

# 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 <a href="http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281795035">http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281795035</a>. 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.

Java Runtime Versio	ons		
Product Name	Version	Location	Java Runtime Param
RE	1.6.0_07	C:\Program Files\J	ava\Xmx256m
	<i>0</i> 2		

**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.

P Filter	1 rows retrieved
Name	Number of Members
Branch	1

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.

emmunity Information			
ommunity Name:	Branch		
umber of devices in co	mmunity: 1		
elect a device in the ta	ble below. Use the buttons at th	e bottom to continue.	
ranch' Community Mer	nbers		
Filter			1 rows retrieved
IP Address	Host Name	Authentication	Discovery Status
172.25,90.43	c2811	Secure	Discovered
		للحلل الحالمالحالك كالل	
	in teleficiente	والمار وكلماعالك إوالا	
		وسنا يحتطفننك إوانن	
	and the second		

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.

Application View Tools Help			
V			
Select Community Hembers           172.25.90.43	Configure > Security > Advanced Secu	rity > Intrusion Prevention	G
🚳 Home	Intrusion Prevention Syst	tem (IPS)	1
🖓 Configure	Create IPS Edit IPS Security Dash		
📴 Router		Download signature file from Cisco.com	
Security	🔒 IPS Policies		
Security Audit	Global Settings		
Firesall and ACL	😫 Auto Update	Signature Package in use: S0.0	
F 🔛 ACL Editor	SEAP Configuration		
NEN CEN	Target Value Rating	Download to: C1Documents and Bettings/All Users/Do Browse	
► 🔄 VPN Components	Event Action Overrides		
# 🛄 AAA	Event Action Filters	Download	
Y CAdvanced Security	🔄 Signatures 🗧		
Web Filter Configuration		Autoupdate	
Intrusion Prevention		F Enable Autoupdate	
MAC		IPS Autoupdate URL Settings	
► C3PL		Userneme. Peseword.	
002.1×		URL	
Port to Application Mappings			
2 20ne Pairs		Example: #px10.77.128.170/05-8254.20	
2ones		Schedule	
C veice			
		Minutes Hours Diste Days	
		Every 0 💌 0 🦰 1 🏠 🔽 Sunday 🖓 Thursday	
		2 3 Enday Enday	
		4 S M F Wednesday	
		Note: It is recommended to synchronize router's clock with PC before configuring Autoupdate.	
			1
		4 T	
			14
Monitor			

- 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.

IPS Signatu	re Update	×
	Do you want to update your router with this latest IPS signature package?	
	Yes No	

# 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.

IPS Wizard	Welcome to the IPS Policies Wizard
ii o mzaru	This wizard helps you to configure the IPS rules for an interface and to specify the location of the configuration and the signature file.
À	This wizard will assist you in configuring the following tasks:
	* Select the interface to apply the IPS rule.
	* Select the traffic flow direction that should be inspected by the IPS rules.
	* Specify the signature file and public key to be used by the router.
	* Specify the config location and select the category of signatures to be applied to the selected interfaces.
	To continue, click Next.
T	

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.

IPS Wizard	Select Interfaces		
	Select the interfaces to which the IPS rule s should be applied to inbound or outbound.	should be applied. Also cho	ose whether the rule
	Interface Name	Inbound	Outbound
4	FastEthernet0/0	L. L.	Г
1-1	FastEthernet0/1	<b>N</b>	Г
	IDS-Sensor0/0	E	Г
10	Vlan1	Г	Г
6 Star	Vlan192		
	5		

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.

Specify Signature File	
C Specify signature file	on flash
File Name on flash:	
🕫 Specify signature file	using URL
Protocol:	tttp 🗾
tftp://	10.1.1.251/IOS-S353-CLI.pkg
Example:	http://10.10.10.1/IOS-S259-CLI.pkg
C Specify signature file	on the PC
Location:	Browse.,
ок	Cancel Help

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: <u>http://www.cisco.com/cgibin/tablebuild.pl/ios-v5sigup</u>. 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 DCD081D9 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

	Signature File and Public	c Key
PS Wizard		
	Signature File	
	Specify the signal	ture file you want to use with IOS IPS.
1	Dianeturo Filor	tftp://10.1.1.251//OS-S353-CLI.pkg
E.K.	Signature File:	htp://10.111231/00-0333-0Ei.phg
	Get the latest sign	nature file from Cisco.com and save to PC.
10	Location:	Browse
Call .	HERE AND A DECEMBER OF A DECEMBER OFOA DECEMBER OFOA DECEMBER OFOA DECEMBER OFOA DECEMBER OFOA DECEM	
10-25		Download
	and the second se	
	3	
	Configure Public K	ey
	Configure Public K Name:	ey realm-cisco.pub
	Name:	realm-cisco.pub
	CON	realm-cisco.pub 30820122 300D0609 2A864886 F70D0101 0105 00C19E93 A8AF124A D6CC7A24 5097A975 2061
	Name:	realm-cisco.pub 30820122 300D0609 2A864886 F70D0101 0105 00C19E93 A8AF124A D6CC7A24 5097A975 206 17E630D5 C02AC252 912BE27F 37FDD9C8 11F
	Name:	realm-cisco.pub 30820122 300D0609 2A864886 F70D0101 0105 00C19E93 A8AF124A D6CC7A24 5097A975 2061
	Name:	realm-cisco.pub 30820122 300D0609 2A864886 F70D0101 0105 00C19E93 A8AF124A D6CC7A24 5097A975 2061 17E630D5 C02AC252 912BE27F 37FDD9C8 11F B199ABCB D34ED0F9 085FADC1 359C189E F3
	Name:	realm-cisco.pub 30820122 300D0609 2A864886 F70D0101 0105 00C19E93 A8AF124A D6CC7A24 5097A975 206 17E630D5 C02AC252 912BE27F 37FDD9C8 11F B199ABCB D34ED0F9 085FADC1 359C189E F3 5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 947 v
	Name:	realm-cisco.pub 30820122 300D0609 2A864886 F70D0101 0105 00C19E93 A8AF124A D6CC7A24 5097A975 206 17E630D5 C02AC252 912BE27F 37FDD9C8 11F B199ABCB D34ED0F9 085FADC1 359C189E F3 5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 947 v

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.

Directory Name:	
C Specify the config location	on using URL.
Protocol:	http:
http://	
Example:	http://10.10.10.1/ips5
Number of Retries (1-5):	
Timeout (1-10):	(sec)

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.

Choose Folder		
New Folder		
OK	Cancel	Help

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.

IPS Wizard	Summary
	Please click 'Finish' to deliver to router
	IPS rule will be applied to the outgoing traffic on the following interfaces. Vian192 IPS rule will be applied to the incoming traffic on the following interfaces. FastEthernet0/1 Signature File location: tftp://10.1.1.251/IOS-S353-CLI.pkg Public Key: Name: realm-cisco.pub Key: 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 0 00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F1 17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007I B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF3 E5305 592146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20730663 9AC64B93 C0112A: FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08E 50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C 006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356/ 2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094 F3020301 0001 Config Location: flash/ips/ Selected category of signatures:

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.

Deliver Configuration to Router	×
Deliver delta commands to the router's running config. Preview commands that will be delivered to the router's running configuration.	
pips name sdm_ips_rule interface Vlan192 ip ips sdm_ips_rule out exit interface FastEthernet0/1 ip ips sdm_ips_rule in exit ip ips config location flash:/ips/ ip ips signature-category category all retired true	<
The differences between the running configuration and the startup configuration are lost whenever the router is turned off.	
Save running config. to router's startup config.	
This operation can take several minutes.	
Deliver Cancel Save to file Help	

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.

Commands Delivery Status	
Command Delivery Status:	
Preparing commands for delivery Submitting 16 commands, please wait Configuration delivered to router.	*
	3
OK	

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

IOS IPS Configuration Status
Please wait. Signatures are being configured on the router. This process might take several minutes.

# 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.

Router       Create IPS       Exit IPS       Security Dashboard       IPS Sensor IPS Migration         Security Audit       Bscurity Audit       Interfaces:       All Interfaces:       Inte	Application View Tools Help							
Intrusion Prevention         Intrusion Prevention         Intrusion Prevention         Intrusion Prevention         Interfaces         Intrusion Prevention         Intrusion Prevention         Intrusion Prevention         Intrusion Prevention <td< th=""><th>19 🗔 🗔 💋 💡</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></td<>	19 🗔 🗔 💋 💡							
Intrusion Prevention     Intrusion Prevention System (IPS)     Intrusion Prevention     Intrusion Prevention <tr< th=""><th>Select Community Member:</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></tr<>	Select Community Member:							
Configure   Router   Security   Add.   Security   WPN   Components   Add.   Security   Security   Web Filter Configuration   Thrusion Prevention   Signatures   Web Filter Configuration   Intrusion Prevention   Signatures   Value   Signatures               Port to Application Mappings   Open to Application Mappings   Open to Application Mappings   Open to Application Mappings   Over   Voice </th <th>172.25.90.43 🛛 🔻</th> <th>Configure &gt; Security &gt; Advanced Secu</th> <th>urity &gt; Intrusion P</th> <th>revention</th> <th></th> <th></th> <th></th> <th></th>	172.25.90.43 🛛 🔻	Configure > Security > Advanced Secu	urity > Intrusion P	revention				
Configure   Pouter   Security   Security Audt   Frevail and ACL   AcL Editor   VPN    VPN   Vandom   Signatures   Voice         Port Adaptication Mappings   2 Cones   Vvice            Pont to Application Mappings   2 Cones   Vvice	home	Intrusion Prevention Sys	tem (IPS)					
Roder         Sacurity         Sacurity Audit         Prevail and ACL         Act Editor         Act Editor         VPN         VPN Components         VPN Components         AAA         Pack Editor         We Shifer Configuration         Intraces Support         Intraces Support         Intraces Support         We Shifer Configuration         Intraces Support         Intraces Support         Intraces Support         Intrace Name         IP Section         Status         Description         Pack Homeout         Intraces Support         Intraces Support         Intrace Name         Interface Name	Configure	~		N IDO MININ	-			
Security Audit         Prevail and ACL         ACL Editor         Actual Update         SEAU VPM         VPN         VPN Components         AAAA         AAAA         AAAA         AAAA         Add Dytate         Signatures         Signatures         Voice	🔁 Router		nboard   IPS Sens	or IPS Migratic	n			
<ul> <li>Firevail and ACL.</li> <li>Firevail and ACL.</li> <li>Adub Update</li> <li>Adub Update</li> <li>SEAP Configuration</li> <li>VPN</li> <li>VPN</li> <li>VPN</li> <li>VPN</li> <li>VPN</li> <li>Vent Action Filters</li> <li>Advanced Security</li> <li>Web Filter Configuration</li> <li>Intrusion Prevention</li> <li>Intrusion Prevention</li> <li>Signatures</li> <li>Signatures</li> <li>Voice</li> </ul>	🛅 Security	🔝 IPS Policies	Interfaces: All	interfaces 💌	🕑 Enable [	🗹 Edit 🥥 Disabl	e 📑 Disable All	
Image: Star Configuration	Security Audit	둸 Global Settings			1	1		[
ACL Editor Act and a standard on a s	Firewall and ACL	🖓 Auto Update						Description
<ul> <li>VPN</li> <li>VPN Components</li> <li>AAA</li> <li>AAA</li> <li>AAA</li> <li>AAA</li> <li>AAA</li> <li>Wab Filter Configuration</li> <li>Totrusion Prevention</li> <li>Intrusion Prevention</li> <li>Intrusion Prevention</li> <li>Signatures</li> <li>Voice</li> </ul>	C1079							
Vani no IP address Disabled off Vani 2 192168.1.3 Disabled off Vani 2 192168.1.3 Disabled on Vani 2 192168.1.3 Disabled o								\$IDMADDR:10.1
AAA Advanced Security Web Filter Configuration Intrusion Prevention Signatures Signatures One Pairs Zones Voice Voice Iter Configuration Happings End to Application Mappings Does Pairs Port to Application Mappings Por	P. Contraction							22
Advanced Security       Web Filter Configuration       Intrusion Prevention       Nac       Octo       02.1x       002.1x       02.1x       0 Port to Application Mappings       2 Cone Pairs       2 Cone S       Voice	and the second se	Grand Contraction Contraction Contraction	Vlan192	192.168.1.3	Disabled	Enabled	on	
Web Filter Configuration     Infrusion Prevention     Infrustry     In								
Intrusion Prevention NAC Solution Display and the second sec		Signatures *						
NAC  CapL  Do2.1x  Port to Application Mappings Cone Pairs Cones Voice  IPS Filter Details:  IPS Filter Details:  IPS rule is enabled, but there is no filter configured for this rule. IPS will scan								
CapL B02:1x Port to Application Mappings 2 one Pairs 2 one s Voice 1 PS Filter Details:  Inbound Filter A 1PS rule is enabled, but there is no filter configured for this rule. IPS will scan								
© 02.1x © Port to Application Mappings © Zone Pairs © Zone Pairs © Zone Pairs © Zone Pairs © Voice ↓ IPS Filter Details: © Inbound Filter ▲ IPS rule is enabled, but there is no filter configured for this rule. IPS will scan	-							
Port to Application Mappings Cone Pairs Cones Voice  IPS Filter Details:  C Inbound Filter  Provide is enabled, but there is no filter configured for this rule. IPS will scan	▶ 🛄 C3PL							
Dene Pairs Dones Voice	302.1×							
⊇ Zones > Voice IPS Filter Details:  ⓒ Inbound Filter ▲ IPS rule is enabled, but there is no filter configured for this rule. IPS will scan	Port to Application Mappings							
toice	Di Zone Pairs							
toice	Zones							
✓ IPS Filter Details:								
IPS Filter Details: IPS rule is enabled, but there is no filter configured for this rule. IPS will scan								
A IPS rule is enabled, but there is no filter configured for this rule. IPS will scan			•					•
A IPS rule is enabled, but there is no filter configured for this rule. IPS will scan			IPS Filter Details	Inhound F	lter C Outh	ound Filter		
all Inbound traffic.					here is no f	ilter configure	d for this rule.	IPS will scan
			all Inbound	l traffic.				
Monitor	3							

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

🚰 172.25.90.31 - TuTTY	
*Sep 13 22:02:42.010:	<pre>%IPS-6-ENGINE BUILDS STARTED: 22:02:42 UTC Sep 13 2008</pre>
Sep 13 22:02:42.022:	%IPS-6-ENGINE BUILDING: multi-string - 9 signatures - 1 of 13 engines
Sep 13 22:02:42.034:	*IPS-6-ENGINE READY: multi-string - build time 12 ms - packets for this engi
will be scanned	
Sep 13 22:02:42.430:	%IPS-6-ENGINE_BUILDING: service-http - 641 signatures - 2 of 13 engines
Sep 13 22:02:42.838:	%IPS-6-ENGINE READY: service-http - build time 404 ms - packets for this eng
will be scanned	
Sep 13 22:02:43.762:	%IPS-6-ENGINE BUILDING: string-tcp - 1106 signatures - 3 of 13 engines
Sep 13 22:02:44.314:	%IPS-6-ENGINE_READY: string-tcp - build time 548 ms - packets for this engin
vill be scanned	
Sep 13 22:02:44.882:	%IPS-6-ENGINE_BUILDING: string-udp - 75 signatures - 4 of 13 engines
Sep 13 22:02:44.910:	%IPS-6-ENGINE_READY: string-udp - build time 24 ms - packets for this engine
11 be scanned	
Sep 13 22:02:44.962:	%IPS-6-ENGINE_BUILDING: state - 31 signatures - 5 of 13 engines
Sep 13 22:02:44.974:	%IPS-6-ENGINE_READY: state - build time 12 ms - packets for this engine will
scanned	
Sep 13 22:02:45.342:	%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 6 of 13 engines
Sep 13 22:02:46.218:	%IPS-6-ENGINE_READY: atomic-ip - build time 872 ms - packets for this engine
ll be scanned	
Sep 13 22:02:46.518:	<pre>%IPS-6-ENGINE_BUILDING: string-icmp - 3 signatures - 7 of 13 engines</pre>
Sep 13 22:02:46.562:	<pre>%IPS-6-ENGINE_READY: string-icmp - build time 44 ms - packets for this engin</pre>
ill be scanned	
Sep 13 22:02:46.566:	%IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13 engines
Sep 13 22:02:46.566:	<pre>%IPS-6-ENGINE_READY: service-ftp - build time 0 ms - packets for this engine</pre>
ll be scanned	
	%IPS-6-ENGINE_BUILDING: service-rpc - 75 signatures - 9 of 13 engines
	%IPS-6-ENGINE_READY: service-rpc - build time 36 ms - packets for this engin
ill be scanned	
	%IPS-6-ENGINE_BUILDING: service-dns - 38 signatures - 10 of 13 engines
Sep 13 22:02:46.750:	%IPS-6-ENGINE_READY: service-dns - build time 16 ms - packets for this engin
vill be scanned	
	%IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13 engines
	%IPS-6-ENGINE_READY: service-smb-advanced - build time 28 ms - packets for t
s engine will be scan	
	<pre>%IPS-6-ENGINE_BUILDING: service-msrpc - 27 signatures - 13 of 13 engines</pre>
	%IPS-6-ENGINE_READY: service-msrpc - build time 40 ms - packets for this eng
e will be scanned	
Sep 13 22:02:46.954:	%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 4944 ms

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.



IPS Policies	🖳 🖓 Impo	ort • Vie	w by:	All Signa	atures \star Criteria: 🗔 🖓 🛶	Total [2363]	Compiled[567]		
둸 Global Settings	R Selec	ct All	🔂 Ad	d • 🖪 E	dit 🔘 Enable 🥥 Disable 🍘 F	Retire 😂 Uni	retire		
8 Auto Update	Enabled	I Si	a ID	SubSig I	Name	Action	Severity	Fidelity Ra	tir
SEAP Configuration	~	a second second	004	0	Bearshare File Request	produce-al	low	100	
😤 Target Value Rating	0	3	128	1	Exchange xexch50 overflo	produce-al	high	75	
Event Action Overrides	0	5	188	3	HTTP Tunneling	produce-al	high	85	-
Event Action Filters	0	3	128	0	Exchange xexch50 overflo	produce-al	high	100	-
🐉 Signatures 🛛 😤	0	5	188	2	HTTP Tunneling	produce-al	high	100	-
All Categories	0	5	188	1	HTTP Tunneling	produce-al	hiah	100	-
🖽 🦲 Attack	0	11	228	0	MSN Chat Joined	produce-al		75	
⊞-· Other Services ⊞-· DoS	0		272	0	Novell iPrint Client ActiveX	20	high	85	-
⊕ 🔁 Reconnaissance	õ		188	0	HTTP Tunneling	produce-al	high	100	-
L2/L3/L4 Protocol	-		406	0	Solaris TTYPROMPT /bin/lc	11	high	85	-
⊞-· Instant Messaging ⊞-· Adware/Spyware	0		520	0	XEXCH50 Command Usag	1		100	-
🖶 🦲 Viruses/Worms/Trojans	0		466	0	Computer Associates Licer	26	high	85	
⊞- 🔁 DDoS ⊞- 🧰 Network Services	0					produce-al	medium	70	_
🗄 🛅 Web Server	0		744	0	IMAP Login DoS				_
🕀 💼 P2P 🕀 🧰 Email	0		170	0	WS_FTP SITE CPWD Buffe	*	high	75	
IOS IPS	•		023	1	DAP Activity	produce-al	low	100	
C Protection     Releases	•	12	023	0	DAP Activity	produce-al	low	85	
E Releases	•	3	117	1	KLEZ worm	produce-al	low	85	
	•	3	117	0	KLEZ Worm	produce-al	low	85	
	•	5	177	1	DoS Arnudp	produce-al	medium	75	
	•								•

© 2009 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

### **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.



Assign Actions	
You can specify actions the sensor should perform when it detect: signature(s). To assign an action, click the checkbox next to the ac indicates the action will be performed. No checkmark indicates the performed. A gray checkmark indicates the action is assigned to s the signatures you selected.	tion. A checkmark e action will not be
<ul> <li>Deny Attacker Inline</li> <li>Deny Connection Inline</li> <li>Deny Packet Inline</li> <li>Produce Alert</li> <li>Reset TCP Connection</li> </ul>	All
OK Cancel Help	

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.

Name	Value	
Signature ID:	6130	
SubSignature ID:	10	
Alert Severity:	Informational 💽	
Sig Fidelity Rating:	60	
Promiscuous Delta:	10	
Sig Description:		
	Signature Name: Microsoft Message Que	
	Alert Notes: This signature is a Meta	
	User Comments: Sig Comment	
	Alert Traits:	
	Release: \$303	
Engine:	String TCP	
	Event Action: Deny Attacker Inline Deny Connection Inline Deny Packet Inline Produce Alert Reset TCP Connection	
	Strip Telnet Options:	
	Snerifi/ Min Match Length:	
	efault Value. Click the icon to edit the value. er-Defined Value. Click the icon to restore the default value.	

# 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.

<ul> <li>IPS Policies</li> <li>Global Settings</li> <li>Auto Update</li> <li>SEAP Configuration</li> <li>Target Value Rating</li> <li>Event Action Overrides</li> <li>Event Action Filters</li> </ul>	Download signature file from Cisco.com  Get the latest Cisco CP file and CLI pkg  List the available files to download  Signature Package in use: \$353.0  Download to:  C:Documents and Settings:\All Users:\Do Browse  Download	-
🦉 Signatures 🐥	Autoupdate  Enable Autoupdate  IPS Autoupdate URL Settings  Username:  Password:  URL:  Example: ftp://10.77.128.170/IOS-8254.zip	
	Schedule Minutes Hours Date Days Every 0 1 2 3 4 5 1 5 5	

- 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'.

IPS Signatu	e Update	X
	Do you want to update your router with this latest IPS signature package?	
	Yes No	

⊡-@ OS ⊡-@ Attack ⊡-@ Other Services	View by:	All Signatures 💌 Criteria:N/A 💌		
🕀 🦳 Other Services	Sig ID	Name	Severity	Deployer
	7220	Pidgin MSN Overflow	high	No
🕀 🛄 DoS 🗄 🧐 Reconnaissance	6066	DNS Tunneling	med	Yes
⊕ 🔄 L2/L3/L4 Protocol ⊕ 🔄 Instant Messaging ⊕ 🔄 Adware/Spyware	7415	OpenLDAP BER Decoding DoS	high	No
	5726	Active Directory Failed Login	med	Yes
sware/Spyware ruses/Worms/Trojar	5726	Active Directory Failed Login	med	Yes
DoS	2157	ICMP Hard Error DoS	med	Yes
Network Services	3109	Long SMTP Command	med	Yes
/eb Server 2P	5477	Possible Heap Payload Construction	high	Yes
mail	3109	Long SMTP Command	med	Yes
STREET STREET	7222	Joomla 1.5 Password Token Bypass	high	No
	7212	Web Application Security Test/Attack	high	No
	7212	Web Application Security Test/Attack	high	No
	6408	IE DHTML Memory Corruption	infor	Yes
	7275	Linux Kernel DCCP dccp_setsockopt_ch	high	No
	3102	Sendmail Invalid Sender	med	Yes
	5807	Indexing Service Cross Site Scripting Vu	high	Yes
IOS IPS UC Protection Releases	7222 7212 7212 6408 7275 3102	Joomla 1.5 Password Token Bypass Web Application Security Test/Attack Web Application Security Test/Attack IE DHTML Memory Corruption Linux Kernel DCCP dccp_setsockopt_cha Sendmail Invalid Sender	hiqh hiqh hiqh infor hiqh med	No No No Yes No 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

Importing Signatures	×
Please wait. Signatures are being imported to the router. This process might take several minutes.	

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

No.	Engine	Status	No of Signatures
R.	multi-string	Loaded	9
2	service-http	Loaded	644
3	string-tcp	Loaded	1108
1	string-udp	Loaded	75
5	state	Loaded	31
6	atomic-ip	Loaded	303
7	string-icmp	Loaded	3
3	service-ftp	Loaded	3
9	service-rpc	Loaded	75
0	service-dns	Compiling	38
1	normalizer	Loaded	9
2	service-smb-advance	Loaded	43
3	service-msrpc	Loaded	27

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

👃 IPS Policies 🛃 Global Settings	Ownload signature file from Cisco.com     Get the latest Cisco CP file and CLI pkg     C List the available files to downlo
👶 Auto Update	Signature Package in use: S354.0
SEAP Configuration	
😤 Target Value Rating	Download to: C:\Documents and Settings\All Users\Do Browse
Event Action Overri	
Event Action Filters	B
🛃 Signatures	» •
	Autoupdate
	🖵 Enable Autoupdate
	IPS Autoupdate URL Settings
	Username: Password:
	URL
	Example: tftp://10.77.128.170/IOS-S254.zip
	Schedule
	Schedule Minutes Hours Date Days
	Minutes Hours Date Days

# Reference

- Cisco IOS IPS on Cisco.com: <u>http://www.cisco.com/go/iosips</u>
- Cisco IOS IPS Signature package: <u>http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup</u>
- Cisco IOS IPS Signature files for CCP: <u>http://www.cisco.com/cgi-bin/tablebuild.pl/iosv5sigup-sdm</u>
- Getting Started with Cisco IOS IPS with 5.x Signature Format:
   <u>http://www.cisco.com/en/US/products/ps6634/products\_white\_paper0900aecd805c4ea8.sh</u>
   <u>tml</u>
- Cisco MySDN: <u>http://tools.cisco.com/MySDN/Intelligence/home.x</u>
- Cisco IOS IPS Configuration Guide: <u>http://www.cisco.com/en/US/products/ps6441/products\_feature\_guide09186a0080747eb0.</u> <u>html</u>
- IPS Management Express: <u>http://www.cisco.com/cgi-bin/tablebuild.pl/ips-ime</u>

...... CISCO.

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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco Stadium/Vision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, IransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems. Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Printed in USA

C11-453847-02 05/09