How to Use CCP to Configure IOS IPS

Introduction

This document guides users through the initial provisioning steps and advanced options in configuring IOS IPS using Cisco Configuration Professional (CCP) version 1.x.

Enhancement in CCP 1.1 related to IOS IPS:

Supports VRF-aware IOS IPS

The tasks involved are:

Task 1: Download and install CCP

Task 2: Download IOS IPS signature package to a local PC using CCP Auto Update

Task 3: Launch IPS Policies Wizard to configure IOS IPS

Task 4: Verify IOS IPS configuration and signatures are properly loaded

Task 5: Signature tuning

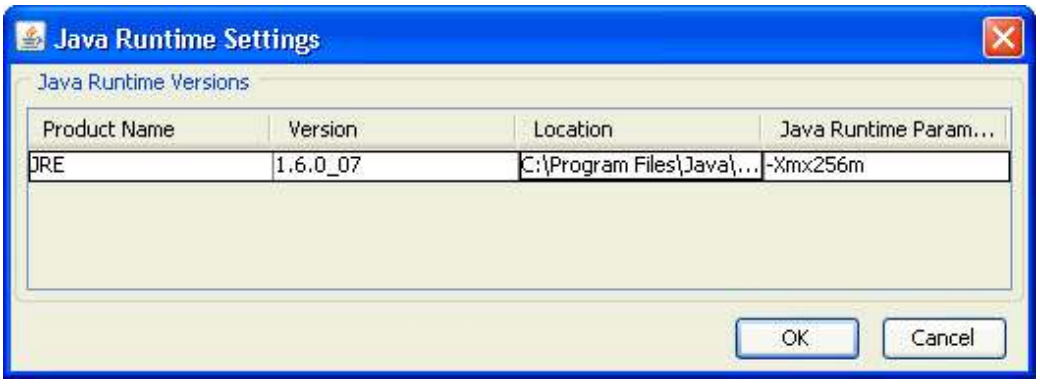
Task 6: Update signature package

Cisco CCP is a web-based configuration tool that simplifies router and security configuration through smart wizards, which help customers quickly and easily deploy, configure, and monitor a Cisco router without requiring knowledge of the command-line interface (CLI).

CCP can be downloaded from Cisco.com at http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281795035. Release Note can be found at the above URL as well.

Note: *12.4(11)T2 is the minimum IOS version CCP works with IOS IPS for version 5.x signature format. Cisco recommends using 12.4(15)T4 or later releases.

Note: Cisco CCP requires Java memory heap size to be no less than 256MB in order to configure IOS IPS. To change the Java memory heap size, open the Java control panel, selects the Java tab, click the 'View' button under Java Applet Runtime Settings, then enter –Xmx256m in the Java Runtime Parameter column.



Note: Open a console or telnet (with 'term monitor' on) session to the router to monitor messages while provisioning IOS IPS using CCP.

Task 1: Download and Install CCP

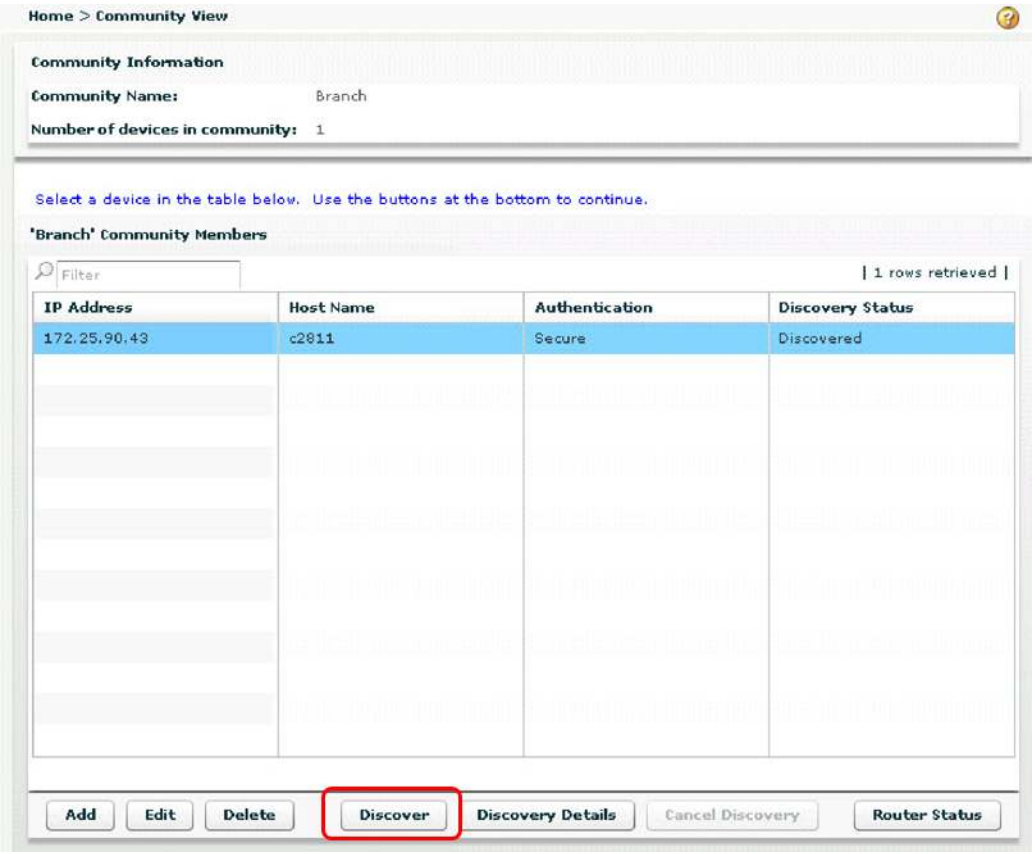
Step 1. Download CCP from Cisco.com at http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281795035 and install it on a local PC. You will need a Cisco.com registered account in order to download CCP.

Task 2: Download IOS IPS Signature Package to a Local PC using CCP Auto Update

Step 2. Run CCP from the local PC. When prompted to verify digital signature for CCP, select "Always trust content from this publisher." Select 'Run' to continue.

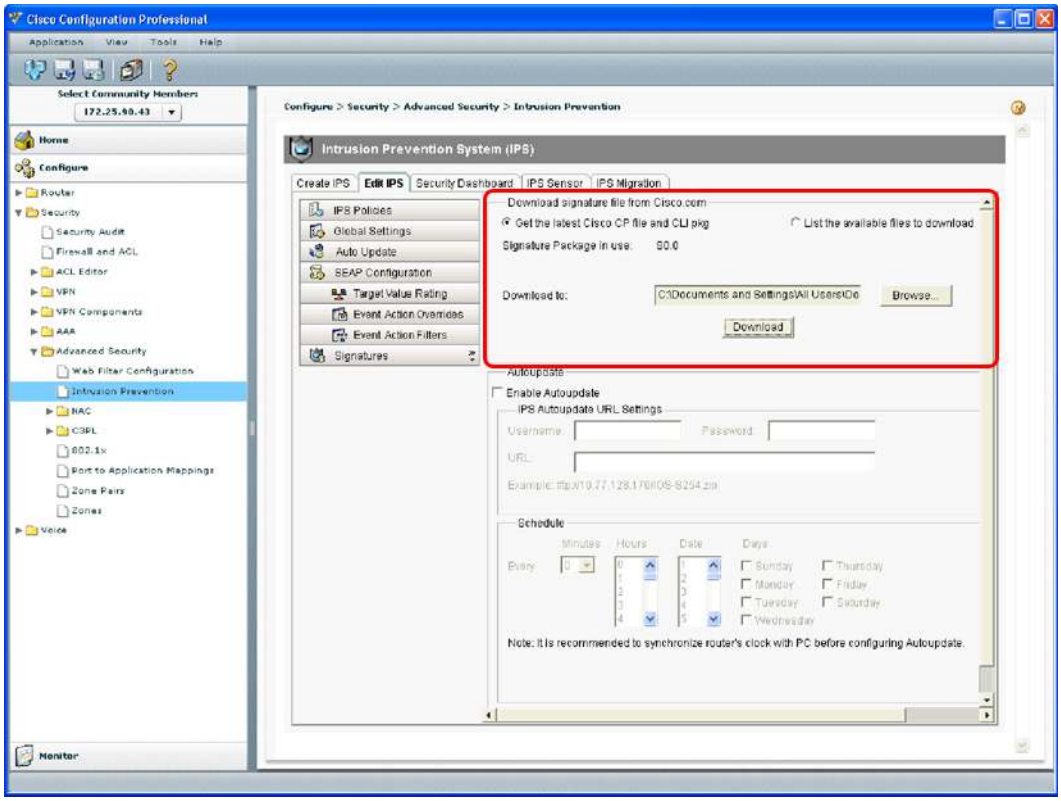
Step 3. Select the 'community' that has the router you want to configure IOS IPS.

Step 4. Highlight the router and click "Discover" if the router has not been discovered already. Discovering allows CCP to login to the router and to modify configurations.



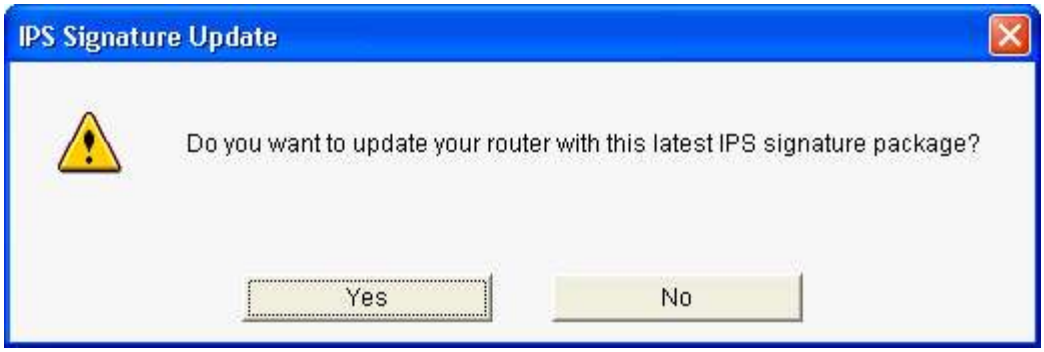
Step 5. Navigate to the Auto Update screen. From CCP home page, at the left panel, select **Configure** -> **Security -> Advanced Security -> Intrusion Prevention**, then at the right panel select **Edit IPS** -> **Auto Update**. If SDEE notification is not enabled on the router, click 'OK' to enable SDEE notification.

Step 6. Download the latest IOS IPS signature package to a local TFTP or FTP server. On the Auto Update screen, select '**Get the latest CCP file and CLI pkg**' radio button. Next click the '**Browse…**' button to select a directory on your local PC to save the downloaded files, you can choose the TFTP or FTP server root directory, which will be used later on when deploying signature package to the router. Next click the '**Download**' button.



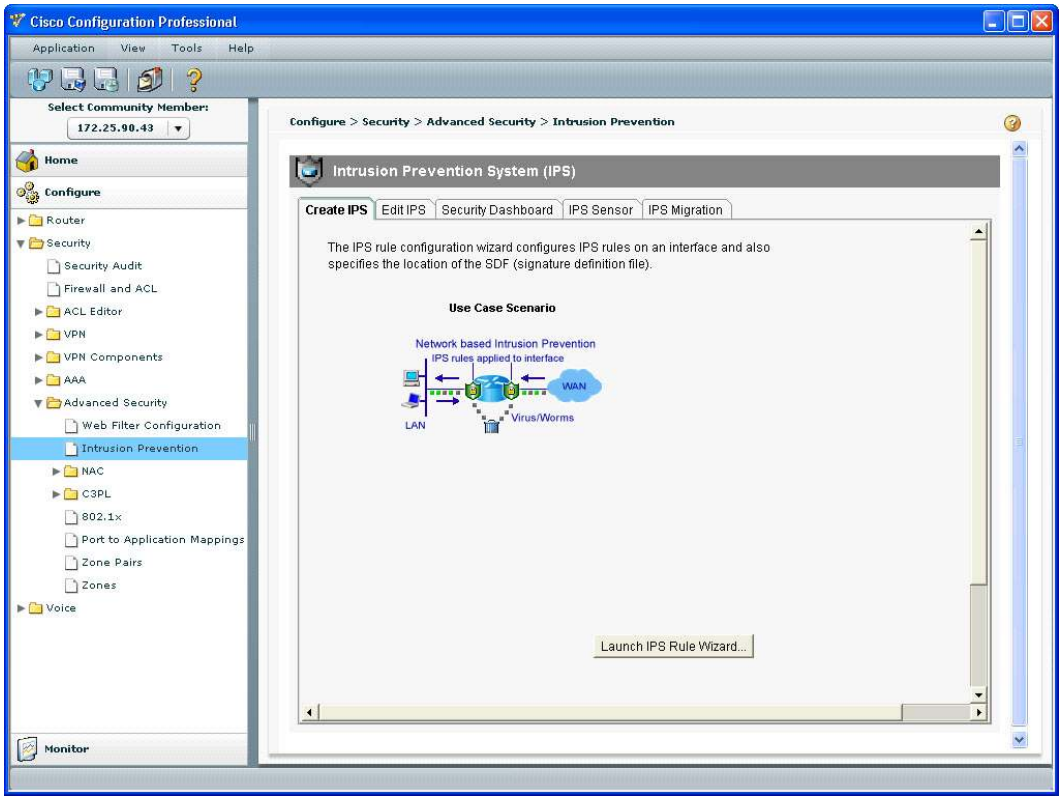
Step 7. When prompted to provide CCO login credential, use your CCO registered username and password.

Step 8. CCP connects to Cisco.com and starts to download both the CCP signature file (e.g. sigv5-SDM-S353.zip) and the CLI signature pkg file (e.g. IOS-S353-CLI.pkg) to the directory selected in Step 6. After both files are downloaded, CCP will prompt the user to push the downloaded signature package to the router, select 'No' as we have not configured IOS IPS on the router yet.

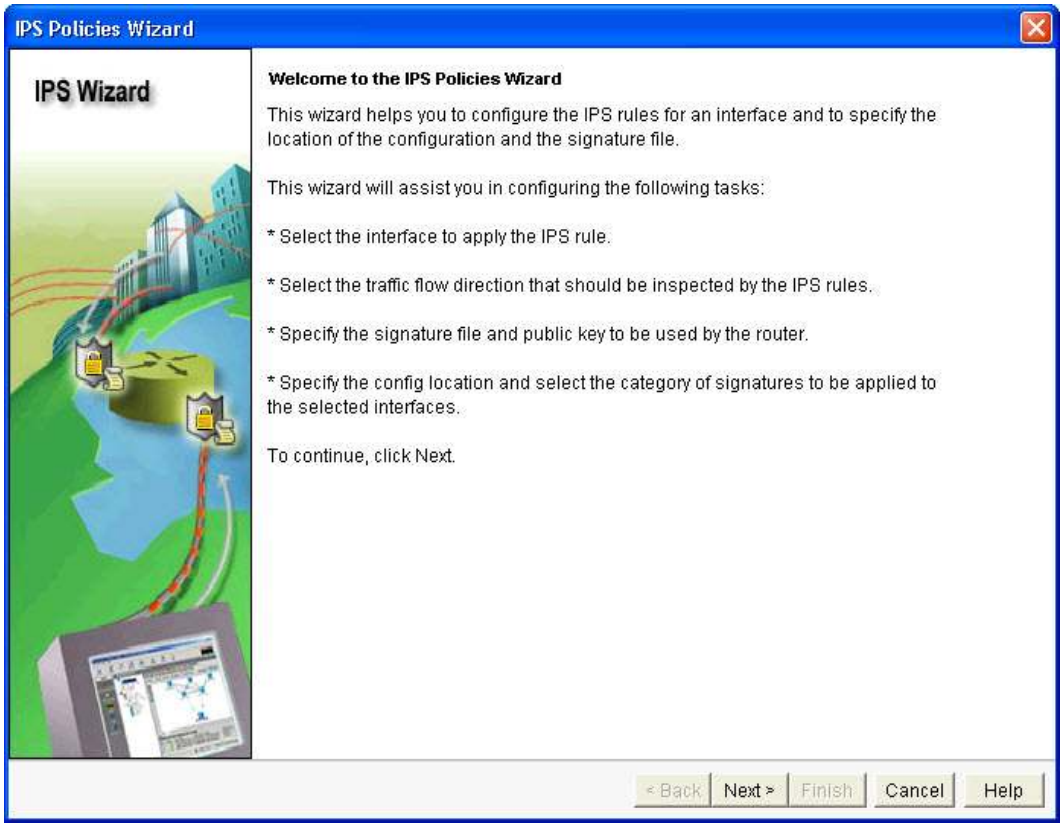


Task 3: Launch IPS Policies Wizard to Configure IOS IPS

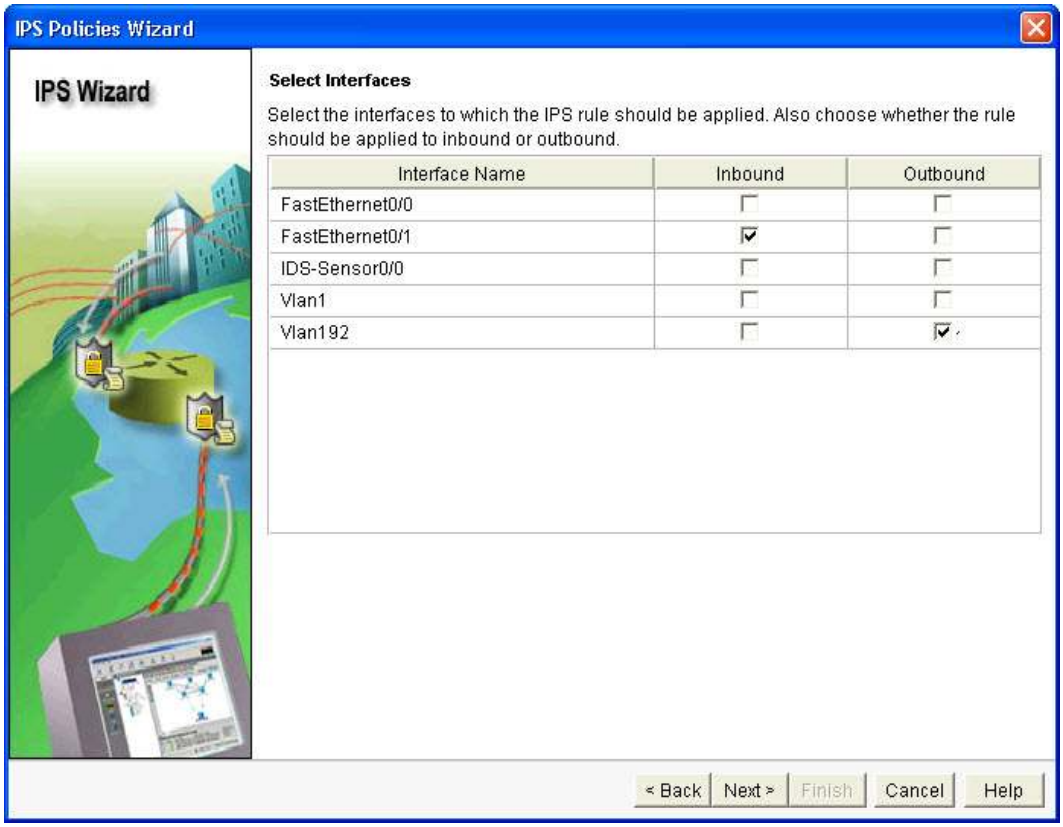
Step 9. After CCP downloaded the latest IOS CLI signature package, go to '**Create IPS**' tab to create initial IOS IPS configuration. If prompted to apply changes to the router, click the 'Apply Changes' button. Next click the '**Launch IPS Rule Wizard…**' button. A pop up window informs you that CCP needs to establish a SDEE subscription to the router to retrieve alerts, click 'OK'.



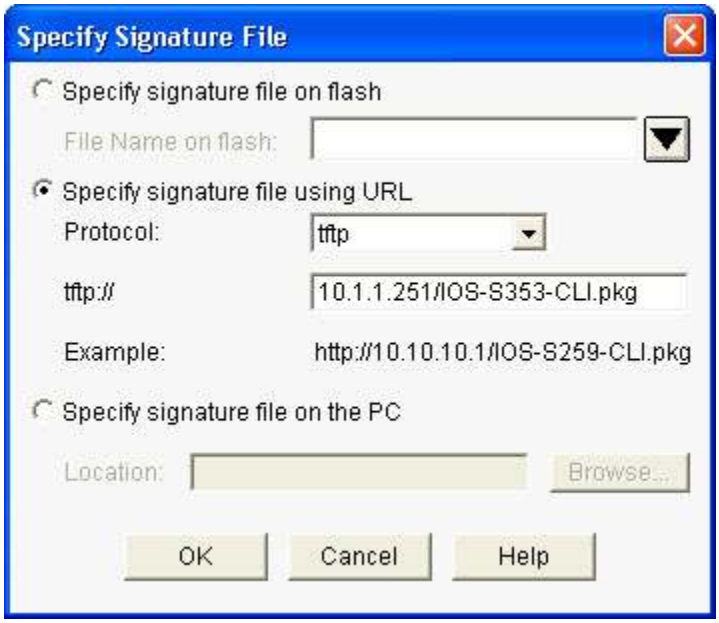
Step 10. Click ‘Next’ at the ‘Welcome to the IPS Policies Wizard’ screen.



Step 11. At the ‘Select Interfaces’ screen, select the interface and the direction that IOS IPS will be applied to, then click ‘Next’ to continue.

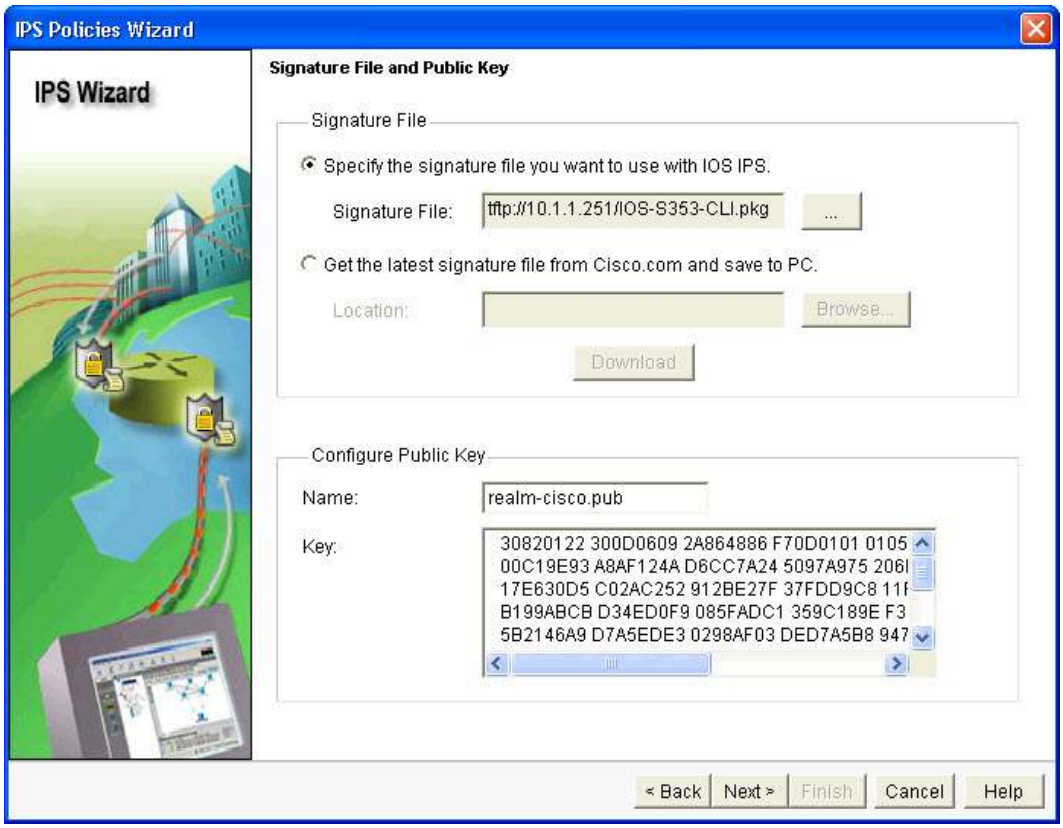


Step 12. At the ‘IPS Policies Wizard’ screen, in the ‘Signature File’ section, select the first radio button “Specify the signature file you want to use with IOS IPS”, then click the “…” button to bring up a dialog box to specify the location of the signature package file, which will be the directory specified in Step 6. In this example, we use tftp to download the signature package to the router.



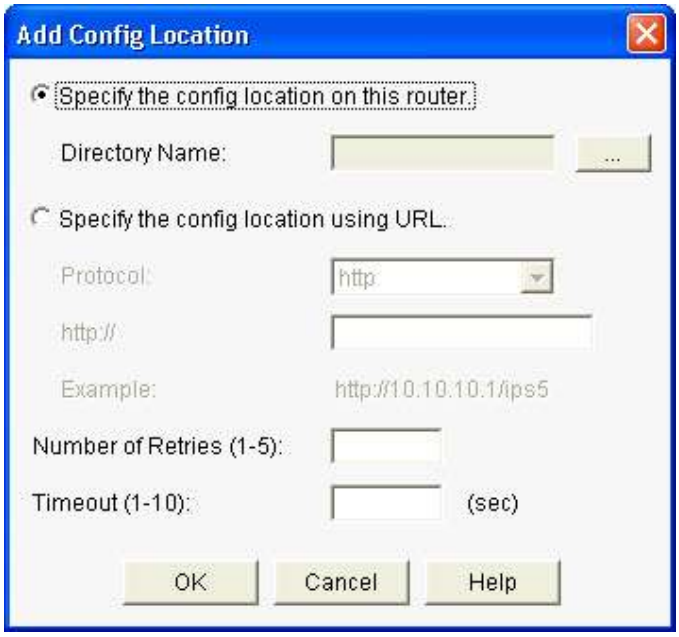
Step 13. In the ‘Configure Public Key’ section, enter ‘realm-cisco.pub’ in the ‘Name’ text field, then copy and paste the following public key’s key-string in the ‘Key’ text field. This public key can be download from Cisco.com at: http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup. Click ‘Next’ to continue.

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
```



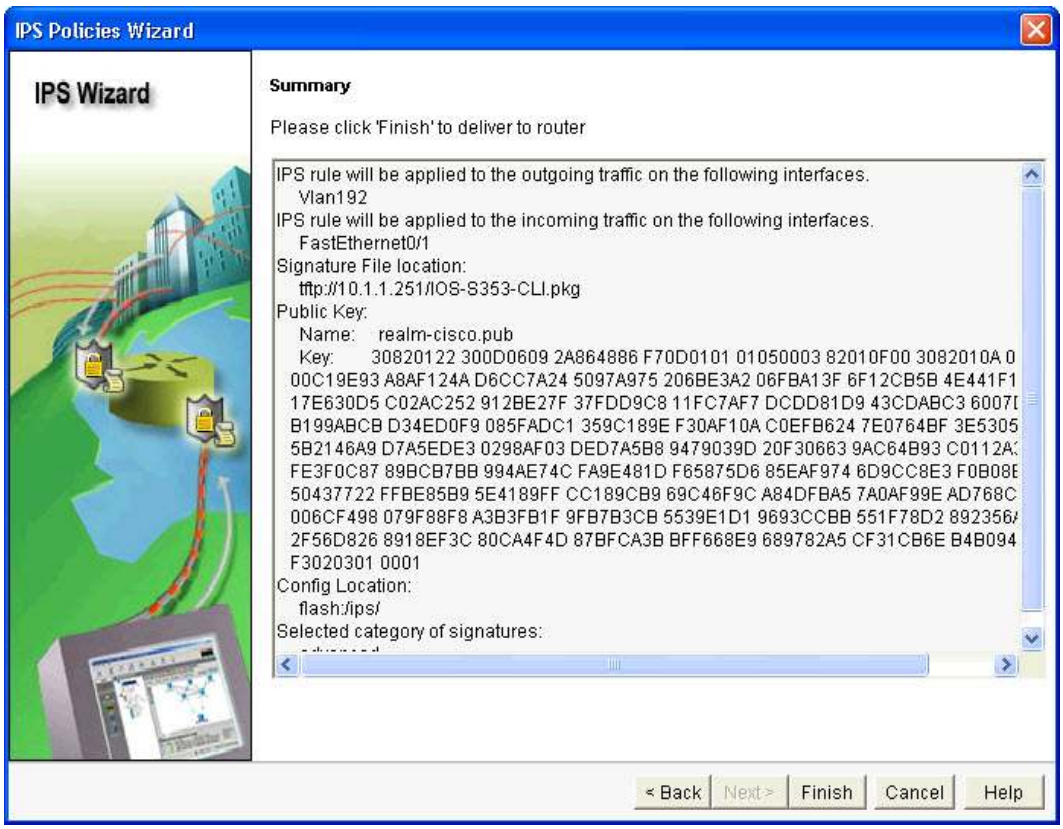
Step 14. At the ‘Config Location and Category’ screen, select a location where the signatures definition and configuration files will be stored by click on the ‘…’ button in the ‘Config Location’ section.

At the ‘Add Config Location’ dialog box, choose the first option “Specify the config location on this router” and then click the ‘…’ button.

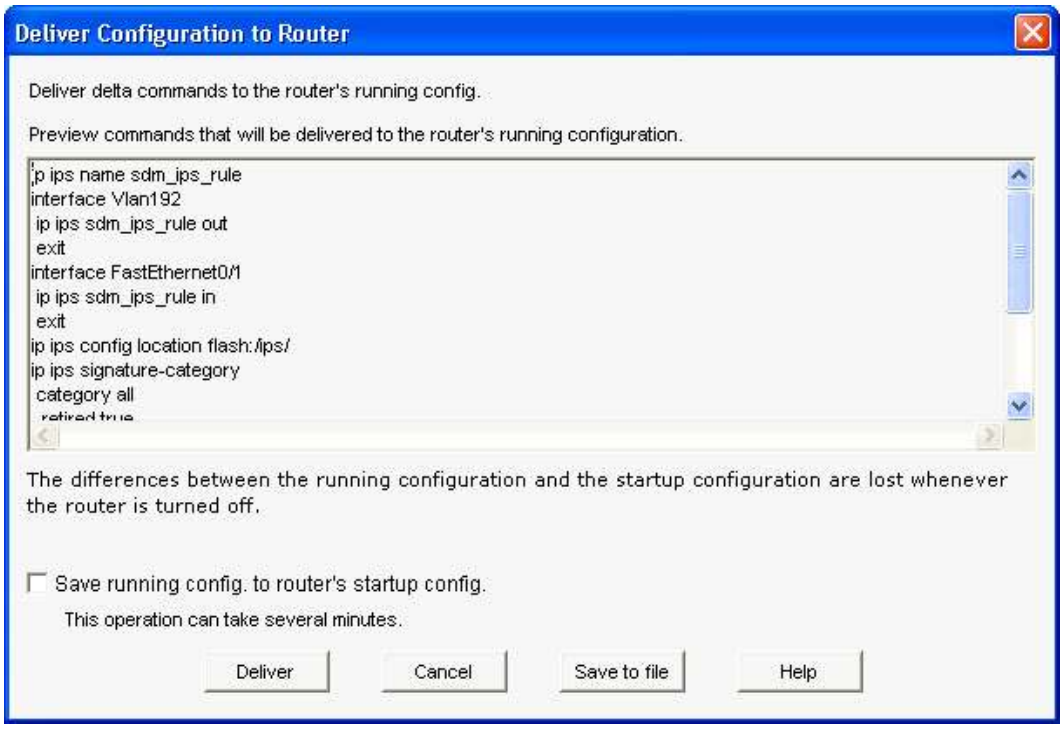


The “Choose Folder” dialog shows up and allows you to select an existing directory or create a new directory on the router flash to store the signature definition and configuration files. Click the ‘New Folder’ button at the top if you want to create a new directory. Once you select the directory, click ‘OK’ at the ‘Choose Folder’ dialog then click ‘OK’ again at the ‘Add Config Location’ dialog to go back to the ‘IPS Policies Wizard’ screen.

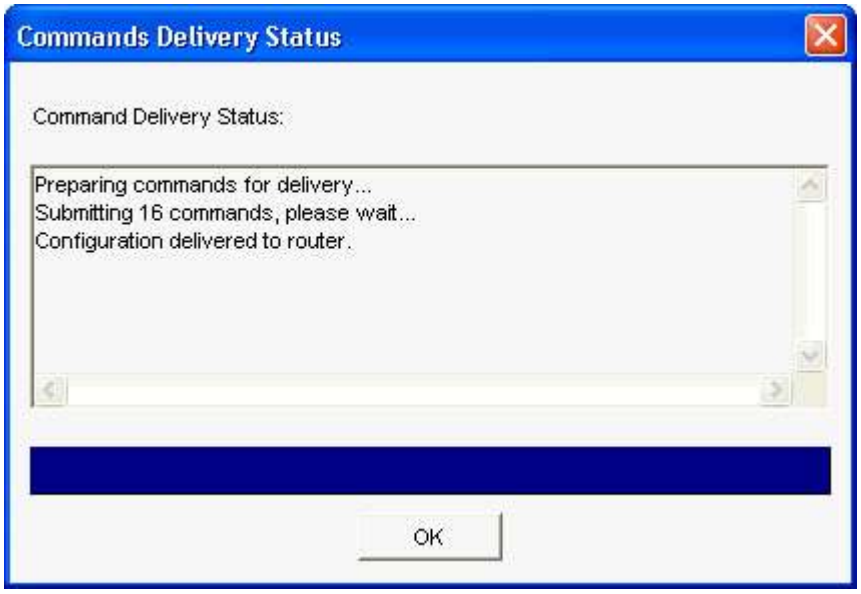
Step 15. Back at the ‘IPS Policies Wizard’ screen, select the signature category according to the amount of memory installed on the router. There are two signature categories you can choose in CCP – ‘Basic’ and ‘Advanced’. If the router has 128MB DRAM installed, Cisco recommends choosing 'Basic' category to avoid memory allocation failures. If the router has 256MB or more DRAM installed, you may choose either category. Once you select a category to use, click ‘Next’ to continue to the last page of the wizard – the summary page. The summary page provides a brief description about the tasks IOS IPS initial configuration.



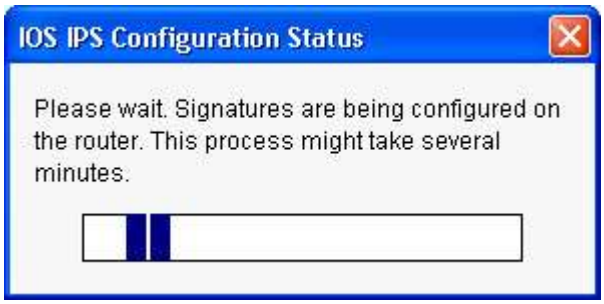
Step 16. Click ‘Finish’ on the summary page to deliver the configurations and signature package to the router. If the preview commands option is enabled on the Preferences settings in CCP, then CCP will display the ‘Deliver Configuration to Router’ dialog, which shows a summary of CLI commands that CCP will deliver to the router. Click ‘Deliver’ to proceed.



Step 17. A ‘Commands Delivery Status’ dialog screen is then displayed to show the commands delivery status. When the commands are delivered to the router, click ‘OK’ to continue.

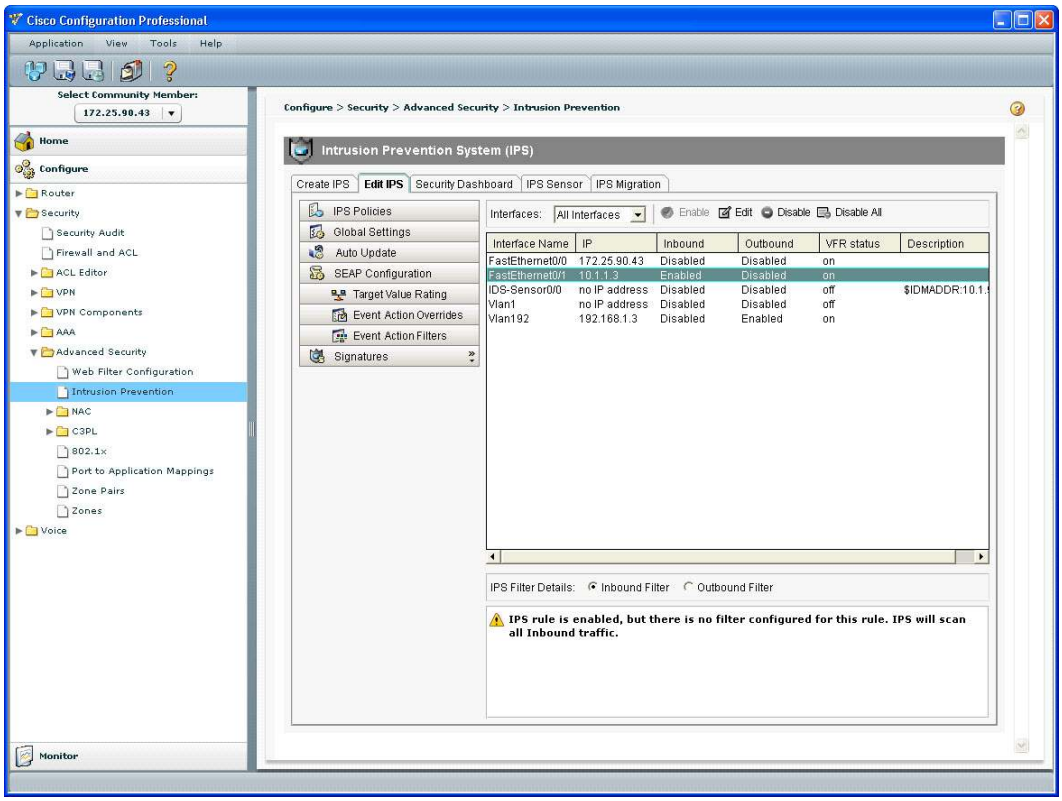


Step 18. An ‘IOS IPS Configuration Status’ dialog screen is displayed to show that signatures are being loaded on the router.

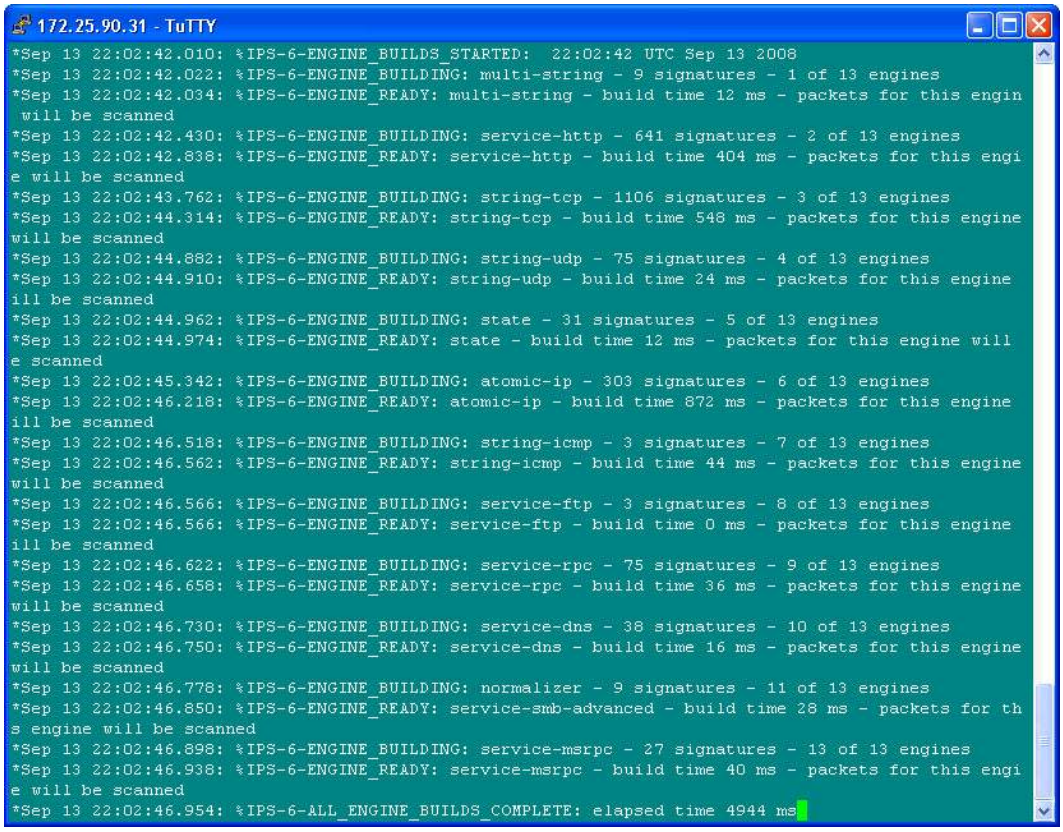


Task 4: Verify IOS IPS Configuration and Signatures are Properly Loaded

Step 19. When the signatures are loaded, CCP then displays the ‘Edit IPS’ tab with the current configuration. Verify the configuration by checking which interface and in what direction is the IOS IPS enabled.



Step 20. The router console shows that signatures' loading is complete

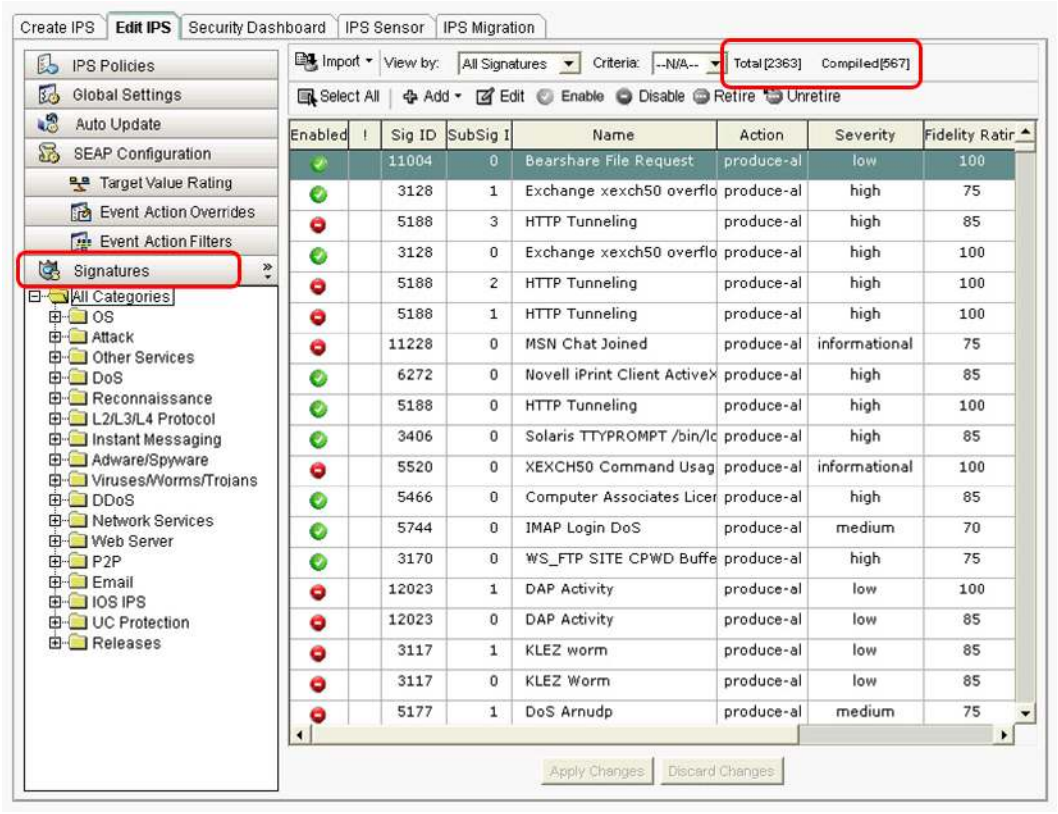


Step 21. Verify the signatures are loaded properly by using this command at the router prompt:

```
router#show ip ips signatures count

Cisco SDF release version S353.0
Trend SDF release version V0.0

|

snip

|

Total Signatures: 2363
   Total Enabled Signatures: 1025
   Total Retired Signatures: 1796
   Total Compiled Signatures: 567
   Total Obsoleted Signatures: 15
```

Congratulations! Now you have finished the initial provisioning of IOS IPS using CCP 1.x.

Step 22. Under **Edit IPS** tab, select **Signatures**. Verify the signature numbers with CCP.



Task 5: Signature Tuning

Step 23. To retire/unretire and enable/disable signatures, select the **Edit IPS** tab, then select **Signatures**. Highlight the signature(s), and then click the **Enable**, **Disable**, **Retire**, or **Unretire** button. Notice the status changed in the **Enabled** or the **Retired** column. A yellow icon appears for the signature(s) in the column next to **Enabled**. The yellow icon means changes have been made to the signature, but have not been applied. Click the **Apply Changes** button to make the changes take effect.

Retire/unretire is to select/de-select which signatures are being used by IOS IPS to scan traffic.

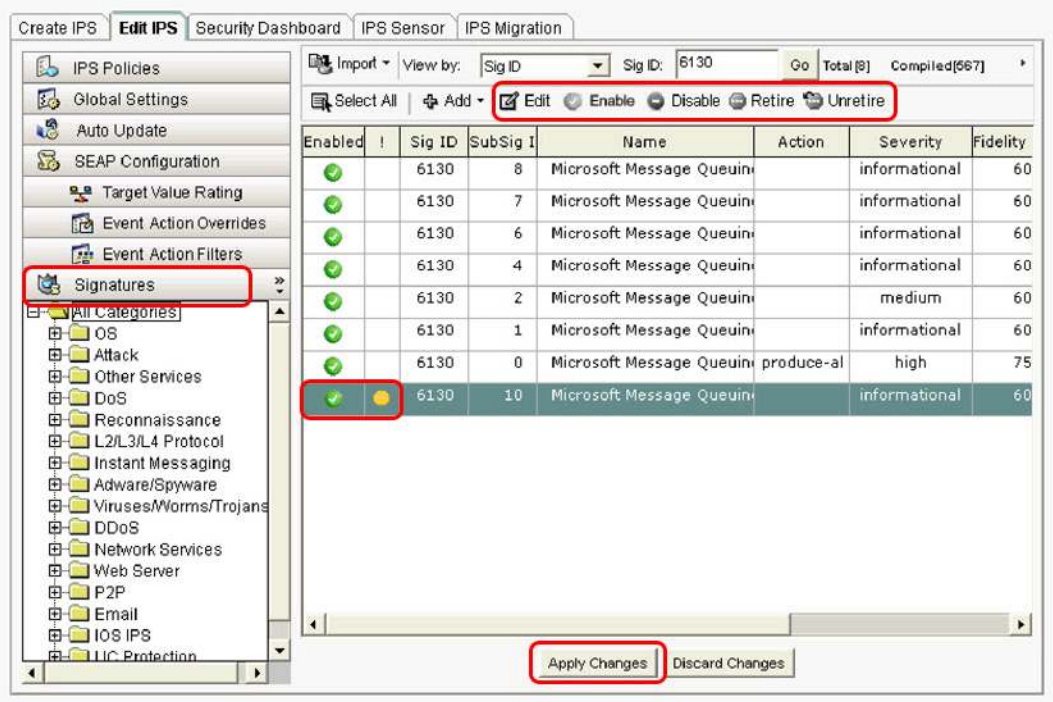
Retiring a signature means IOS IPS will NOT compile that signature into memory for scanning.

Unretiring a signature instructs IOS IPS to compile the signature into memory and use the signature to scan traffic.

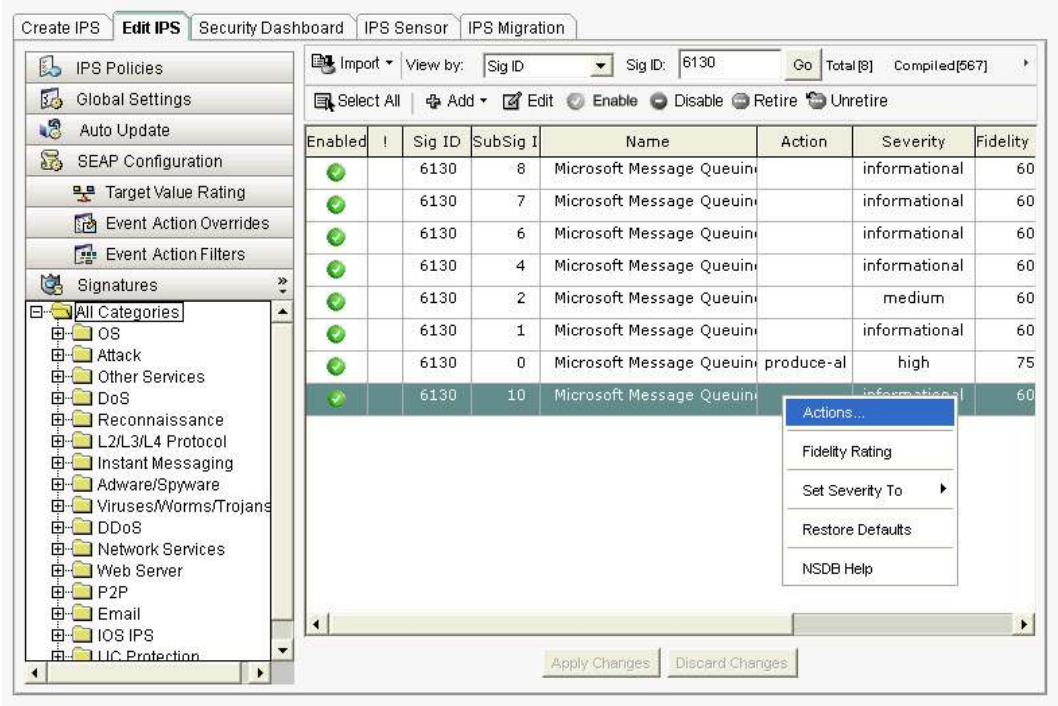
Enable/disable does NOT select/de-select signatures to be used by IOS IPS.

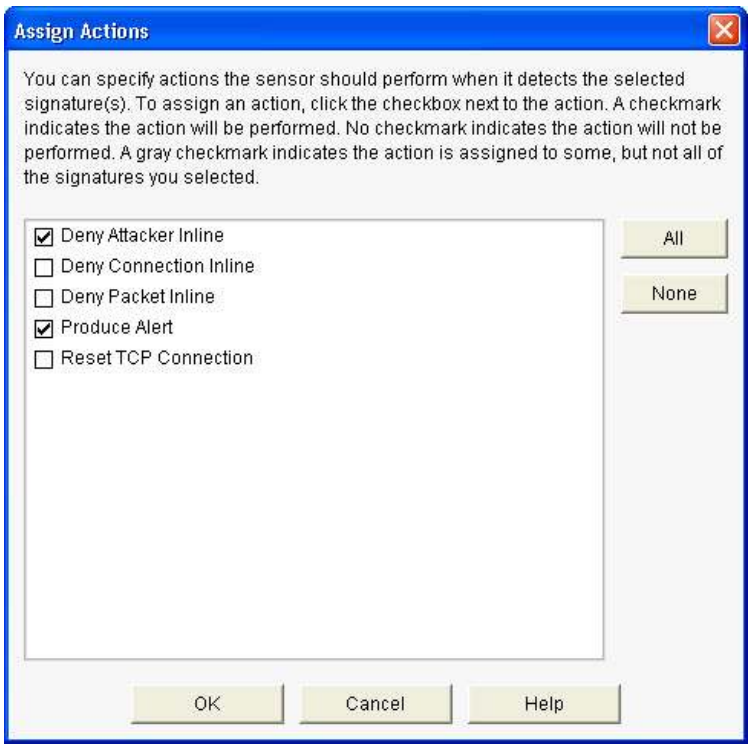
Enabling a signature means that when triggered by a matching packet (or packet flow), the signature takes the appropriate action associated with it. However, only unretired AND successfully compiled signatures will take the action when they are enabled. In other words, if a signature is retired, even though it is enabled, it will not be compiled (because it is retired) and it will not take the action associated with it.

Disabling a signature means that when triggered by a matching packet (or packet flow), the signature DOES NOT take the appropriate action associated with it. In other words, when a signature is disabled, even though it is unretired and successfully compiled, it will not take the action associated with it.

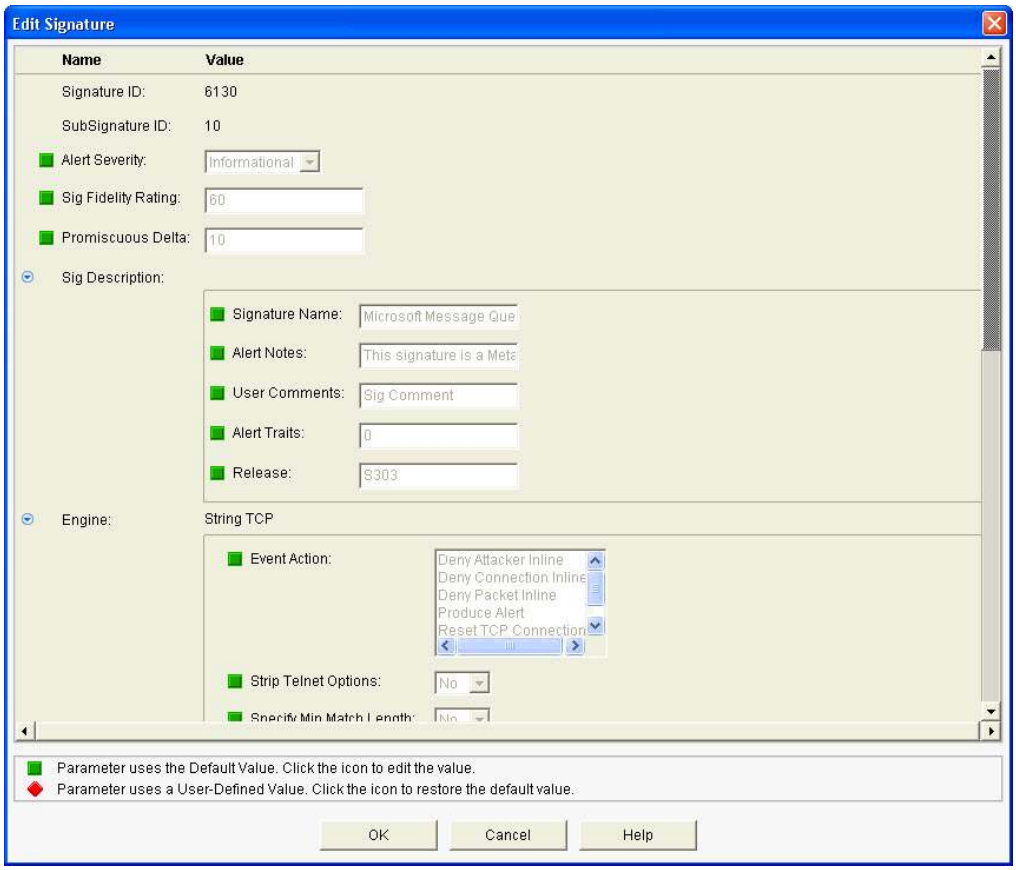


Step 24. To change the action associated with a signature, highlight the signature, then right click, select **Actions**, then select/de-select the actions to be associated with this signature. A yellow icon appears for the signature in the column next to **Enabled**. The yellow icon means changes have been made to the signature, but have not been applied. Click the **Apply Changes** button to make the changes take effect.



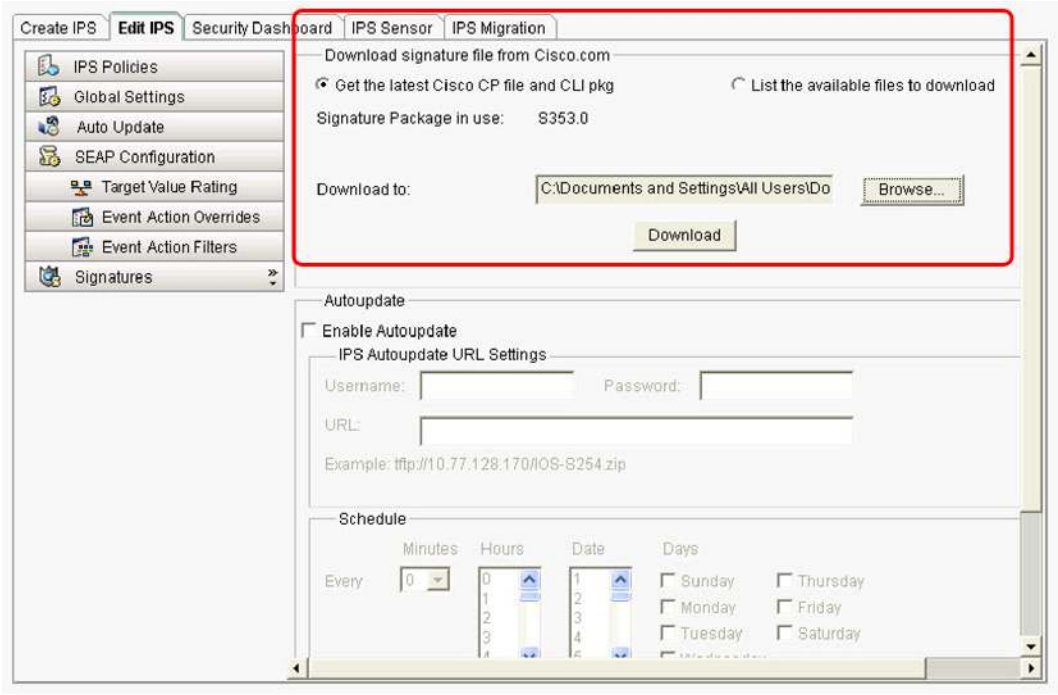


Step 25. You can also use the signature edit function to retire/unretired/enable/disable signature(s) and change signature actions. Highlight the signature, the click the **Edit** button next to the **Enable** button. The edit function also allows granular signature customization by allowing you to modify all parameters associated with the signature.



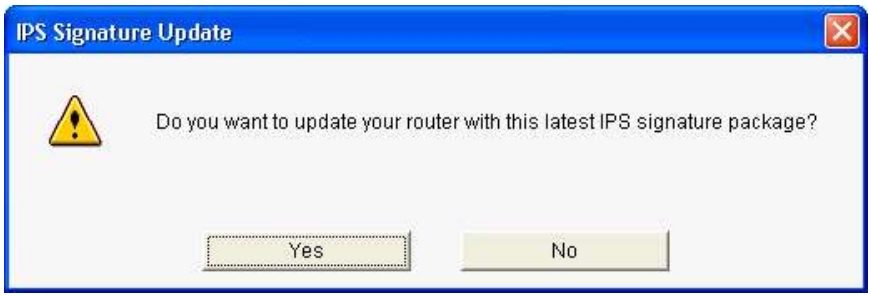
Task 6: Update Signature Package

Step 26. To update signature package when signature updates are available, go to **Edit IPS** tab and select **Auto Update**. Select '**Get the latest CCP file and CLI pkg**' radio button. Next click the '**Browse…**' button to select a directory on your local PC to save the downloaded files. Next click the '**Download**' button.

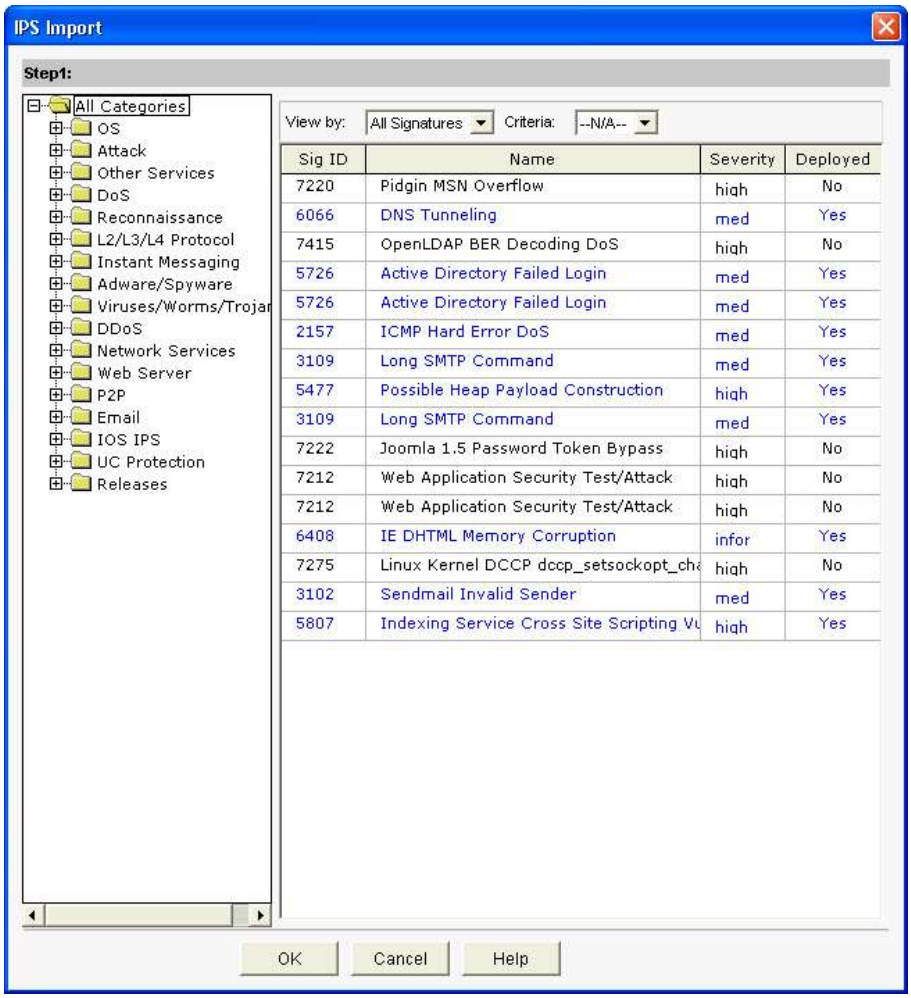


Step 27. When prompted to provide CCO login credential, use your CCO registered username and password.

Step 28. CCP connects to Cisco.com and starts to download both the CCP signature file (e.g. sigv5-SDM-S354.zip) and the CLI signature pkg file (e.g. IOS-S353-CLI.pkg) to the directory selected in Step 26. After both files are downloaded, CCP prompts the user to update the latest signature package to the router, select 'Yes'.

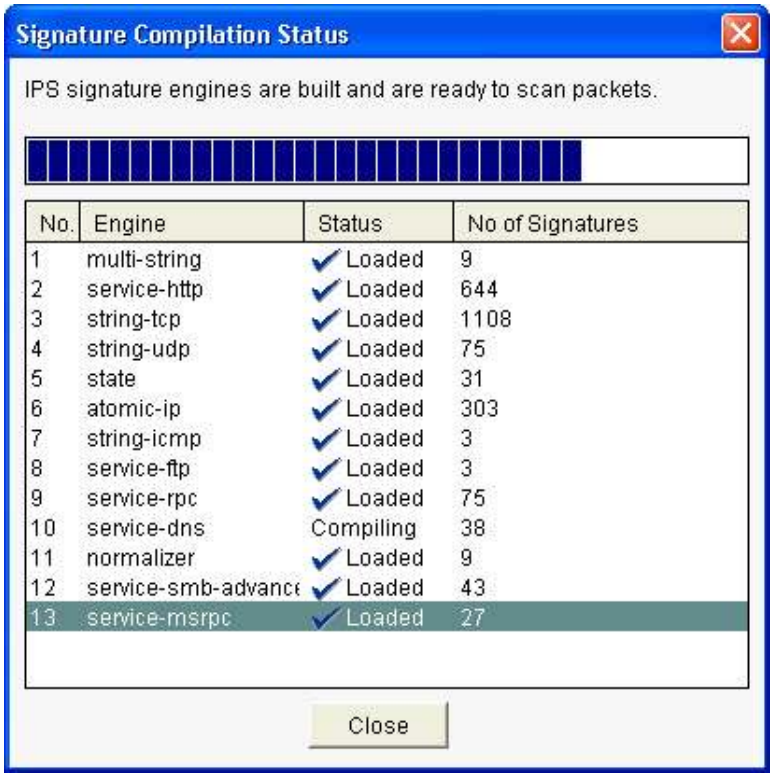


Step 29. Click **OK** when the **IPS Import** prompt appears.

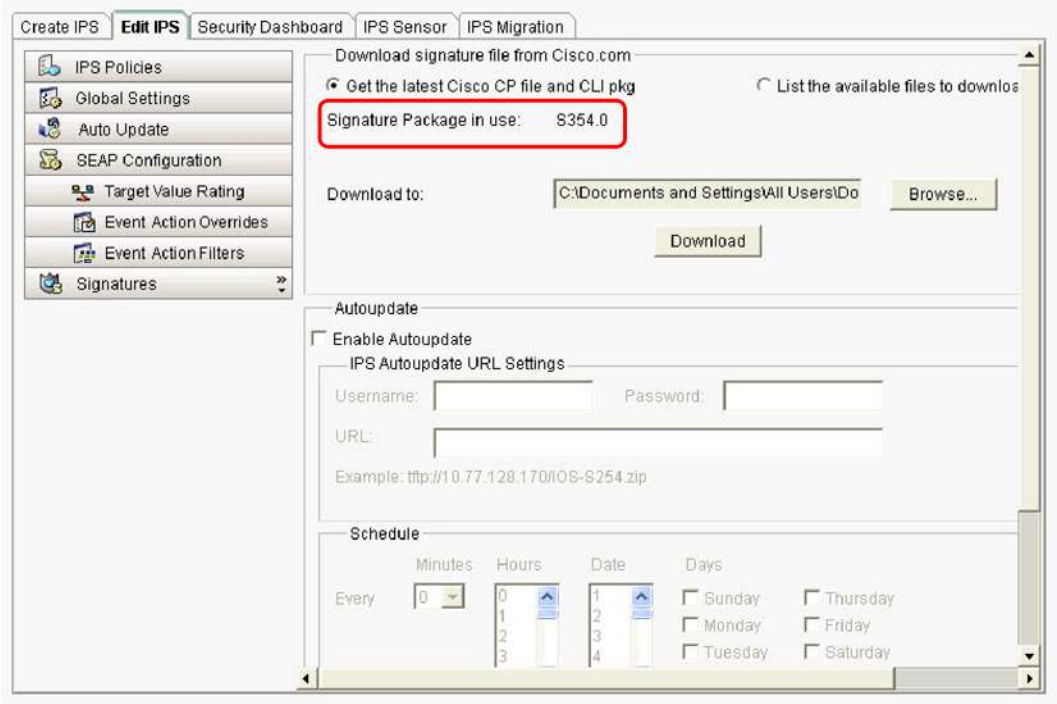


Step 30. An **Importing Signatures** dialog screen is displayed to show that signatures are being loaded on the router

Step 31. Once the new signature package is loaded on the router, click **Close** at the **Signature Compilation Status** dialog screen.



Step 32. At the **Auto Update** window, notice that the signature package version changed to the new version in **Signature Package in use**.



Reference

- Cisco IOS IPS on Cisco.com: http://www.cisco.com/go/iosips
- Cisco IOS IPS Signature package: http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup
- Cisco IOS IPS Signature files for CCP: http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup-sdm
- Getting Started with Cisco IOS IPS with 5.x Signature Format: http://www.cisco.com/en/US/products/ps6634/products_white_paper0900aecd805c4ea8.shtml
- Cisco MySDN: http://tools.cisco.com/MySDN/Intelligence/home.x
- Cisco IOS IPS Configuration Guide: http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a0080747eb0.html
- IPS Management Express: http://www.cisco.com/cgi-bin/tablebuild.pl/ips-ime

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-453847-02 05/09