

How to Use CSM to Configure IOS IPS

Cisco[®] Security Manager(CSM) 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, including new features in Version 3.1, refer to the Cisco Security Manager 3.1 data sheet at

http://www.cisco.com/go/csmanager. Customer can download CSM 3.1 from Cisco.com at http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app

This document will guide users step by step by using CSM 3.1 to perform initial configuration of IOS IPS. For routers already configured with IOS IPS, customers can directly use CSM 3.1 for provisioning tasks.

Note: CSM 3.1 supports only IOS 12.4(11)T2 and later IOS images for configuring IOS IPS.

Step 2 Click on File menu and select New Device to add a device onto the CSM 3.1 Cisco Security Manager - admin Connected to '172.25.90.8" - IO × Edit View Policy Map Icols Help New Device... 3 ? Clone Device... Device: 172-25.90.91 Policy: FlexConfigs Delete Device... Chil+S Prepended FlexConfigs Save View Changes... No. Validate Submit Submit and Deploy... Deploy .. Discard Edit Device Groups... New Device Group. Add Devices to Group Chi+P Ctrl+Q Exit... Inspection Rules Appended FlexConfig No. E Settings Transparent Rules Web Filter Rules E IPS NAT Site to Site VPN Remote Access VPN FT SSL VPN Interfaces FI Platform FlexConfigs Yalues... Preview... 🔺 🐳 🖊 🍵 Sau

Step 1 Run CSM 3.1 client from the local pc

Step 3 In the New Device screen, choose how you would like to add the device. In our case, we choose to Add Device From Network. Click Next.

w 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	3
When you add a device using its configuration file, Cisco Security Manager discovers the device's identifying information, properties and policies from the file.	Ī
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.	
Back Next Finish	Cancel Help

Step 4 Enter the Identity details of the device which you want to add like the hostname, ip address. Click Next.

IP Type: Host Name: Domain Name:	Static	
Domain Name:		
IP Address:	172.25.90.91	
Display Name:*	172.25.90.91	
OS Type:*	×	
	IO5 - 12.3+ IO5 - 12.2, 12.1	
	IO5 - Catalyst 6500/7600	
Discover Device Setti	PIX FWSM	
Discover:	IPS	
	ASA	
	Firewall Policies	
	TPS Policies	
	RA VPN Policies	
	Discover Policies for Security Contexts	

Step 5 Enter the Primary Credentials like Username, Password, Enable password for the IOS Router which you want to add. Click on Finish to add the device onto CSM.

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:	[
RX-Boot Mode	SNMP			

Note: Here we assume that, the user already has a preconfigured router and can login to the router using the credentials.

Step 6 You will see the Discovery Status screen which shows the status of the discovery. If you see that the Status as "Discovery completed" then, you have successfully added a device onto the CSM. Proceed to the next step.

very S	(0(0)				
1		100%			
Devices	to be discovered; discovered successfully; discovered with errors;	Discovery compl 1 1 0	ated with warn	ings	
	ery Details				Discovered From
Туре	Name	Severity		State	
3	172.25.90.91	۵	Discovery C	ompleted with Warnings	Live Device
	172.25.90.91 Messages	0	Discovery Co Severity	Description	
		•		Description The following interface ng a new Access-rule o	s are wide open for traffic as there is no ACL applied on them. Addi In these interfaces means that there will no longer be such implicit p
nterfac	Messages	©	Severity	Description The following interface	s are wide open for traffic as there is no ACL applied on them. Addi in these interfaces means that there will no longer be such implicit p more:
nterfac olicies (Messages es wide open for traffic	©	Severity	Description The following interface ng a new Access-rule of emission of traffic any FastEthernet0 FastEthernet1	s are wide open for traffic as there is no ACL applied on them. Addi in these interfaces means that there will no longer be such implicit p more:
nterfac olicies (xisting	Messages es wide open for traffic discovered	©	Severity A O	Description The following interface ng a new Access-rule ermission of traffic any FastEthernet0	s are wide open for traffic as there is no ACL applied on them. Addi a

Step 7 The 1st thing to do for enabling IPS is to assign a public key, Navigate to FlexConfigs configuration screen on the left menu. Click on the FlexConfigs user interface on the right side of the screen, Press on the Add button.

Cisco Security Manager - admin Elle Edit View Bolicy Map Tools			
10 Eur jen Cury He Fun			
Devices 🖓 🛱		nicy: Flexi onfins	
Filter : 🛛 none 🖌 🖌	Prepended FlexConfig	ß	
 Department Location All 172.25.90.33 172.25.90.34 	No.	Name	Description
AAA Rules	Appended FlexConfigs	s Name	Description
🗍 Transparent Rules	No.	Neme	Description
🗾 Web Filter Rules			
E IPS			
🗍 Signatures			
Event Actions			
General Settings			
Interface Rules			
ST NAT			
Site to Site VPN			
Remote Access VPN			
E SSL VPN			
E Interfaces			
E Platform			Values Proview 💿 🗣 (🕸 🖉 💼
FlexConfigs			Add
			Save
N			

Step 8 Select IOS_IPS_PUBLIC_KEY FlexConfigs from the table and click OK. Click on Save button to save the changes. "IOS_IPS_PUBLIC_KEY" has the config for Public Key.

Filter : none	Name IOS_IPS_PUBLIC_KEY
 CAT6K_ECLB_portchannel CAT6K_firewall_multiple_vlan_interfaces IOS_add_bridge_interface_desc IOS_cA_server IOS_compress_config IOS_console_AAA_bypass IOS_console_AAA_bypass IOS_copy_Image IOS_enable_SSL IOS_PFM IOS_SET_GOAK IOS_Set_clock IOS_VOIP_advance IOS_VOIP_simple IOS_VPN_set_interface_desc IOS_VPN_shutdown_inside_interface IOS_VRF_on_vFW 	
2	

Step 9 Click on the IPS section and navigate to General Settings. Provide the IPS config location on the flash. This location will be used to place the IPS configs. Click on Save button to save changes.

🅼 Cisco Security Manager - admi	in Connected to '172.25.90.8'	_io ×
Ele Edit Yew Bolicy Map Ico	als Heb	
💓 🖉 🗿 🍃 🗿 🕼	B ?	
Devices 🚭	Povice: 172.25.90.33 Policy: General Settings	
Devices	Usivitai 172-23-30-33 Policy, deneral decango	
Filter : 🔤 none 🖌	Block Traffic when IPS engine unavailable	
C Department		
Location	Apply Deny Action on: Ingress Interface	
→) Al	SDEE Properties	
172.25.90.33	Maximum Subscriptions:* 1	
172,25.90.34	Maximum Alerts:* 200	
	Maximum Messages:* 200	
	IPS Config Location Properties	
	IPS Config Location: [lash:/ps	
and the second se	Max retries; 1	
Access Rules		
Inspection Rules	Timeout seconds between retries: 0	
Settings	8	
Transparent Rules	1	
🗾 Web Filter Rules		
E PS		
☐ Signatures		
Event Actions		
General Settings	2	
NAT		
Site to Site VPN		
Remote Access VPN		
E SSL VPN		
🗉 Interfaces		
Platform		
FlexConfigs	×	
		Save
	the second se	Jave

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

Step 10 To Enable IPS, navigate to Interface Rules and Check on "Enable IPS" check box and then, press on the Add Row button.

Step 11 In the Add/Edit IPS Rule screen, enter a Rule Name for the IPS. Click on the Add Row button to include the interfaces on which IPS has to be applied.

Fiter :	22.25.90.33 Policy: Interface Rules ble IPS o. Rule Name ACL Name ADD IPS Rule Add/Edit IPS Rule Rule Name:* mytos ACL Name:	Interface (Direction)	
Device: Device: Fiter: Image: Constraint of the second se	ble IPS o. Rule Name ACL Name ADD IPS Rule Add/Edit IPS Rule Rule Name:* mytos		
Filter : Inone - V Department Location 172.25.90.33 T72.25.90.34	ble IPS o. Rule Name ACL Name ADD IPS Rule Add/Edit IPS Rule Rule Name:* mytos		
	o. Rule Name ACL Name ADD IPS Rule Add/Edit IPS Rule Rule Name;* myjos		
Department Location AI T72.25.90.33 C 172.25.90.34	o. Rule Name ACL Name ADD IPS Rule Add/Edit IPS Rule Rule Name;* myjos		
Location AI AI T72,25.90.33 G172,25.90.34	ADD IPS Rule Add/Edit IPS Rule Rule Name;* myjos		
Al 172.25.90.33 172.25.90.34 (a) AAA Rules Access Rules	Add/Edit IPS Rule Rule Name i* mytos		
 172.25.90.33 172.25.90.34 AAA Rules Access Rules 	Add/Edit IPS Rule Rule Name i* mytos		
SAAA Rules ▲ S Access Rules	Rule Name :* myips		
Access Rules	Rule Name :* myips		
Access Rules			
Access Rules			
Access Rules		Select	
Access Rules	Interface (Direction)	Direction	
Access Rules			
S Inspection Rules			
Settings			
Transparent Rules	E.		
🗾 Web Filter Rules			
E IPS		[Add Row]	
☐ Signatures			
E Event Actions	0	K Cancel Help	
General Settings			
Interface Rules			
Site to Site VPN Remote Access VPN			
SSL VPN			
Jose VPN Interfaces			
Platform			
🗍 FlexConfigs 🗸			
			-

Step 12 Select the Direction in which the IPS rule has to be applied and Click on the Select button to choose the Interfaces.

Direction:*			
◯In	Out	Both	
Interfaces:*		Select	

Filter :	none	~	
sexteen n	2		
	ot11Radio0		
	astEthernet0		
	astEthernet1 astEthernet2		
	astEthernet3		
	astEthernet4		
	an1		
A 🗐	ll-Interfaces		
- And State	xternal		
In In	iternal		
elected:			
/lan1			
₽ /	1		
0.0			

Step 13 Select the Interface from the Interface Selector and Press OK.

Step 14 Click on the Save button to Save the changes.

Cisco Security Manager - admir Edit View Policy Map Took		
	-9.7	
Devices 🔮 🛃	Device: 172.25.90.33 Policy: Interface Rules	
Filter : none 💌	Enable IPS	
Contract Con	No. Rule Name ACL Name Interface (Direction)	
Jucation	1 mylps 🛄 Vlan1 (both)	
- 🧿 Al		
3 172.25.90.33		

E Firewall		
AAA Rules		
Access Rules		
Inspection Rules		
Settings		
Transparent Rules		
🔂 Web Filter Rules		
ej IPS		
🗍 Signatures		
Event Actions		
General Settings		
Thterface Rules		
NAT		
Site to Site VPN		
E Remote Access VPN		
E SSL VPN		
∃ Interfaces		
MILLION COM		

le Edit View Policy Map			1-				
P Devices		Device Properties Policy Object Manager	ace Rules				
Devices	50	Site-To-Site VPN Manager	des ridics				
Filter : - none - N		Deployment Manager					
Department	-	Policy Discovery Status	ACL Name	1	Interface (Direction)	fi -	
Location		Show Containment	All and the second s	Vian1	isototean assembly as		
🕶 🧿 Al.		Inventory Status					
3 172.25.90.33	-	Catalyst Summary Info					
3 172.25.90.34		Device Manager					
		IPS Event Viewer					
	C	Apply IPS Update					
		Preview Configuration					
\$ \$ \$		Device OS Management	×:				
AAA Rules	B	Audit Report					
Access Rules	- 6						
☐ Inspection Rules E Settings	100	Configuration Archive					
Transparent Rules		Backup					
Web Filter Rules		Security Manager Diagnostics					
IPS	-	Security Manager Administration					
☐ Signatures	0	Security Holigager Automotionation					
Event Actions							
General Settings		E					
Interface Rules							
Site to Site VPN							
Bite to bite VPN Remote Access VPN							
E SSL VPN							
Interfaces							
Platform							
FlexConfigs		× .					

Step 15 Click on the Tools menu and Select Apply IPS Update to install the latest IPS signatures.



ype: Signatu	re Updates 🐱			Latest Available:	IPS-CS-MGR-sig-S282-reg-E1.zip
	File	Sig.	Engine	Latest Downloaded:	IPS-CS-MGR-sig-S282-req-E1.zip
S-CS-MGR-sig-S		278	1	Latest Applied:	IP5-CS-MGR-sig-5282-req-E1.zip
o co marcolg o	ero rod erieb	270	•	Latest Deployed:	IPS-CS-MGR-sig-S282-req-E1.zip
S-CS-MGR-sig-S	280-req-E1.zip	280	1	Last Checked On:	Apr 19 2007 10:46:37
S-CS-MGR-sig-S	282-reg-E1.zip	282	1	Last Downloaded On:	Apr 19 2007 10:45:48
			-774	Last Deployed On:	Apr 23 2007 17:56:38
					Check For Updates
					Download Latest Updates
Jpdate Details	e			1	
File: Description:		g-5282-req-E1.zip g-5282-req-E1.zip			
Date:	Apr 19 2007	Size:	3.8MB		
Release:	5282	Required Engine Le	vel: E1		
			Back	Next	inish Cancel

Type: Local Signatures Policies	172.25.90.33	
Department		
 ✓ All ✓ ▲ 172.25,90.33 		
172:25.90.33		
Select All Deselect All		

Step 17 Select the devices on which the IPS update has to be applied and click Next.

Step 18 Click on the Finish button to apply the signatures.

1000 0 IP options-Bad Option List Produce Alert Informational 75 Default to	Enabled Risk I
	lse 25
	lse 25
1003 0 IP options-Provide s,c,h,tcc Produce Alert Informational 100 Default fo	lse 25
1004 0 IP options-Loose Source Route Produce Alert. High 100 Default fo	lse (100
1005 8 IP options-SATNET ID Produce Alert Informational 100 Default fr	lse 25
	ue 100
	1

	3 3 ?							
Devices	Dev	ke: 172.25.9	90.33 Policy: Signatures					
Filter : none		Filter: (→ n						
a Department			×	~		Apoly	Clear	
Jucation		ID Sub	A REAL PROPERTY AND A REAL	Actions	Sevenky	Fideity	Source	a,
🕶 🧿 Al	1	000_0	IP options-Bad Option List	Produce Alert	Informational	75	Default	1
3 172.25.90.33		<u>(10)</u> 0	IP options-Record Packet Route	Produce Alert	Informational	100	Default	8
	1	002 8	IP options-Timestomp	Produce Alert	Informational	100	Default	3
	1	003 0	IP options-Provide s,c,h,tcc	Produce Alert	Informational	100	Default	8
	3	0 400	TP options-Loose Source Route	Produce Alert	High	100	Default	
	1	005 0	IP options-SATNET ID	Produce Alert	Informational	100	Dafault	ġ.
***	1	006 0	IP options-Strict Source Route	Produce Alert	High	100	Default	1
] Firewall	A 19	007. 0	IPvő over IPv4	Produce Alert	Informational	100	Default	s.
AAA Rules		101 0	Unknown IP Protocol	Produce Alert	Informational	11111	Default	1
Access Rules		102 0	Impossible IP Packet	Produce Alert	High	100	Default	
Settings			and the second	Produce Alert	10000	100	Default	
Transparent Rules		an weeks	IP Localhost Source Spoof	Handbackseenselless	High	in a state		
Web Filter Rules		102 0	RFC 1918 Addresses Seen	Produce Alert	Informational	111111	Default	8
] IPS	1	108 0	IP Packet with Proto 11	Produce Alert	High	100	Default	
Signatures	= 4	103 0	Cisco IOS Interface DoS	Produce Alert	Medium	75	Default	8
E Event Actions	1	102 1	Gisco IOS Interface DoS	Produce Alert	Medium	75	Default	3
General Settings	1	109 2	Cloco IOS Interface DoS	Produce Alert	Medium	75	Default	2
Interface Rules	1	102 3	Gisco JOS Interface DoS	Produce Alert	Medium	75	Default	
NAT	1	201 0	IP Fragment Overlap	Deny Packet Inline, Produce Alert	Informational	100	Default	8
Site to Site VPN Remote Access VPN	-	202 0	IP Fragment Overrun - Datagram Too Long	Deny Packet Inline, Produce Alert	High	100	Default	-
E SSL VPN		2 CF (10)		and the second secon	975977		>	- C
Interfaces	1				View Update Level		AN	-
8 Platform	*				Herr opdate Level		0000	<u>II</u>)

Step 19 Navigate to IPS and Click on Signatures to view the list of all the signatures.

Step 20 Go to File Menu and click on "Submit and Deploy..." to deploy IPS on the IOS router.

New Device Ctrl+N @	3 ? Deuroi 172/25/9	1.33 Policy: Signatures					
Delete Device		100.1001130010103			_		1
Save ColeS	- Filter: (no	ne)					
View Changes	1	~	× .		Apply	Cisai	
<u>V</u> alidate	ID Sub	Name	Actions	Severity	Fidelity	Source	ŝ,
Submit	<u>1000</u> 0	IP options-Bad Option List	Produce Alert	Informational	75	Default	1
Submit and Deploy	1001 0	IP options-Record Packet Route	Produce Alert	Informational	100	Default	
Deploy	1002 0	IP options-Timestamp	Produce Alert	Informational	160	Default	2
Discard	1003 0	IP options-Provide s, c, h, to:	Produce Alert	Informational	160	Default	
Edit Device Groups	1004 0	IP options-Loose Source Route	Produce Alert	High	160	Default	5
New Device Group	1005 0	IP options-SATNET ID	Produce Alert	Informational	100	Default	
Add Devices to Group	1006 0	IP options-Strict Source Route	Produce Alert	High	100	Default	1
Eriot Chil+P	1007 0	IPv6 over IPv4	Produce Alert	Informational	100	Default	8
Egit Ctrl+Q	1101 0	Unknown IP Protocol	Produce Alert	Informational	75	Default	2
T Inspection Rules	1102 0	Impossible IP Packet	Produce Alert	High	100	Default	
E Settings	1104 0	IP Localhost Source Spoof	Produce Alert	High:	100	Default	
🗇 Transparent Rules	1107 8	RFC 1918 Addresses Seen	Produce Alert	Informational	160	Dafault	8
Web Filter Rules	1105 0	IP Packet with Proto 11	Produce Alert	High	100	Default	1
I IPS	1109 0	Cisco IOS Interface DoS	Produce Alert	Medium	35/11/	Default	8
Signatures = Event Actions	1109 1	Cisco IOS Interface DoS	Produce Alert	Medium	75	Default	2
General Settings	1109 2	Cisco IOS Interface DoS	Produce Alert	Medium	75	Default	
Interface Rules	1109 3	Gisco IOS Interface DoS	Produce Alert	Medium	75	Default	
NAT	1201 0	IP Fragment Overlap	Deny Packet Inline, Produce Alert	Informational	12222	Default	
Site to Site VPN	111111111	AUMUNUMUNUMUNU	Deny Packet Inline, Produce Alert	High	100	Default	8
Remote Access VPN	1202 0	IP Fragment Overrun - Datagram Too Long	Deny Packet Initie, Produce Alert	nign	100	Deraut	
E SSL VPN	1×		7			1000 U.S.	
] Interfaces				View Update Level		7/	

▼ ☑ ☐ Changed Devices	
172.25.90.33	
Edit deploy meth	hod Add other devices

Step 21 Select the device on which you want to deploy the changes and Click "Deploy"

Step 22 View the Deploy status to verify if there are any errors.

		oyment started by admi			
oloyment Status Detai	ls				
	44	XEX	-		
Status:		Deployed (1 out of 1 device	completed.)		
Deployment Job Name	91	admin_job_2007-04-24 10:5	3:10.468		
Devices To Be Deploye		1			
Devices Deployed Suc		1			
Devices Deployed With	h Errors:	0			
- Long to be to the	(1 Jac - Jac 10				
eployment Details (1 Device	/1 loaded) Stat	us Summar	/ Method	Config	Transcript
72.25.90.33	SUCCEEDED	Warning: 2	Device	Ģ	Ģ
					F
					F
Mec	canec		Description		
1/10/02/2	sages	Severity	Description >>>> Difference of file "C:\PR	OGRA~1\C5COpx\MDC\te	mp\2007.04.24_10.53
ut of Band Change: CLI	isagēs		Description >>>> Difference of file "C:\PR 15_job_admin_job_2007-04-24 740\diff_archived" and file "C:\	OGRA~1\C5COpx\MDC\te 10_53_10_468\\phase1\1 PROGRA~1\C5COpx\MDC\	mp\(2007.04.24_10.53) 72_25_90_33_429498i temp\(2007.04.24_10.5
ut of Band Change: CLI peration Successful		Severity A @	Description >>>> Difference of file "C:\PR 15_job_admin_job_2007-04-24	OGRA~1\C5COpx\MDC\te 10_53_10_468\\phase1\1 PROGRA~1\C5COpx\MDC\	mp\(2007.04.24_10.53) 72_25_90_33_429498i temp\(2007.04.24_10.5
ut of Band Change: CLI peration Successful g update compilation warr	ning	Severity	Description >>>> Difference of file "C:\PR 15 job_admin_job_2007-04-24 740\diff_archived" and file "C:\ 3.15_job_admin_job_2007-04-2 80740\diff_uploaded".	OGRA~1\C5COpx\MDC\te 10_53_10_468\\phase1\1 PROGRA~1\C5COpx\MDC\	mp\(2007.04.24_10.53) 72_25_90_33_429498i temp\(2007.04.24_10.5
ut of Band Change: CLI peration Successful g update compilation warr g update engine compilati	ning	Sevenity () () () () () () () () () ()	Description >>>> Difference of file "C:\PR 15_job_admin_job_2007-04-24 740\diff_archived" and file "C:\ 3.15_job_admin_job_2007-04-3 80740\diff_uploaded". 9a >	OGRA~1\C5COpx\MDC\te 10_53_10_468\\phase1\1 PROGRA~1\C5COpx\MDC\	mp\(2007.04.24_10.53) 72_25_90_33_429498i temp\(2007.04.24_10.5
ut of Band Change: CLI iperation Successful ig update compilation warr ig update engine compilati iperation Successful	ning	Severity (i) (i) (i) (i) (i) (i) (i) (i)	Description >>>> Difference of file "C:\PR 15_job_admin_job_2007-04-24 740(dff_archived" and file "C:\ 3.15_job_admin_job_2007-04-3 80740\dff_uploaded". 9a	OGRA~1\C5COpx\MDC\te 10_53_10_468\\phase1\1 PROGRA~1\C5COpx\MDC\	mp\2007.04.24_10.53 72_25_90_33_429498 temp\2007.04.24_10.5
ut of Band Change: CLI iperation Successful ig update compilation war ig update engine compilati	ning	Severity	Description >>>> Difference of file "C:\PR 15_job_admin_job_2007-04-24 740\diff_archived" and file "C:\ 3.15_job_admin_job_2007-04-3 80740\diff_uploaded". 9a >	OGRA~1\C5COpx\MDC\te 10_53_10_468\\phase1\1 PROGRA~1\C5COpx\MDC\	mp\2007.04.24_10.53 72_25_90_33_429498 temp\2007.04.24_10.5
ut of Band Change: CLI peration Successful ig update compilation warr ig update engine compilati peration Successful	ning	Severity (i) (i) (i) (i) (i) (i) (i) (i)	Description >>>> Difference of file "C:\PR 15_job_admin_job_2007-04-24 740\diff_archived" and file "C:\ 3.15_job_admin_job_2007-04-3 80740\diff_uploaded". 9a >	OGRA~1\C5COpx\MDC\te 10_53_10_468\\phase1\1 PROGRA~1\C5COpx\MDC\	mp\2007.04.24_10.53 72_25_90_33_429498 temp\2007.04.24_10.5
ut of Band Change: CLI peration Successful ig update compilation warr ig update engine compilati peration Successful	ning	Severity (i) (i) (i) (i) (i) (i) (i) (i)	Description >>>> Difference of file "C:\PR 15_job_admin_job_2007-04-24 740\diff_archived" and file "C:\ 3.15_job_admin_job_2007-04-3 80740\diff_uploaded". 9a >	OGRA~1\C5COpx\MDC\te 10_53_10_468\\phase1\1 PROGRA~1\C5COpx\MDC\	mp\2007.04.24_10.53 72_25_90_33_429498 temp\2007.04.24_10.5

Reference

- Cisco IOS IPS on Cisco.com: <u>http://www.cisco.com/go/iosips</u>
- Getting Started with Cisco IOS IPS with 5.x Signature Format: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod/white_paper0900aecd805c4ea8.shtml
- Cisco IOS IPS Configuration Guide: <u>http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a0080747eb0.</u> html



Americas Headquarters Cisco Systems, Inc. 172 West Teamer Drive San Jose, CA 95134-1706 USA www.cisco.com Tel: 405 526-4000 300 353 NETS (6537) Fax: 408 527-5683 Asia Pacific Headquartens Cisco Systems, inc. 169 Robanson Road #28-01 Capital Tower Singepore 059812 www.daca.com Tel:+85 6817 7777 Fac:+85 6817 7799 Europe Headquarters Cieco Systems International BV Hoarterbergpark Haarterbergwag 13-19 1101 CH Amsterdam The Netherlands www-europe.cisc.com Tel: -310 620 620 0791 Fax: -310 20 857 1100

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

@2007 Olace Systems, Inc. All rights baserved. COVP, the Gisco logo, and the Gisco Balere Bridge logo are trademarks of Gisco Systems, Inc., Changling the Way We Work, Live, Play, and Learn te a service mark of Caso Systems, Inc. and Access Register, Altrand, BYX, Calalyst, CCIA, CODP, COIP, CQMA, CONP, CCBP, Cisco, the Cisco Carlified Internativer's Expertised, Gisco Press, Cisco Systems, Capital, the Gisco Systems, Inc., and Access Register, Altrand, BYX, Calalyst, CCIA, CODP, COIP, CQMA, CONP, CCBP, Cisco, the Cisco Carlified Internativer's Expertised, Gisco Press, Cisco Systems, Capital, the Gisco Carlified Internativer's Expertised, Gisco Press, Cisco Systems, Capital, the Gisco Systems logo, Cisco Unity, Enterprised/Solars, Ether/Channel, EtherSwith, Fest Stop, Follow Me Browsing, FormShare, Gisco Press, Cisco, Lincy, Enterprised/Solars, Hardinary, Motter, Fest Stop, Follow Me Browsing, FormShare, Gisco Press, Cisco, Lincy, Enterprised/Solars, Hardinary, Motter, Fest Stop, Follow Me Browsing, FormShare, Gisco Press, Cisco, Lincy, Hondow, MartingPiaco, Mott, Network, Fest Stop, Follow Me Browsing, FormShare, Gisco Press, Cisco, Lincy, StockWise, The Fest Step, Follow Me Browsing, FormShare, Register, Resket, PK, ProCenner, Sontal State, StackWise, The Featuret Way to Increase Your Informed, Capital State State

All other trademerks mentioned in this document or Wobelia are the property of their respective extrems. The use of the word partner does not imply a partnership relationship between Glace and any other company. (27059)

Printed in USA

C27-411960-00 6/07