Konfigurationsbeispiel für CiscoWorks IPS MC in Cisco IOS IPS

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Konfigurieren
Grundlegendes Verständnis von Konfigurationsaufgaben
Erstkonfiguration von Cisco IOS IPS Routern
Importieren eines Cisco IOS IPS-Routers in einen IPS MC
Konfigurieren des Cisco IOS IPS-Routers für die Verwendung vorkonfigurierter Signaturdateien
Ändern von vordefinierten SDF-Signaturen
Benutzerdefinierte Signaturen auswählen
Erstellen einer Regel für die Schnittstelle(n)
Bereitstellung der Konfiguration
Signatur-Updates automatisch herunterladen
Aktualisieren des Cisco IOS IPS-Routers mit neuen SDF-Dateien
Zugehörige Informationen

Einführung

Das CiscoWorks Management Center für IPS-Sensoren (IPS MC) ist die Managementkonsole für Cisco IPS-Geräte. IPS MC Version 2.2 unterstützt die Bereitstellung der IPS-Funktion (Intrusion Prevention System) auf Cisco IOS® Software-Routern. Dieses Dokument beschreibt die Verwendung von IPS MC 2.2 zum Konfigurieren von Cisco IOS IPS.

Weitere Informationen zur Verwendung von IPS MC (einschließlich der Konfiguration von Geräten, die nicht auf der Cisco IOS Software basieren) finden Sie in der Dokumentation zu CiscoWorks Management Center for IPS Sensors unter der URL:

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

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf CiscoWorks Management Center for IPS Sensors (IPS MC) Version 2.2.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

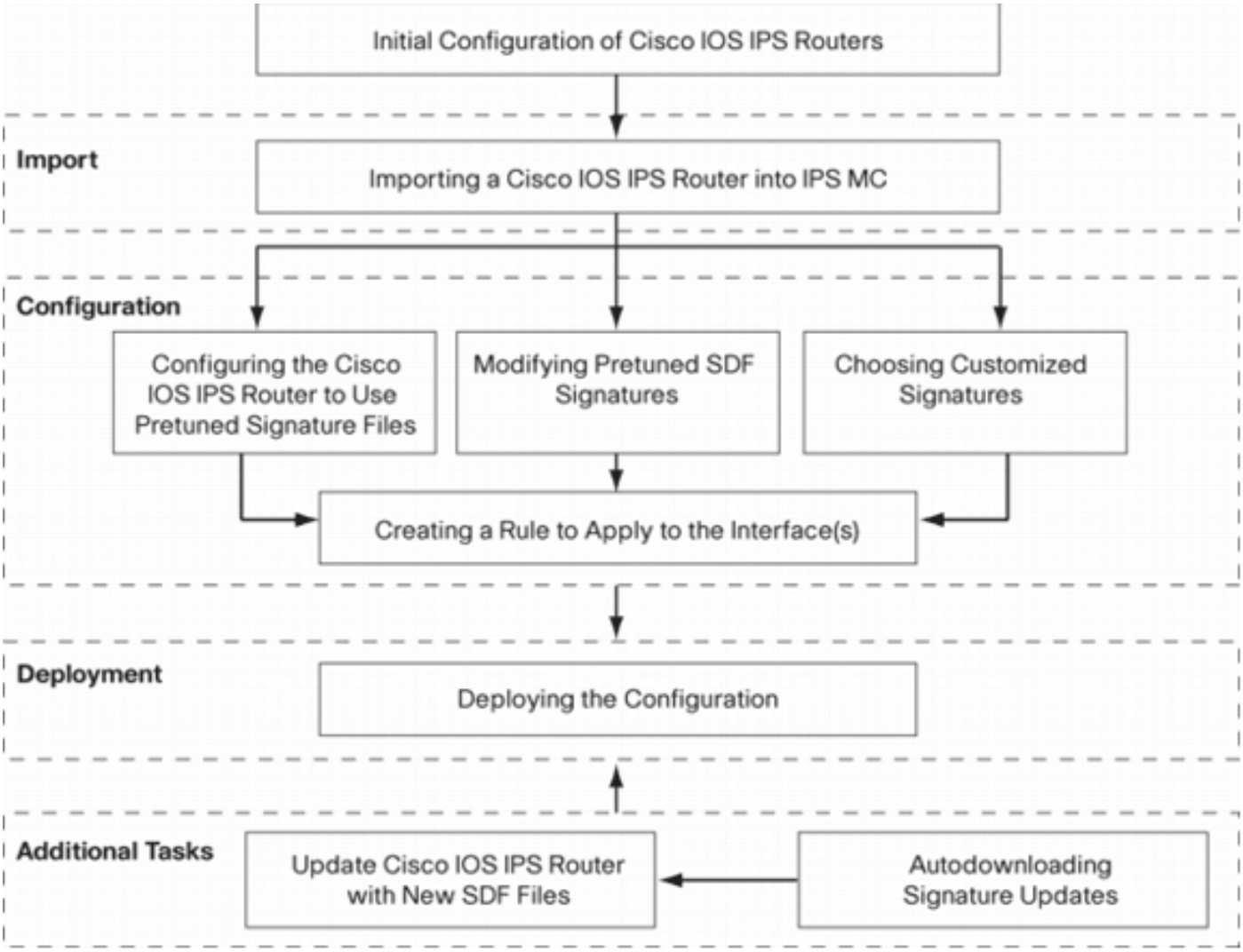
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

Grundlegendes Verständnis von Konfigurationsaufgaben

IPS MC wird zur Verwaltung der Konfiguration einer Gruppe von Cisco IOS IPS-Routern verwendet. Beachten Sie, dass IPS MC die Warnmeldungen von Routern, die IPS ausführen, nicht verwaltet. Cisco empfiehlt das Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) für die IPS-Überwachung. Das Konfigurationsmanagement besteht aus einer Reihe von Aufgaben, die in diesem Dokument beschrieben werden. Diese Aufgaben können in drei Phasen unterteilt werden: Importieren, Konfigurieren und Bereitstellen wie in diesem Bild gezeigt.



Jede Phase hat eigene Verantwortlichkeiten und Aufgaben:

- *Import* - Einen Router in IPS MC importieren. Sie müssen einen Router in IPS MC importieren, bevor Sie ihn mit IPS MC konfigurieren können. Ein Router kann nur importiert werden, wenn auf dem Router eine erste IPS-Konfiguration vorhanden ist (Details hierzu finden Sie weiter unten in diesem Dokument).
- *Konfiguration* - Konfigurieren Sie das Gerät. Sie können beispielsweise einen Cisco IOS IPS-Router so konfigurieren, dass er eine der von Cisco empfohlenen vordefinierten Signaturdateien verwendet. Konfigurationsänderungen werden im IPS MC gespeichert, aber in dieser Phase nicht an den Router gesendet.
- *Bereitstellung* - Konfigurationsänderungen werden am Gerät vorgenommen. In dieser Phase verpflichten Sie sich, die bei Konfigurationsaufgaben vorgenommenen Änderungen an die Router zu übertragen.
- *Zusätzliche Aufgaben* - IPS MC bietet eine Funktion zum automatischen Herunterladen von Signatur-Updates von Cisco.com.

Sie müssen diesen schrittweisen Ansatz verstehen, um IPS MC effektiv nutzen zu können. Sie unterscheidet sich von gerätebasierten Verwaltungs-GUIs, z. B. Cisco Router und Security Device Manager (SDM). Gerätebasierte GUIs agieren direkt auf einem einzelnen Router, während IPS MC für die netzwerkweite Nutzung von Routergruppen (und anderen IPS-Geräten wie Cisco IPS Sensoren der Serie 4200) entwickelt wurde.

Dieses Dokument enthält Informationen zu den einzelnen Aufgaben im Diagramm, die Sie bei der Verwaltung von Cisco IOS IPS-Routern mithilfe von IPS MC unterstützen.

Erstkonfiguration von Cisco IOS IPS Routern

Um einen Cisco IOS IPS-Router erfolgreich zu importieren oder dem IPS MC hinzuzufügen, müssen Sie bestimmte Schritte zur Erstkonfiguration auf den Cisco IOS IPS-Routern ausführen. In diesem Abschnitt werden diese Schritte beschrieben.

Sie müssen Secure Shell (SSH) Protocol in einem Cisco IOS IPS-Router für die Konfiguration, den Import und die Bereitstellung über Cisco IPS MC aktivieren. Darüber hinaus muss das Security Device Event Exchange (SDEE)-Protokoll für Ereignisberichte aktiviert werden (obwohl diese Warnungen nicht an IPS MC gesendet werden, da IPS MC nur für die Bereitstellung, nicht für die Berichterstellung verwendet wird). Schließlich müssen Sie sicherstellen, dass die Uhreneinstellung auf dem IPS-Router mit dem IPS MC synchronisiert wird.

Gehen Sie wie folgt vor, um Ihre IOS IPS-Router zu konfigurieren:

1. Erstellen Sie einen lokalen Benutzernamen und ein lokales Kennwort für den Router.
```
Router#config terminal
Router(config)#username <username> password <password>
```

2. Aktivieren Sie die lokale Anmeldung auf der VTY-Leitungsschnittstelle.
```
Router#config terminal
Router(config)#line vty 0 15
Router(config-line)#login local
Router(config-line)#exit
```

   Wenn die CLI (Transport Input/Transport Output Command Line Interface) unter der VTY-Leitungskonfiguration konfiguriert ist, stellen Sie sicher, dass SSH aktiviert ist. Beispiel:
```
Router#conf terminal
Router(config)#line vty 0 15
Router(config-line)#transport input ssh telnet
Router(config-line)#exit
```

3. Generieren Sie einen 1024-Bit-RSA-Schlüssel (falls noch kein Schlüssel vorhanden ist).SSH wird nach der Generierung von Verschlüsselungsschlüsseln automatisch aktiviert.
```
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. Aktivieren Sie SDEE auf dem Router.
```
Router(config)#ip ips notify sdee
```

5. Aktivieren Sie HTTPS.HTTP oder HTTPS ist erforderlich, damit IPS MC mit dem Router mit SDEE kommunizieren kann, um Ereignisinformationen zu erfassen.
```
Router(config)#ip http authentication local
Router(config)#ip http secure-server
```

6. Verwenden Sie den externen NTP-Server (Network Time Protocol) oder den Befehl clock,

um die Uhreneinstellung auf dem IPS-Router zu konfigurieren.

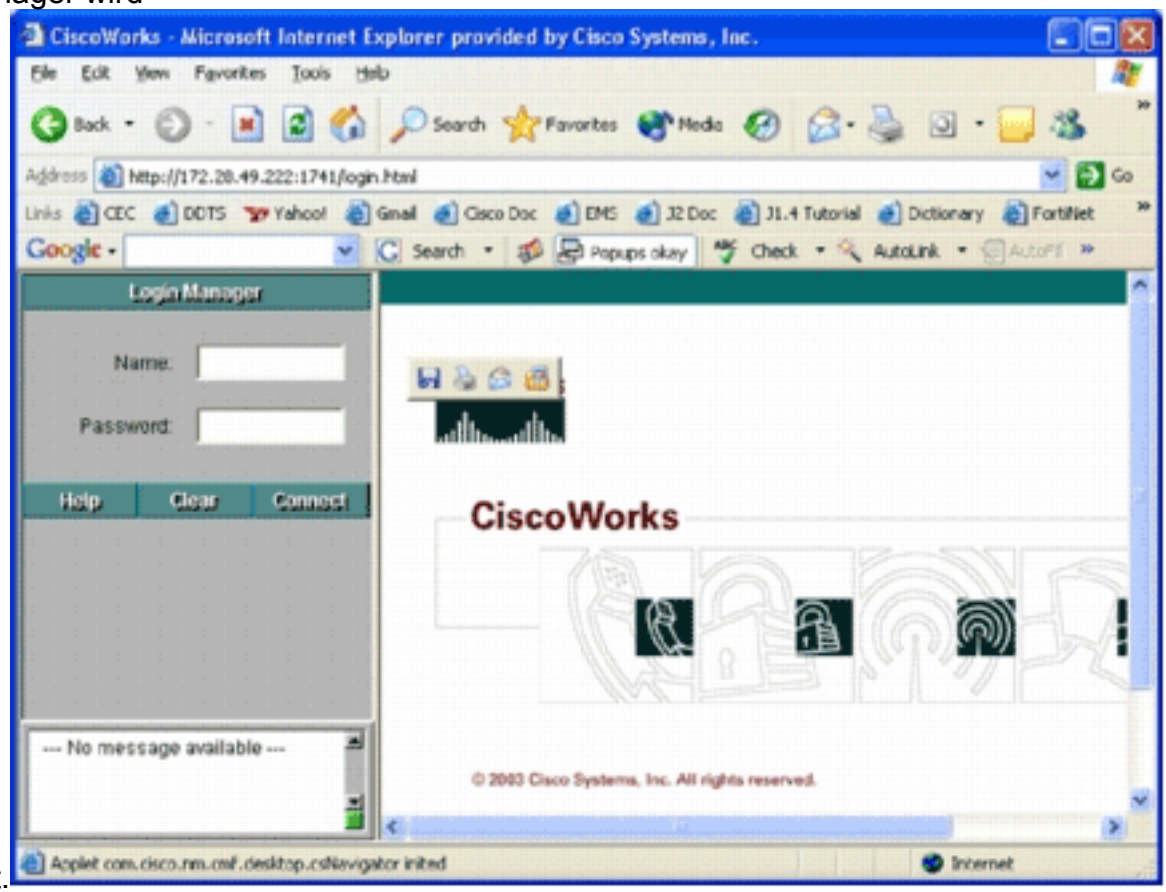
```
Router(config)#clock set hh:mm:ss day month year
```

Jetzt ist der Cisco IOS IPS-Router bereit und kann für weitere Konfigurations- und Verwaltungszwecke in das IPS-MC importiert werden.

Importieren eines Cisco IOS IPS-Routers in einen IPS MC

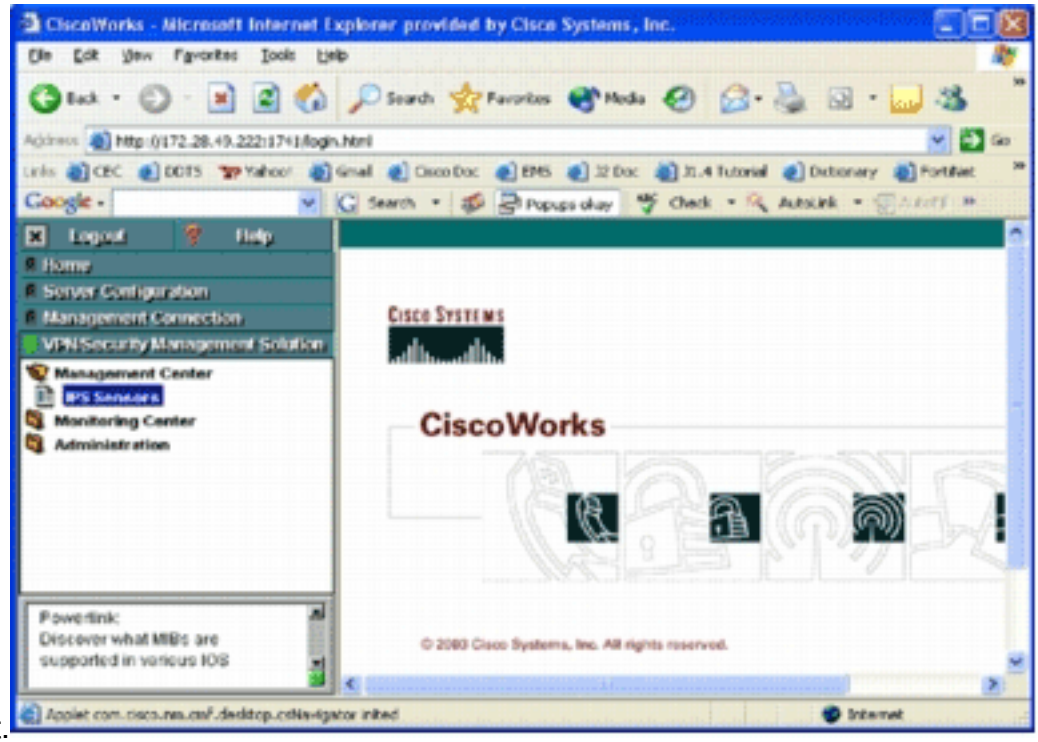
Wenn Sie die Erstkonfiguration des Routers abgeschlossen haben, können Sie diese dem IPS MC hinzufügen (oder in dieses importieren).

1. Starten Sie den Webbrowser, und zeigen Sie auf den CiscoWorks-Server.Der CiscoWorks Login Manager wird angezeigt.



Hinweis: Die Standard-Portnummer des Webservers ist 1741. Daher sollten Sie eine URL verwenden, die ähnlich wie http://<*Server-IP-Adresse*>:1741/ ist.

2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein, um sich anzumelden.Die Hauptseite von CiscoWorks wird



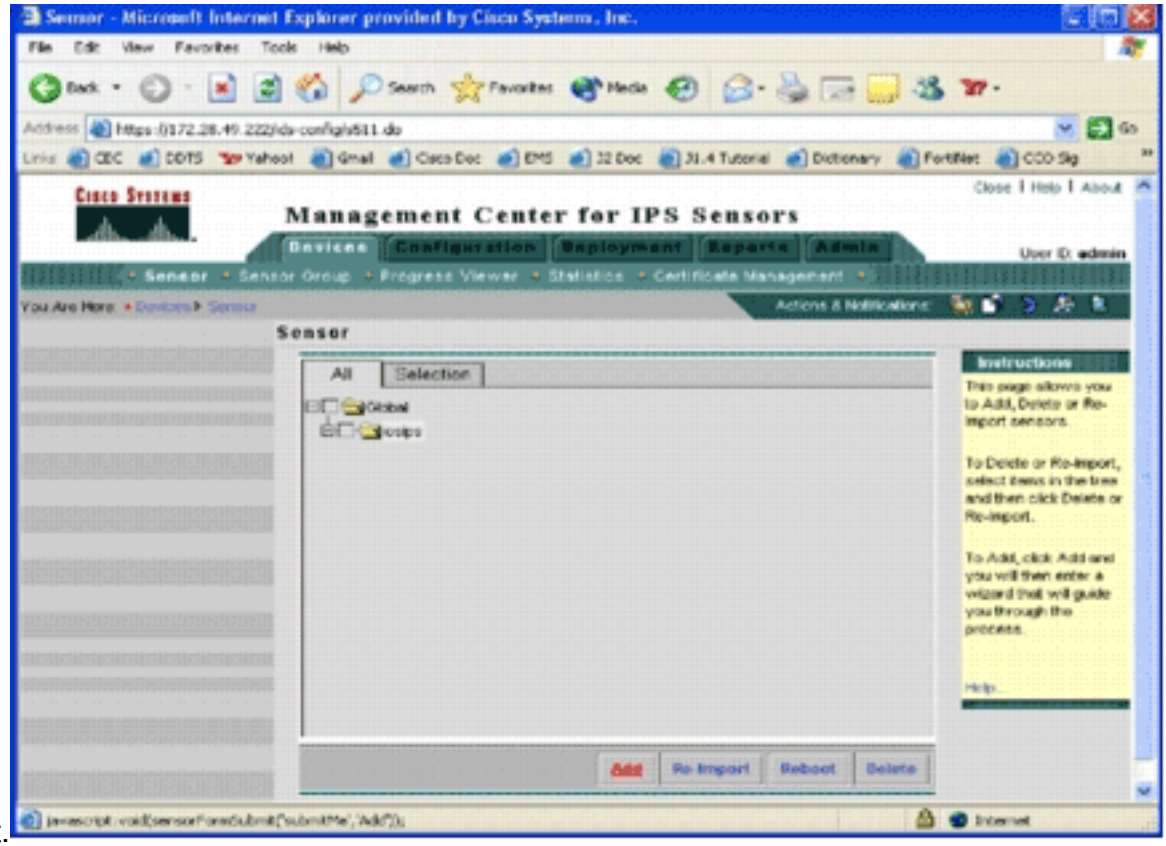
angezeigt.

3. Wählen Sie im linken Navigationsbereich die Option **VPN/Security Management Solution** (VPN/Sicherheitsmanagement-Lösung) aus, und wählen Sie dann **Management Center** aus.Die Seite Management Center for IPS Sensors (Management Center für IPS-Sensoren) wird

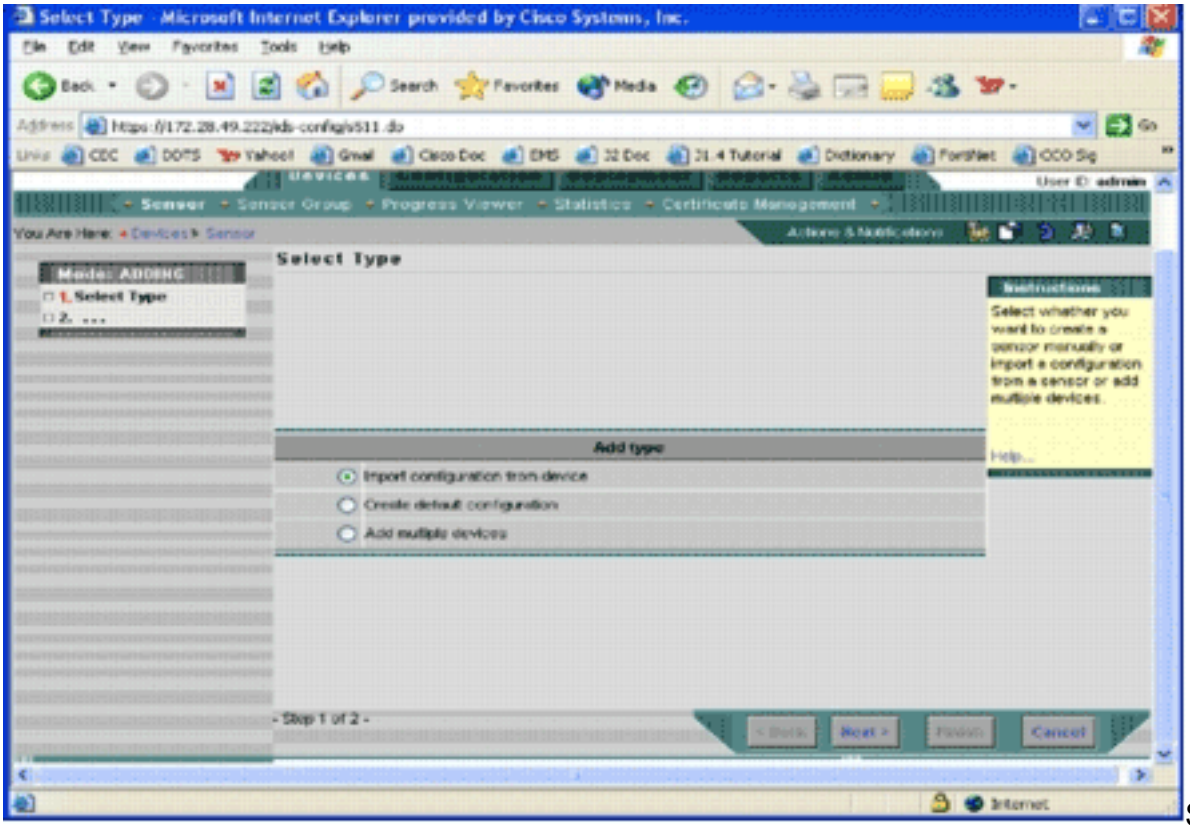
angezeigt.Au f dieser Seite werden die folgenden fünf Registerkarten angezeigt:*Geräte*: Auf der Registerkarte "Geräte" können Sie die Ersteinrichtung und Verwaltung aller Geräte im System durchführen.*Konfiguration* - Auf der Registerkarte "Konfiguration" können Sie Bereitstellungsfunktionen ausführen. Sie können Geräte auf individueller Geräteebene oder auf Gruppenebene konfigurieren. Eine Gerätegruppe kann mehrere Geräte enthalten. Alle durch Konfigurationsaufgaben vorgenommenen Änderungen müssen gespeichert werden. Die Konfigurationsfunktion nimmt nicht sofort Änderungen an den Geräten vor. Sie müssen

die Bereitstellungsfunktion verwenden, um die Änderungen bereitzustellen.*Bereitstellung*: Auf der Registerkarte "Bereitstellung" können Sie Konfigurationsänderungen auf Geräten bereitstellen. Die Funktion "Zeitplan" bietet eine flexible Kontrolle darüber, wann die Konfigurationsänderungen wirksam werden sollen.*Berichte*: Auf der Registerkarte "Berichte" können Sie verschiedene Berichte zum Systembetrieb erstellen.*Admin*: Auf der Registerkarte Admin können Sie Systemverwaltungsaufgaben wie Datenbankverwaltung, Systemkonfiguration und Lizenzverwaltung ausführen.

4. Klicken Sie auf die Registerkarte **Geräte**, um ein neues Gerät hinzuzufügen.Die Seite "Sensor" wird angezeigt.

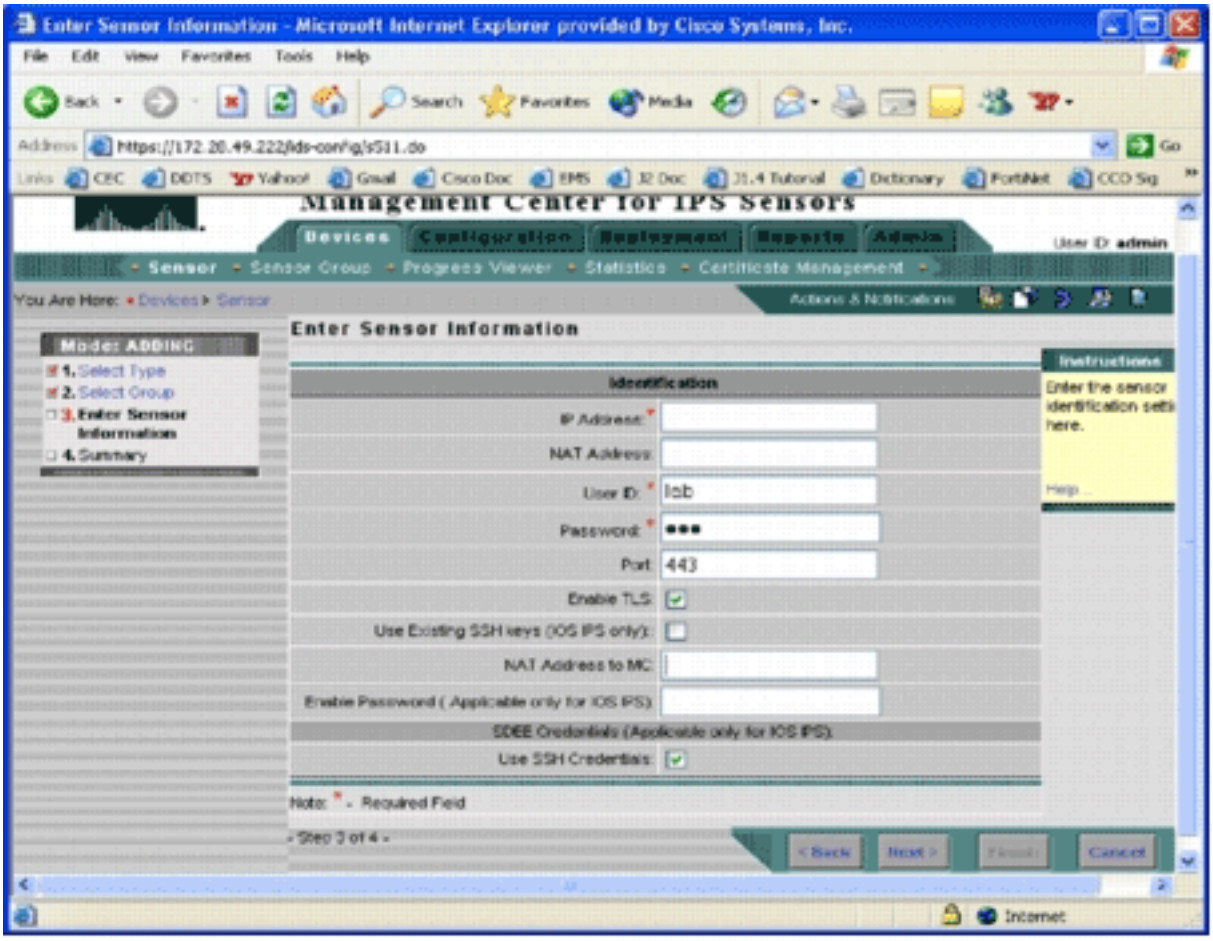


5. Klicken Sie auf **Hinzufügen**.Die Seite "Typ auswählen" wird angezeigt.



Sie müssen IPS MC darüber informieren, welche Funktion Sie ausführen möchten. In dieser Liste werden die einzelnen Optionen beschrieben:*Konfiguration vom Gerät importieren* - Verwenden Sie diese Option, um IPS MC-Geräten hinzuzufügen, die derzeit im Netzwerk ausgeführt werden.*Standardkonfiguration erstellen* - Verwenden Sie diese Option, um Geräte hinzuzufügen, die noch nicht im Netzwerk ausgeführt werden.*Mehrere Geräte hinzufügen* - Verwenden Sie diese Option, um mehrere Geräte hinzuzufügen. Sie können eine CSV- oder XML-Datei erstellen, die alle Geräteinformationen enthält, und diese anschließend in IPS MC importieren, um die Geräte gleichzeitig hinzuzufügen.**Tipp:** Die Beispieldateien im CSV-Format und XML-Format befinden sich in: InstallDirectory\MDC\etc\ids\ and are named MultipleAddDevices-format.csv bzw. MultipleAddDevices-format.xml.

6. Wählen Sie die entsprechende Option Add type (Typ hinzufügen) aus, und klicken Sie auf **Next (Weiter)**.
7. Wählen Sie die Gruppe aus, der Sie den Cisco IOS IPS-Router hinzufügen möchten, oder verwenden Sie die globale Standardgruppe, und klicken Sie dann auf **Weiter**.Die Seite "Sensor Information" (Sensorinformationen eingeben) wird angezeigt.



8. Geben Sie auf der Seite Identifikation die Identifikationsdaten für das Gerät ein.**Hinweis:** Wenn der Benutzer über keine Zugriffsrechte der Berechtigungsebene 15 verfügt, müssen Sie das enable-Kennwort angeben. Aktivieren Sie in der letzten Zeile der Identifizierungsseite das Kontrollkästchen **SSH-Anmeldeinformationen verwenden**.
9. Klicken Sie auf **Weiter**.Die Add Sensor Summary (Sensorübersicht hinzufügen) wird angezeigt.
10. Klicken Sie auf **Fertig stellen**.Das Gerät wurde erfolgreich zum IPS MC hinzugefügt.**Hinweis:** Wenn während des Importvorgangs Fehler auftreten, aktivieren Sie die folgenden Optionen:*Erforderliche Konfiguration* - Diese Konfigurationen sind für die Kommunikation zwischen IPS MC und Cisco IOS IPS-Routern erforderlich.*Konnektivität* - Stellen Sie sicher, dass IPS MC die Cisco IOS IPS-Router erreichen kann.*Clock*: Überprüfen Sie die Zeiten auf dem IPS MC und dem Cisco IOS IPS-Router. Die Uhrzeit ist eine kritische Komponente des HTTPS-Zertifikats, die für die Authentifizierung verwendet wird. Die Zeiten müssen innerhalb von 12 Stunden voneinander liegen. (Best Practice ist höchstens ein paar Stunden.)*Cisco IOS IPS-Zertifikat* - Manchmal ist das gespeicherte Cisco IOS IPS-Zertifikat falsch. Um ein Zertifikat aus Cisco IOS IPS zu löschen, müssen Sie den Trustpoint aus dem Cisco IOS IPS-Router entfernen.*Zusätzliche Konfiguration*: Wenn die **ip http timeout-Richtlinie** mit einer geringen Anzahl von Maximalanforderungen konfiguriert ist, wie **ip http timeout-policy idle 600 life 86400 anforderungen 1**, müssen Sie die maximale Anfragenummer erhöhen. Beispiel: **ip http timeout-policy idle 600 life 86400 Requests 8400**

Konfigurieren des Cisco IOS IPS-Routers für die Verwendung vorkonfigurierter Signaturdateien

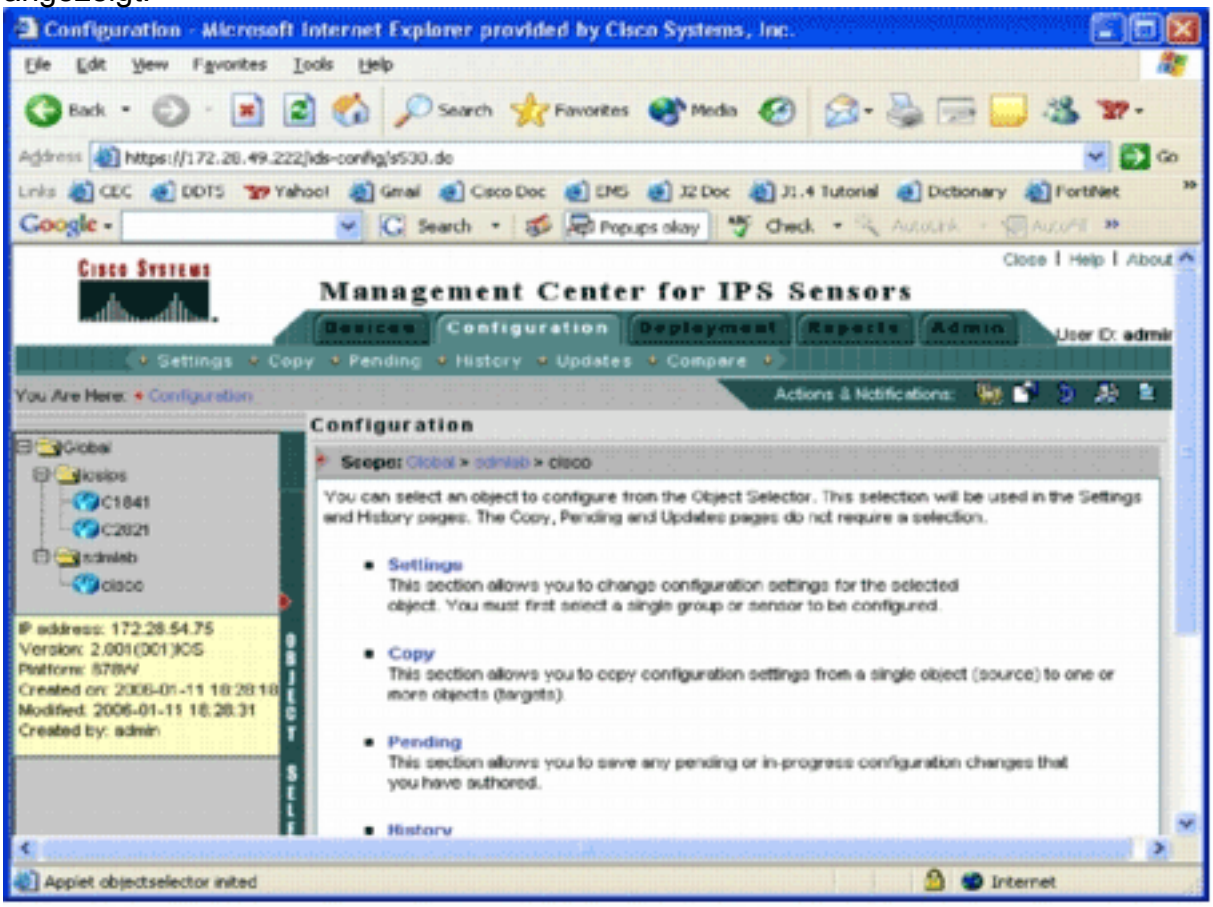
Nachdem Sie den Router in das IPS MC importiert haben, müssen Sie die Signature Definition

File (SDF) (eine textbasierte Datei, die die vom IPS-Router verwendeten Bedrohungssignaturen enthält) und die Aktion auswählen, die beim Auslösen jeder Signatur zu ergreifen ist (z. B. Drop, TCP Reset, Alarm).

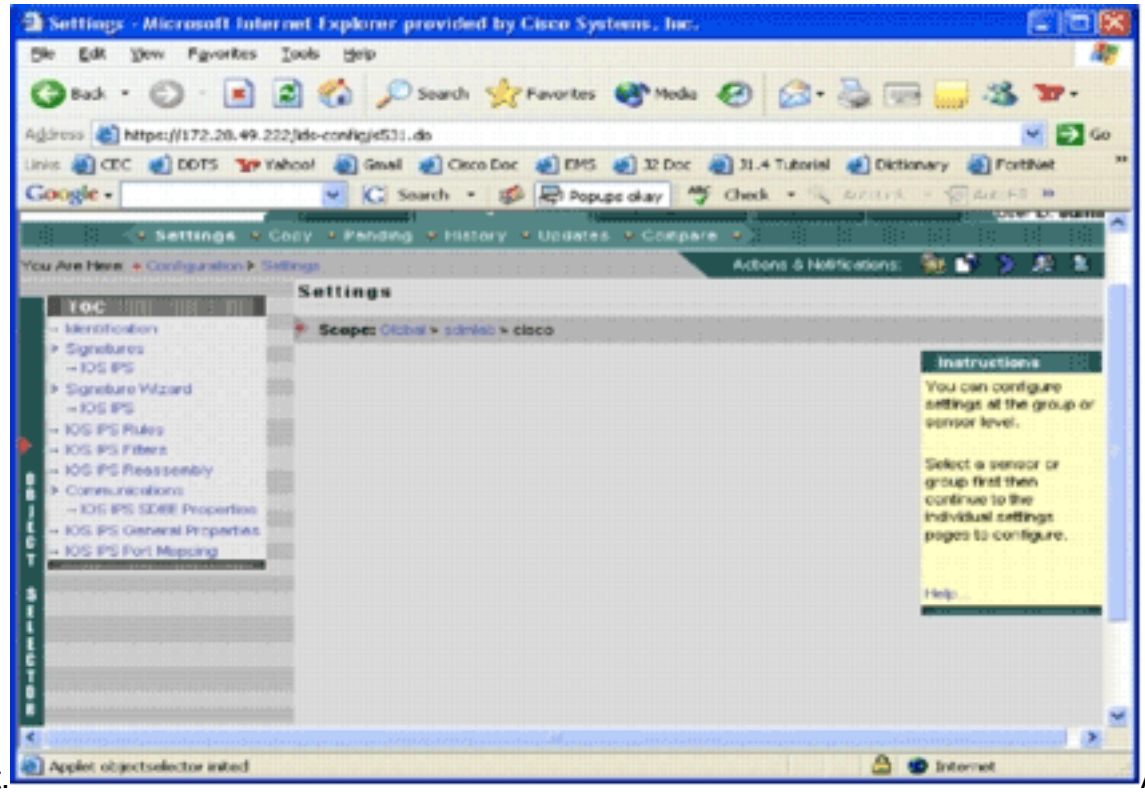
Cisco Systems® empfiehlt, vordefinierte SDF-Dateien von Cisco zu verwenden. Derzeit gibt es drei solcher Dateien: attack-drop.sdf, 128 MB.sdf und 256 MB.sdf. IPS MC kann diese Dateien automatisch von Cisco.com herunterladen. Weitere Informationen finden Sie unter Automatische Signaturaktualisierungen herunterladen.

Bei diesem Verfahren wird ein einzelnes Gerät als Beispiel verwendet, und es beginnt ein Router ohne IPS-Konfiguration. Sie können dieses Verfahren auch für mehrere Geräte auf Gruppenebene verwenden.

1. Klicken Sie auf die Registerkarte **Konfiguration**.Die Seite "Konfiguration" wird angezeigt.

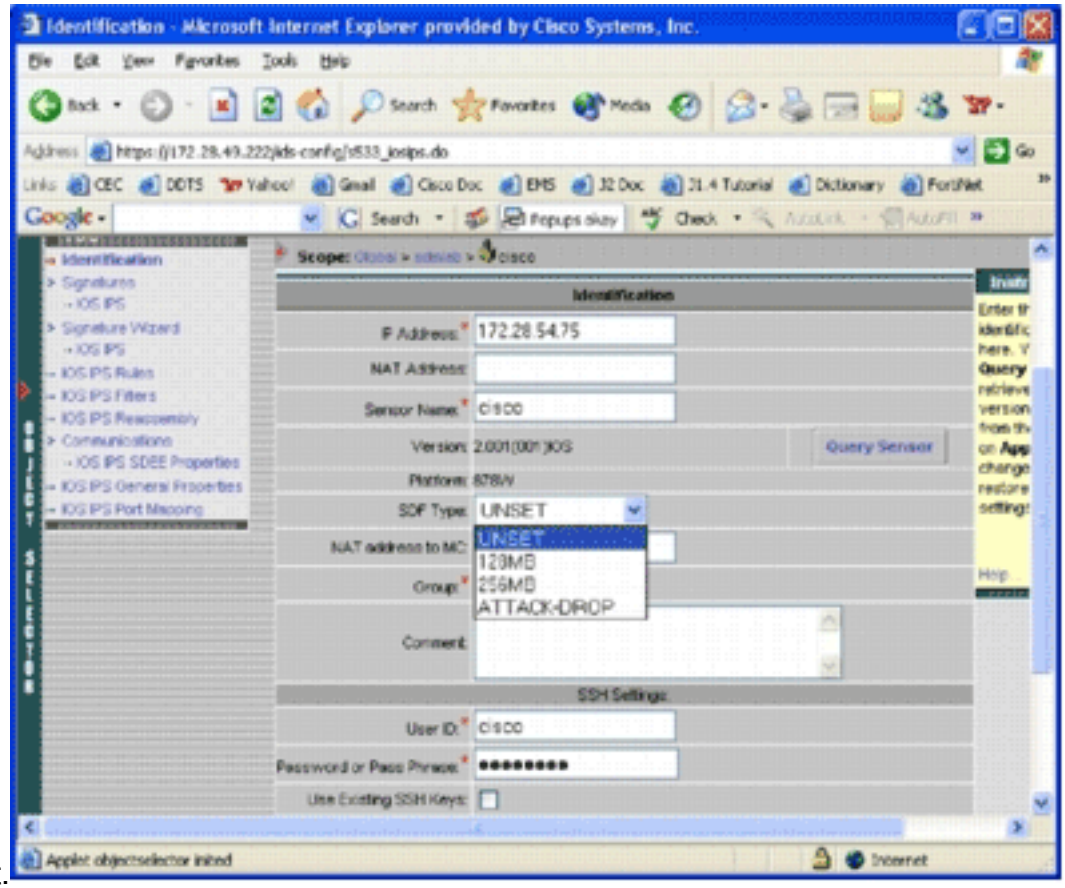


2. Wählen Sie in der Objektauswahl links auf der Seite den Cisco IOS IPS-Router aus, den Sie konfigurieren möchten.**Hinweis:** Die meisten Konfigurationseinstellungen in IPS MC 2.2 können sowohl auf Gruppen- als auch auf Geräteebene konfiguriert werden. Beispielsweise sind die globalen, die iosips-und die sdmlab-Gruppen alle konfigurierbare Objektgruppen. In diesem Beispiel wird ein einzelnes Gerät (cisco) der sdmlab-Gruppe verwendet.Sobald Sie den zu konfigurierenden Router ausgewählt haben, zeigt die Pfadleiste oben auf der Konfigurationsseite den aktuellen Konfigurationsbereich an. Der Bereich für dieses Beispiel ist beispielsweise *Global > sdmlab > cisco*. *cisco* ist das aktuelle Konfigurationsobjekt (d. h. der Router, der aus dem Objektauswahl-Fenster ausgewählt wurde.
3. Klicken Sie in der Menüleiste Konfiguration auf **Einstellungen**.Die Seite Einstellungen wird



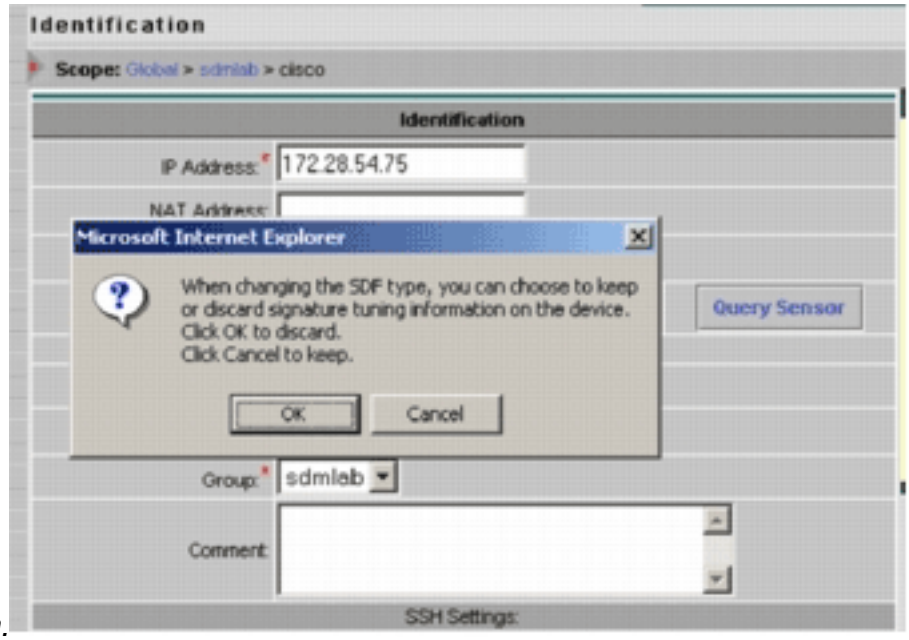
angezeigt.Auf der Seite Einstellungen können Sie die Konfigurationseinstellungen für das ausgewählte Objekt ändern. Die für Cisco IOS IPS-Router spezifischen Konfigurationseinstellungen finden Sie im Abschnitt "Nutzungsbedingungen" auf der linken Seite. Im TOC-Abschnitt sind folgende Aufgaben verfügbar:*Identifikation* - grundlegende Informationen zum Cisco IOS IPS-Router Hier können Sie eine vordefinierte SDF-Datei angeben.*Signatur* - Cisco IOS IPS-Router-Signaturen*Signaturassistent* - Signaturassistent zum Hinzufügen benutzerdefinierter Signaturen*Cisco IOS IPS-Regeln* - Zum Konfigurieren von Cisco IOS IPS-Regeln, die für Schnittstellen verwendet werden*Cisco IOS IPS-Filter* - Cisco IOS IPS-Filter*Cisco IOS IPS Reassembly* - Konfiguration der virtuellen IP-Reassemblierung der Schnittstelle*Cisco IOS IPS SDEE-Eigenschaften* - Zum Konfigurieren der SDEE-Einstellungen*Allgemeine Eigenschaften von Cisco IOS IPS* - zusätzliche Konfigurationen im Zusammenhang mit Cisco IOS IPS

4. Wählen Sie **Identification**, um vordefinierte SDF-Dateien zu konfigurieren.Die Identifizierungsseite wird

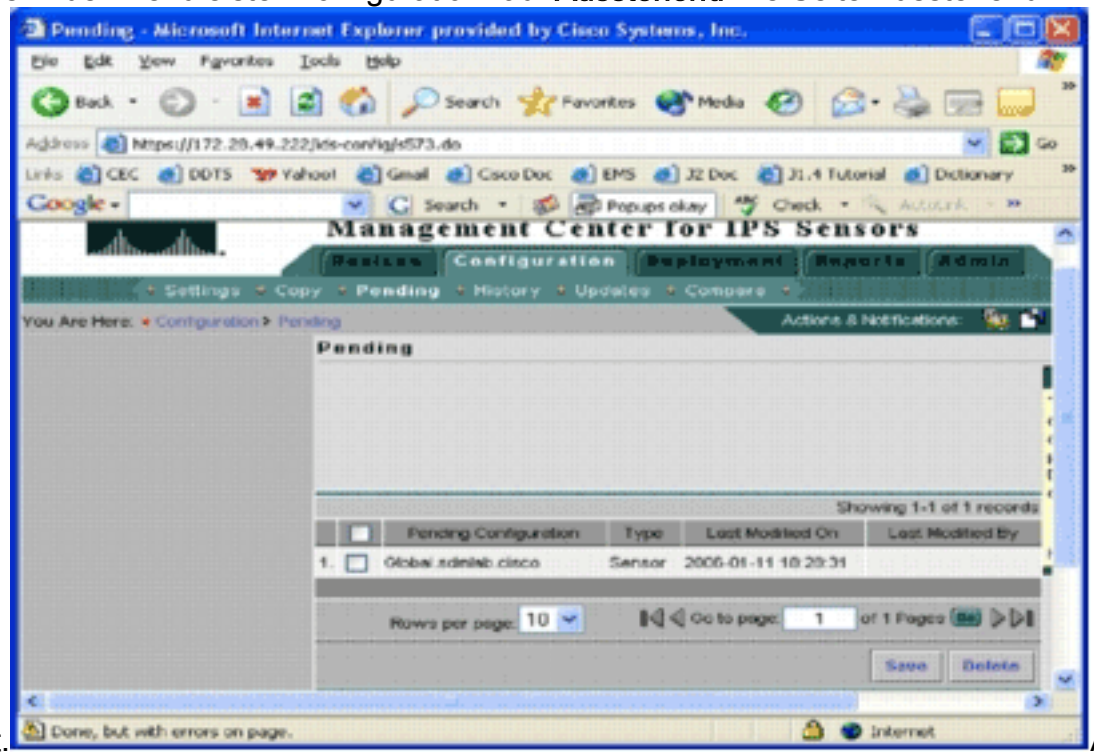


angezeigt.

5. Wählen Sie in der Dropdown-Liste "SDF-Typ" die entsprechende vordefinierte SDF aus, und klicken Sie dann auf **Apply (Übernehmen)**, um die Änderungen anzuwenden.Das Cisco IOS IPS unterstützt mehr als 1.600 Signaturen, was über die Speicherkapazität der Router hinausgeht. Die SDFs wurden als praktische Methode entwickelt, um die wichtigsten Signaturen auszuwählen und zu laden. Derzeit können Sie aus drei SDFs wählen. Sie variieren in ihrer Größe, damit Sie eine SDF-Datei entsprechend der DRAM-Kapazität Ihrer Router auswählen können. Die verfügbaren Optionen werden hier beschrieben:UNSET - Der SDF-Typ ist nicht festgelegt.ATTACK-DROP: Dieses SDF ist für Router mit 64 MB DRAM geeignet.256 MB - Dieses SDF ist für Router mit 256 MB DRAM geeignet.128 MB - Dieses SDF ist für Router mit 128 MB DRAM geeignet.**Hinweis:** Die SDFs mit 128 und 256 MB erfordern mindestens 2,001 Engine. Diese Informationen finden Sie im Feld **Einstellungen > Identifikations-Benutzeroberfläche > Version**.**Warnung:** IPS MC enthält keine Speicherverwaltungsfunktionen für Cisco IOS IPS-Router. Seien Sie vorsichtig, wenn Sie SDF-Dateien für Ihren Cisco IOS IPS-Router auswählen. Stellen Sie sicher, dass der Cisco IOS IPS-Router über ausreichend Speicherplatz für die Ausführung der ausgewählten SDF-Datei verfügt.**Hinweis:** Wenn Sie den SDF-Typ ändern, erhalten Sie möglicherweise folgende Meldung: *Wenn Sie den SDF-Typ ändern, können Sie festlegen, dass Signaturoptimierungsinformationen auf dem Gerät beibehalten oder verworfen werden. Klicken Sie zum Verwerfen auf OK. Klicken Sie auf Abbrechen, um*



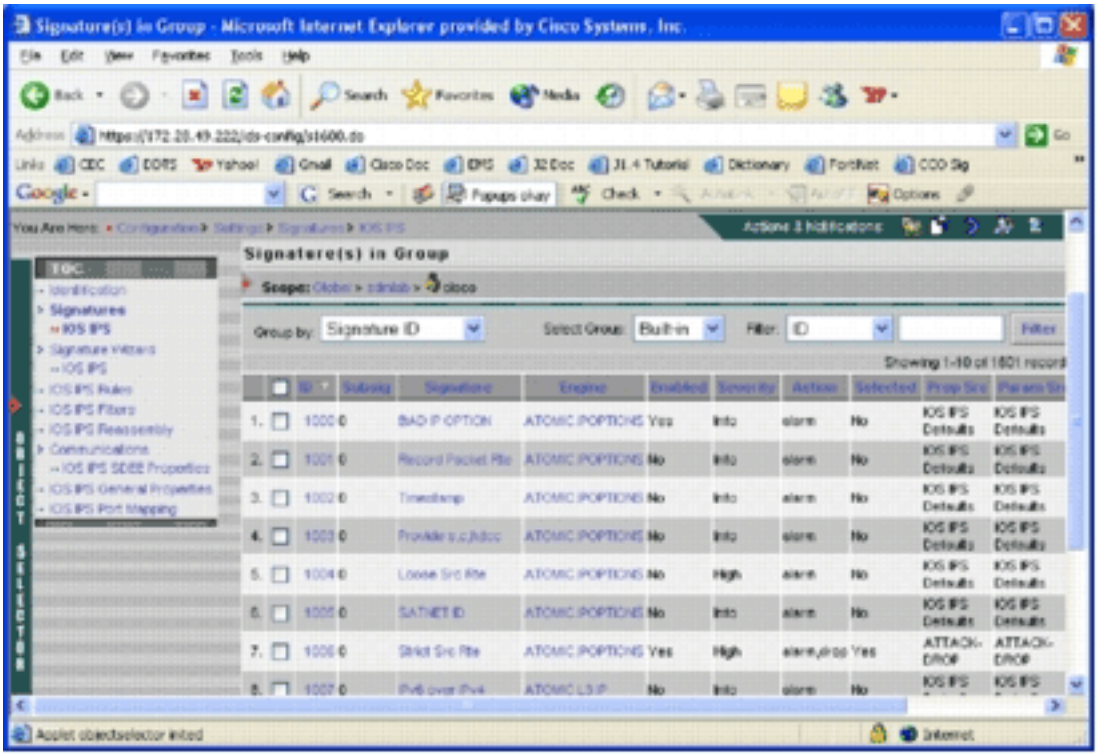
fortzufahren.

6. Klicken Sie auf **Abbrechen**, um Ihre Signatur-Tuning-Informationen beizubehalten.Nachdem Sie nun erfolgreich ein vordefiniertes SDF für den Router-Cisco ausgewählt haben, können Sie eine weitere Signaturanpassung wie Hinzufügen oder Bearbeiten durchführen oder sogar Ihre eigenen Signaturen erstellen. Sie können die Signatur-Tuning-Aufgaben überspringen und direkt zu Create a Rule to Apply to the Interface(s) wechseln.
7. Klicken Sie in der Menüleiste "Konfiguration" auf **Ausstehend**.Die Seite Ausstehend wird angezeigt. 

An diesem Punkt ist die Konfigurationsaufgabe abgeschlossen. Sie müssen jedoch die Bereitstellungsaufgabe abschließen, um die Änderungen auf dem Zielgerät bereitzustellen.

Ändern von vordefinierten SDF-Signaturen

Nachdem Sie eine vordefinierte SDF-Datei für einen Router ausgewählt haben, können Sie weitere Aufgaben zur Signaturanpassung ausführen. Sie können Signaturen nach Belieben hinzufügen, bearbeiten, löschen und ändern oder bei Bedarf eigene Signaturen erstellen. In diesem Beispiel wird IPS MC verwendet, um zusätzliche Signaturen hinzuzufügen und die Aktionen zu ändern. Dieses Bild zeigt die Signaturkonfigurationsschnittstelle.



Sie können die Signaturkonfiguration verwenden, um Signaturaktionen zu aktivieren oder zu deaktivieren, sie auszuwählen oder zu deaktivieren, eine Signatur hinzuzufügen, eine Signatur zu löschen, Signaturaktionen zu ändern und Signaturparameter zu bearbeiten. Erstellen Sie mit dem Signaturassistenten links benutzerdefinierte Signaturen.

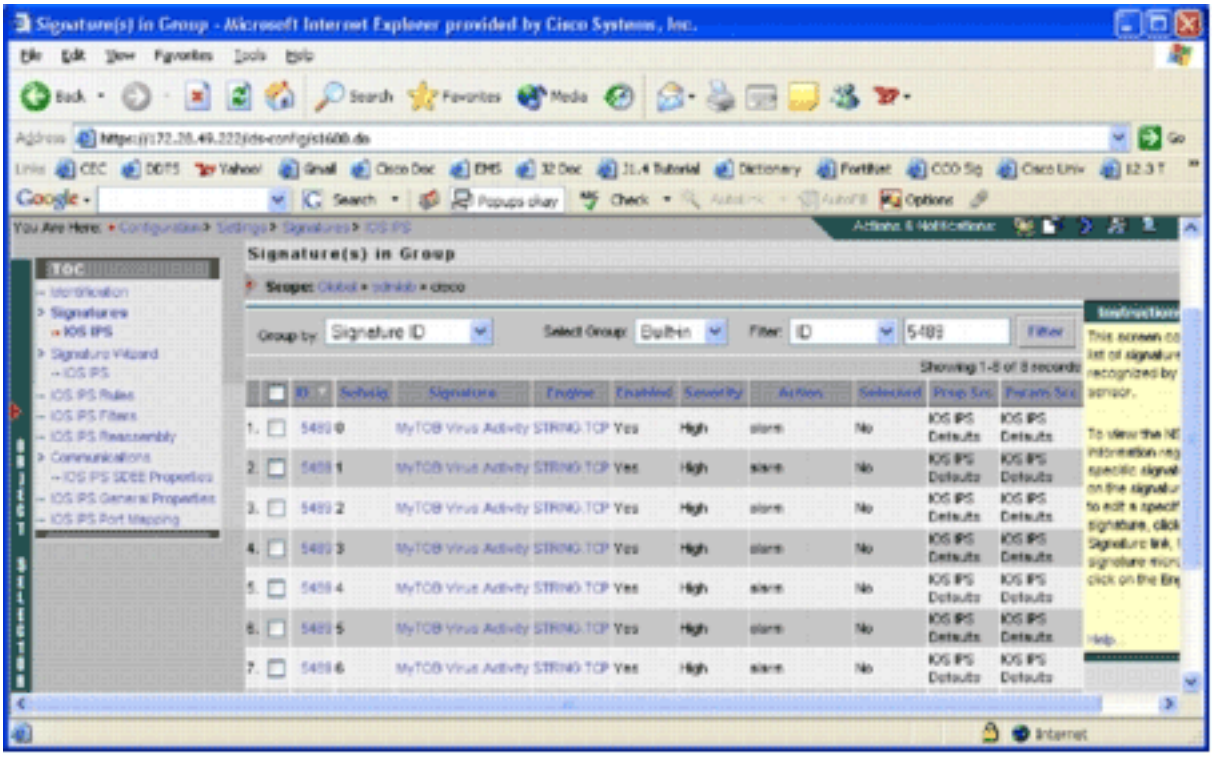
In der Benutzeroberfläche für die Signaturkonfiguration werden einige Informationen standardmäßig angezeigt. Selected gibt an, ob die Signatur in die SDF-Datei aufgenommen wird, die an den Router gesendet wird. Wenn keine Signatur ausgewählt ist, wird sie nicht hinzugefügt. Aktiviert wird nur angewendet, wenn eine Signatur ausgewählt ist. Wenn eine Signatur deaktiviert ist, senden die IPS-Engines keine Ereignisse für diese spezifische Signatur. Wenn eine Signatur deaktiviert ist, wird sie ebenfalls automatisch deaktiviert.

Die letzten beiden Spalten (Prop Src und Param Src) geben an, woher die Signatur bzw. ihr Parameter kommen. Die Signatur könnte aus vorkonfigurierten SDF-Dateien oder aus der werkseitigen Standardeinstellung stammen, die Sie in den IOS-Sxxx.zip-Dateiaktualisierungen finden (wird als IOS IPS Defaults angezeigt). Diese Werte gelten auch für die Parameterspalte.

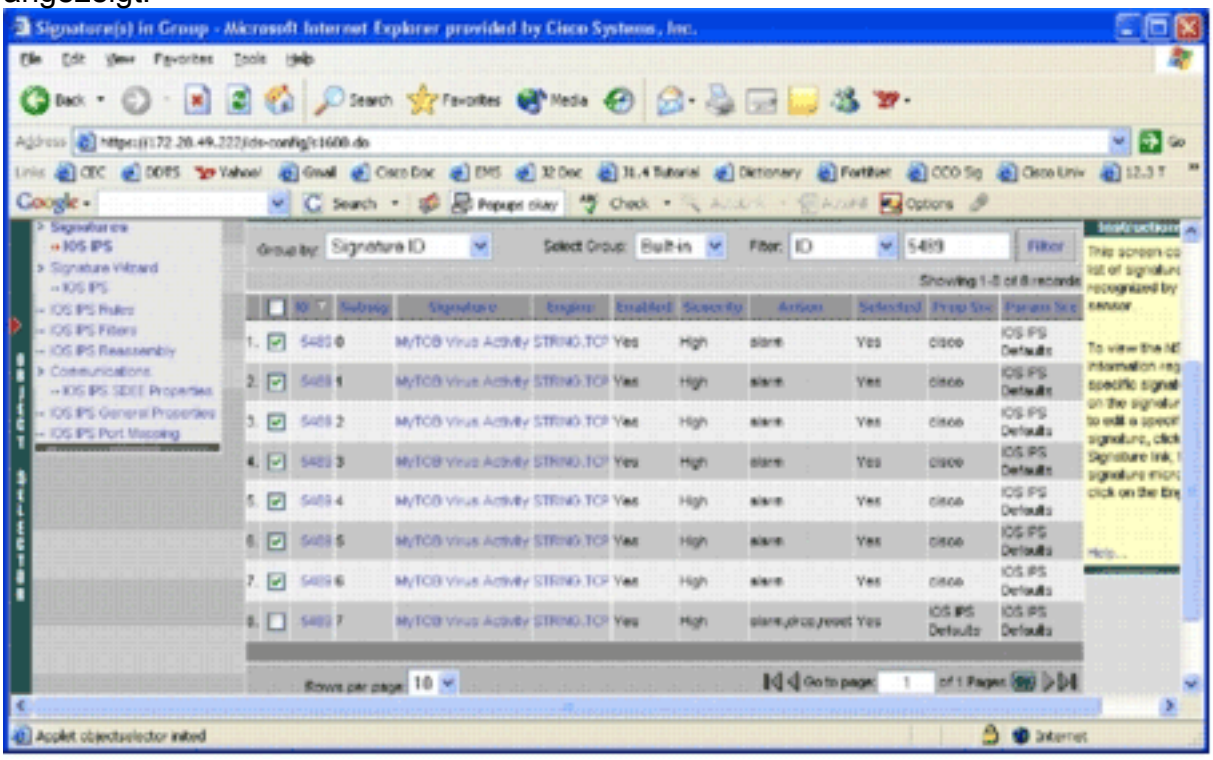
Beim Hinzufügen von Signaturen zu Cisco IOS IPS-Routern müssen Speicheraspekte berücksichtigt werden. Wenn Sie mehr Signaturen hinzufügen, als der Cisco IOS IPS-Router verarbeiten kann, kann IPS MC die Konfigurationsänderungen nicht auf den Geräten bereitstellen.

Gehen Sie wie folgt vor, um dem Cisco IOS IPS-Router die Signaturen 5489/x hinzuzufügen:

1. Wählen Sie **Konfiguration aus**, und wählen Sie dann mit dem Objektauswahl-Tool den Cisco IOS IPS-Router aus, für den Sie IPS-Signaturen konfigurieren möchten.
2. Wählen Sie **Konfiguration > Einstellungen > Signaturen > IOS IPS aus**.Die Signatur(en) auf der Seite Gruppe wird (werden)
   angezeigt.

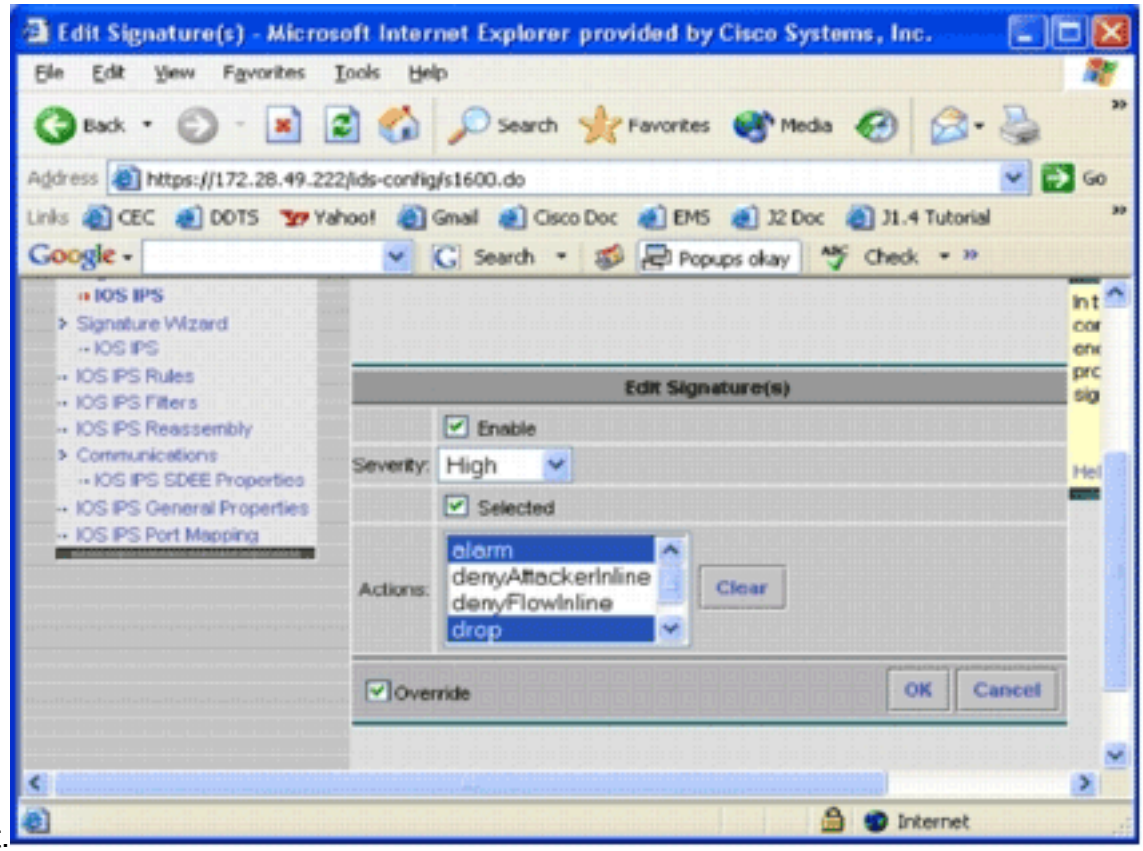


3. Wählen Sie in der sich ergebenden Signaturliste die Option Nach ID filtern aus, und geben Sie die Signatur-ID 5489 ein.
4. Klicken Sie auf **Filtern**, um nach Signaturen zu suchen.Die Suchergebnisse werden angezeigt.



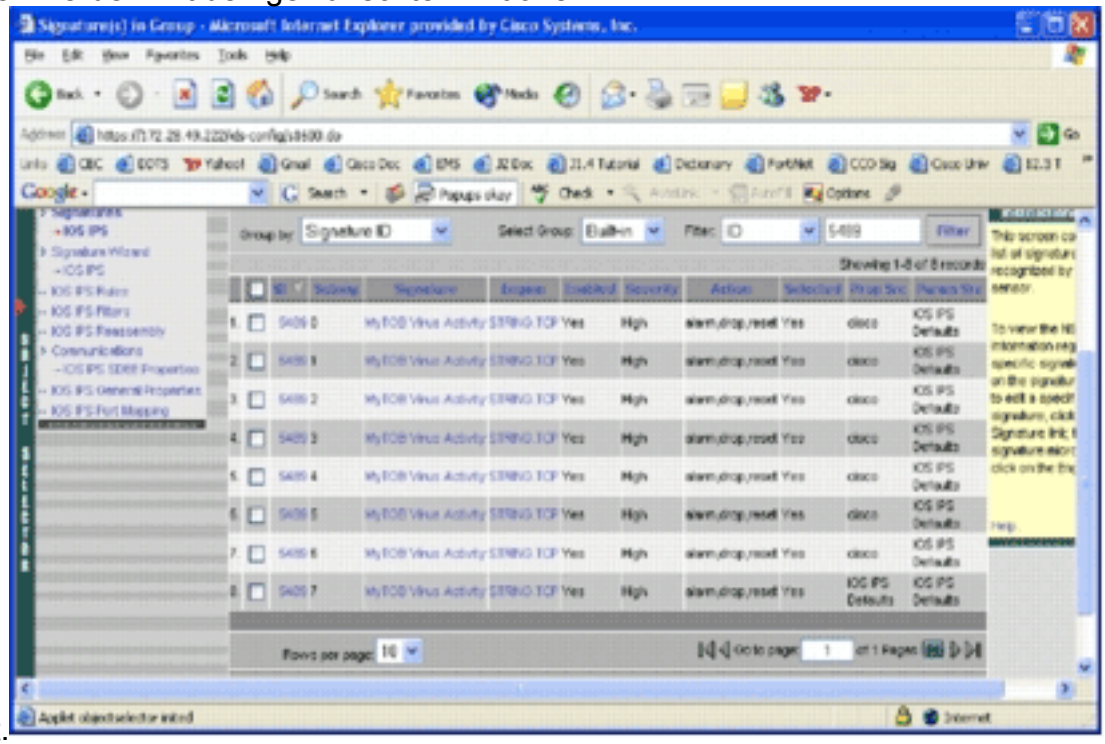
Hinweis: IPS MC unterstützt keine neue Kategorisierung in Cisco SDM.

5. Aktivieren Sie das Kontrollkästchen neben nicht ausgewählten Signaturen, und klicken Sie in der unteren Symbolleiste auf **Auswählen**.
6. Klicken Sie auf **Bearbeiten**, um Signaturaktionen zu ändern.Die Seite Signatur(en) bearbeiten wird



angezeigt.

7. Aktivieren Sie das **Kontrollkästchen Ausgewählt**, und wählen Sie **alarm**, **Drop** und **Reset** aus der Aktionsliste aus.
8. Aktivieren Sie das Kontrollkästchen **Überschreiben**, und klicken Sie dann auf **OK**.Alle Signaturen werden mit den gewünschten Aktionen



geändert.

9. Wechseln Sie zur Task "Ausstehend", und speichern Sie alle Änderungen. Damit ist die Konfigurationsaufgabe abgeschlossen.**Tipp:** Achten Sie genau auf die Spalte Prop Src. Nach der Änderung wurde die Quelle auf das Gerät mit dem Namen *cisco* geändert, d. h., alle Tuning-Informationen werden getrennt von den voreingestellten SDF-Dateien gespeichert. Dieser Mechanismus ermöglicht es dem IPS MC, benutzerdefinierte Signaturänderungen beizubehalten.

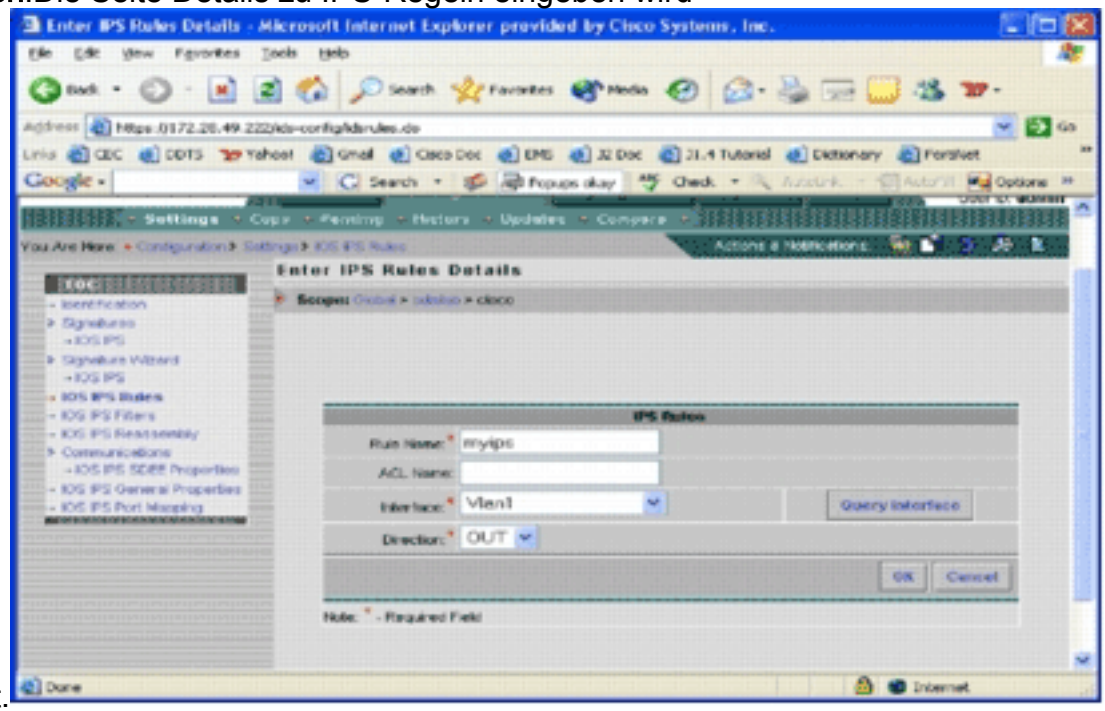
Im vorherigen Abschnitt, in dem Sie die SDF-Dateitypen geändert haben, fragte das IPS MC Sie, ob Sie die Signatur-Tuning-Informationen beibehalten möchten. Dies sind die Signatur-Tuning-Informationen, auf die verwiesen wird.

Benutzerdefinierte Signaturen auswählen

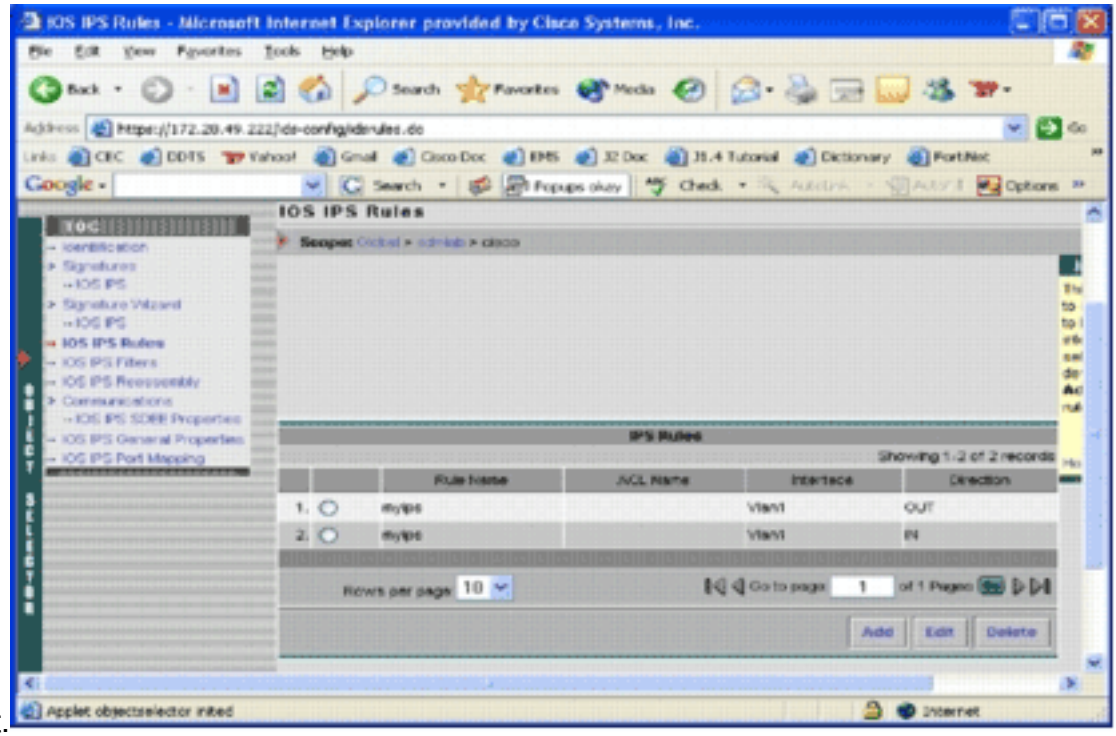
Wenn Sie die voreingestellten SDF-Standarddateien nicht verwenden möchten, können Sie die im Abschnitt Ändern von vorkonfigurierten SDF-Signaturen angegebenen Schritte verwenden, um die Tuning-Signaturen für Ihre Geräte auszuwählen. Auf der Identifizierungsseite müssen Sie sicherstellen, dass der SDF-Typ UNSET ist. Weitere Informationen finden Sie in Schritt 3 unter Konfigurieren des Cisco IOS IPS-Routers für die Verwendung vorkonfigurierter Signaturdateien.

Erstellen einer Regel für die Schnittstelle(n)

Nach dem Einstellen der Signatur müssen Sie IPS auf den Cisco IOS-Routern aktivieren. Um IPS auf dem Router zu aktivieren, müssen Sie eine IPS-Regel erstellen und auf mindestens eine Schnittstelle anwenden.

1. Wählen Sie **Konfiguration aus**, und wählen Sie dann mit dem Objektauswahl-Fenster den Cisco IOS IPS-Router aus, den Sie konfigurieren möchten. Überprüfen Sie in der Pfadleiste, ob Ihr Bereich auf Geräteebene und nicht auf Gruppenebene liegt.
2. Wählen Sie **Konfiguration > Einstellungen > IOS IPS Rules aus**, und klicken Sie dann auf **Hinzufügen**.Die Seite Details zu IPS-Regeln eingeben wird angezeigt. 

3. Geben Sie Informationen für den Regelnamen und die Schnittstelle ein, auf die Sie die Regel und die Richtung anwenden möchten.
4. Klicken Sie auf **OK**.Die Seite IOS IPS Rules (IOS-IPS-Regeln) wird



angezeigt. Ebenso können Sie Regeln für beide Richtungen für eine Schnittstelle erstellen.

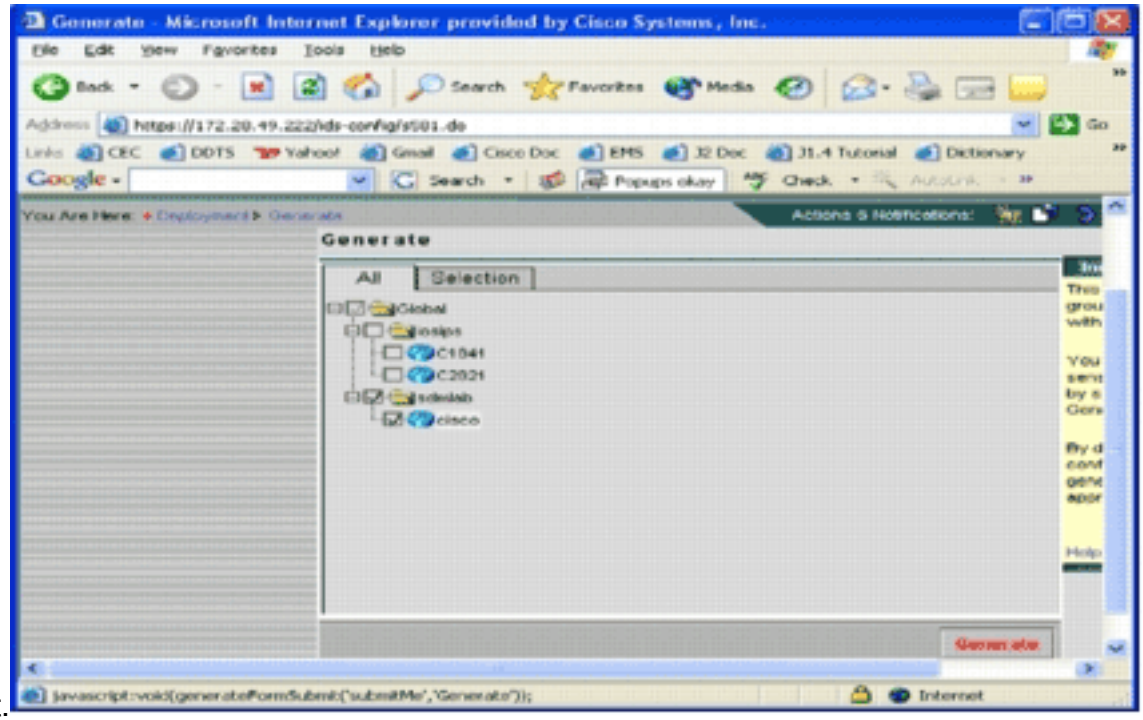
5. Sie müssen die Konfigurationsänderungen speichern und den Bereitstellungsprozess durchlaufen, um Änderungen an dem betroffenen Gerät oder der betroffenen Gerätegruppe zu übertragen.Sie können auch andere IPS-bezogene Konfigurationen durchführen, aber alle anderen Aufgaben sind optional und nicht erforderlich. Sie finden alle Optionen links neben der Konfigurationsbenutzeroberfläche. Die optionalen Konfigurationsoptionen werden in diesem Dokument nicht behandelt.

Bereitstellung der Konfiguration

Nachdem Sie alle Konfigurationsänderungen vorgenommen haben, müssen Sie die Bereitstellungsaufgabe verwenden, um die Änderungen auf die Geräte zu übertragen. Alle bisher vorgenommenen Konfigurationen werden lokal auf dem IPS MC-Server gespeichert.

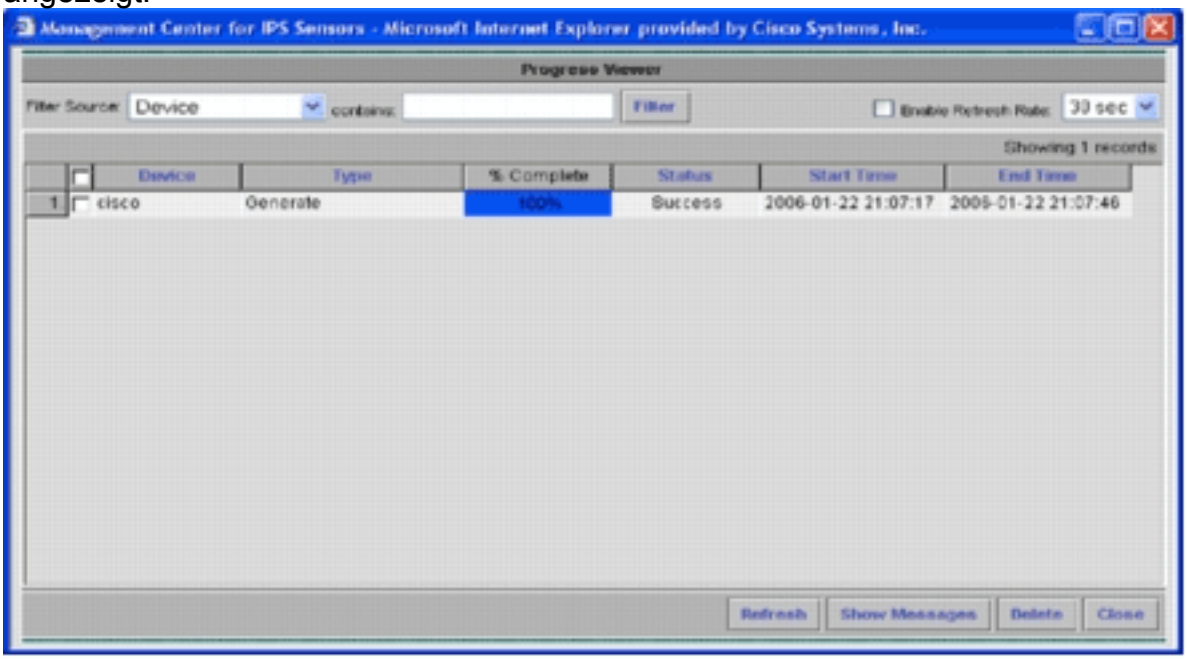
Um Konfigurationsänderungen bereitzustellen, rufen Sie die Bereitstellungsseite auf, und führen Sie die folgenden Schritte aus:

1. Klicken Sie auf die Registerkarte **Bereitstellung**, und wählen Sie **Generate (Erstellen)** aus, um Konfigurationsänderungen zu generieren.Die Seite Generate (Erstellen) wird

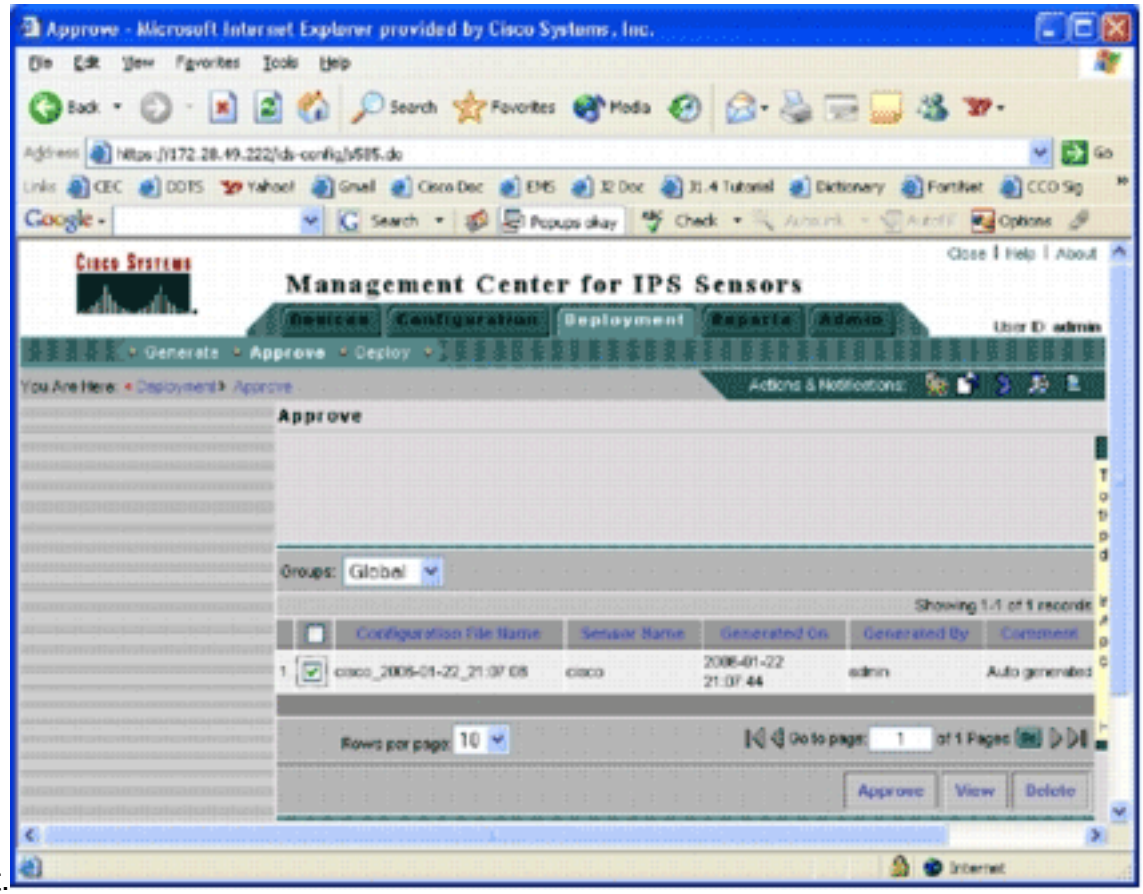


angezeigt.

2. Wählen Sie das *Cisco* Gerät aus, das Sie gerade konfiguriert haben, und klicken Sie auf **Generieren**.
3. Klicken Sie auf **OK**, um die generierte Konfiguration zu akzeptieren, und klicken Sie dann auf **OK**.Eine Statusseite wird angezeigt.

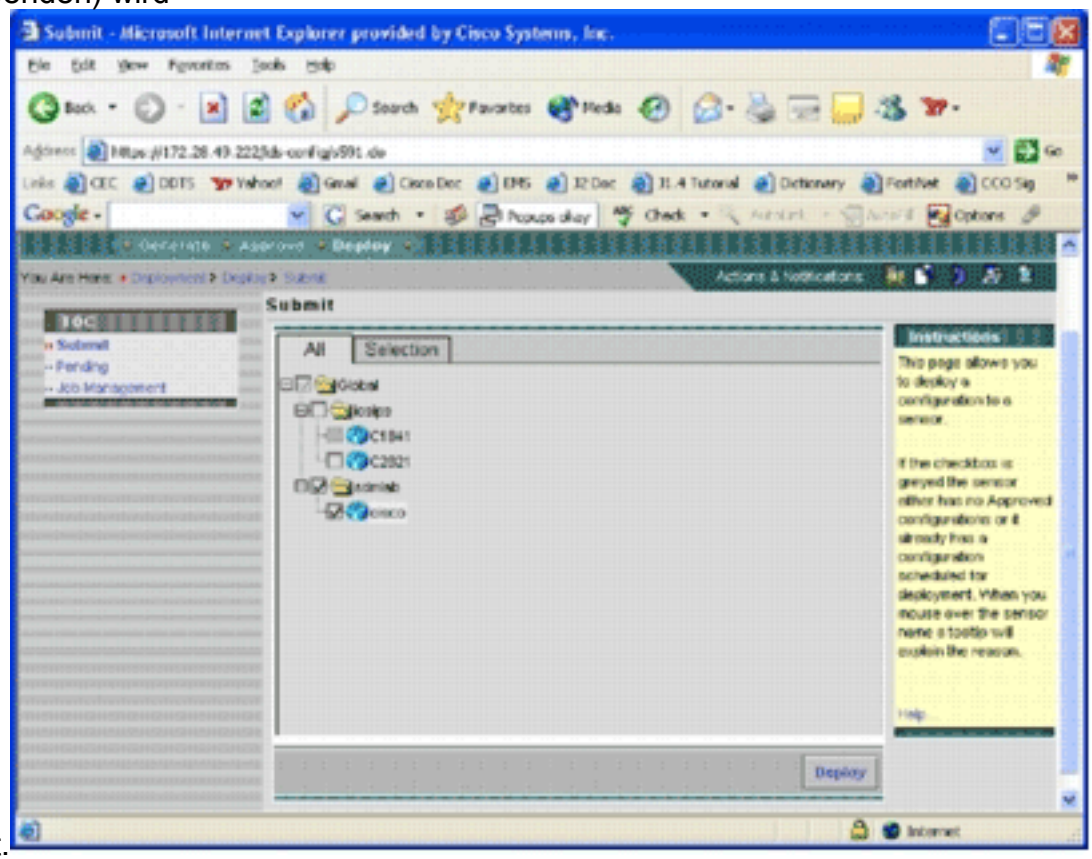


4. Klicken Sie auf **Aktualisieren**, bis die Aufgabe Generierung erfolgreich abgeschlossen ist.
5. Klicken Sie in der Menüleiste "Bereitstellung" und in der Gruppe "SDMLAB" auf **Genehmigen**, um eine Liste der Konfigurationen anzuzeigen, die genehmigt werden müssen.Die Seite "Genehmigen" wird



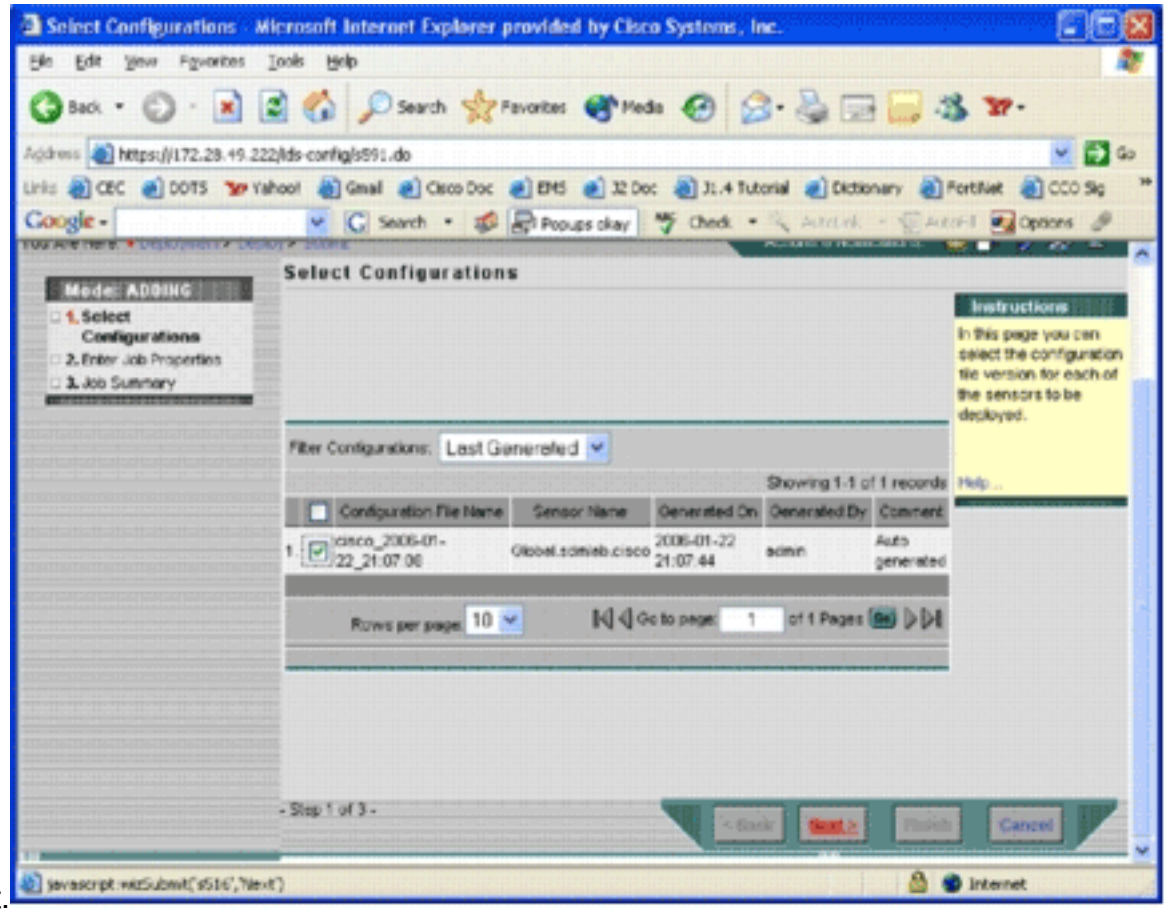
angezeigt.

6. Wählen Sie die Aufgabe(en) aus, und klicken Sie auf **Genehmigen**.Klicken Sie in der Menüleiste "Bereitstellung" auf **Bereitstellen**, und klicken Sie dann auf **Senden**.Die Seite Submit (Senden) wird



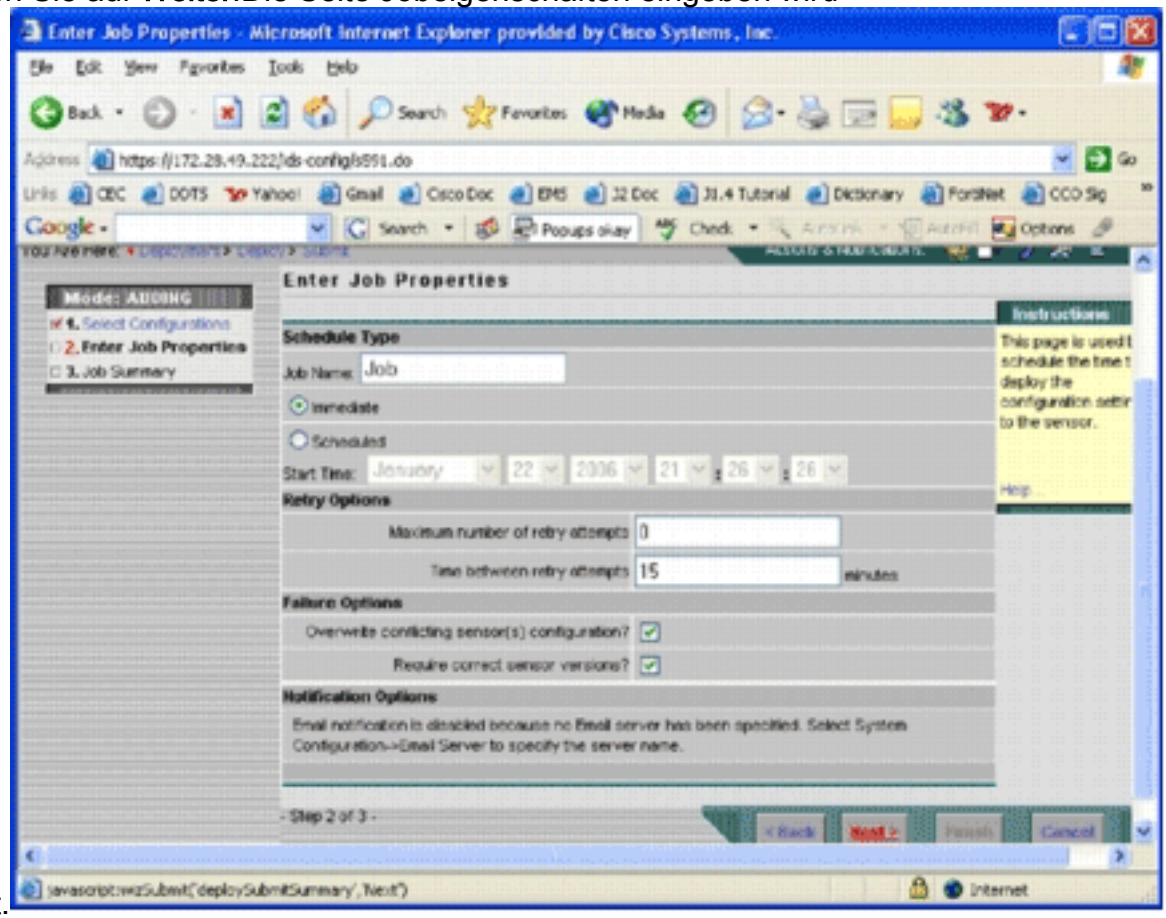
angezeigt.

7. Wählen Sie die Geräte aus, für die Sie die Bereitstellungsaufgabe senden möchten.
8. Wählen Sie das *Cisco* Gerät aus, und klicken Sie auf **Bereitstellen**.Die Seite "Konfigurationen auswählen" wird



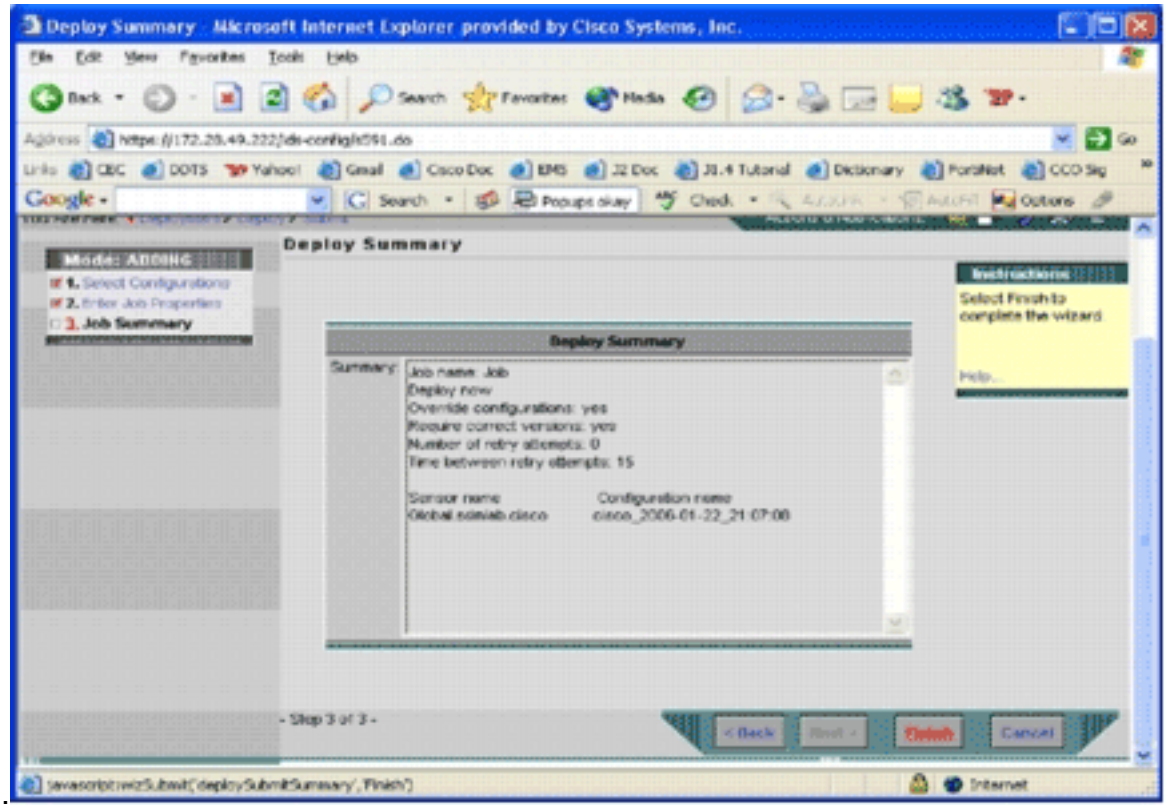
angezeigt.

9. Wählen Sie die Konfiguration aus, die Sie gerade auf dem *Cisco* Gerät vorgenommen haben, und klicken Sie auf **Weiter**.Die Seite Jobeigenschaften eingeben wird



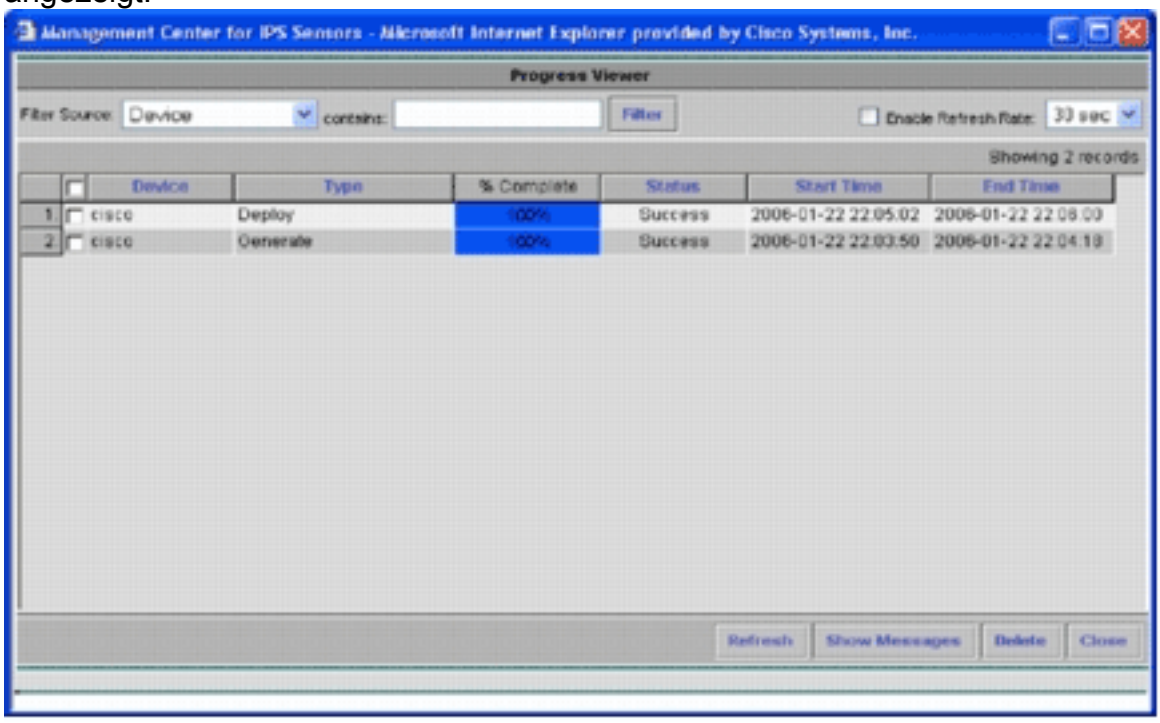
angezeigt.

10. Sie können die Änderungen entweder sofort bereitstellen oder zu einem späteren Zeitpunkt eine Aufgabe planen. Wählen Sie in diesem Beispiel die Option **Sofort** und klicken Sie dann auf **Weiter**.Eine kurze Aufgabenübersicht wird angezeigt und kann bereitgestellt

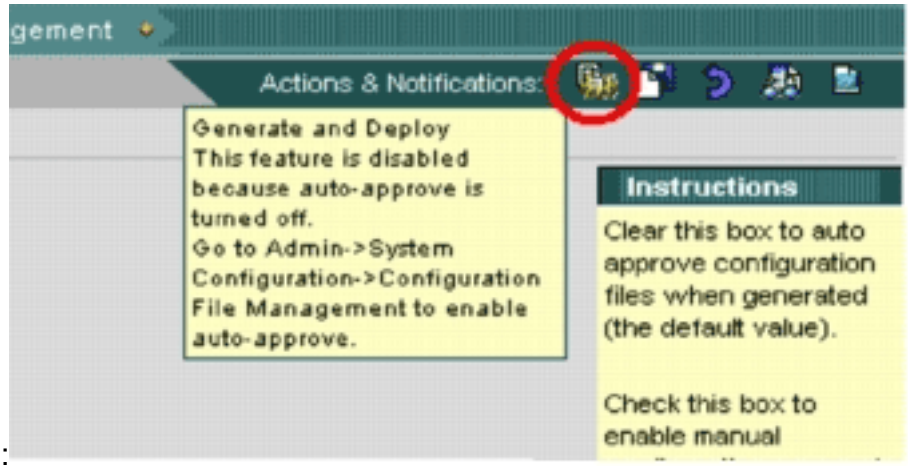


werden.

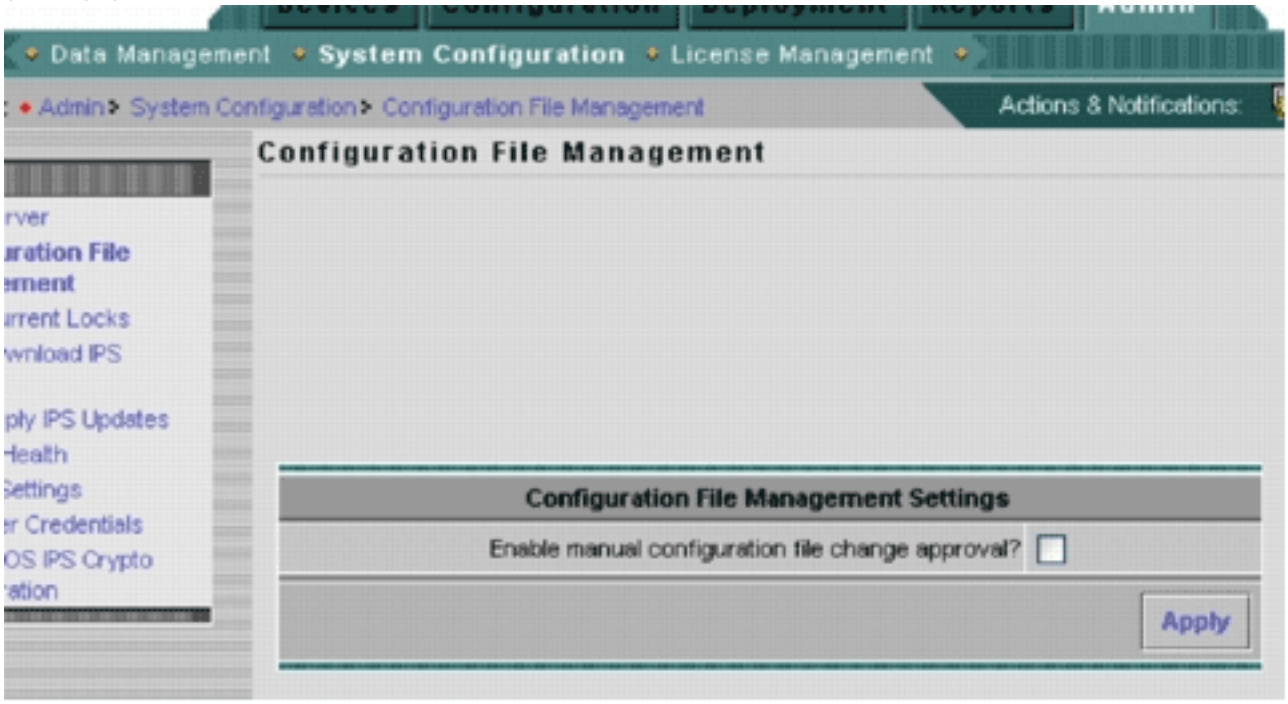
11. Klicken Sie auf **Fertig stellen**.Am Ende der Bereitstellung wird der Status des Bereitstellungsprozesses in einem Dialogfeld angezeigt.



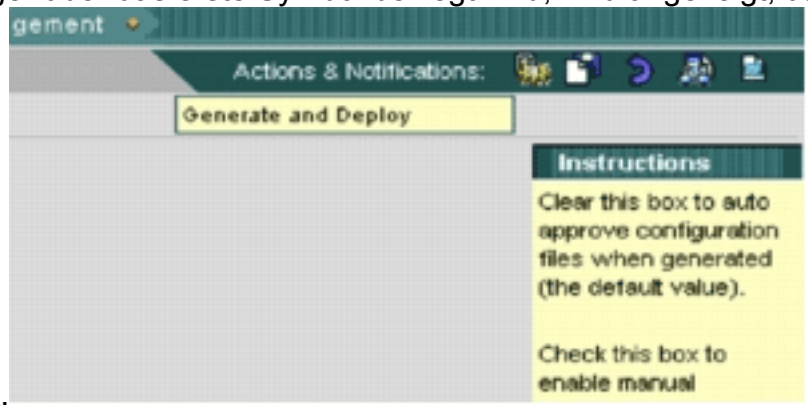
Sie haben erfolgreich Cisco IOS IPS-Konfigurationen auf dem Gerät bereitgestellt. Wenn Sie mehrere Geräte konfigurieren, können Sie Konfigurationsänderungen auf Gruppenebene vornehmen und die Änderungen dann auf alle Cisco IOS IPS-Router anwenden, die derselben Gruppe angehören.**Tipp:** Dieser Prozess ist langwierig, aber eine Funktion zur schnellen Bereitstellung ist verfügbar. Wenn Sie diese Funktion verwenden, müssen Sie nicht den Prozess **Generate > Approve > Deploy** (**Generieren > Genehmigen > Bereitstellen)** durchlaufen. Gehen Sie wie folgt vor, um die Funktion zu verwenden:Oben auf der Benutzeroberfläche befindet sich eine Reihe kleiner Symbole. Bewegen Sie den Mauszeiger über das erste Symbol, und zeigen Sie den in diesem Bild angezeigten



QuickInfo an: Um die Aufgabe "Erstellen und Bereitstellen" zu aktivieren, gehen Sie zu **Admin > Systemkonfiguration > Konfigurationsdateiverwaltung**, und deaktivieren Sie das Kontrollkästchen **Manuelle Konfigurationsdateiänderung aktivieren**.



Wenn der Mauszeiger über das erste Symbol bewegt wird, wird angezeigt, dass die Aufgabe aktiviert ist.



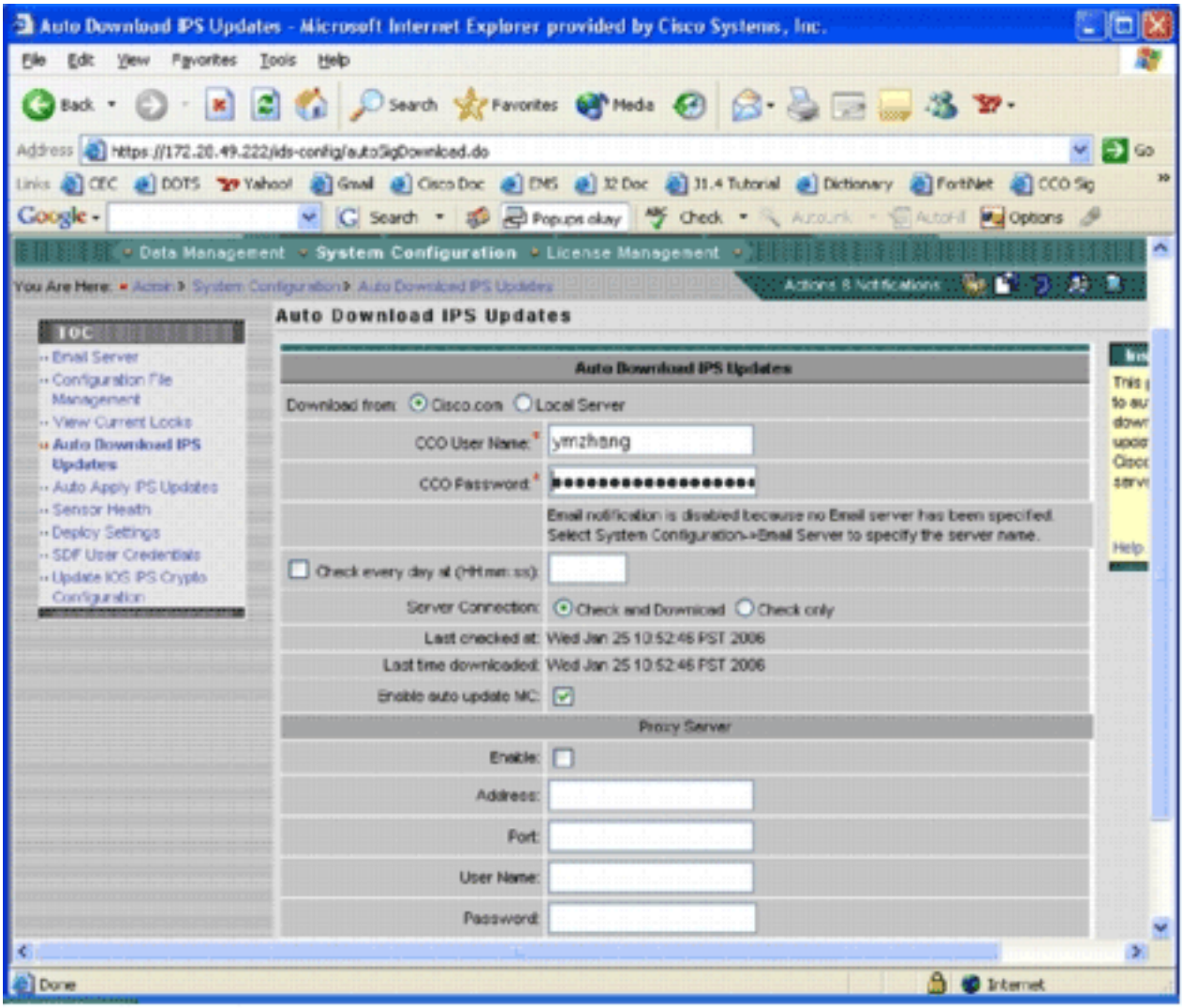
Klicken Sie auf dieses Symbol.IPS MC generiert automatisch Konfigurationsänderungen und stellt diese auf den Geräten bereit.

Signatur-Updates automatisch herunterladen

IPS MC unterstützt Updates für die automatische Download-Signatur von Cisco.com. Signatur-

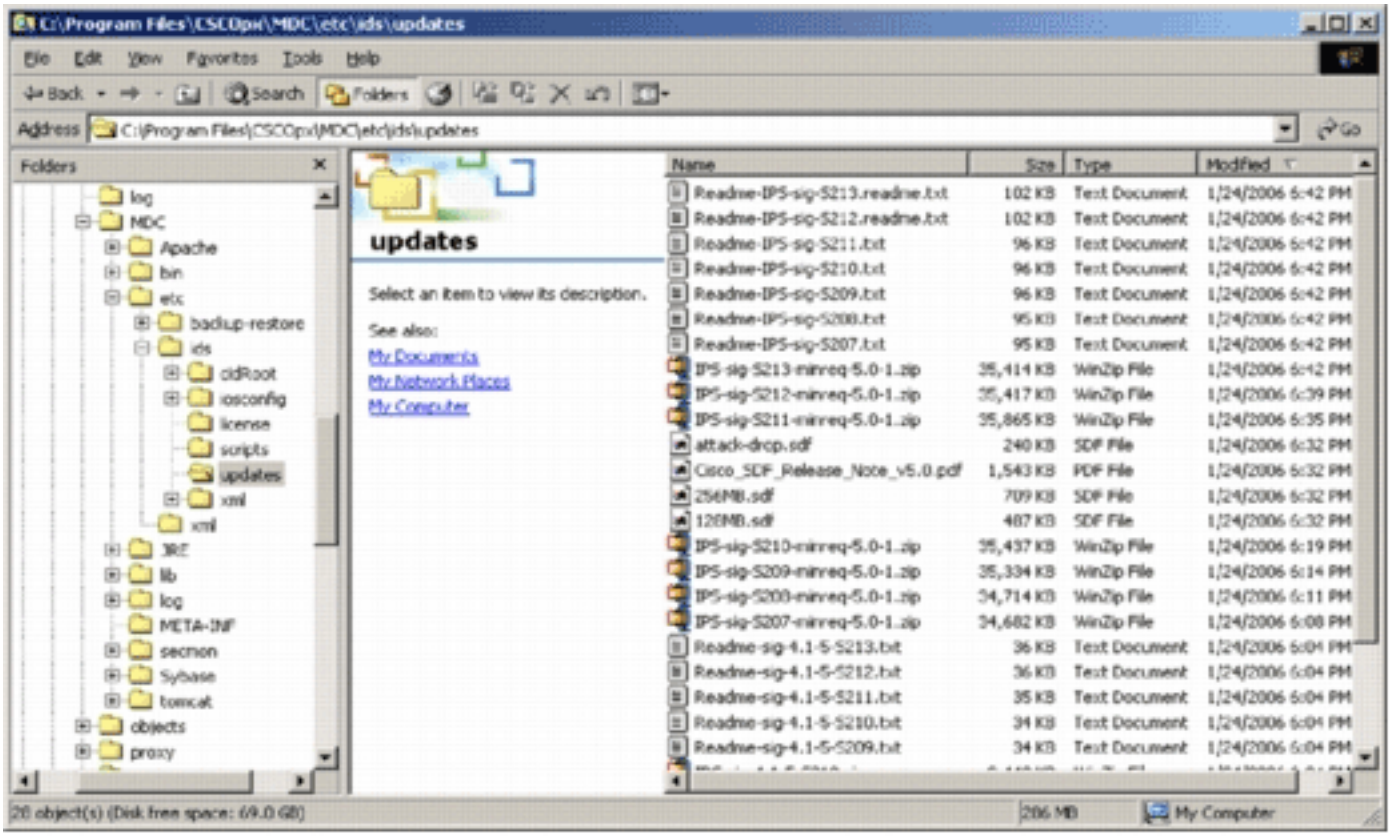
Updates können für Sensorplattformen sowie für Cisco IOS IPS-Plattformen heruntergeladen werden. Um diese Funktion zu konfigurieren, gehen Sie zu **Admin > System Configuration > Auto Download IPS Updates**.

Die Seite "IPS-Aktualisierung automatisch herunterladen" wird angezeigt.



Sie benötigen ein gültiges Cisco.com-Konto, um dieses Signatur-Update herunterzuladen. Um die automatisch heruntergeladenen Dateien zu überprüfen, gehen Sie zum Hauptverzeichnis der IPS MC-Installation. Standardmäßig ist dies das Programm files\CSCOpx\MDC\etc\ids\updates.

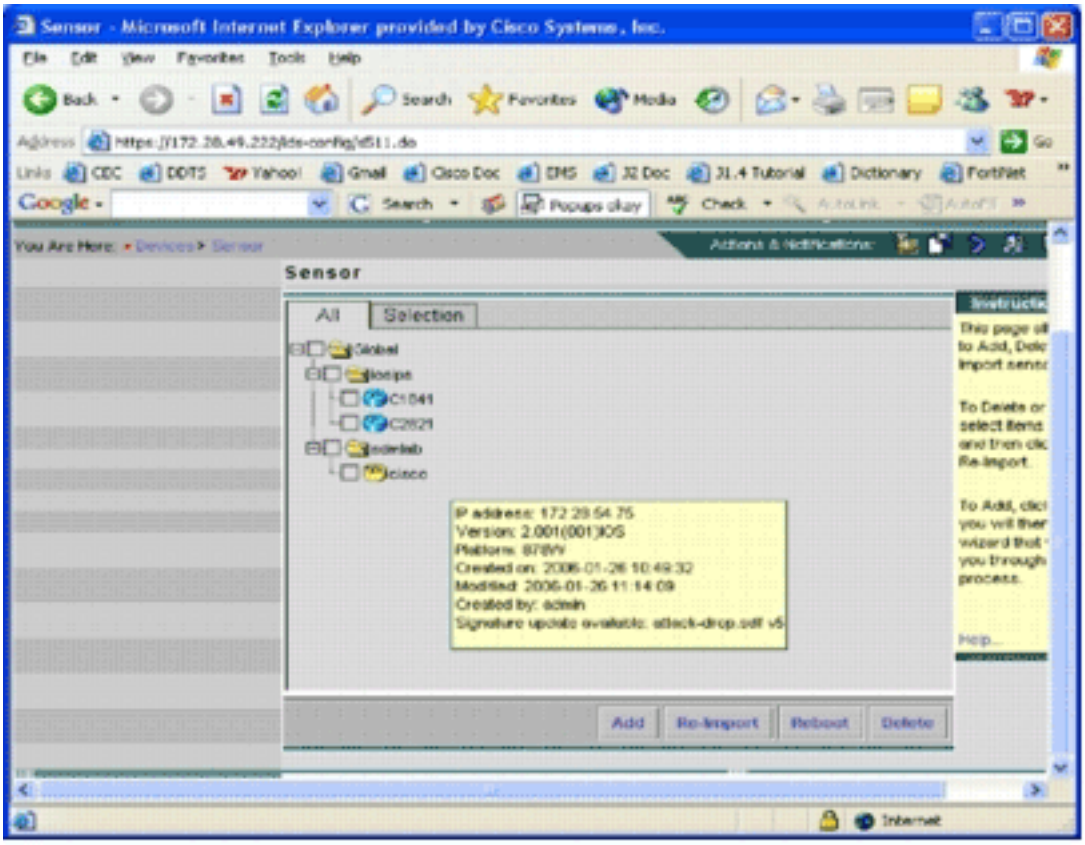
Dieses Bild zeigt ein Bild der heruntergeladenen Dateien in diesem Verzeichnis.



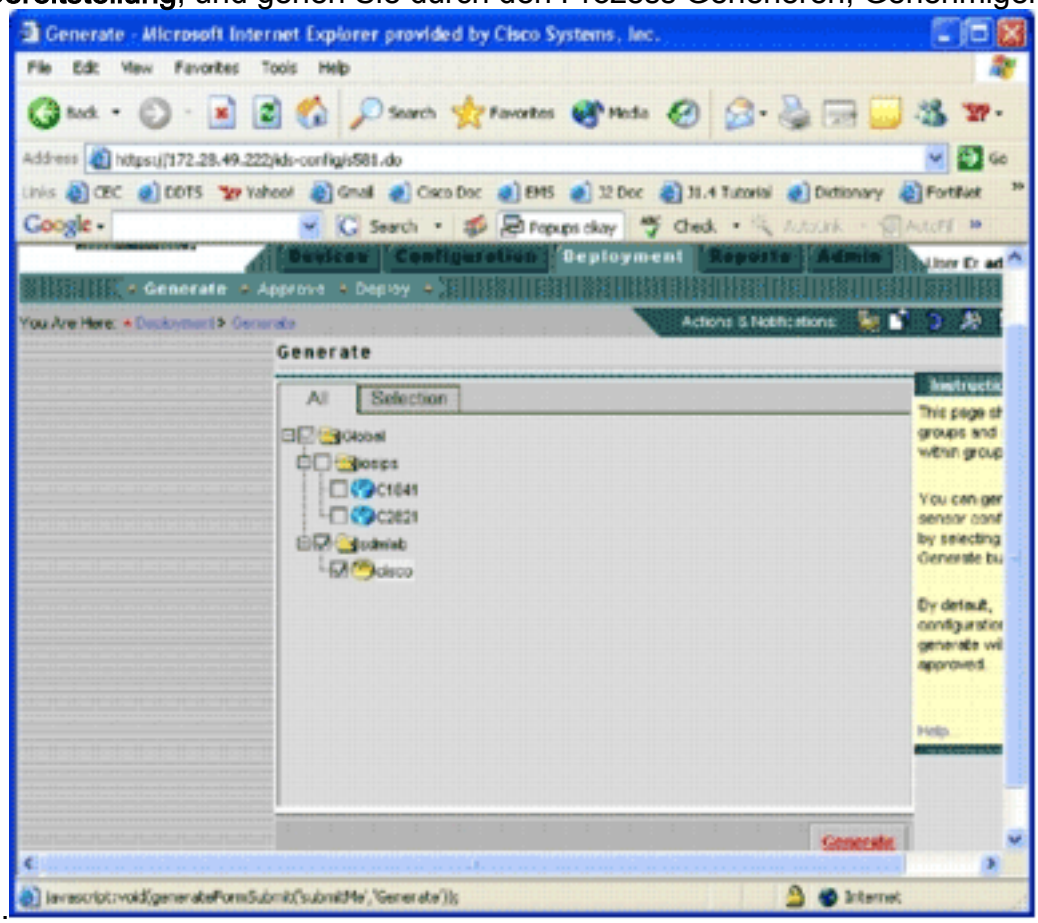
Sie sehen, dass die Sensor-Update-Dateien. Die Cisco IOS Software-Update-Datei und die vorkonfigurierten SDF-Dateien werden heruntergeladen.

Aktualisieren des Cisco IOS IPS-Routers mit neuen SDF-Dateien

Bei Cisco IOS IPS-Routern, die mit vordefinierten SDF-Dateien bereitgestellt werden, erkennt Cisco IPS MC die neue Version, sobald eine neue Version der SDF-Dateien über das automatische Herunterladen oder Kopieren in das Aktualisierungsverzeichnis verfügbar ist. Nach einer Aktualisierung der Benutzeroberfläche werden die Gerätesymbole für die entsprechenden Geräte gelb.



1. Klicken Sie auf **Bereitstellung**, und gehen Sie durch den Prozess Generieren, Genehmigen und Bereitstellen.



2. Nach erfolgreicher Bereitstellung verwendet der Cisco IOS IPS-Router eine neue Version von SDF-Dateien.

Zugehörige Informationen

- Cisco Intrusion Prevention System