページにある [デバイスの詳細（Device Details）] タブで **[システム（System）]** > **[概要（Summary）]** を選択します。 [インベントリ（Inventory）] 領域に [未認定のソフトウェアバージョン（Uncertified Software Version）] が表示されるかどうかを確認します。
最小デバイス ソフトウェア バージョンが必須なデバイス	**[ヘルプ（Help）]** > **[サポートされるデバイス（Supported Devices）]** を選択し、[ソフトウェアバージョン（Software Version）] 列で **>=x.x** のようなテキストを確認します（たとえば **>=12.2** は、デバイスが少なくともデバイス ソフトウェア バージョン 12.2 を実行する必要があることを意味します）。

汎用デバイスのサポート

Cisco EPN Managerでは、公式に（機能が）サポートされていない、インベントリ機能と障害機能が制限された汎用のシスコ デバイスとサードパーティ製デバイスを管理できます。

表 *1* : 汎用デバイスのサポート

汎用デバイスのタイプ	サポートされる機能	サポートされている **MIB**	サポートされる障害
シスコ デバイス	[システム（System）] - [概要（Summary）] [システム（System）] - [電源オプションとファン（Power Options & Fans）] [システム（System）] - [シビックロケーション（Civic Location）] [システム（System）] - [モジュール（Modules）] [システム（System）] - [物理ポート（Physical Ports）] [システム（System）] - [センサー（Sensor）] [インターフェイス（Interfaces）] - [すべてのインターフェイス（All Interfaces）] [インターフェイス（Interfaces）] - [イーサネットインターフェイス（Ethernet Interfaces）] [物理リンク（Physical Links）]	SNMPv2 ENTITY-MIB IF-MIB LLDP-MIB CISCO-ENTITY-FRU-CONTROL-MIB	リンクアップ/リンクダウン（IF-MIB） ウォームスタート（SNMPv2-MIB） コールドスタート（SNMPv2-MIB） 認証エラー（SNMPv2-MIB） BDI インターフェイスのダウン/アップ（BDI にローカライズされるリンクダウン/アップ）（IF-MIB） entSensorThresholdNotification（CISCO-ENTITY-SENSOR-MIB）

汎用デバイスのタイプ	サポートされる機能	サポートされている MIB	サポートされる障害
シスコ以外のデバイス	[システム（System）] - [概要（Summary）] [システム（System）] - [モジュール（Modules）] [システム（System）] - [物理ポート（Physical Ports）] [インターフェイス（Interfaces）] - [すべてのインターフェイス（All Interfaces）] [物理リンク（Physical Links）]	SNMPv2 ENTITY-MIB IF-MIB LLDP-MIB	リンクアップ/リンクダウン（IF-MIB） ウォームスタート（SNMPv2-MIB） コールドスタート（SNMPv2-MIB） 認証エラー（SNMPv2-MIB）

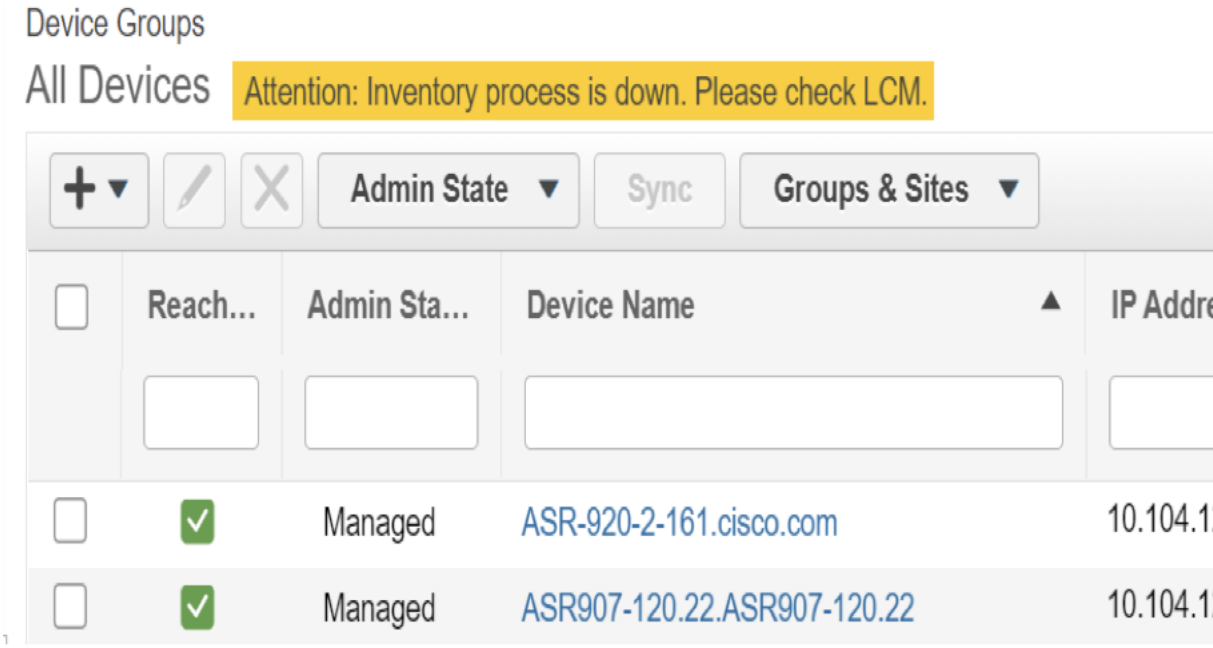
インベントリ検出プロセス

Cisco EPN Manager でデバイスのスケーリングを有効にするには、EPNM プロセスのインベントリ検出コンポーネントを別のプロセス（inventory-discovery-process）として実行します。インベントリ収集に関連するすべての機能（デバイスの追加またはインポート、手動同期、詳細同期および事後同期、失敗した機能の同期、インベントリの切り替え、およびユーザ定義のインベントリ検出を含む）は、nventory-discovery-process によって実行されます。

inventory-discovery-process がダウンした場合の動作

Cisco EPN Manager は、インベントリ検出プロセスがダウンすると、[ネットワークデバイス（Network Devices）] ページにエラーメッセージを表示します。

（注） inventory-discovery-process がダウンしている場合は、インベントリ操作を実行できません。プロセスが起動するまで待ってから、インベントリ操作を再開してください。



inventory-discovery-process に関連するログは、`/opt/CSCOlumos/logs/inventory-discovery-process` に保存されます。詳細については、インベントリ検出プロセスのログを参照してください。

inventory-discovery-process のステータス（started、stopped、stopped、unreachable、および restarting）は **[モニタ（Monitor）]** > **[アラームおよびイベント（Alarms and Events）]** ページにシステム生成イベントとして表示されます。

たとえば、「Process inventory-discovery-process is unreachable and will try to restart」というイベントは、inventory-discovery-process に到達できず、自動的に再起動されることを示します。

重要 「Process inventory-discovery-process reached auto-restart limit」というイベントは、inventory-discovery-process が複数回再試行したにもかかわらず自動的に再起動できなかったことを示します。この場合、Cisco Technical Assistance Center（TAC）でサポートケースを開くことをお勧めします。シスコ サポート ケースの登録 を参照してください。

Cisco EPN Manager へのデバイスの追加

Cisco Evolved Programmable Network Manager はデバイス、ロケーション、およびポート グループを使用して、ネットワーク内の要素を整理します。デバイスをテーブルまたはマップ（ネットワーク トポロジ）で表示すると、デバイスは属しているグループを単位として整理されます。デバイスが Cisco EPN Manager に追加されると、**Unassigned Group** という名前のグループに割り当てられます。その後、簡単な管理と設定のためのデバイス グループの作成 （41 ページ） で説明されているように、デバイスを目的のグループに移動できます。

（注） Cisco WLC を Cisco EPN Manager に追加するには、サポートされていないアクセス ポイント（AP）がないことを確認してください。そのようにしないと、Cisco EPN Manager はその WLC から AP を検出しません。

表 2: デバイスの追加方法

サポートされているデバイスの追加方法	参照先：
以下を使用してシード デバイスのネイバーを検出して複数のデバイスを追加する	ディスカバリを使用したデバイスの追加（7 ページ）。
• Ping スイープと SNMP ポーリング（クイック ディスカバリ）	• クイック ディスカバリの実行 （9 ページ）
• カスタマイズされたプロトコル、クレデンシャル、およびフィルタ設定（ディスカバリ ジョブを繰り返す場合に便利）	• カスタマイズされたディスカバリ設定でのディスカバリの実行 （9 ページ）
CSV ファイルで指定された設定を使用して複数のデバイスを追加する	CSV ファイルを使用したデバイスのインポート （12 ページ）。
単一のデバイスを追加する（たとえば、新しいデバイス タイプの場合）	手動によるデバイスの追加（新規デバイス タイプまたはデバイス シリーズ） （14 ページ）

次のトピックでは、キャリア イーサネットと光デバイスを Cisco EPN Manager に追加する方法の例を示します。

- 例：単一の Cisco NCS 2000 または NCS 4000 シリーズ デバイスの追加 （15 ページ）
- 例：プロキシ設定を使用した ENE としてのネットワーク要素の追加 （16 ページ）

Cisco EPN Manager での Cisco ME1200 デバイスの追加

Cisco EPN Manager で Cisco ME1200 デバイスを追加する際は、次の設定に従ってください。

- SNMP：他のデバイスと同じ SNMP 設定を使用します。
- CLI：プロトコル設定が [SSH2] に設定されていることを確認します。ポートを使用して telnet 経由でデバイスにアクセスできますが、SSH プロトコルを使用することを推奨します。telnet が使用されている場合は、使用されるカスタム telnet ポートは 2323 でなければなりません。
- HTTP：正しい http クレデンシャルを指定してください。

- Cisco ME1200 デバイスの設定変更は Cisco EPN Manager によって自動的に検出されないことに留意してください。変更後、デバイスを手動で同期する必要があります。これを行うには、[ネットワークデバイス（Network Devices）] テーブルで必要なデバイスを選択し、[同期（Sync）] をクリックします。

ディスカバリを使用したデバイスの追加

Cisco EPN Manager は、次の 2 つのディスカバリ方式をサポートしています。

- シード デバイスからの ping スイープ（クイック ディスカバリ）。デバイス名、SNMP コミュニティ、シード IP アドレス、およびサブネット マスクが必要です。この方法は、光デバイスのディスカバリには使用できません。クイック ディスカバリの実行 （9 ページ）を参照してください
- カスタマイズされたディスカバリ方法（ディスカバリ設定）の使用：設定を行い、今後ディスカバリを再実行する場合は、この方法をお勧めします。光デバイスを検出する場合は、この方法を使用します。カスタマイズされたディスカバリ設定でのディスカバリの実行 （9 ページ）を参照してください。

（注）

- ディスカバリ ジョブが既存のデバイスを再検出し、デバイスの最後のインベントリ収集ステータスが [完了済み（Completed）] である場合、Cisco EPN Manager は、既存のクレデンシャルを、ディスカバリ設定で指定されたクレデンシャルで上書きしません。他のすべてのステータス（既存のデバイス上）の場合、Cisco EPN Manager は、デバイスのクレデンシャルを、ディスカバリ設定で指定されたクレデンシャルで上書きします。
- データベースのメンテナンス期間中に多数のデバイスが追加された場合、サービス検出に通常より時間がかかることがあります。したがって、夜間や週末には大規模な作業を回避することをお勧めします。
- 自律 AP がディスカバリ プロセスから除外され、検出時間が最適化されます。[デバイスのインポート（Import Devices）] または [クレデンシャルプロファイル（Credential Profile）] を使用して、自律 AP を手動で追加する必要があります。

デバイスのディスカバリ プロセスは、次に示す順序で実行されます。Cisco EPN Manager はディスカバリの実行時に、デバイスの到達可能性状態（[到達可能（Reachable）]、[ping 到達可能（Ping Reachable）]、または [到達不能（Unreachable）]）を設定します。状態の詳細については、「デバイスの到達可能性状態と管理状態 （34 ページ）」を参照してください。

1. Cisco EPN Manager は、ICMP ping を使用して、デバイスに到達可能であるかどうかを判別します。デバイスに到達できない場合、到達可能状態は [到達不能（Unreachable）] に設定されます。
2. サーバは、SNMP 通信が可能かどうかをチェックします。

- ICMP がデバイスに到達可能で、SNMP 通信が不可能な場合、その到達可能性状態は [ping 到達可能（Ping Reachable）] に設定されます。
- ICMP と SNMP の両方がデバイスに到達できる場合、その到達可能性状態は [到達可能（Reachable）] です。

3. デバイスの Telnet および SSH クレデンシャルが確認されます。クレデンシャルに障害が起きた場合は、障害に関する詳細が [ネットワークデバイス（Network Devices）] テーブルの [最後のインベントリ収集ステータス（Last Inventory Collection Status）] 列に表示されます（たとえば、「**Wrong CLI Credentials**」など）。到達可能性の状態は変更されません。
4. Cisco EPN Manager が SNMP を使用して必要な通知を受信できるように、デバイス設定が変更されて、トラップの受信者が追加されます。
5. インベントリ収集プロセスが開始され、すべてのデバイス情報が収集されます。
6. Web GUI にすべての情報（ディスカバリが完全に成功したか、部分的に成功したかなど）が表示されます。

（注） Cisco EPN Manager がデバイスの SNMP 読み取り/書き込みクレデンシャルを検証すると、デバイス ログが更新され、Cisco EPN Manager（IP アドレスで識別される）によって構成が変更されたことが示されます。

SNMP 通信の確認

デバイスの到達可能性の状態が [ping到達可能（Ping Reachable）] に設定されている場合は、次の手順を実行します。

（注） Cisco NCS 2000 デバイスの場合は、SNMP のクレデンシャルに加えて（または代わりに）TL1 のクレデンシャルを確認します。

ステップ 1 Cisco EPN Manager によってデバイスの検証に使用されるクレデンシャルが正しいことを確認します。

ステップ 2 デバイス上で SNMP が有効になっており、デバイスに設定されている SNMP 資格情報が、Cisco EPN Manager で設定されている資格情報と一致することを確認します。

ステップ 3 管理対象デバイスと Cisco EPN Manager サーバ間での SNMP パケットの転送に関与するすべてのネットワーク デバイスのセキュリティ設定（デフォルト動作）により、SNMP パケットがドロップされているかどうかを確認します。

検出されたデバイスの管理 IP アドレス タイプ（IPv4/IPv6）の指定

検出されたデュアルホーム（IPv4/IPv6）デバイスでは、Cisco EPN Manager が管理 IP アドレスとして IPv4 アドレスまたは IPv6 アドレスを使用するかどうかを指定します。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）] > [検出（Discovery）]** を選択します。

ステップ 2 [管理アドレスに対する IPv4/IPv6 設定（IPv4/IPv6 Preference for Management Address）] ドロップダウンリストから [v4] または [v6] のいずれかを選択します。

ステップ 3 [保存（Save）] をクリックします。

クイック ディスカバリの実行

単一のシードデバイスを使用して ping スイープを実行する場合には、この方法を使用します。デバイス名、SNMP コミュニティ、シードの IP アドレスおよびサブネット マスクのみが必要です。構成管理機能の使用を計画している場合は、プロトコル、ユーザ名、パスワード、およびイネーブル パスワードを入力する必要があります。

始める前に

デバイスが正しく設定されていることを確認するには、デバイスをモデル化してモニタできるように設定する （19 ページ）を参照してください。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ディスカバリ（Discovery）]** の順に選択して、ウィンドウ右上の [クイック ディスカバリ（Quick Discovery）] リンクをクリックします。

ステップ 2 少なくとも、名前、SNMP コミュニティ、シードの IP アドレス、およびサブネットマスクを入力します。

ステップ 3 [今すぐ実行（Run Now）] をクリックします。

次のタスク

結果を表示するには、[ディスカバリ ジョブ インスタンス（Discovery Job Instances）] 領域の、[ジョブ（Job）] ハイパーリンクをクリックします。

カスタマイズされたディスカバリ設定でのディスカバリの実行

Cisco EPN Manager は、ディスカバリ プロファイルを使用してネットワーク デバイスを検出できます。ディスカバリ プロファイルには、ネットワーク要素を検索し、それらに接続してインベントリを収集する方法を Cisco EPN Manager に指示する設定のコレクションが含まれています。たとえば、Cisco EPN Manager に CDP、LLDP、OSPF を使用してデバイスを検出することや、単純な ping スイープの実行を指示できます（ping スイープの結果の例は「ping スイープのサンプルの IPv4 IP アドレス （10 ページ）」に記載されています）。フィルタを作成して、

コレクションの微調整、クレデンシャルセットの指定、およびその他のディスカバリ設定を行うこともできます。プロファイルは必要な数だけ作成できます。

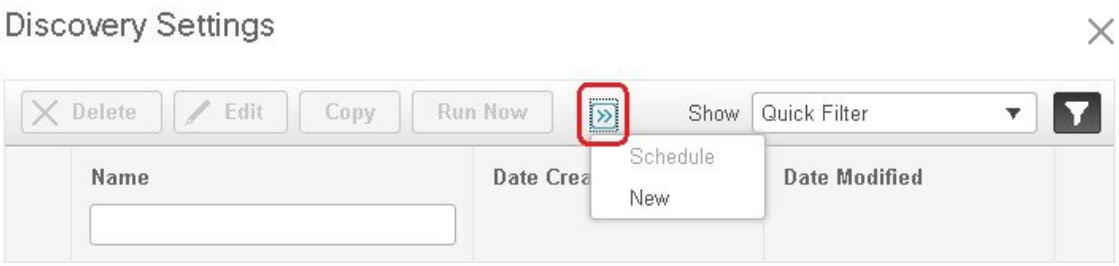
プロファイルの作成後、プロファイルを使用するディスカバリ ジョブを作成し、実行します。ディスカバリジョブの結果は [ディスカバリ（Discovery）] ページで確認できます。ジョブをスケジュールして、定期的に実行を繰り返すこともできます。

始める前に

Cisco EPN Manager がデバイスを検出できるように、デバイスが正しく設定されていることを確認するには、デバイスをモデル化してモニタできるように設定する （19 ページ）を参照してください。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ディスカバリ（Discovery）] を選択して、ウィンドウ右上の [ディスカバリ設定（Discovery Settings）] リンクをクリックします。（[ディスカバリ設定（Discovery Settings）] リンクが表示されない場合は、[クイックディスカバリ（Quick Discovery）] リンクの隣の矢印アイコンをクリックします）。

ステップ 2 [検出設定（Discovery Settings）] ポップアップで、[新規（New）] をクリックします。



ステップ 3 [ディスカバリ設定（Discovery Settings）] ウィンドウに設定を入力します。その設定に関する情報を取得するには、設定の隣にある [?] をクリックします。たとえば、[SNMPv2 クレデンシャル（SNMPv2 Credentials）] の横にある [?] をクリックすると、ヘルプのポップアップにプロトコルと必須の属性がすべて表示されます。

ステップ 4 [今すぐ実行（Run Now）] をクリックしてジョブをすぐに実行するか、[保存（Save）] をクリックして設定を保存し、後で実行するようにディスカバリをスケジュールします。

ping スイープのサンプルの IPv4 IP アドレス

次の表に、ping スイープ結果の例を記載します。

サブネット範囲	ビット数	IP アドレスの数	サンプルのシード IP アドレス	開始 IP アドレス	終了 IP アドレス
255.255.240.0	20	4094	205.169.62.11	205.169.48.1	205.169.63.254
255.255.248.0	21	2046	205.169.62.11	205.169.56.1	205.169.63.254

255.255.252.0	22	1022	205.169.62.11	205.169.60.1	205.169.63.254
255.255.254.0	23	510	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.0	24	254	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.128	25	126	205.169.62.11	205.169.62.1	205.169.63.127
255.255.255.192	26	62	205.169.62.11	205.169.62.1	205.169.63.62
255.255.255.224	27	30	205.169.62.11	205.169.62.1	205.169.63.30
255.255.255.240	36	18	205.169.62.11	205.169.62.1	205.169.63.14
255.255.255.248	29	6	205.169.62.11	205.169.62.9	205.169.63.14
255.255.255.252	30	2	205.169.62.11	205.169.62.9	205.169.63.10
255.255.255.254	31	0	205.169.62.11		
255.255.255.255	32	1	205.169.62.11	205.169.62.11	205.169.62.11

例：ディスカバリを使用した光デバイスの追加

次の例に、シードデバイスと OTS プロトコルを使用して Cisco NCS 2000 デバイスを検出する方法を示します。

始める前に

デバイスをモデル化してモニタできるように設定する （19 ページ）を参照して、光デバイスが正しく設定されていることを確認します。

ステップ 1 **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[検出（Discovery）]** を選択して、ウィンドウ右上の [ディスカバリ設定（Discovery Settings）] リンクをクリックします。

ステップ 2 [ディスカバリ設定（Discovery Settings）] ウィンドウで、[新規（New）] をクリックして新しい検出プロファイルを作成します。

a) ディスカバリ プロファイル名（**NCS2k_3_OTS** など）を入力します。

b) OTS プロトコルのシード デバイスとホップ カウントの情報を入力します。

1. [詳細プロトコル（Advanced Protocols）] の横にある矢印をクリックして検出プロトコルリストを開きます。
2. [OTS トポロジ（OTS Topology）] の横にある矢印をクリックして OTS プロトコルウィンドウを開きます。
3. [OTSを有効にする（Enable OTS）] チェックボックスをオンにします。
4. [行の追加（Add Row）]（[+]）アイコンをクリックします。
5. シード デバイスの IP アドレスとホップ カウント（例：**209.165.200.224** と **3**）を入力し、[保存（Save）] をクリックしてシード デバイス情報を追加します。

6. OTS プロトコル ウィンドウで [保存（Save）] をクリックしてウィンドウを閉じます。必要に応じて、OTS プロトコル ウィンドウの外側をクリックしてウィンドウを閉じます。

c) Cisco NCS 2000 シード デバイスの TL1 デバイス クレデンシャルを入力します。

1. [クレデンシャル設定（Credential Settings）] 領域で、[TL1 クレデンシャル（TL1 Credential）] の横にある矢印をクリックして TL1 クレデンシャルウィンドウを開きます。
2. [行の追加（Add Row）]（[+]）アイコンをクリックします。
3. シードデバイスの IP アドレス、ユーザ名、パスワード、および、必要に応じて、プロキシ IP アドレスを入力します。
4. セキュア TL1 アクセスの場合は [SSH] ドロップダウンリストから [有効化（Enabled）] を選択します。非セキュア TL1 の場合は、[無効化（Disabled）] を選択します。
5. [保存（Save）] をクリックしてクレデンシャル情報を追加します。
6. TL1 クレデンシャル ウィンドウで [保存（Save] をクリックしてウィンドウを閉じます。必要に応じて、TL1 クレデンシャル ウィンドウの外側をクリックしてウィンドウを閉じます。

ステップ 3 [保存（Save）] をクリックして新しいディスカバリ プロファイルを保存します。新しい **NCS2k_3_OTS** プロファイルが [ディスカバリ設定（Discovery Settings）] ウィンドウに追加されます。

（注） エラー メッセージが表示された場合は、プロトコルが有効になっていることを確認してください（これは一般的なエラーです）。

ステップ 4 [NCS2k_3_OTS] を選択し、[今すぐ起動（Run Now）] をクリックしてディスカバリ ジョブを開始します。

ステップ 5 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ディスカバリ（Discovery）]** を選択して、ジョブの結果を確認します。

CSV ファイルを使用したデバイスのインポート

デバイスをインポートする既存の管理システムがある場合、またはスプレッドシートに異なる値を指定する場合は、CSV ファイルを使用してデバイスを追加します。

• CSV ファイルの作成 （12 ページ）
• CSV ファイルのインポート （13 ページ）

CSV ファイルの作成

次の手順に従って、CSV ファイルを作成します。

ステップ 1 [一括インポート（Bulk Import）] ダイアログボックスで使用可能なテンプレートを使用して、一括インポート CSV ファイルを作成します。ダイアログボックスを開くには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択し、[ネットワークデ

バイス（Network Devices）]テーブルの上にある＋アイコンをクリックし、[一括インポート（Bulk Import）]を選択します。[一括デバイス追加サンプル テンプレート（bulk device add sample template）] を使用します。

ステップ 2 各種フィールドの意味と必要なフィールドを確認するには、Web GUI にある情報を使用します。この情報は、1 つのデバイスを追加する場合でも、デバイスを一括して追加する場合でも同じです。この情報を取得するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択し、[ネットワークデバイス（Network Devices）] テーブルの上にある＋アイコンをクリックし、[デバイスの追加（Add Device）] を選択します。必須フィールドはアスタリスクで示されます。説明が必要なフィールドの横には [?] アイコンが表示されます（[?] アイコンにカーソルを置くと、フィールドの詳細が表示されます）。

ステップ 3 作業が完了したら、変更を保存し、ファイルの場所を書き留めておきます。これにより、「CSV ファイルのインポート （13 ページ）」の説明に従ってインポートすることができます。

CSV ファイルのインポート

CSV ファイルを使用してデバイスをインポートするには、次の手順に従います。

始める前に

デバイスが正しく設定されていることを確認するには、デバイスをモデル化してモニタできるように設定する （19 ページ）を参照してください。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] を選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）]テーブルの上にある＋アイコンをクリックし、[一括インポート（Bulk Import）] を選択します。

ステップ 3 [一括インポート（Bulk Import）] ダイアログで、次の手順を実行します。

a) [操作（Operation）] ドロップダウンリストで [デバイス（Device）] が選択されていることを確認します。

b) [参照（Browse）]をクリックしてCSVファイルに移動し、[インポート（Import）]をクリックします。

（注） 一括デバイス追加サンプル テンプレートのダウンロードの一環としてすでにエクスポート済みの CSV ファイルを選択します。csv ファイルは手動で編集しないでください。

ステップ 4 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** の順に選択して、インポートのステータスを確認します。

ステップ 5 矢印をクリックして、ジョブの詳細を展開し、インポート ジョブの詳細と履歴を表示します。問題が発生した場合は、追加されたデバイスの検証と問題のトラブルシューティング （36 ページ）を参照してください。

手動によるデバイスの追加（新規デバイス タイプまたはデバイス シリーズ）

新しいデバイス タイプを追加して、それらの設定をデバイスのグループに適用する前にテストするには、次の手順に従います。

始める前に

デバイスが正しく設定されていることを確認するには、デバイスをモデル化してモニタできるように設定する （19 ページ）を参照してください。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）] の順に選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルの上にある ＋ アイコンをクリックし、[デバイスの追加（Add Device）] を選択します。

ステップ 3 [デバイスの追加（Add Device）] ダイアログボックスで、必須フィールドに値を入力します。フィールドの横にある [?] をクリックすると、そのフィールドの説明が表示されます。

（注） （ほとんどの Cisco NCS デバイスなどの）デバイスには、Telnet/SSH 情報が必須です。Telnet/SSH（60 秒）と SNMP（10 秒）のデフォルト タイムアウトがネットワーク遅延に基づいてデバイスにより異なる場合でも、デバイスを構成できます。

[管理（Administration）] > [設定（Settings ）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [インベントリ（Inventory）] ページで [SSH の厳格なホスト チェック キー（Strict host check key for SSH）] チェック ボックスを選択して、追加したデバイスの SSH キーの検証を強制することができます。これにより、Telnet/SSH のパラメータの下でアルゴリズムおよび SSH キーを指定することができます。

デバイスを追加するときにアルゴリズムと SSH キーを手動で指定しない場合は、[管理（Administration）] > [設定（Settings ）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [インベントリ（Inventory）] ページで [最初の使用で SSH キーを信頼する（Trust SSH key on first use）] チェック ボックスを選択します。その最初の通信中にデバイスから送信された SSH キーは、信頼されデバイスのクレデンシャルに追加されます。この保存されたキーは、その後デバイスが追加されたときに自動入力され、検証に使用されます。

ステップ 4 （任意）デバイスを追加する前にクレデンシャルを確認するには、[クレデンシャルの確認（Verify Credentials）] をクリックします。

ステップ 5 [追加（Add）] をクリックして、指定した設定でデバイスを追加します。

（注） NCS 2000 デバイスの場合は、TL1 ユーザにスーパーユーザ プロファイルを提供します。提供しないとデバイスが [警告付き完了（Completed with Warning）] ステータスになり、[シャーシビュー（Chassis View）] で [設定（Configuration）] > [セキュリティ（Security）] タブを利用できなくなります。

（注） Telnet/SSH クレデンシャルを指定しないと、一部のインベントリデータのみが収集される場合があります。

（注） NCS 2000 デバイスの場合、[シングルセッション TL1 を有効にする（Enable Single Session TL1）] の設定はリリース 11.0 以降を実行しているデバイスに対してのみ有効です。

（注） Cisco EPN Manager は、デフォルトでは UCS を自己署名証明書で承認しません。ユーザがこれを手動で有効にするには、*/opt/CSCOlumos/xmp_inventory/xde-home/inventoryDefaults/ncsCIMC.def* ファイルに次の行を追加します。

```
<default attribute="HTTPS_TRUST_CONDITION">always</default>

<default attribute="HTTPS_HOSTNAME_VERIFICATION_STRATEGY">allow_all</default>
```

（注） 各デバイスには、一意の SNMP エンジン ID が必要です。同じエンジン ID が 2 つのデバイスで使用されている場合、競合するデバイスの詳細でアラームが発生します。SNMP v3 ログイン情報でデバイスを管理する場合にのみ、SNMP エンジン ID の一意のチェックが行われます。

例：単一の Cisco NCS 2000 または NCS 4000 シリーズ デバイスの追加

Cisco NCS 2000 シリーズは TL1 ベースのデバイスであり、Cisco EPN Manager は TL1 プロトコルを使用してこれらのデバイスと通信します。NCS2K デバイスの推奨 TL1 アクティブセッションの数は 15 以下です。アクティブセッションの数が 15 を超えると、Cisco EPN Manager では詳細または事後対応型のインベントリ操作でデバイスから TL1 イベントを受信できなくなる場合があります。一方、Cisco NCS 4000 シリーズのデバイスは Cisco IOS XR デバイスであり、Cisco EPN Manager は SNMP および Telnet/SSH プロトコルを使用してこれらのデバイスと通信します。

始める前に

Cisco NCS デバイスが正しく設定されていることを確認するには、デバイスをモデル化してモニタできるように設定する （19 ページ）を確認してください。

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルの上にある ＋ アイコンをクリックし、[デバイスの追加（Add Device）] を選択します。

ステップ 3 [デバイスの追加（Add Device）] ダイアログボックスで、必須フィールドに値を入力します。フィールドの横にある [?] をクリックすると、そのフィールドの説明が表示されます。

- Cisco NCS 2000 シリーズおよび Cisco ONS 15454：TL1 パラメータを入力します
- Cisco NCS 4000 シリーズ：SNMP および Telnet/SSH のパラメータを入力します。

ステップ 4 [クレデンシャルの確認（Verify Credentials）] をクリックして Cisco EPN Manager がデバイスに到達できることを検証します。

ステップ 5 [追加（Add）] をクリックして、デバイスを Cisco EPN Manager に追加します。

例：プロキシ設定を使用した ENE としてのネットワーク要素の追加

特定のネットワーク要素に送信したメッセージは、ネットワーク内の他の NE を通過する必要があります。メッセージを渡すには、1 つ以上のノードがゲートウェイ ネットワーク要素（GNE）となり、ネットワーク内の他の NE に接続することができます。TL1 セッションを確立して別のノードに送信する必要があるコマンドを入力すると、ノードは GNE になります。別のノードから処理のために TL1 メッセージを受け取るノードがエンドポイント ネットワーク要素（ENE）です。ENE からのメッセージは、GNE を通じてネットワーク内の別の NE に送信されます。

始める前に

デバイスが正しく設定されていることを確認するには、デバイスをモデル化してモニタできるように設定する （19 ページ）を確認してください。

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルの上にある ＋ アイコンをクリックし、[デバイスの追加（Add Device）] を選択します。

ステップ 3 [デバイスの追加（Add Device）] ダイアログ ボックスで、追加する ENE の IP アドレスまたは DNS 名を [一般パラメータ（General Parameters）] の下に入力します。そのフィールドの説明を確認するには、フォールドの横にある [?] をクリックします。

ステップ 4 **[TL1パラメータ（TL1 Parameters）]** に、ENE として使用するノードのプライマリおよびセカンダリ プロキシ IP アドレスを入力します。

（注） セカンダリ プロキシ IP アドレスは任意であり、プライマリ プロキシに障害が発生した場合にのみアクティブ化されます。

ステップ 5 [クレデンシャルの確認（Verify Credentials）] をクリックして Cisco EPN Manager がデバイスに接続できないことを検証します。

ステップ 6 [追加（Add）] をクリックして、デバイスを Cisco EPN Manager に追加します。

例：Cisco NCS 2000 シリーズ デバイスでシングル セッションを有効にする

Cisco NCS 2000 シリーズのデバイスは TL1-ベースのデバイスであり、Cisco EPN Manager は TL1 プロトコルを使用してこれらのデバイスと通信します。新しく追加されたデバイスを編集するか、既存の NCS 2000 デバイスを設定して、シングル セッションでマシン（EMS）アカウントを制限できます。

ステップ 1 **[インベントリ（Inventory）]>[デバイス管理（Device Management）]>[ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 デバイスを選択して [編集（Edit）] アイコンをクリックします。[デバイスの編集（Edit Device）] ウィンドウが表示されます。

ステップ 3 新しいデバイスまたは既存のデバイスでシングル セッションを編集するには、次のパラメータを設定します。

a) [TL1 パラメータ（TL1 Parameters）] の下にある [シングルセッション TL1 を有効にする（Enable Single Session TL1）] チェックボックスをオンにします。

b) 必須パラメータを入力します。

c) 次のいずれかを実行します。

- データベース上のシングル セッション設定のみを更新する場合は、[更新（Update）] をクリックします。
- データベースとデバイスの両方でシングルセッション設定を更新する場合は、[更新と同期（Update & Sync）] をクリックします。

ステップ 4 （オプション）一括インポート操作および一括編集操作でシングル セッションを編集することもできます。

（注） デフォルトにより、一括編集ではシングルセッションが無効になっています。[シングルセッションTL1を有効にする（Enable Single Session TL1）] チェック ボックスをオンにして、インポート先のすべてのデバイスに対して有効にする必要があります。[一括インポート（Bulk Import）] オプションを選択すると、シングル セッション フラグが影響を受ける可能性があります。

次のタスク

次の手順で有効なシングル セッションを確認します。

1. Cisco Transport Controller を起動し、シングル セッションが有効になっているデバイスを選択します。
2. **[プロビジョニング（Provisoning）] > [セキュリティ（Security）] > [アクティブログイン（Active Logins）]** を選択して、シングル セッションを含むアクティブ デバイスをすべて表示します。シングル セッションが無効になっているデバイスは表示されません。

（注） クレデンシャルの確認は、シングル セッション タスク実行中の唯一の例外です。

インベントリはどのように収集されていますか。

デバイスが追加されて検出されると、Cisco EPN Manager は物理的および論理的なインベントリ情報を収集し、データベースに保存します。次の表に、インベントリ収集がどのようにトリガーされるかについて示します。

インベントリ収集のトリガー	説明
着信イベントに応答して	Cisco EPN Manager は、NE の変更を通知する着信 NE SNMP トラップ、syslog、または TL1 メッセージを受信します。着信イベントには、次のようなものがあります。 • デバイス設定の変更を通知する設定変更イベント。これらのイベントは通常、syslog またはトラップです。 • その他のインベントリ イベント（トンネルのアップ/ダウン、リンクのアップ/ダウン、モジュールの入出力など）。 Cisco EPN Manager は、NE のインベントリと状態情報を収集して、データベース内の情報が NE の情報に準拠していることを確認することによって、これらの着信イベントに反応します。ほとんどのイベントは、詳細なインベントリ収集をトリガーします。Cisco EPN Manager は、変更イベントに関連するデータのみを収集します。その他のイベントは、NE の物理および論理インベントリの完全な収集（同期）をトリガーします。Cisco EPN Manager が収集するデータは、Cisco EPN Manager で定義されているメタデータとともに、着信イベントの情報によって決まります。Cisco EPN Manager のメタデータは、収集される情報を細かく調整するために、迅速なイベント、反応的なインベントリ、詳細なポーリングといったメカニズムを組み合わせて使用します。 たとえば、Cisco EPN Manager が GMPLS トンネル状態変更イベントを受信した場合は、ODU トンネルインベントリ情報を収集して、トンネルのミッドポイントと Z エンドポイントを検出します。
オン デマンド	ユーザは、次の場所から即時にインベントリ収集（[同期（Sync）] と呼ばれる）を実行できます。 • [ネットワーク デバイス（Network Devices）] ページ：（チェックボックスをオンにして）1 つ以上のデバイスを選択し、[同期（Sync）] をクリックします。 • [デバイス 360（Device 360）] ビュー：**[アクション（Actions）]** > **[今すぐ同期（Sync Now）]** を選択します。 デバイスのインベントリの即時収集（同期）を参照してください。
スケジュール（日単位）	通常のインベントリ収集は一晩中実行されます。十分な権限を持つユーザは、**[管理（Administration）]** > **[ダッシュボード（Dashboards）]** > **[ジョブ ダッシュボード（Job Dashboard）]** を選択し、[システム ジョブ（System Jobs）] > [インベントリおよびディスカバリ ジョブ（Inventory and Discovery Jobs）] を選択して、インベントリが収集された日時と収集ジョブの状況を確認できます。

デバイスをモデル化してモニタできるように設定する

（注） 異なるデバイス ファミリのサポート対象の構成については、『Cisco Evolved Programmable Network Manager のサポート対象デバイス』を参照してください。

デバイスが Cisco EPN Manager で完全なユーザ権限（特権 EXEC モード）で管理されていることを確認します。

にイベントを転送するようにデバイスを設定する Cisco EPN Manager

Cisco EPN Manager がデバイスに問い合わせてイベントと通知を受信できるようにするには、イベントを Cisco EPN Manager サーバに転送するようにデバイスを設定する必要があります。ほとんどのデバイスにとって、これは SNMP トラップと syslog を転送するように設定する必要があることを意味します。

それ以外のデバイス（一部の光デバイスなど）の場合は、TL1 メッセージを転送するようにデバイスを設定する必要があることを意味します。

ハイ アベイラビリティ展開を使用している場合は、イベントをプライマリ サーバとセカンダリ サーバの両方に転送するようにデバイスを設定する必要があります（仮想 IP アドレスを使用していない場合。HA での仮想 IP アドレッシングの使用を参照）。

ほとんどの場合、この設定を行うには **snmp-server host** コマンドを使用する必要があります。さまざまなデバイスのオペレーティングシステムの前提条件が一覧表示された本書内のトピックを参照してください。

（注） デバイスで詳細なインベントリを有効にするために必要な設定については、Cisco Evolved Programmable Network Manager のサポート対象 Syslogを参照してください

必要な設定：Cisco IOS および IOS-XE デバイス オペレーティング システム

```
snmp-server host server_IP
snmp-server community public-cmty RO
snmp-server community private-cmty RW
snmp-server ifindex persist

logging server_IP
logging on
logging buffered 64000 informational

logging source-interface interface_name
logging trap informational
logging event link-status default
```

Telnet/SSH コマンド応答の遅延を回避するために、ドメイン ルックアップを無効にします。

```
no ip domain-lookup
```

SSH の有効化

```
crypto key generate rsa
ip ssh rsa keypair-name keypair-name
crypto key generate rsa usage-keys label key-label modulus modulus-size
ip ssh version [1 | 2]
```

VTY オプションを設定します。

```
line vty <number of vty>
exec-timeout
session-timeout
transport input ssh (requird only if ssh is used)
transport output ssh (required only if ssh isused)
```

CFM モデリングを有効にします。

```
snmp-server view all 1.3.111.2.802.1.1.8 included
```

SNMPv2 の場合のみ、コミュニティ ストリングを設定します。

```
snmp-server community ReadonlyCommunityName RO
```

SNMPv3 の場合のみ、次の設定を行います。

```
snmp-server user User Group v3 auth sha Password priv des Password
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group

snmp-server group Group v3 priv read v1default write v1default notify v1default
snmp-server group Group v3 priv
snmp-server group Group v3 priv notify epnm read epnm
```

（注）

- デバイスが Cisco EPN Manager でシームレスに動作するには、デバイスで生成/設定された SNMP EngineID がネットワーク内で一意である必要があります。
- クレデンシャルが機能するように、SNMP EngineID をデバイスで再設定する場合は SNMP ユーザを再作成する必要があります。

SNMP インターフェイスの応答時間を改善するために、次の設定を使用してグローバル レベルでキャッシュを設定します。

```
snmp-server cache
```

syslog は、アラームおよびイベント管理のために Cisco EPN Manager によって使用されます。NTP 設定により、Cisco EPN Manager はイベントの正しいタイムスタンプを確実に受信します。デバイスで syslog を設定するには、次の設定を追加します。

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
update-calendar
logging facility local7
logging Server_IP vrf default severity info [port default]
```

必須の設定：Cisco IOS XR デバイスのオペレーティング システム

```
snmp-server community community_name SystemOwner
snmp-server community community_name RO
snmp-server entityindex persist
snmp-server ifindex persist

logging server_IP
logging on
logging buffered <307200-125000000>

logging source-interface interface_name

logging trap informational
logging events level informational
logging events link-status
logging events link-status software-interfaces

no cli whitespace completion
domain ipv4 host server_name server_IP
```

VTY オプションを設定します。

```
line default
exec-timeout 10 0
session-limit 10
session-timeout 100
transport input ssh
transport output ssh
vty-pool default 0 99 line-template default
```

Telnet と SSH の設定は次のとおりです。

```
telnet ipv4 server max-servers no-limit
telnet vrf default ipv4 server max-servers 100
```

```
ssh server v2
ssh server rate-limit 60
cinetd rate-limit 60
```

Netconf エージェントと XML エージェントを設定します。

```
xml agent tty
netconf agent tty
```

仮想 IP アドレスを持つデバイスをモニタします。

```
ipv4 virtual address use-as-src-addr
ipv4 virtual address Virtual_IP_Address/Subnet_Mask
```

CFM モデリングを有効にします。

```
snmp-server view all 1.3.111.2.802.1.1.8 included
```

SNMPv2 の場合のみ、コミュニティ ストリングを設定します。

```
snmp-server community ReadonlyCommunityName RO SystemOwner
```

SNMPv3 の場合のみ、次の設定を行います。

```
snmp-server user User Group v3 auth sha encrypted Password priv des56 encrypted
Password SystemOwner
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group
snmp-server group Group v3 priv read v1default write v1default notify v1default
```

（注） または、**[設定（Configuration）] > [テンプレート（Templates）] > [機能およびテクノロジー（Features & Technologies）]** に移動できます。左側の [テンプレート（Templates）] タブで **[CLIテンプレート（CLI Templates）] > [システムテンプレート - CLI（System Templates - CLI）]** を選択し、Default_Manageability_Config-IOS-XR テンプレートを展開して Cisco EPN Manager のディスカバリに必要な IOS-XR デバイス設定を行います。

（注）

- デバイスが Cisco EPN Manager でシームレスに動作するには、デバイスで生成/設定された SNMP EngineID がネットワーク内で一意である必要があります。
- クレデンシャルが機能するように、SNMP EngineID をデバイスで再設定する場合は SNMP ユーザを再作成する必要があります。

次の設定を行って、SNMP インターフェイス統計情報の応答時間を改善します。

```
snmp-server ifmib stats cache
```

リンクダウン シナリオが確実にキャプチャされるように、仮想インターフェイスの SNMP トラップを設定します。

```
snmp-server interface subset 2 regular-expression Forty*
notification linkupdown
!
snmp-server interface subset 3 regular-expression Ten*
notification linkupdown
!
```

```
snmp-server interface subset 1 regular-expression Hun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression TwoHun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression FourHun*
notification linkupdown
```

syslog は、アラームおよびイベント管理のために Cisco EPN Manager によって使用されます。NTP の設定によって、Cisco EPN Manager がイベントの正しいタイムスタンプを確実に受信します。デバイスで syslog を設定するには、次の設定を追加します。

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
logging facility local7
logging Server_IP vrf name
```

すべての光データ ユニット（ODU）コントローラでパフォーマンス管理を有効にします。

```
controller oduX R/S/I/P
per-mon enable
```

タンデム接続モニタリング（TCM）のパフォーマンス管理を有効にします。

```
tcm id {1-6}
perf-mon enable
```

Cisco EPN Manager から Cisco Transport Controller（CTC）を開くには、HTTP/HTTPS サーバを有効化します。

```
http server ssl
```

[設定アーカイブ（Configuration Archive）]の使用を予定している場合は、デバイスをセキュアデバイスとして設定する必要があります。CTC からデバイスを設定する手順は次のとおりです。

1. **[プロビジョニング（Provisioning）]** > **[セキュリティ（Security）]** > **[アクセス（Access）]** を選択します。
2. [EMSアクセス（EMS Access）] を [セキュア（secure）] に設定します。

（注）

- MPLS パッケージと K9 パッケージの両方がデバイスにインストールされていることを確認してください。
- Cisco IOS XR Manageability Package（MGBL）をインストールしてください。
- または、CLI テンプレートを使用して上記の前提条件をすべて適用することもできます。**[設定（Configuration）]** > **[テンプレート（Templates）]** > **[機能およびテクノロジー（Features & Technologies）]** に移動します。左ペインの [テンプレート（Templates）] タブで、**[CLIテンプレート（CLI Templates）]** > **[システムテンプレート - CLI（System Templates - CLI）]** を選択し、**Default_Manageability_Config** テンプレートを展開します。
- 詳細については、『Supported Traps』と『Supported Syslogs』を参照してください。.

必須設定：Cisco NCS シリーズ デバイス

必須設定：Cisco NCS 4000 シリーズ デバイス

注目 次の手順を実行する前に、MPLS パッケージと K9 パッケージの両方がデバイスにインストールされていることを確認してください。

- Cisco EPN Manager は SSH を使用して、Cisco NCS 4000 シリーズ デバイスとの通信を保護します。SSH を有効にするには、デバイスで次の構成時の設定を適用します。

```
ssh server v2
ssh server rate-limit 600
```

- MPLS トラフィック エンジニアリング設定モードで、イベント ロギングを有効化します。

```
mpls traffic-eng logging events all
```

- VTY オプションを設定します。

```
line default
exec-timeout 10 0
session-limit 10
session-timeout 100
transport input ssh
transport output ssh
vty-pool default 0 99 line-template default
```

- LMP リンクを設定します。

```
router-id ipv4 unicast local IP address
```

local IP address はデバイスの IP アドレスです。

- Netconf エージェントと XML エージェントを設定します。

```
xml agent tty
netconf agent tty
```

- デバイスで SNMP を設定します。

```
snmp-server host server_IP
snmp-server community public RO SystemOwner
snmp-server community private RW SystemOwner
snmp-server ifindex persist
```

SNMPv2 または SNMPv3 を使用できます。

  - SNMPv2 の場合のみ、コミュニティ ストリングを設定します。

```
snmp-server community ReadonlyCommunityName RO SystemOwner
```

  - SNMPv3 の場合のみ、次の設定を行います。

```
snmp-server user User Group v3 auth sha encrypted Password priv des56 encrypted
 Password SystemOwner
snmp-server view Group 1.3.6 included
snmp-server group Group v3 priv notify Group read Group
```

ポーリングおよび設定ビューを設定するには、次のいずれかの設定オプションを選択します。

- SNMPv3 のデフォルト設定（SNMPv3 のポーリングとデフォルト設定の表示に使用）：

  ```
  snmp-server group Group v3 priv read v1default write v1default notify
  v1default
  ```

- SNMPv3 固有の設定：
  - SNMPv3 ポーリングの場合のみ：

    ```
    snmp-server group Group v3 priv
    ```

  - SNMPv3 セット、ポーリング、およびトラップ/通知の設定を表示する場合：

    ```
    snmp-server group Group v3 priv notify epnm read epnm write epnm
    ```

  - SNMPv3：LLDP MIB OID 設定を表示する場合：

    ```
    snmp-server view Group 1.0.8802.1.1.2 included
    ```

LAG リンクを表示するには、デバイスに次の設定を追加します。

```
snmp-server view all 1.0.8802 included
```

（注） 最初の行の *User* と *Group* は、値を入力するために必要な 2 つの異なる変数です。

- 設定 `Snmp-server ifmib stats cache` を使用して、SNMP インターフェイスの統計情報の応答時間を改善するように stats コマンドを設定します。
- リンクダウンシナリオが確実にキャプチャされるように、仮想インターフェイスの SNMP トラップを設定します。

```
snmp-server interface subset 1 regular-expression Hun*
notification linkupdown
!
snmp-server interface subset 2 regular-expression Forty*
notification linkupdown
!
snmp-server interface subset 3 regular-expression Ten*
notification linkupdown
!
```

- syslog は、アラームおよびイベント管理のために Cisco EPN Manager によって使用されます。NTP の設定によって、Cisco EPN Manager がイベントの正しいタイムスタンプを確実に受信します。デバイスで syslog を設定するには、次の設定を追加します。

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
```

```
ntp server NTP_Server
logging facility local7
logging Server_IP vrf name
```

次の点に注意してください。

- タイムゾーンを指定するときには、タイムゾーンの略語と協定世界時（UTC）との時間差（時間単位）を入力します。たとえば、ロサンゼルスにあるデバイスのタイムゾーンを指定するには、`clock timezone PDT -7` と入力します。
- *Server_IP* を、ホスト Cisco EPN Manager の IP アドレスに置き換えます。

- 仮想 IP アドレスを設定します。

```
ipv4 virtual address NCS4K_Virtual_IP_Address/Subnet_Mask
ipv4 virtual address use-as-src-addr
```

（注） *NCS4K_Virtual_IP_Address* と *Subnet_Mask* は、スラッシュで区切られた 2 つの異なる変数です。必ず両方の変数値を入力してください。

- すべての光データユニット（ODU）コントローラでパフォーマンス管理を有効にします。

```
controller oduX R/S/I/P
per-mon enable
```

- Cisco IOS リリース 6.1.42 以降を実行している Cisco NCS4000 デバイスの光学コントローラのリンク ステータス メッセージのイベント ロギングを有効にします。

```
controller Optics <x/y/z/w>
logging events link-status
```

- タンデム接続モニタリング（TCM）のパフォーマンス管理を有効にします。

```
tcm id {1-6}
perf-mon enable
```

- サービス要求を受け入れるための Telnet または SSH レート制限を設定します。
  - Telnet の場合、*1* 秒あたりに受け付ける要求の数（1 ～ 100、デフォルトは 1）を設定します。

    ```
    cinetd rate-limit 100
    ```

  - SSH の場合、*1* 分あたりに受け付ける要求の数（1 ～ 600、デフォルトは 60）を設定します。

    ```
    ssh server rate-limit 600
    ```

- Cisco EPN Manager（[デバイス 360（Device 360）] ビュー）から Cisco Transport Controller（CTC）を開くには、HTTP/HTTPS サーバを有効化します。

```
http server ssl
```

- [設定アーカイブ（Configuration Archive）] 機能を使用する予定の場合は、デバイスを [保護済み（secured）] として設定する必要があります。これを CTC から行うには、次のようにします。

  1. **[プロビジョニング（Provisioning）] > [セキュリティ（Security）] > [アクセス（Access）]** を選択します。
  2. EMS アクセスを [セキュア（secure）] に設定します。

- 複数の Cisco NCS 4000 シリーズ デバイスが同時に情報を送信していることが原因でパフォーマンス上の問題が発生した場合は、*1* 秒あたりの Telnet セッション数を増やします。

```
cinetd rate-limit 100
```

必須設定：Cisco NCS 4200 シリーズ デバイス

- Cisco EPN Manager は SSH を使用して、Cisco NCS 4200 シリーズ デバイスとの通信を保護します。SSH を有効にするには、デバイスで次の構成時の設定を適用します。

  - ```
    enable
    configure terminal
    hostname name
    ip domain-name name
    crypto key generate rsa
    ```

  - ```
    enable
    configure terminal
    ip ssh rsa keypair-name keypair-name
    crypto key generate rsa usage-keys label key-label modulus modulus-size
    ip ssh version [1 | 2]
    ```

- VTY オプションを設定します。

```
line vty <#>
exec-timeout
session-timeout
transport input ssh
transport output ssh
```

- デバイスで SNMP を設定します。

```
snmp-server host server_IP
snmp-server community public RO
snmp-server community private RW
```

  SNMPv2 または SNMPv3 を使用できます。

  - SNMPv2 の場合のみ、コミュニティ ストリングを設定します。

    ```
    snmp-server community ReadonlyCommunityName RO
    ```

  - SNMPv3 の場合のみ、次の設定を行います。

    ```
    snmp-server user User Group v3 auth sha Password priv des  Password
    snmp-server view Group 1.3.6 included
    snmp-server group Group v3 priv notify Group
    ```

ポーリングおよび設定ビューを設定するには、次のいずれかの設定オプションを選択します。

- SNMPv3 のデフォルト設定（SNMPv3 のポーリングとデフォルト設定の表示に使用）：

```
snmp-server group Group v3 priv read v1default write v1default notify
v1default
```

- SNMPv3 固有の設定：
  - SNMPv3 ポーリングの場合のみ：

```
snmp-server group Group v3 priv
```

  - SNMPv3 セット、ポーリング、およびトラップ/通知の設定を表示する場合：

```
snmp-server group Group v3 priv notify epnm read epnm
```

  - SNMPv3：LLDP MIB OID 設定を表示する場合：

```
snmp-server view Group 1.0.8802.1.1.2 included
```

（注） 最初の行の *User* と *Group* は、値を入力するために必要な 2 つの異なる変数です。

- 構成 `Snmp-server cache` を使用して SNMP インターフェイスの応答時間を改善するためにグローバル レベルでキャッシュを設定します。
- syslog は、アラームおよびイベント管理のために Cisco EPN Manager によって使用されます。NTP の設定によって、Cisco EPN Manager がイベントの正しいタイムスタンプを確実に受信します。デバイスで syslog を設定するには、次の設定を追加します。

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
update-calendar
logging facility local7
logging Server_IP vrf default severity info [port default]
mpls traffic-eng logging events all
mpls traffic-eng logging lsp setups
mpls traffic-eng logging lsp teardowns
```

次の点に注意してください。

- タイムゾーンを指定するときには、タイムゾーンの略語と協定世界時（UTC）との時間差（時間単位）を入力します。たとえば、ロサンゼルスにあるデバイスのタイムゾーンを指定するには、`clock timezone PDT -7` と入力します。
- *Server_IP* を、ホスト Cisco EPN Manager の IP アドレスに置き換えます。

必要とされる設定の自動プッシュ

新しいデバイス（IOS、IOS-XE、および IOS-XR）がインベントリに追加されたときに、必須のデバイス管理性設定を自動的に適用できます。これにより、Cisco EPN Manager がデバイスを自動的に管理できるようになり、収集の一部が失敗するというインシデントの割合が減少し、デバイスに手動で設定を適用する必要がなくなります。Cisco EPN Manager デバイスの管理性の必須設定は、事前設定されたテンプレートにまとめられています。このテンプレートはデバイス管理性テンプレートとも呼ばれます。

（注） デバイス管理性テンプレートは、既存の設定が存在する場合にそれを上書きします。

テンプレートをデバイスに自動的に展開するには、**[管理（Administration）]** > **[設定（Settings）]** > **[システム設定（System Settings）]** > **[インベントリ（Inventory）]** > **[インベントリ（Inventory）]** を選択し、[デバイス管理性を有効にする（Enable Device Manageability）] チェックボックスをオンにします。デフォルトで、このオプションは有効になっています。このオプションを有効にすると、追加されたデバイスのタイプに基づいて、デバイスの追加時に次のテンプレートのいずれかが展開されます（たとえば、XR デバイスを追加した場合は *AutoDeploy_Manageability_Config-IOS-XR* テンプレートが展開されます）。

- AutoDeploy_Manageability_Config-IOS
- AutoDeploy_Manageability_Config-IOS-XE
- AutoDeploy_Manageability_Config-IOS-XR

これらのテンプレートは **[設定（Configuration）]** > **[テンプレート（Templates）]** > **[機能およびテクノロジー（Features & Technologies）]** > **[CLIテンプレート（CLI Templates）]** > **[システムテンプレート - CLI（System Templates-CLI）]** にあります。

（注） システム定義テンプレートが適切でない場合は、これらのシステムテンプレートに基づいてユーザ定義テンプレートを作成できます。各デバイスタイプの「`/opt/CSCOlumos/conf/ifm/ifm_inventory`」プロパティファイルの下の新しいテンプレート名を更新します。この変更は 5 分後に有効になります。サーバの再起動は必要ありません。

ifm_inventory.properties のエントリを終了します。

```
ifm.inventory.manageability.prerequisite.ios=AutoDeploy_Manageability_Config-IOS
ifm.inventory.manageability.prerequisite.iosxr=AutoDeploy_Manageability_Config-IOS-XR
ifm.inventory.manageability.prerequisite.iosxe=AutoDeploy_Manageability_Config-IOS-XE
```

上記のエントリを更新して、新しいテンプレート名を指定できます。たとえば、ユーザが IOS-XR デバイス用のテンプレート `Updated_AutoDeploy_Manageability_Config-IOS-XR` を追加する場合は、ファイル内のエントリを次のように更新する必要があります。

```
ifm.inventory.manageability.prerequisite.iosxr=Updated_AutoDeploy_Manageability_Config-IOS-XR
```

「変更監査ダッシュボード」（**[モニタ（Monitor）] > [ツール（Tools）] > [変更監査ダッシュボード（Change Audit Dashboard）]** を選択）には、各デバイスの追加とそれに対応するテンプレートの展開の監査ログが表示されます。

制限事項：

SNMP/CLI のタイムアウトを更新すると、デバイスの同期が完了していない状態でもテンプレートがデプロイされます。

必要な設定：Cisco ONS デバイス オペレーティング システム

設定アーカイブ機能を使用することを予定している場合、デバイスをセキュアデバイスとして設定する必要があります。それには、CTC で次の操作を行います。

1. CTC で、**[プロビジョニング（Provisioning）] > [セキュリティ（Security）] > [アクセス（Access）]** の順に選択します。
2. EMS アクセスをセキュアとして設定します。

必須設定：Cisco NCS2K シリーズ デバイス

NCS2K デバイスで設定アーカイブ機能を使用する場合は、HTTP/HTTPS サーバを有効にします。

（注） シングルセッションが有効になっていない、または適用できないデバイスの場合は、次の手順を実行して EPNM で使用する接続数を制限します。

1. $XMP_HOME/xmp_inventory/xde-home/inventoryDefaults/onsTL1.def を開きます。
2. 次のように新しい属性タグを追加します。</test> タグの後の ConnectionCount は実際の番号（5 など）に置き換える必要があります。

   <default attribute="DEVICE_THROTTLING">ConnectionCount</default>

IPv6 デバイスに必要な設定

IPv6 アドレスを使用するデバイスにアクセスするには、次の手順を実行することによって、Cisco EPN Manager サーバ（仮想マシン）で IPv6 アドレスとスタティック ルートを設定します。

1. インターフェイスから ipv6 address autoconfig を削除します。
2. Cisco EPN Manager サーバで IPv6 アドレスを設定します。
3. スタティック ルートを Cisco EPN Manager サーバに追加します。

デバイス上のアーカイブ ロギングの有効化

デバイス上でアーカイブ ロギングを有効にするには、次の手順を実行して、Cisco EPN Manager 上のデバイスに対して詳細なインベントリを有効にします。

Cisco IOS-XR デバイスの場合：

```
logging  <epnm server ip>  vrf default severity alerts
logging  <epnm server ip>  vrf default severity critical
logging  <epnm server ip>  vrf default severity error
logging  <epnm server ip>  vrf default severity warning
logging  <epnm server ip>  vrf default severity notifications
logging  <epnm server ip>  vrf default severity info
snmp-server host <epnm server ip>  traps version 2c public
```

Cisco IOS および IOS-XE デバイスの場合：

```
logging host <epnm server ip>  transport udp port 514
logging host <epnm server ip>  vrf Mgmt-intf transport udp port 514
snmp-server host <epnm server ip>  traps version 2c public
```

クレデンシャルプロファイルを使用したデバイスクレデンシャルの一貫した適用

資格情報のプロファイルは、TL1、HTTP、Telnet/SSH SNMP デバイスの認証情報のコレクションです。デバイスを追加するときは、デバイスを使用する必要があります資格情報のプロファイルを指定できます。これにより、デバイス間で一貫して資格情報の設定を適用できます。

資格情報の変更、デバイスのパスワードの変更などを行う必要がある場合は、設定がプロファイルを使用するすべてのデバイスにわたって更新されるプロファイルを編集できます。

既存のプロファイルを表示するには、[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャルプロファイル（Credential Profiles）] を選択します。

新しいクレデンシャル プロファイルの作成

この手順を使用して、新しいクレデンシャルプロファイルを作成します。次に、そのプロファイルを使用し、製品全体か、または新しいデバイスの追加時に、クレデンシャルを一貫して適用できます。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択します。

ステップ 2 既存のクレデンシャルプロファイルに必要な設定のほとんどがある場合は、それを選択し、[コピー（Copy）] をクリックします。それ以外の場合は、[追加（Add）] をクリックします。

ステップ 3 プロファイル名と説明を入力します。名前と説明が [クレデンシャルプロファイル（Credential Profiles）] ページに表示されるため、クレデンシャルプロファイルが多くなる場合は可能な限り識別しやすい名前と説明にします。

ステップ 4 プロファイルのクレデンシャルを入力します。このプロファイルを使用してデバイスを追加または更新すると、ここで指定した内容がそのデバイスに適用されます。

SNMP 読み取りコミュニティ ストリングは必須です。

ステップ 5 [変更の保存（Save Changes）] をクリックします。

既存のデバイスへの新規または変更されたプロファイルの適用

次の手順を使用して、デバイスを一括編集し、そのデバイスが関連付けられているクレデンシャル プロファイルを変更します。この操作は、デバイスとクレデンシャル プロファイル間の既存の関連付けを上書きします。また、この操作を使用して、デバイス設定を新しい設定と同期させることもできます。

（注） この手順を実行して [**Update and Sync**] を選択する前に、プロファイルのクレデンシャル設定が正しいことを確認してください。この操作によって、デバイスは新しいプロファイルと同期します。

ステップ 1 次のいずれかの方法を使用して、クレデンシャル プロファイルを設定します。

- 新しいクレデンシャル プロファイルを作成するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択し、[追加（Add）] をクリックします。
- 既存のプロファイルを編集するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択し、プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 2 プロファイルに納得できたら、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 3 変更するすべてのデバイスをフィルタリングして選択します（一括編集）。

ステップ 4 [編集（Edit）] をクリックし、[クレデンシャル プロファイル（Credential Profile）] ドロップダウン リストから新しいクレデンシャル プロファイルを選択します。

ステップ 5 次のように変更を保存します。

- [更新（Update）] は、変更を Cisco EPN Manager データベースに保存します。
- [更新して同期（Update and Sync）] は、変更を Cisco EPN Manager データベースに保存し、デバイスの物理インベントリと論理インベントリを収集して、インベントリのすべての変更を Cisco EPN Manager データベースに保存します。

クレデンシャル プロファイルの削除

この手順で、クレデンシャル プロファイルを Cisco EPN Manager から削除します。現在、プロファイルがデバイスに関連付けられている場合は、デバイスの関連付けをそのプロファイルから解除する必要があります。

ステップ 1 何らかのデバイスがプロファイルを使用しているかどうかを確認します。

a) **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** に移動します。

b) 削除するクレデンシャル プロファイルを選択します。

c) [編集（Edit）] をクリックし、[デバイス リスト（Device List）] ページにデバイスが一覧表示されているかどうかを確認します。デバイスが一覧表示されている場合は、それらをメモします。

ステップ 2 必要に応じて、プロファイルからデバイスの関連付けを解除します。

a) **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** に移動します。

b) 変更するすべてのデバイスをフィルタリングして選択します（一括編集）。

c) [編集（Edit）] をクリックし、[クレデンシャル プロファイル（Credential Profile）] ドロップダウン リストから [--選択--（--Select--）] を選択します。

d) 警告ダイアログボックスで [OK] をクリックし、古いプロファイルからデバイスの関連付けを解除します。

ステップ 3 クレデンシャル プロファイルを削除するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [クレデンシャル プロファイル（Credential Profiles）]** を選択し、プロファイルを選択し、[削除（Delete）] をクリックします。

デバイスの到達可能性の状態および管理ステータスの確認

次の手順を実行して、Cisco EPN Manager がデバイスと通信できるか（到達可能性の状態）や、そのホストを管理しているか（管理ステータス）を判断します。また、管理ステータスでは、デバイスが Cisco EPN Manager によって正常に管理されているかどうかの情報も提供されます。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** の順に選択します。

ステップ 2 [ネットワーク デバイス（Network Devices）] テーブルでデバイスを確認します。

a) [表示（Show）] ドロップダウン リスト（テーブルの右上）から [クイック フィルタ（Quick Filter）] を選択します。

b) [デバイス名（Device Name）] 列の下にあるテキスト ボックスにデバイスの名前（またはその一部）を入力します。

ステップ 3 [到達可能性（Reachability）]列と[管理ステータス（Admin Status）]列の情報を確認します。これらの状態の説明については、デバイスの到達可能性状態と管理状態 （34 ページ）を参照してください。

デバイスの到達可能性状態と管理状態

デバイスの到達可能性状態：Cisco EPN Manager が設定されたすべてのプロトコルを使用してデバイスと通信できるかどうかを表します。

表 *3:* デバイスの到達可能性状態

アイコン	デバイスの到達可能性状態	説明	トラブルシューティング
	到達可能	Cisco EPN Manager は、SNMP を使用してデバイスに、または ICMP を使用して NCS 2K デバイスにアクセスすることができます。	—
	ping 到達可能	Cisco EPN Manager は、ping を使用してデバイスに到達できますが、SNMP 経由では到達できません。	ICMP ping は成功しますが、SNMP 通信が失敗する原因すべてをチェックします。デバイス SNMP クレデンシャルがデバイスと Cisco EPN Manager の両方で同じであること、SNMP がデバイス上で有効になっているかどうか、またはトランスポートネットワークが設定ミスなどの理由で SNMP パケットをドロップしていないかどうかをチェックします。基本的なデバイスプロパティの変更を参照してください。
	到達不能	Cisco EPN Manager は、ping を使用してデバイスに到達できません。	物理デバイスが動作中でネットワークに接続されていることを確認します。
	不明	Cisco EPN Manager は、デバイスに接続できません。	デバイスをチェックします。

デバイスの管理状態：デバイスの設定状態を表します（たとえば、デバイスが ping によって到達できないためにダウンしている場合や、管理者が手動でデバイスをシャットダウンした場合などです）。

表 *4:* デバイスの管理状態

デバイスの管理状態	説明	トラブルシューティング
管理対象	Cisco EPN Manager は、デバイスを積極的にモニタしています。	該当なし。
メンテナンス	Cisco EPN Manager は、デバイスの到達可能性をチェックしていますが、トラップ、syslog、または TL1 メッセージを処理していません。	デバイスを管理対象状態に移行するには、デバイスのメンテナンス状態の切り替え （36 ページ）を参照してください。
管理対象外	Cisco EPN Manager は、デバイスをモニタしていません。	[ネットワーク デバイス（Network Devices）] テーブルで、デバイスを特定し、[最新のインベントリ収集ステータス（Last Inventory Collection Status）] 列でデータの横にある [i] アイコンをクリックします。ポップアップ ウィンドウに、詳細とトラブルシューティングのヒントが表示されます。収集問題の一般的な原因は次のとおりです。 • デバイス SNMP クレデンシャルが間違っている。 • Cisco EPN Manager 展開がライセンスで許可されているデバイスの数を上回っている。 • デバイスがスイッチ パス トレース専用になっている。 デバイス タイプがサポートされていない場合は、その [デバイス タイプ（Device Type）] が [不明（Unknown）] になります。そのデバイス タイプのサポートが Cisco.com で提供されているかをチェックするには、**[管理（Administration）] > [ライセンスおよびソフトウェアアップデート（Licenses and Software Updates）] > [ソフトウェアアップデート（Software Update）]** を選択してから、[更新の確認（Check for Updates）] をクリックします。
不明	Cisco EPN Manager は、デバイスに接続できません。	デバイスをチェックします。

デバイスのメンテナンス状態の切り替え

デバイスの管理ステータスが [メンテナンス（Maintenance）] に変更されると、Cisco EPN Manager はデバイスのインベントリ変更用のポーリング操作も、デバイスで生成されたトラップまたは Syslog の処理も行わなくなります。ただし、Cisco EPN Manager は引き続き既存のリンクを維持し、デバイスの到達可能性をチェックします。

すべての管理状態および対応するアイコンのリストについては、デバイスの到達可能性状態と管理状態 （34 ページ）を参照してください。

ステップ 1 [ネットワーク デバイス（Network Devices）] テーブルで、**[管理状態（Admin State）] > [メンテナンス ステートに設定（Set to Maintenance State）]** の順に選択します。

ステップ 2 デバイスを完全な管理状態に戻すには、**[管理状態（Admin State）] > [管理対象状態に設定（Set to Managed State）]** の順に選択します。

（注） [メンテナンス状態をスケジュール（Schedule Maintenance State）] および [管理状態をスケジュール（Schedule Managed State）] オプションを使用して、特定の日時にメンテナンスを行い、特定の日時に管理状態に戻すようにデバイスをスケジュールすることもできます。

追加されたデバイスの検証と問題のトラブルシューティング

ディスカバリ プロセスをモニタするには、次の手順を実行します。

ステップ 1 ディスカバリ プロセスを確認するには、**[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ディスカバリ（Discovery）]** を選択します。

ステップ 2 ジョブ インスタンスを展開して詳細を表示し、次の各タブをクリックして、そのデバイスのディスカバリに関する詳細を表示します。

- [到達可能（Reachable）]：ICMP を使用して到達したデバイス。デバイスは到達可能ですが、モデル化されていない可能性があります。これは、ディスカバリを使用したデバイスの追加 （7 ページ）で示されているように、さまざまな理由で発生する可能性があります。このタブの情報から問題がないか確認してください。
- [フィルタ済み（Filtered）]：カスタマイズされたディスカバリ設定に従ってフィルタ処理されたデバイス。
- [ping で到達可能（Ping Reachable）]：ICMP ping で到達可能だったものの、SNMP を使用して通信できなかったデバイス。これには、複数の理由（無効な SNMP クレデンシャル、SNMP がデバイスで有効になっていない、ネットワークで SNMP パケットが廃棄されたなど）が原因が考えられます。

- [到達不能（Unreachable）]：障害により ICMP ping に応答しなかったデバイス。
- [不明（Unknown）]：Cisco EPN Manager は、ICMP または SNMP によってデバイスに接続できません。

（注） TL1 プロトコルを使用するデバイスの場合は、ノード名にスペースが含まれないようにしてください。そうでない場合、接続障害が発生します。

ステップ 3 デバイスが正常に Cisco EPN Manager に追加されたことを確認するには、**[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワーク デバイス（Network Devices）]** の順に選択します。次のアクションを実行します。

- 追加したデバイスがリストに表示されていることを確認します。Cisco EPN Manager がデバイスから収集したデバイス設定とソフトウェア イメージを表示するには、デバイス名をクリックします。
- [インベントリ収集ステータス（Inventory Collection Status）] フィールドの上にマウス カーソルを合わせ、表示されるアイコンをクリックすると、デバイスから収集された情報の詳細が表示されます。
- デバイスの到達可能性ステータスの列と管理者ステータスの列を確認します。デバイスの到達可能性状態と管理状態 （34 ページ）を参照してください。

デバイス情報を編集する必要がある場合は、基本的なデバイス プロパティの変更を参照してください。

Cisco EPN Manager がデバイスをサポートしていることを確認するには、Cisco Evolved Programmable Network Manager のサポート対象デバイスを参照してください。

Cisco EPN Manager がデバイスをサポートしていることを確認するには、[設定（Settings）] アイコン（⚙）をクリックし、[サポートされているデバイス（Supported Devices）] を選択します。

インベントリ収集またはディスカバリの問題があるデバイスの検索

クイック フィルタを使用して、ディスカバリまたは収集の問題があるデバイスを特定します。

ステップ 1 **[インベントリ（Inventory）]** > **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** を選択して [ネットワークデバイス（Network Devices）] ページを開きます。

ステップ 2 テーブルの左上にある [表示（Show）] ドロップダウンに [クイック フィルタ（Quick Filter）] がリストされていることを確認します。

ステップ 3 [最終インベントリ収集ステータス（Last Inventory Collection Status）] の下にあるクイックフィルタフィールドにカーソルを置き、表示されるドロップダウンリストからステータスを選択します。選択したステータスに応じてデバイスがフィルタリングされます。トラブルシューティング手順については、追加されたデバイスの検証と問題のトラブルシューティング （36 ページ）を参照してください。

デバイス モデリングの再試行ジョブ

デバイスの検出中に特定の一時的な状態により、デバイスの [最終インベントリ収集ステータス（Last Inventory Collection Status）] 値が [警告付き完了（Completed with Warning）] と表示される場合があります。この場合、これらのデバイスの障害が発生した機能は、[障害が発生した機能の同期（Failed Feature Sync）] を使用して自動的に回復します。

（注） [警告付き完了（Completed with Warning）] 状態は、デバイスが [完了（Completed）] 状態に移行して Cisco EPN Manager から使用できるようになっても、障害が発生しているために特定の機能が使用できない場合に示されます。障害が発生した機能は具体的に一覧表示され、ユーザが推奨処置を実行することで回復できます。

（注）

- [障害が発生した機能の同期（Failed Feature Sync）] ジョブは、[警告付き完了（Completed with Warning）] 状態のデバイスのみを対象に、特定の回復可能な障害（タイムアウト エラーなど）に対して使用されます。永続的なエラーまたはシステムベースのエラー（ユーザ認証エラーや不明なエラーなど）は自動回復できません。エラー シナリオの詳細については、管理チームにお問い合わせください。
- [同期失敗（Failed Feature Sync）] ジョブは、Cisco EPN Manager 3.0 以降のバージョンでのみ機能します。以前のバージョンの Cisco EPN Manager ですでに [警告付き完了（Completed with Warning）] 状態になっていたデバイスを 3.0 以降のバージョンにアップグレードした場合、ユーザは [同期失敗（Failed Feature Sync）] ジョブを有効にする前に、デバイスの再同期を手動で実行する必要があります。ユーザは手動で再同期する代わりに、日次同期ジョブで再同期が自動的に行われるのを待機することもできます。詳細については、システム ジョブについての [スイッチインベントリ（Switch Inventory）] ジョブを参照してください。

[障害が発生した機能の同期（Failed Feature Sync）] ジョブ（**[管理（Administration）]** > **[ダッシュボード（Dashboard）]** > **[ジョブダッシュボード（Job Dashboard）]** に移動し、左側のサイドバーで **[システムジョブ（System Jobs）]** > **[インベントリおよびディスカバリジョブ（Inventory and Discovery Jobs）]** を選択）は、システムが過負荷状態にならないようにデフォルトで無効になっており、ユーザが手動で有効にする必要があります。デフォルトのジョブ間隔（30 分）は [スケジュールの編集（Edit Schedule）] オプションを使用して編集できますが、緊急時を除き、短縮した間隔でジョブを実行することはお勧めしません。

（注） [警告付き完了（Completed with Warning）] 状態のデバイスの数が多い場合は、[障害が発生した機能の同期（Failed Feature Sync）] ジョブをできるだけ低い頻度で実行することをお勧めします。

また、Cisco EPN Manager には、[警告付き完了（Completed with Warning）] 状態のデバイスに対して、エラーを解決してデバイスを [完了（Completed）] 状態に移行するためにユーザが実行できる追加手順が用意されています。[ネットワークデバイス（Network Devices）] テーブルでデバイスを特定し、[最新のインベントリ収集ステータス（Last Inventory Collection Status）] 列でデータの横にある [i] アイコンをクリックします。ポップアップ ウィンドウに、詳細とトラブルシューティングのヒント（[障害（Failure）]、[影響（Impact）]、[考えられる原因（Possible Causes）]、および [推奨アクション（Recommended Actions）]）が表示されます。ユーザが推奨アクションを実行した後、デバイスを手動同期（「誤ったCLIクレデンシャル（Wrong CLI credentials）」などのエラーに適用可能）によって [完了（Completed）] 状態に移行させることも、次回の [障害が発生した機能の同期（Failed Feature Sync）] ジョブで自動的に回復させることもできます。

[警告付き完了（Completed with Warning）] のシナリオと対応する推奨アクションの一部を次に示します。

表 *5 : [*警告付き完了（*Completed with Warning***）*]* 状態のシナリオ**

考えられる原因	推奨処置
デバイスへの接続に失敗した	デバイスが着信 CLI/SNMP 接続を受け入れることを確認し、再試行します。
デバイスへの接続が切断される	デバイスが着信 CLI/SNMP 接続を受け入れることを確認し、再試行します。
データ制限を超えた	収集エラー：インベントリ ログを使用して管理者に問い合わせてください。
TL1 プロトコルの予期しない状態	デバイスが着信 TL1 接続を受け入れることを確認し、再試行します。
HTTP プロトコルの一般的な予期しない状態	デバイスが着信 HTTP 接続を受け入れることを確認し、再試行します。
NETCONF/XML からの取得中にエラーが発生した	NETCONF/XML が設定されていることを確認し、再試行します。
NETCONF によって RPC エラーが報告された	収集エラー：インベントリ ログを使用して管理者に問い合わせてください。
CLI_SESSION_SCRIPT ドキュメントでエラーが発生した	デバイスが新しい CLI セッションを受け入れることを確認し、再試行します。
セッションのセットアップ時または切断時のエラーを示すパターンに一致した	デバイスが新しい CLI セッションを受け入れることを確認し、再試行します。
デバイスに到達できない	インベントリ ログを管理者に問い合わせてください。

考えられる原因	推奨処置
デバイスとの通信の試行中にフェールセーフタイムアウトが発生した	デバイスの応答性と負荷を確認します。
デバイスとの通信の試行中にタイムアウトが発生した	デバイスに設定されたタイムアウトによってCLI 接続が停止されないことを確認し、再試行します。
SNMP GET 要求に対する応答がない	デバイスが着信 SNMP 要求を受け入れることを確認し、再試行します。
SNMP Get 要求の実行に失敗した	デバイスが着信 SNMP 要求を受け入れることを確認し、再試行します。
SNMP Get 要求の応答エラー	デバイスが着信 SNMP 要求を受け入れることを確認し、再試行します。

CSV ファイルへのデバイス情報のエクスポート

デバイス リストをファイルにエクスポートすると、すべてのデバイス情報が CSV ファイルにエクスポートされます。次に、選択したパスワードを使用してファイルが圧縮され、暗号化されます。エクスポートしたファイルには、デバイスの SNMP クレデンシャル、CLI 設定、および地理的座標に関する情報が含まれています。エクスポートされたファイルにはデバイスのクレデンシャルが含まれていますが、クレデンシャルのプロファイルは含まれていません。

⚠

注意 CSV ファイルにはエクスポートしたデバイスのすべてのクレデンシャルのリストが含まれるため、十分に注意して使用してください。デバイスのエクスポートは特殊な権限を持つユーザのみが実行できるようにする必要があります。

Cisco EPN Manager は、オペレーティングシステムのデフォルトの zip ユーティリティを使用して、エクスポートされたファイルを開くための ZipCrypto 暗号化方式をサポートしています。ZipCrypto 暗号化方式を有効にするには、**[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）] > [インベントリ（Inventory）] > [インベントリ（Inventory）]** を選択し、[「エクスポートデバイス」用の ZipCrypto 暗号化の有効化（Enable ZipCrypto encryption for 'Export Device'）] チェックボックスをオンにします。デフォルトでは、このオプションは無効になっています。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワーク デバイス（Network Devices）]** を選択します。

ステップ 2 エクスポートするデバイスを選択し、[デバイスのエクスポート（Export Device）] を選択します（または、 をクリックして [デバイスのエクスポート（Export Device）] を選択します）。

ステップ 3 [デバイスのエクスポート（Export Device）] ダイアログボックスで、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。ユーザはエクスポートされたファイルを開くのにこのパスワードを指定する必要があります。

ステップ 4 パスワード、確認パスワード、またはエクスポートファイル名を入力し、[エクスポート（Export）] をクリックします。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。

簡単な管理と設定のためのデバイス グループの作成

デバイスを論理グループに編成すると、デバイスの管理、モニタリング、設定が簡素化されます。グループに操作を適用できるため、グループ化によって時間が節約され、ネットワーク全体で設定が一貫して適用されます。すべてのデバイスを同じ設定で構成できる小規模の構成では、ただ1つの一般的なデバイス グループを作成するだけで済みます。グループ化メカニズムは、サブグループもサポートしています。これらのグループは、多くの Cisco EPN Manager GUI ウィンドウに表示されます。

デバイスが Cisco EPN Manager に追加されると、[未定義（Unassigned）] という名前のロケーション グループに割り当てられます。多数のデバイスを管理している場合は、デバイスを他のグループに移動して、[未定義（Unassigned）] のグループ メンバーシップが大きくなりすぎないようにしてください。

グループの仕組み

グループは、デバイスやポートなどのネットワーク要素の論理コンテナです。たとえば、デバイスの種類や場所など、展開に固有のグループを作成できます。新しいデバイスが条件に一致する場合に自動的に追加されるようにグループを設定することも、手動でデバイスを追加することもできます。

特定のタイプのグループについては、関連項目 ネットワーク デバイス グループ （42 ページ） および ポート グループ （44 ページ） を参照してください。

グループに要素を追加する方法については、グループに要素を追加する方法：動的、手動、および混在グループ （45 ページ） を参照してください。

ネットワーク デバイス グループ

次の表に、サポートされているネットワーク デバイス グループのタイプを示します。デバイス グループにはインベントリからアクセスできます。

ネットワーク デバイス グループの種類	メンバーシップの条件	ユーザが作成または編集できるか
デバイス タイプ（Device Type）	デバイスはファミリごとにグループ化されます（たとえば、オプティカル ネットワーキング、ルータ、スイッチおよびハブなど）。各デバイス ファミリの下で、デバイスはさらにシリーズごとにグループ化されます。新しいデバイスは、適切なファミリおよびシリーズ グループに自動的に割り当てられます。たとえば、Cisco ASR 9006 は、ルータ（ファミリ）および Cisco ASR 9000 シリーズ アグリゲーション サービス ルータ（シリーズ）に属します。 次の点に注意してください。 • デバイス タイプ グループを作成することはできません。これらはシステム定義の動的グループです。代わりに、デバイス基準を使用してユーザ定義のグループを作成し、適切なデバイス名を付けます。 • デバイス タイプ グループはネットワーク トポロジ マップには表示されません。 • [Cisco EPN Manager] で検出されたサポート対象外のデバイスには [サポート対象外のシスコデバイス（Unsupported Cisco Device）] デバイスタイプが自動的に割り当てられ、**[デバイスタイプ（Device Type）] > [サポート対象外のシスコデバイスファミリ（Unsupported Cisco Device Family）]** に表示されます。	いいえ

ロケーション（Location）	ロケーション グループを使用して、ロケーションごとにデバイスをグループ化できます。デバイスを手動で追加するか、またはデバイスを動的に追加して、ロケーション グループの階層（シアター、国、地域、キャンパス、ビルディング、フロアなど）を作成できます。 デバイスは 1 つのロケーション グループのみに表示されるはずですが、上位レベルの「親」グループにもそのデバイスが含まれています。たとえば、ビルディングのロケーション グループに属するデバイスは、親のキャンパス グループにも間接的に属している場合があります。 デフォルトでは、階層の上位のロケーションが [すべてのロケーション（All Locations）] グループとなります。ロケーションに割り当てられていないデバイスはすべて、[すべてのロケーション（All Locations）] の下の [未割り当て（Unassigned）] グループに表示されます。	はい
ユーザ定義（User Defined）	デバイスは、デバイスおよびロケーション条件のカスタマイズ可能な組み合わせによってグループ化されます。グループ名をカスタマイズして、必要なデバイスおよびロケーション基準を使用できます。	対応

ロケーショングループのインポート

[ネットワークデバイスグループ（Network Device Groups）] ページで、CSV ファイルを使用してロケーショングループをインポートできます。Cisco EPN Manager に追加するグループのすべての属性のリストが示される CSV ファイルを使用してロケーション グループをインポートするには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 [グループのインポート（Import Groups）] ボタンをクリックします。[グループのインポート（Import Groups）] ダイアログが開きます。

ステップ 3 表示されたダイアログの下部にある [こちら（here）] をクリックしてサンプルテンプレートをダウンロードします。CSV ファイルを作成し、テンプレート内の形式と情報をガイドとして使用して、グループの名前、親階層、場所の設定、物理アドレス、緯度および経度の詳細を入力します。CSV ファイルを保存します。

ステップ 4 [グループのインポート（Import Groups）] ダイアログで [参照（Browse）] をクリックし、インポートするグループが含まれている CSV ファイルを選択します。

ステップ 5 **[管理（Administration）] > [ダッシュボード（Dashboards）] > [ジョブ ダッシュボード（Job Dashboard）]** を選択し、[グループのインポート（Import Groups）] をクリックしてジョブのステータスを表示します。

ロケーショングループのエクスポート（Export Location Groups）

ロケーショングループの情報を CSV ファイルとしてエクスポートするには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 [グループのエクスポート（Export Groups）] ボタンをクリックします。[グループのエクスポート（Export Groups）] ダイアログが開きます。

ステップ 3 目的の場所にCSVファイルを保存します。CSVファイルには、グループ名、親階層、場所の設定、物理アドレス、緯度、経度などの詳細が示されます。

ポート グループ

次の表に、サポートされているポート グループのタイプを示します。

ポート グループの種類	メンバーシップの条件	ユーザが作成または編集できるか
ポート タイプ（Port Type）	ポートの種類、速度、名前、または説明ごとにグループ化されます。新しいデバイスのポートは、適切なポート グループに自動的に割り当てられます。 ポート タイプのグループは作成できません。代わりに、デバイス基準を使用してユーザ定義グループを作成し、ユーザ定義グループの下にサブグループを作成します。	いいえ。代わりに、ユーザ定義グループを作成します。

システム定義（System Defined）	ポートの使用状況または状態別にグループ化されます。新しいデバイスのポートは、適切なポート グループに自動的に割り当てられます。 [リンクポート（Link Ports）]：別のシスコ デバイスまたは他のネットワーク デバイスに接続され、「VLAN」モードで動作し、VLAN に割り当てられるポート。 [トランクポート（Trunk Ports）]：シスコ デバイスまたは他のネットワーク デバイス（スイッチ、ルータ、ファイアウォール、サードパーティ デバイス）に接続され、すべてのVLANのトラフィックを伝送する「トランク」モードで動作しているポート。 ポートのステータスがダウンすると、そのポートは[未接続ポート（Unconnected Port）]グループに自動的に追加されます。このグループ内のポートを削除することはできません。また、このグループを他のグループのサブ グループとして再作成することはできません。 ワイヤレス デバイスおよびデータセンター デバイスは、AVC 設定済みインターフェイス、UCS インターフェイス、UCS アップリンク インターフェイス、WANインターフェイスなど、その他のシステム定義のポート グループを使用します。 システム定義のポート グループは作成できません。代わりに、デバイス基準を使用してユーザ定義グループを作成し、ユーザ定義グループの下にサブグループを作成します。 （注） [WAN インターフェイス（WAN Interfaces）] はスタティックグループであるため、自動ポートの追加は適用されません。したがって、手動でグループにポートを追加する必要があります。	いいえ。代わりに、ユーザ定義グループを作成します。
ユーザ定義（User Defined）	ポート基準のカスタマイズ可能な組み合わせによってグループ化され、グループに名前を付けることができます。グループが動的でポートが条件に一致する場合は、そのグループに追加されます。	対応

グループに要素を追加する方法：動的、手動、および混在グループ

グループに要素を追加する方法は、グループが動的か、手動か、混在かによって異なります。

デバイスの追加方法	説明

動的	要素がグループ基準を満たしている場合、Cisco EPN Manager はグループに新しい要素を自動的に追加します。指定できるルールの数に制限はありませんが、ルールを追加するにしたがい更新のパフォーマンスに影響が及ぶ場合があります。
手動	グループの作成時またはグループの編集時に、ユーザは手動で要素を追加します。
混合	要素は、動的ルールと手動追加の組み合わせによって追加されます。

親/子のユーザ定義グループおよびロケーション グループにおけるデバイスの継承は次のとおりです。

- ユーザ定義グループ：子グループを作成する場合：
  - 親グループと子グループの両方がダイナミックの場合、子グループは親グループ内のデバイスにのみアクセスできます。
  - 親グループが静的で、子グループが動的である場合、子グループは親グループ外のデバイスにアクセスできます。
  - 親グループと子グループが動的かつ静的である場合、子グループは親のデバイス グループからデバイスを「継承」します。
- ロケーション グループ：親グループは子のグループ デバイスを継承します。

グループおよび仮想ドメイン

グループは要素の論理コンテナですが、要素へのアクセスは仮想ドメインによって制御されます。次の例は、グループと仮想ドメインの関係を示しています。

- **SanJoseDevices** という名前のグループに 100 台のデバイスが含まれています。
- **NorthernCalifornia** という名前の仮想ドメインに 400 台のデバイスが含まれています。これらのデバイスはさまざまなグループに属しており、**SanJoseDevices** グループのデバイスが 20 台含まれています。

NorthernCalifornia 仮想ドメインにアクセスできるユーザは、**SanJoseDevices** グループの 20 台のデバイスにアクセスできますが、このグループ内の他の 80 台のデバイスにはアクセスできません。詳細については、デバイスへのユーザアクセスを制御するための仮想ドメインの作成を参照してください。

ユーザ定義のデバイス グループの作成

新しいデバイス タイプ グループを作成するには、ユーザ定義グループのメカニズムを使用します。デバイス タイプ グループは Cisco EPN Manager 全体で使用される特殊なカテゴリであるため、このメカニズムを使用する必要があります。作成するグループが [ユーザ定義（User Defined）] カテゴリに表示されます。

（注） Cisco ASR サテライトは、ロケーション グループにのみ所属できます。詳細については、Cisco EPN Manager でのサテライトの考慮事項を参照してください。

新しいグループを作成するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 [デバイスグループ（Device Groups）] ペインで [+]（**追加**）アイコンをクリックし、[ユーザ定義グループの作成（Create User Defined Group）] を選択します。

ステップ 3 グループの名前と説明を入力します。他のユーザ定義デバイス タイプ グループが存在する場合、[親グループ（Parent Group）] ドロップダウン リストからグループを選択することで、そのグループを親グループとして設定できます。親グループを選択しなかった場合は、新しいグループが [ユーザ定義（User-Defined）] フォルダに配置されます（デフォルト）。

ステップ 4 次のように、デバイスを新しい グループに追加します。

条件を満たすデバイスを自動的に追加する場合は、[デバイスを動的に追加（Add Devices Dynamically）] 領域に条件を入力します。IP アドレスの特定の範囲内に入るデバイスをグループ化するには、角カッコ内にその範囲を入力します。たとえば、次を指定できます。

- IPv4-10.[101-155].[1-255].[1-255] および 10.126.170.[1-180]
- IPv6-2014::5217:[0000-ffff]:fe22:[1e40-1f41]

（注） ダイナミック グループに指定できるルールの数に制限はありませんが、ルールの数が増えるとグループの更新パフォーマンスが低下する可能性があります。

デバイスを手動で追加する場合は、次の手順を実行します。

1. [デバイスを手動で追加（Add Devices Manually）] 領域を展開し、[追加（Add）] をクリックします。
2. [デバイスの追加（Add Devices）] ダイアログボックスで、追加するデバイスのチェックボックスをオンにして、[追加（Add）] をクリックします。

ステップ 5 [プレビュー（Preview）] タブをクリックしてグループのメンバーを表示します。

ステップ 6 [保存（Save）] をクリックします。

ステップ 3 で選択したフォルダに新しいデバイス グループが表示されます。

ロケーション グループの作成

（注） Cisco ASR サテライトは、ロケーション グループにのみ属することができます。詳細については、Cisco EPN Manager でのサテライトの考慮事項を参照してください。

ロケーション グループを作成するには、次の手順を実行します。

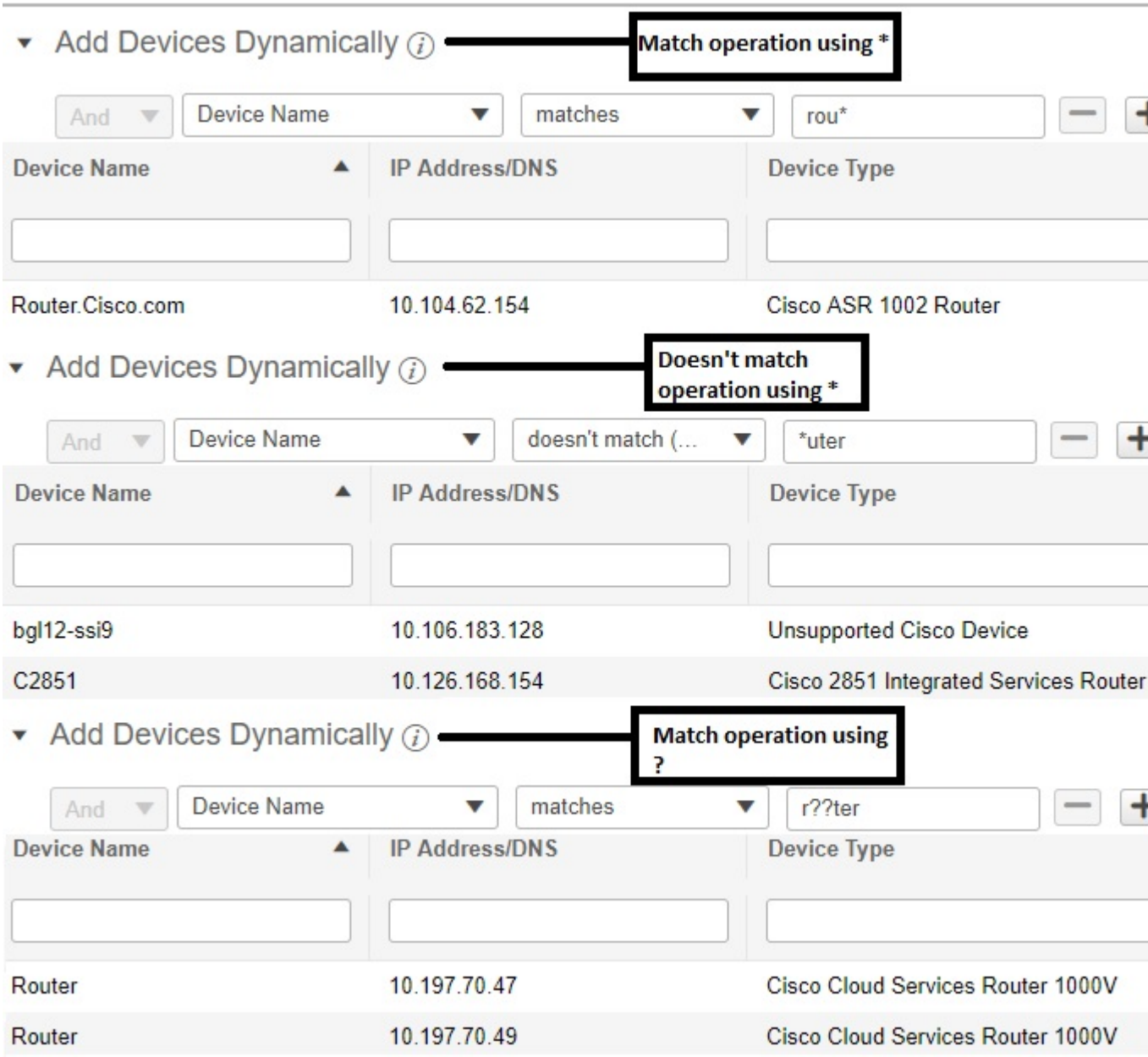
ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 左側の [デバイス グループ（Device Groups）] ペインで、[追加（Add）] アイコンをクリックし、[ロケーション グループの作成（Create Location Group）] を選択します。

ステップ 3 名前と説明を入力し、[親グループ（Parent Group）] ドロップダウンリストからグループを選択します。デフォルトでは、[すべてのロケーション（All Locations）] のサブグループになります（つまり、[すべてのロケーション（All Locations）] フォルダに表示されます）。

ステップ 4 たとえば、特定の住所のビルディングにあるすべてのデバイスなど、地理的なロケーションに基づいてデバイス グループを作成する場合は、[地理的なロケーション（Geographical Location）] チェックボックスをオンにしてグループの GPS 座標を指定するか、または [マップの表示（View Map）] リンクをクリックし、マップ内の必要な場所をクリックします。この場合は、GPS 座標が自動的に入力されます。地理的なロケーションで定義されたロケーション グループは、Geo マップのグループ アイコンで表されます。グループに追加するデバイスは、そのグループの GPS 座標を継承します。詳細については、Geo マップのデバイス グループ を参照してください。地理的なロケーションが一連のデバイスをグループ化する主たる理由の場合は、グループに追加するデバイスに、そのグループとは異なる独自の GPS 座標を持たせないことを推奨します。

ステップ 5 特定の基準を満たしている場合にデバイスが自動的に追加されるようにするには、[デバイスを動的に追加（Add Devices Dynamically）] 領域に基準を入力します。それ以外の場合は、この領域を空欄のままにします。



ダイナミック グループに指定できるルールの数に制限はありませんが、ルールの数が増えると、グループ更新のパフォーマンスが低下する可能性があります。

ステップ 6 デバイスを手動で追加する場合は、次の手順を実行します。

a) [デバイスを手動で追加（Add Devices Manually）] で、[追加（Add）] をクリックします。

b) [デバイスの追加（Add Devices）] ダイアログボックスで、追加するデバイスを見つけて、[追加（Add）] をクリックします。

ステップ 7 [プレビュー（Preview）] タブをクリックして、グループ メンバーを確認します。

ステップ 8 [保存（Save）] をクリックすると、ステップ 3 で選択したフォルダ（デフォルトでは [すべてのロケーション（All Locations）]）の下に新しいロケーション グループが表示されます。

Maps GUI を起動して建物をクリックします。

ロケーショングループを編集する場合は、次の条件を満たしている場合にグループタイプを変更できます。

- グループ タイプがデフォルト。
- グループにサブグループがない。

ポート グループの作成

ポート グループを作成するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ポート グループ（Port Groups）]** を選択します。

ステップ 2 **[ポートグループ（Port Groups）] > [ユーザ定義（User Defined）]** から、[ユーザ定義（User Defined）] の横にある [i] アイコンの上にカーソルを置き、ポップアップウィンドウの [サブグループの追加（Add SubGroup）] をクリックします。

ステップ 3 名前と説明を入力し、[親グループ（Parent Group）] ドロップダウンリストからグループを選択します。デフォルトでは、ポート グループは [ユーザ定義（User Defined）] フォルダに配置されます。

ステップ 4 グループに追加するためにポートが属している必要があるデバイスを選択します。[デバイスの選択（Device Selection）] ドロップダウンリストから、次を選択できます。

- [デバイス（Device）]：すべてのデバイスのフラット リストからデバイスを選択します。
- [デバイス グループ（Device Group）]：デバイス グループを選択します（[デバイス タイプ（Device Type）]、[ロケーション（Location）]、および [ユーザ定義（User Defined）] グループのリストが表示されます）。

ステップ 5 条件を満たしている場合にポートが自動的に追加されるようにするには、[ポートを動的に追加（Add Ports Dynamically）] 領域にその条件を入力します。それ以外の場合は、この領域を空欄のままにします。

ダイナミックグループに指定できるルールの数に制限はありませんが、ルールの数が増えると、グループ更新のパフォーマンスが低下する可能性があります。

ステップ 6 デバイスを手動で追加する場合は、次の手順を実行します。

a) [ポートを手動で追加（Add Port Manually）] で、[追加（Add）] をクリックします。
b) [ポートの追加（Add Devices）] ダイアログボックスで、追加するデバイスを見つけて、[追加（Add）] をクリックします。

ステップ 7 [プレビュー（Preview）] タブをクリックして、グループ メンバーを確認します。

ステップ 8 [保存（Save）] をクリックすると、ステップ 3 で選択したフォルダ（デフォルトでは [ユーザ定義（User Defined）]）の下に新しいポート グループが表示されます。

グループのコピーの作成

グループの複製を作成すると、Cisco EPN Manager はデフォルトでそのグループに **CopyOf***group-name* という名前を付けます。名前は必要に応じて変更できます。

グループを複製するには、次の手順を実行します。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 左側の [デバイス グループ（Device Groups）] ペインから、グループを選択します。

ステップ 3 コピーするデバイス グループを見つけ、その横にある [i] をクリックするとポップアップ ウィンドウが開きます。

ステップ 4 [グループの複製（Duplicate Group）] をクリックし（この時点では変更を加えない）、[保存（Save）] をクリックします。Cisco EPN Manager によって **CopyOf***group-name* という新しいグループが作成されます。

ステップ 5 ユーザ定義のデバイス グループの作成 （46 ページ）とロケーション グループの作成 （48 ページ）の説明に従ってグループを設定します。

ステップ 6 [プレビュー（Preview）] タブをクリックし、グループメンバーを調査して、グループの設定を確認します。

ステップ 7 [保存（Save）] をクリックして、グループを保存します。

メンバーがいないグループの非表示

デフォルトでは、グループにメンバーが存在しなくても、Cisco EPN Manager は Web GUI にグループを表示します。管理者権限を持つユーザが、この設定を変更して空のグループが非表示になる、つまり Web GUI に表示されないようにすることができます。（非表示グループは Cisco EPN Manager から削除されません）。

ステップ 1 **[管理（Administration）] > [設定（Settings）] > [システム設定（System Settings）]** を選択し、**[インベントリ（Inventory）] > [グループ化（Grouping）]** を選択します。

ステップ 2 [メンバーが存在しないグループの表示（Display groups with no members）] をオフにし、[保存（Save）] をクリックします。

グループやデバイスが多数ある場合は、[メンバーが存在しないグループの表示（Display groups with no members）]チェックボックスをオンのままにすることをお勧めします。これをオフにすると、システムのパフォーマンス速度が低下します。

グループの削除

削除するグループにメンバーが含まれていないことを確認します。メンバーが含まれている場合、Cisco EPN Manager で操作を続行することはできません。

ステップ 1 **[インベントリ（Inventory）] > [グループ管理（Group Management）] > [ネットワークデバイスグループ（Network Device Groups）]** の順に選択します。

ステップ 2 削除するデバイス グループを左側の [デバイス グループ（Device Groups）] ペインで見つけ、その横にある [i] をクリックするとポップアップ ウィンドウが開きます。

ステップ 3 [グループの削除（Delete Group）] をクリックし、[OK] をクリックします。

デバイスの削除

デバイスを削除すると、Cisco EPN Manager でそのデバイスのモデリングおよびモニタリングは行われなくなります。

始める前に

デバイスに Cisco EPN Manager を使用してプロビジョニングされたサービスがある場合は、デバイスを削除する前にそれらのサービスを削除する必要があります。ただし、デバイス自体で検出またはプロビジョニングしたサービス（つまり、Cisco EPN Manager によって作成されていないサービス）があっても、デバイスの削除は可能です。デバイス上のサービスを検索するには、[デバイス360（Device 360）] ビューを使用します（特定のデバイスの回線/VC の表示を参照）。

ステップ 1 **[インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** を選択して [ネットワークデバイス（Network Devices）] ページを開きます。

ステップ 2 削除するデバイスを見つけます。たとえば、[デバイスグループ（Device Groups）] リスト内を移動したり、[クイックフィルタ（Quick Filter）] ボックスにテキストを入力したりできます。

ステップ 3 デバイスを選択し、[デバイスの削除（Delete device）] アイコンをクリックします。

既存のネットワーク装置（NE）の置換

既存のネットワーク装置（NE）を、古いデバイスとまったく同じ新しいネットワーク装置に置き換えるには、次の手順を実行します。

ステップ 1 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）] を選択し、[完了（Completed）] 状態になったときに置換する必要があるデバイスの設定バックアップを取得します。

ステップ 2 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）] を選択し、置換する必要があるデバイスのデバイスの状態を [メンテナンス（Maintenance）] に変更します。

ステップ 3 古いハードウェアと同じスロットにインストールされた RP およびラインカードを含めて、ネットワーク装置（NE）を同じハードウェアに置き換えます。

ステップ 4 古いハードウェアを接続したのと同じ方法で、新しいハードウェアを管理ポートに再接続します。

ステップ 5 新しいデバイスの基本管理設定を、古いデバイスと同じように設定します。たとえば、[管理IP（Management IP）]、[サブネット（Subnet）]、[ホスト名（Hostname）] などです。

ステップ 6 [インベントリ（Inventory）] > [デバイス管理（Device Management）] > [設定アーカイブ（Configuration Archive）]を選択し、新しいデバイス上の古いデバイスから設定バックアップを[ロールバック（Roll Back）] します。

ステップ 7 [ネットワークデバイス（Network Devices）] ページで、デバイスの状態を [管理対象（Managed）] に変更し、ステータスが [完了（Completed）] に変わるまで待機します。

次のタスク

すべての基本的なデバイス設定、サービス、パフォーマンス、および障害データがそのまま維持されて、新しい設定が正しいことを確認します。