Cisco IOS IPS 設定例での CiscoWorks IPS MC

内容

概要

CiscoWorks Management Center for IPS Sensors（IPS MC）は、Cisco IPS デバイスの管理コンソールです。IPS MC バージョン 2.2 では、Cisco IOS® Software ルータの侵入防御システム（IPS）機能のプロビジョニングがサポートされています。このドキュメントでは、IPS MC 2.2 を使用して Cisco IOS IPS を設定する方法について説明します。

IPS MC の使用方法の詳細（IPS MC を使用して Cisco IOS ソフトウェアに基づいていないデバイスを設定する方法を含む）については、次の URL にある CiscoWorks Management Center for IPS Sensors のドキュメントを参照してください。

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/index.html

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 CiscoWorks Management Center for IPS Sensors（IPS MC）バージョン 2.2 に基づいています。

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。

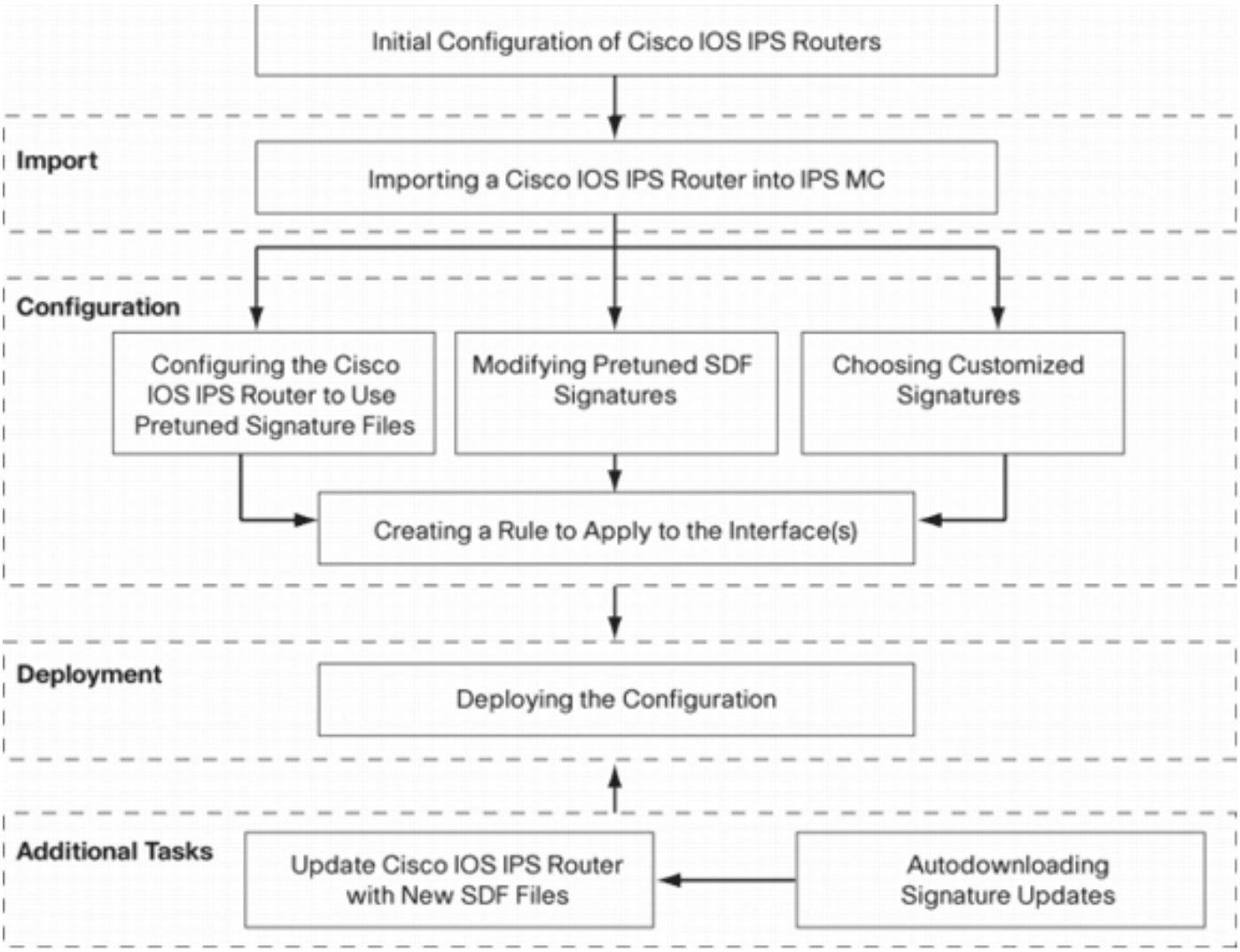
表記法

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

設定タスクに関する基本的な知識

IPS MC は、Cisco IOS IPS ルータのグループの設定を管理するために使用されます。IPS MC では、IPS が稼働するルータからのアラートは管理されない点に注意してください。IPS のモニタリングに Cisco Security Monitoring, Analysis and Response System（Cisco Security MARS）を使用することを推奨します。このドキュメントでは、一連の設定管理作業を説明します。次の図に示すように、これらの作業は 3 つのフェーズ（インポート、設定、導入）に分割されます。



各フェーズには固有の責任と役割があります。

- *インポート*：ルータを IPS MC にインポートします。IPS MC を使用してルータを設定する前に、IPS MC にルータをインポートしておく必要があります。ルータで初期 IPS 設定がない場合はルータをインポートできません（詳細についてはこのドキュメントで後述します）。
- *設定*：デバイスを設定します。たとえば、シスコ推奨の事前調整シグニチャ ファイルの 1 つを使用するように Cisco IOS IPS ルータを設定できます。設定の変更は IPS MC に保管されますが、このフェーズではルータには送信されません。
- *導入*：実際のデバイスに設定の変更を導入します。このフェーズでは、設定タスクで行った変更をルータにコミットします。
- *追加作業*：IPS MC には、Cisco.com からシグニチャ更新を自動的にダウンロードする自動ダウンロード機能があります。

IPS MC を効果的に使用するには、このフェーズ方式のアプローチを理解しておく必要があります。これは、デバイス ベースの管理 GUI（Cisco ルータや Security Device Manager（SDM）など）とは異なります。 デバイス ベースの GUI はシングル ルータに対して直接機能しますが、IPS MC はネットワーク全体でルータ（および Cisco IPS 4200 シリーズ センサなどのその他の IPS デバイス）のグループに対して機能します。

このドキュメントでは、ダイアグラムに示されている各タスクについて説明し、IPS MC を使用した Cisco IOS IPS ルータの管理を支援します。

Cisco IOS IPS ルータの初期設定

Cisco IOS IPS ルータを IPS MC に適切にインポートまたは追加するには、Cisco IOS IPS ルータで以下の初期設定手順を実行する必要があります。このセクションでは初期設定手順について説明します。

Cisco IPS MC で設定、インポート、および導入を実行できるようにするため、Cisco IOS IPS ルータでセキュア シェル（SSH）プロトコルを有効にする必要があります。また、イベント報告のために Security Device Event Exchange（SDEE）プロトコルを有効にする必要があります（ただし、IPS MC は報告ではなくプロビジョニングのみに使用されるため、アラートは IPS MC に送信されません）。 また、IPS ルータのクロック設定が IPS MC と同期していることを確認する必要があります。

IOS IPS ルータを設定するには、次の手順を実行します。

1. ルータのローカル ユーザ名とパスワードを作成します。
```
Router#config terminal
Router(config)#username <username> password <password>
```

2. vty 回線インターフェイスでローカル ログオンを有効にします。
```
Router#config terminal
Router(config)#line vty 0 15
Router(config-line)#login local
Router(config-line)#exit
```

   トランスポート入力またはトランスポート出力コマンドライン インターフェイス（CLI）を vty 回線設定で設定している場合、SSH が有効になっていることを確認します。以下に、いくつかの例を示します。
```
Router#conf terminal
Router(config)#line vty 0 15
```

```
Router(config-line)#transport input ssh telnet
Router(config-line)#exit
```

3. 1024 ビットの RSA 鍵を生成します（鍵がまだ存在していない場合）。暗号鍵の生成後に SSH が自動的に有効になります。

```
Router#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto key generate rsa
The name for the keys will be: Router.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys.
    Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Router(config)#
*Jan 23 00:44:40.952: %SSH-5-ENABLED: SSH 1.99 has been enabled
Router config)#
```

4. ルータで SDEE を有効にします。

```
Router(config)#ip ips notify sdee
```

5. HTTPS を有効にします。IPS MC が、SDEE が有効なルータと通信してイベント情報を収集するには、HTTP または HTTPS が必要です。

```
Router(config)#ip http authentication local
Router(config)#ip http secure-server
```

6. IPS ルータのクロック設定を行うには、外部 Network Time Protocol（NTP）サーバまたはクロック コマンドを使用します。

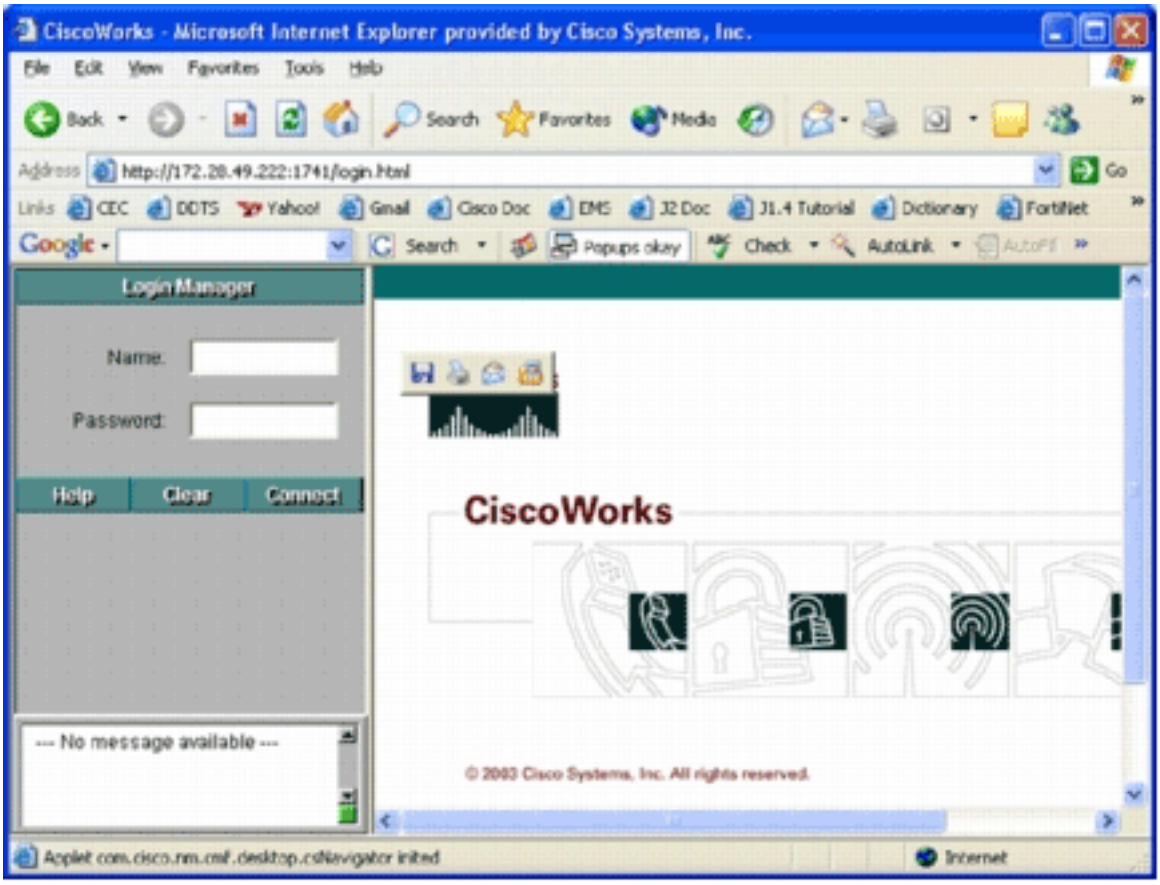
```
Router(config)#clock set hh:mm:ss day month year
```

これで Cisco IOS IPS ルータの準備ができました。IPS MC にルータをインポートして、設定および管理を進めることができます。

IPS MC への Cisco IOS IPS ルータのインポート

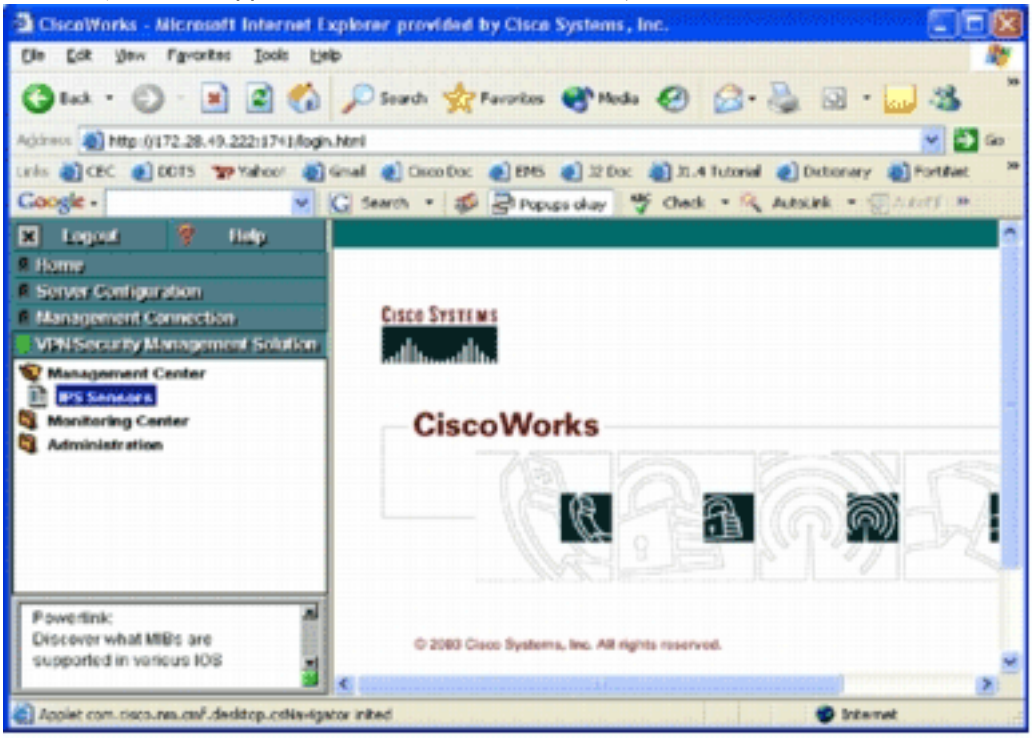
ルータの初期設定が完了したら、ルータを IPS MC に追加（インポート）できます。

1. Web ブラウザを開き、CiscoWorks サーバを指し示します。CiscoWorks Login Manager が表示されます。



注：Webサーバのデフォルトのポート番号は1741です。したがって http://<*server ip address*>:1741/ のような URL を使用してください。

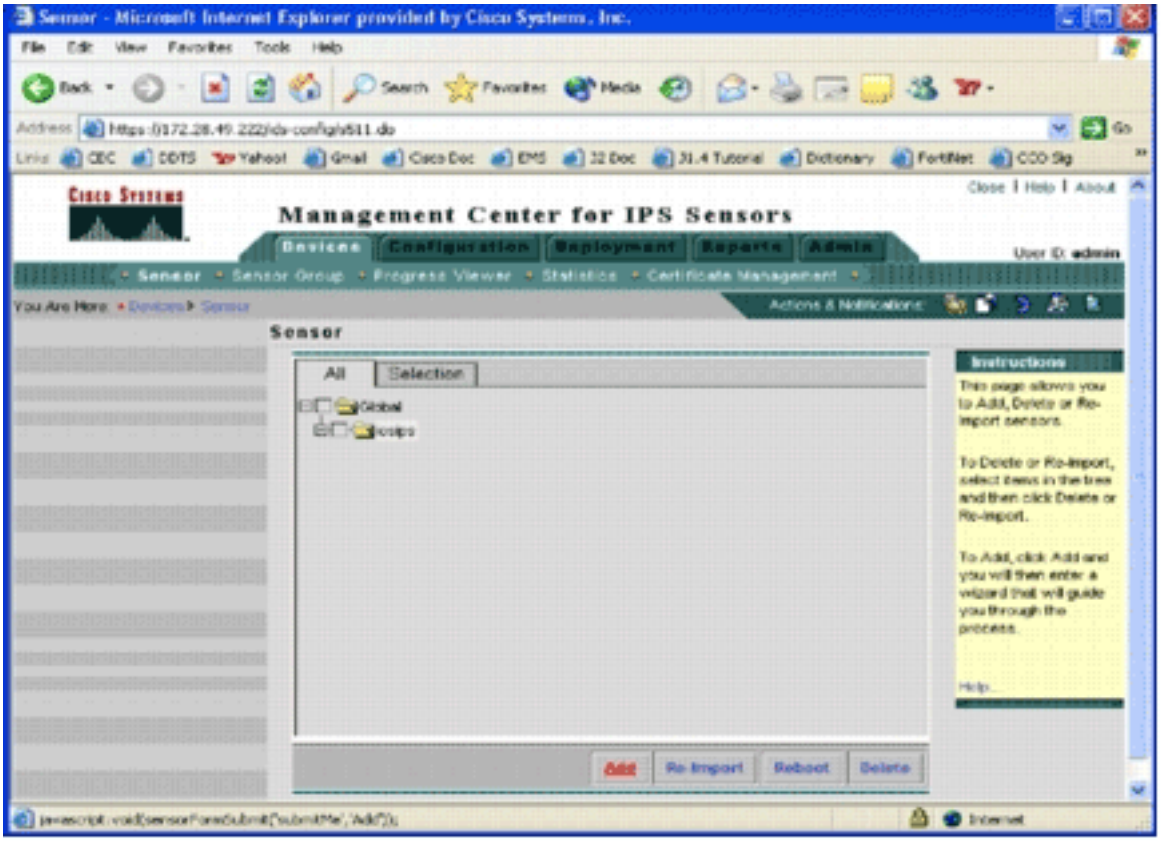
2. ログインするため、ユーザ名とパスワードを入力します。CiscoWorks メイン ページが表示されます。



3. 左側のナビゲーション ペインで [VPN/Security Management Solution] を選択し、次に [Management Center] を選択します。[Management Center for IPS Sensors] ページが表示さ

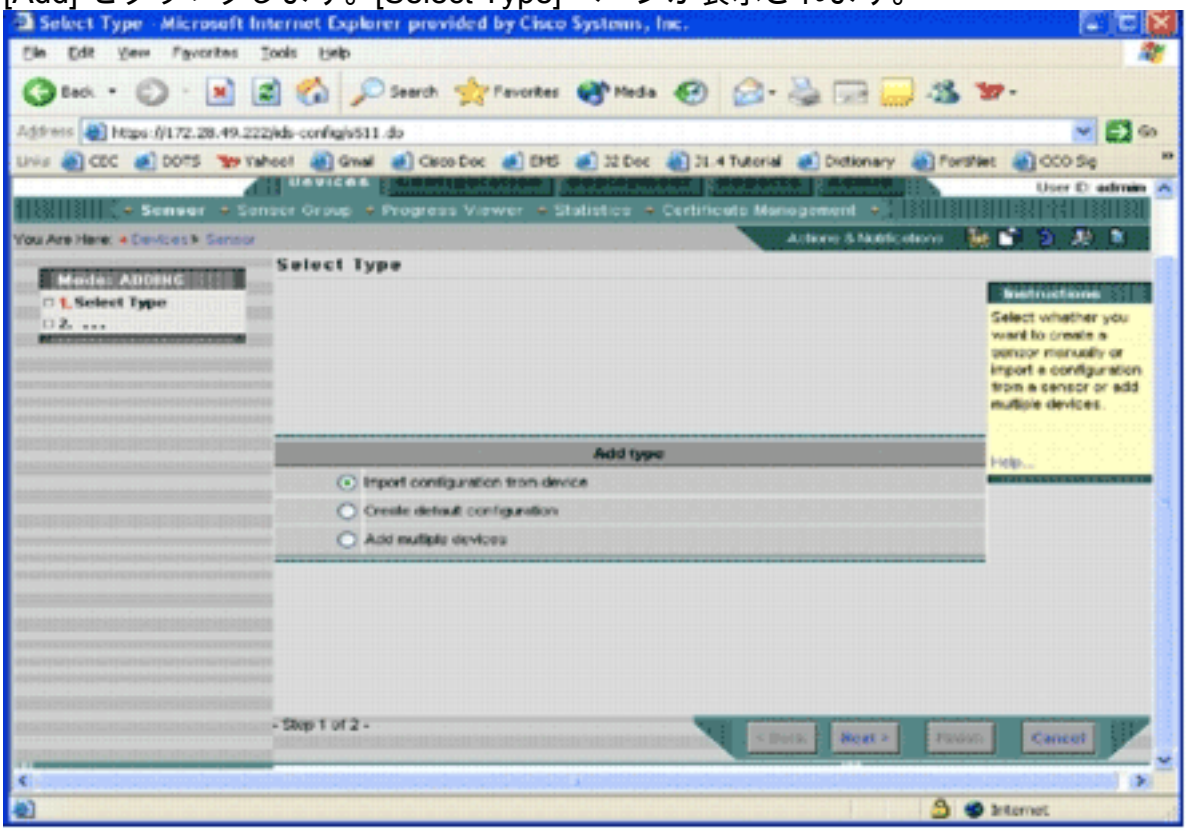
れます。このページには次の 5 つのタブが表示されます。*Devices* : [Devices] タブでは、システムのすべてのデバイスの初期設定と管理を行います。*Configuration* : [Configuration] タブでは、プロビジョニング機能を実行できます。個別のデバイス レベルまたはグループ レベルでデバイスを設定できます。1 つのデバイス グループに複数のデバイスを含めることができます。設定タスクによって行った変更はすべて保存する必要があります。設定機能は、変更をデバイスにただちに反映しません。変更を導入するには、導入機能を使用する必要があります。*Deployment* : [Deployment] タブでは、設定変更をデバイスに導入できます。スケジュール機能により、設定の変更が有効になる時点を柔軟に制御できます。*Reports* : [Reports] タブでは、さまざまなシステム運用レポートを作成できます。*Admin* : [Admin] タブでは、データベース管理、システム設定、ライセンス管理などのシステム管理タスクを実行できます。

4. 新しいデバイスを追加するには、[Devices] タブをクリックします。[Sensor] ページが表示



されます。

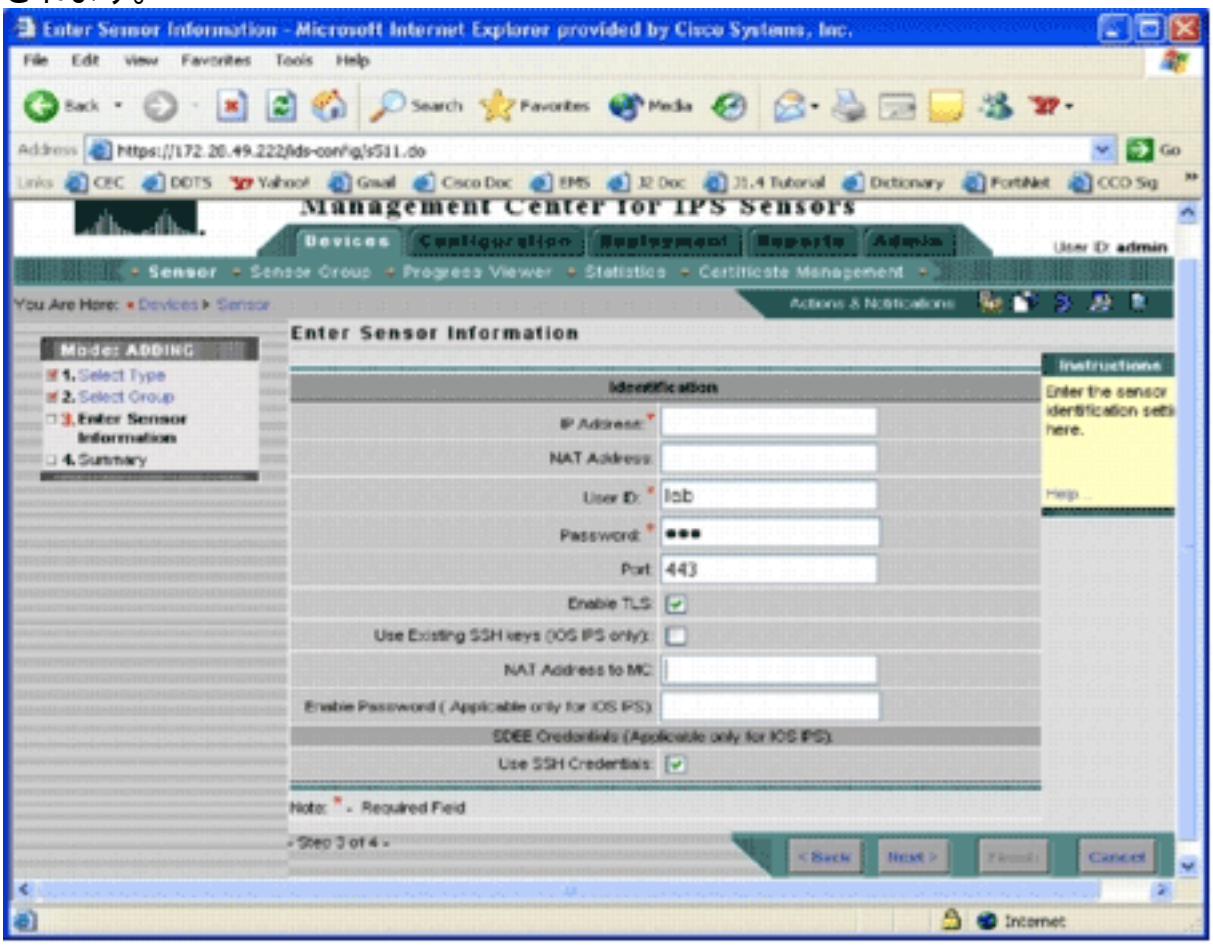
5. [Add] をクリックします。[Select Type] ページが表示されます。



IPS MC に対し、実行する追加機能のタイプを通知する必要があります。各オプションについて以下で説明します。*Import configuration from device*：このオプションは、現在ネットワーク上で稼働している IPS MC デバイスに追加するときに使用します。*Create default configuration*：このオプションは、現在ネットワーク上で稼働していないデバイスを追加するときに使用します。*Add multiple devices*：このオプションは、複数のデバイスを追加するときに使用します。デバイスを一括で追加するには、すべてのデバイスの情報を記述した .csv または .xml ファイルを作成して IPS MC にインポートできます。**ヒント：サンプルの**.csv形式および.xml形式ファイルは次の場所にあります。InstallDirectory\MDC\etc\ids\ にあ

ります。これらのファイルの名前は MultipleAddDevices-format.csv と MultipleAddDevices-format.xml です。

6. 該当する追加タイプのオプションを選択して [Next] をクリックします。
7. Cisco IOS IPS ルータの追加先グループを選択するか、またはデフォルトのグローバル グループを使用します。次に [Next] をクリックします。[Enter Sensor Information] ページが表示されます。



8. [Identification] ページでデバイスの識別情報を入力します。**注：ユーザ**に権限レベル15のアクセス権がない場合は、イネーブルパスワードを指定する必要があります。[Identification] ページの最後の行で [Use SSH Credentials] チェック ボックスをオンにします。
9. [next] をクリックします。[Add Sensor Summary] ページが表示されます。
10. [Finish] をクリックします。デバイスが IPS MC に正常に追加されました。**注：インポート**プロセス中にエラーが発生した場合は、次の項目を確認してください。*前提条件の設定*：IPS MC が Cisco IOS IPS ルータと通信するために必要な設定です。*接続*：IPS MC が Cisco IOS IPS ルータに到達できることを確認します。*クロック*：IPS MC の時刻と Cisco IOS IPS ルータの時刻を確認します。認証に使用する https 証明書では、時刻は重要な要素です。この 2 つの時刻の差は 12 時間以内でなければなりません（ベスト プラクティスは数時間です）。*Cisco IOS IPS 証明書*：保管されている Cisco IOS IPS 証明書が正しくないことがあります。Cisco IOS IPS から証明書を削除するには、Cisco IOS IPS ルータからトラストポイントを削除する必要があります。*追加の設定*：**ip http timeout-policy** に要求の最大数として小さな値が設定されている場合（例：**ip http timeout-policy idle 600 life 86400 requests 1**）、最大要求数を増加する必要があります。以下に、いくつかの例を示します。**ip http timeout-policy idle 600 life 86400 requests 8400**

事前調整シグニチャ ファイルを使用する Cisco IOS IPS ルータの設定

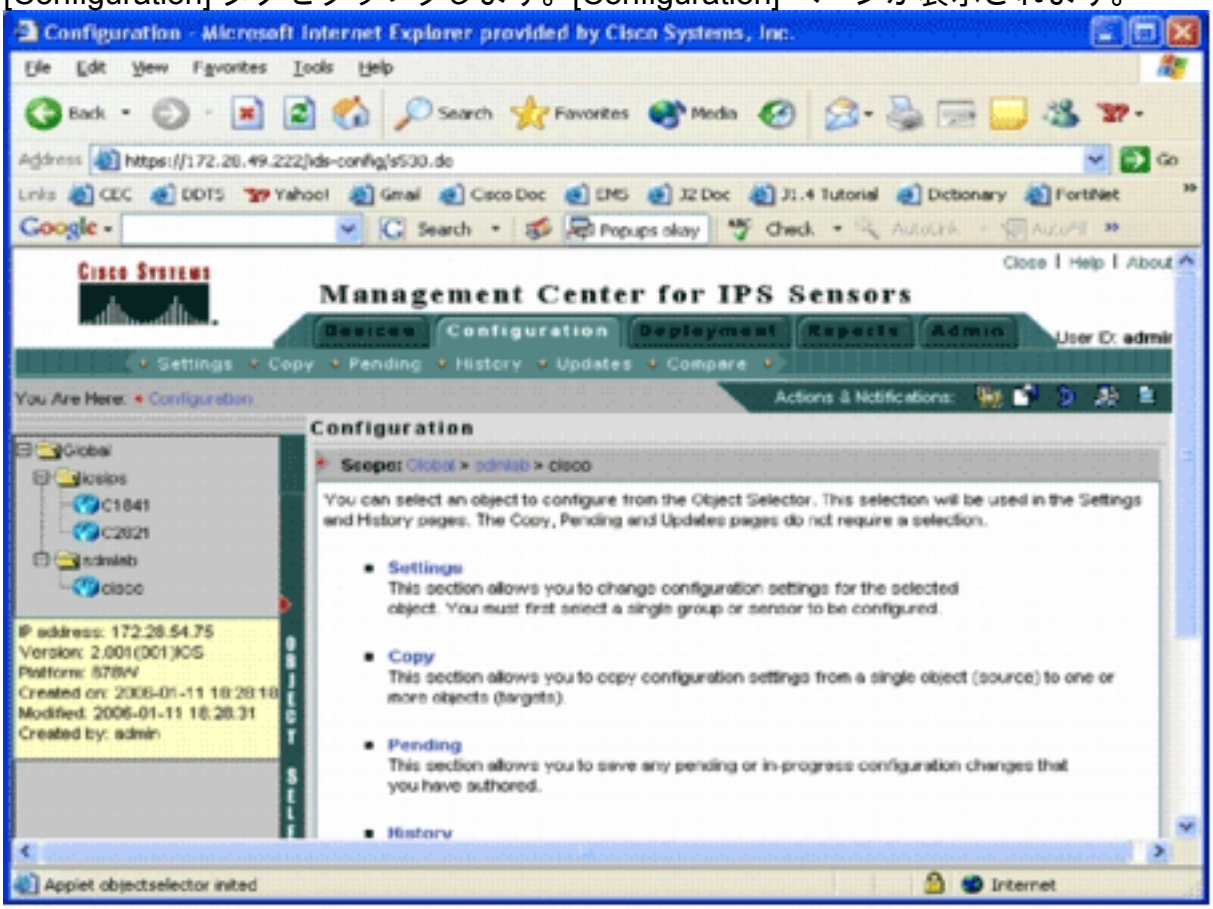
ルータを IPS MC にインポートした後で、シグニチャ定義ファイル（SDF）（IPS ルータが使用

する脅威のシグニチャが記述されているテキスト ベースのファイル）と、シグニチャがトリガーされた場合に実行するアクション（ドロップ、TCP リセット、アラームなど）を選択する必要があります。

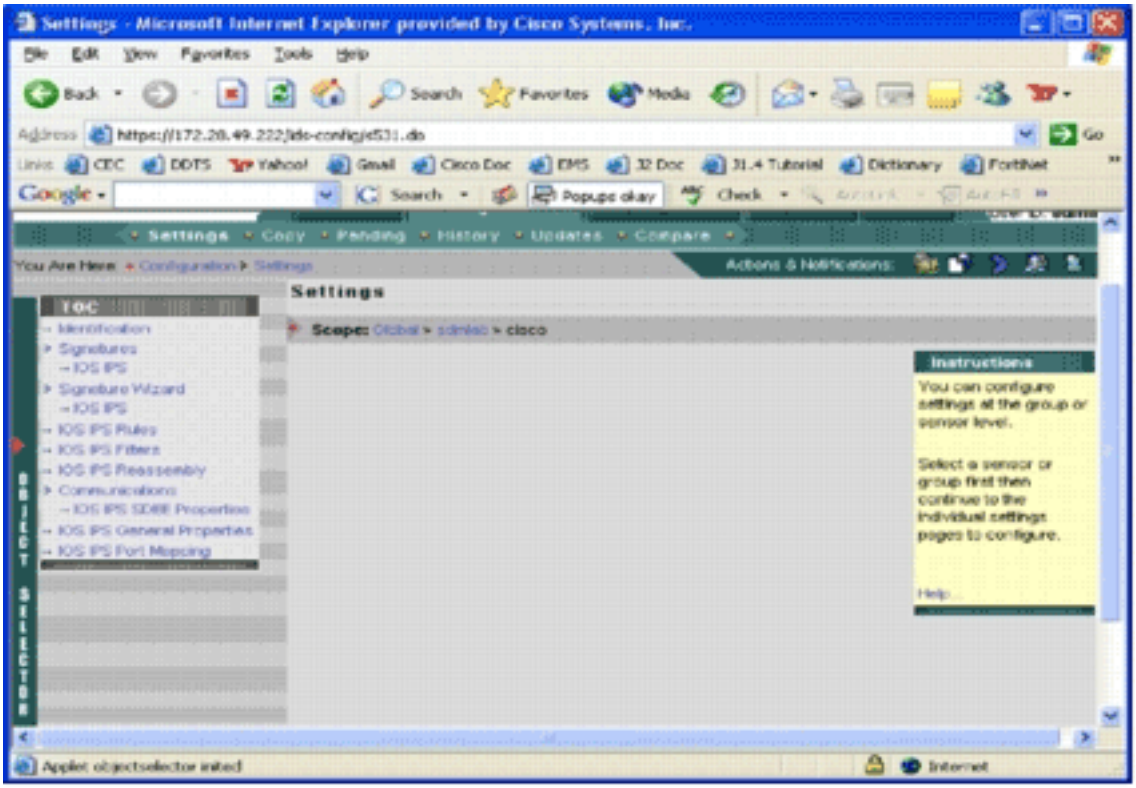
Cisco Systems® では、Cisco事前調整SDFファイルを使用することを推奨しています。現時点では 3 種類のファイルがあります（attack-drop.sdf、128MB.sdf、256MB.sdf）。IPS MC はこれらのファイルを Cisco.com から自動的にダウロードできます。詳細については、「シグニチャ更新の自動ダウンロード」を参照してください。

この手順では、1 つのデバイスを例に、IPS を設定せずにルータを開始する方法を示します。この手順は、グループ レベルで複数のデバイスに対しても使用できます。

1. [Configuration] タブをクリックします。[Configuration] ページが表示されます。

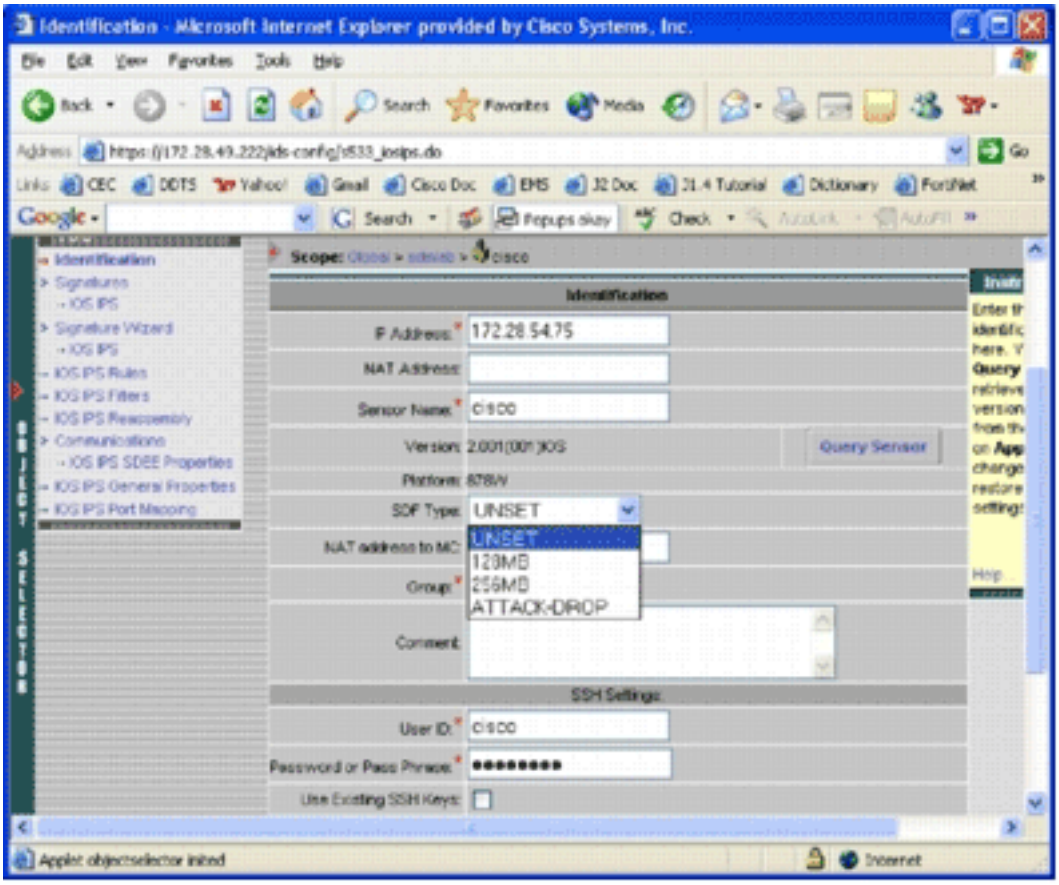


2. ページ左側にある [Object Selector] で、設定する Cisco IOS IPS ルータを選択します。**注**：IPS MC 2.2の設定の大部分は、グループレベルでも個々のデバイスレベルでも設定できます。たとえば、global、iosips、sdmlab グループはすべて設定可能なオブジェクト グループです。この例では、個々のデバイス（sdmlab グループの cisco）を使用します。設定するルータを選択したら、[Configuration] ページ上部のパス バーに、現在の設定範囲が表示されます。たとえばこの例の範囲は *Global* > *sdmlab* > *cisco* です。*cisco* は現在の設定オブジェクト（[Object Selector] から選択されたルータ）です。
3. [Configuration] メニュー バーで [Settings] をクリックします。[Settings] ページが表示されます。

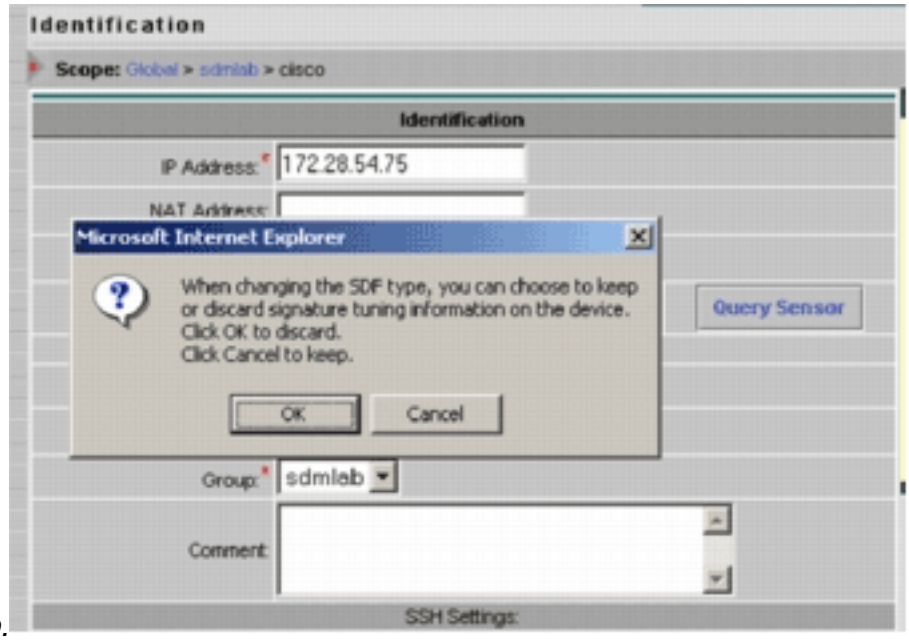


[Settings] ページで、選択されているオブジェクトの設定を変更できます。Cisco IOS IPS ルータ固有の設定は、ページ左側の [TOC] セクションに表示されます。[TOC] セクションの下で使用可能なタスクを以下に示します。*[Identification]* : Cisco IOS IPS ルータの基本情報です。事前調整 SDF ファイルをここで指定できます。*[Signature]* : Cisco IOS IPS ルータのシグニチャです。*[Signature Wizard]* : カスタマイズしたシグニチャを追加するためのシグニチャ ウィザードです。*[Cisco IOS IPS Rules]* : インターフェイスに適用する Cisco IOS IPS ルールを設定します。*[Cisco IOS IPS Filters]* : Cisco IOS IPS フィルタです。*[Cisco IOS IPS Reassembly]* : インターフェイス IP 仮想再構成設定です。*[Cisco IOS IPS SDEE Properties]* : SDEE 設定を編集できます。*[Cisco IOS IPS General Properties]* : 追加の Cisco IOS IPS 関連設定です。

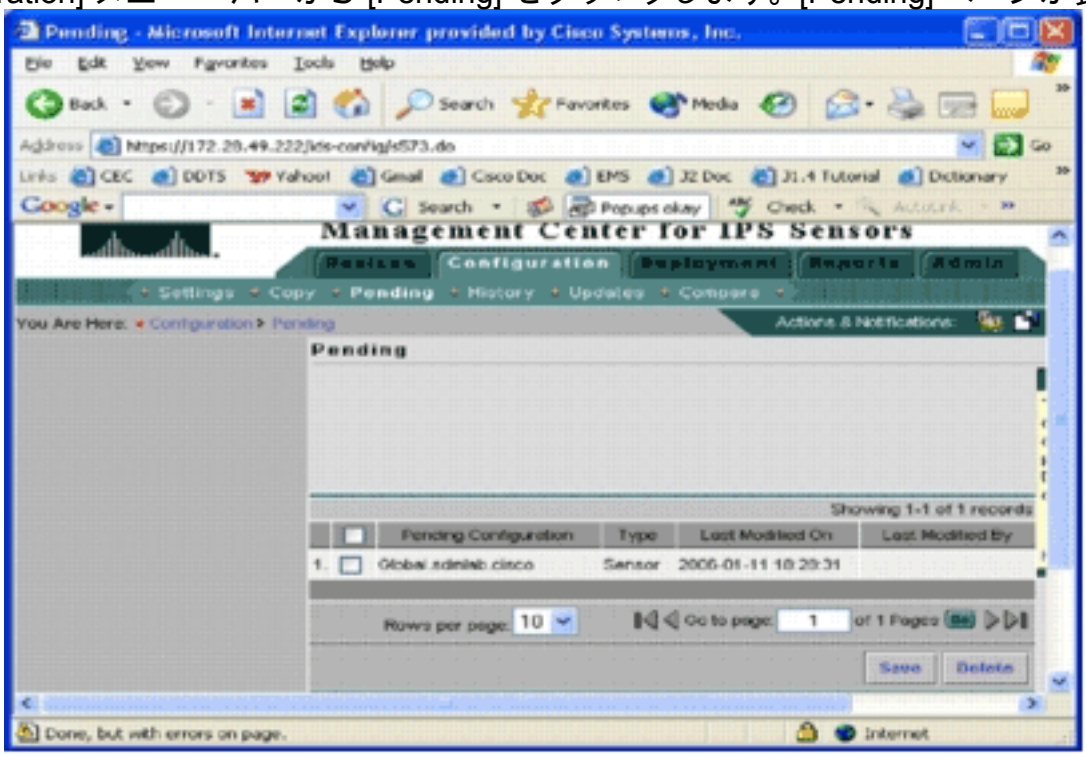
4. 事前調整 SDF ファイルを設定するには、[Identification] を選択します。[Identification] ページが表示されます。



5. [SDF Type] ドロップダウン リストから該当する事前調整 SDF を選択し、[Apply] をクリックして変更を適用します。Cisco IOS IPS では 1600 を超えるシグニチャがサポートされていますが、これはルータのメモリ許容量を超えています。SDF は、最も重要なシグニチャを選択してロードするための手段として開発されました。現時点では、3 つの SDF から選択できます。ルータの DRAM の容量に基づいて SDF ファイルを選択できるように、これらの SDF ファイルのサイズは異なります。選択可能な項目を以下に示します。UNSET：SDF タイプが設定されていません。ATTACK-DROP：この SDF は、64 MB の DRAM を搭載したルータ向けです。256MB：この SDF は、256 MB の DRAM を搭載したルータ向けです。128MB：このSDFは、128 MBのDRAMを搭載したルータ用です。**注：128**および256 MBのSDFには2.001以上のエンジンが必要です。この情報は、[Settings] > [Identification UI] > [Version] フィールドで確認できます。**警告：**IPS MCには、Cisco IOS IPSルータのメモリ管理機能は含まれていません。ご使用の Cisco IOS IPS ルータに対して SDF ファイルを選択するときには注意してください。Cisco IOS IPS ルータに、選択した SDF ファイルを実行できる十分なメモリが搭載されていることを確認してください。**注：SDFの**種類を変更すると、次のメッセージが表示されることがあります。*When changing the SDF type, you can choose to keep or discard signature tuning information on the device.Click OK to*



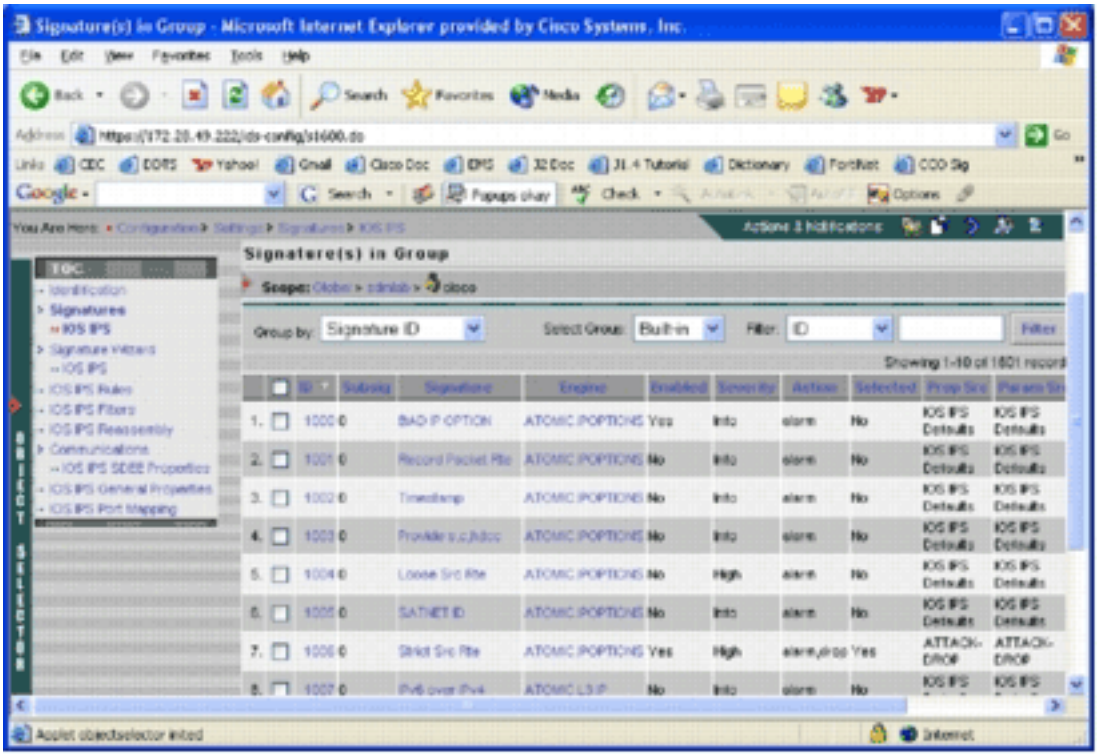
discard.Click Cancel to keep.

6. シグニチャ調整情報を維持する場合は [Cancel] をクリックします。これで、ルータ cisco の事前調整 SDF を選択できました。次に、シグニチャの追加、編集、専用シグニチャの作成などのシグニチャ調整作業を行うか、またはシグニチャ調整作業を行わずに「インターフェイスに適用するルールの作成」に直接進むことができます。
7. [Configuration] メニュー バーから [Pending] をクリックします。[Pending] ページが表示されます。 

この時点で設定タスクは完了です。ただし、ターゲット デバイスに変更を導入するには、導入タスクを実行する必要があります。

事前調整 SDF シグニチャの変更

ルータに対して事前調整 SDF ファイルを選択したら、追加のシグニチャ調整タスクを実行できます。ニーズに対応するようにシグニチャを追加、編集、削除、変更するか、または必要に応じて独自のシグニチャを作成することができます。この例では、シグニチャを追加してアクションを変更するために IPS MC を使用します。次の画像は、シグニチャ設定インターフェイスを示します。



シグニチャ設定を使用して、シグニチャの有効化および無効化、選択および選択解除、追加、削除、シグニチャ アクションの変更、シグニチャ パラメータの編集を行うことができます。左側の Signature Wizard を使用して、カスタマイズしたシグニチャを作成します。

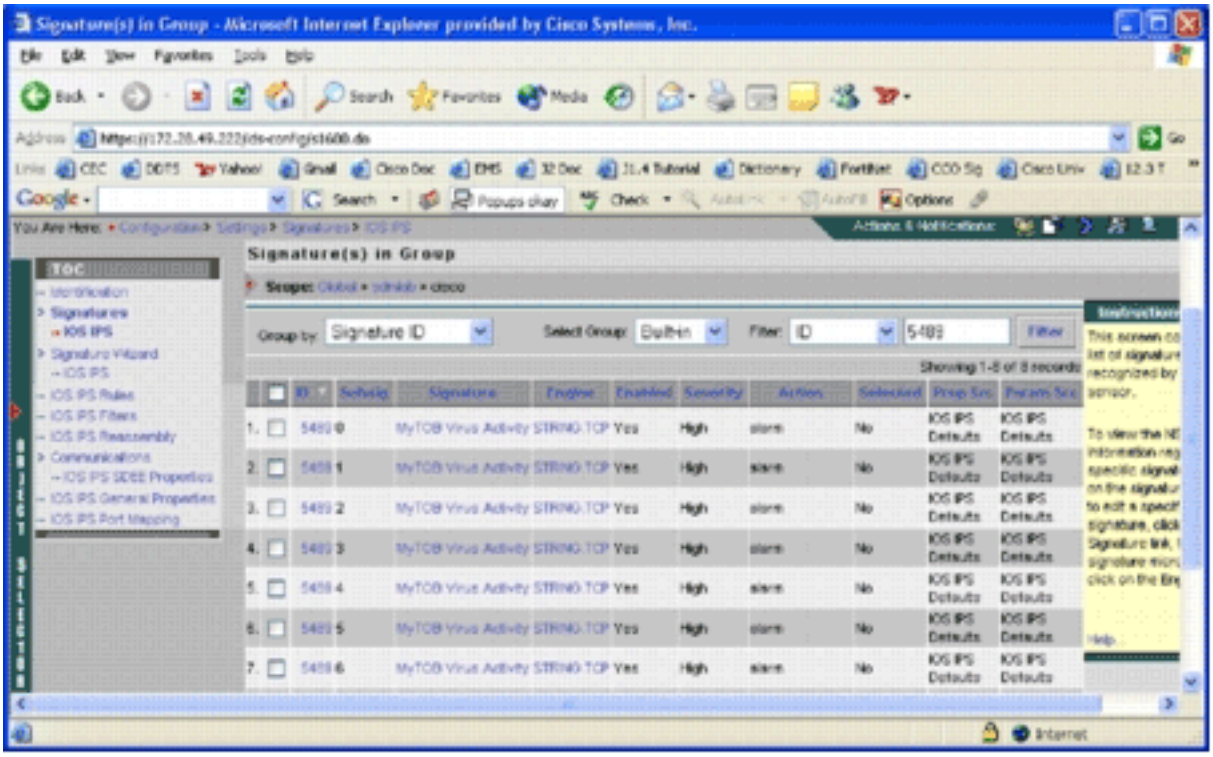
デフォルトでは、シグニチャ設定インターフェイスに一部の情報が表示されます。[Selected] は、ルータに送信される SDF ファイルにシグニチャが含まれるかどうかを示します。シグニチャが選択されていない場合、そのシグニチャは追加されません。[Enabled] は、シグニチャが選択されている場合にのみ適用されます。シグニチャが無効になっている場合、IPS エンジンはそのシグニチャのイベントを送信しません。シグニチャの選択が解除されると、自動的に無効になります。

最後の 2 列（[Prop Src] と [Param Src]）は、シグニチャとそのパラメータの取得元を示します。シグニチャは事前調整 SDF ファイルから取得されるか、または工場出荷時デフォルトから取得されます。工場出荷時デフォルトは、IOS-Sxxx.zip ファイル更新で確認できます（[IOS IPS Deafults] として示されます）。 これらの値はパラメータ列にも適用されます。

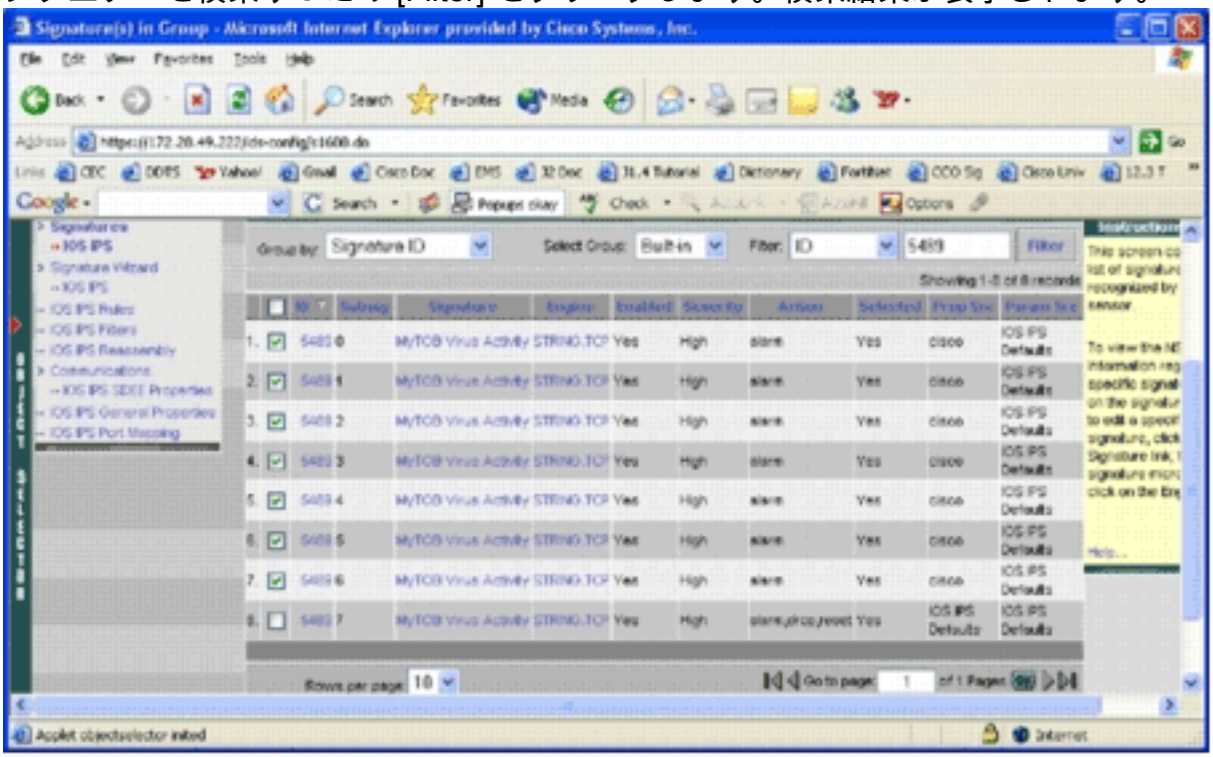
Cisco IOS IPS ルータにシグニチャを追加するときには、メモリに関する考慮事項を検討する必要があります。Cisco IOS IPS ルータで処理可能な上限を上回るシグニチャを追加すると、IPS MC は設定変更をデバイスに導入できなくなります。

シグニチャ 5489/x を Cisco IOS IPS ルータに追加するには、次の手順を実行します。

1. [Configuration] を選択し、[Object Selector] を使用して IPS シグニチャを設定する Cisco IOS IPS ルータを選択します。
2. [Configuration] > [Settings] > [Signatures] > [IOS IPS] を選択します。[Signature(s) in Group] ページが表示されます。

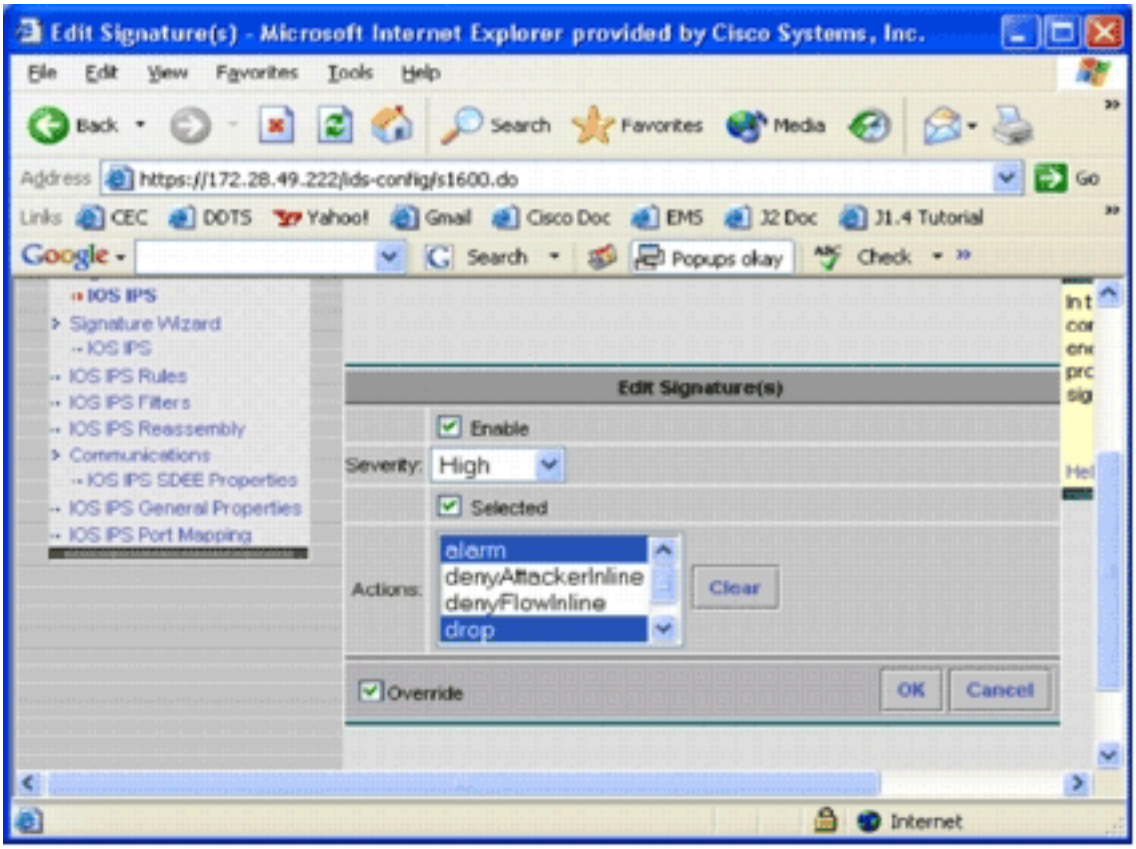


3. 表示されるシグニチャ リストで [Filter by ID] を選択し、シグニチャ ID 5489 を入力します。
4. シグニチャを検索するため [Filter] をクリックします。検索結果が表示されます。

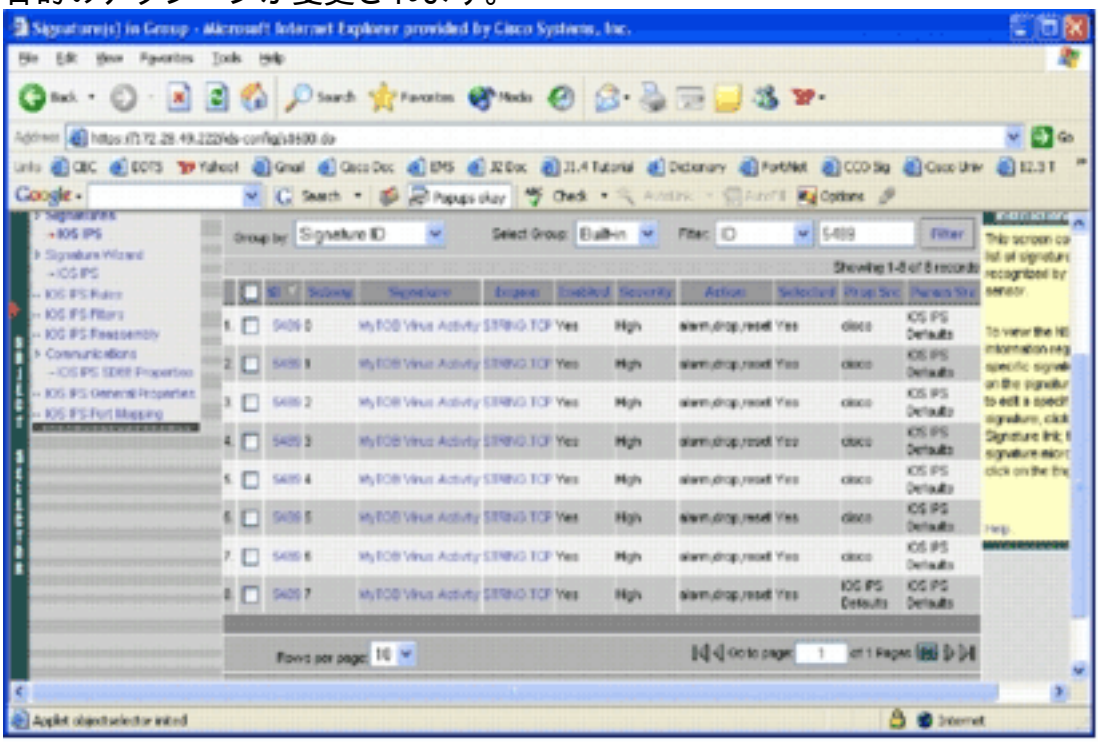


注：IPS MCでは、Cisco SDMで使用できる新しい分類はサポートされていません。

5. 選択されていないシグニチャの横のチェック ボックスをオンにし、下部ツール バーの [Select] をクリックします。
6. シグニチャ アクションを変更するため [Edit] をクリックします。[Edit Signature(s)] ページが表示されます。



7. [Selected] チェック ボックスをオンにし、[Actions] リストから [alarm] 、[drop] 、および [reset] を選択します。
8. [Override] チェックボックスをオンにして、[OK] をクリックします。すべてのシグニチャの目的のアクションが変更されます。



9. [Pending] タスクに移動してすべての変更を保存します。これで設定タスクが完了しました。**ヒント**：[Prop Src]列に注意してください。変更完了後に、ソースがデバイス *cisco* に変更されています。つまり、すべての調整情報がデフォルトの事前調整 SDF ファイルから個別に保存されています。このメカニズムにより、IPS MC はカスタマイズしたシグニチャの変更を維持できます。

前のセクションでは、SDF ファイル タイプを変更したときに、IPS MC からシグニチャ調整情報を維持するかどうかを尋ねられました。これは、参照されるシグニチャ調整情報です。

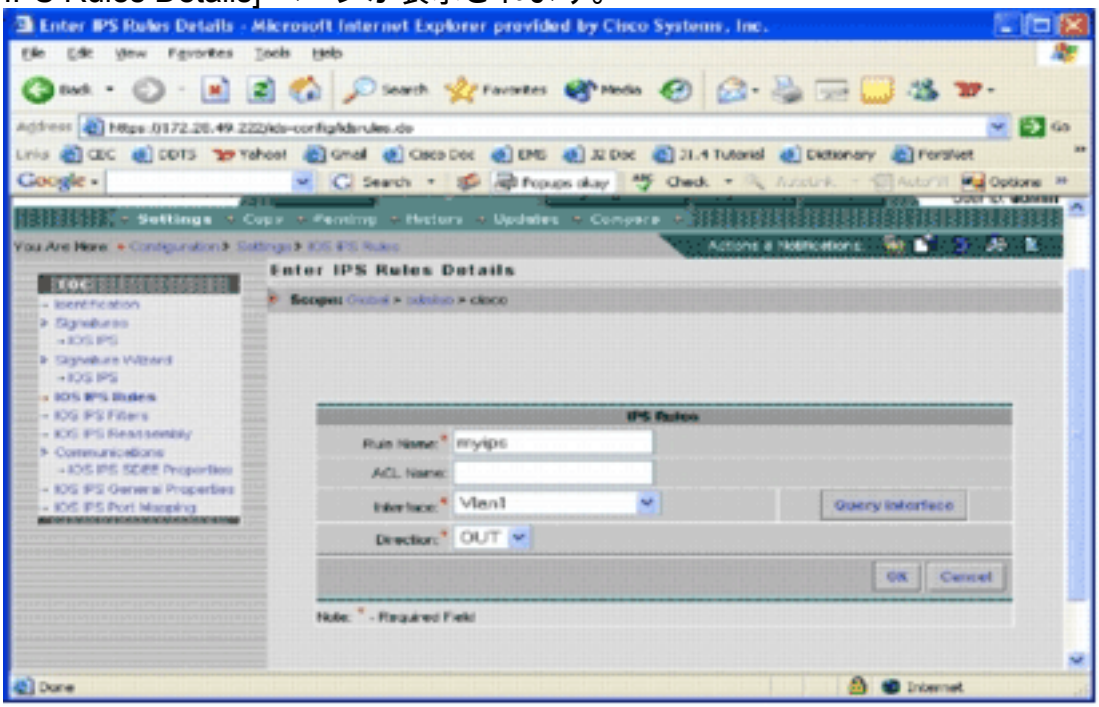
カスタマイズしたシグニチャの選択

デフォルトの事前調整 SDF ファイルを使用しない場合は、「事前調整 SDF シグニチャの変更」で説明する手順に従って、デバイスの調整シグニチャを選択できます。識別ページで SDF タイプが UNSET であることを確認する必要があります。「事前調整シグニチャ ファイルを使用する Cisco IOS IPS ルータの設定」のステップ 3 を参照してください。

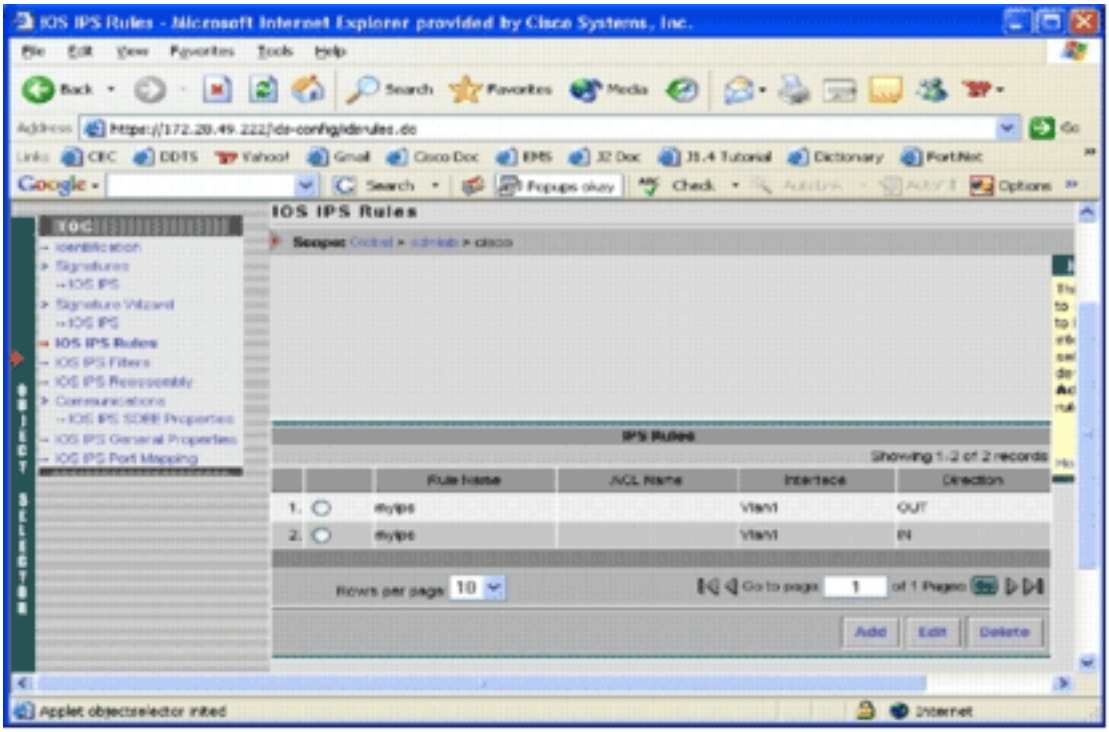
インターフェイスに適用するルールの作成

シグニチャの調整後に、Cisco IOS ルータで IPS を有効にする必要があります。ルータで IPS を有効にするには、IPS ルールを作成し、1 つ以上のインターフェイスに適用する必要があります。

1. [Configuration を選択し、[Object Selector] を使用して設定する Cisco IOS IPS ルータを選択します。パス バーで、範囲がグループ レベルではなくデバイス レベルであることを確認します。
2. [Configuration] > [Settings] > [IOS IPS Rules] を選択し、[Add] をクリックします。[Enter IPS Rules Details] ページが表示されます。



3. ルール名と、ルールと方向を適用するインターフェイスに関する情報を入力します。
4. [OK] をクリックします。[IOS IPS Rules] ページが表示されます。



同様に、インターフェイスに対して両方向のルールを作成できます。

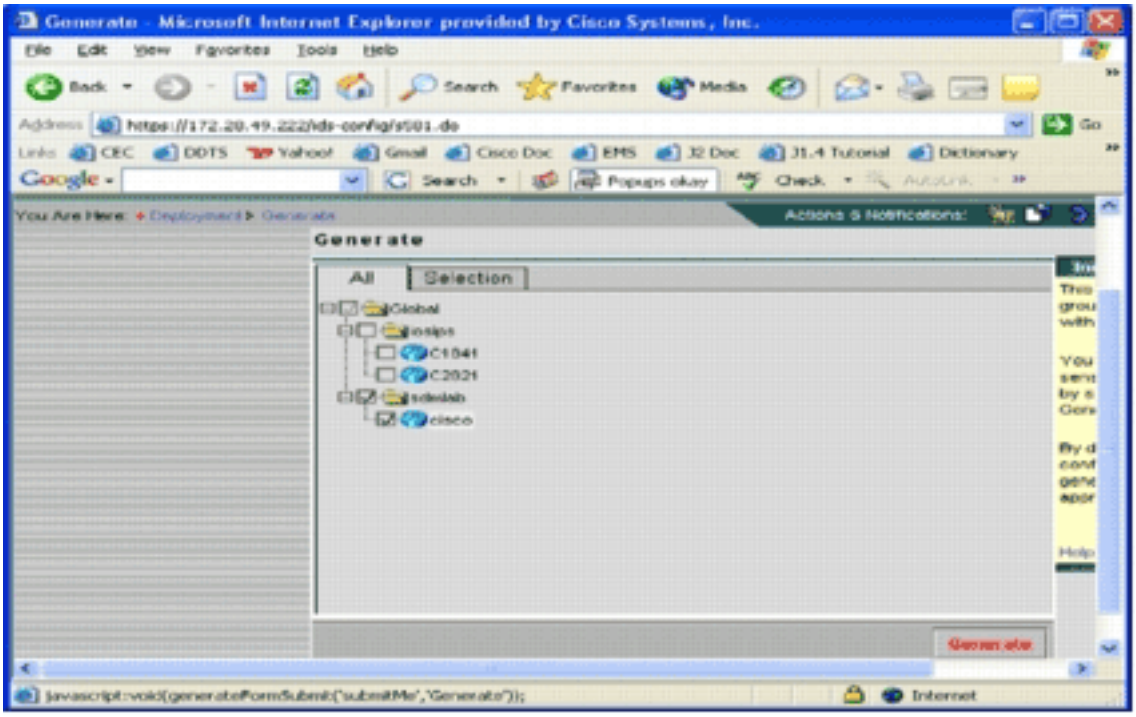
5. 変更を該当するデバイスまたはデバイス グループに導入するには、設定変更内容を保存し、導入プロセスを実行する必要があります。その他の IPS 関連設定も実行できますが、その他のタスクはすべてオプションであり、必須ではありません。すべてのオプションが設定ユーザ インターフェイスの左側に表示されています。このドキュメントでは、任意の設定オプションについては説明しません。

設定の導入

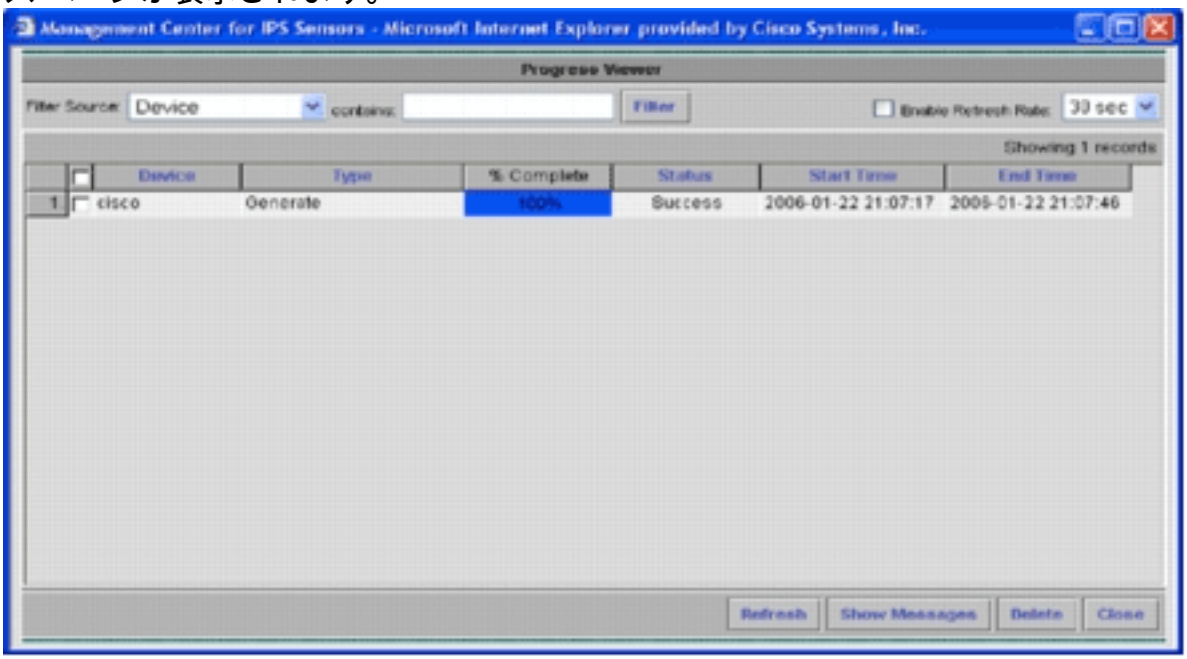
すべての設定変更を行ったら、導入タスクを使用して変更をデバイスにコミットする必要があります。これまでに行ったすべての設定は、IPS MC サーバにローカルに保存されています。

設定変更を導入するには、[Deployment] ページに移動して次の手順を実行します。

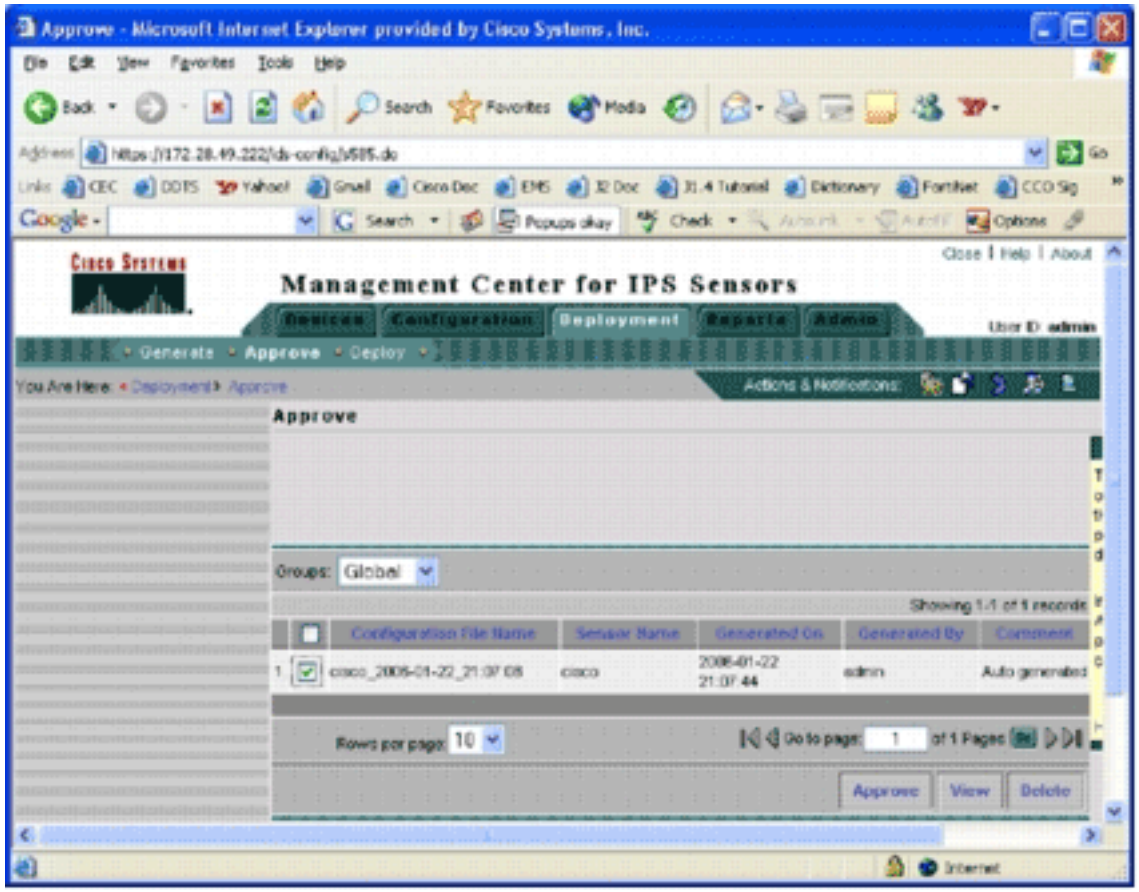
1. [Deployment] タブで、設定変更を生成するため [Generate] を選択します。[Generate] ページが表示されます。



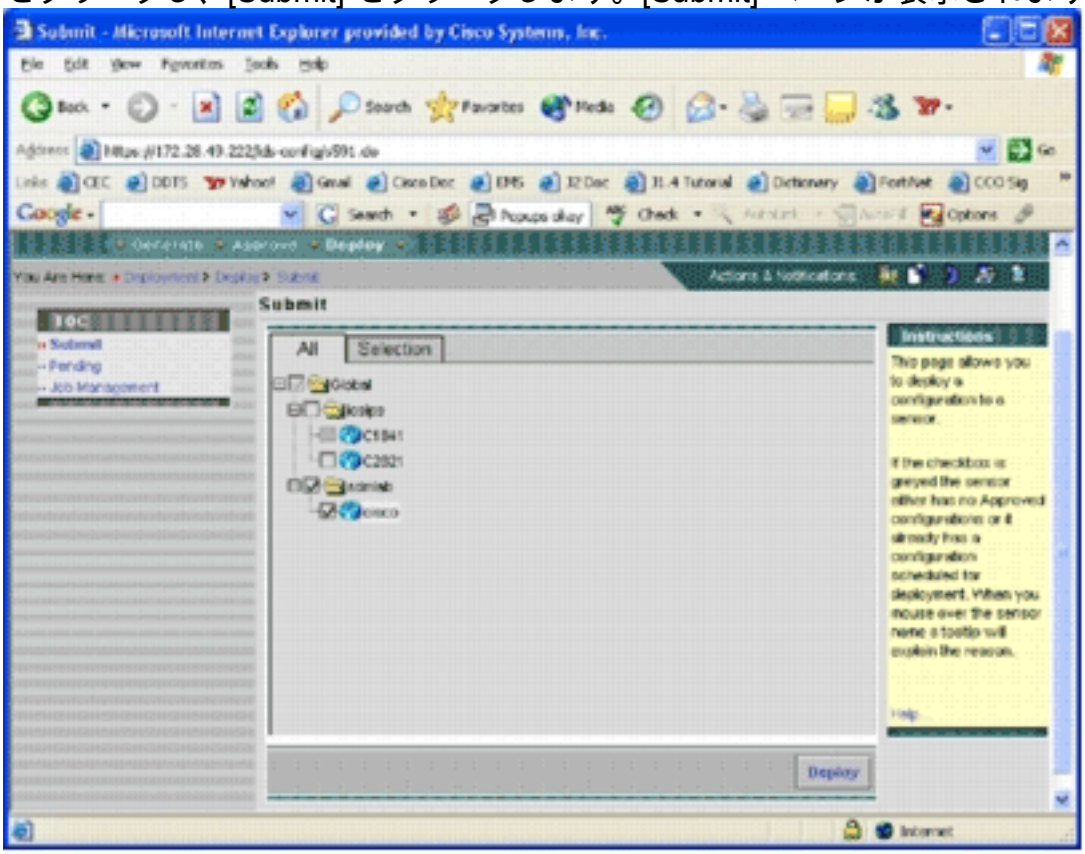
2. 設定した *cisco* デバイスを選択し、[Generate] をクリックします。
3. [OK] をクリックして生成された設定を受け入れ、その後 [OK] をクリックします。ステータス ページが表示されます。



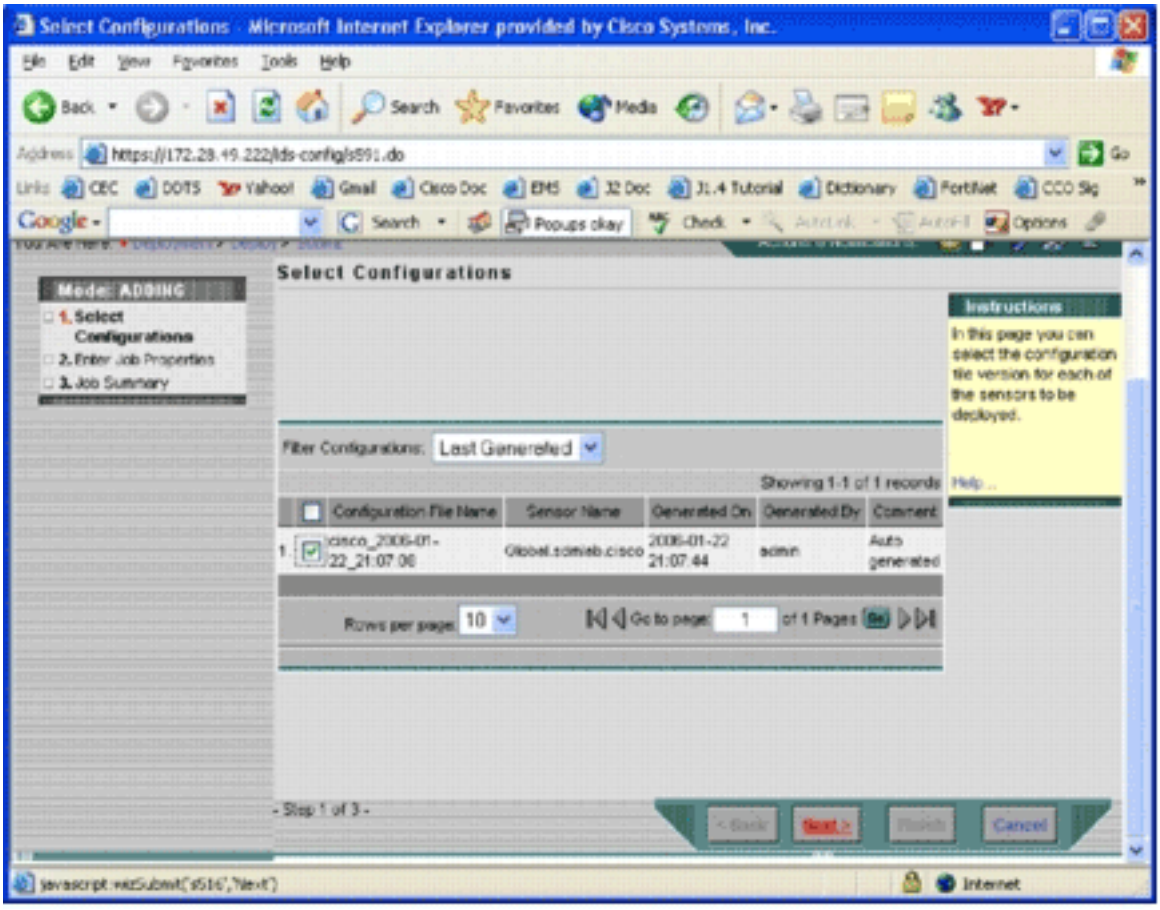
4. 生成タスクが正常に完了するまで、[Refresh] をクリックします。
5. 承認が必要な設定のリストを表示するため、[Deployment] メニュー バーにある [Approve] と sdmlab グループをクリックします。[Approve] ページが表示されます。



6. タスクを選択して [Approve] をクリックします。[Deployment] メニュー バーにある [Deploy] をクリックし、[Submit] をクリックします。[Submit] ページが表示されます。

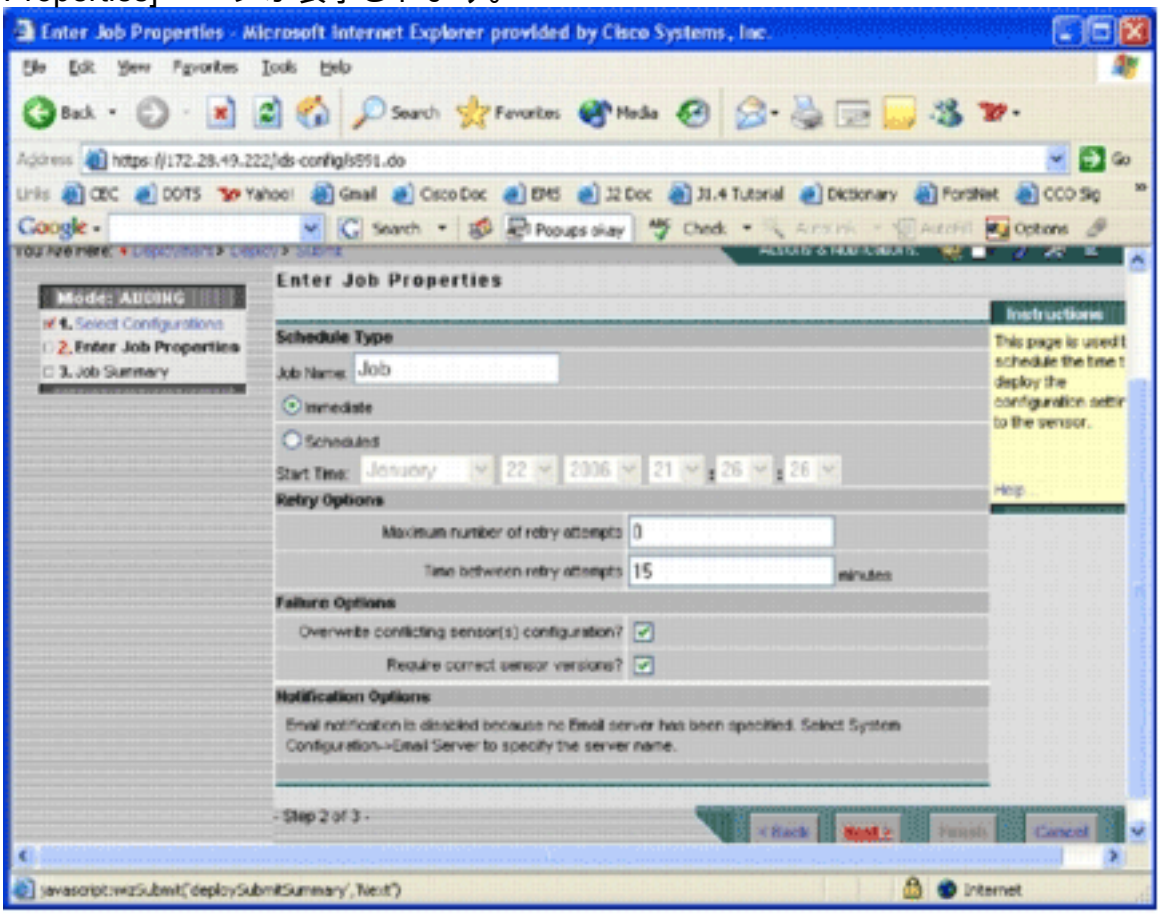


7. 導入タスクを送信するデバイスを選択します。
8. *cisco* デバイスを選択して [Deploy] をクリックします。[Select Configurations] ページが表示

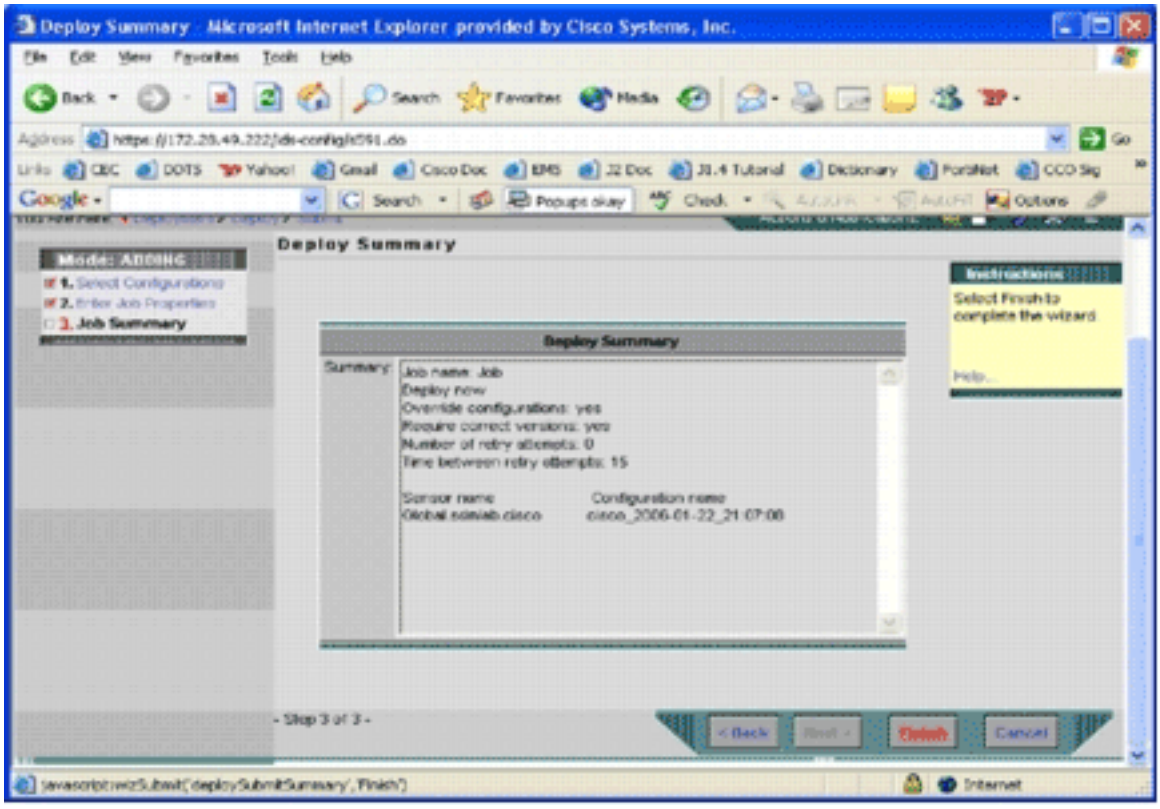


されます。

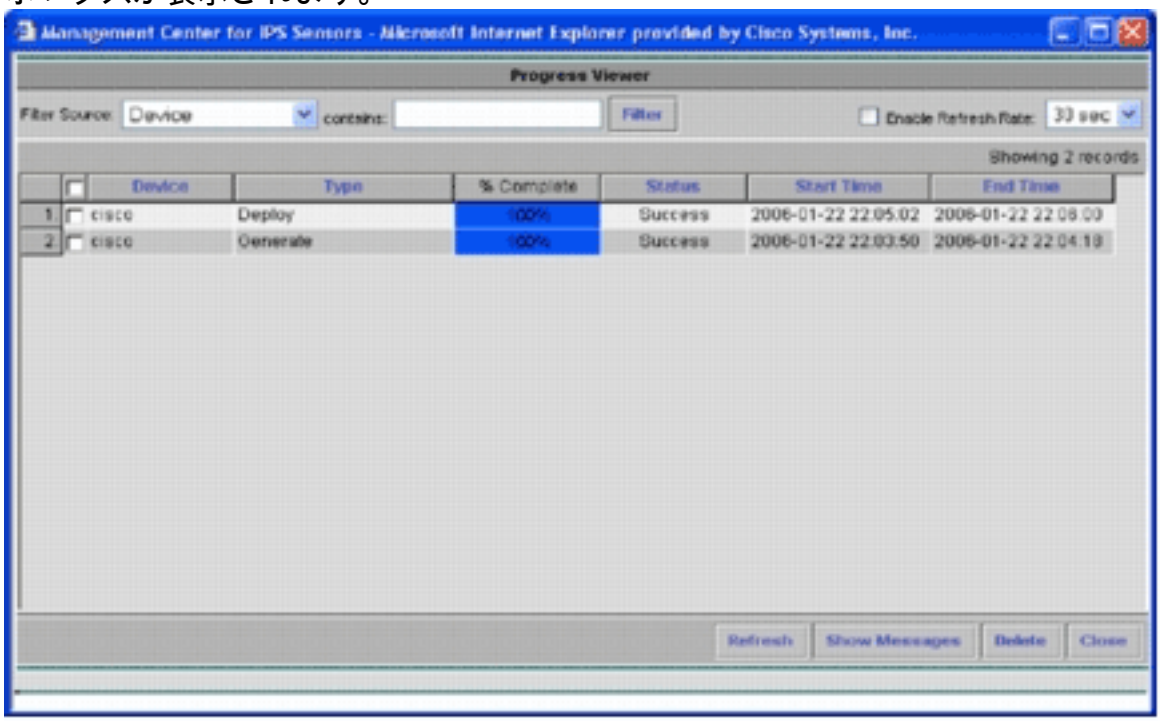
9. *cisco* デバイスに対して行った設定を選択して [Next] をクリックします。[Enter Job Properties] ページが表示されます。



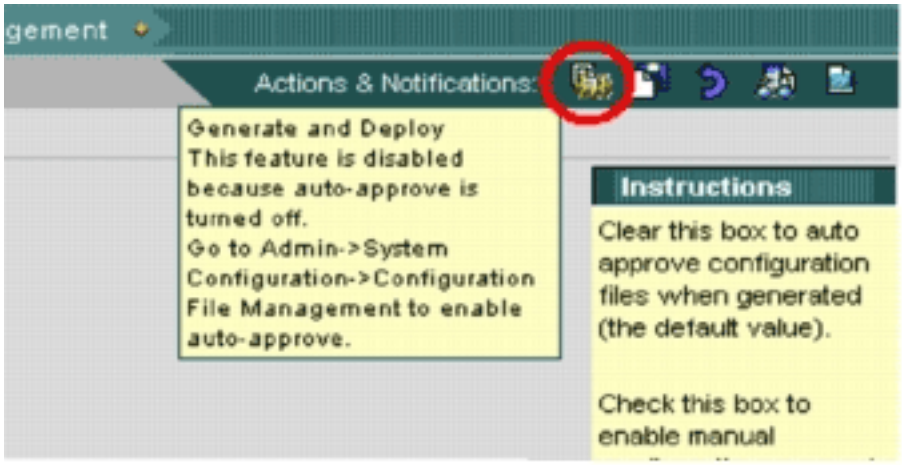
10. 変更を即時に導入するか、または後で導入するようにタスクをスケジュールできます。この例では [Immediate] オプションを選択して [Next] をクリックします。簡単なジョブの要約が表示され、導入可能な状態になります。



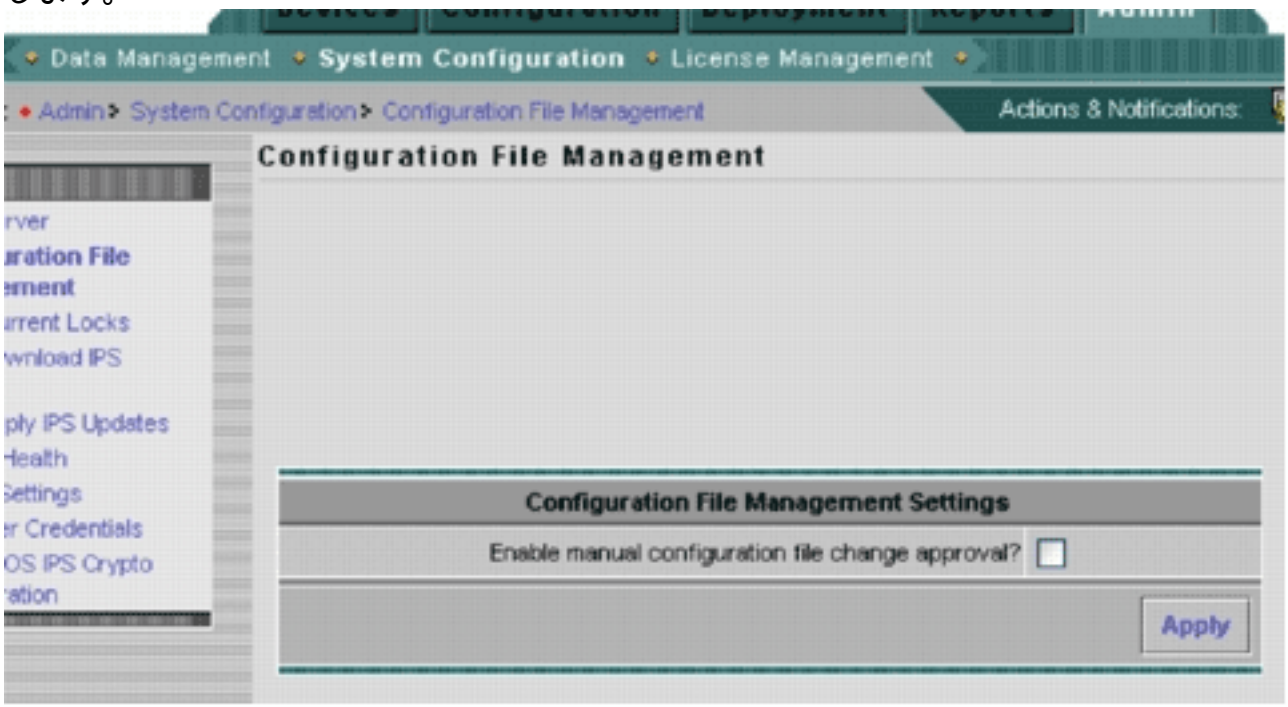
11. [Finish] をクリックします。導入の最後で、導入プロセスのステータスを示すダイアログ ボックスが表示されます。



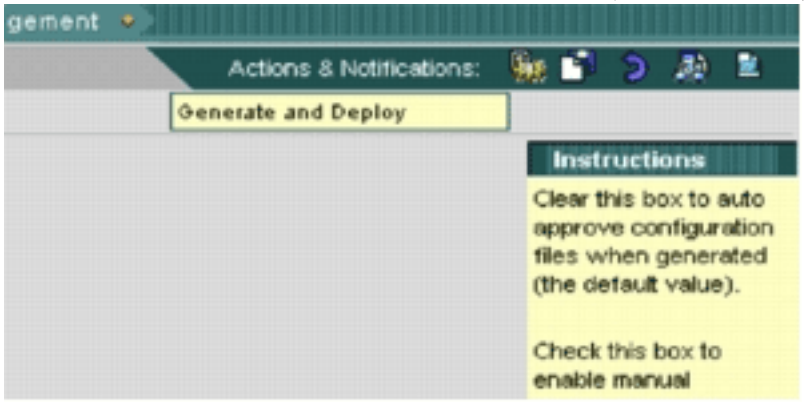
これで Cisco IOS IPS 設定をデバイスに導入できました。複数デバイスを設定する際には、設定変更をグループ レベルで行い、同じグループに属するすべての Cisco IOS IPS ルータに変更を適用できます。**ヒント：**このプロセスは時間がかかりますが、クイック配信機能を使用できます。この機能を使用する場合は、[Generate] > [Approve] > [Deploy] プロセスを実行する必要はありません。この機能を使用するには、次の手順を実行します。ユーザ インターフェイス上部に小さいアイコンが表示される行があります。1 番目のアイコンにカーソルを合わせると、次の図に示すようなツールのヒントが表示されます。



[Generate and Deploy] タスクを有効にするには、[Admin] > [System Configuration] > [Configuration File Management] に移動し、[Enable manual configuration file change approval] チェック ボックスをオフにします。



1 番目のアイコンにカーソルを合わせると、タスクが有効になったことが示されます。



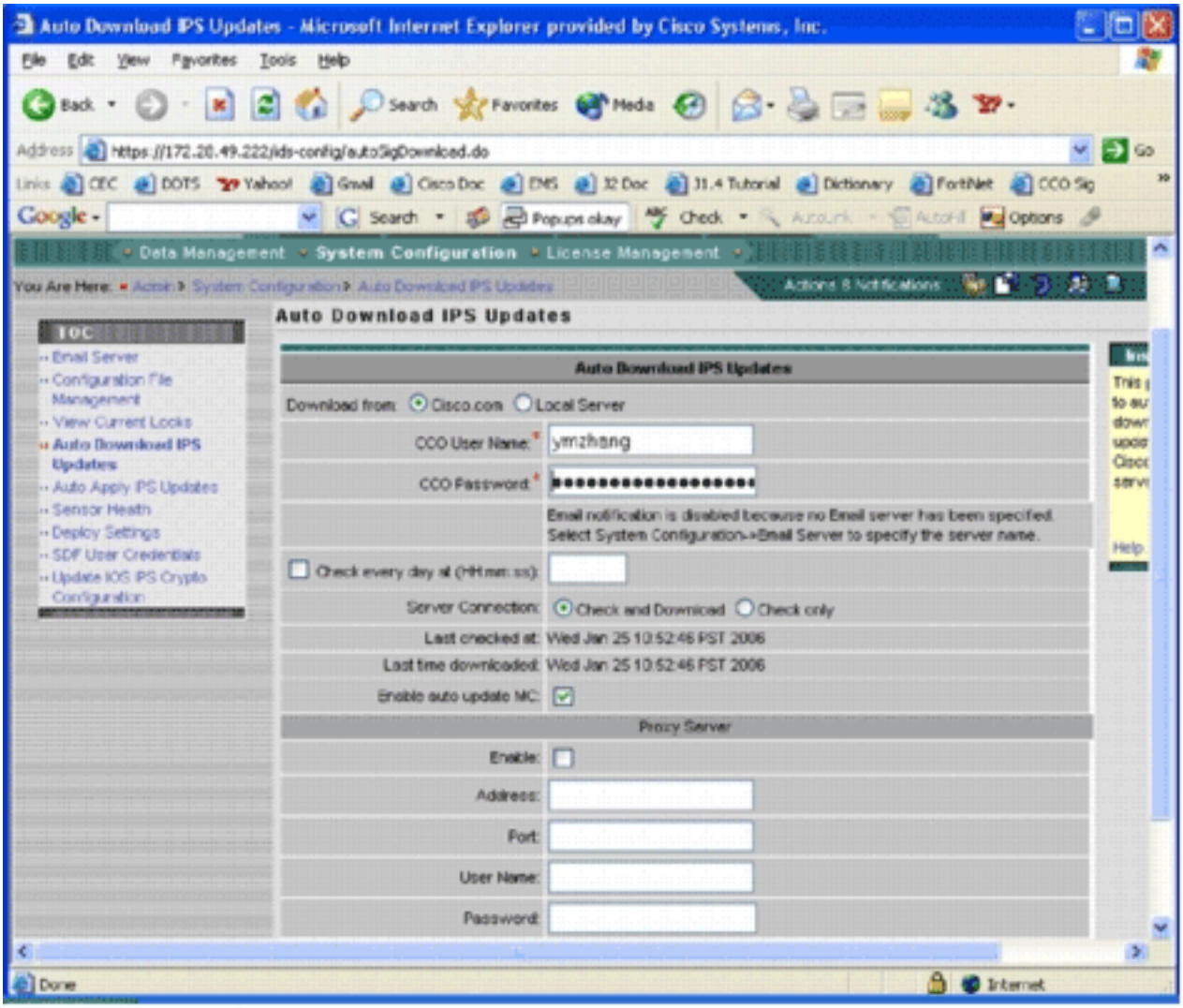
このアイコンをクリックします。IPS MC により設定変更が自動的に生成され、デバイスに導入されます。

シグニチャ更新の自動ダウンロード

IPS MC では、Cisco.com からシグニチャ更新を自動的にダウンロードできます。センサ プラットフォームのシグニチャ更新と Cisco IOS IPS プラットフォームのシグニチャ更新をダウンロードできます。この機能を設定するには、[Admin] > [System Configuration] > [Auto Download IPS

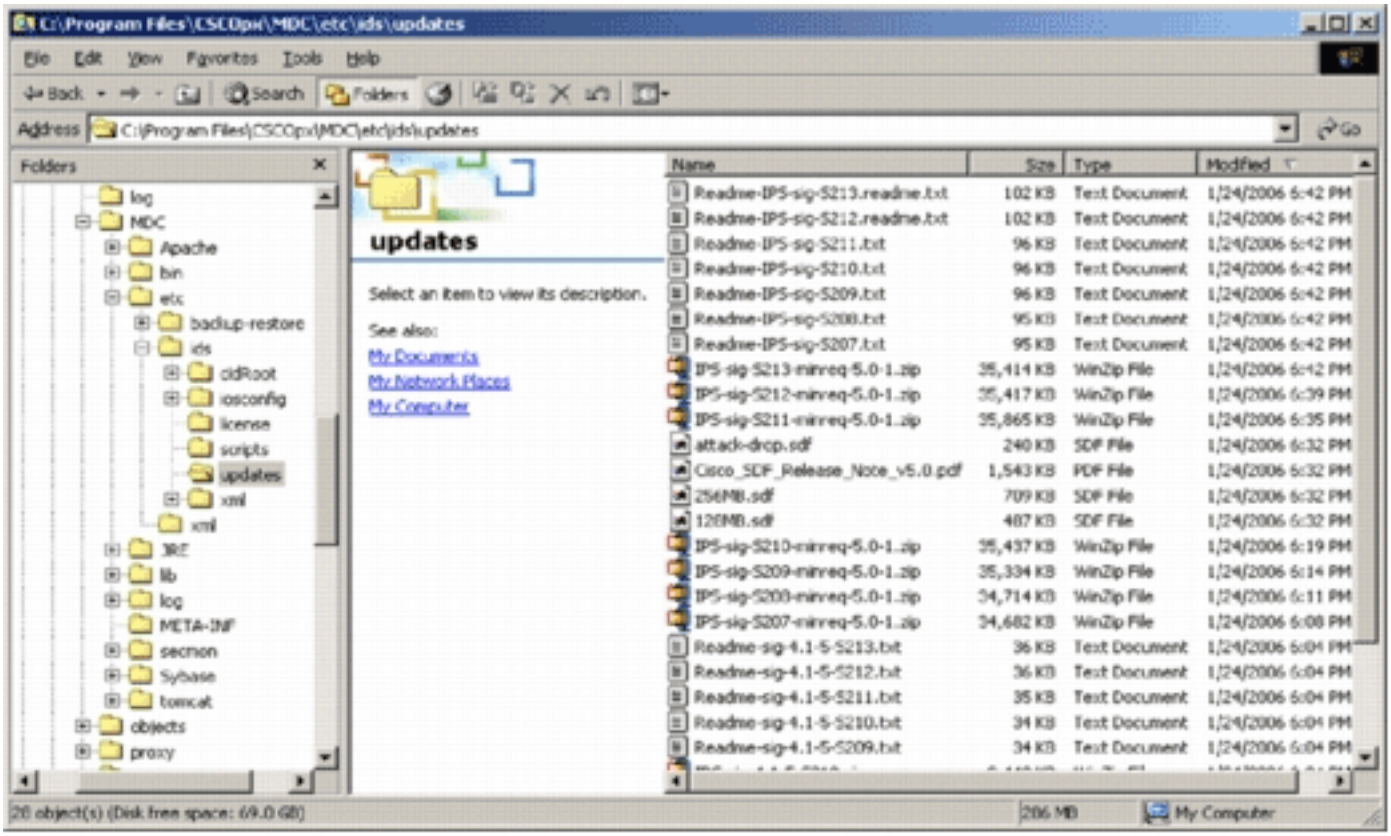
Updates] に移動します。

[Auto Download IPS Update] ページが表示されます。



このシグニチャ更新をダウンロードするには、有効な Cisco.com アカウントが必要です。自動ダウンロードしたファイルを確認するため、IPS MC インストール ホーム ディレクトリに移動します。デフォルトではこれは \program files\CSCOpx\MDC\etc\ids\updates です。

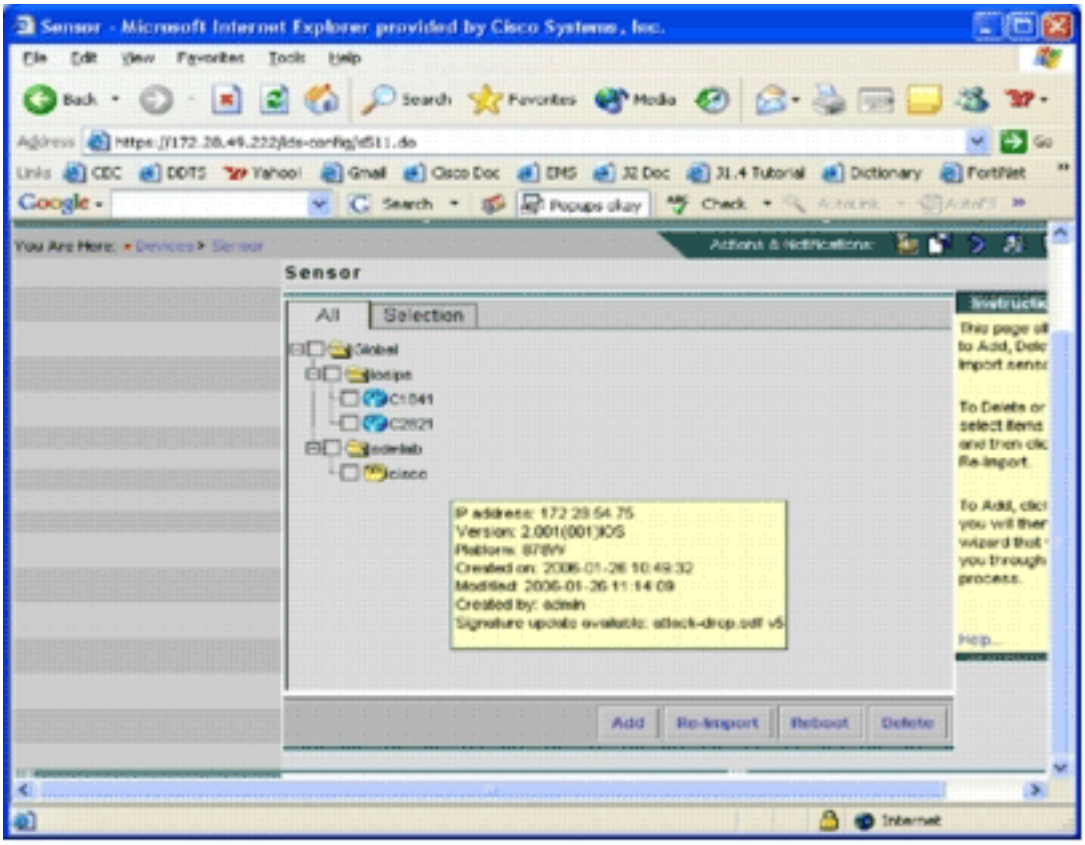
次の画像は、このディレクトリ内のダウンロード ファイルを示します。

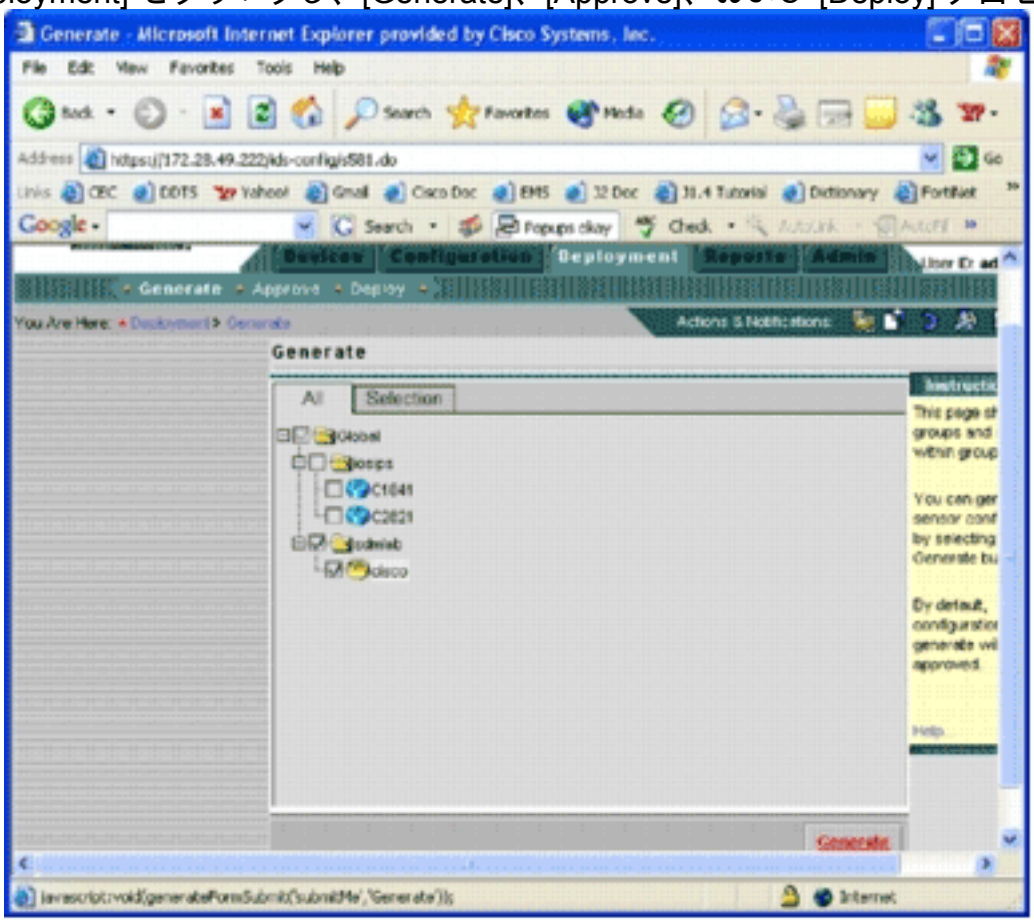


センサ更新ファイルがあることがわかります。Cisco IOS ソフトウェア更新ファイルと事前調整 SDF ファイルがダウンロードされました。

新しい SDF ファイルを使用した Cisco IOS IPS ルータの更新

事前調整 SDF ファイルが導入されている Cisco IOS IPS ルータでは、自動ダウンロードで新しいバージョンの SDF ファイルが使用可能になるか、または updates ディレクトリにコピーされるとただちに、Cisco IPS MC が新しいバージョンを認識します。ユーザ インターフェイスの更新後に、適用可能なデバイスのデバイス アイコンが黄色になります。



1. [Deployment] をクリックし、[Generate]、[Approve]、および [Deploy] プロセスを実行しま


す。
2. 導入が正常に完了すると、Cisco IOS IPS ルータは新しいバージョンの SDF ファイルを使用します。

関連情報

- Cisco Intrusion Prevention System