

Migrating Cisco IPS Version 4.x Signature Format to Version 5.x for Cisco IOS IPS

Starting with Cisco IOS® Software Release 12.4(11)T, Cisco IOS Intrusion Prevention System (IPS) introduces support for the Cisco IPS Software Version 5.x signature format. The 5.x signature format is a version-based signature definition XML format also used by other Cisco appliance-based IPS products. Support for signatures and signature definition files (SDFs) in Cisco IPS Version 4.x are discontinued in this and further Cisco IOS T-Train Software releases.

Customers running Cisco IOS IPS with Version 4.x signature format SDFs can reconfigure Cisco IOS IPS to use Cisco predefined signature categories—Basic and Advanced signature sets—or use the Cisco IOS IPS migration utility to migrate previous Version 4.x SDF files into Cisco IPS Version 5.x format signature sets.

This document details the steps for migrating from a Cisco IPS 4.x format SDF and enabling the migrated signature set in Cisco IOS Software Releases 12.4(11)T or later. For more details on how to configure Cisco IOS IPS in Cisco IOS Software Release 12.4(11)T or later, please refer to the Cisco IOS IPS Configuration Guide at

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/ips_v5.htm

It is highly recommended to run Cisco IOS IPS migration before upgrading to Cisco IOS Software Release 12.4(11)T or a later image.

Steps to Migrate Version 4.x SDF Files

The migration script requires a Cisco IPS 4.x format SDF file and optionally the CLI configuration file that contains Cisco IOS IPS configuration information used on a router that was running a Cisco IOS Software release earlier than 12.4(11)T. The migration script searches for commands containing **ip ips signature <sigid> [<sigsubid>] disabled** within the router configuration file. If the configuration file does not contain this CLI command(s), there is no need for the migration script to read the CLI configuration file. Conversion of signatures, as such, will be based solely on the SDF.

If running the migration script before upgrading Cisco IOS IPS to Cisco IOS Software Release 12.4(11)T or later, follow the process “Executing Cisco IOS IPS Migration Script”.

If running the migration script after upgrading Cisco IOS IPS to Cisco IOS Software Release 12.4(11)T or later:

1. Verify any need to convert CLI commands, **ip ips signature <sigid> [<sigsubid.>] disabled** as mentioned above.
2. Save the router’s CLI configuration to a file, for example, use the command **copy running-config flash:ipscfg.cfg**. This command will back up the existing router configuration to flash in a file named **ipscfg.cfg**. The migration will use this file later for full 4.x to 5.x signature

format conversion. The process “Executing Cisco IOS IPS Migration Script” can then be followed.

Executing Cisco IOS IPS Migration Script

The migration script is available from Cisco.com at: <http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup>. Save the migration script to the router's flash or to a router-accessible location, such as a Trivial File Transfer Protocol (TFTP) server.

The migration script will convert an SDF from Cisco IPS Version 4.x format to Version 5.x format. The migration script supports only the following signature parameters:

```
severity
action
enabled.
```

In addition, the migration script can also read from a pre- Cisco IOS Software Release 12.4(11)T IOS IPS configuration file and migrate disabled signatures that were configured by the CLI **ip ips signature <sigid> <sigsubid> disabled** command.

Note: Custom (non Cisco) signatures will not be converted using this script.

Following is an example to migrate the IPS 4.x formatted file **sdmips.sdf** to Cisco IOS IPS in Cisco IOS Software Release 12.4(11)T with Cisco IOS IPS 5.x signature format support.

```
C2821#tclsh flash:ios-ips-migrate.tbc
This migration script will migrate Signature Definition Files from 4.x
format to 5.x format.
The migration script will migrate only the following signature
parameters - severity, action, enabled - for Cisco (non-custom)
signatures.
Do you want to continue? [y/n] y
Please choose an IOS config file from which to migrate IOS IPS
configuration.
Config File: [startup-config]
The following SDF locations were found configured in startup-config:
flash://sdmips.sdf
Please provide SDF to migrate from the above list or of your own
choice: flash://sdmips.sdf
Migrating following SDF file (this will a take few minutes):
flash://sdmips.sdf
Time Elapsed: 0:02:23
Migration completed successfully. The migrated file is
C2821-sigdef-delta.xml
C2821#
```

The migration script will first display a brief text about its function. Next, the script provides an option to choose a location from where to read the current (pre-migration) configuration for Cisco IOS IPS. The default reads from the startup configuration. If you have previously saved a configuration to a TFTP server or the router's flash, specify the location at the prompt.

For example

Use `ftp:// 192.168.1.5/<router CLI configuration>` to tell the script to load a CLI configuration from TFTP server 192.168.1.5.

Use `flash://<saved-configuration>` to read from a file saved on flash.

Loading Migrated Signatures into Cisco IOS IPS in Cisco IOS Software Release 12.4(11)T

After signature migration is complete, upgrade the router's Cisco IOS image to 12.4(11)T if you have not already done so. Once the router is reloaded, perform the following steps.

1. Enable Cisco IOS IPS

Following is an example to enable Cisco IOS IPS on a Cisco 2821 router. For detailed information of how to configure Cisco IOS IPS, please refer to the Cisco IOS IPS Configuration Guide at

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t11/ips_v5.htm.

```
C2821#mkdir ips
Create directory filename [ips]?
Created dir flash:ips
C2821#conf t
Enter configuration commands, one per line. End with CNTL/Z.
C2821(config)#ip ips name MYIPS
C2821(config)#ip ips config location ips
C2821(config)#ip ips signature-category
C2821(config-ips-category)#category all
C2821(config-ips-category-action)#retired true
C2821(config-ips-category-action)#exit
C2821(config-ips-category)#exit
Do you want to accept these changes? [confirm]
C2821(config)#
```

Next, configure crypto signature public key. Copy and paste the following key into the router.

```

crypto key pubkey-chain rsa
  named-key realm-cisco.pub signature
  key-string
  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
  quit
  exit
  exit

```

Finally, enable Cisco IOS IPS on interfaces.

```

C2821(config)#
C2821(config)#interface gigabitEthernet 0/0
C2821(config-if)#ip ips MYIPS in
C2821(config-if)#ip ips MYIPS out
C2821(config-if)#exit

```

2. Load Latest Signature Package

```

C2821#copy tftp://192.168.1.5/IOS-S253-CLI.pkg idconf

```

This command will load signatures from signature package **IOS-S253-CLI.pkg** into Cisco IOS IPS. Please note that **ios-ips signature category all** was configured in Step 1; this retired all signatures. After the signature package is successfully loaded, no signatures will be selected and compiled.

3. Load Migrated Signatures

The last step is to load the migrated signatures. Use the following command to load the migrated XML file (**<router-hostname>-sigdef-delta.xml**) to Cisco IOS IPS.

```

copy flash:C2821-sigdef-delta.xml idconf

```

Once the router has parsed the Version 5.x formatted signature file, successful migration is complete. Use **show ip ips signature count** to check signature summary status and **show ip ips signature details** to view specific details on all signatures.



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0609R)