

# Cisco IOS IPSでのSecurity Managerの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[関連情報](#)

## 概要

Cisco Security ManagerはCisco Security Management Suiteの一部であり、Cisco Self-Defending Networkの包括的なポリシー管理と適用を提供します。Cisco Security Managerは、セキュリティを管理するための業界をリードするエンタープライズクラスのアプリケーションです。Cisco Security Managerは、シスコルータ、セキュリティアプライアンス、およびセキュリティサービスモジュール全体にわたるファイアウォール、VPN、および侵入防御システム(IPS)セキュリティサービスの構成管理に対応します。

Cisco Security Managerの機能と利点、およびバージョン3.1の新機能の概要については、Cisco Security Manager 3.1データシート

([http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product\\_data\\_sheet0900aecd8062bf6e.html](http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_data_sheet0900aecd8062bf6e.html))を参照してく**ださい**。Cisco Security Manager 3.1は、Cisco.comの<http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app> (登録ユーザ専用) からダウンロードできます。

このドキュメントでは、IOS IPSの初期設定を実行するためにCisco Security Manager(CSM)3.1を使用する方法について説明します。IOS IPSがすでに設定されているルータでは、プロビジョニングタスクにCisco Security Manager 3.1を直接使用できます。

注：Cisco Security Manager 3.1は、IOS IPSを設定するためにIOS 12.4(11)T2以降のIOSイメージのみをサポートします。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 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 3.1
- Cisco IOS 12.4(11)T2

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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

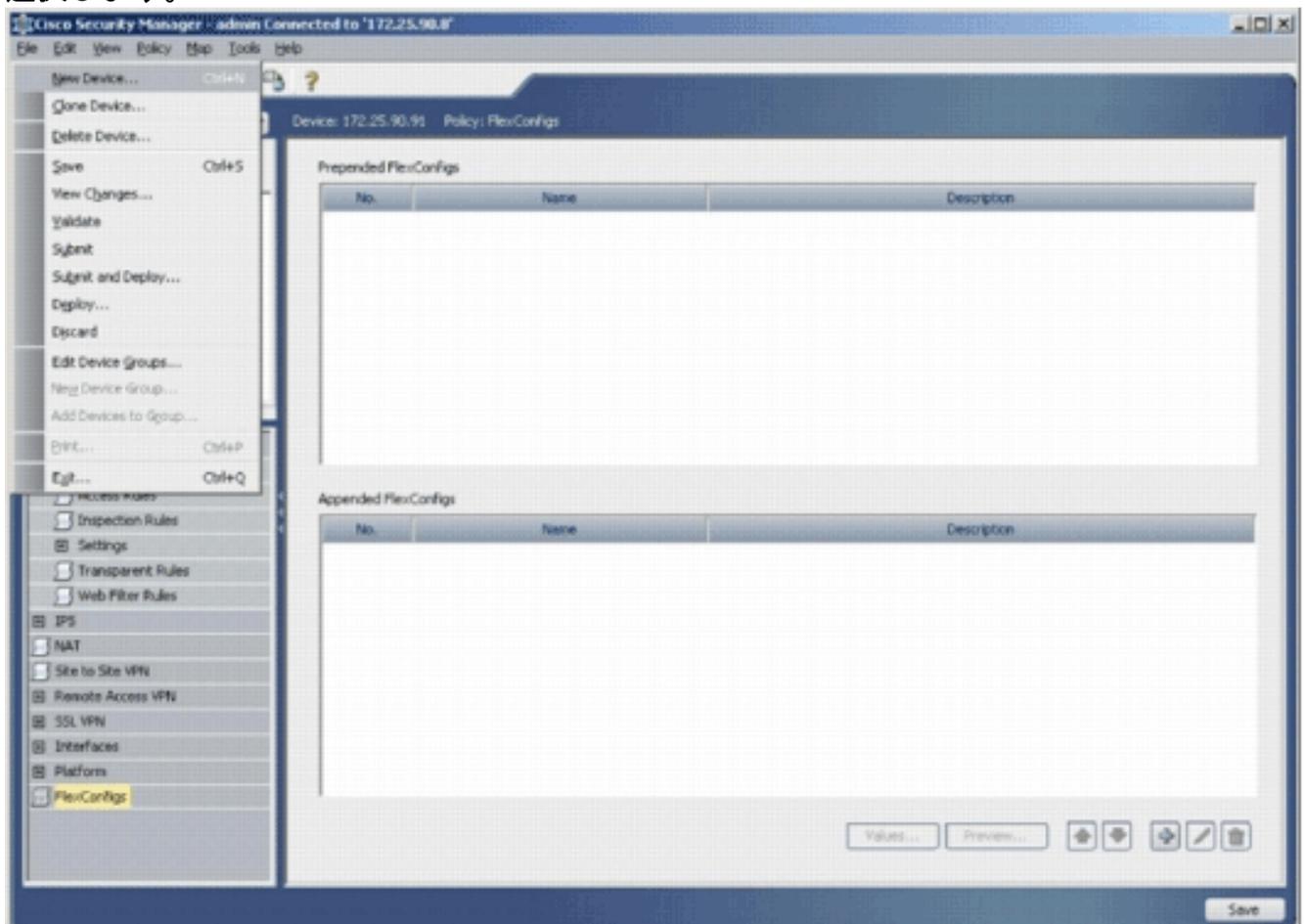
## 表記法

ドキュメント表記の詳細については、『[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。

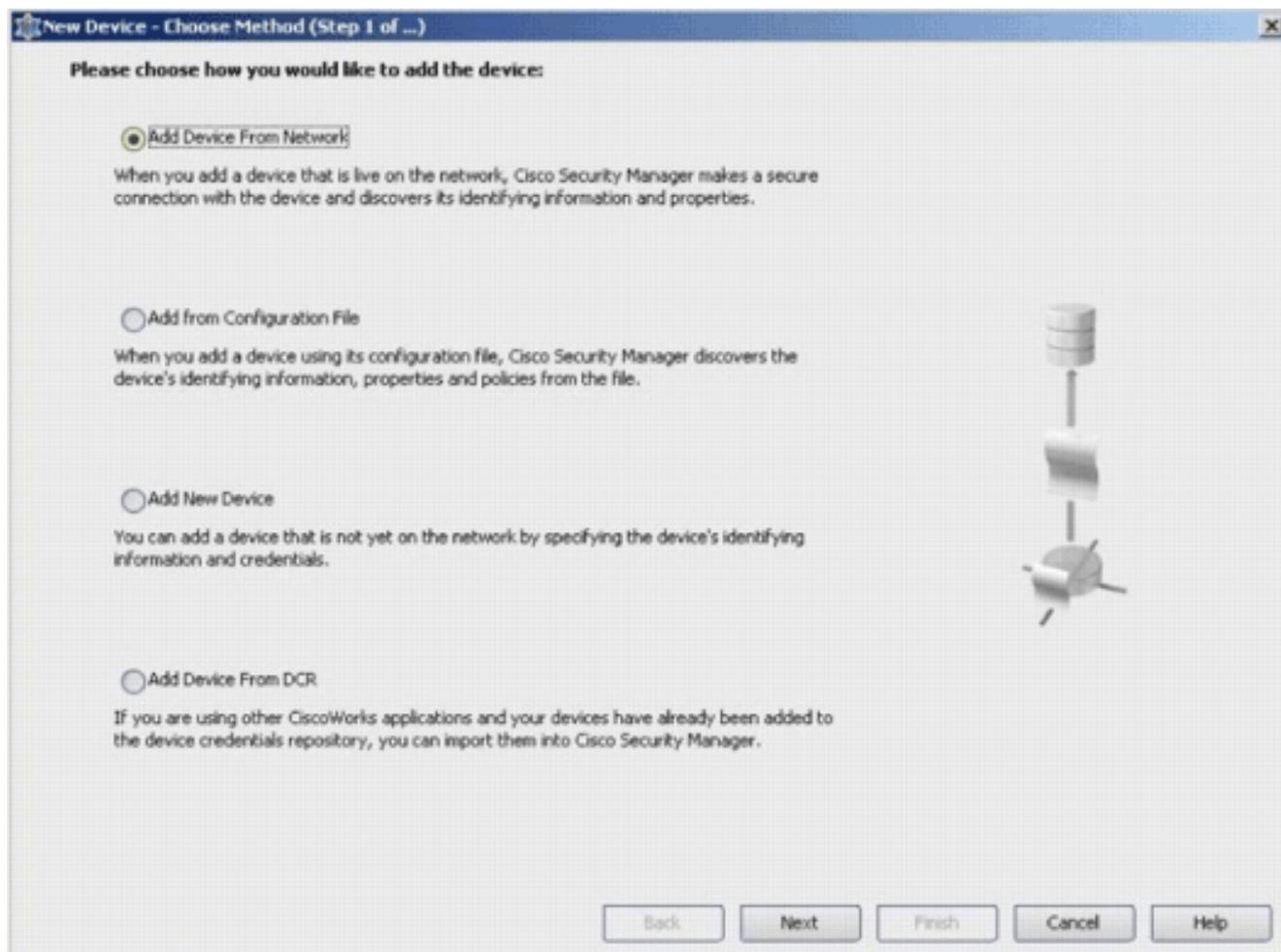
## 設定

IOS IPSを設定するには、次の手順を実行します。

1. ローカルPCからCisco Security Manager 3.1クライアントを実行します。
2. Cisco Security Manager 3.1にデバイスを追加するには、[File]メニューから[New Device]を選択します。



3. [New Device]ウィンドウで、デバイスの追加方法を選択します。この例では、ネットワークからデバイスを追加します。



4. [next] をクリックします。

5. 追加するデバイスのIDの詳細を入力します。たとえば、ホスト名とIPアドレスです。

**New Device - Device Information (Step 2 of 4)**

**Identity**

IP Type: Static

Host Name:

Domain Name:

IP Address: 172.25.90.91

Display Name:\* 172.25.90.91

OS Type:\*

- IOS - 12.3+
- IOS - 12.2, 12.1
- IOS - Catalyst 6500/7600
- PIX
- FW5M
- IPS
- ASA

**Discover Device Settings**

Discover:

- Firewall Policies
- IPS Policies
- RA VPN Policies
- Discover Policies for Security Contexts

Back Next Finish Cancel Help

6. [next] をクリックします。
7. 追加するIOSルータのユーザ名、パスワード、イネーブルパスワードなどのプライマリクレデンシャルを入力します。
8. [Finish]をクリックして、Cisco Security Managerにデバイスを追加します。注：この例では、ユーザがすでに設定済みのルータを持ち、適切なクレデンシャルでルータにログインできることを前提としています。

New Device - Device Credentials (Step 3 of 4)

**Primary Credentials**

Username:

Password:\*  Confirm:\*

Enable Password:  Confirm:

**HTTP Credentials**

Use Primary Credentials

Username:

Password:

Confirm:

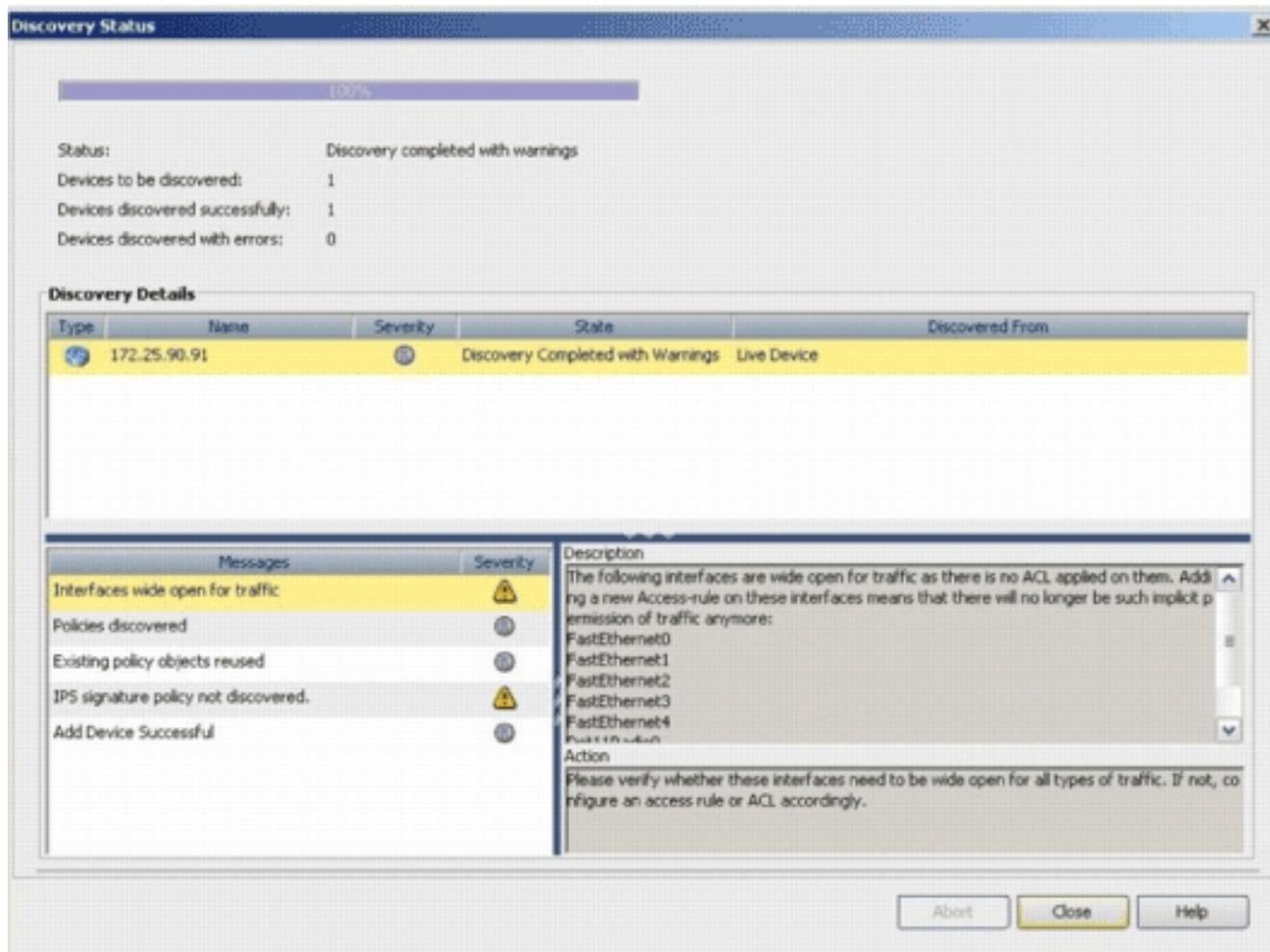
HTTP Port:

HTTPS Port:

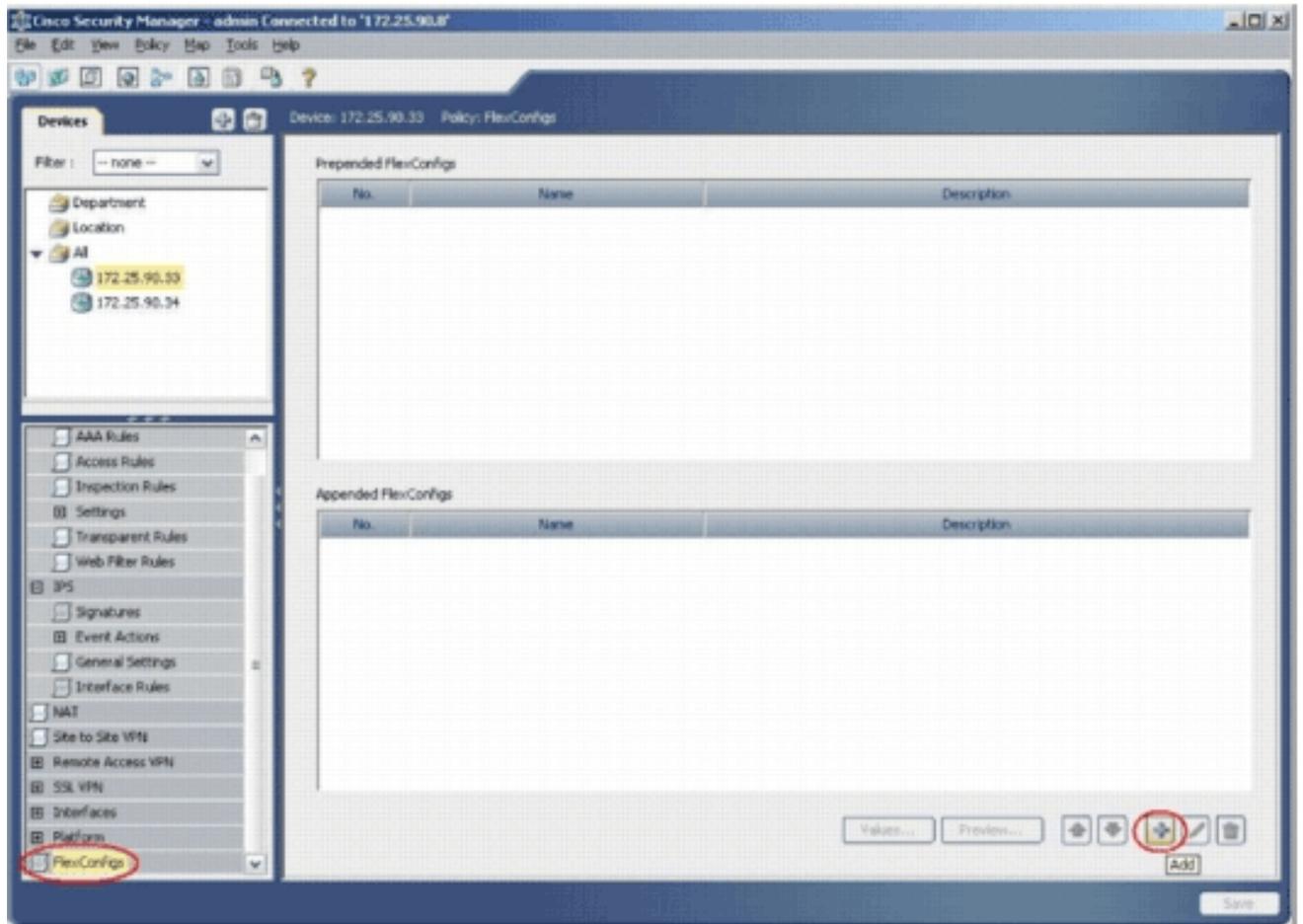
IPS RDEP Mode:

Certificate Common Name:  Confirm:

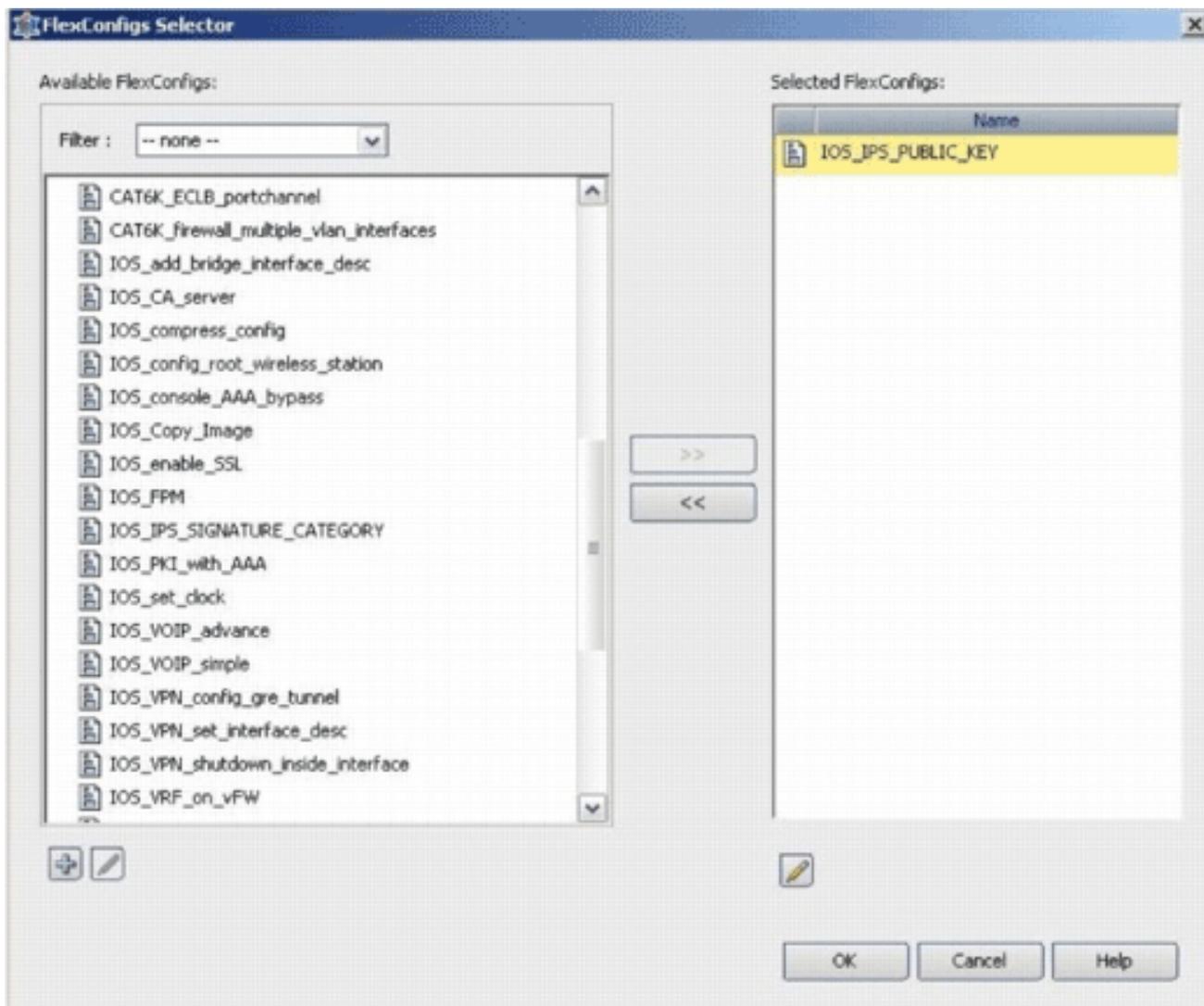
[Discovery Status]ウィンドウに[Discovery completed]と表示されたら、Cisco Security Managerにデバイスを正常に追加しました。Cisco Security Managerにデバイスを正常に追加したら、IPSを有効にするために公開キーを割り当てる必要があります。



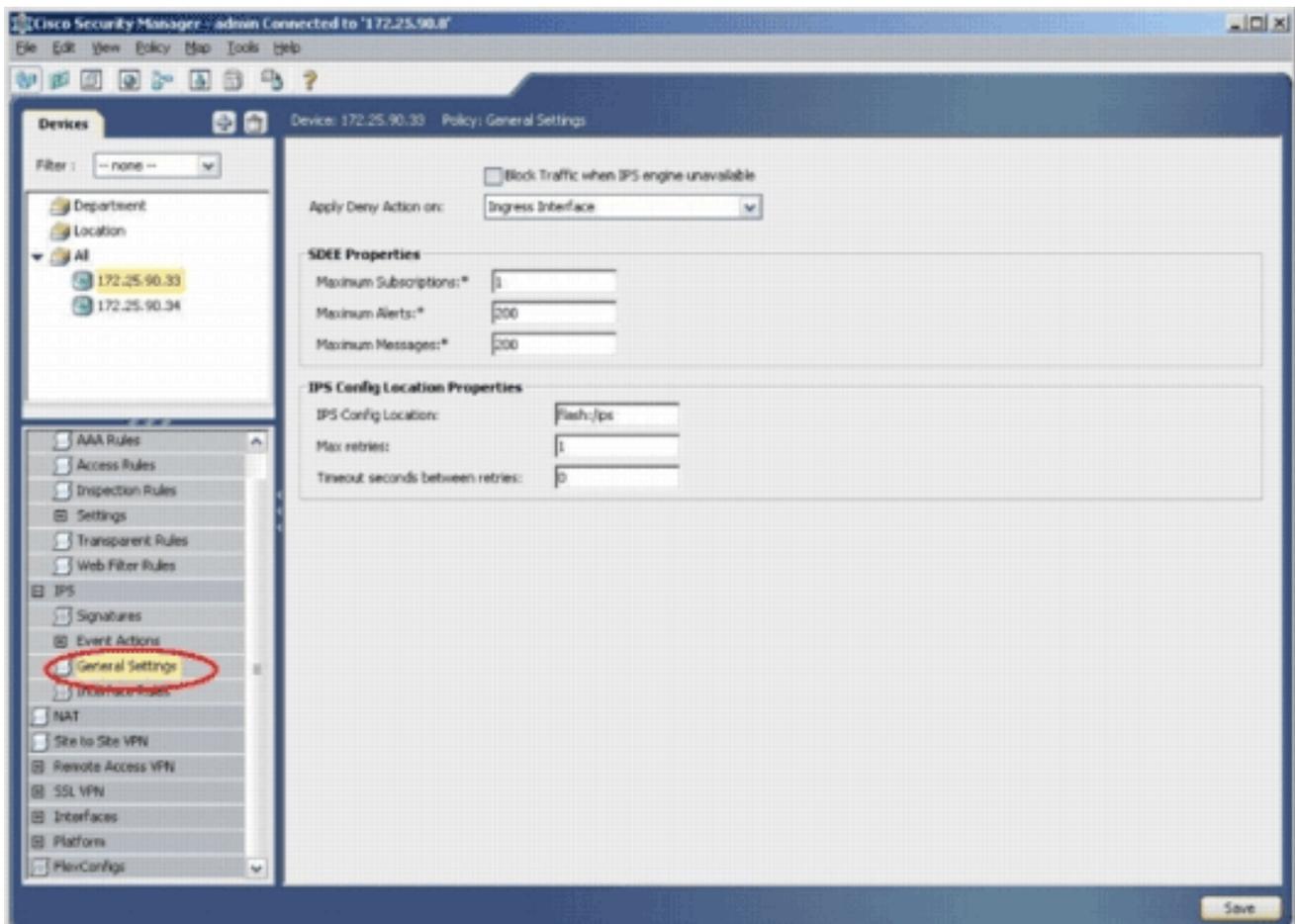
9. 左側のメニューから、[FlexConfigs configuration]画面に移動します。
10. 画面の右側にあるFlexConfigsユーザーインターフェイスをクリックし、[追加]アイコンをクリックします。



11. [Selected FlexConfigs]リストで、[IOS\_IPS\_PUBLIC\_KEY]を選択し、[OK]をクリックします。

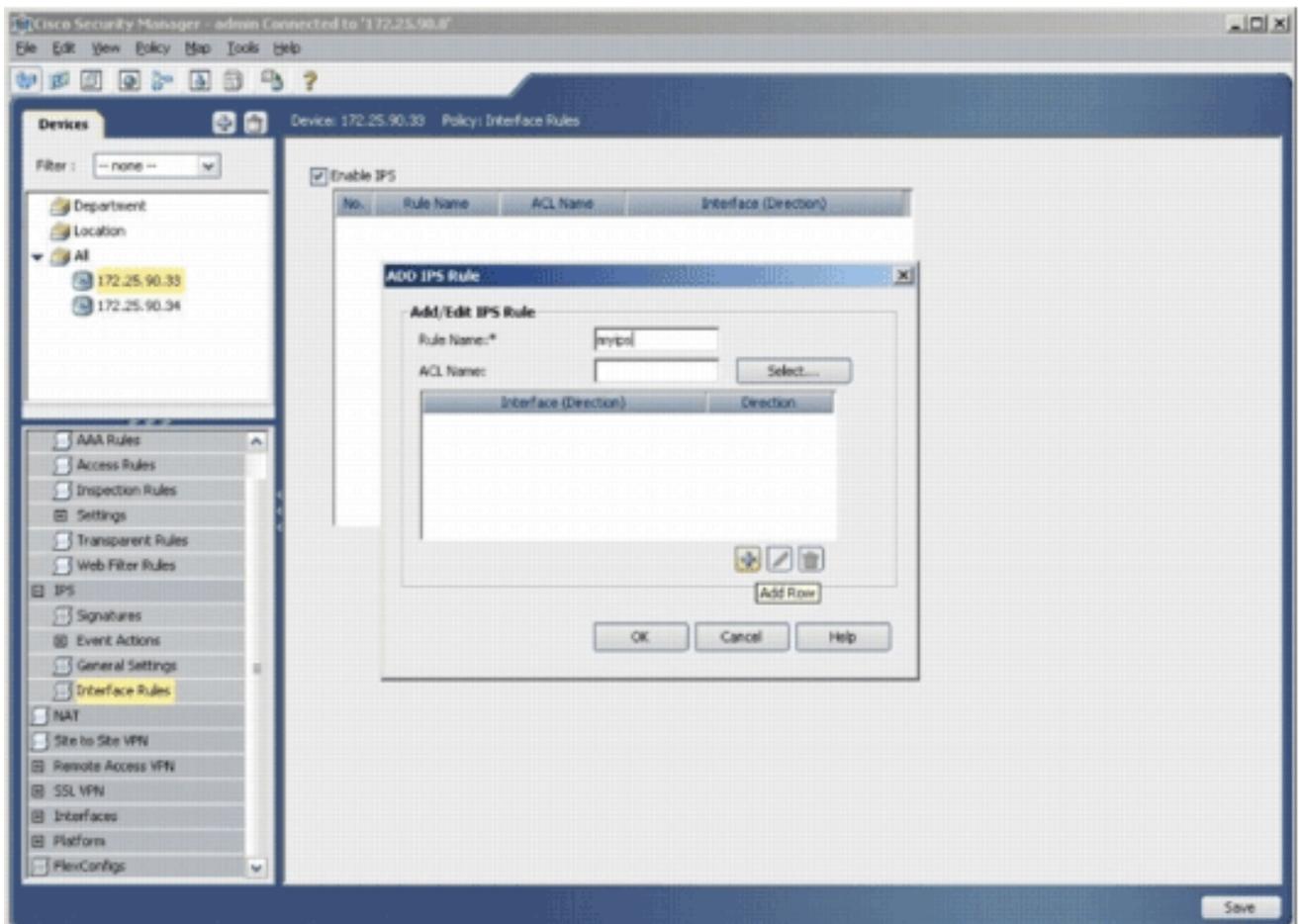


12. [Save] をクリックして変更を保存します。注：IOS\_IPS\_PUBLIC\_KEY FlexConfigは公開キーの設定を保持します。
13. 左側のメニューから、IPSの見出しの下にある**General Settings**を選択します。
14. フラッシュ上のIPS設定の場所を入力します。これは、IPS設定が配置される場所です。
15. [Save] をクリックして変更を保存します。

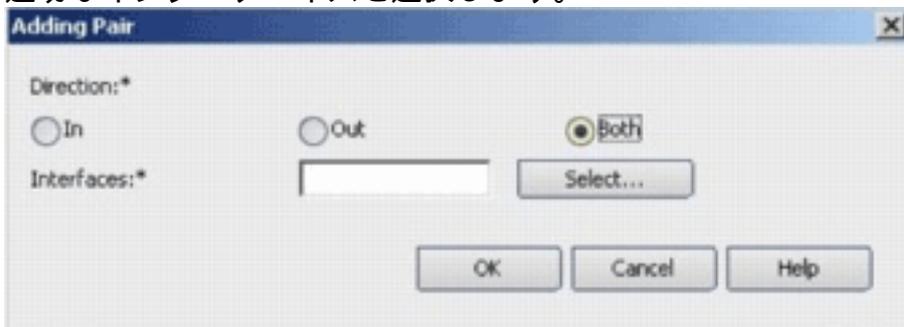


注：ロケーションディレクトリがルータフラッシュにすでに作成されていることを確認します。そうでない場合は、`mkdir <directory_name>`コマンドを使用して、ロケーションディレクトリを作成します。

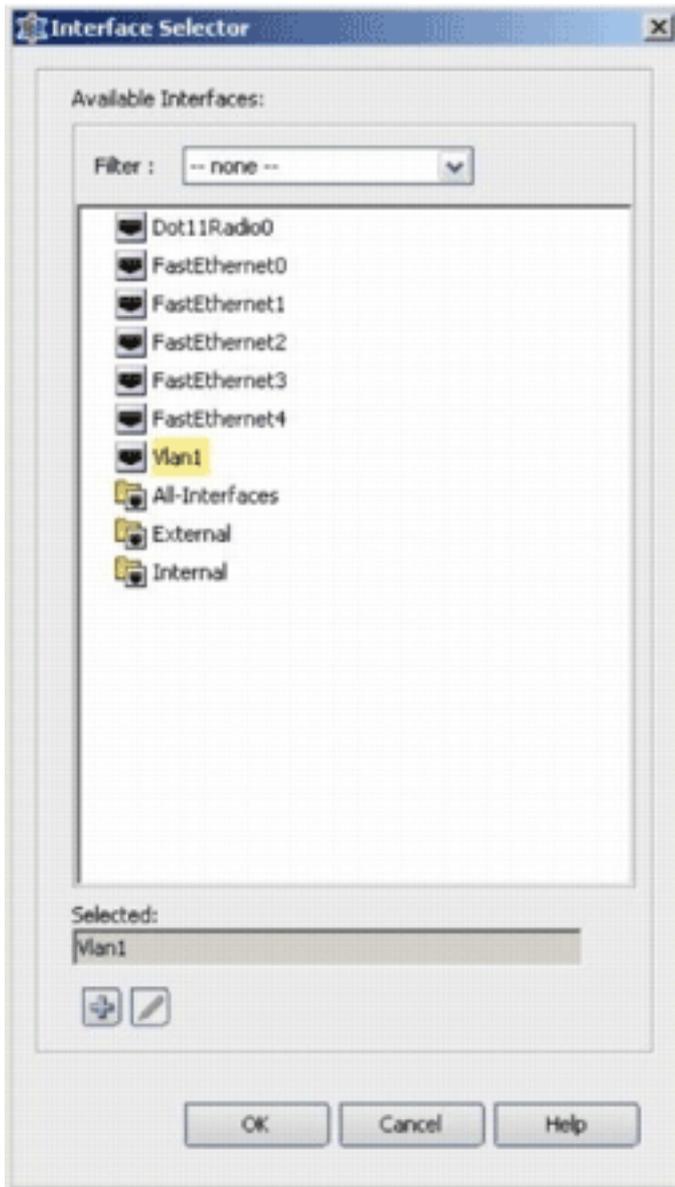
16. IPSを有効にするには、[Interface Rules]に移動し、[Enable IPS]チェックボックスをオンにして、[Add Row]をクリックします。
17. [Add IPS Rule]ダイアログボックスで、[Rule Name]フィールドにIPSルールの名前を入力し、[Add Row]をクリックして、IPSを適用する必要があるインターフェイスを含めます。



18. IPSルールを適用する方向を示すオプションボタンをクリックし、[Select]をクリックして適切なインターフェイスを選択します。

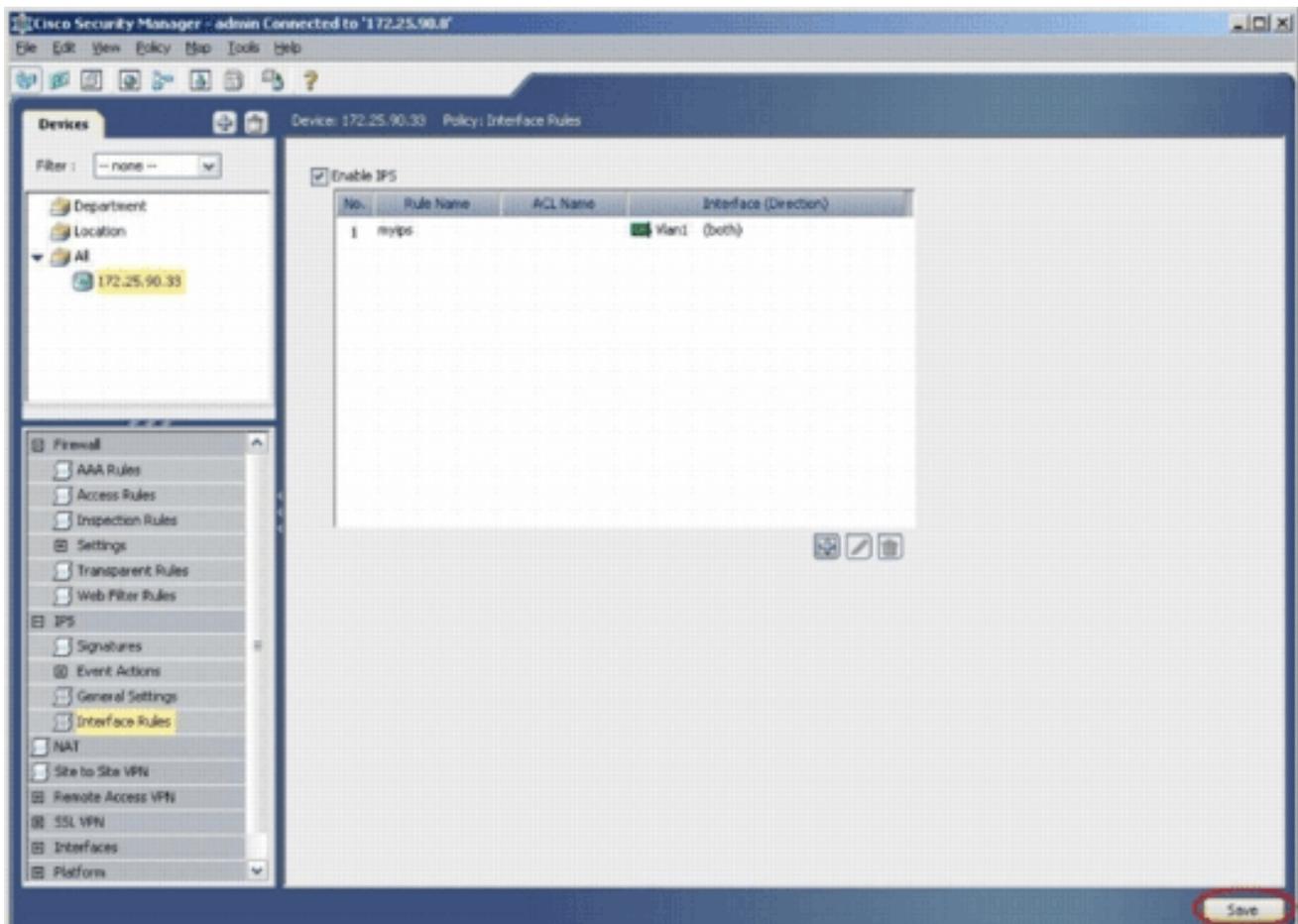


19. 「インターフェイス・セレクト」リストからインターフェイスを選択し、「OK」をクリックし

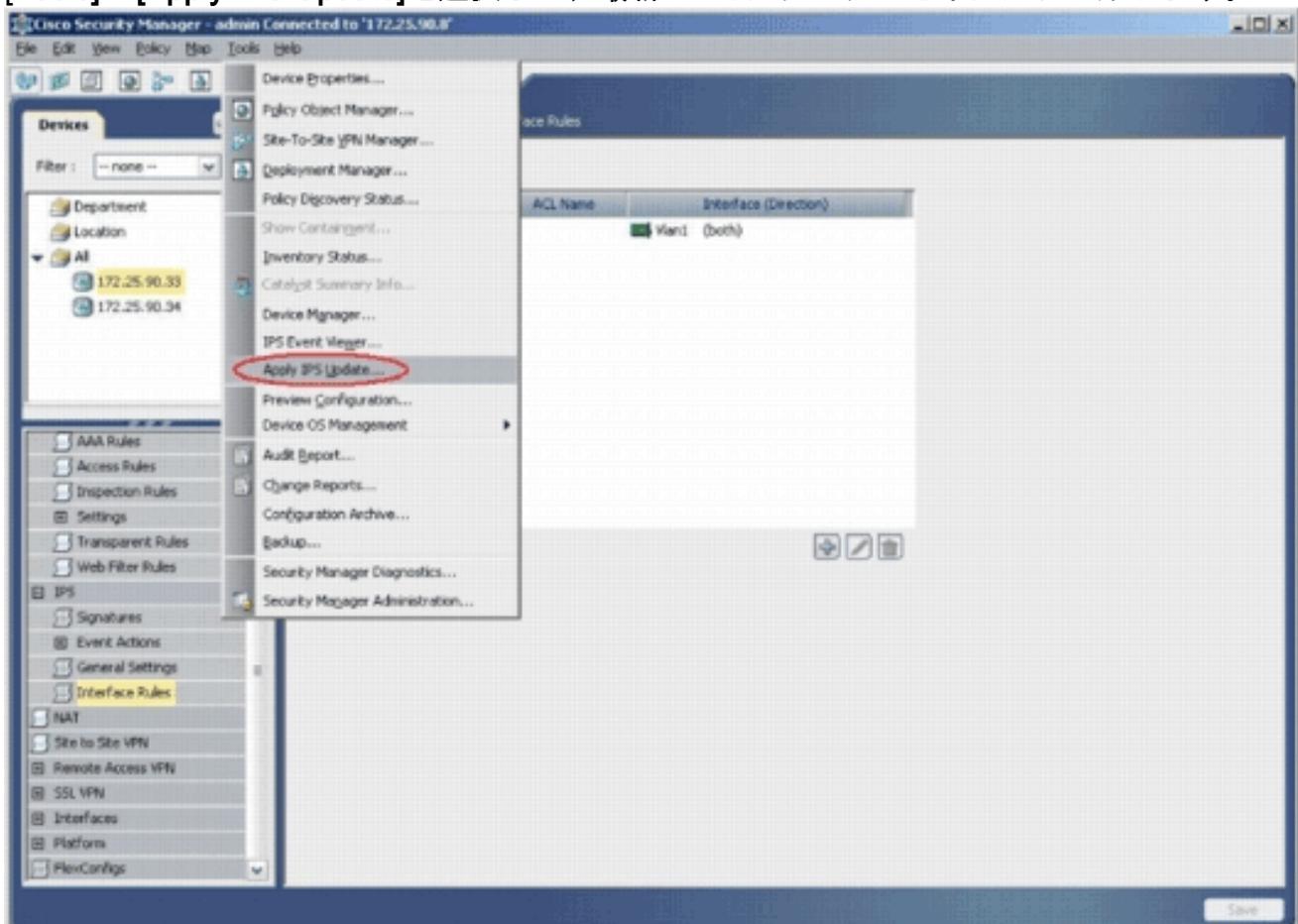


ます。

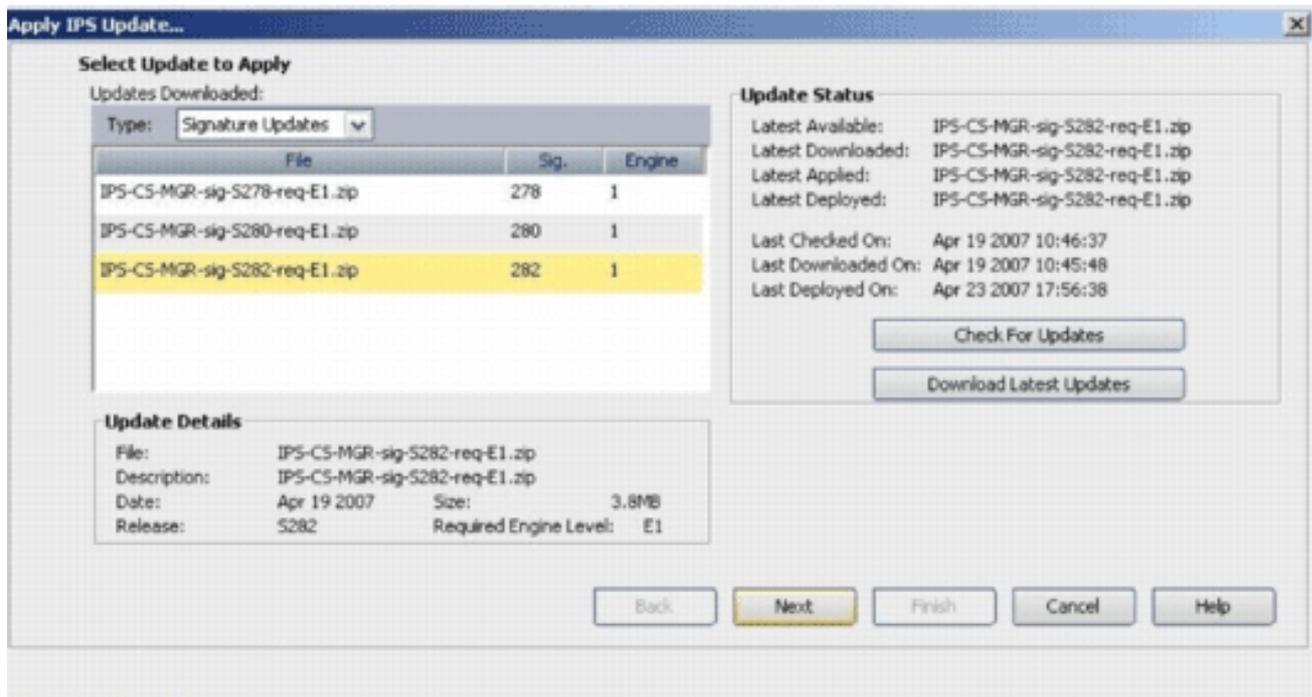
20. [Save] をクリックして変更を保存します。



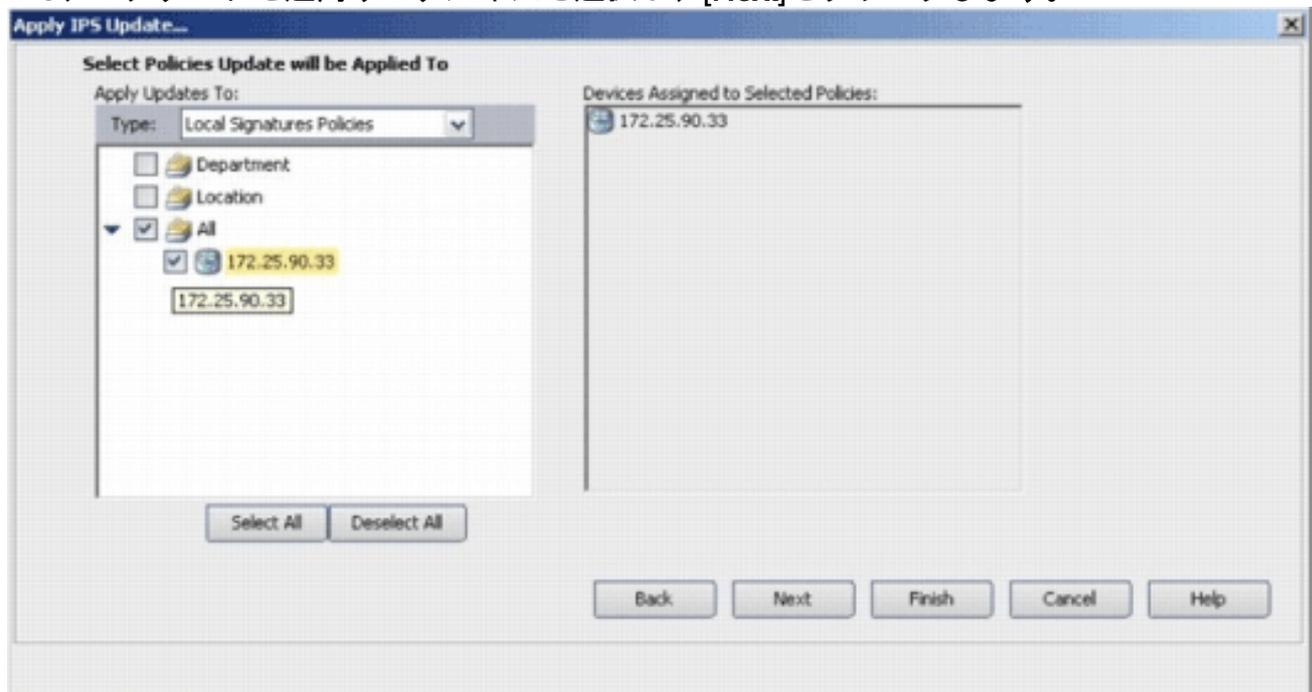
21. [Tools] > [Apply IPS Update]を選択して、最新のIPSシグニチャをインストールします。



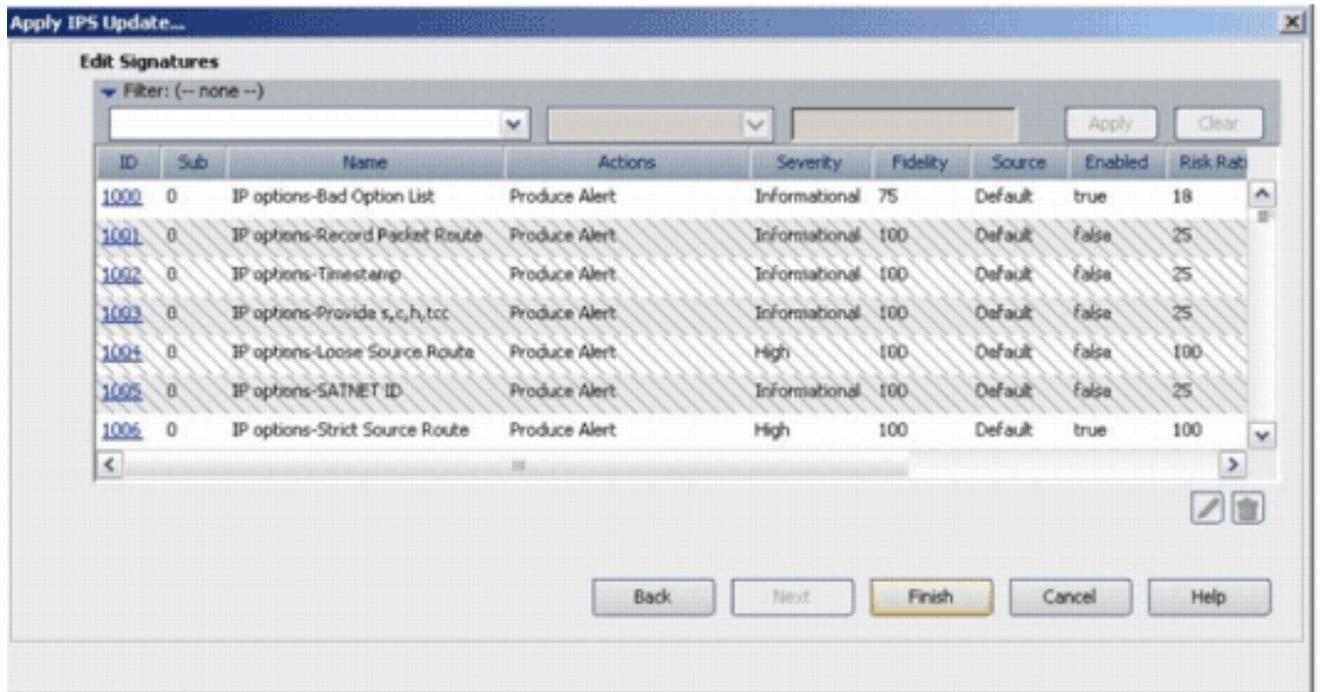
22. 最新の署名ファイルを選択し、[Next]をクリックします。



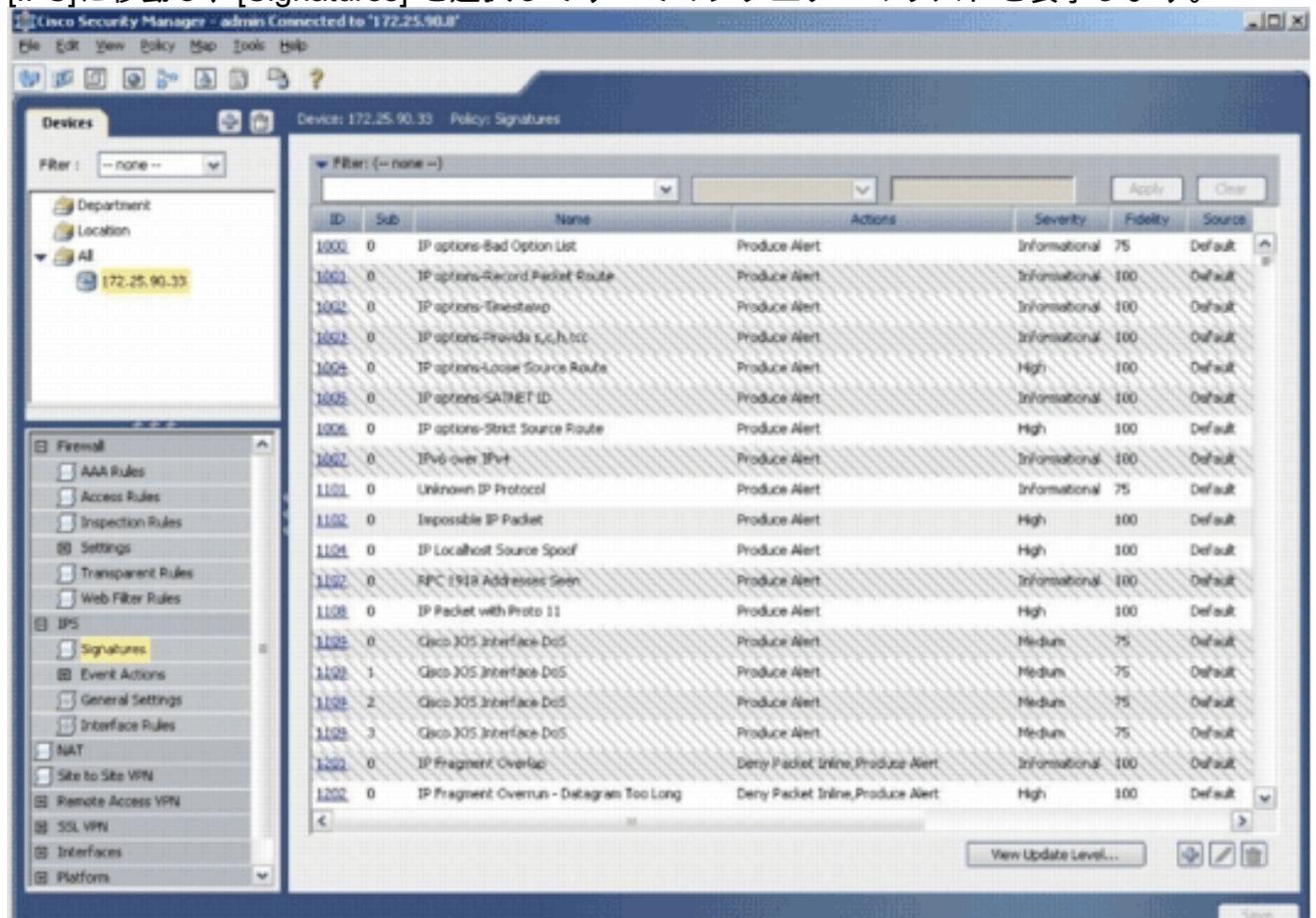
23. IPSアップデートを適用するデバイスを選択し、[Next]をクリックします。



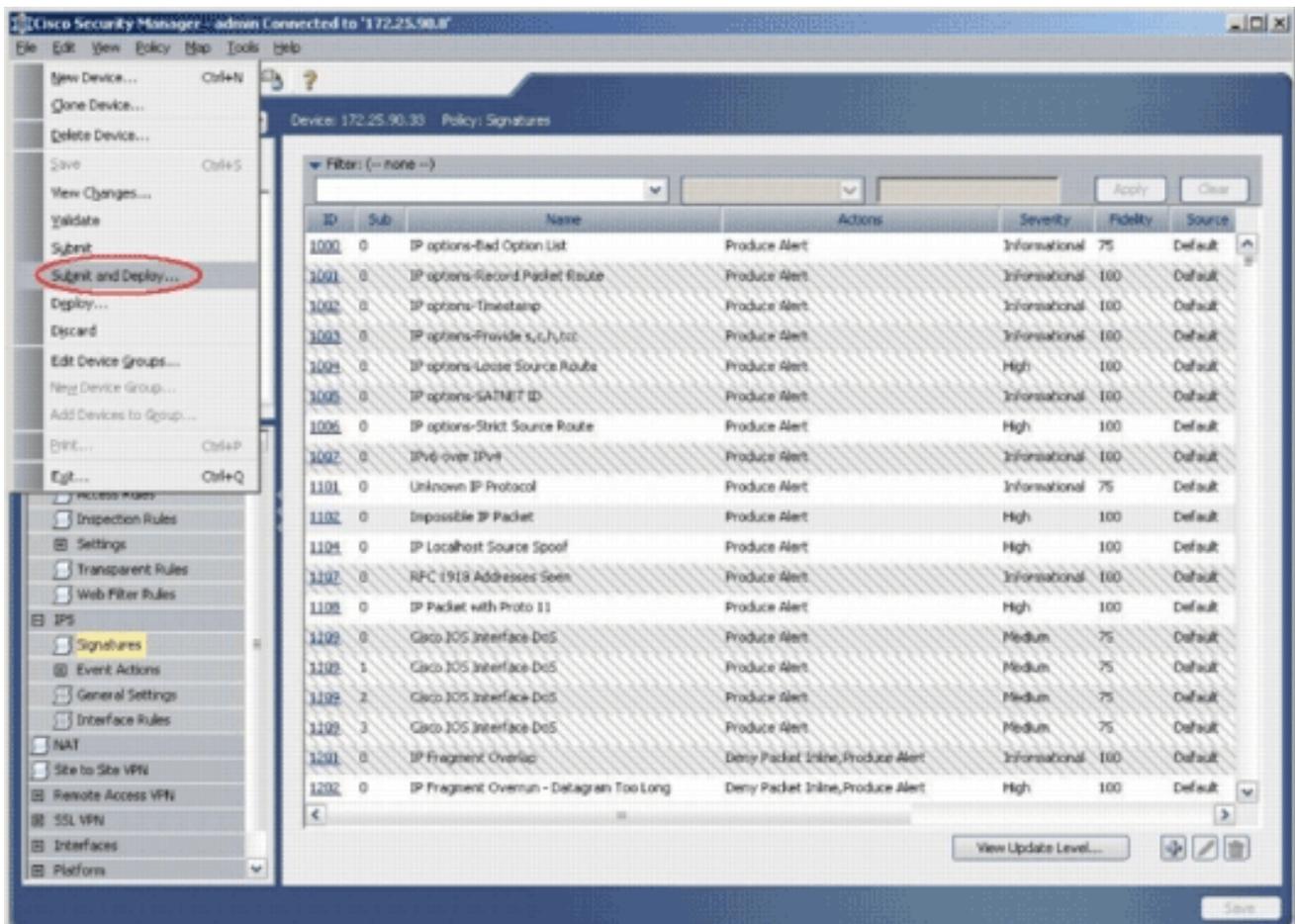
24. [Finish]をクリックして、シグニチャを適用します。



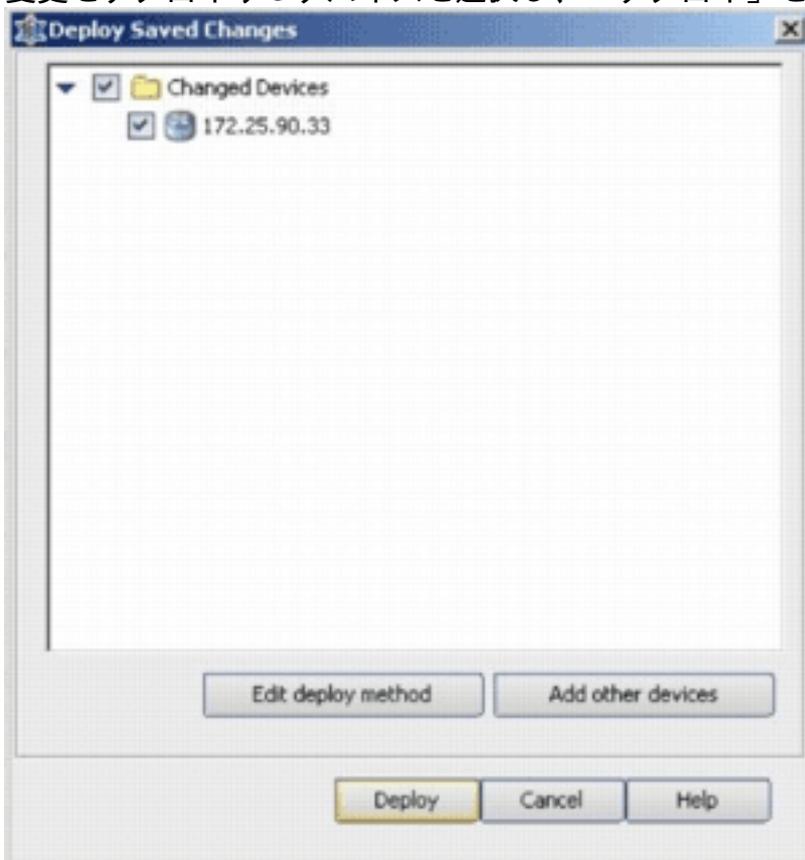
25. [IPS]に移動し、[Signatures] を選択してすべてのシグニチャのリストを表示します。



26. IOSルータにIPSを導入するには、[File] > [Submit and Deploy]の順に選択します。



27. 変更をデプロイするデバイスを選択し、「デプロイ」をクリックします。



28. 展開ステータスを表示して、エラーがあるかどうかを確認します。

Deployment Status Details for deployment started by admin at Tue Apr 24 10:53:10 PDT 2007

**Deployment Status Details**

Status: Deployed (1 out of 1 devices completed.)  
Deployment Job Name: admin\_job\_2007-04-24 10:53:10.468  
Devices To Be Deployed: 1  
Devices Deployed Successfully: 1  
Devices Deployed With Errors: 0

**Deployment Details (1/1 loaded)**

Device	Status	Summary	Method	Config	Transcript
172.25.90.33	SUCCEEDED	Warning: 2	Device		

**Messages**

Messages	Severity	Description
Out of Band Change: CLI		>>>> Difference of file "C:\PROGRAM~1\CISCOpx\MDC\temp\2007.04.24_10.53.15_job_admin_job_2007-04-24_10_53_10_468\phase1\172_25_90_33_4294980740\diff_archived" and file "C:\PROGRAM~1\CISCOpx\MDC\temp\2007.04.24_10.53.15_job_admin_job_2007-04-24_10_53_10_468\phase1\172_25_90_33_4294980740\diff_uploaded".
Operation Successful		
Sig update compilation warning		
Sig update engine compilation status		
Operation Successful		
Deployment Log		

Refresh Abort Close Help

## 関連情報

- [Cisco IOS 侵入防御システム \(IPS\) 製品 & サービス ページ](#)
- [5.x シグニチャ形式を使用した Cisco IOS IPS の導入](#)
- [IPS 5.x シグニチャ形式のサポートおよびユーザビリティ拡張](#)
- [Cisco Intrusion Prevention System](#)
- [セキュリティ製品に関する Field Notices \( CiscoSecure Intrusion Detection を含む \)](#)
- [テクニカルサポート - Cisco Systems](#)