



デバイスおよびホストの管理

- [デバイスインベントリの管理, 1 ページ](#)
- [ホストインベントリの管理, 36 ページ](#)

デバイス インベントリの管理

[デバイスインベントリ (Device Inventory)] ウィンドウに、検出スキャンの結果が表示されます。[検出 (Discovery)] ウィンドウに、[ナビゲーション (Navigation)] ペインからアクセスするには、[デバイスインベントリ (Device Inventory)] をクリックします。

図 1: [デバイスインベントリ (Device Inventory)] ウィンドウ

Device Name	IP Address	Reachability Status	Up Time	Last Updated Time	Poller Time	Last Inventory Collection Status
SDN-DEV-2969-BR4.cisco.com	10.10.10.10	Reachable	9 days, 18:36:36.81	a few seconds ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-3650-BR4	10.10.10.10	Reachable	9 days, 18:35:15.72	a few seconds ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-4132-1-CA2.cisco.com	10.10.10.10	Reachable	9 days, 18:37:19.58	a minute ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-4508-CA2	10.10.10.10	Reachable	9 days, 18:35:52.88	a minute ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-N17X-CA2	10.10.10.10	Reachable	102 days, 0:26:42.43	a few seconds ago	00:25:00	Managed



(注) 表示される情報は、選択したレイアウトによって異なります。

最初の検出後、ネットワーク デバイスは 30 分ごとにポーリングされます。ポーリングはデバイス、リンク、ホスト、およびインターフェイスごとに実行されます。アクティブ状態が一日未満のデバイスのみが表示されます。これによって、古いデバイスデータが表示されないようにします。500 個のデバイスのポーリングに約 20 分かかります。

[Device Inventory] ウィンドウから実行できるアクションについては、[\[Device Inventory\] のタスク](#)、[\(9 ページ\)](#) を参照してください。

次の表に、[Device Inventory] テーブルの主な要素の説明を示します。

ウィンドウ要素	説明
[デバイスの選択 (Device Selection)] チェックボックス	タスクを実行するデバイスを選択できます。 デバイスを選択すると、[Device Inventory] テーブルの上にアクション ボタンが表示されます。これらのボタンおよびそのアクションに関する情報については、 [Device Inventory] のタスク 、 (9 ページ) を参照してください。
Filters	テーブルに表示されるデバイスを名前、ロケーションタグ、および IP アドレスごとに絞りこむことができます。 フィルタを削除するには、[Clear Filters] をクリックします。
レイアウト	次の 3 つの定義済みレイアウト、またはカスタマイズしたレイアウトから選択できます。 <ul style="list-style-type: none"> • [ステータス (Status)]: レイアウトでは、デバイス名、IP アドレス、デバイスの状態、稼動時間、最終更新時間が表示されます。 • [ハードウェア (Hardware)]: レイアウトでは、デバイス名、IP アドレス、デバイス ファミリ、プラットフォーム、シリアル番号、MAC アドレス、ロール、および IOS/ファームウェアのバージョンとコンフィギュレーション ファイルへのリンクが表示されます。 • [タグging (Tagging)]: レイアウトでは、デバイス名、IP アドレス、MAC アドレス、デバイス ロール、ロケーション、およびタグが表示されます。 • [カスタマイズ (Customize)]: レイアウトでは、表示対象として選択した列の情報が示されます。 <p>表示できる情報の列の説明については、次の表「デバイス インベントリ情報」を参照してください。</p>

[デバイス インベントリ (Device Inventory)] テーブルの下で、テーブルに表示されるデバイス数 (10、25、50、100) を調整できます。[最初 (First)]、[前 (Previous)]、[次 (Next)]、[最後 (Last)]、またはページ番号をクリックして、テーブル間を移動します。

デバイス インベントリ情報

[デバイス インベントリ (Device Inventory)] テーブルに、検出された各デバイスに関する次の情報が表示されます。[構成 (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。カラム ヘッダーをクリックすると、行が昇順にソートされます。カラム ヘッダーを再度クリックすると、行が降順にソートされます。

詳細については、『*Cisco Application Policy Infrastructure Controller Enterprise Module Configuration Guide*』を参照してください。

表 1: デバイスインベントリ情報

カラム名	説明
デバイス ステータス	<p>デバイスの状態。</p> <ul style="list-style-type: none"> • 接続中 (Connecting) : コントローラはデバイスに接続しています。 • 到達可能 (Reachable) : <ul style="list-style-type: none"> ◦ 検出済み (Discovered) : コントローラがデバイスに接続し、CLIを使用してシスココマンドを実行できます。 ◦ 失敗 (Failure) : コントローラがデバイスに接続しましたが、CLIを使用してシスココマンドを実行できません。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。 • 認証失敗 (Authentication Failed) : コントローラがデバイスに接続しましたが、どのタイプのデバイスであるか判断できません。このデバイスの状態も通常は、デバイスがシスコデバイスではないことを示します。 • 到達不能 (Not reachable) : コントローラがデバイスに接続できません。 <ul style="list-style-type: none"> (注) 検出要求の前にクレデンシャルが提供されていない場合に、デバイスの状態が「到達不能」と表示されます。正しいクレデンシャルを提供した上で新しく検出を実行する必要があります。

コラム名	説明
デバイス名 (Device Name)	デバイスの名前。[デバイス概要 (Device Overview)] ダイアログボックスに次の情報を表示するには、デバイス名をクリックします。 <ul style="list-style-type: none"> • デバイスのシリアル番号 • デバイスの IP アドレス • MAC address • Cisco OS バージョン • Up time • Product ID • ベンダー • メモリ サイズ (注) インベントリが 30 分以上更新されていないデバイスに対して、デバイス名が赤色で表示されます。 [デバイス概要 (Device Overview)] ダイアログボックスには、次のインターフェイスデータを含む[インターフェイス (Interfaces)] タブも含まれます。 <ul style="list-style-type: none"> • 状態 (Status) : アップまたはダウン。 • インターフェイス名 (Interface Name) : インターフェイスの名前。 • MAC アドレス (MAC Address) : インターフェイスの MAC アドレス。
MAC アドレス	デバイスの MAC アドレス。
IP アドレス	デバイスの IP アドレス。
IOS/ファームウェア (IOS/Firmware)	現在デバイス上で実行されている Cisco IOS ソフトウェア。
Platform	シスコ製品の部品番号。
Serial Number	シスコ デバイスのシリアル番号。
Up Time	デバイスが起動してから、稼働している時間。

カラム名	説明
Config	<p>CLI の show running-config コマンドの出力と同様の設定情報を表示するには、[表示 (View)] をクリックします。</p> <p>(注) この機能は、アクセス ポイントとワイヤレス LAN コントローラではサポートされていないため、これらのデバイス タイプに対して設定データは返されません。</p>
デバイス ロール	<p>スキャンプロセス中に、検出された各デバイスに割り当てられているロール。デバイスロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。コントローラがデバイスロールを確認できない場合、デバイスロールは不明と設定されます。</p> <p>(注) ネットワーク トポロジが変更されるのに従い、コントローラはデバイスロールを変更できますが、デバイスロールを手動で変更する場合は、そのロールはネットワーク トポロジの変更に伴い変更されません。</p> <p>必要に応じて、このカラムのドロップダウンリストを使用して、割り当てられたデバイスロールを変更することができます。次のデバイスロールを使用できます。</p> <ul style="list-style-type: none"> • 不明 (Unknown) • アクセス • Core • Distribution • ボーダー ルータ

コラム名	説明
Location	<p>地理的位置を示すために、デバイスに適用できるタグ。いくつかのデバイスに同じタグを適用すると、共通の属性に基づいてそれらのタグをグループ化できます。[デバイス インベントリ (Device Inventory)] ウィンドウと [トポロジ (Topology)] ウィンドウはロケーションタグをサポートしています。</p> <p>ロケーションタグを作成する場合は、次の注意事項に留意してください。</p> <ul style="list-style-type: none"> • ロケーションタグの情報はコントローラのみで保持され、デバイスに展開されることもデバイスから導出されることもありません。 • コントローラに定義されるロケーションは、一部のデバイスがサポートしている「シビックロケーション」プロパティではありません。 • [トポロジ (Topology)] ウィンドウではロケーションタグの作成、使用、検索をすることはできません。 • ホストにロケーションタグを付けることはできません。 • 1つのデバイスに適用できるのは1つのロケーションタグのみです。ただし、ロケーションタグとデバイスタグを同時に使用することは可能です。 <p>ロケーションタグの追加については、ロケーションタグの追加または削除、(23 ページ) を参照してください。</p> <p>ロケーションタグとともに、世界地図の地理的なマーカーをデバイスに追加できます。詳細については、ロケーションマーカーの追加または変更、(25 ページ) を参照してください。</p>

カラム名	説明
デバイス タグ (Device Tag)	<p>一般的な属性によってデバイスを識別するために、デバイスに割り当てられたタグ。たとえば、プラットフォーム ID や Cisco IOS リリースに基づいてタグを作成し、それを使用してデバイスをグループ化できます。</p> <p>[タグ (Tag)]カラムの数字は、そのデバイスに適用されたタグの数を示します。</p> <p>(注) ロケーションタグとデバイスタグの両方を同時に使用することができます。</p> <p>デバイスタグの追加または削除については、デバイスインベントリでのデバイスタグの追加または削除, (20 ページ) を参照してください。</p> <p>コントローラデータベースからのタグの削除については、タグの削除, (27 ページ) を参照してください。</p>
ポリシー タグ (Policy Tag)	<p>同じポリシーを共有するデバイスのグループに適用されるタグ。</p> <p>ポリシー タグを適用した後は、同じポリシータグを持つデバイスに適用されるポリシーを設定する必要があります。QoS ポリシーの設定方法については、<i>Cisco EasyQoS Application for APIC-EM User Guide</i>を参照してください。</p>
Last Updated Time	デバイスが最後にスキャンされ、コントローラデータベースが更新された日時。
デバイス ファミリ (Device Family)	<p>関連するデバイス グループ。</p> <ul style="list-style-type: none"> • Cisco Interfaces and Modules • ルータ • Switches and Hubs • サードパーティ デバイス • サポート対象外のシスコ デバイス • ワイヤレス コントローラ
デバイス シリーズ	デバイスのシリーズ番号 (たとえば、Cisco Catalyst 4500 シリーズ スイッチ)。

カラム名	説明
最終インベントリ収集ステータス (Last Inventory Collection Status)	<p>デバイス最終検出のスキャン状態。</p> <ul style="list-style-type: none"> • 管理対象 (Managed) : デバイスが完全に管理されている状態にあります。 • 部分的な収集の失敗 (Partial Collection Failure) : デバイスが部分的に収集された状態であり、すべてのインベントリ情報が集められませんでした。障害の追加情報を表示するには、[情報 (Information)] (i) アイコンにマウスを合わせます。 • 到達不能 (Unreachable) : デバイス接続の問題が原因で、デバイスが到達できず、インベントリ情報を集められませんでした。この状態は定期的に収集される際に発生することがあります。 • 誤ったクレデンシャル (Wrong Credentials) : デバイスクレデンシャルがデバイスをインベントリに追加した後に変更された場合、この状態が表示されます。 • 進行中 (In Progress) : インベントリ収集が実行されています。

[Device Inventory] のタスク

[Device Inventory] ウィンドウから実行できるアクションは、選択したレイアウトによって異なります。1つ以上のデバイスを選択した状態で次のボタンのいずれかをクリックすると、それに対応するアクションが実行されます。

表 2 : [Device Inventory] のボタン

ボタン	Action
Add Device	<p>特定のデバイスを検出して、インベントリに追加できます。クレデンシャルが無効なためにデバイスの認証が失敗すると、デバイスは収集失敗の状態になります。詳細については、手動によるデバイスの追加、(11 ページ) を参照してください。</p>

ボタン	Action
[Set Location]	地図上のロケーションタグに関連付けられているデバイスの場所を設定します。詳細については、 ロケーションマーカールの追加または変更 、 (25 ページ) を参照してください。
[Set Device Tags]	一般的な属性に従ってデバイスをグループ化します。詳細については、 デバイスインベントリでのデバイスタグの追加または削除 、 (20 ページ) を参照してください。
[Set Policy Tag]	デバイスをグループ化して、同じ QoS ポリシーを複数のデバイスに同時に導入できるようにします。詳細については、 デバイスインベントリでのポリシータグの追加または削除 、 (22 ページ) を参照してください。
Delete	選択したデバイスをインベントリから削除します。詳細については、 デバイスの削除 、 (14 ページ) を参照してください。
Update Credentials	選択したデバイスのクレデンシャルを変更します。これ以降の検出では、グローバルなクレデンシャルやディスクバリジョブ固有のクレデンシャルではなく、これらのクレデンシャルが、選択したデバイスに使用されます。詳細については、次の資料を参照してください。 デバイスクレデンシャルの更新 、 (29 ページ)
[Update Polling Interval]	選択したデバイスのポーリング間隔を更新できます。選択したデバイスに対しては、これらのデバイス固有の設定が、グローバル設定およびジョブ固有の設定よりも優先されます。詳細については、 デバイスのポーリング間隔の更新 、 (34 ページ) を参照してください。
[Resync] (デバイスの再同期)	更新されたデバイス情報およびステータスの収集のためデバイスをただちにポーリングします。詳細については、 デバイス情報の再同期 、 (33 ページ) を参照してください。

ボタン	Action
[Command Runner]	API コマンドを使用して、選択したデバイスに CLI コマンドを送信します。現時点では、 show およびその他の読み取り専用コマンドが使用可能です。詳細については、 デバイスでのコマンド実行 、(33 ページ) を参照してください。

手動によるデバイスの追加

インベントリに手動でデバイスを追加できます。

図 2 : [Add Device] ダイアログ ボックス

Add Device

* Device IP

▼ SNMP

* Version

* Read Community

Write Community

▶ SNMP RETRIES AND TIMEOUT

▶ CLI

i Please make sure the authenticity of credentials, in case of invalid credentials device will go in collection failure state.

Add **Cancel**

はじめる前に

この手順を実行するには、管理者 (ROLE_ADMIN) 権限と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** [ナビゲーション (Navigation)] ペインで、[デバイス インベントリ (Device Inventory)] をクリックします。
- 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 [Device IP] フィールドにデバイスの IP アドレスを入力します。
- ステップ 4** [Version] フィールドで、ドロップダウン リストから SNMP バージョン ([V2C] または [V3]) を選択し、対応するフィールドに入力します。

表 3: **SNMP V2C** のフィールド

フィールド	説明
Read Community	デバイスに対する接続とアクセスをコントローラに許可するデバイスで設定されている read-only コミュニティ ストリング 値。このコミュニティ ストリング 値は、デバイスで事前設定されているコミュニティ ストリング 値と一致する必要があります。
Write Community	デバイスに対する接続、アクセス、変更をコントローラに許可するデバイスで設定されている write コミュニティ ストリング 値。このコミュニティ ストリング 値は、デバイスで事前設定されているコミュニティ ストリング 値と一致する必要があります。

表 4: **SNMP V3** のフィールド

フィールド	説明
モード	使用する認証モード。有効なモードとして、[Authentication and Privacy]、[Authentication, No Privacy]、[No Authentication, No Privacy] があります。

フィールド	説明
Auth.タイプ	<p>[Authentication and Privacy] または [Authentication, No Privacy] を選択したときにのみ有効。2つの認証タイプがあります。</p> <ul style="list-style-type: none"> • [SHA] : セキュアハッシュアルゴリズム (SHA) に基づく認証。SHA は、パケット データの認証に使用されるハッシュ アルゴリズムです。 • [MD5] : Message Digest 5 (MD5) アルゴリズムに基づく認証。MD5は、パケットデータの認証に使用されるハッシュ アルゴリズムです。
[Username]	<p>[SHA] または [MD5] を選択したときにのみ有効。 SNMP ユーザおよび選択された認証タイプ (MD5 または SHA) に関連付けられる文字列。</p>
Auth.パスワード	<p>[SHA] または [MD5] を選択したときにのみ有効。 SNMP ユーザパスワードとして保存され、認証タイプ (MD5 または SHA) に関連付けられる、暗号化された文字列。</p>
Privacy Type	<p>[Authentication and Privacy] モードを選択したときにのみ有効。2つのプライバシー タイプがあります。</p> <ul style="list-style-type: none"> • DES : データ暗号規格 (DES) の 56 ビット暗号化、および暗号ブロック連鎖 (CBC) DES (DES-56) 標準に基づく認証 • AES128 : 暗号ブロック連鎖 (CBC) モードの AES 暗号化
Privacy Password	<p>選択したプライバシーのタイプ (DES または AES128) に関連付けられ、デバイスとやり取りするメッセージの暗号化用秘密キーの生成に使用される、SNMPv3 プライバシー パスワード。</p>

ステップ 5 [SNMP Retries and Timeout] エリアがまだ展開されていない場合は展開し、次のフィールドに入力します。

表 5 : [SNMP Retries and Timeout] のフィールド

フィールド	説明
Retries	<p>コントローラが SNMP を使用してデバイスとの通信を試みる回数。デフォルトは、3 回です。</p>

フィールド	説明
Timeout	コントローラが SNMP を使用してデバイスとの通信を試みる際に、失敗とみなされるまでに待機する秒数。デフォルトは 5 秒です。

ステップ 6 [CLI] エリアがまだ展開されていない場合は展開し、次のフィールドに入力します。

表 6: [CLI] のフィールド

フィールド	説明
Protocol	リモート管理ステーションからデバイス CLI 接続のために使用されるプロトコル。有効なオプションとして、[Telnet] (Telnet TCP/IP)、[SSH2] (セキュアシェル 2.0) があります。
[Username]	デバイスの CLI にログインするために使用される ID。
Password	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。
Enable Password	CLI へのログインが成功した後で、特権 EXEC モードへのアクセスに使用されるパスワード。

ステップ 7 [Add] をクリックします。

デバイスの削除

Cisco APIC-EM データベースからデバイスを削除できます。

はじめる前に

この手順を実行するには、管理者 (ROLE_ADMIN) 権限と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** [ナビゲーション (Navigation)] ペインで、[デバイス インベントリ (Device Inventory)] をクリックします。
- 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クリックします。
ツールバーが開きます。
- (注) ツールバーが開いた後でも、その他のチェックボックスをクリックして複数のデバイスを選択したり、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することができます。
- ステップ 3** 開いたツールバーから [削除 (Delete)] をクリックします。
-

[デバイスインベントリ (Device Inventory)] ウィンドウでデバイスをフィルタリングする

[デバイスインベントリ (Devices Inventory)] ウィンドウに表示されるデバイスを、デバイス名、ロケーション、IP アドレス、および VRF インスタンスでフィルタリングできます。



(注) フィルタを削除するには、[Clear Filters] をクリックします。

図 3: フィルタが表示された [Device Inventory] ウィンドウ

DEVICE NAME	Device Name	IP Address	Reachability Status	Up Time	Last Updated Time	Poller Time	Last Inventory Collection Status
SDN-DEV-2960-BR4.cisco.com	SDN-DEV-2960-BR4.cisco.com	10.10.10.10	Reachable	9 days, 18:36:38.81	a few seconds ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-3650-BR4	SDN-DEV-3650-BR4	10.10.10.10	Reachable	9 days, 18:35:15.72	a few seconds ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-4332-1-CA2.cisco.com	SDN-DEV-4332-1-CA2.cisco.com	10.10.10.10	Reachable	9 days, 18:37:19.58	a minute ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-4506-CA2	SDN-DEV-4506-CA2	10.10.10.10	Reachable	9 days, 18:35:52.88	a minute ago	00:25:00	ERROR-ENABLE-PASSWORD
SDN-DEV-7K-CA2	SDN-DEV-7K-CA2	10.10.10.10	Reachable	102 days, 0:26:42.43	a few seconds ago	00:25:00	Managed

はじめる前に

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 [デバイス インベントリ (Device Inventory)] ツールバーで、[フィルタ (Filters)] をクリックします。以下のフィルタが表示されます。

- デバイス名 (Device Name)
- Device Location
- Device IP Address
- [デバイス VRF (Device VRF)]

ステップ 2 選択したフィルタのフィールドに適切な値を入力します。例えば、[デバイス名 (Device Name)] フィルタであれば、デバイスの名前を入力します。

他のフィールドに値を入力するときは、コントローラにより自動入力値が提示されます。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。

(注) これらのフィルタにワイルドカード (アスタリスク) を使用することもできます。文字列値の先頭、末尾、または中間にアスタリスクがある値を入力できます。

- ステップ 3** プラス (+) アイコンをクリックして、フィルタを実行します。
[デバイス (Devices)] テーブルに表示されるデータは、フィルタ選択に従って自動的に更新されます。
- ステップ 4** (省略可能) 必要な場合は、上記の手順に従って更にフィルタを追加します。
(注) フィルタごとに複数の値でフィルタリングすることも、複数の異なるフィルタタイプでフィルタリングすることもできます。
- ステップ 5** フィルタを削除するには、フィルタ値の横にある [x] アイコンをクリックします。

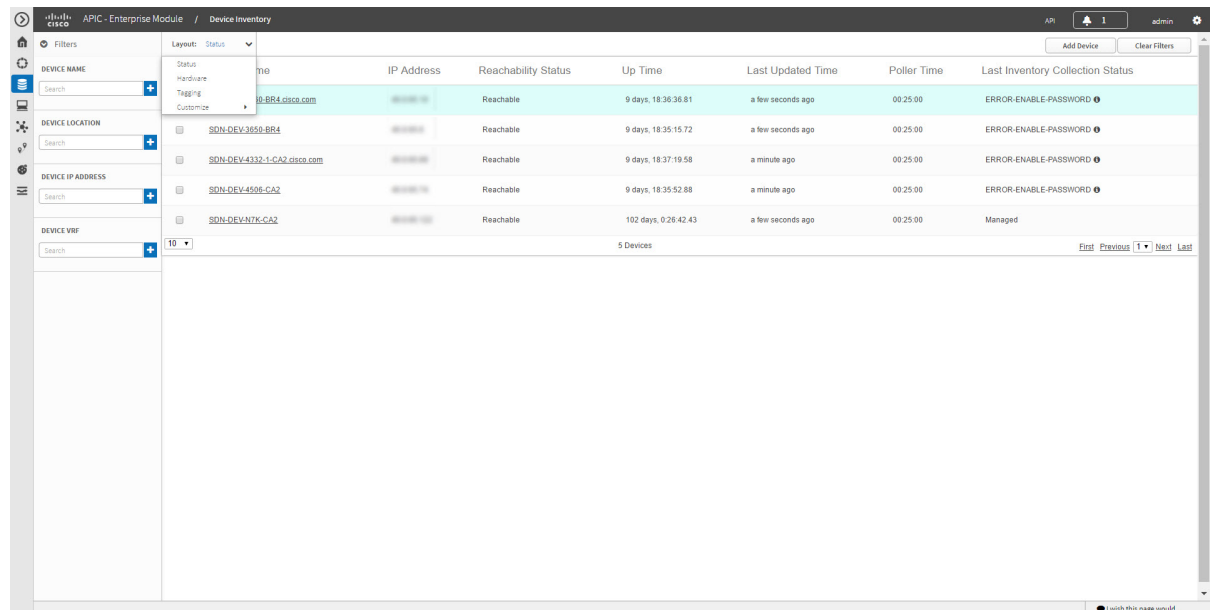
次の作業

[デバイス インベントリ (Device Inventory)] ウィンドウに表示される更新された情報を確認します。ネットワーク構成で必要な場合は、[デバイス (Devices)] テーブルビューに表示されるカラムを変更します。

デバイス レイアウト ビューの変更

さまざまなレイアウトビューを選択、またはネットワーク内のデバイスのレイアウトビューをカスタマイズすることにより、[デバイス (Devices)] テーブルに表示される情報を変更できます。

図 4: [Layout] のオプションが表示された [Device Inventory] ウィンドウ



はじめる前に

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 [Device Inventory] ツールバーで [Layout] フィールドをクリックして、ドロップダウンリストから次のいずれかのレイアウト オプションを選択します。

- ステータス (Status) : アップタイム、更新頻度、更新回数などの一般的なデバイスステータス情報を表示します。
- ハードウェア (Hardware) : IOS/ファームウェア、シリアル番号、デバイスロールなどのハードウェア情報を表示します。
- タギング (Tagging) : デバイス ロール、場所、タグなどのタギング情報を表示します。
- カスタマイズ (Customize) : 独自のレイアウトを作成するために選択できるオプションのリストを表示します。

APIC-EM は、選択したレイアウトの情報を表示します。

ステップ 2 特定のレイアウトをカスタマイズするには、[カスタマイズ (Customize)] を選択して、目的の表示オプションを選択します。
表示オプションのオン/オフが切り替わります。チェックマークの付いた青いオプションは、そのオプションが有効で、テーブルに表示されていることを意味しています。

次の作業

[デバイス インベントリ (Device Inventory)] ウィンドウに表示される更新された情報を確認します。ネットワーク設定の必要に応じて調整してください。

デバイス ロールの変更

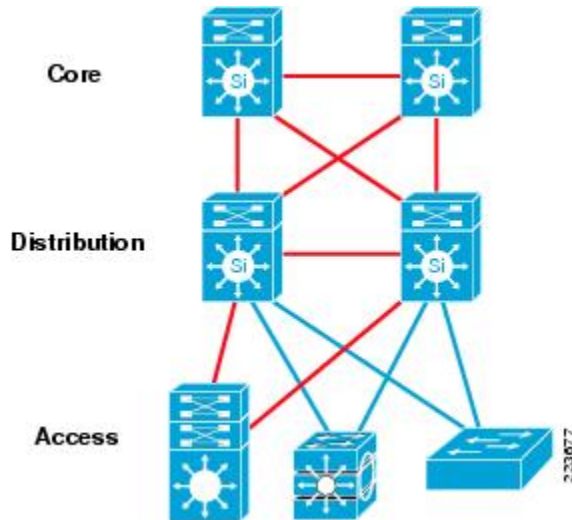
スキャンプロセス中、コントローラは、検出された各デバイスにロールを割り当てます。デバイス ロールは、ネットワーク内での役目と配置に従って、デバイスを識別およびグループ分けするために使用されます。

デバイスは、以下のいずれかのロールを持つことができます。

- 不明 (Unknown) : デバイス ロールが不明です。
- アクセス (Access) : デバイスはネットワークのアクセスレイヤまたは第1階層/エッジに配置され、必要なタスクを実行します。
- ボーダー ルータ (Border Router) : デバイスはボーダー ルータで必要なタスクを実行します。

- ディストリビューション (Distribution) : デバイスはネットワークのディストリビューションレイヤに配置され、必要なタスクを実行します。
- コア (Core) : デバイスはネットワークのコアに配置され、必要なタスクを実行します。

図 5: デバイス ロールとネットワークの場所



デバイス ロールは、[デバイス インベントリ (Device Inventory)] ウィンドウで変更できます。



(注) デバイス ロールは、[トポロジ (Topology)] ウィンドウでも変更できます。[トポロジ (Topology)] ウィンドウ上でのデバイス ロールの変更を参照してください。

はじめる前に

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) 権限またはポリシー管理者 (ROLE_POLICY_ADMIN) 権限と、適切な RBAC 範囲が必要です。

- ステップ 1** [ナビゲーション (Navigation)] ペインで、[デバイス インベントリ (Device Inventory)] をクリックします。
[デバイス インベントリ (Device Inventory)] ウィンドウが表示されます。
- ステップ 2** [デバイス インベントリ (Device Inventory)] ツールバーで、[レイアウト (Layout)] ドロップダウンリストからいずれかのオプションを選択します。
有効なオプションは、[ハードウェア (Hardware)]、[タグging (Tagging)]、または[カスタマイズ (Customize)]>[デバイス ロール (Device Role)] です。テーブルが更新され、[デバイス ロール (Device Role)] のカラムが含まれます。

- ステップ 3** 変更するデバイスを見つけ、[デバイス ロール (Device Role)] カラムのドロップダウン リストから新しいロールを選択します。
- 有効な選択肢は、[不明 (Unknown)]、[アクセス (Access)]、[コア (Core)]、[ディストリビューション (Distribution)]、または [ボーダー ルータ (Border Router)] です。

次の作業

必要に応じて、[デバイス インベントリ (Device Inventory)] ウィンドウで他のデバイスのロールを変更します。

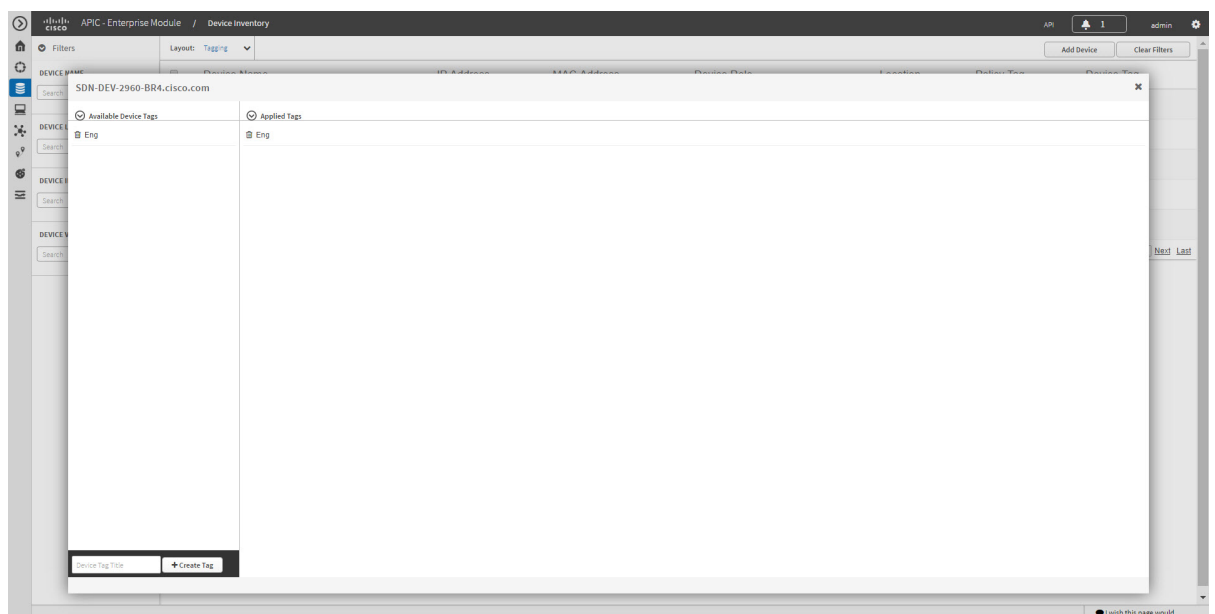
デバイス インベントリでのデバイス タグの追加または削除

デバイス タグを適用することによって、共通の属性に従ってデバイスをグループ化できます。例えば、デバイス タグを適用して、プラットフォーム ID や Cisco IOS リリースによってデバイスをグループ化できます。1 つのデバイスに複数のデバイス タグを設定できます。同様に、1 つのデバイス タグを複数のデバイスに適用することもできます。



- (注) ポリシー タグとロケーション タグの詳細については、[デバイス インベントリでのポリシー タグの追加または削除](#)、(22 ページ) および [ロケーション タグの追加または削除](#)、(23 ページ) を参照してください。

図 6 : [Device Tags] ダイアログ ボックス



はじめる前に

この手順を実行するには、管理者 (ROLE_ADMIN) 権限と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** [ナビゲーション (Navigation)] ペインで、[デバイス インベントリ (Device Inventory)] をクリックします。
- ステップ 2** [デバイス インベントリ (Device Inventory)] ツールバーで、ドロップダウン リストから [レイアウト (Layout)] > [タギング (Tagging)] の順に選択します。
表が更新され、[デバイスタグ (Device Tag)] 列が他の列に加えて表示されます。
- ステップ 3** 対象のデバイスの左にあるチェックボックスをオンにして、[デバイスタグの設定 (Set Device Tags)] をクリックします。
(注) 1つのデバイスについて、[デバイスタグ (Device Tag)] 列に表示されている番号をクリックすることもできます。
- ステップ 4** 次のいずれかを実行します。
- デバイス タグを適用するには、[使用可能なタグ (Available Tags)] リストから、選択したデバイスに適用するタグをクリックします。
 - (注) 目的のタグがリストにない場合は、タグの名前を入力し、[新しいタグの追加 (+New Tag)] をクリックします。
 - デバイス タグを削除するには、[適用済みタグ (Applied Tags)] リストで、選択したデバイスの削除したいタグの横にある [ゴミ箱 (Trash can)] アイコンをクリックします。
 - (注) 選択した1つ以上のデバイスにタグが適用されている場合のみ、[適用済みタグ (Applied Tags)] リストにデータが入力されます。
- ステップ 5** [x] をクリックして、ダイアログボックスを閉じます。
-

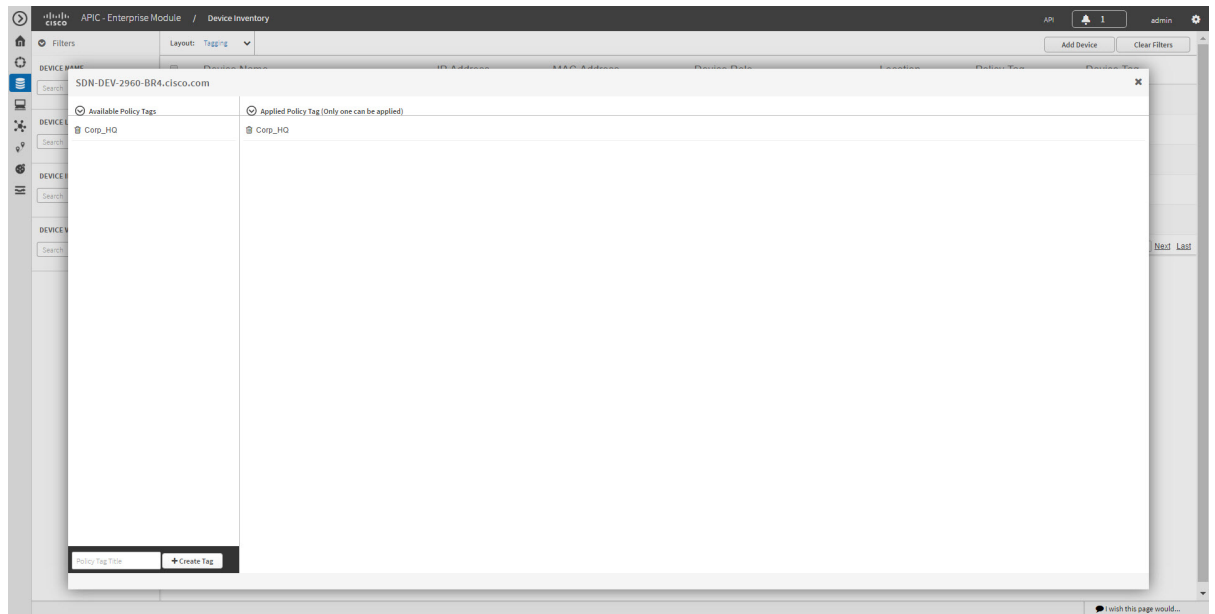
次の作業

ネットワーク設定の必要に応じて、デバイスにロケーションタグまたはポリシータグを追加します。

デバイスインベントリでのポリシータグの追加または削除

ポリシータグをデバイスのグループに適用して、同じQoSポリシーを同時に複数のデバイスに展開できるようにします。

図 7: [Policy Tag] ダイアログボックス



はじめる前に

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。

手順の概要

1. [ナビゲーション (Navigation)] ペインで、[デバイスインベントリ (Device Inventory)] をクリックします。
2. [デバイスインベントリ (Device Inventory)] ツールバーで、ドロップダウンリストから [レイアウト (Layout)] > [タグging (Tagging)] の順に選択します。
3. 対象のデバイスの左にあるチェックボックスをオンにして、[ポリシータグの設定 (Set Policy Tag)] をクリックします。
4. 次のいずれかを実行します。
5. [x] をクリックして、ダイアログボックスを閉じます。

手順の詳細

- ステップ 1** [ナビゲーション (Navigation)] ペインで、[デバイス インベントリ (Device Inventory)] をクリックします。
- ステップ 2** [デバイス インベントリ (Device Inventory)] ツールバーで、ドロップダウン リストから [レイアウト (Layout)] > [タギング (Tagging)] の順に選択します。
表が更新され、[ポリシータグ (Policy Tag)] 列が他の列に加えて表示されます。
- ステップ 3** 対象のデバイスの左にあるチェックボックスをオンにして、[ポリシータグの設定 (Set Policy Tag)] をクリックします。
(注) デバイスが 1 つの場合、[ポリシータグ (Policy Tag)] 列に表示されている [追加 (Add)] をクリックすることもできます。
- ステップ 4** 次のいずれかを実行します。
- ポリシー タグを適用するには、[使用可能なタグ (Available Tags)] リストから、選択したデバイスに適用するタグをクリックします。
 - (注) 目的のタグがリストにない場合は、タグの名前を入力し、[新しいタグの追加 (+New Tag)] をクリックします。
 - ポリシー タグを削除するには、[適用済みタグ (Applied Tags)] リストで、選択したデバイスの削除したいタグの横にある [ゴミ箱 (Trash can)] アイコンをクリックします。
 - (注) 選択した 1 つ以上のデバイスにタグが適用されている場合のみ、[適用済みタグ (Applied Tags)] リストにデータが入力されています。
- ステップ 5** [x] をクリックして、ダイアログボックスを閉じます。

次の作業

デバイスにポリシータグを追加済みの状態で、QoS ポリシーを設定したい場合は、*Cisco EasyQoS Application for APIC-EM User Guide* を参照してください。

ロケーションタグの追加または削除

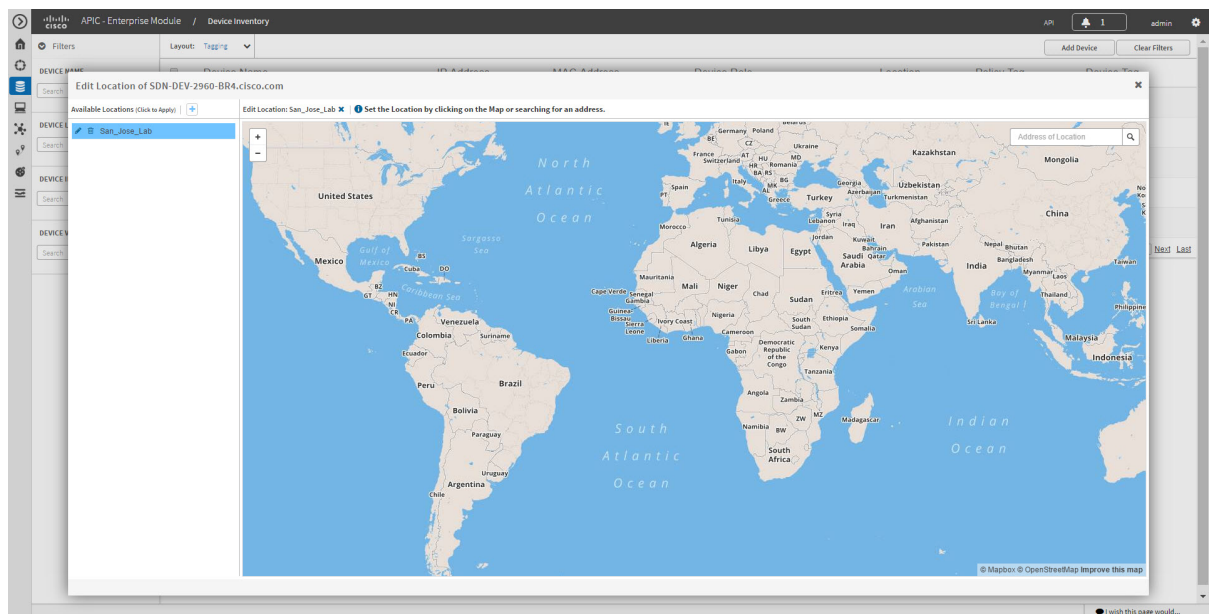
デバイスにロケーションタグを適用して、デバイスの地理的位置に名前を付けることができます。複数のデバイスに同じタグを適用すると、その共通の場所に基づいてデバイスをグループ化することができます。ロケーションタグを作成し、必要に応じて、対応するロケーション マーカーを地図上に配置することができます。詳細については、[ロケーション マーカーの追加または変更](#)、(25 ページ) を参照してください。

ロケーション タグを追加する場合は、次のガイドラインを使用します。

- ロケーションタグの情報はコントローラのみで保持され、デバイスに展開されることもデバイスから導出されることもありません。

- ロケーションタグおよびマーカを使用すると、[Topology] ウィンドウで、地図上にタグとマーカが表示されます。
- コントローラに定義されるロケーションは、一部のデバイスがサポートしている「シビックロケーション」プロパティではありません。
- ホストにロケーションタグを付けることはできません。
- 1つのデバイスに適用できるのは1つのロケーションタグのみです。ただし、ロケーションタグとデバイスタグを同時に使用することは可能です。

図 8 : [Set Location Tag] ダイアログボックス



はじめる前に

この手順を実行するには、管理者（ROLE_ADMIN）権限とすべてのデバイスへのアクセス権（[RBAC Scope] を [ALL] に設定）が必要です。

- ステップ 1** [ナビゲーション (Navigation)] ペインで、[デバイスインベントリ (Device Inventory)] をクリックします。
- ステップ 2** [デバイスインベントリ (Device Inventory)] ツールバーで、ドロップダウンリストから [レイアウト (Layout)] > [タグging (Tagging)] の順に選択します。
表が更新され、[ロケーション (Location)] 列が他の列に加えて表示されます。
- ステップ 3** 目的のデバイスの左側のチェックボックスを選択（または、すべてのデバイスを選択する場合はリストの上部にあるチェックボックスを選択）し、[Set Location] をクリックします。
(注) デバイスが1つの場合は、そのデバイスの [Location] 列に表示される [Add] リンクをクリックすることもできます。

ステップ4 次のいずれかを実行します。

- ロケーションタグを適用するには、[Available Tags] リストから、選択したデバイスに適用するタグをクリックします。目的のタグがリストにない場合は、プラス記号 (+) のアイコンをクリックし、タグの名前を入力して、チェックマークのアイコンをクリックします。
- デバイスからロケーションタグの割り当てを解除するには、[Edit Location] フィールドで [x] アイコンをクリックします。これで、デバイスに割り当てられたロケーションタグはなくなります。
- 現在のロケーションタグを別のタグに変更するには、割り当てる新しいロケーションタグをクリックします。
- ロケーションタグを削除するには、まず、それがどこにも使用されていないことを確認します（デバイス割り当てを他のロケーションタグに変更するか、タグの割り当てをすべて解除します）。その後、削除したいロケーションタグの横にあるゴミ箱のアイコンをクリックします。

ステップ5 完了したら、[x] をクリックして、このダイアログボックスを閉じます。

次の作業

ネットワーク設定の必要に応じて、他のデバイスに対して他のロケーションタグを追加または削除したり、ロケーションマーカを追加したりします。

関連トピック

[ロケーションマーカの追加または変更](#)、(25 ページ)

ロケーションマーカの追加または変更

ロケーションマーカとは、デバイスの場所を示すために使用される、地図上のロケーションタグに関連付けられたアイコンです。[Device Inventory] ウィンドウで、デバイスにロケーションマーカを追加することができます。

はじめる前に

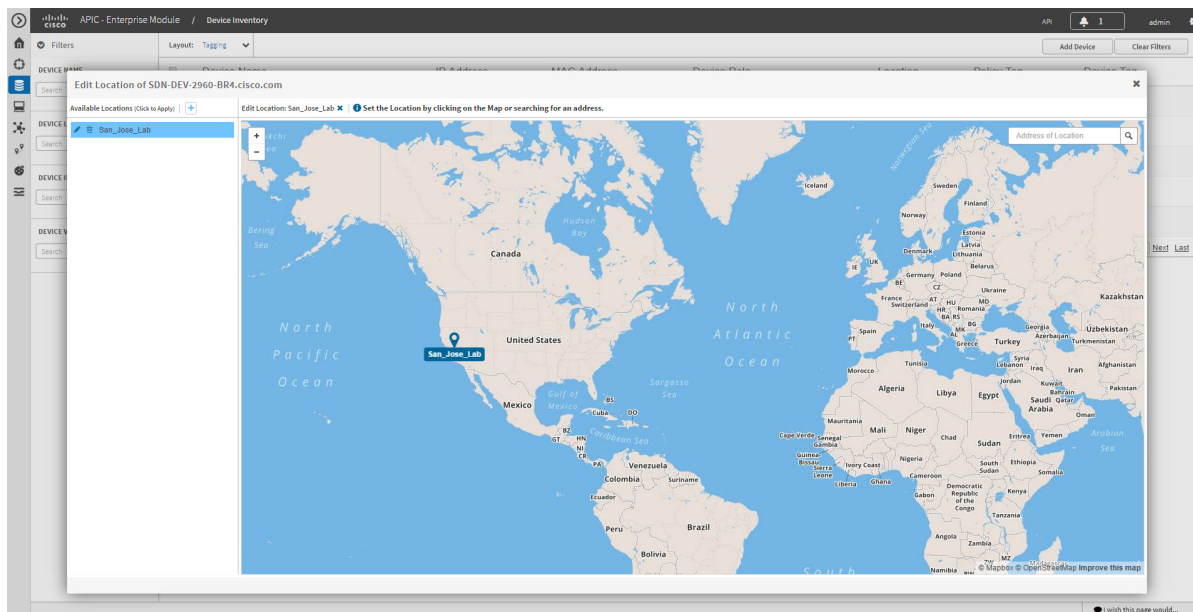
この手順を実行するには、管理者 (ROLE_ADMIN) 権限とすべてのデバイスへのアクセス権 ([RBAC Scope] を [ALL] に設定) が必要です。

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。

デバイスにすでにロケーション タグを追加しています。

-
- ステップ 1** [ナビゲーション (Navigation)] ペインで、[デバイス インベントリ (Device Inventory)] をクリックします。
- ステップ 2** [デバイス インベントリ (Device Inventory)] ツールバーで、ドロップダウン リストから [レイアウト (Layout)] > [タギング (Tagging)] の順に選択します。
表が更新され、[ロケーション (Location)] 列が他の列に加えて表示されます。
- ステップ 3** (省略可能) 特定のロケーション タグを持つデバイスを表示するには、[デバイス インベントリ (Device Inventory)] ツールバーで、[フィルタ (Filters)] をクリックし、[デバイスロケーション (Device Location)] フィールドにロケーション タグを入力し、[+] アイコンをクリックします。
- ステップ 4** [Locations] 列から目的のロケーション タグを選択します。
(注) ロケーション タグを割り当てないため、どのデバイスを選択するかは重要ではありません。ロケーション マーカーを追加または削除すると、その変更はロケーション タグに適用され、ロケーション タグが付けられているすべてのデバイスが更新されます。
- ステップ 5** ロケーション マーカーを追加または変更するには、[Available Locations] ペインからロケーション タグを選択し、次のいずれかを実行します。
- 地図の右側の [Address of Location] フィールドで、ロケーション マーカーを配置する住所を入力します。入力する住所は、すべてでも一部（都市名や郵便番号など）でもかまいません。Cisco APIC-EM が地図上に場所を表示します。地図上でマーカーを配置する場所をクリックし、表示される確認ダイアログ ボックスでアクションを確認します。
 - マウスを使ったドラッグ アンド ドロップで目的の場所のできるだけ近くに地図を動かし、拡大または縮小して、地図をクリックします。
- (注) マーカーの位置を変更する場合は、地図上でマーカーを置く場所を再びクリックします。

図 9: ロケーション マーカーが表示された *Edit Location* ダイアログ ボックス



- ステップ 6 (任意) 別のロケーション マーカーを追加するには、別のロケーション タグをクリックし、ステップ 5 を繰り返します。
- ステップ 7 完了したら、[x] をクリックして、このダイアログボックスを閉じます。

タグの削除

デバイス タグ、ポリシー タグ、またはロケーション タグが不要になった場合は削除することができ、コントローラから永続的に削除されます。[デバイスインベントリ (Device Inventory)] ウィンドウまたは [トポロジ (Topology)] ウィンドウを使用して、デバイス タグを削除できます。ポリシー タグとロケーション タグは [デバイスインベントリ (Device Inventory)] ウィンドウでのみ削除できます。この手順では、[デバイスインベントリ (Device Inventory)] ウィンドウでタグを削除する方法を示します。

はじめる前に

この手順を実行するには、管理者 (ROLE_ADMIN) 権限と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。

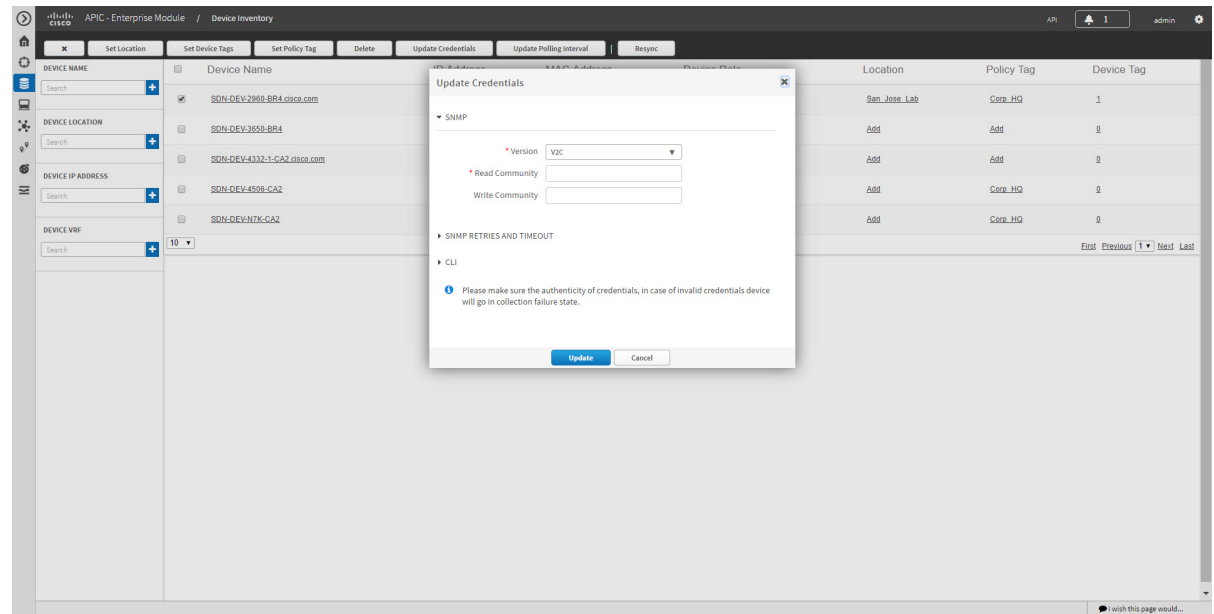
タグを削除する前に、そのタグが割り当てられているすべてのデバイスからそのタグを削除する必要があります。

-
- ステップ 1** [ナビゲーション (Navigation)] ペインで、[デバイス インベントリ (Device Inventory)] をクリックします。
- ステップ 2** [デバイス インベントリ (Device Inventory)] ツールバーで、ドロップダウン リストから [レイアウト (Layout)] > [タグging (Tagging)] の順に選択します。
- ステップ 3** 次のいずれかを実行します。
- デバイス タグを削除するには、[デバイス タグ (Device Tag)] カラムで任意の番号をクリックします。[使用可能なタグ (Available Tags)] リストで、削除するタグの横にある [ゴミ箱 (Trash can)] アイコンをクリックします。
 - ポリシー タグを削除するには、[ポリシー タグ (Policy Tag)] カラムで [追加 (Add)] をクリックするか、ポリシー タグの名前をクリックします。[使用可能なタグ (Available Tags)] リストで、削除するタグの横にある [ゴミ箱 (Trash can)] アイコンをクリックします。
 - ロケーション タグを削除するには、[ロケーション (Location)] カラムで [追加 (Add)] をクリックするか、ロケーション タグ名をクリックします。[使用可能なロケーション (Available Locations)] リストで、削除するタグの横にある [ゴミ箱 (Trash can)] アイコンをクリックします。
- ステップ 4** [OK] をクリックして、削除を実行します。
タグはコントローラから永続的に削除されます。
- 削除が失敗した場合、タグはデバイスに割り当てられたままになっている可能性があります。これらのデバイスからタグを削除してから、再度タグを削除してみます。
- ステップ 5** [x] をクリックして、ダイアログボックスを閉じます。
-

デバイス クレデンシャルの更新

選択したデバイスの検出クレデンシャルを更新できます。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。

図 10 : [Update Device Credentials] ダイアログ ボックス



はじめる前に

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) 権限またはポリシー管理者 (ROLE_POLICY_ADMIN) 権限と、適切な RBAC 範囲が必要です。

- ステップ 1 [ナビゲーション (Navigation)] ペインで、[デバイス インベントリ (Device Inventory)] をクリックします。
- ステップ 2 更新するデバイスを選択します。
- ステップ 3 [Update Credentials] をクリックします。
- ステップ 4 [OK] をクリックして、このアクションを確認します。
- ステップ 5 [Update Credentials] ダイアログ ボックスの [SNMP] エリアがまだ展開されていない場合は、展開します。
- ステップ 6 [Version] フィールドで、ドロップダウン リストから SNMP バージョン ([V2C] または [V3]) を選択し、対応する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 クレデンシャルのみを提供すると、Cisco APIC-EM は SNMP クレデンシャルのみを保存します。CLI クレデンシャルは更新されません。

表 7: **SNMP V2C** のフィールド

フィールド	説明
Read Community	デバイスに対する接続とアクセスをコントローラに許可するデバイスで設定されている read-only コミュニティストリング値。このコミュニティストリング値は、デバイスで事前設定されているコミュニティストリング値と一致する必要があります。
Write Community	デバイスに対する接続、アクセス、変更をコントローラに許可するデバイスで設定されている write コミュニティストリング値。このコミュニティストリング値は、デバイスで事前設定されているコミュニティストリング値と一致する必要があります。

表 8: **SNMP V3** のフィールド

フィールド	説明
モード	使用する認証モード。有効なモードとして、[Authentication and Privacy]、[Authentication, No Privacy]、[No Authentication, No Privacy] があります。
Auth.タイプ	[Authentication and Privacy] または [Authentication, No Privacy] を選択したときにのみ有効。2つの認証タイプがあります。 <ul style="list-style-type: none"> • [SHA] : セキュアハッシュアルゴリズム (SHA) に基づく認証。SHA は、パケットデータの認証に使用されるハッシュアルゴリズムです。 • [MD5] : Message Digest 5 (MD5) アルゴリズムに基づく認証。MD5 は、パケットデータの認証に使用されるハッシュアルゴリズムです。
ユーザ名	[SHA] または [MD5] を選択したときにのみ有効。 SNMP ユーザおよび選択された認証タイプ (MD5 または SHA) に関連付けられる文字列。

フィールド	説明
Auth.パスワード	[SHA] または [MD5] を選択したときにのみ有効。 SNMP ユーザパスワードとして保存され、認証タイプ (MD5 または SHA) に関連付けられる、暗号化された文字列。
Privacy Type	[Authentication and Privacy] モードを選択したときにのみ有効。 2つのプライバシータイプがあります。 <ul style="list-style-type: none"> • DES : データ暗号規格 (DES) の 56 ビット暗号化、および暗号ブロック連鎖 (CBC) DES (DES-56) 標準に基づく認証 • AES128 : 暗号ブロック連鎖 (CBC) モードの AES 暗号化
Privacy Password	選択したプライバシーのタイプ (DES または AES128) に関連付けられ、デバイスとやり取りするメッセージの暗号化用秘密キーの生成に使用される、SNMPv3 プライバシーパスワード。

ステップ 7 [SNMP Retries and Timeout] エリアがまだ展開されていない場合は展開し、次のフィールドに入力します。

表 9 : [SNMP Retries and Timeout] のフィールド

フィールド	説明
Retries	コントローラが SNMP を使用してデバイスとの通信を試みる回数。デフォルトは、3 回です。
Timeout	コントローラが SNMP を使用してデバイスとの通信を試みる際に、失敗とみなされるまでに待機する秒数。デフォルトは 5 秒です。

ステップ 8 [CLI] エリアがまだ展開されていない場合は展開し、次のフィールドに入力します。

(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 クレデンシャルのみを提供すると、Cisco APIC-EM は SNMP クレデンシャルのみを保存します。CLI クレデンシャルは更新されません。

表 10 : [CLI] のフィールド

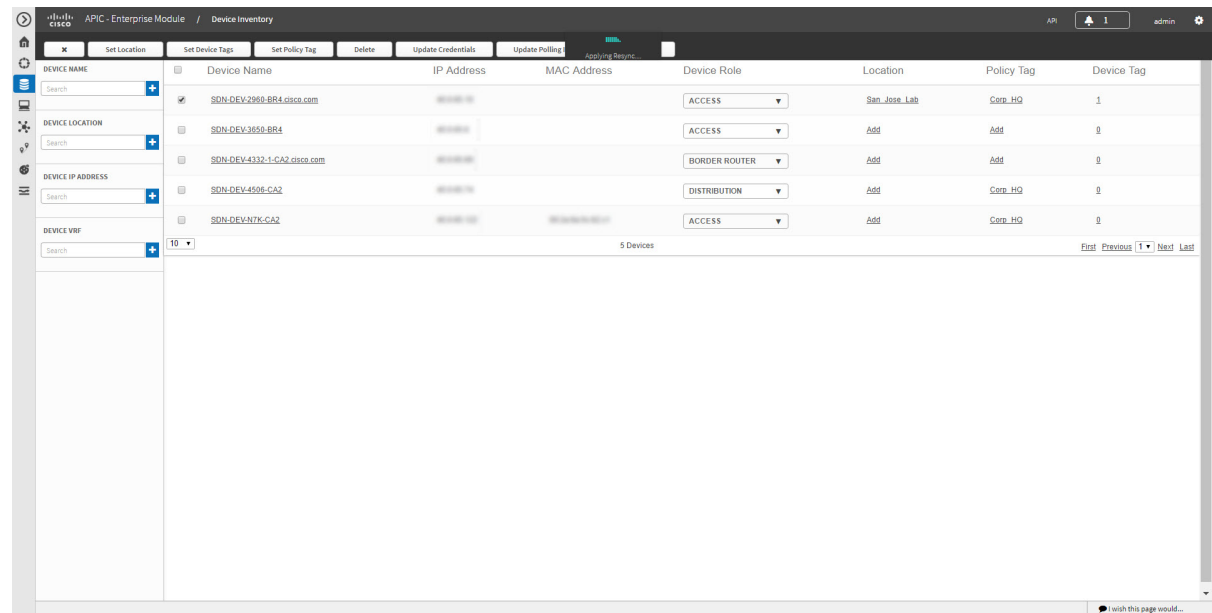
フィールド	説明
Protocol	リモート管理ステーションからデバイス CLI 接続のために使用されるプロトコル。有効なオプションとして、[Telnet] (Telnet TCP/IP)、[SSH2] (セキュアシェル 2.0) があります。
Username	デバイスの CLI にログインするために使用される ID。
パスワード	デバイスの CLI にログインするために使用されるパスワード。
Enable Password	CLI へのログインが成功した後で、特権 EXEC モードへのアクセスに使用されるパスワード。

ステップ 9 [Update] をクリックします。

デバイス情報の再同期

設定されているポーリング間隔にかかわらず、今すぐポーリングするデバイスを選択して、更新されたデバイスおよびステータス情報を収集することが可能です。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。

図 11：再同期が進行中であることを示す [Device Inventory] ウィンドウ



- ステップ 1 [ナビゲーション (Navigation)] ペインで、[デバイス インベントリ (Device Inventory)] をクリックします。
- ステップ 2 情報収集の対象とするデバイスを選択します。
- ステップ 3 [Resync] をクリックします。
- ステップ 4 [OK] をクリックして再同期を確認します。

デバイスでのコマンド実行

選択したデバイスで [show] コマンドやその他の読み取り専用コマンドを実行して、出力を Cisco APIC-EM に表示することができます。可能なコマンドキーワードを判定するには、グローバル ツールバーから [API] > [Network Poller] > [network-device-poller] > [/network-device-poller/cli/legit-reads] > [Try it out!] をクリックします。

GUI から、デバイス 1 台あたり最大 5 つのコマンドを実行できます。要求 1 つにつき可能な最大デバイス数は 20 です。あるデバイスが別の要求に含まれていて、その要求が未完了である場合には、そのデバイスで他のコマンドが実行されることはありません。

アクセスポイントはサポートされていません。アクセスポイントを選択しても、それはコマンドの実行では無視されます。コマンドは、選択されている他のデバイスでのみ動作します。

はじめる前に

デフォルトでは Cisco APIC-EM にコマンドランナーアプリケーションはインストールされていません。コマンドランニングアプリケーションを使用するには、Cisco.com からイメージをダウンロードしてインストールし、コマンドランナーアプリケーションを有効にする必要があります。詳細については、*Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide* を参照してください。

この手順を実行するには、管理者 (ROLE_ADMIN) 権限またはポリシー管理者 (ROLE_POLICY_ADMIN) 権限と、適切な RBAC 範囲が必要です。

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。

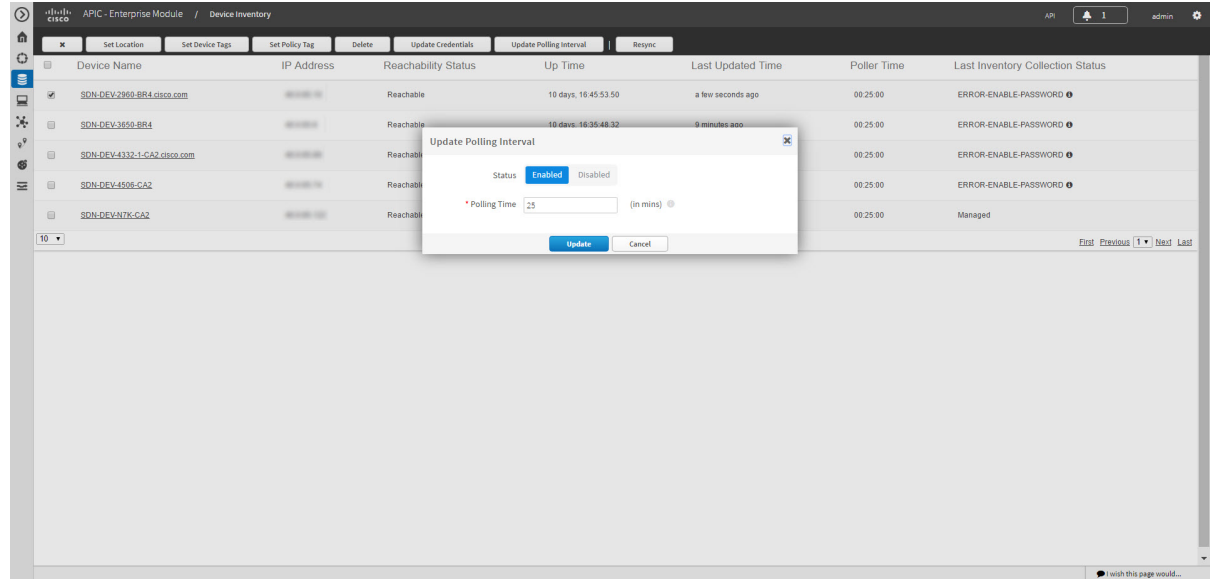
-
- ステップ 1 [ナビゲーション (Navigation)] ペインで、[デバイス インベントリ (Device Inventory)] をクリックします。
 - ステップ 2 コマンドを実行するデバイスを選択します。
 - ステップ 3 [Command Runner] をクリックします。
 - ステップ 4 [Command] フィールドに、実行したいコマンドを入力し、プラス記号 (+) のアイコンをクリックしてコマンドを実行コマンドのリストに追加します。
追加可能なコマンドの数は、一度に 1 つずつ、合計で 5 つまでです。
 - ステップ 5 実行するコマンドすべてを定義したら、[Run] をクリックします。
Cisco APIC-EM により、選択されたデバイスでコマンドが実行され、コマンド出力が表示されます。
(注) コマンドランナーでは、コマンド結果のキャッシュまたは履歴は保持されません。コマンド実行後にウィンドウを終了または別のウィンドウに移動すると、コマンドランナーで実行されたすべてのアクションとその結果は失われます。
-

デバイスのポーリング間隔の更新

ポーリング間隔の更新は、すべてのデバイスに適用するグローバル レベルの場合は [Settings] > [Polling Interval] ページで、または特定のデバイスに適用するデバイス レベルの場合は [Device Inventory] ウィンドウで、それぞれ実施できます。デバイス レベルのポーリング間隔を設定すると、その値はグローバルなポーリング間隔値よりも優先されます。

グローバル レベルのポーリング間隔の設定については、*Cisco Application Policy Infrastructure Controller Enterprise Module Administrator Guide*を参照してください。

図 12 : [Update Polling Interval] ダイアログ ボックス



はじめる前に

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) 権限またはポリシー管理者 (ROLE_POLICY_ADMIN) 権限と、適切な RBAC 範囲が必要です。

- ステップ 1 [ナビゲーション (Navigation)] ペインで、[デバイス インベントリ (Device Inventory)] をクリックします。
- ステップ 2 更新するデバイスを選択します。
- ステップ 3 [Update Polling Interval] をクリックします
- ステップ 4 [OK] をクリックして、このアクションを確認します。
- ステップ 5 [Update Polling Interval] ダイアログ ボックスの [Status] フィールドで、[Enabled] をクリックしてポーリングを有効にするか、[Disabled] をクリックしてポーリングを無効にします。
- ステップ 6 [Polling Time] フィールドには、継続的なポーリング サイクルの間隔 (分単位) を入力します。有効な値は、25 ~ 1,440 分 (24 時間) です。
(注) デバイス固有のポーリング時間は、グローバルなポーリング時間より優先されます。デバイス固有のポーリング時間を設定した後でグローバルなポーリング時間を変更した場合、Cisco APIC-EM は引き続きデバイス固有のポーリング時間を使用します。

ステップ7 [Update] をクリックします。

ホストインベントリの管理

Cisco APIC-EM では、[ホストインベントリ (Host Inventory)] ウィンドウで検出されたホストに関する情報を表示します。

次の表に、インベントリのホストについて表示される情報を示します。



(注) 表に表示されるホスト数 (10、25、50、100) を制限するには、またはホストのグループ (最初、前、次、最後、または1-3) を一度に表示するには、[ホストインベントリ (Host Inventory)] テーブルの下にあるフィルタを使用します。

図 13: [ホストインベントリ (Host Inventory)] ウィンドウ

Host MAC Address	Host IP Address	Host Type	Connected Device IP Address	Connected Interface Name	Host Name
02:50:56:b0:75:02	10.10.10.1	WIRELESS	10.10.10.1	GigabitEthernet1/0/1	
02:50:56:b0:75:03	10.10.10.2	WIRELESS	10.10.10.2	GigabitEthernet1/0/2	
02:50:56:b0:75:04	10.10.10.3	WIRELESS	10.10.10.3	GigabitEthernet1/0/3	
02:50:56:b0:75:05	10.10.10.4	WIRELESS	10.10.10.4	GigabitEthernet1/0/4	
02:50:56:b0:75:06	10.10.10.5	WIRELESS	10.10.10.5	GigabitEthernet1/0/5	
02:50:56:b0:75:07	10.10.10.6	WIRELESS	10.10.10.6	GigabitEthernet1/0/6	
02:50:56:b0:75:08	10.10.10.7	WIRELESS	10.10.10.7	GigabitEthernet1/0/7	
02:50:56:b0:75:09	10.10.10.8	WIRELESS	10.10.10.8	GigabitEthernet1/0/8	
02:50:56:b0:75:10	10.10.10.9	WIRELESS	10.10.10.9	GigabitEthernet1/0/9	
02:50:56:b0:75:11	10.10.10.10	WIRELESS	10.10.10.10	GigabitEthernet1/0/10	

次の表に、インベントリのホストについて表示される情報を示します。

表 11: ホストインベントリ (Host Inventory)

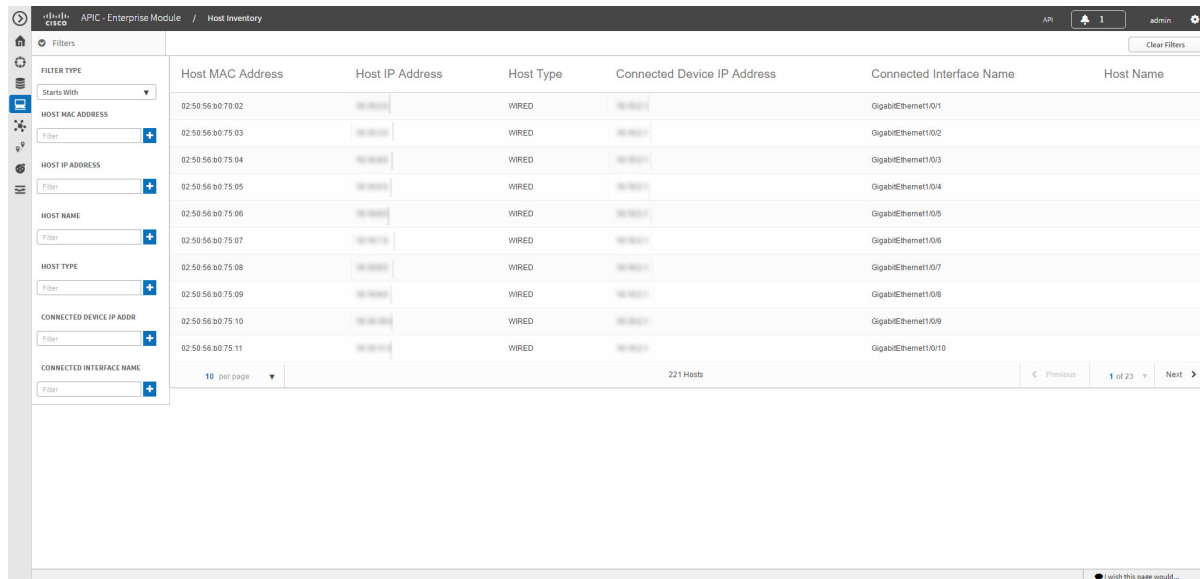
ホストインベントリ (Host Inventory)	説明
Host Name	ホストの名前。
ホスト MAC アドレス (Host MAC address)	ホストの MAC アドレス。

ホスト インベントリ (Host Inventory)	説明
ホスト IP アドレス	ホストの IP アドレス。
ホスト タイプ (Host Type)	ホストのタイプ (有線またはワイヤレス)。
接続されたネットワーク デバイスの IP アドレス (Connected Network Device IP Address)	ホストに接続されているデバイスの IP アドレス。 (注) 有線デバイスの IP アドレスのみが表示されます。
接続されたインターフェイス名 (Connected Interface Name)	デバイスが接続されているインターフェイスの名前。たとえば、GigabitEthernet1/0/24。

[Host Inventory] ウィンドウでのホストのフィルタリング

[Host Inventory] ウィンドウに表示されているホストを、ホストの MAC アドレス、ホストの IP アドレス、ホスト名、ホストのタイプ、接続されたネットワークデバイスの IP アドレス、接続されているインターフェイス名によりフィルタリングすることができます。

図 14 : [Filter] ペインが表示された [Host Inventory] ウィンドウ



はじめる前に

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

ステップ 1 [Host Inventory] ツールバーで、[Filters] をクリックします。
次のフィルタ オプションから選択できます。

- Host MAC Address
- Host IP Address
- Host Name
- Host Type
- 接続されたネットワーク デバイスの IP アドレス (Connected Network Device IP Address)
- 接続されたインターフェイス名 (Connected Interface Name)

ステップ 2 選択したフィルタのフィールドに適切な値を入力します。
たとえば、[Host Name] フィルタであれば、ホストの名前を入力します。

他のフィールドに値を入力するときは、コントローラにより自動入力値が提示されます。いずれかの推奨値を選択するか、または値の入力を終了します。

(注) これらのフィルタにワイルドカード (アスタリスク) を使用することもできます。文字列値の先頭、末尾、または中間にアスタリスクがある値を入力できます。

ステップ 3 プラス (+) アイコンをクリックして、フィルタを実行します。
[デバイス (Devices)] テーブルに表示されるデータは、フィルタ選択に従って自動的に更新されます。

ステップ 4 (省略可能) 必要な場合は、上記の手順に従って更にフィルタを追加します。
(注) フィルタごとに複数の値でフィルタリングすることも、複数の異なるフィルタ タイプでフィルタリングすることもできます。

ステップ 5 フィルタを削除するには、フィルタ値の横にある [x] アイコンをクリックします。
