デバイスからSecurity Managerへの同期の設定

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

背景説明

デモンストレーションの方法

単一デバイスの検出

単一デバイス検出を実行する手順：

単一デバイス検出を実行する手順：

- ステップ 1：
- ステップ 2：

デバイスの一括検出

デバイスの一括検出を実行する手順：

- ステップ 1：
- ステップ 2：
- ステップ 3：

はじめに

このドキュメントでは、ASAからCSMへの設定同期のさまざまな方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Security Manager
- 適応型セキュリティデバイス

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Security Manager 4.25
- 適応型セキュリティアプライアンス

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Cisco Security Managerは、Cisco ASAデバイスに対する中央集中型の管理およびモニタリングサービスを提供します。

デモンストレーションの方法

このドキュメントでは、ASAからCSMに設定を同期するための2つの異なる方法またはオプションについて説明します。

- 単一デバイスの検出
- デバイスの一括再検出

単一デバイスの検出

デバイスがインベントリに追加されている場合にのみ、1つの検出を実行できます。このコマンドは、デバイスが次の条件を満たしている場合にのみ実行できます。

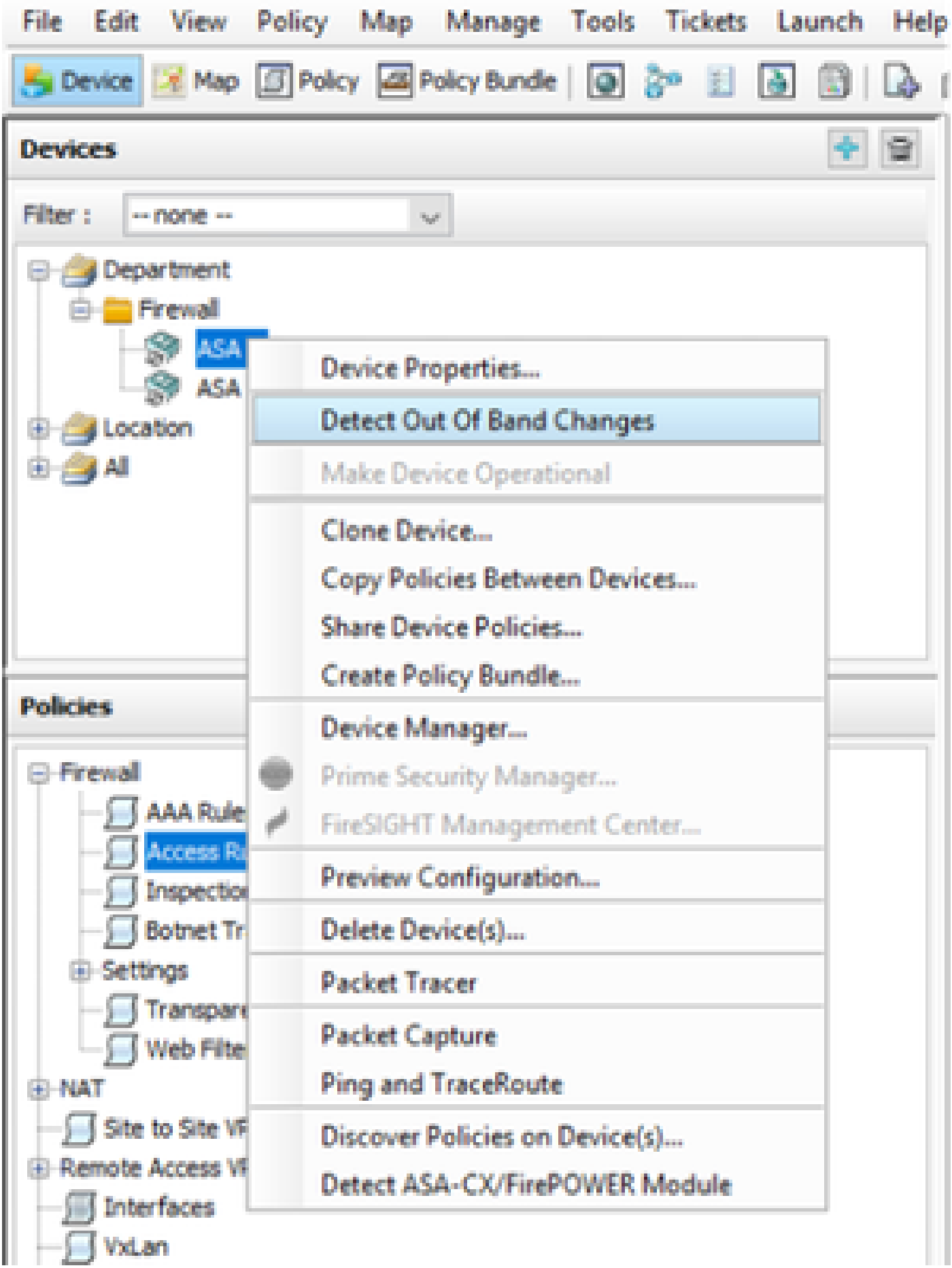
- マルチコンテキストモードで動作するASA、PIX、およびFWSMデバイスのセキュリティコンテキスト設定。
- IPSデバイス用の仮想センサー設定。
- Catalystデバイスのサービスモジュール情報。

単一デバイス検出を実行する手順：

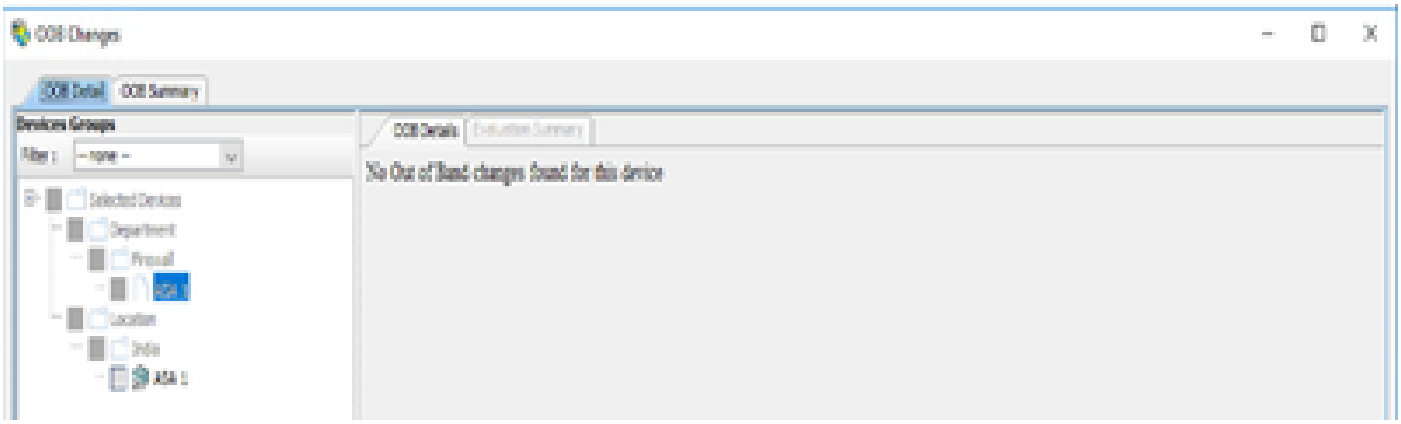
デバイスCLIで変更を行った後、またはデバイスを削除して再度追加した場合に、デバイス検出を実行できます。

保留中の変更がまだ同期されていないかどうかを確認するには、前述の例を参照してください。

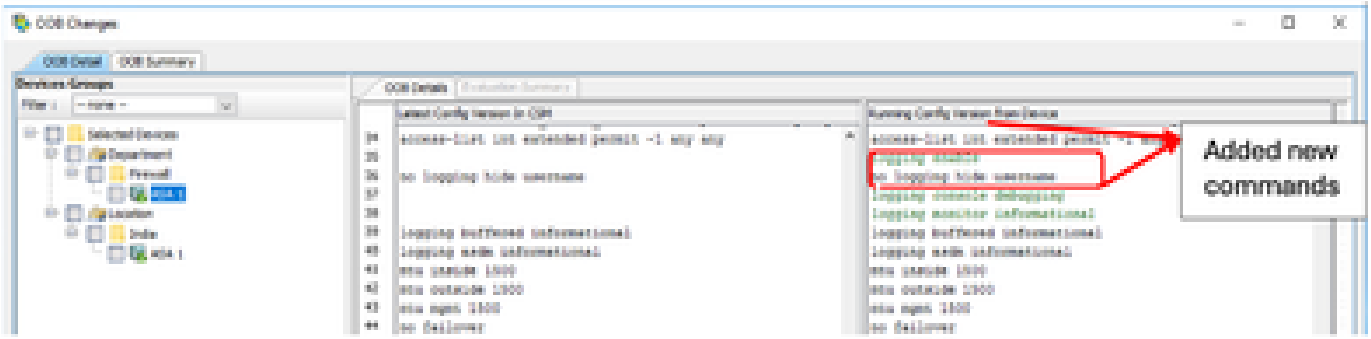
デバイスペインでそれぞれのデバイスを右クリックし、Detect out of band changesオプションを選択します。



変更がない場合（変更がない場合）、ページには、このデバイスに対する範囲外の変更は見つからないと表示されます。



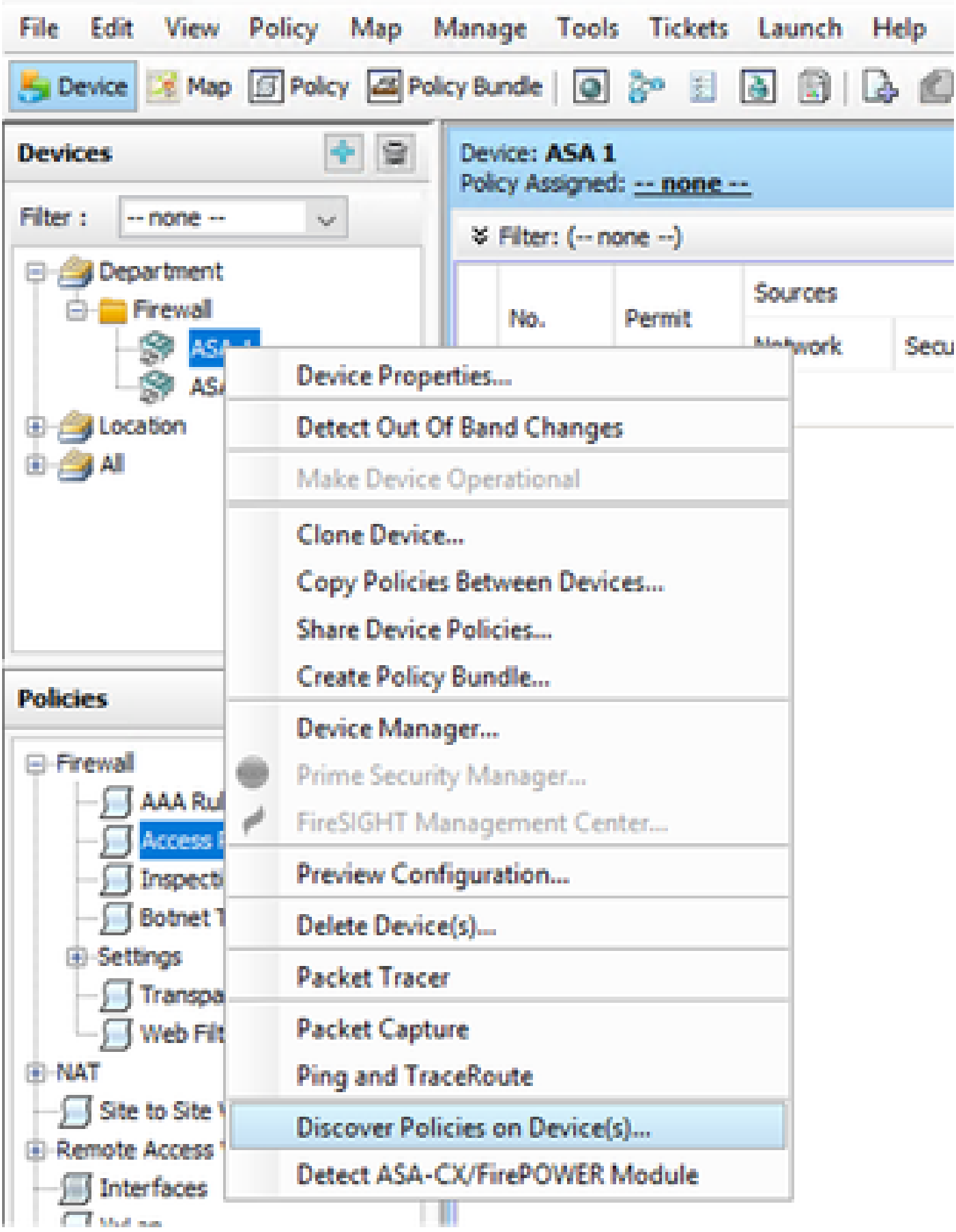
何らかの変更が行われた場合（たとえば、変更が加えられた場合）、その行は凡例に従って強調表示されます。



単一デバイス検出を実行する手順：

ステップ 1：

デバイスペインでそれぞれのデバイス名を右クリックし、Discover policies on Device(s)オプションを選択します。

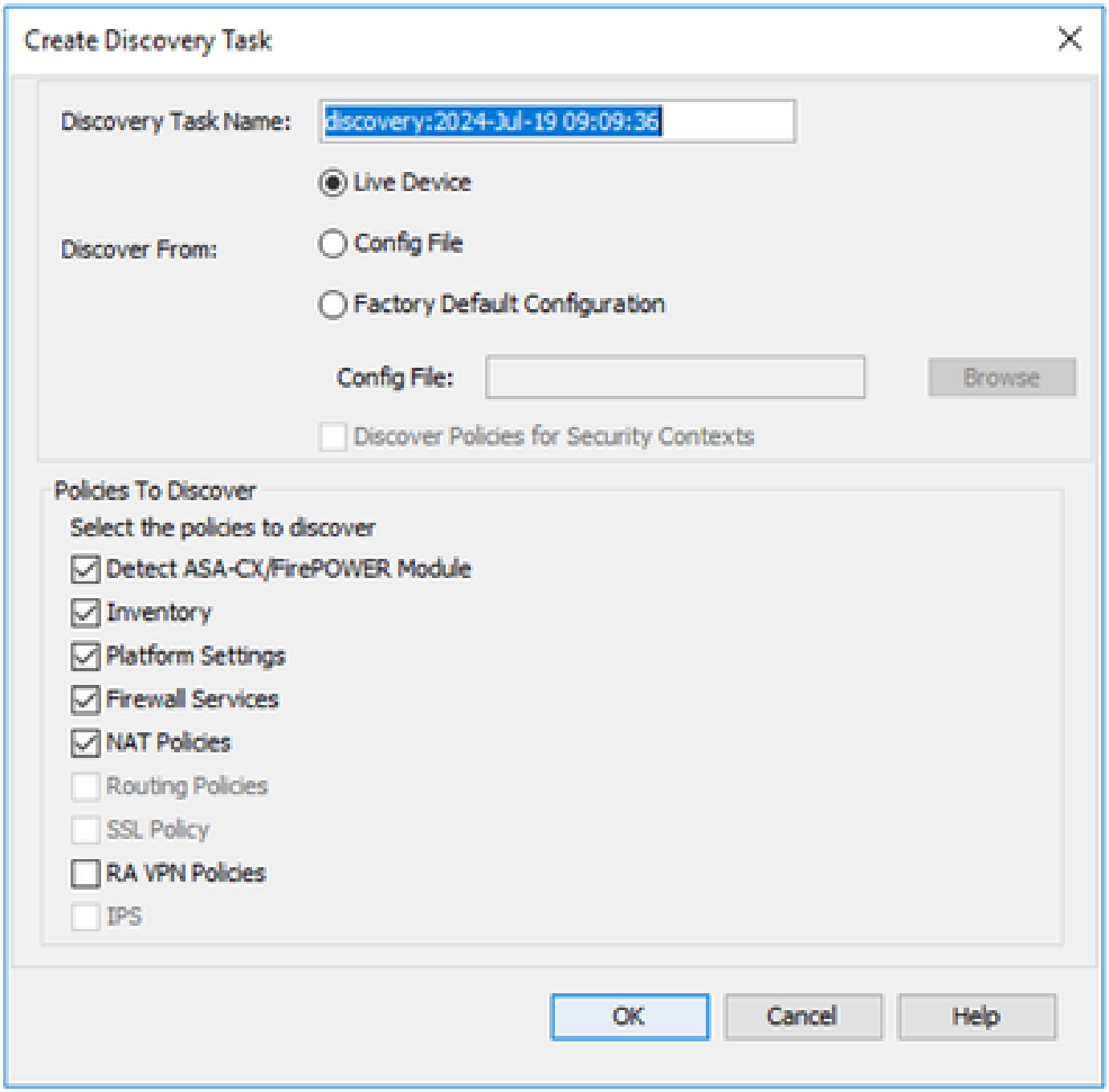

File Edit View Policy Map Manage Tools Tickets Launch Help
Device Map Policy Policy Bundle
Devices
Filter : -- none --
Department
Firewall
Location
All
Device: ASA 1
Policy Assigned: -- none --
Filter: (-- none --)
No.
Permit
Sources
Device Properties...
Detect Out Of Band Changes
Make Device Operational
Clone Device...
Copy Policies Between Devices...
Share Device Policies...
Create Policy Bundle...
Device Manager...
Prime Security Manager...
FireSIGHT Management Center...
Preview Configuration...
Delete Device(s)...
Packet Tracer
Packet Capture
Ping and TraceRoute
Discover Policies on Device(s)...
Detect ASA-CX/FirePOWER Module
Policies
Firewall
Settings
NAT
Interfaces

ステップ 2 :

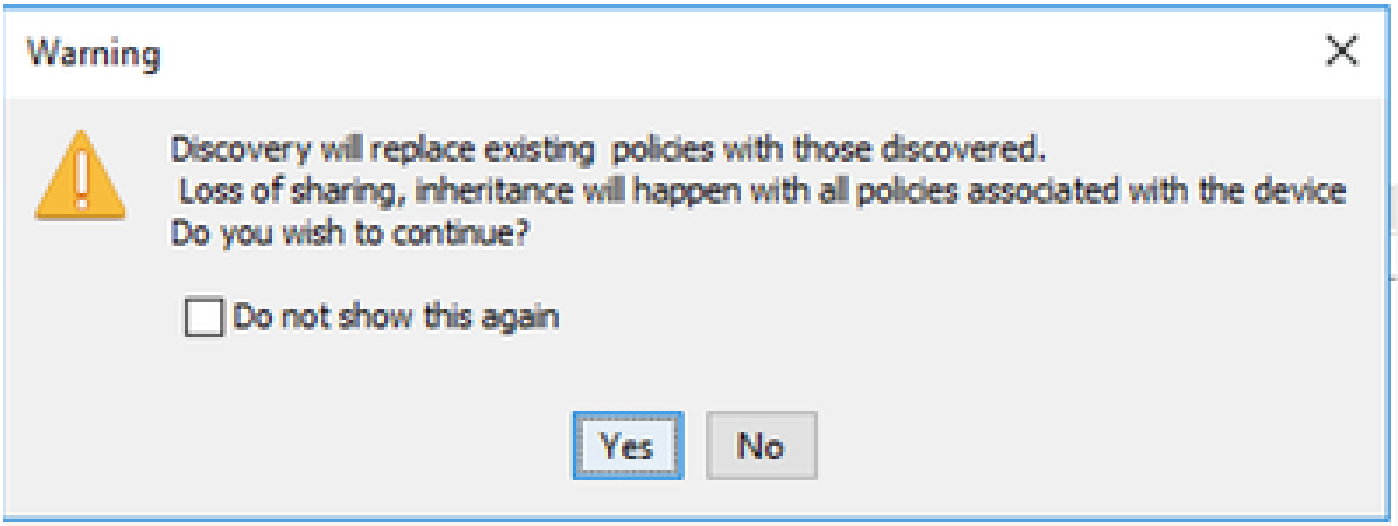
単一デバイスのリカバリ方法の場合、[Create Discovery Task]ダイアログ・ボックスのみが表示されます。バルク検出ダイアログボックスが表示される場合は、親切に閉じて、もう一度開いてください。

ディスカバリを実行するオプションは3つあります。

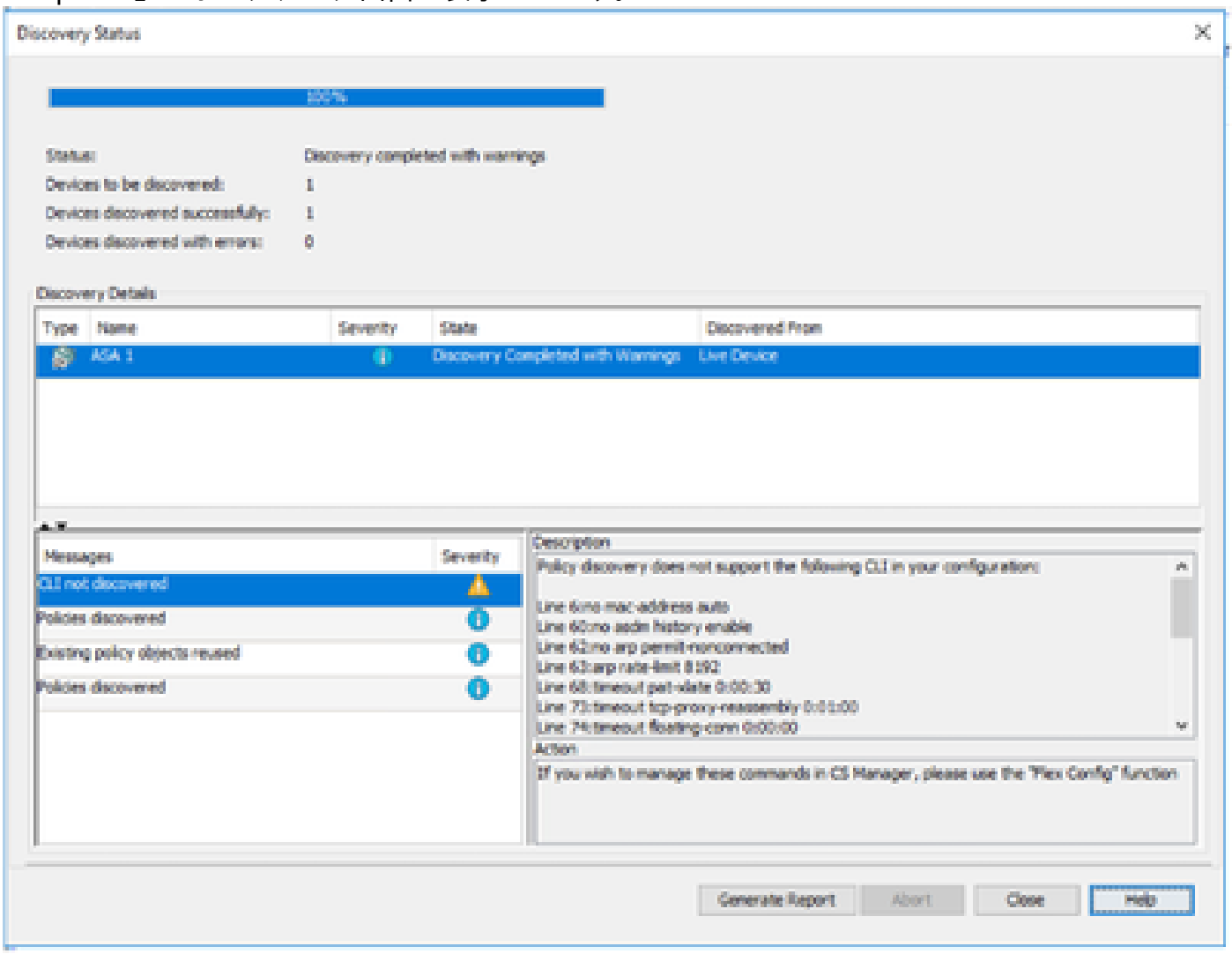
- ライブデバイス：ネットワーク内にあるライブデバイス(LTE)から設定を取得します。
- コンフィギュレーションファイル：コンフィギュレーションファイルを選択して、ディスカバリを続行できます。
- 工場出荷時のデフォルト設定：デバイスをデフォルト設定にリセットします。この方法は、シングルコンテキストモードのみを実行するデバイス、または個々のセキュリティコンテキストを使用するデバイスに使用できます。



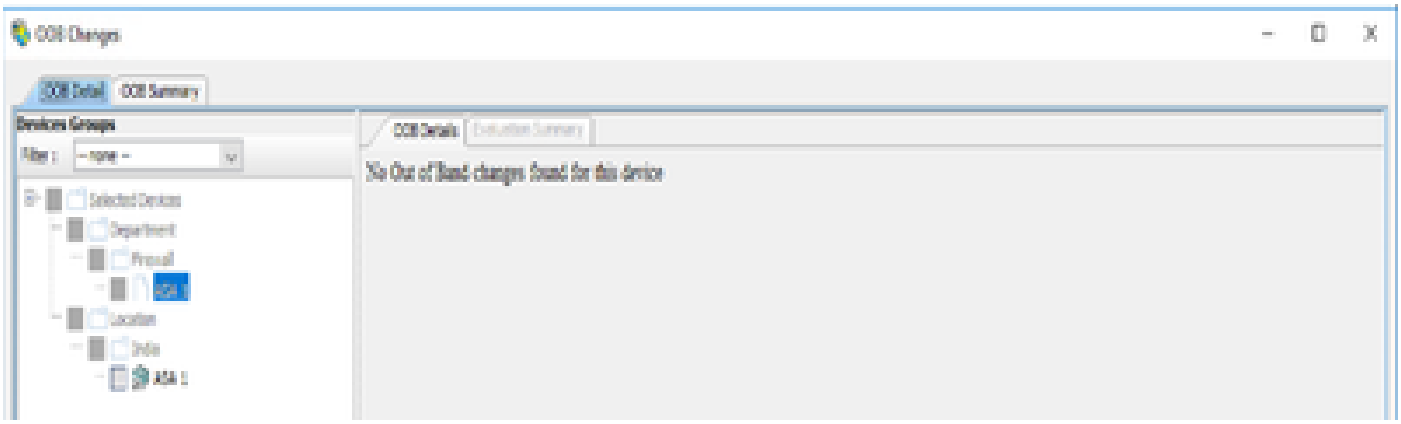
検出を開始する前に、ネットワークトポロジと、ネットワークで発生する可能性のある変更を確認してください。



ディスカバリが完了すると（ディスカバリが正常に終了した後）、ステータスが「Discovery completed」のポップアップ画面が表示されます。



また、アウトオブバンドの変更も変更できません。



デバイスの一括検出

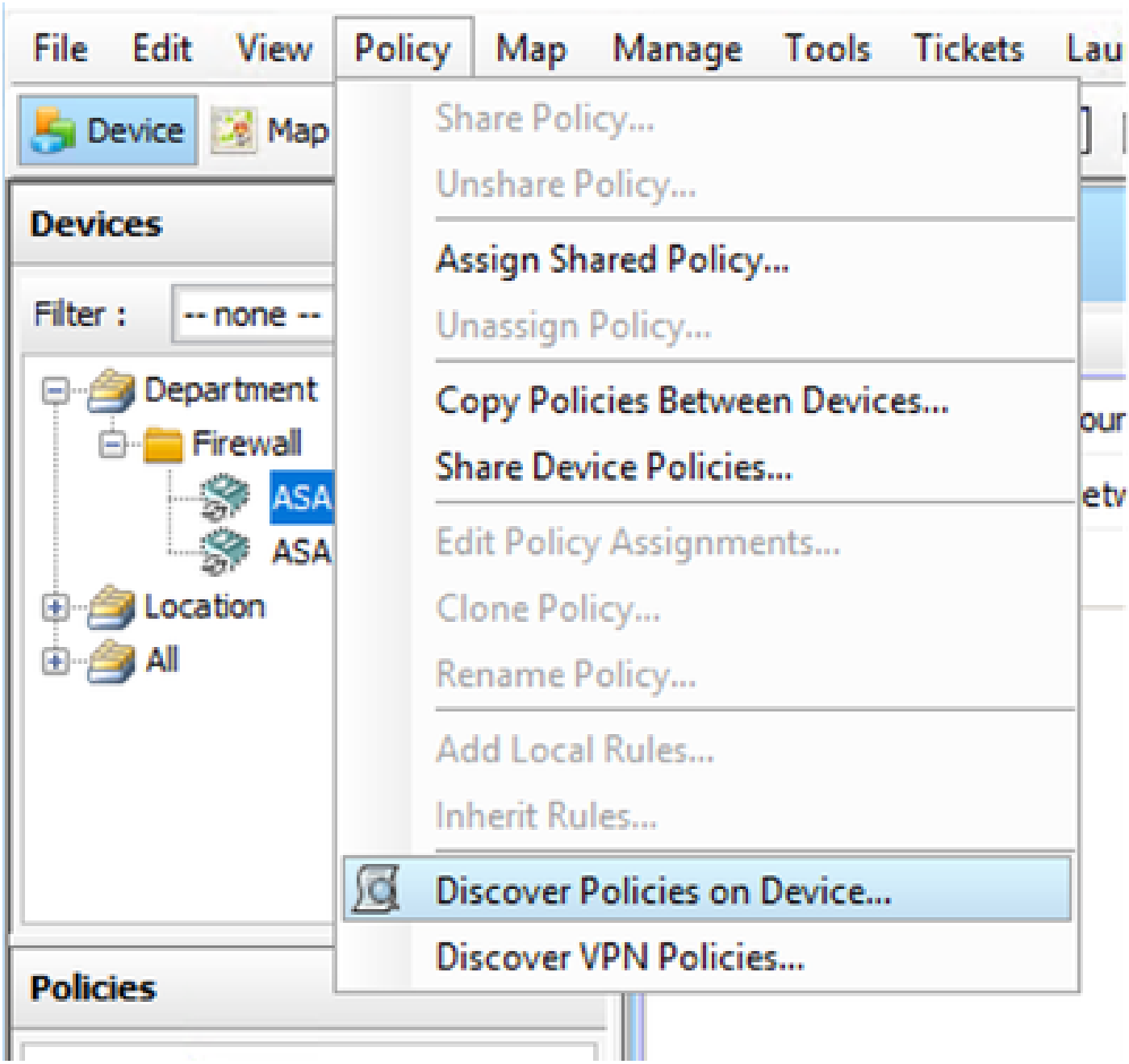
複数のデバイスのポリシーを検出するには、一括再検出を実行します。バルク再検出は、ネットワーク内で現在動作し、アクセス可能な実稼働中のデバイス（たとえば、ネットワーク内のリンクなど）に制限されることに注意してください。

セキュリティコンテキストの仮想センサーでは一括検出を実行できません。サービスモジュールは、個別に選択して検出できます。

デバイスの一括検出を実行する手順：

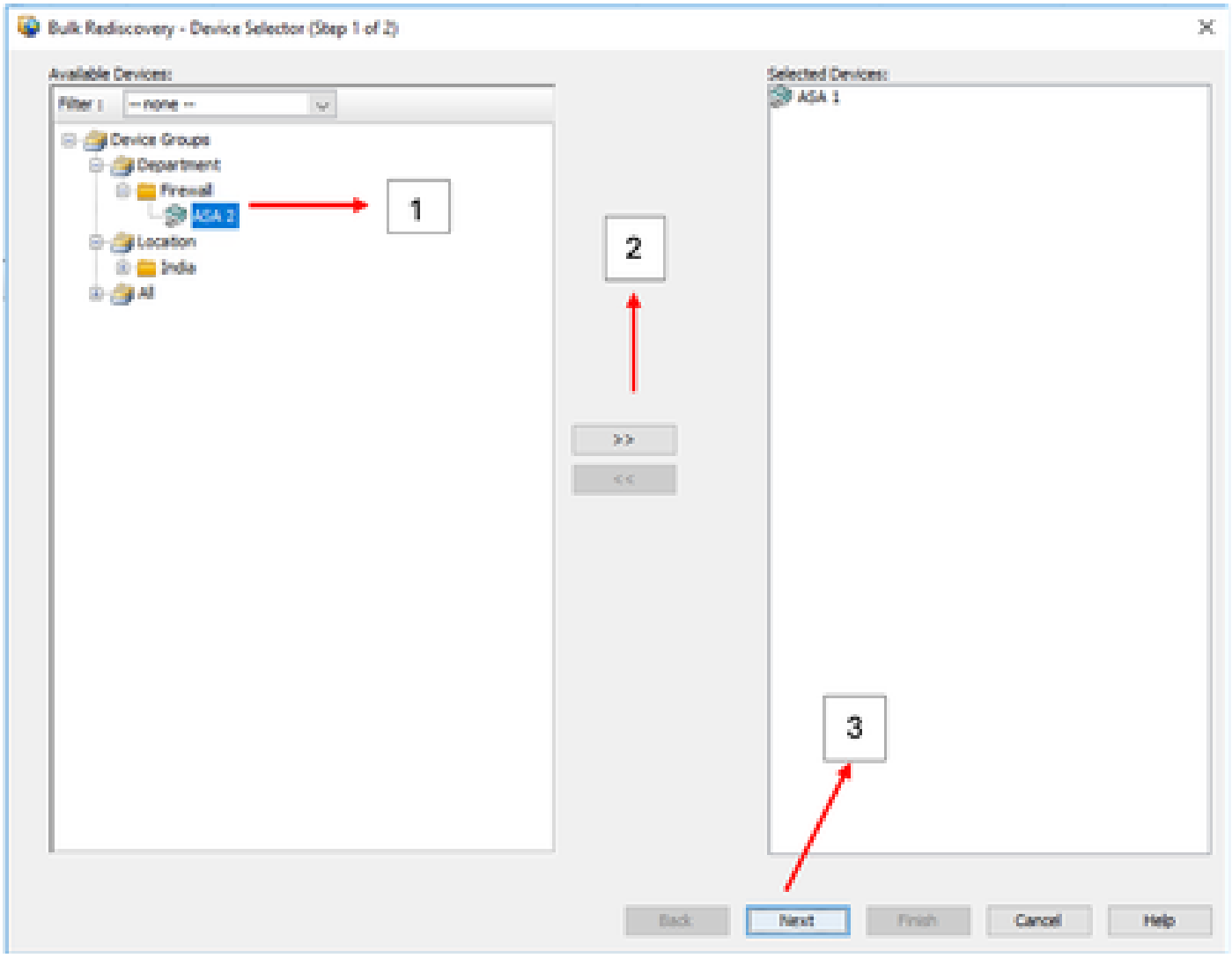
ステップ 1：

デバイスでPolicy > Discover Policiesの順に移動します



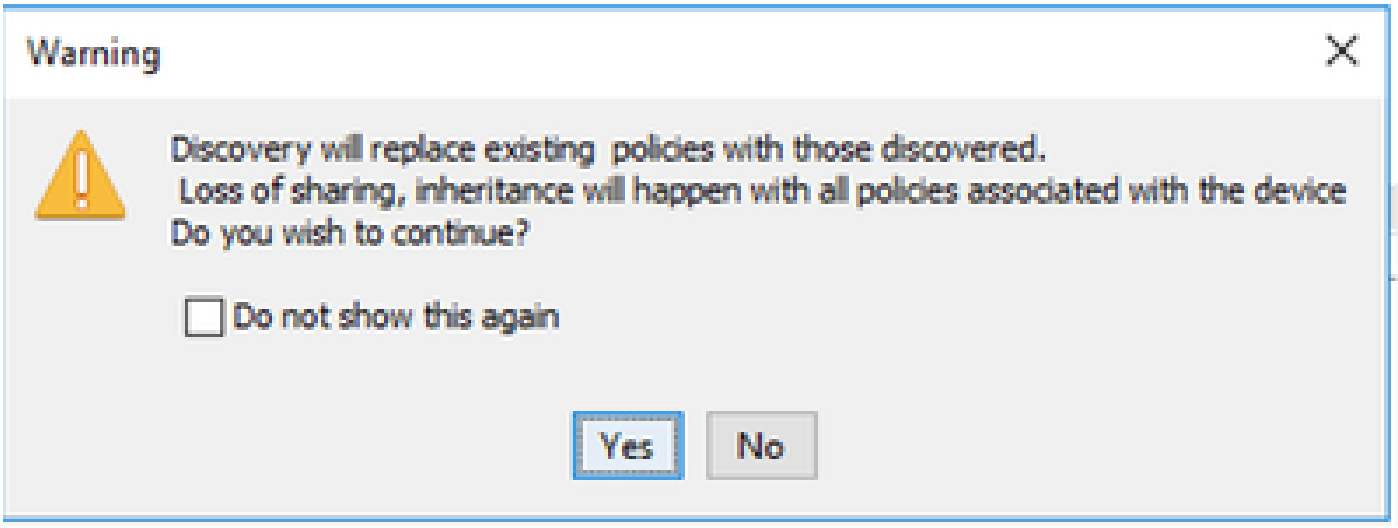
ステップ 2：

バルク再検出を実行している場合（たとえば、バルク再検出を実行している場合）、バルク再検出のダイアログボックスだけが表示されます。
左側のペインの使用可能なデバイスから、ポリシーを検出するデバイスのリストを選択し、右側に移動します。

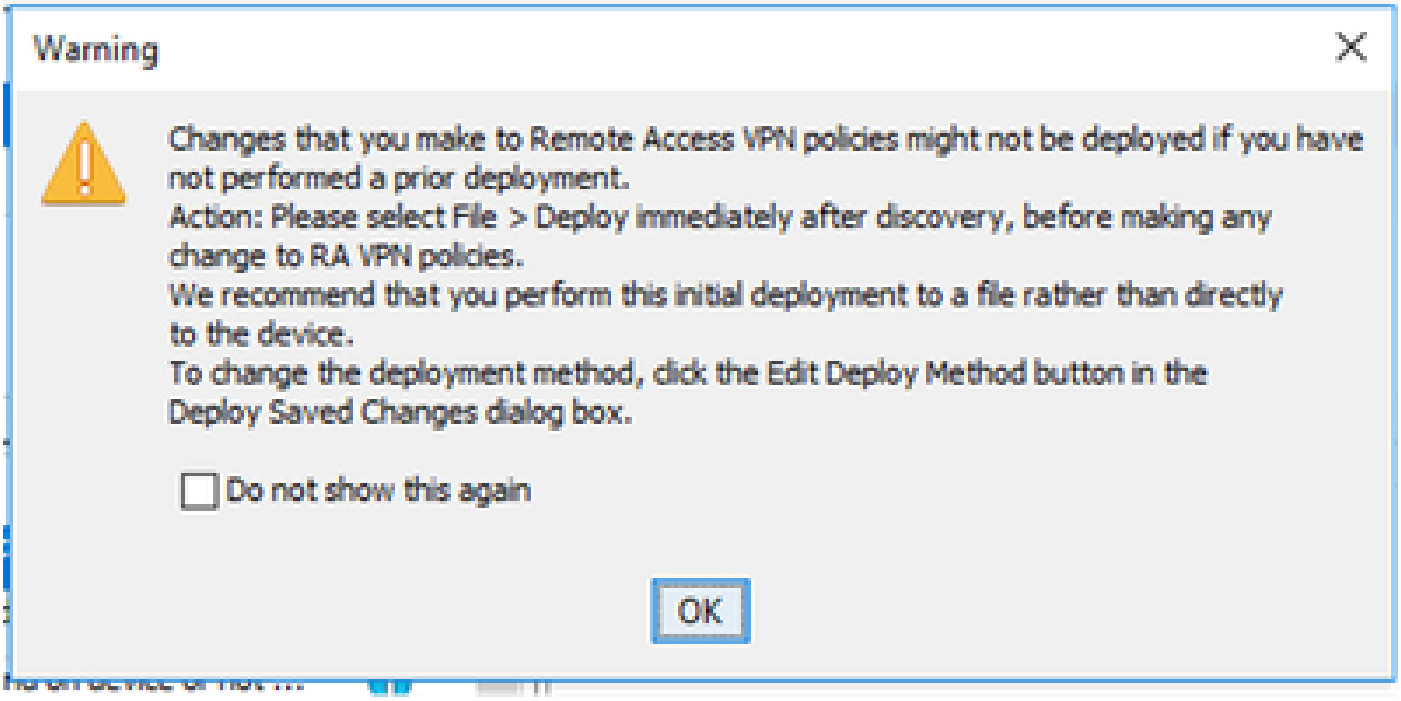


ステップ 3：

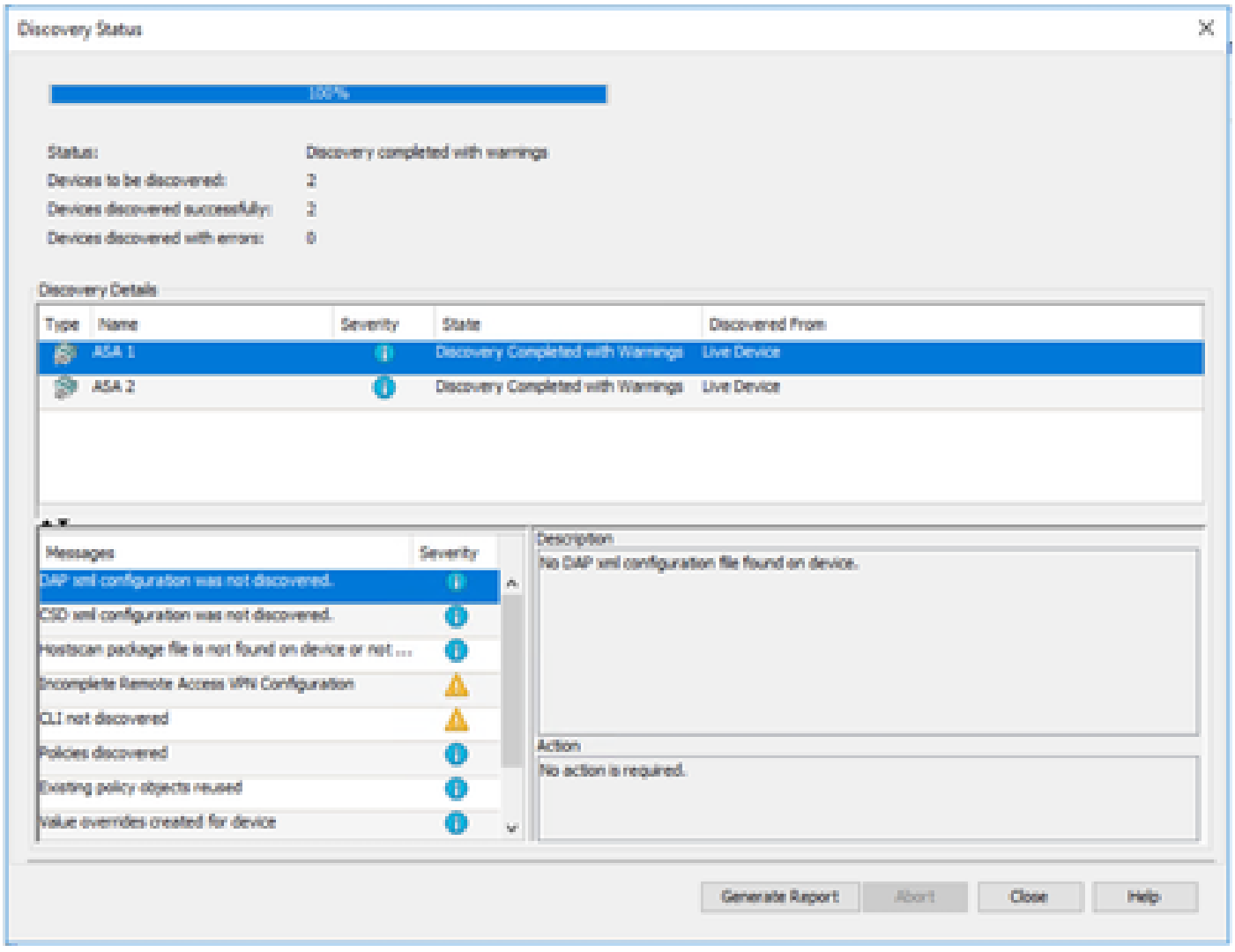
選択したすべてのデバイスがリストされていることを確認し、Finishをクリックして一括再検出を続行します。
検出を開始する前に、ネットワークトポロジと、ネットワークで発生する可能性のある変更を確認してください。



ディスカバリが完了すると、次のような例が表示されます



両方のデバイスが正常に検出されます。



翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。