CSM 3.x： Security Manager インベントリに IDS Sensor とモジュールを追加する

目次

概要

このドキュメントでは、Cisco Security Manager（CSM）に侵入検知システム（IDS）のセンサーとモジュール（Catalyst 6500 スイッチの IDSM、ルータの NM-CIDS、および ASA の AIP-SSM を含む）追加する方法について説明します。

注: IPS 6.2 は CSM 3.2 ではサポートされていませんが、 CSM 3.3 ではサポートされています。

前提条件

要件

このドキュメントでは、CSM デバイスと IDS デバイスが設置され、正しく機能することを前提としています。

使用するコンポーネント

このドキュメントの情報は、CSM 3.0.1 に基づいています。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Security Manager インベントリへのデバイスの追加

デバイスを Security Manager に追加するときには、DNS 名や IP アドレスなど、デバイスの一連の識別情報を指定します。 追加したデバイスは、Security Manager デバイス インベントリに表示されます。 インベントリに追加した後は、Security Manager でデバイスを管理できます。

デバイスを Security Manager インベントリに追加する方法を以下に挙げます。

- ネットワークからデバイスを追加する。
- ネットワーク上にまだ存在していない新しいデバイスを追加する。
- Device and Credentials Repository（DCR）から 1 つ以上のデバイスを追加する。
- 設定ファイルから 1 つ以上のデバイスを追加する。

注: このドキュメントでは、次の方法について説明します。 ネットワーク上にまだ存在していない新しいデバイスを追加する。

IDS センサーとモジュールを追加するための手順

1 つのデバイスを Security Manager インベントリに追加するには、[Add New Device] オプションを使用します。 このオプションは、事前プロビジョニングに使用できます。 デバイスのハードウェアを受け取る前に、システムでデバイスを作成し、ポリシーをデバイスに割り当て、設定ファイルを生成できます。

デバイスのハードウェアを受け取ったら、Security Manager で管理するデバイスを準備する必要があります。 詳細については、Security Manager で管理するデバイスの準備を参照してください。

この手順では、新しい IDS センサーとモジュールを追加する方法について説明します。

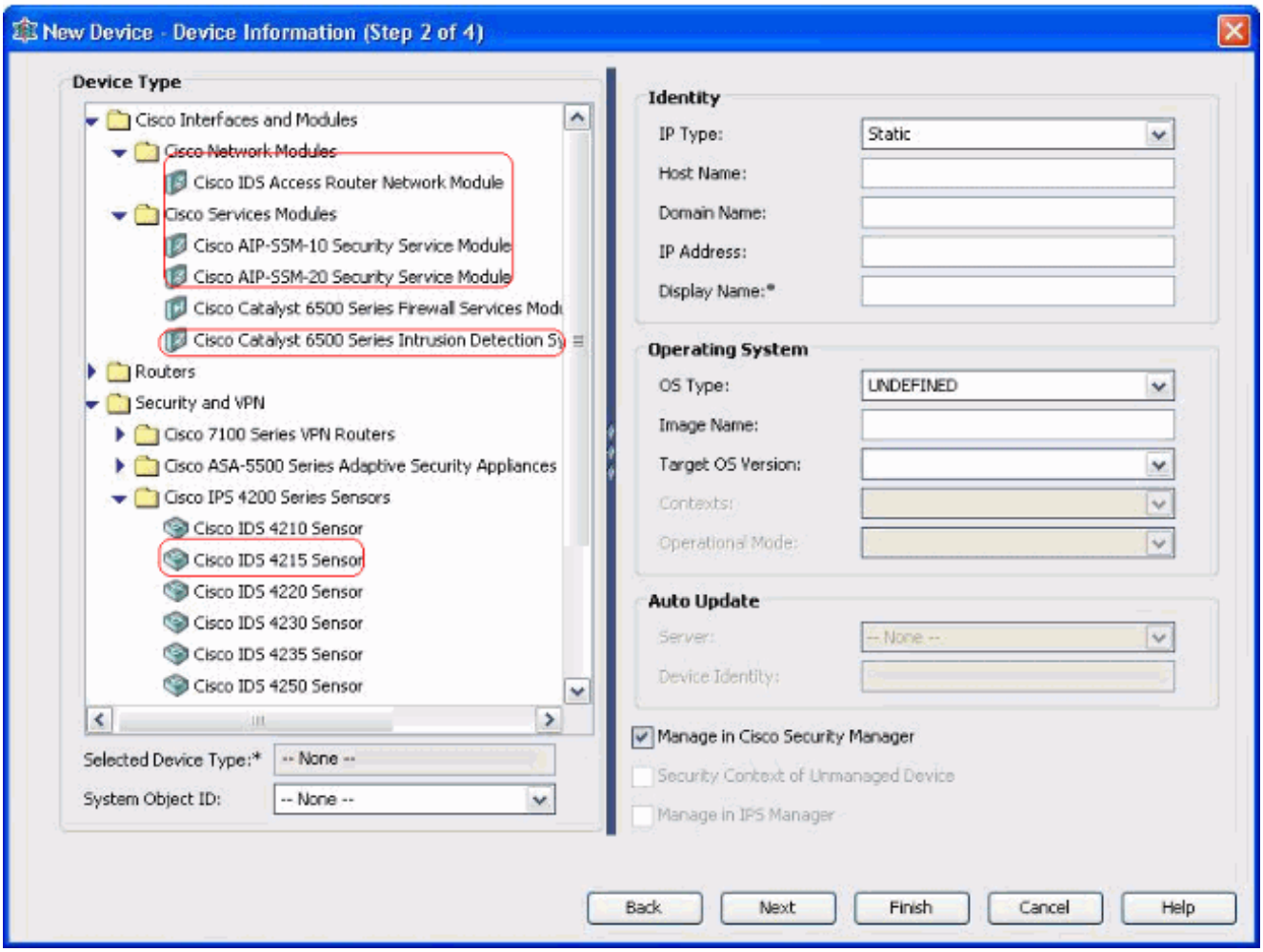
1. ツールバーの [Device View] ボタンをクリックします。[Devices] ページが表示されます。
2. デバイス セレクタで [Add] をクリックします。[New Device - Choose Method] ページが開き、4 つのオプションが表示されます。
3. [Add New Device] を選択し、[Next] をクリックします。[New Device - Device Information] ページが表示されます。
4. 該当するフィールドにデバイス情報を入力します。詳細については、「デバイス情報の指定：新しいデバイス」セクションを参照してください。
5. **[Finish] をクリックします。**システムが、次のようなデバイスの検証タスクを実行します。データが正しくない場合は、システムがエラー メッセージを生成し、エラーが発生したページが表示され、対応する場所に赤のエラー アイコンが表示されます。データが正しい場合は、デバイスがインベントリに追加され、デバイス セレクタに表示されます。

デバイス情報の指定：新しいデバイス

次の手順を実行します。

1. 新しいデバイスのデバイス タイプを選択します。サポートされているデバイス ファミリを表示するには、最上位のデバイス タイプのフォルダを選択します。サポートされているデバイス タイプを表示するには、デバイス ファミリのフォルダを選択します。[Cisco

Interfaces and Modules] > [Cisco Network Modules] を選択して、[Cisco IDS Access Router Network Module] を追加します。 同様に、[Cisco Interfaces and Modules] > [Cisco Services Modules] を選択して、AIP-SSM モジュールと IDSM モジュールを追加します (図を参照) 。[Security and VPN]> [Cisco IPS 4200 Series Sensors] を選択して、[Cisco IDS 4210 Sensor] を CSM インベントリに追加します。



デバイス タイプを選択します。**注:** デバイスを追加した後で、デバイス タイプを変更することはできません。[SysObjectId] フィールドに、そのデバイス タイプのシステム オブジェクト ID が表示されます。 最初のシステム オブジェクト ID がデフォルトで選択されています。 必要に応じて、別の ID を選択できます。

2. [IP Type] ([Static] または [Dynamic]) 、[Host Name]、[Domain Name]、[IP Address]、[Display Name] など、デバイス識別情報を入力します。
3. [OS Type]、[Image Name]、[Target OS Version]、[Contexts]、[Operational Mode] など、デバイスのオペレーティング システムに関する情報を入力します。
4. 選択したデバイス タイプに応じて、[Auto Update] または [CNS-Configuration Engine] フィールドが表示されます。[Auto Update]：PIX Firewall および ASA デバイスの場合に表示されます。[CNS-Configuration Engine]：Cisco IOS® ルータの場合に表示されます。**注** : Catalyst 6500/7600 および FWSM デバイスの場合、このフィールドはアクティブになりません。
5. 次の手順を実行します。[Auto Update]：矢印をクリックすると、サーバのリストが表示されます。 デバイスを管理するサーバを選択します。 サーバがリストに表示されない場合は、次の手順を実行します。矢印をクリックし、[+ Add Server...] を選択します。 [Server Properties] ダイアログボックスが表示されます。必須フィールドに情報を入力します。[OK] をクリックします。 新しいサーバが、選択可能なサーバのリストに追加されます。[CNS-Configuration Engine]：[IP Type] として [Static] と [Dynammic] のどちらを選択したかによ

って、異なる情報が表示されます。**[Static]**：矢印をクリックすると、構成エンジンのリストが表示されます。 デバイスを管理する構成エンジンを選択します。 リストに構成エンジンが表示されない場合は、次の手順を実行します。矢印をクリックし、[+ Add Configuration Engine...] を選択します。 [Configuration Engine Properties] ダイアログボックスが表示されます。必須フィールドに情報を入力します。[OK] をクリックします。 新しい構成エンジンが、選択可能な構成エンジンのリストに追加されます。**[Dynamic]**：矢印をクリックすると、サーバのリストが表示されます。 デバイスを管理するサーバを選択します。 サーバがリストに表示されない場合は、次の手順を実行します。矢印をクリックし、[+ Add Server...] を選択します。 [Server Properties] ダイアログボックスが表示されます。必須フィールドに情報を入力します。[OK] をクリックします。 新しいサーバが、選択可能なサーバのリストに追加されます。

6. 次の手順を実行します。Security Manager でデバイスを管理するには、[Manage in Cisco Security Manager] チェックボックスをオンにします。 これはデフォルトです。追加しようとしているデバイスの唯一の機能が VPN エンド ポイントとしての機能性である場合は、[Manage in Cisco Security Manager] チェックボックスをオフにします。Security Manager は設定を管理せず、このデバイスの設定をアップロードもダウンロードもしません。
7. 親デバイス（PIX Firewall、ASA、または FWSM）が Security Manager によって管理されていないセキュリティ コンテキストを管理するには、[Security Context of Unmanaged Device] チェックボックスをオンにします。1 つの PIX ファイアウォール、ASA、または FWSM のパーティションを、セキュリティ コンテキストとも呼ばれる複数のセキュリティ ファイアウォールに分けることができます。 各コンテキストは、それぞれに独自の設定およびポリシーを持つ独立したシステムです。 このようなスタンドアロンのコンテキストは、親デバイス（PIX Firewall、ASA、または FWSM）が Security Manager の管理対象外であっても、Security Manager で管理できます。**注:** このフィールドがアクティブになるのは、デバイス セレクタで選択したデバイスが PIX Firewall、ASA、FWSM などのファイアウォール デバイスで、かつそのファイアウォール デバイスがセキュリティ コンテキストをサポートしている場合のみです。
8. IPS Manager で Cisco IOS ルータを管理するには、[Manage in IPS Manager] チェックボックスをオンにします。このフィールドは、デバイス セレクタで Cisco IOS ルータを選択した場合にのみアクティブになります。**注:** IPS Manager は、IPS 機能を備えた Cisco IOS ルータでのみ、IPS 機能を管理できます。 詳細については、IPS の資料を参照してください。[Manage in IPS Manager] チェックボックスをオンにした場合は、[Manage in Cisco Security Manager] チェックボックスもオンにする必要があります。選択したデバイスが IDS である場合、このフィールドはアクティブになりません。 ただし、IPS Manager は IDS センサーを管理するため、チェックボックスはオンになっています。選択したデバイスが PIX Firewall、ASA、または FWSM である場合は、IPS Manager がこれらのデバイス タイプを管理しないため、このフィールドはアクティブになりません。
9. **[Finish] をクリックします。**システムが、次のようなデバイスの検証タスクを実行します。入力したデータが正しくない場合は、システムがエラー メッセージを生成し、エラーが発生したページが表示されます。入力したデータが正しい場合は、デバイスがインベントリに追加され、デバイス セレクタに表示されます。

トラブルシューティング

ここでは、設定に関するトラブルシューティングについて説明します。

エラー メッセージ

CSM に IPS を追加すると、[Invalid device: Could not deduce the SysObjId for the platform type] というエラー メッセージが表示されます。

解決策

このエラー メッセージを解決するには、次の手順を実行してください。

1. Windows で CSM Daemon サービスを停止し、[Program Files] > [CSCOpx] > [MDC] > [athena] > [config] > [Directory] を選択し、VMS-SysObjID.xml を見つけます。
2. CSM システムで、C:\Program Files\CSCOpx\MDC\athena\config\directory にデフォルトである最新の VMSSysObjID.xml オリジナル VMSSysObjID.xml ファイルを置き換えて下さい
3. CSM Daemon Manager サービス（CRMDmgtd）を再起動し、問題が発生していたデバイスの追加または検出を再試行します。

関連情報

- Cisco Security Manager に関するサポート ページ
- シスコ侵入検知システム サポート ページ
- テクニカル サポートとドキュメント – Cisco Systems