Konfigurationsbeispiel eines Cisco IOS Intrusion Prevention System Security Manager

Inhalt

Einleitung

Cisco Security Manager ist Teil der Cisco Security Management Suite, die eine umfassende Richtlinienverwaltung und -durchsetzung für das Cisco Self-Defending Network bereitstellt. Cisco Security Manager ist eine branchenführende Anwendung der Enterprise-Klasse für das Sicherheitsmanagement. Cisco Security Manager befasst sich mit dem Konfigurationsmanagement von Firewall-, VPN- und IPS-Sicherheitsservices (Intrusion Prevention System) für Cisco Router, Security Appliances und Security Services-Module.

Eine Zusammenfassung der Funktionen und Vorteile von Cisco Security Manager sowie der neuen Funktionen in Version 3.1 finden Sie im Datenblatt zu Cisco Security Manager 3.1 unter http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_data_sheet0900aecd8062bf6e.html. Sie können Cisco Security Manager 3.1 von Cisco.com unter http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app herunterladen (nur registrierte Kunden).

In diesem Dokument wird beschrieben, wie Sie Cisco Security Manager 3.1 zum Durchführen der Erstkonfiguration von IOS IPS verwenden. Für Router, die bereits mit IOS IPS konfiguriert sind, können Kunden Cisco Security Manager 3.1 direkt für Bereitstellungsaufgaben verwenden.

Hinweis: Cisco Security Manager 3.1 unterstützt nur IOS 12.4(11)T2- und spätere IOS-Images, um IOS IPS zu konfigurieren.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Security Manager 3.1
- Cisco IOS 12.4(11)T2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

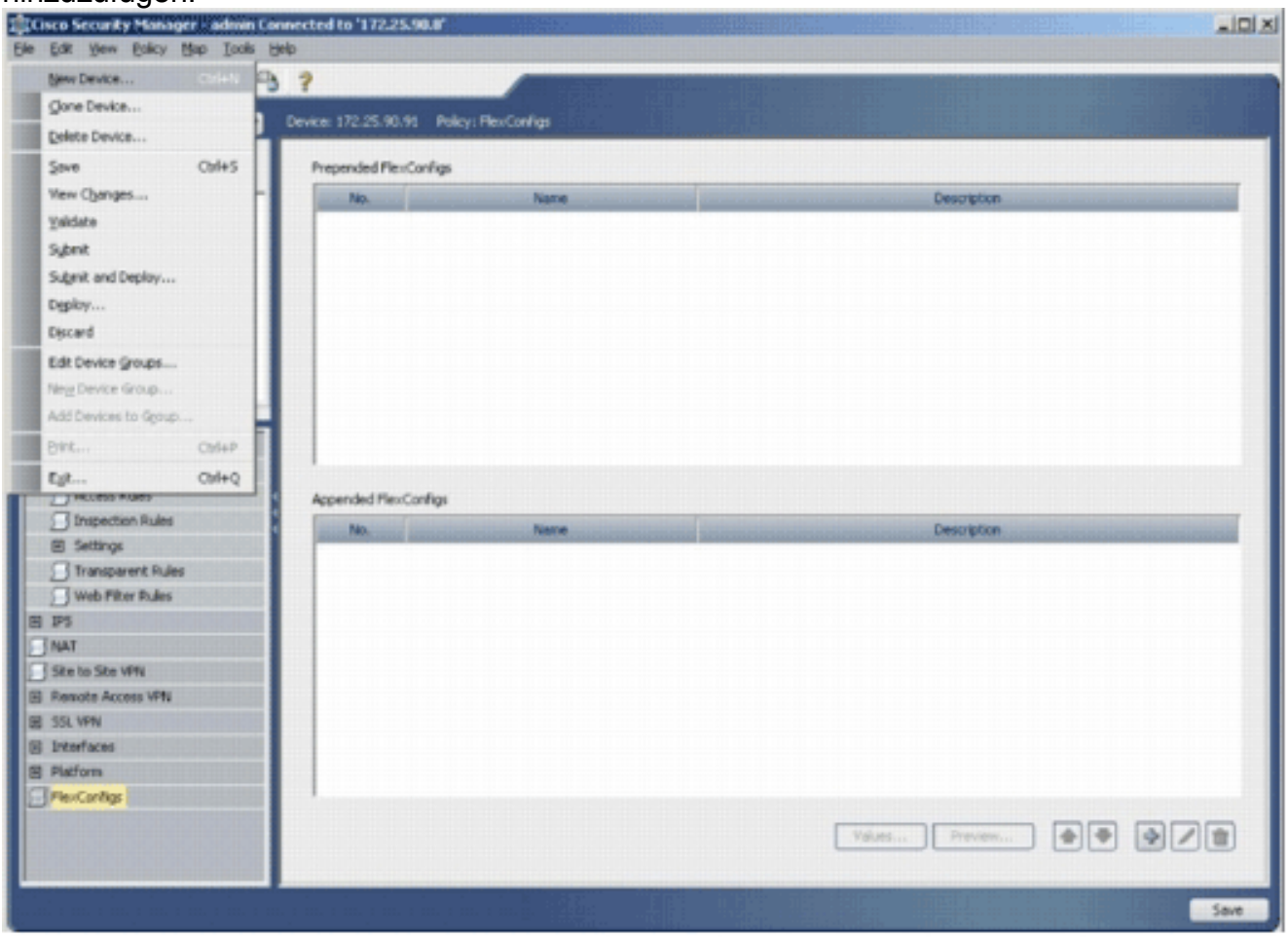
Konventionen

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

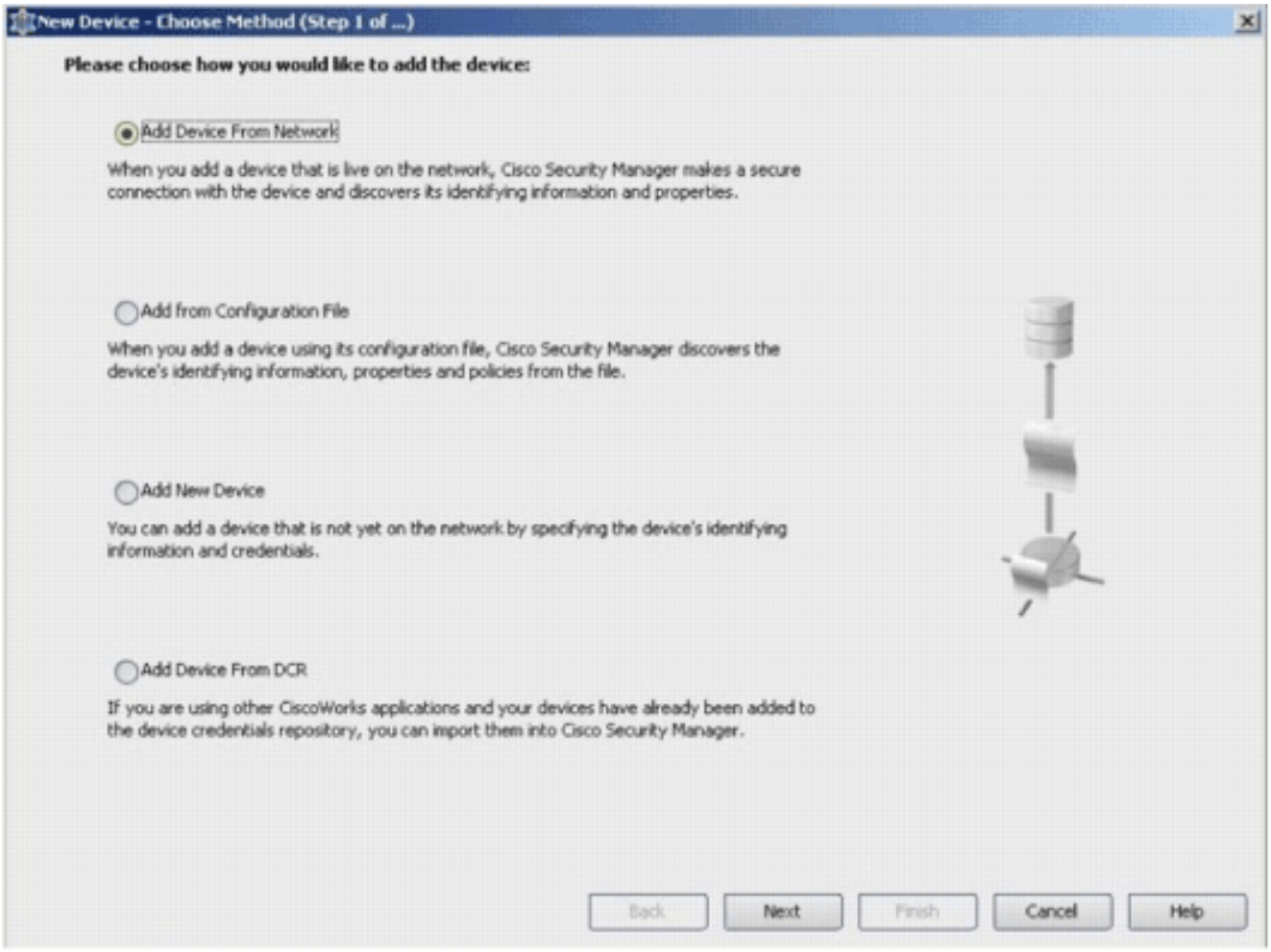
Konfigurieren

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

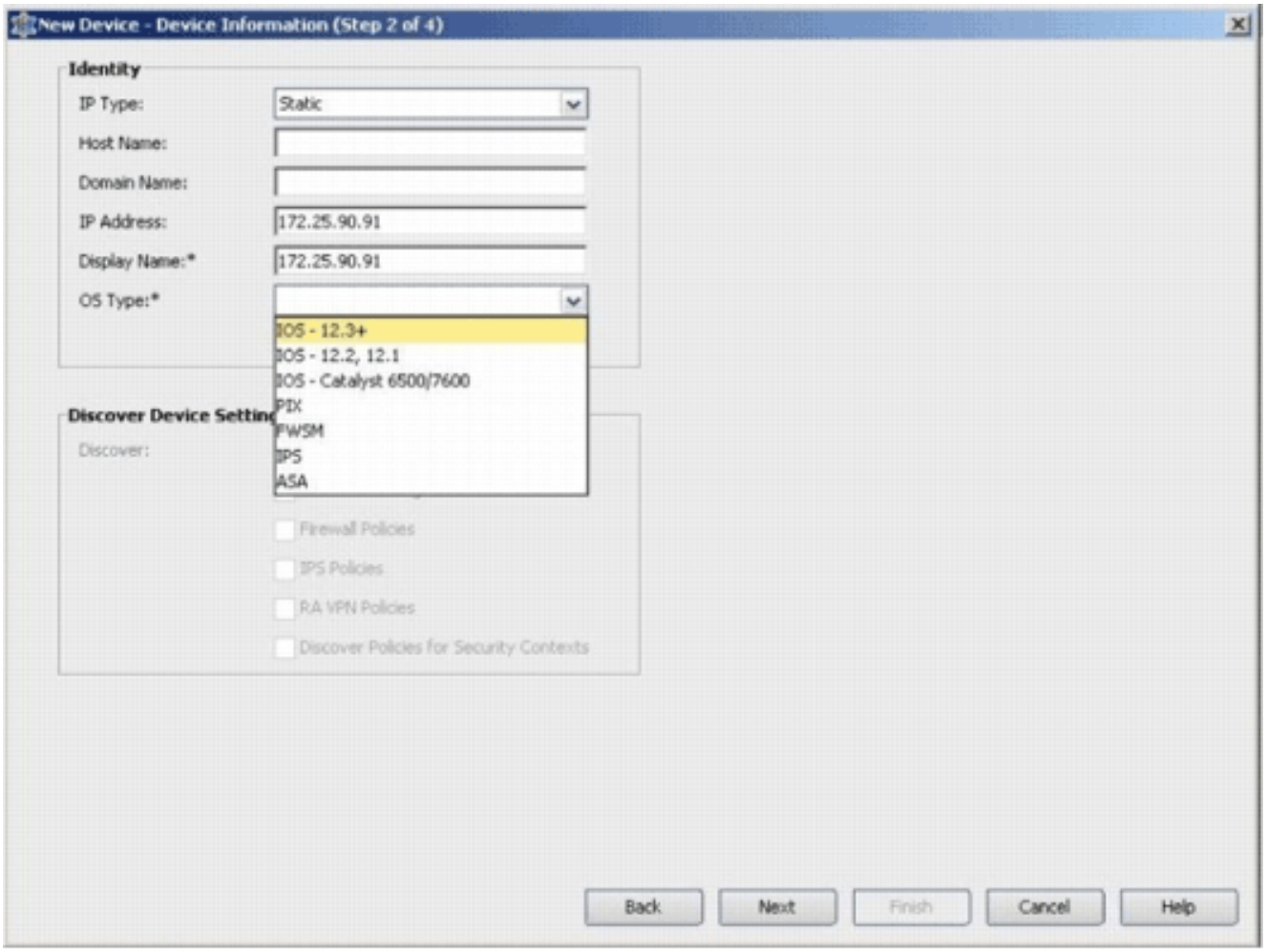
1. Führen Sie den Cisco Security Manager 3.1-Client von Ihrem lokalen PC aus.
2. Wählen Sie **Neues Gerät** im Menü Datei aus, um ein Gerät zum Cisco Security Manager 3.1 hinzuzufügen.



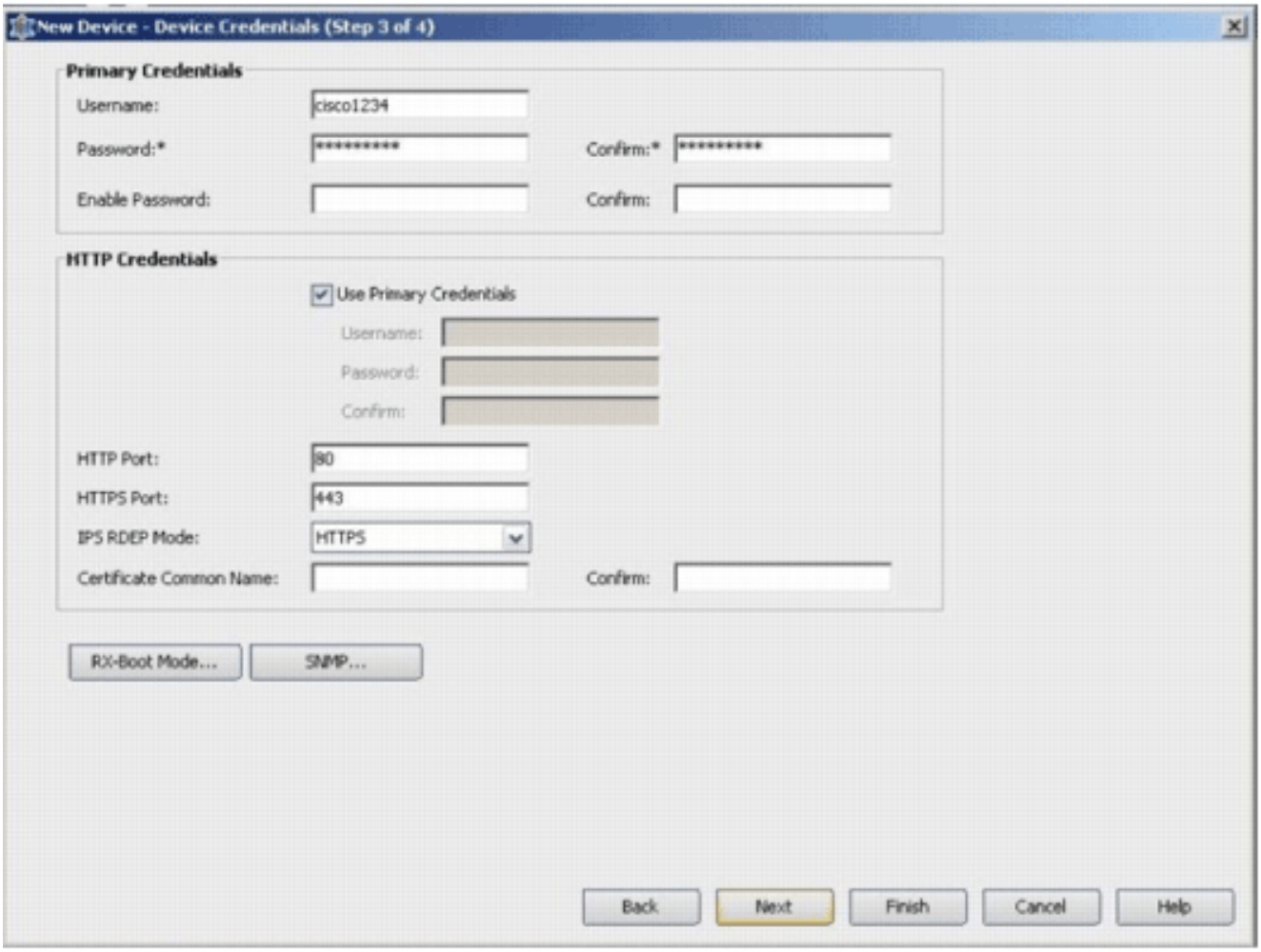
3. Wählen Sie im Fenster Neues Gerät aus, wie Sie das Gerät hinzufügen möchten. In diesem Beispiel wird das Gerät aus dem Netzwerk hinzugefügt.



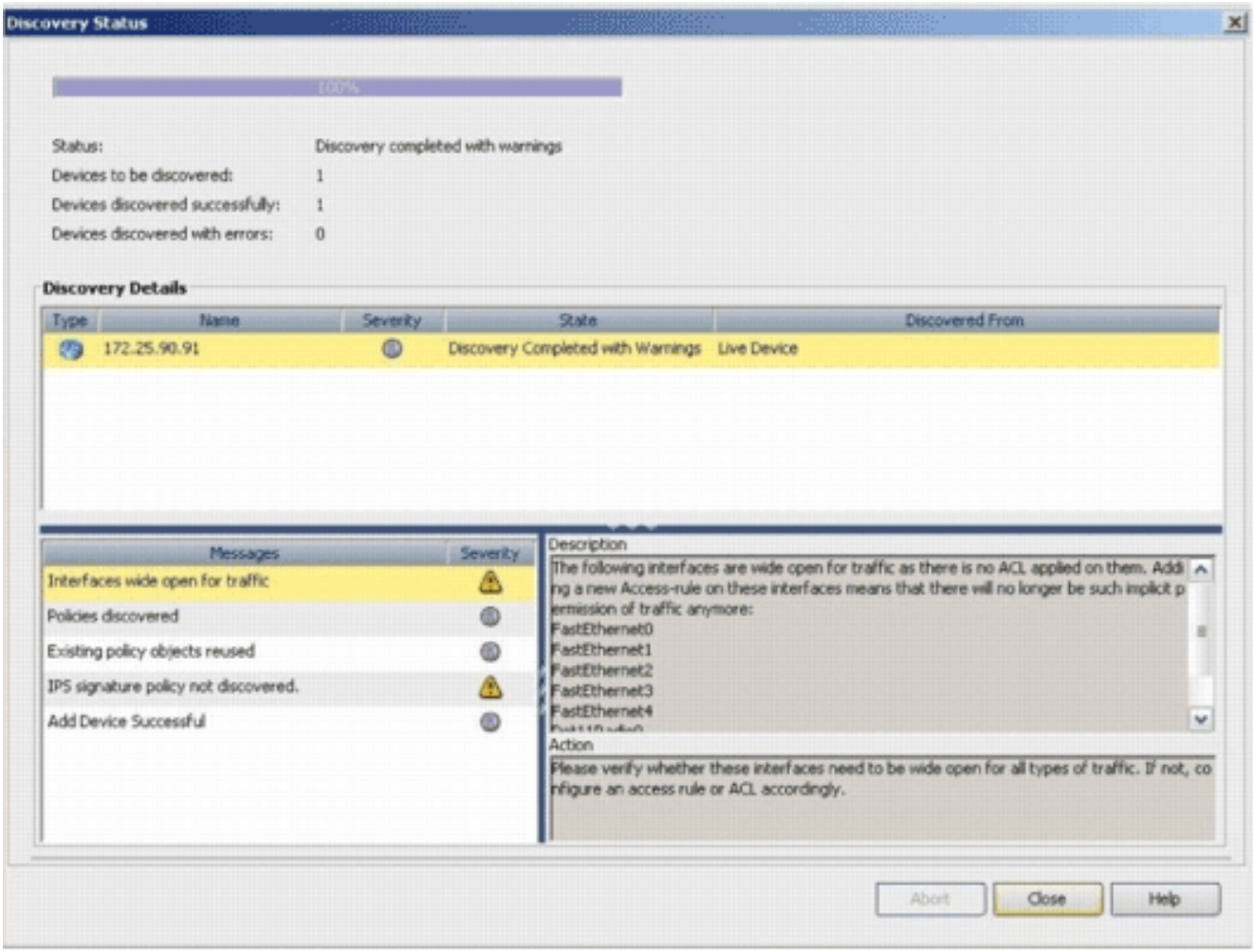
4. Klicken Sie auf **Weiter**.
5. Geben Sie die Identitätsdetails für das Gerät ein, das Sie hinzufügen möchten. Beispiel: Hostname und IP-
   Adresse.



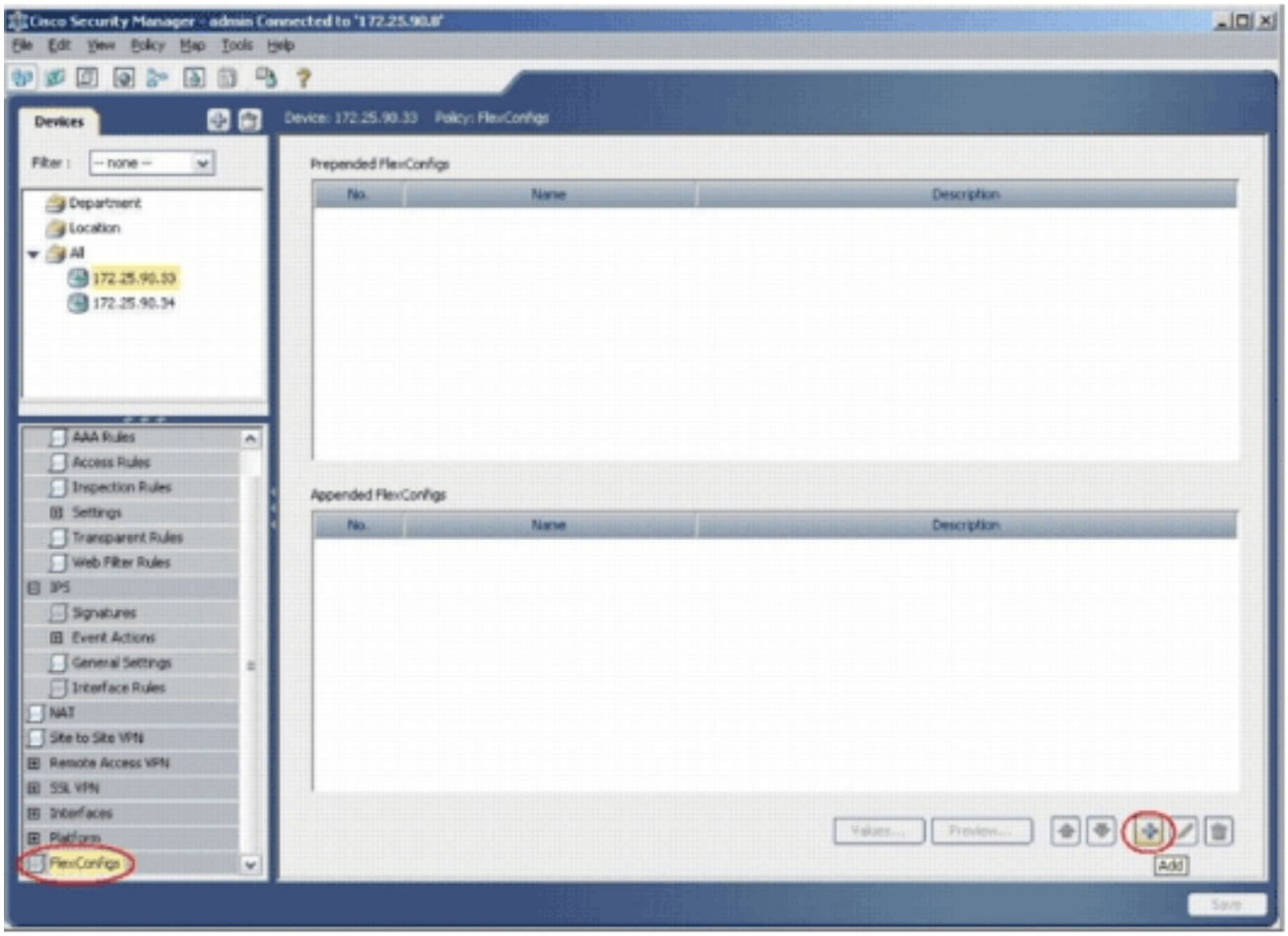
6. Klicken Sie auf **Weiter**.
7. Geben Sie die primären Anmeldeinformationen ein, z. B. Benutzername, Kennwort und Kennwort aktivieren für den IOS-Router, den Sie hinzufügen möchten.
8. Klicken Sie auf **Fertig stellen**, um das Gerät dem Cisco Security Manager hinzuzufügen.**Hinweis:** In diesem Beispiel wird davon ausgegangen, dass der Benutzer bereits über einen vorkonfigurierten Router verfügt und sich mit den entsprechenden Anmeldeinformationen beim Router anmelden
kann.



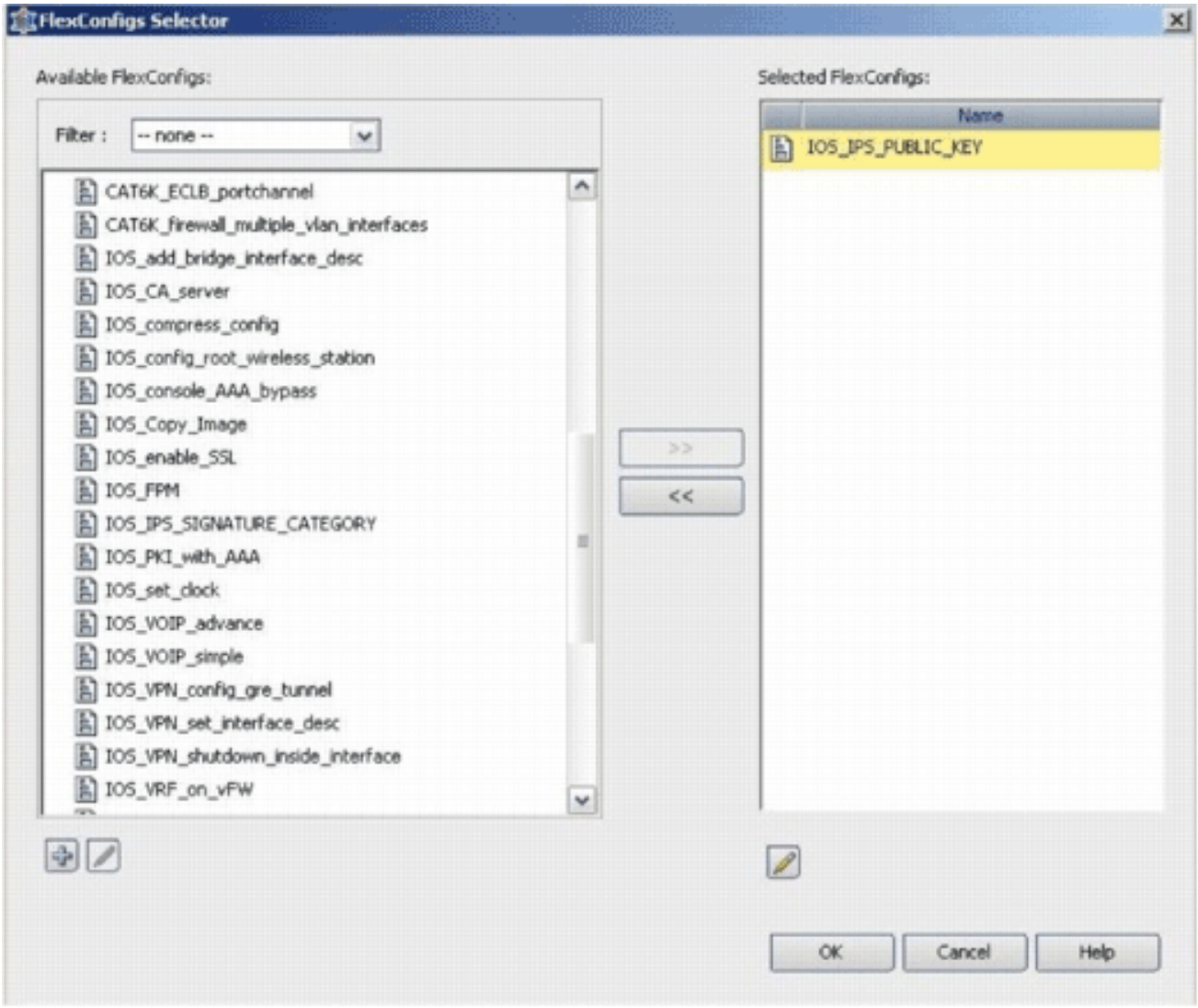
Wenn im Fenster "Discovery Status" (Erkennungsstatus) "Discovery completed" (Suche abgeschlossen) angezeigt wird, haben Sie dem Cisco Security Manager erfolgreich ein Gerät hinzugefügt. Wenn Sie dem Cisco Security Manager erfolgreich ein Gerät hinzugefügt haben, müssen Sie einen öffentlichen Schlüssel zuweisen, um IPS zu aktivieren.



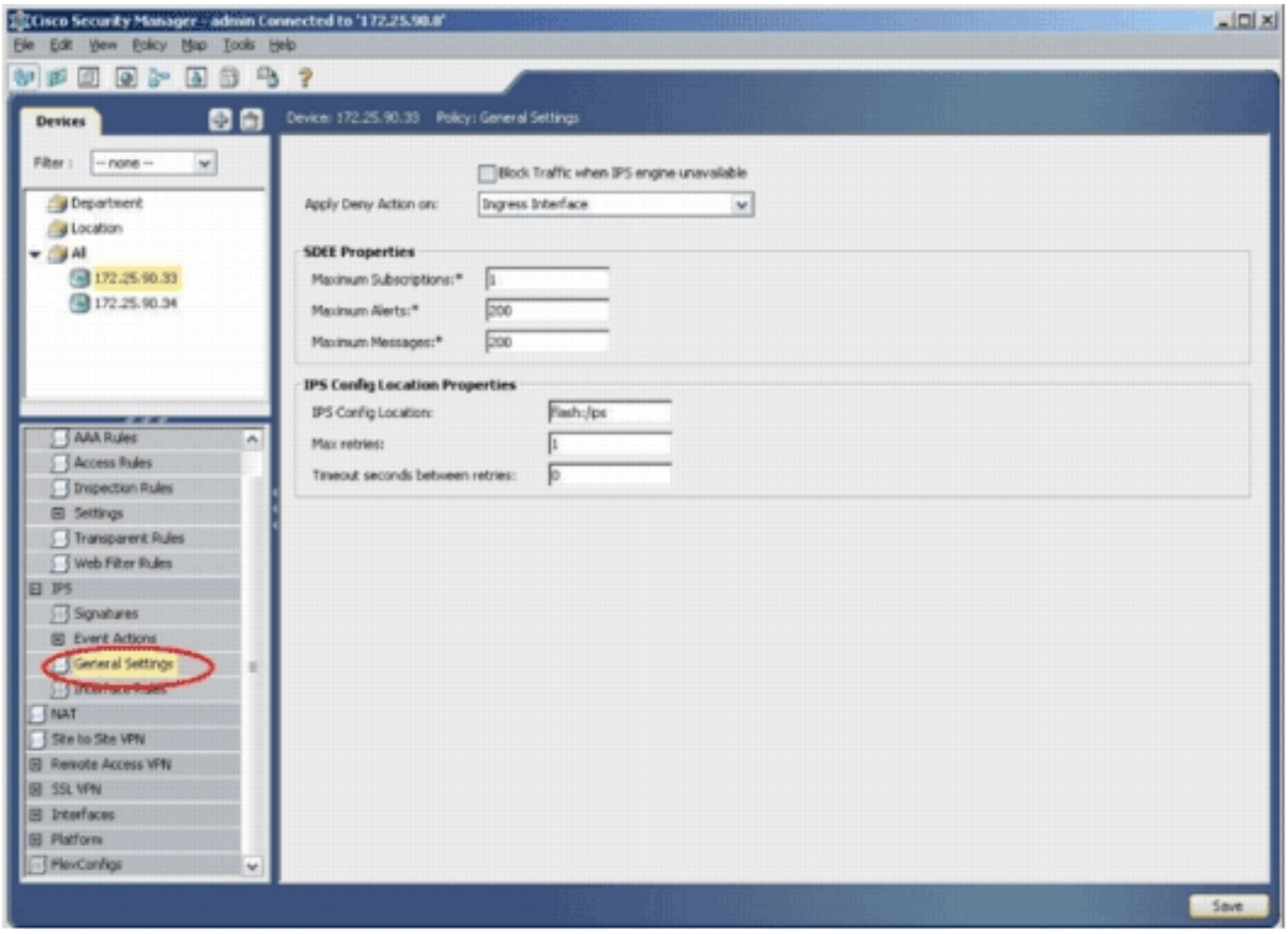
9. Navigieren Sie im Menü links zum Konfigurationsbildschirm FlexConfigs.
10. Klicken Sie auf der rechten Seite des Bildschirms auf die FlexConfigs-Benutzeroberfläche und anschließend auf das Symbol
    Hinzufügen.



11. Wählen Sie in der Liste "Ausgewählte FlexConfigs" die Option **IOS_IPS_PUBLIC_KEY aus**, und klicken Sie auf
OK.

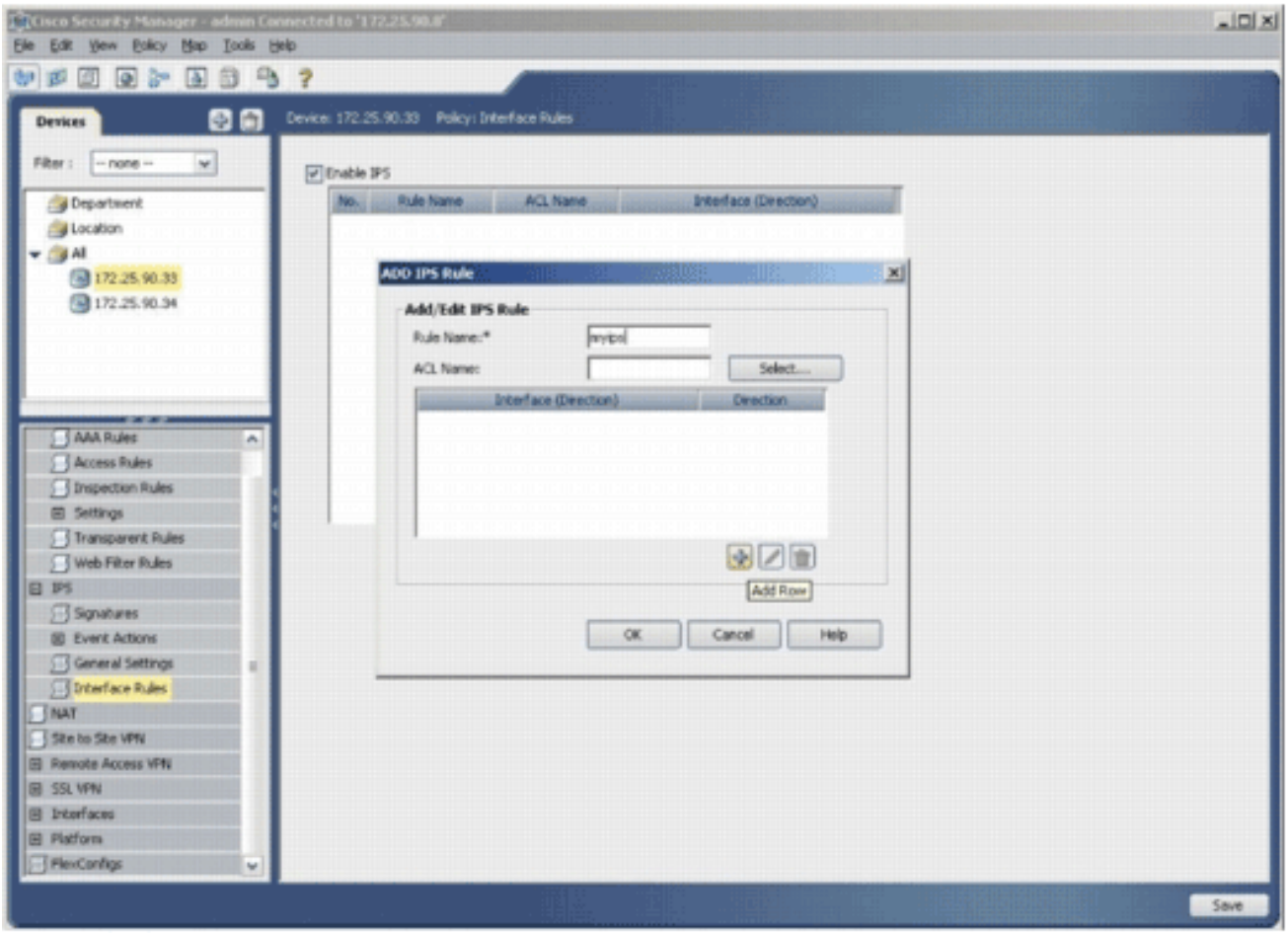


12. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.**Hinweis:** Die IOS_IPS_PUBLIC_KEY FlexConfig enthält die Konfiguration für den öffentlichen Schlüssel.
13. Wählen Sie im Menü auf der linken Seite die Option **General Settings (Allgemeine Einstellungen**) unter der Überschrift IPS aus.
14. Geben Sie den IPS-Konfigurationsstandort im Flash-Speicher ein. Dies ist der Ort, an dem die IPS-Konfigurationen platziert werden.
15. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

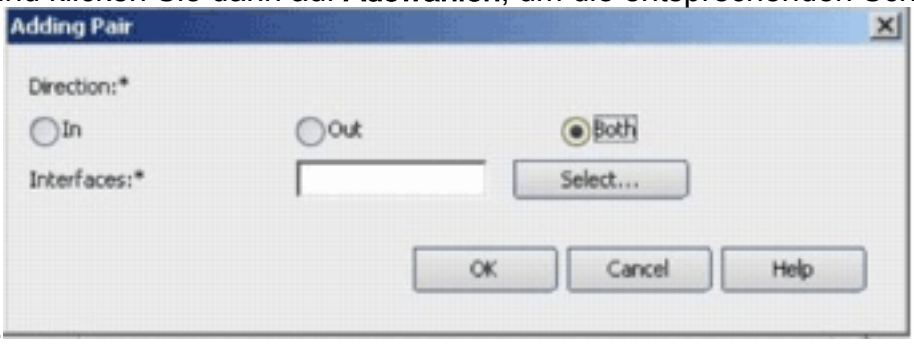


Hinweis: Stellen Sie sicher, dass das Verzeichnis für den Speicherort bereits im Router-Flash erstellt wurde. Falls nicht, verwenden Sie den Befehl **mkdir <directory_name>**, um das Verzeichnis location zu erstellen.

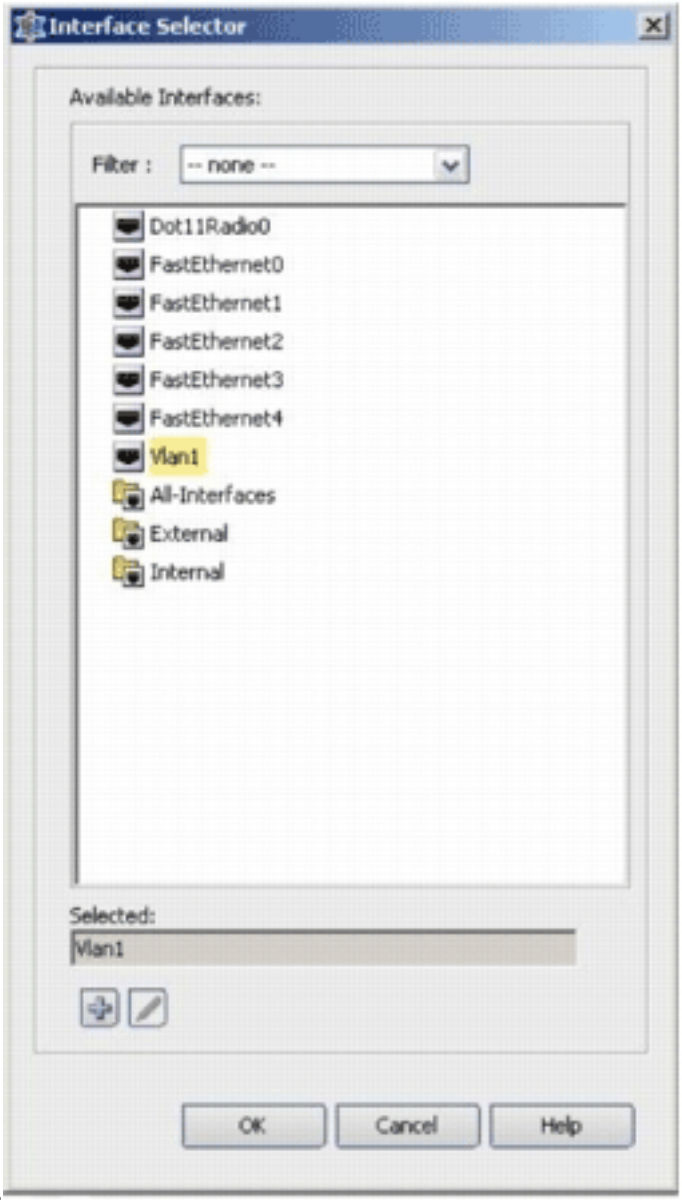
16. Um IPS zu aktivieren, navigieren Sie zu Schnittstellenregeln, aktivieren Sie das Kontrollkästchen **IPS aktivieren**, und klicken Sie dann auf **Zeile hinzufügen**.
17. Geben Sie im Dialogfeld IPS-Regel hinzufügen im Feld Regelname einen Namen für die IPS-Regel ein, und klicken Sie dann auf **Zeile hinzufügen**, um die Schnittstellen einzuschließen, auf die IPS angewendet werden soll.



18. Klicken Sie auf das Optionsfeld, das angibt, in welche Richtung die IPS-Regel angewendet werden soll, und klicken Sie dann auf **Auswählen**, um die entsprechenden Schnittstellen auszuwählen.

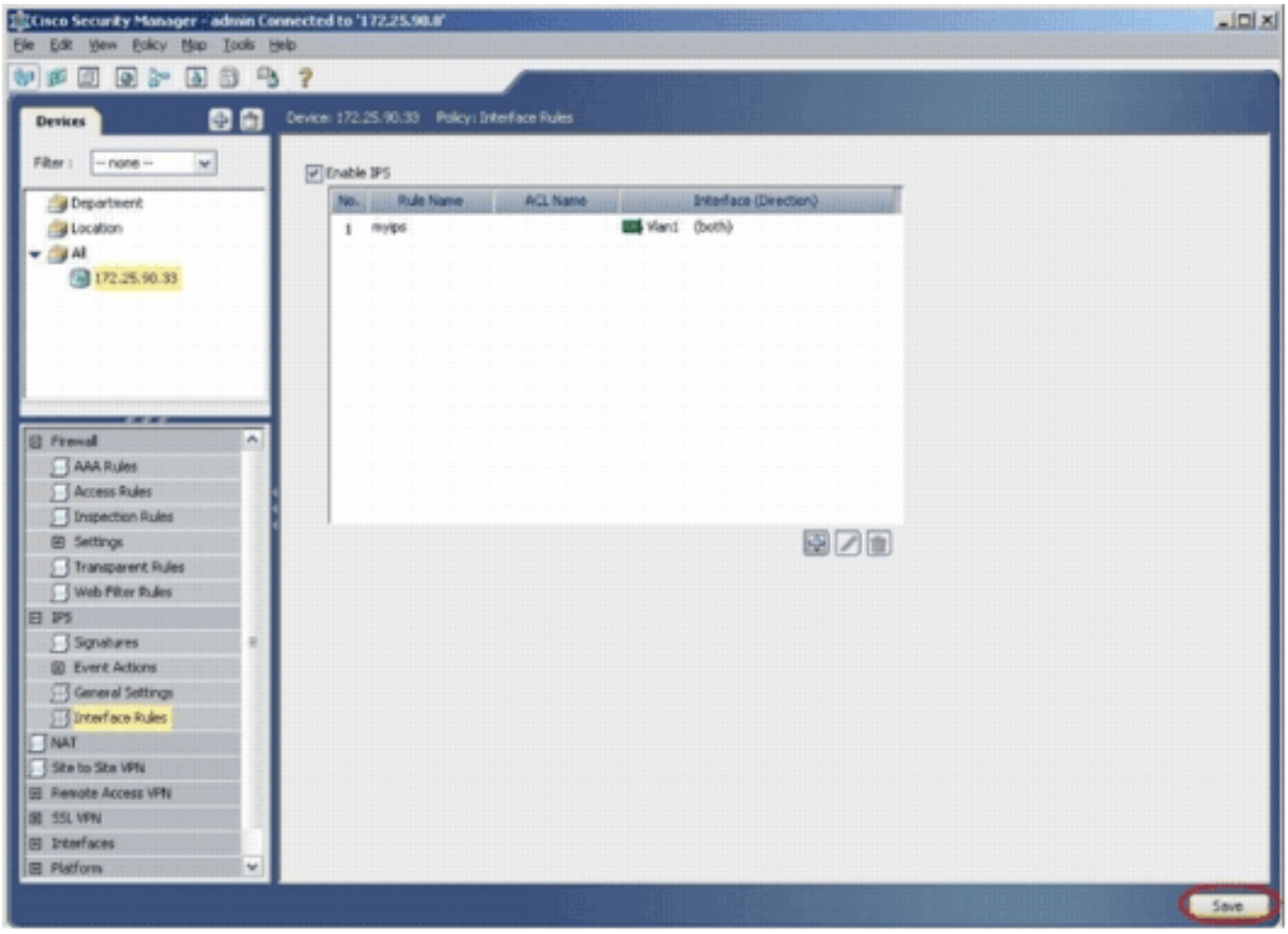


19. Wählen Sie eine Schnittstelle aus der Schnittstellenauswahl-Liste aus, und klicken Sie auf

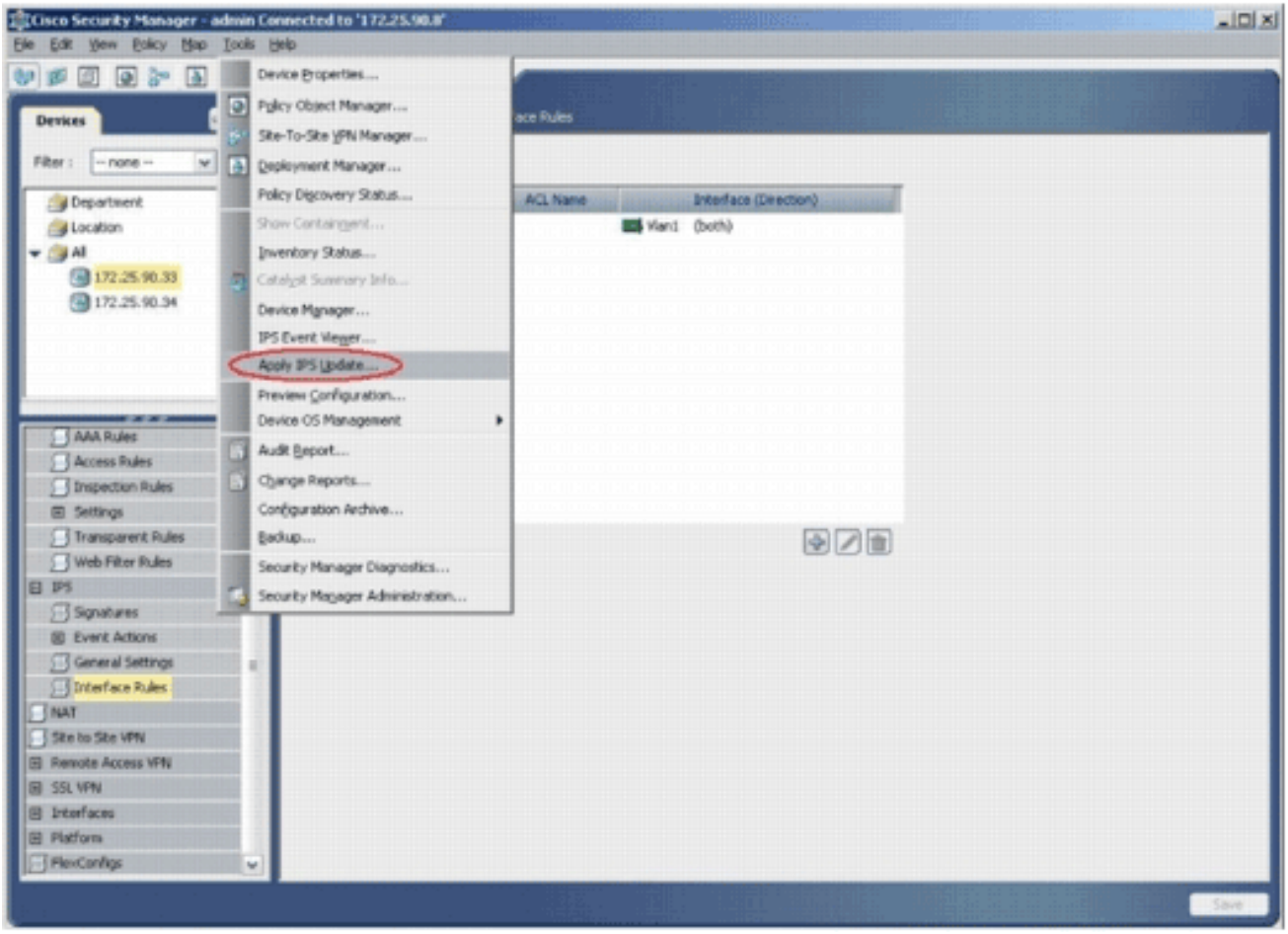


OK.

20. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

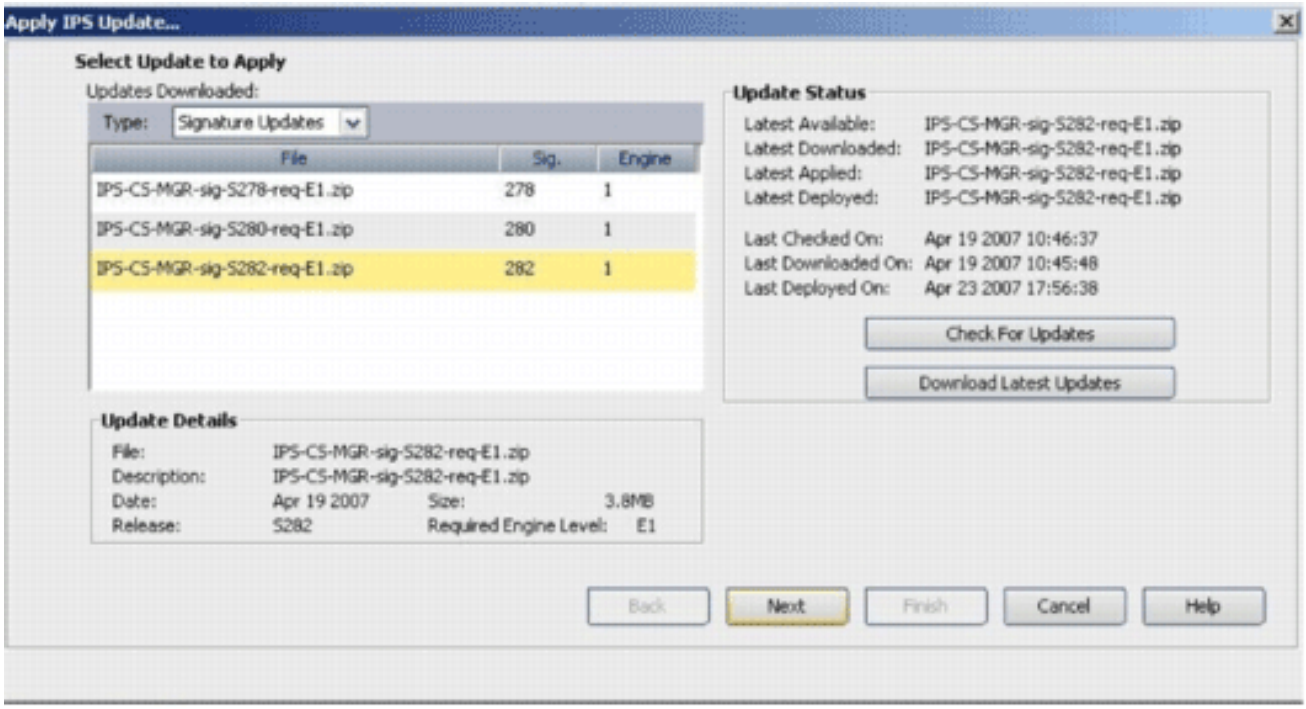


21. Wählen Sie **Extras > IPS-Update anwenden**, um die neuesten IPS-Signaturen zu installieren.

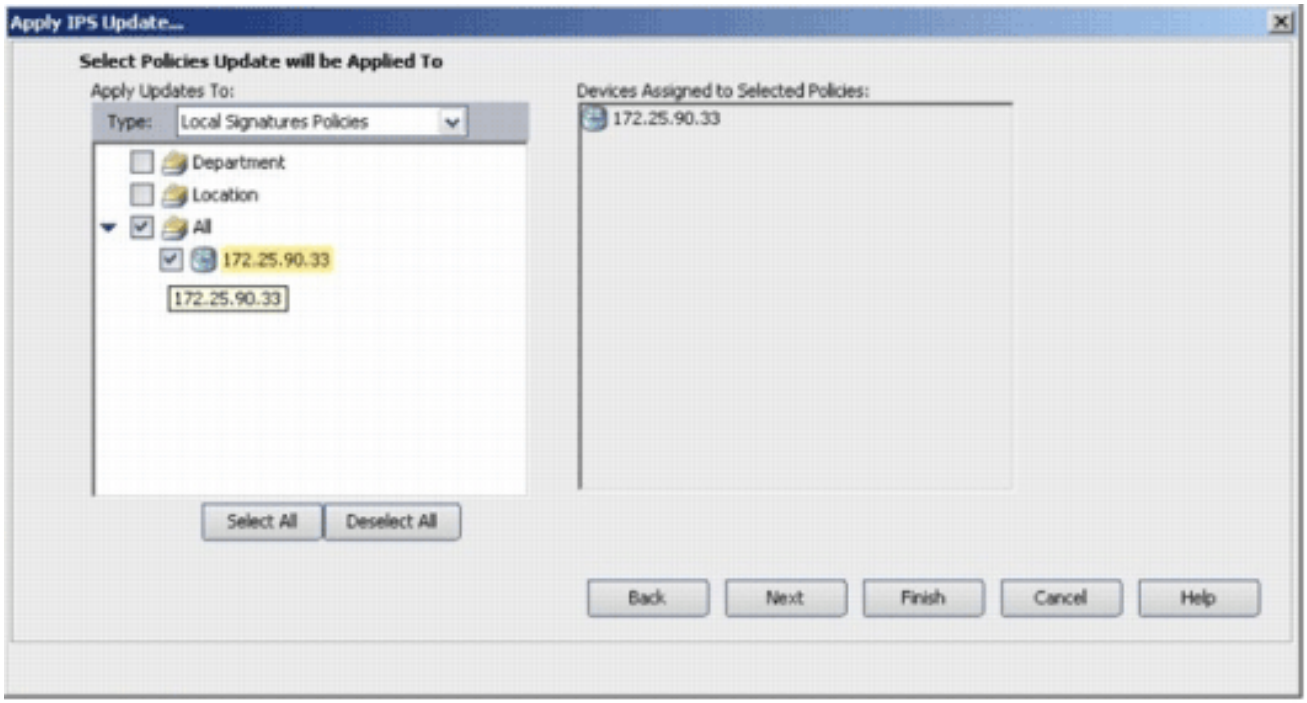


22. Wählen Sie die neueste Signaturdatei aus, und klicken Sie auf

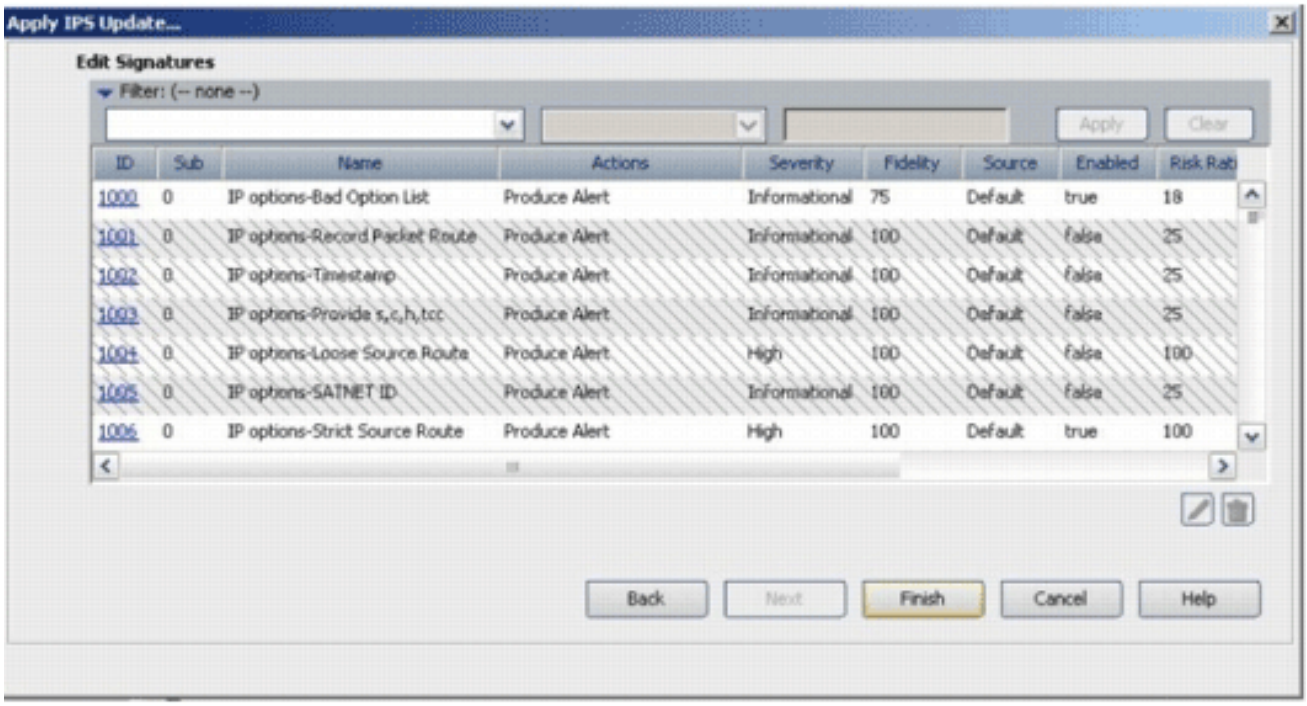
Weiter.



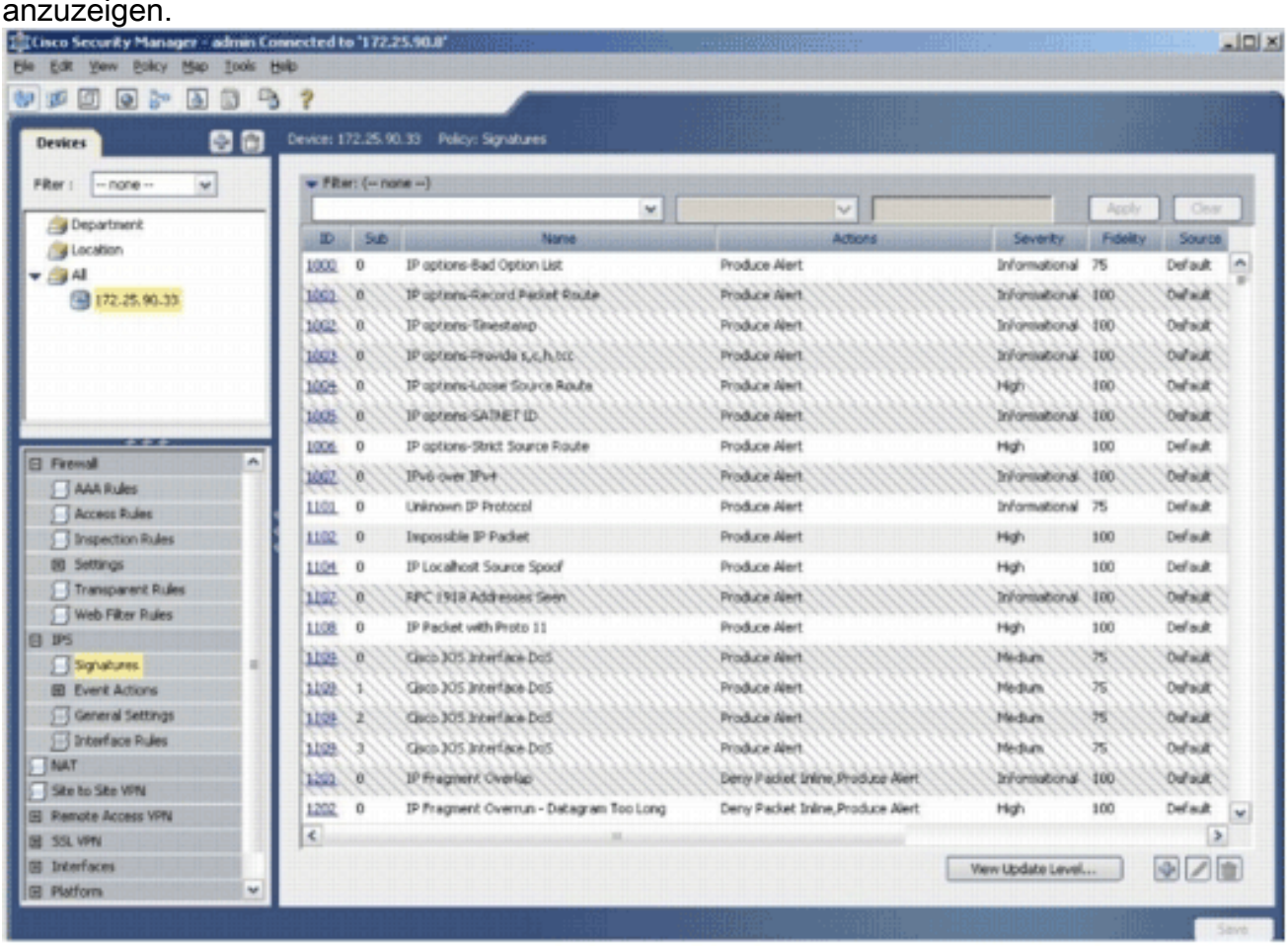
23. Wählen Sie die Geräte aus, auf die das IPS-Update angewendet werden soll, und klicken Sie auf **Weiter**.



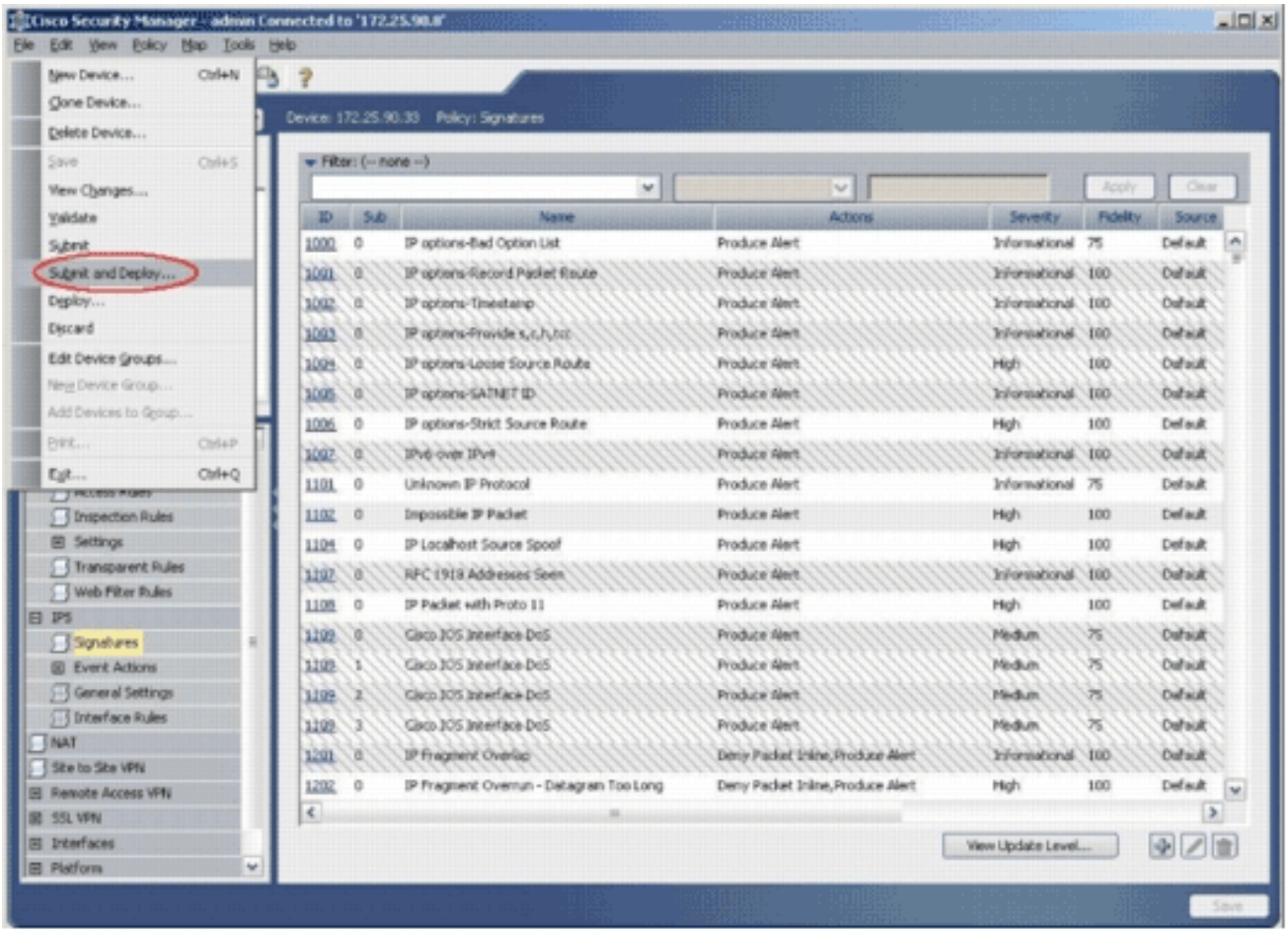
24. Klicken Sie auf **Fertig stellen**, um die Signaturen anzuwenden.



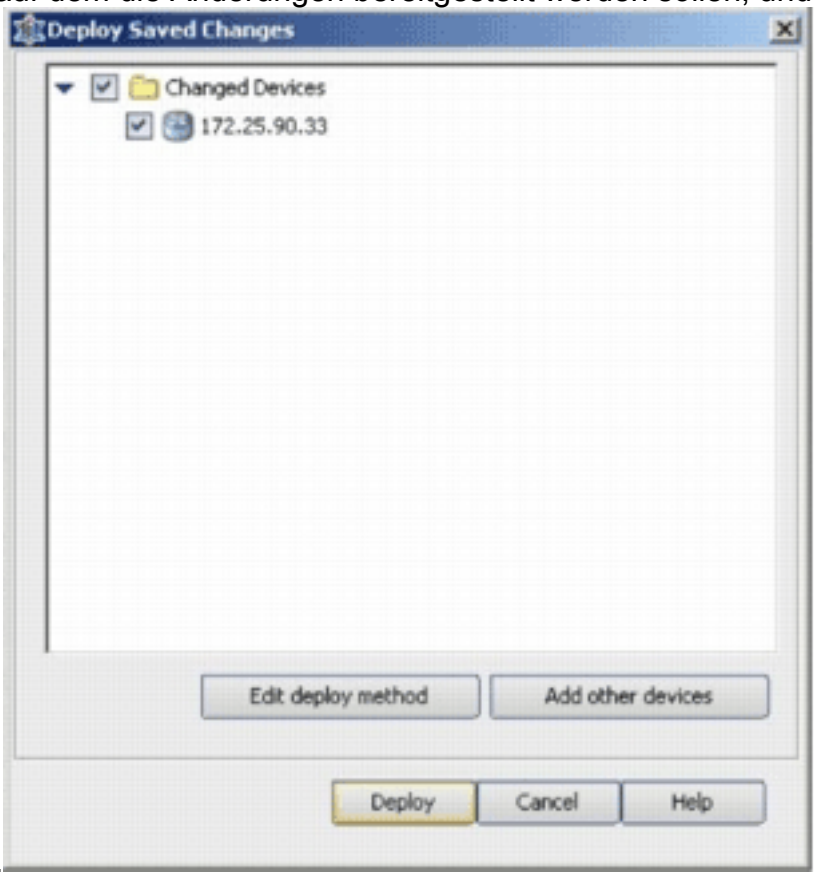
25. Navigieren Sie zu IPS, und wählen Sie **Signatures (Signaturen)** aus, um die Liste aller Signaturen
anzuzeigen.



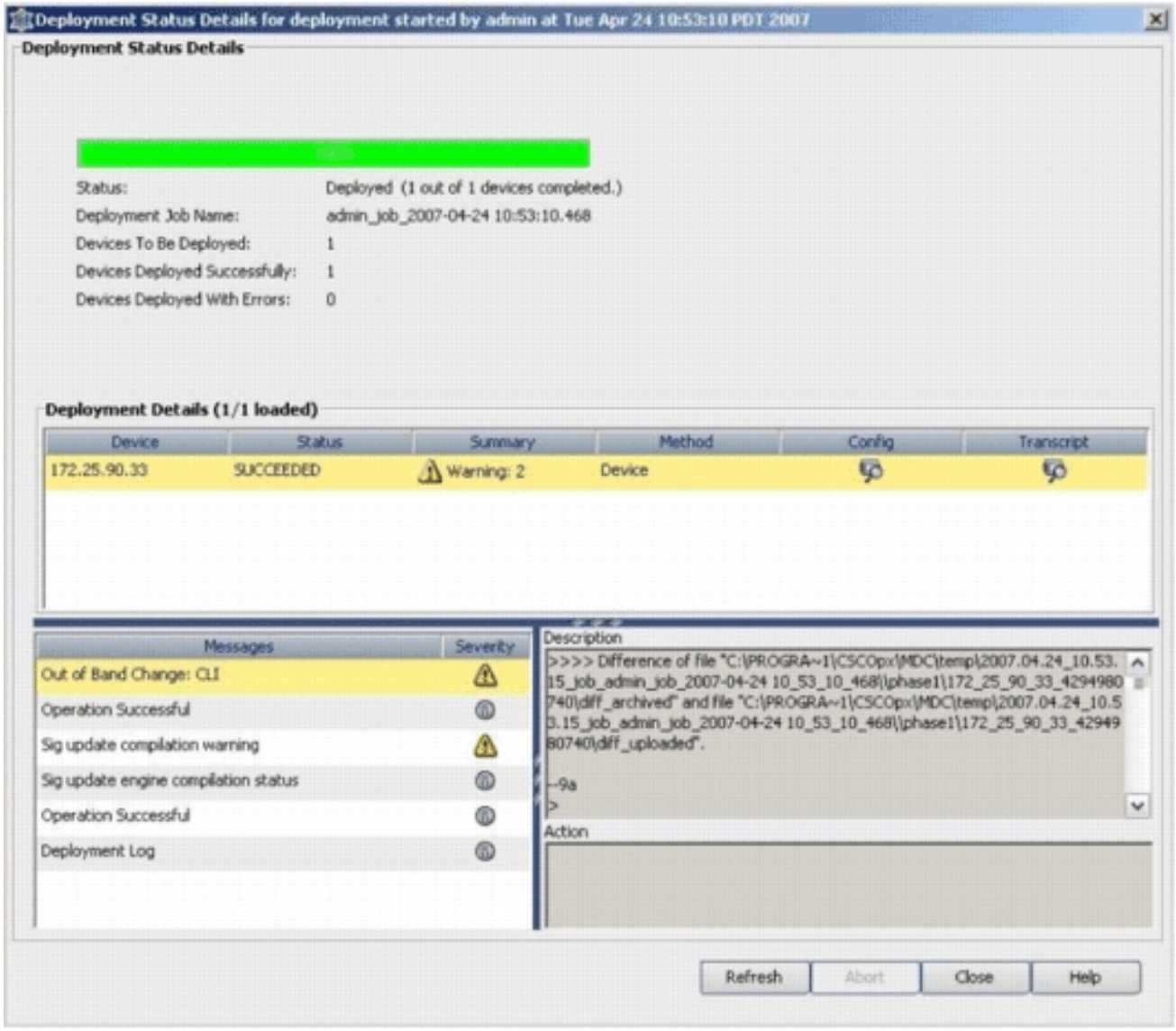
26. Wählen Sie **Datei > Senden und Bereitstellen**, um IPS auf dem IOS-Router bereitzustellen.



27. Wählen Sie das Gerät aus, auf dem die Änderungen bereitgestellt werden sollen, und klicken Sie auf **Bereitstellen**.



28. Zeigen Sie den Bereitstellungsstatus an, um zu überprüfen, ob Fehler vorliegen.



Zugehörige Informationen

- Cisco IOS Intrusion Prevention System (IPS) - Produkte und Services-Seite
- Erste Schritte mit Cisco IOS IPS mit 5.x-Signaturformat
- Unterstützung für IPS 5.x-Signaturformat und verbesserte Benutzerfreundlichkeit
- Cisco Intrusion Prevention System
- Problemhinweise zu Sicherheitsprodukten (einschließlich CiscoSecure Intrusion Detection)
- Technischer Support – Cisco Systems