Security Manager in Cisco IOS Intrusion Prevention System Configuration Example

Document ID: 105626

Contents

Introduction

Cisco Security Manager is part of the Cisco Security Management Suite, which delivers comprehensive policy administration and enforcement for the Cisco Self−Defending Network. Cisco Security Manager is an industry−leading enterprise−class application for managing security. Cisco Security Manager addresses configuration management of firewall, VPN, and Intrusion Prevention System (IPS) security services across Cisco routers, security appliances, and security services modules.

For a summary of Cisco Security Manager Features and benefits, as well as new features in version 3.1, refer to the Cisco Security Manager 3.1 data sheet at http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_data_sheet0900aecd8062bf6e.html. You can download Cisco Security Manager 3.1 from Cisco.com at http://www.cisco.com/cgi−bin/tablebuild.pl/csm−app (registered customers only) .

This document describes how to use Cisco Security Manager 3.1 in order to perform initial configuration of IOS IPS. For routers already configured with IOS IPS, customers can directly use Cisco Security Manager 3.1 for provisioning tasks.

Note: Cisco Security Manager 3.1 supports only IOS 12.4(11)T2 and later IOS images in order to configure IOS IPS.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

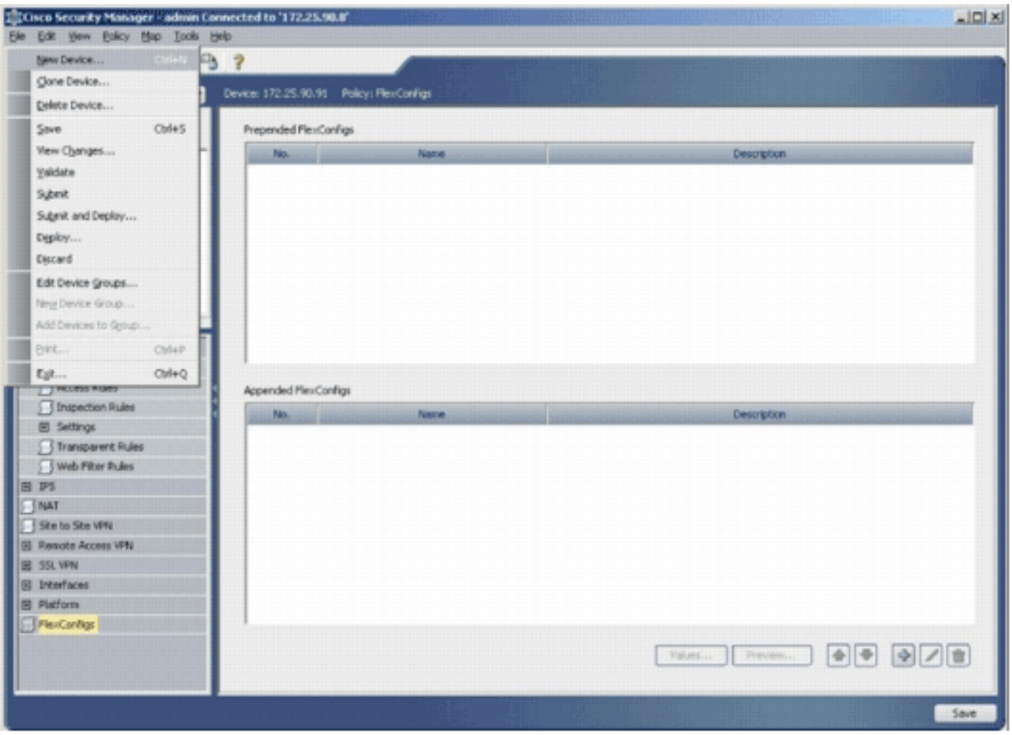
Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

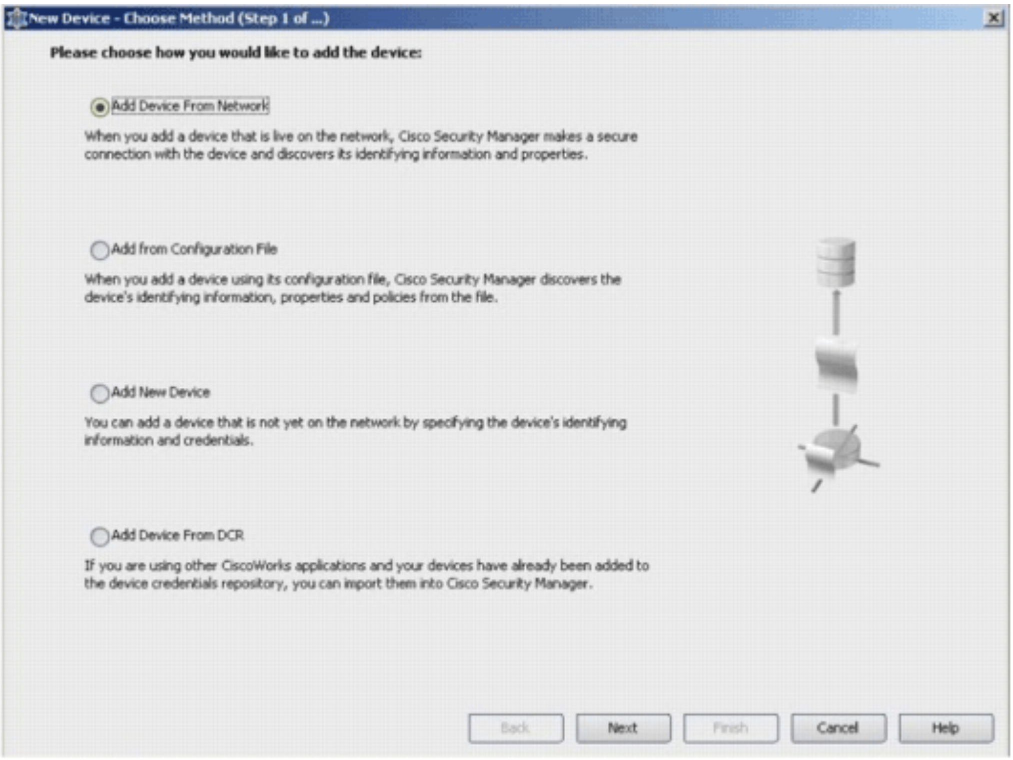
Configure

Complete these steps in order to configure IOS IPS:

1. Run the Cisco Security Manager 3.1 client from your local PC.
2. Choose **New Device** from the File menu in order to add a device onto the Cisco Security Manager 3.1.



3. In the New Device window, choose how you would like to add the device. This example adds the device from the network.



New Device - Choose Method (Step 1 of ...)

Please choose how you would like to add the device:

● Add Device From Network

When you add a device that is live on the network, Cisco Security Manager makes a secure connection with the device and discovers its identifying information and properties.

○ Add from Configuration File

When you add a device using its configuration file, Cisco Security Manager discovers the device's identifying information, properties and policies from the file.

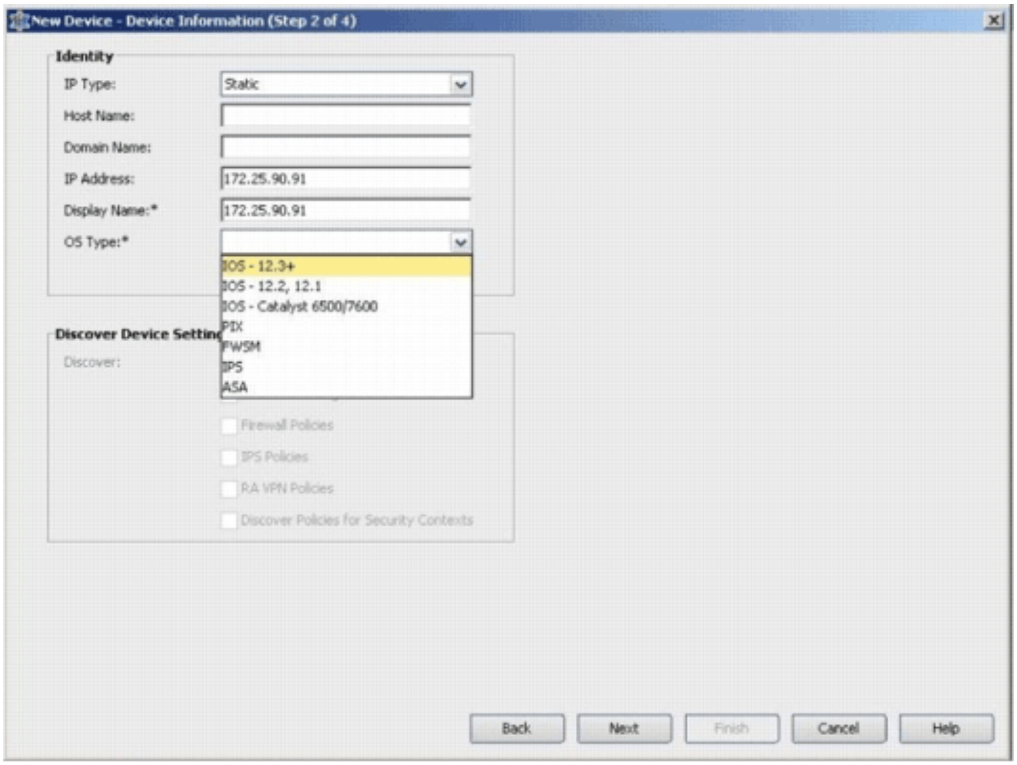
○ Add New Device

You can add a device that is not yet on the network by specifying the device's identifying information and credentials.

○ Add Device From DCR

If you are using other CiscoWorks applications and your devices have already been added to the device credentials repository, you can import them into Cisco Security Manager.

4. Click **Next**.
5. Enter the Identity details for the device that you want to add. For example, host name and IP address.



New Device - Device Information (Step 2 of 4)

Identity

IP Type: Static

Host Name:

Domain Name:

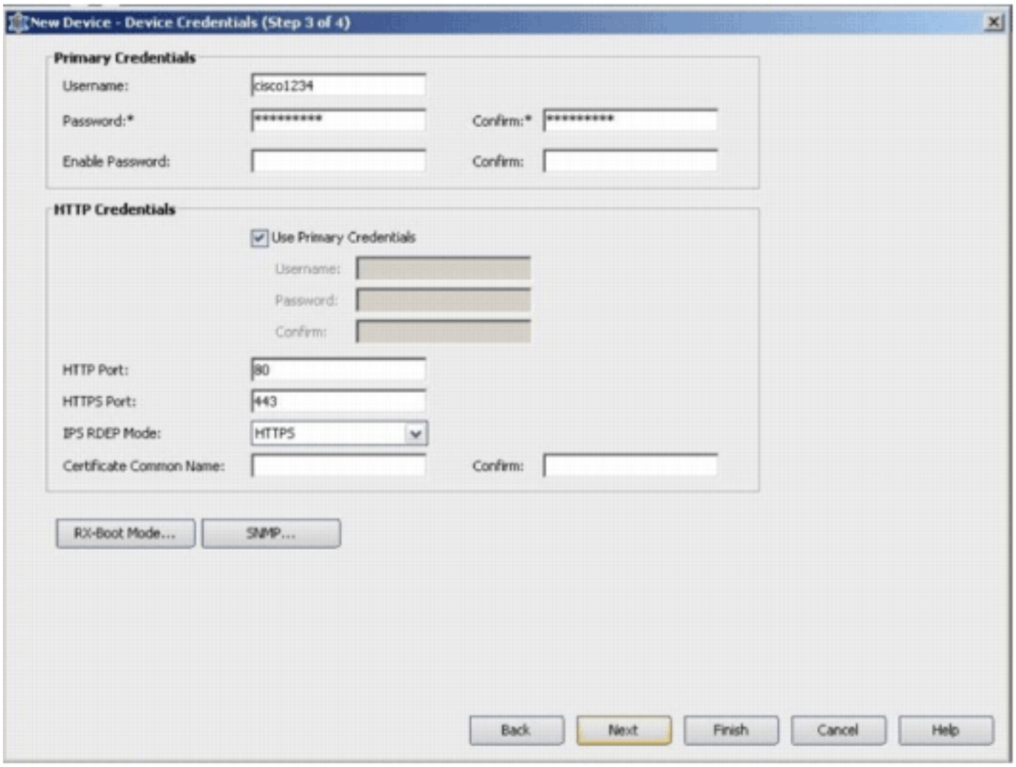
IP Address: 172.25.90.91

Display Name:* 172.25.90.91

OS Type:*

6. Click **Next**.
7. Enter the primary credentials, such as user name, password, Enable password for the IOS Router which you want to add.
8. Click **Finish** in order to add the device onto Cisco Security Manager.

   Note: This example assume that the user already has a preconfigured router and can log in to the router with the proper credentials.



New Device - Device Credentials (Step 3 of 4)

Primary Credentials

Username: cisco1234

Password:* ********** Confirm:* **********

Enable Password: Confirm:

HTTP Credentials

☑ Use Primary Credentials

Username:

Password:

Confirm:

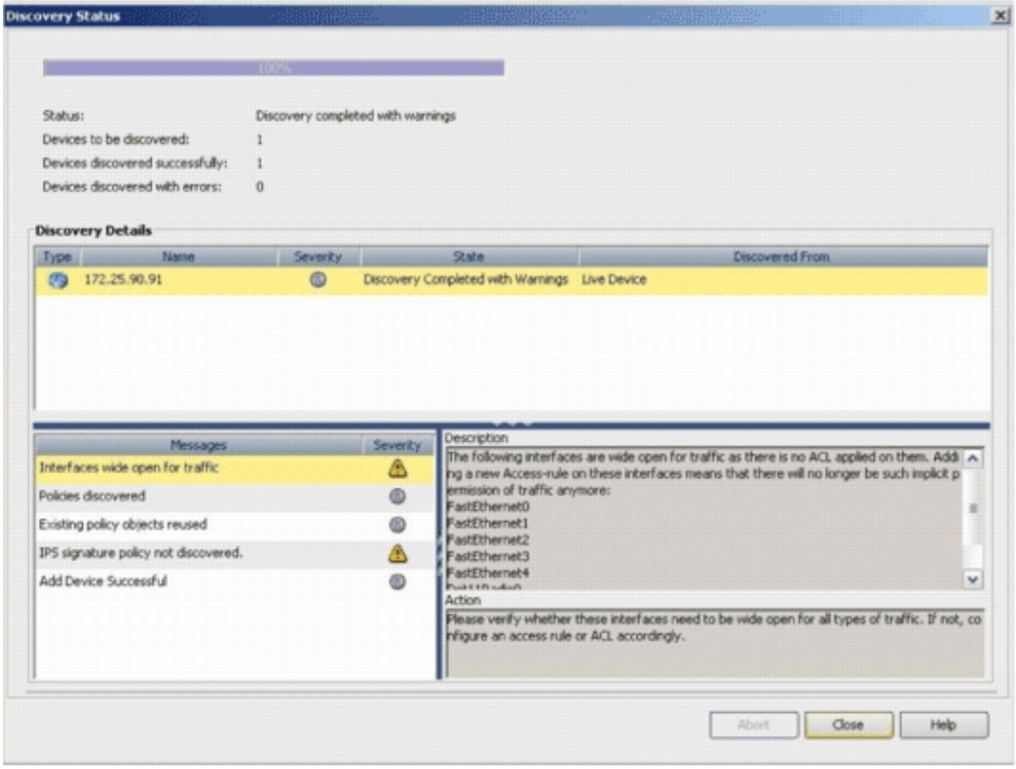
HTTP Port: 80

HTTPS Port: 443

IPS RDEP Mode: HTTPS

Certificate Common Name: Confirm:

When "Discovery completed" appears in the Discovery Status window, you have successfully added a device onto the Cisco Security Manager. Once you have successfully added a device onto the Cisco Security Manager, you must assign a public key in order to enable IPS.



Discovery Status

100%

Status: Discovery completed with warnings

Devices to be discovered: 1

Devices discovered successfully: 1

Devices discovered with errors: 0

Discovery Details

Type	Name	Severity	State	Discovered From
	172.25.90.91		Discovery Completed with Warnings	Live Device

Messages	Severity
Interfaces wide open for traffic	⚠
Policies discovered	●
Existing policy objects reused	●
IPS signature policy not discovered.	⚠
Add Device Successful	●

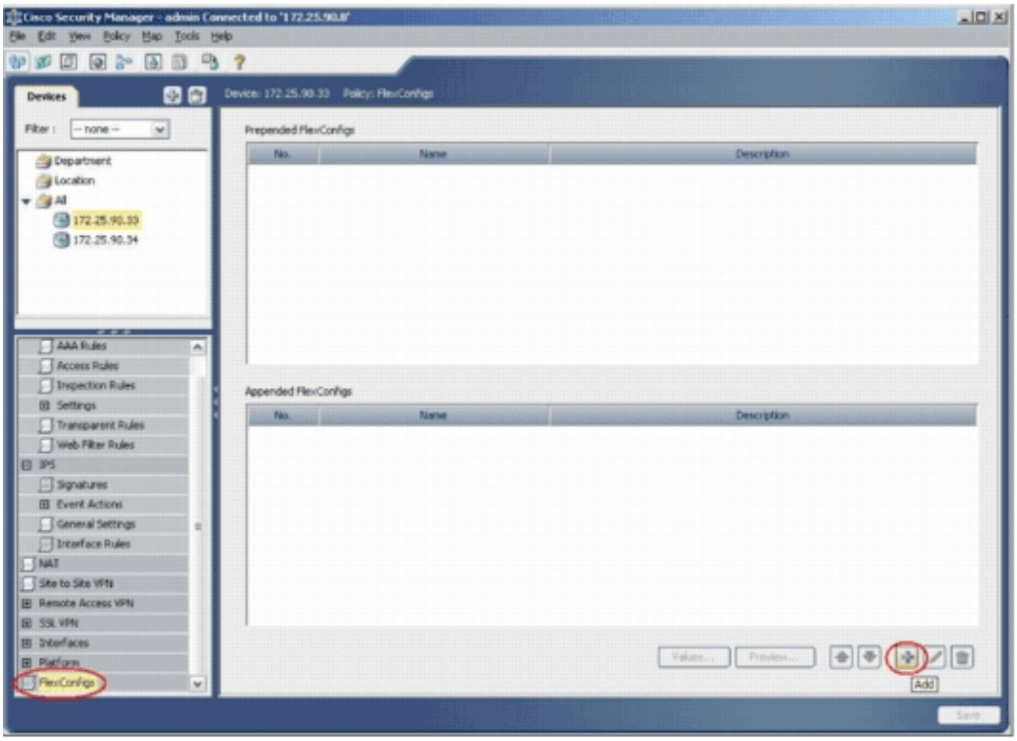
Description

The following interfaces are wide open for traffic as there is no ACL applied on them. Adding a new Access-rule on these interfaces means that there will no longer be such implicit permission of traffic anymore:
FastEthernet0
FastEthernet1
FastEthernet2
FastEthernet3
FastEthernet4

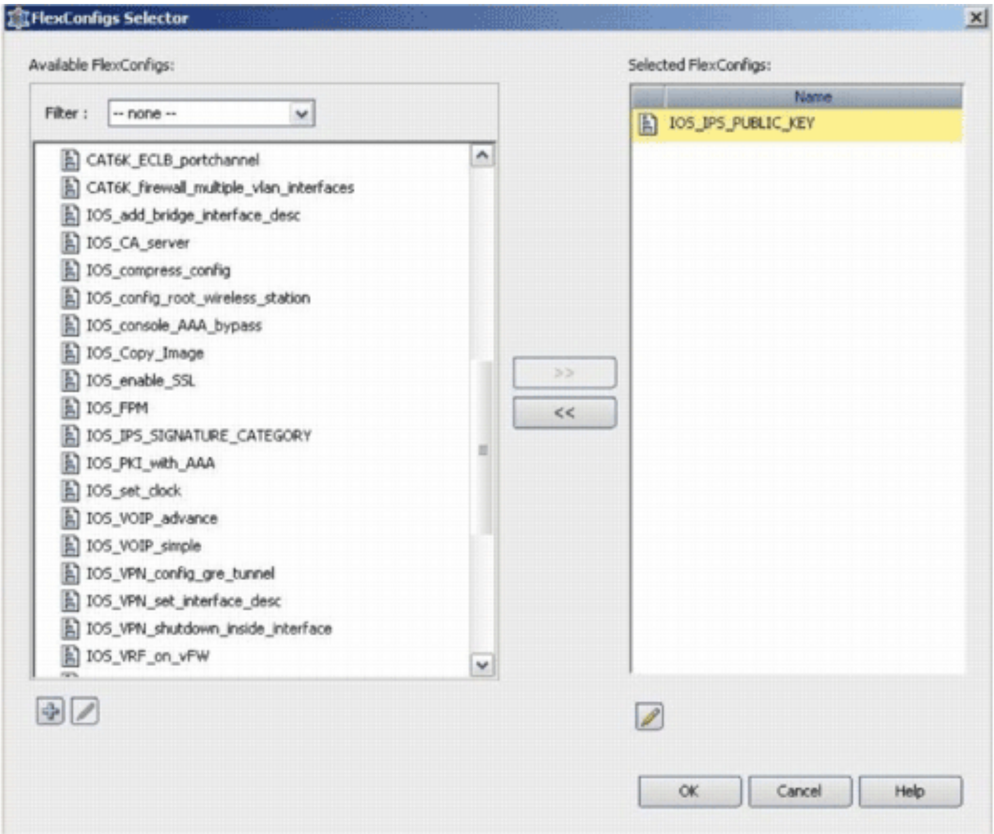
Action

Please verify whether these interfaces need to be wide open for all types of traffic. If not, configure an access rule or ACL accordingly.

9. From the menu on the left, navigate to the FlexConfigs configuration screen.
10. Click the FlexConfigs user interface on the right side of the screen, and then click the **Add** icon.

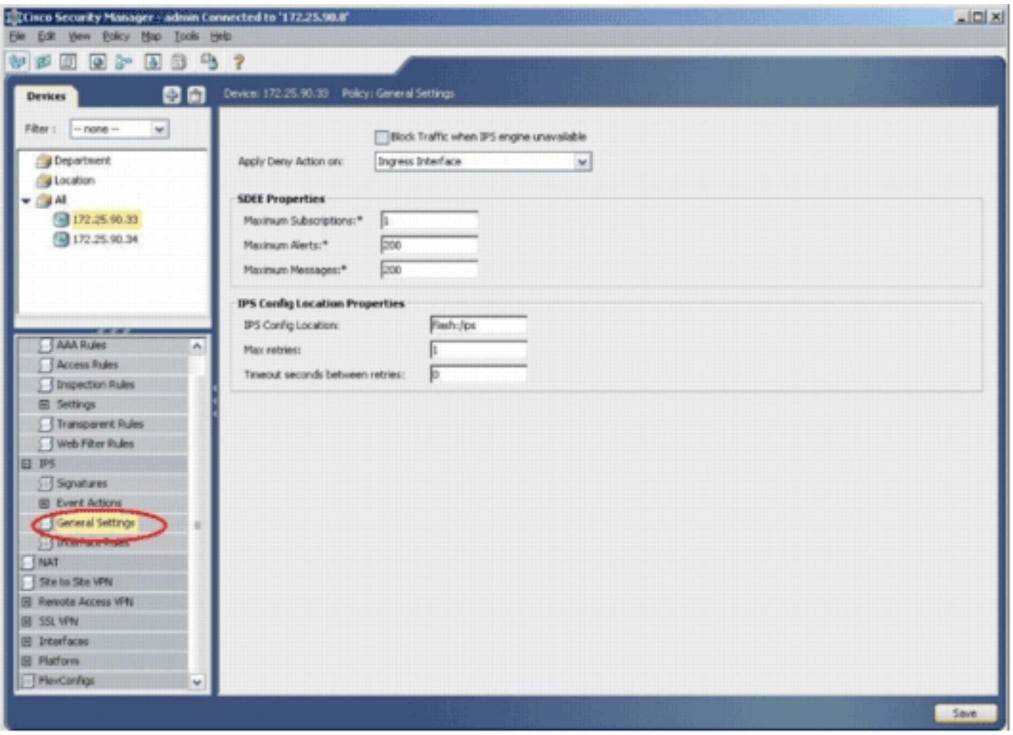


11. In the Selected FlexConfigs list, choose **IOS_IPS_PUBLIC_KEY**, and click **OK**.



12. Click **Save** in order to save the changes.

    Note: The IOS_IPS_PUBLIC_KEY FlexConfig holds the configuration for the public key.
13. From the menu on the left, choose **General Settings** located beneath the IPS heading.
14. Enter the IPS configuration location on the flash. This is the location in which the IPS configurations are placed.
15. Click **Save** in order to save the changes.



Device: 172.25.90.33 Policy: General Settings

□ Block Traffic when IPS engine unavailable

Apply Deny Action on: Ingress Interface

SDEE Properties

Maximum Subscriptions:* 1

Maximum Alerts:* 200

Maximum Messages:* 200

IPS Config Location Properties

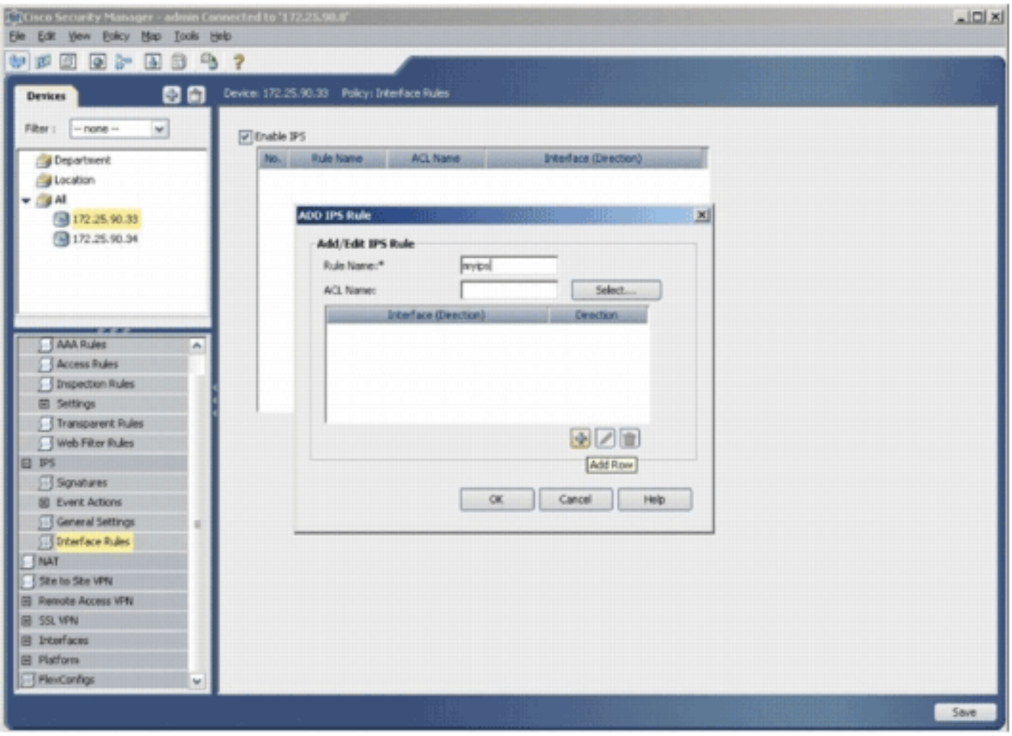
IPS Config Location: flash:/ips

Max retries: 1

Timeout seconds between retries: 0

Note: Make sure the location directory has already been created on router flash. If not, use the **mkdir <directory_name>** command in order to create the location directory.

16. In order to enable IPS, navigate to Interface Rules, check the **Enable IPS** check box, and then click **Add Row**.
17. In the Add IPS Rule dialog box, enter a name for the IPS rule in the Rule Name field, and then click **Add Row** in order to include the interfaces on which IPS must be applied.



Device: 172.25.90.33 Policy: Interface Rules

☑ Enable IPS

No.	Rule Name	ACL Name	Interface (Direction)

ADD IPS Rule

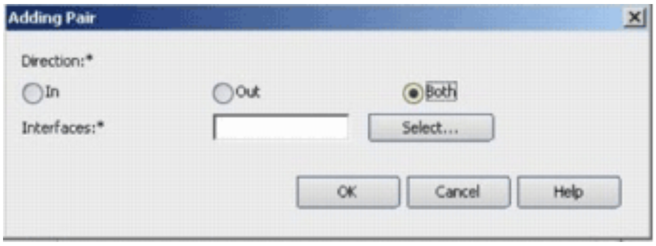
Add/Edit IPS Rule

Rule Name:* myips

ACL Name:

Interface (Direction)	Direction

18. Click the radio button that indicates in which direction the IPS rule must be applied, and then click **Select** in order to choose the appropriate interfaces.



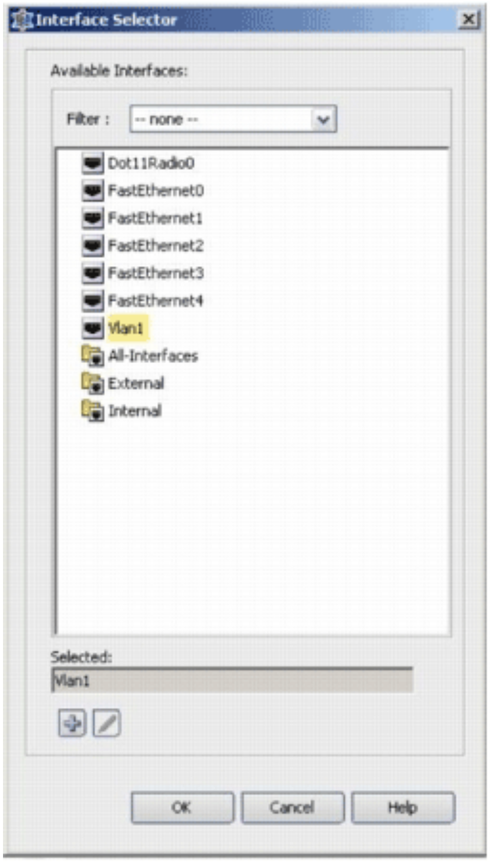
Adding Pair

Direction:*

○ In ○ Out ● Both

Interfaces:*

19. Choose an interface from the Interface Selector list, and click **OK**.



Interface Selector

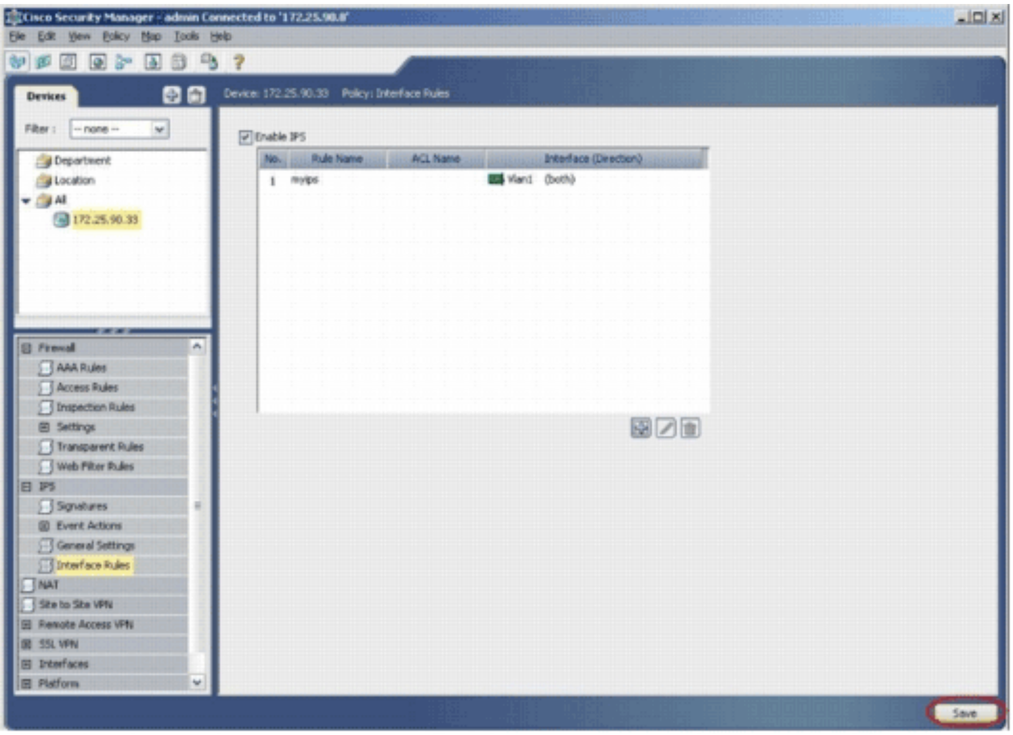
Available Interfaces:

Filter : -- none --

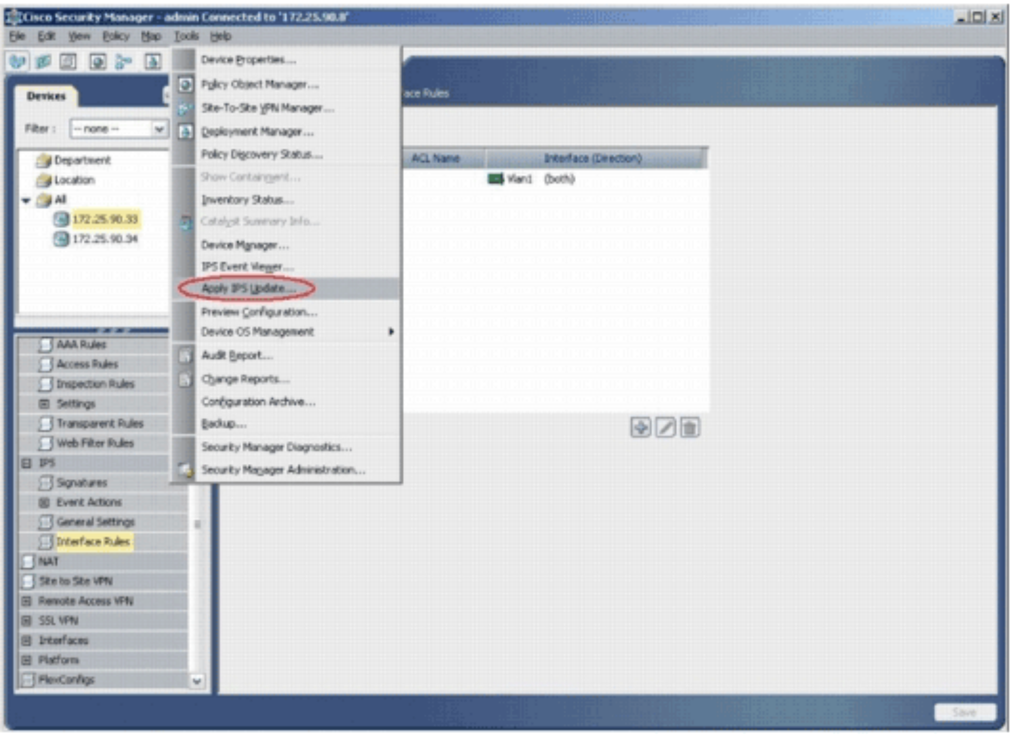
- Dot11Radio0
- FastEthernet0
- FastEthernet1
- FastEthernet2
- FastEthernet3
- FastEthernet4
- Vlan1
- All-Interfaces
- External
- Internal

Selected: Vlan1

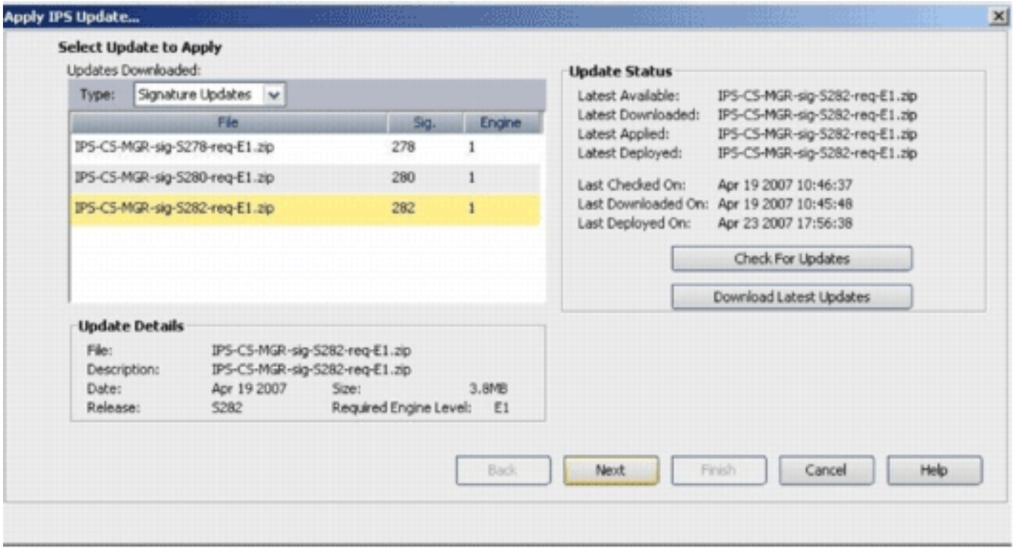
20. Click **Save** in order to save the changes.



21. Choose **Tools > Apply IPS Update** in order to install the latest IPS signatures.



22. Choose the latest signature file, and click **Next**.



Select Update to Apply

Updates Downloaded:

Type: Signature Updates

File	Sig.	Engine
IPS-CS-MGR-sig-S278-req-E1.zip	278	1
IPS-CS-MGR-sig-S280-req-E1.zip	280	1
IPS-CS-MGR-sig-S282-req-E1.zip	282	1

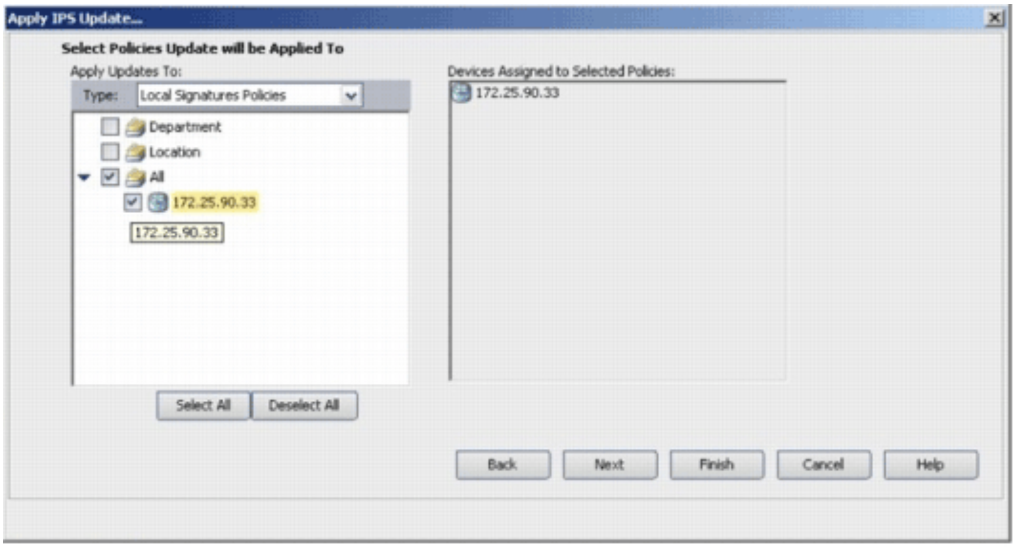
Update Status

Latest Available:	IPS-CS-MGR-sig-S282-req-E1.zip
Latest Downloaded:	IPS-CS-MGR-sig-S282-req-E1.zip
Latest Applied:	IPS-CS-MGR-sig-S282-req-E1.zip
Latest Deployed:	IPS-CS-MGR-sig-S282-req-E1.zip
Last Checked On:	Apr 19 2007 10:46:37
Last Downloaded On:	Apr 19 2007 10:45:48
Last Deployed On:	Apr 23 2007 17:56:38

Update Details

File:	IPS-CS-MGR-sig-S282-req-E1.zip		
Description:	IPS-CS-MGR-sig-S282-req-E1.zip		
Date:	Apr 19 2007	Size:	3.8MB
Release:	S282	Required Engine Level:	E1

23. Choose the devices on which the IPS update must be applied, and click **Next**.



Select Policies Update will be Applied To

Apply Updates To:

Type: Local Signatures Policies

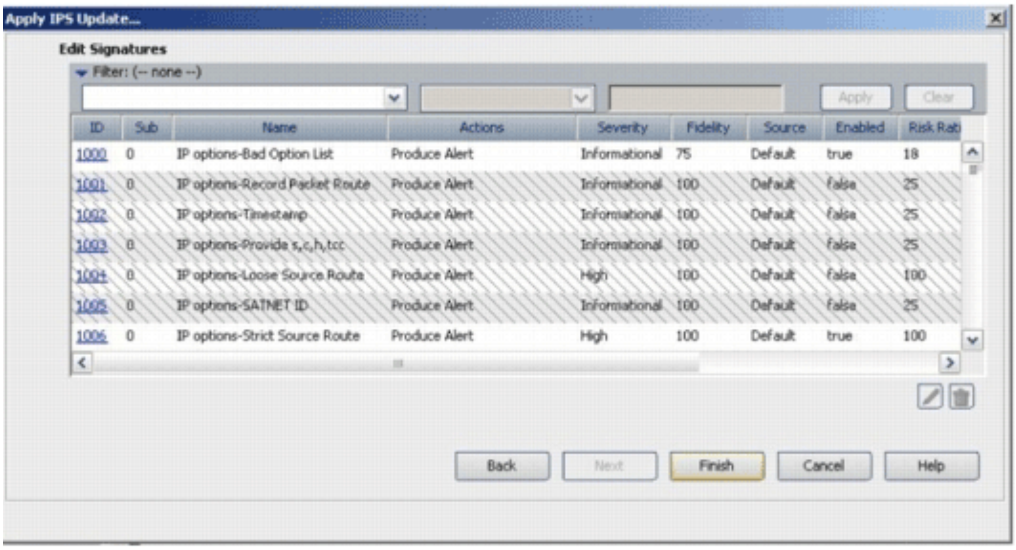
- □ Department
- □ Location
- ☑ All
  - ☑ 172.25.90.33

172.25.90.33

Devices Assigned to Selected Policies:

172.25.90.33

24. Click **Finish** in order to apply the signatures.

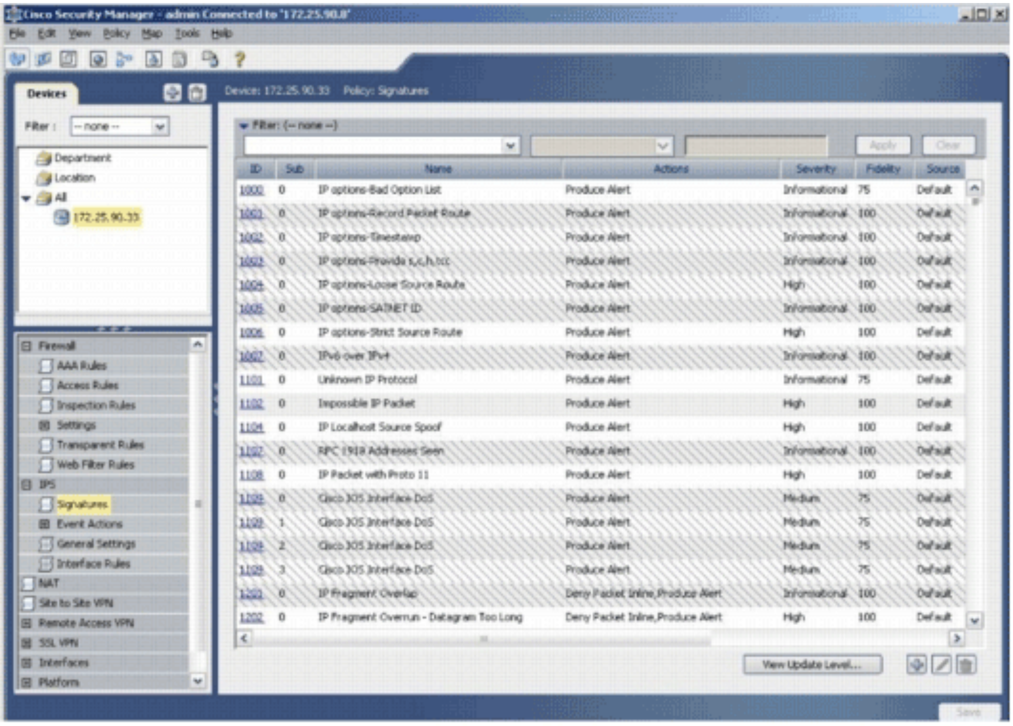


Edit Signatures

Filter: (-- none --)

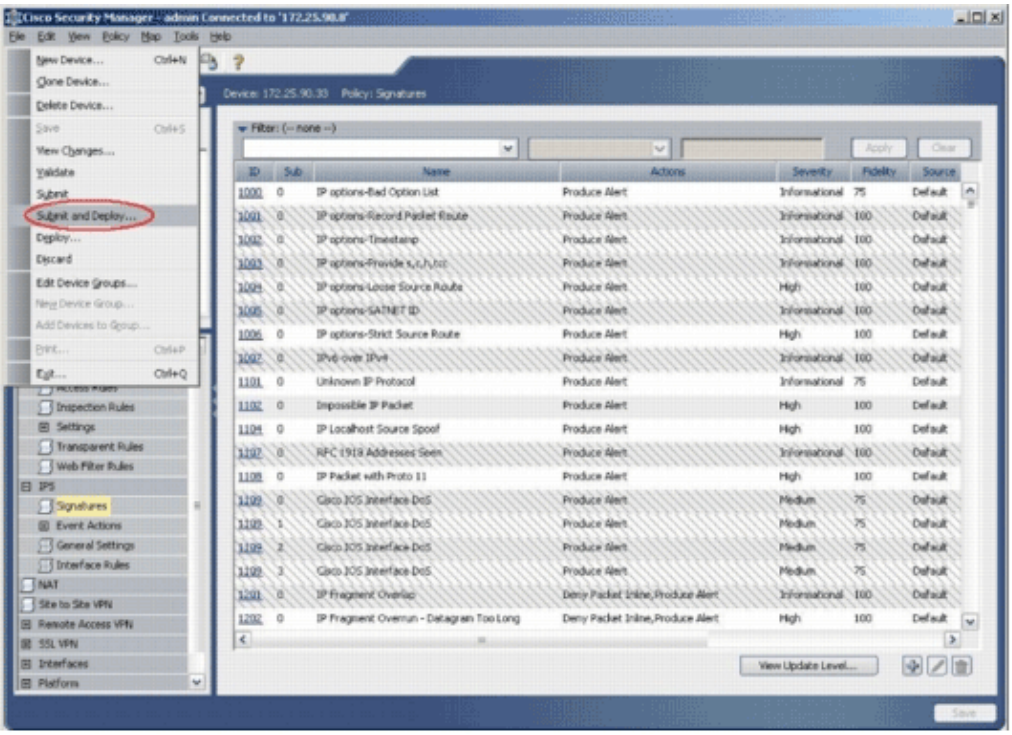
ID	Sub	Name	Actions	Severity	Fidelity	Source	Enabled	Risk Rat
1000	0	IP options-Bad Option List	Produce Alert	Informational	75	Default	true	18
1001	0	IP options-Record Packet Route	Produce Alert	Informational	100	Default	false	25
1002	0	IP options-Timestamp	Produce Alert	Informational	100	Default	false	25
1003	0	IP options-Provide s,c,h,tcc	Produce Alert	Informational	100	Default	false	25
1004	0	IP options-Loose Source Route	Produce Alert	High	100	Default	false	100
1005	0	IP options-SATNET ID	Produce Alert	Informational	100	Default	false	25
1006	0	IP options-Strict Source Route	Produce Alert	High	100	Default	true	100

25. Navigate to IPS, and choose **Signatures** in order to view the list of all the signatures.



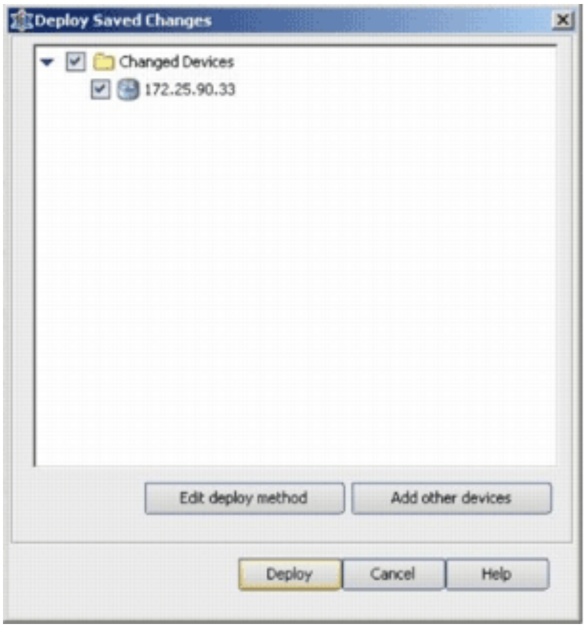
ID	Sub	Name	Actions	Severity	Fidelity	Source
1000	0	IP options-Bad Option List	Produce Alert	Informational	75	Default
1001	0	IP options-Record Packet Route	Produce Alert	Informational	100	Default
1002	0	IP options-Timestamp	Produce Alert	Informational	100	Default
1003	0	IP options-Provide s,c,h,tcc	Produce Alert	Informational	100	Default
1004	0	IP options-Loose Source Route	Produce Alert	High	100	Default
1005	0	IP options-SATNET ID	Produce Alert	Informational	100	Default
1006	0	IP options-Strict Source Route	Produce Alert	High	100	Default
1007	0	IPv6 over IPv4	Produce Alert	Informational	100	Default
1101	0	Unknown IP Protocol	Produce Alert	Informational	75	Default
1102	0	Impossible IP Packet	Produce Alert	High	100	Default
1104	0	IP Localhost Source Spoof	Produce Alert	High	100	Default
1107	0	RFC 1918 Addresses Seen	Produce Alert	Informational	100	Default
1108	0	IP Packet with Proto 11	Produce Alert	High	100	Default
1109	0	Cisco IOS Interface DoS	Produce Alert	Medium	75	Default
1109	1	Cisco IOS Interface DoS	Produce Alert	Medium	75	Default
1109	2	Cisco IOS Interface DoS	Produce Alert	Medium	75	Default
1109	3	Cisco IOS Interface DoS	Produce Alert	Medium	75	Default
1201	0	IP Fragment Overlap	Deny Packet Inline,Produce Alert	Informational	100	Default
1202	0	IP Fragment Overrun - Datagram Too Long	Deny Packet Inline,Produce Alert	High	100	Default

26. Choose **File > Submit and Deploy** in order to deploy IPS on the IOS router.

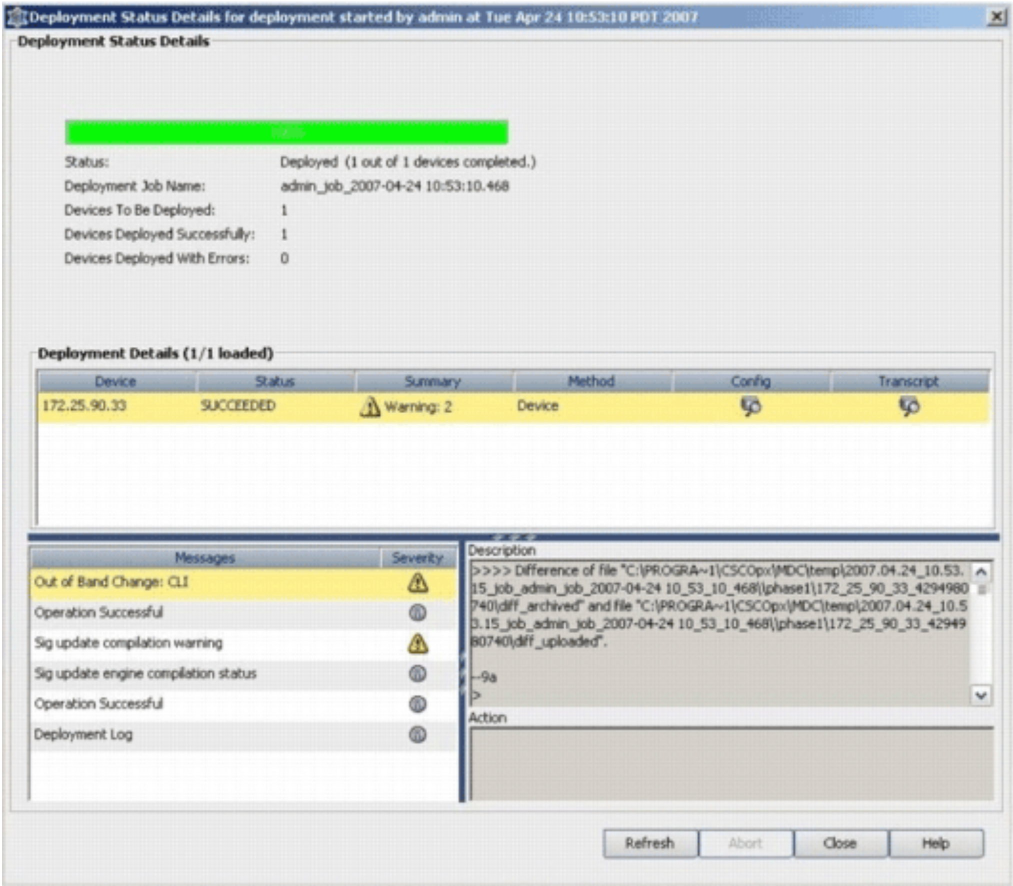


ID	Sub	Name	Actions	Severity	Fidelity	Source
1000	0	IP options-Bad Option List	Produce Alert	Informational	75	Default
1001	0	IP options-Record Packet Route	Produce Alert	Informational	100	Default
1002	0	IP options-Timestamp	Produce Alert	Informational	100	Default
1003	0	IP options-Provide s,c,h,tcc	Produce Alert	Informational	100	Default
1004	0	IP options-Loose Source Route	Produce Alert	High	100	Default
1005	0	IP options-SATNET ID	Produce Alert	Informational	100	Default
1006	0	IP options-Strict Source Route	Produce Alert	High	100	Default
1007	0	IPv6 over IPv4	Produce Alert	Informational	100	Default
1101	0	Unknown IP Protocol	Produce Alert	Informational	75	Default
1102	0	Impossible IP Packet	Produce Alert	High	100	Default
1104	0	IP Localhost Source Spoof	Produce Alert	High	100	Default
1107	0	RFC 1918 Addresses Seen	Produce Alert	Informational	100	Default
1108	0	IP Packet with Proto 11	Produce Alert	High	100	Default
1109	0	Cisco IOS Interface DoS	Produce Alert	Medium	75	Default
1109	1	Cisco IOS Interface DoS	Produce Alert	Medium	75	Default
1109	2	Cisco IOS Interface DoS	Produce Alert	Medium	75	Default
1109	3	Cisco IOS Interface DoS	Produce Alert	Medium	75	Default
1201	0	IP Fragment Overlap	Deny Packet Inline,Produce Alert	Informational	100	Default
1202	0	IP Fragment Overrun - Datagram Too Long	Deny Packet Inline,Produce Alert	High	100	Default

27. Choose the device on which you want to deploy the changes, and click **Deploy**.



28. View the deploy status in order to verify if there are any errors.



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	Severity
Out of Band Change: CLI	⚠
Operation Successful	ⓘ
Sig update compilation warning	⚠
Sig update engine compilation status	ⓘ
Operation Successful	ⓘ
Deployment Log	ⓘ

Description

```
>>>> Difference of file "C:\PROGRA~1\CSCOpx\MDC\temp\2007.04.24_10.53.
15_job_admin_job_2007-04-24 10_53_10_468\\phase1\172_25_90_33_4294980
740\diff_archived" and file "C:\PROGRA~1\CSCOpx\MDC\temp\2007.04.24_10.5
3.15_job_admin_job_2007-04-24 10_53_10_468\\phase1\172_25_90_33_42949
80740\diff_uploaded".


--9a
>
```

Action

Related Information

- **Cisco IOS Intrusion Prevention System (IPS) Products & Services Page**
- **Getting Started with Cisco IOS IPS with 5.x Signature Format**
- **IPS 5.x Signature Format Support and Usability Enhancements**
- **Cisco Intrusion Prevention System**
- **Security Product Field Notices (including CiscoSecure Intrusion Detection)**
- **Technical Support − Cisco Systems**

Updated: May 17, 2008 Document ID: 105626