Release Notes for Cisco Configuration Professional 1.3

April 21, 2009

These release notes support Cisco Configuration Professional (Cisco CP) version 1.3. They should be used with the documents listed in the "Related Documentation" section.

These release notes are updated as needed. To ensure that you have the latest version of these release notes, go to http://www.cisco.com/go/ciscocp. In the Support box, click **General Information** > **Release Notes**. Then, find the latest release notes for your release.

Contents

This document contains the following sections:

Introduction

Cisco CP is a GUI-based device management tool that allows you to configure Cisco IOS-based access routers, including Cisco integrated services routers, Cisco 7200 series routers, and the Cisco 7301 router. Cisco CP simplifies router, security, unified communications, wireless, WAN, and basic LAN configuration through GUI-based, easy-to-use wizards. Cisco CP is installed on a PC.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Routers that are ordered with Cisco CP are shipped with Cisco Configuration Professional Express (Cisco CP Express) installed in router flash memory. Cisco CP Express is a light weight version of Cisco CP. You can use Cisco CP Express to configure basic security features on the router's LAN and WAN interfaces. Cisco CP Express is available on the router Flash memory.

System Requirements

This sections describes PC and router system requirements. It contains the following parts:

- PC System Requirements
- Router System Requirements
- Cisco CP Ordering Options

PC System Requirements

Table 1 lists the system requirements for a PC running Cisco CP. Although the Cisco CP application requires JRE to run, the Cisco CP Express application included with Cisco CP can run under the native Java Virtual Machine in the supported browsers, and also JRE.

Table 1 PC System Requirements

System Component	Requirement
Processor	2 GHz processor or faster
Random Access Memory	1 GB
Hard disk available memory	400 MB
Operating System	Any of the following: • Microsoft Windows Vista Business Edition • Microsoft Windows Vista Ultimate Edition • Microsoft Windows XP with Service Pack 2 or later • Mac OSX 10.5.6 running Windows XP using VMWare 2.0
Browser	Internet Explorer 6.0 or Internet Explorer 7.0
Screen Resolution	1024 X 768
Java Runtime Environment	JRE versions minimum 1.5.0_11 upto 1.6.0_10 are supported.
Adobe Flash Player	Version 10.0 or later, with Debug set to No
Secure Shell (SSH)	Required for secure connections with the router. Versions 1.99 and 2.0 are supported.

Router System Requirements

Router System Requirements are described in the following parts:

- Supported Routers
- Supported Network Modules
- Supported Interface Cards
- Supported Adapters, Processing Engines, and Service Engines
- Cisco IOS Releases
- Cisco IOS IPS Feature History
- Required IP Address Configuration Information
- Router Configuration Requirements

Supported Routers

Table 2 lists the routers that Cisco CP supports. Cisco CP does not support Telco/CO router models.

Table 2 Supported Routers

Cisco 800 Series	Cisco 1800 Series	Cisco 2800 Series	Cisco 3800 Series	Cisco 7000 Series
CISCO815 CISCO815-VPN-K9	CISCO1801 CISCO1801-M CISCO1801/K9 CISCO1801-M/K9 CISCO1801WM-AGE/K9 CISCO1801W-AG-E/K9 CISCO1801W-AG-B/K9 CISCO1801W-AG-C/K9 CISCO1801W-AG-N/K9	Cisco 2801 Cisco 2811 Cisco 2821 Cisco 2851	Cisco 3825 Cisco 3825-NOVPN Cisco 3845 Cisco 3845-NOVPN	Cisco 7204VXR Cisco 7206VXR Cisco 7301
CISCO851-K9 CISCO851W-G-A-K9 CISCO851W-G-E-K9 CISCO851W-G-J-K9	CISCO1802 CISCO1802/K9 CISCO1802W-AG-E/K9			
CISCO857-K9 CISCO857W-G-A-K9 CISCO857W-G-E-K9	CISCO1803/K9 CISCO1803W-AG-B/K9 CISCO1803W-AG-E/K9			
CISCO861-K9 CISCO861W-GN-A-K9 CISCO861W-GN-E-K9 CISCO861W-GN-P-K9	CISCO1805-D CISCO 1805-D/K9			

Table 2 Supported Routers

Cisco 800 Series	Cisco 1800 Series	Cisco 2800 Series	Cisco 3800 Series	Cisco 7000 Series
CISCO871-K9 CISCO871-SEC-K9 CISCO871W-G-A-K9 CISCO871W-G-E-K9 CISCO871W-G-J-K9	CISCO1811/K9 CISCO1811W-AG-B/K9 CISCO1811W-AG-C/K9 CISCO1811W-AG-N/K9			
CISCO876-K9 CISCO876-SEC-K9 CISCO876-SEC-I-K9 CISCO876W-G-E-K9	CISCO1812/K9 CISCO1812 W-AG-E/K9 CISCO1812 W-AG-C/K9			
CISCO877-K9 CISCO877-M-K9 CISCO877-SEC-K9 CISCO877W-G-A-K9 CISCO877W-G-E-K9 CISCO877W-G-E-M-K9	CISCO1841			
CISCO878-K9 CISCO878-SEC-K9 CISCO878W-G-A-K9 CISCO878W-G-E-K9	C1861-UC-4FXO-K9 C1861-UC-2BRI-K9 C1861-SRST-B/K9 C1861-SRST-C-B/K9 C1861-SRST-C-F/K9 C1861-SRST-F/K9			
CISCO881-K9 CISCO881W-GN-A-K9 CISCO881W-GN-E-K9 CISCO881W-GN-P-K9 CISCO881G-K9 CISCO881GW-GN-A-K9 CISCO881GW-GN-E-K9 CISCO881G-S-K9 CISCO881G-V-K9 CISCO881G-A-K9 C881SRST-K9 C881SRSTW-GN-A-K9 C881SRSTW-GN-E-K9				
CISCO887V-K9				

Table 2 Supported Routers

Cisco 800 Series	Cisco 1800 Series	Cisco 2800 Series	Cisco 3800 Series	Cisco 7000 Series
CISCO888-K9 CISCO888W-GN-A-K9 CISCO888W-GN-E-K9 CISCO888G-K9 CISCO888GW-G-AN-K9 CISCO888GW-G-EN-K9				
C888SRST-K9 C888SRSTW-GN-A-K9 C888SRSTW-GN-E-K9				
CISCO891-K9 CISCO891W-AGN-A-K9 CISCO891W-AGN-N-K9				
CISCO892-K9 CISCO892W-AGN-E-K9				

Supported Network Modules

Table 3 lists the network modules that Cisco CP supports.

Table 3 Supported Network Modules

Network Modules	Enhanced Network Modules	Wide Area Application Services (WAAS) Modules	Advanced Integration Modules (AIMs)	Voice Network Modules
NM-4T	NME-IPS-K9	NME-WAE-502-K9	AIM-VPN/BP II PLUS	NM-HD-1V
NM-1FE2W-V2	NME-16ES-1G-P	NME-WAE-522-K9	AIM-VPN/EP II PLUS	NM-HD-2V
NM-1FE-FX-V2	NME-X-23ES-1G-P	NME-WAE-302-K9	AIM-VPN/HP II PLUS	NM-HD-2VE
NM-2FE2W-V2	NME-XD-24ES-1S-P		AIM-VPN/SSL-1	NM-HDA-4FXS
NM-1FE-FX	NME-XD-48ES-2S-P		AIM-VPN/SSL-2	NM-HDV2
NM-4A/S (synchronous only)	NME-VMSS-16		AIM-VPN/SSL-3	NM-HDV2-1T1/E1
NM-8A/S (synchronous only)	NME-VMSS-HP-16		AIM-IPS-K9	NM-HDV2-2T1/E1
NM-CIDS-K9	NME-VMSS-HP-32		AIM-CUE	EVM-HD-8FXS/DID
NM-16ESW	NME-TPO		AIM-TPO1	EM-HDA-8FXS
NM-16ESW-1GIG			AIM-TPO2	EM-HDA-4FXO
NM-16ESW-PWR				EM2-HDA-4FXO
NM-16ESW-PWR-1GIG				EM-HDA-3FXS/4FXO
NMD-36ESW-PWR				EM-HDA-6FXO
NMD-36ESW-PWR-2GIG				EM-4BRI-NT/TE
				NM-CUE
				NM-CUE-EC
				NME-CUE

Supported Interface Cards

Table 4 lists the interface cards that Cisco CP supports.

Table 4 Supported Cards

WAN Interface Cards (WICs)	High-speed WAN Interface Cards (HWICs)	Voice Interface Cards
WIC-1T	HWIC-1T	VWIC2-1MFT-T1/E
WIC-2T	HWIC-2T	VWIC2-2MFT-T1/E1
WIC-2A/S (Frame Relay, PPP, HDLC, no asynchronous)	HWIC-4T	VIC2-4FXO
WIC-1ADSL	HWIC-2A/S	VIC2-2FXS
WIC-1DSU-T1-V2	HWIC-4A/S	VIC2-2FXO
WIC-1B-S/T-V3	HWIC-4ESW	VIC2-2BRI-NT/TE
WIC-1AM	HWIC-4ESW-POE	VIC-2DID
WIC-2AM	HWIC-8A	VIC-4FXS/DID
WIC-4ESW	HWIC-8A/S-232	VIC3-4FXS/DID
WIC-1SHDSL-V2	HWIC-D-9ESW	VIC3-2FXS/DID
WIC-1SHDSL-V3	HWIC-D-9ESW-POE	VIC3-2FXS-EDID
WIC 1ADSL-DG	HWIC-1DSU-T1	
WIC 1ADSL-I-DG	HWIC-16A	
	HWIC-ADSL-B/ST	
	HWIC-ADSLI-B/ST	
	HWIC-1ADSL	
	HWIC-1ADSLI	
	HWIC-1ADSL-M (WIC card with Annex M)	
	HWIC-2SHDSL	
	HWIC-4SHDSL	
	HWIC1-ADSL-M	
	HWIC-1CABLE-D-2	
	HWIC-1CABLE-E/J-2	
	HWIC-1FE	
	HWIC-2FE	
	HWIC-AP-AG-A	
	HWIC-AP-AG-E	
	HWIC-AP-AG-J	
	HWIC-AP-G-A	
	HWIC-AP-G-E	
	HWIC-AP-G-J	

Supported Adapters, Processing Engines, and Service Engines

Table 5 lists the adapters, processing engines and service engines that Cisco CP supports.

Table 5 Supported Adapters, Processing Engines, and Service Engines

Port Adapters on Cisco 7000 Series Routers	Service Adapters on Cisco 7000 Series Routers	Network Processing Engines and Network Service Engines on Cisco 7000 Series Routers
PA-2FE-TX	SA-VAM	NPE-225
PA-2FE-FX	SA-VAM2	NPE-400
PA-8E	SA-VAM2+	NPE-G1
PA-4E	C7200-VSA	NPE-G2
		NSE-1

Cisco IOS Releases

Cisco CP is compatible with the Cisco IOS releases listed in Table 6.

Table 6 Cisco CP-Supported Routers and Cisco IOS Versions

Router Model	Earliest Cisco CP-Supported Cisco IOS Versions
Cisco 815	• 12.4(11)T
Cisco 850 series	• 12.4(9)T
Cisco 860 series	• 12.4(15)XZ
Cisco 870 series	• 12.4(9)T
Cisco 880 series	• 12.4(15)XZ
Cisco 887 series Cisco 890 series	• 12.4(15)YB1
Cisco 1801 Cisco 1802 Cisco 1803	• 12.4(9)T
Cisco 1805	• 12.4(15)XY
Cisco 1811 Cisco 1812	• 12.4(9)T
Cisco 1841	• 12.4(9)T
Cisco 1861	• 12.4(11)XW
Cisco 2800	• 12.4(9)T
Cisco 3800	• 12.4(9)T
Cisco 7000	• 12.4(9)T

Cisco IOS IPS Feature History

Table 7 shows the Cisco IOS IPS feature history, and lists the Cisco IOS releases that offered each set of features, beginning with the latest release. This information is available in the Cisco IOS IPS Deployment Guide available at the following link.

http://www.cisco.com/en/US/products/ps6634/prod_white_papers_list.html

Note Cisco CP supports Cisco IOS version 12.4(9)T and later.

Table 7 Feature History of Cisco IOS IPS

Cisco IOS Release	Cisco IOS IPS Features or Improvements
12.4(11)T2	Support for a versioned-based signature definition format used by Cisco appliance-based IPS products, and the predefined Basic and Advanced signature categories.
12.4(6)T	Session setup rate performance improvements
12.4(3a)/12.4(4)T	String engine memory optimization
12.4(4)T	MULTI-STRING engine support for Trend Labs and Cisco Incident Control System Performance improvements Distributed Threat Mitigation (DTM) support
12.4(2)T	Layer 2 transparent intrusion prevention system (IPS) support
12.3(14)T	Support for three string engines (STRING.TCP, STRING.UDP, and STRING.ICMP) Support for two new local shunning event actions: denyAttackerInline and denyFlowInline
12.3(8)T	Support for Security Device Event Exchange (SDEE) protocol Support for ATOMIC.IP, ATOMIC.ICMP, ATOMIC.IPOPTIONS, ATOMIC.UDP, ATOMIC.TCP, SERVICE.DNS, SERVICE.RPC, SERVICE.SMTP, SERVICE.HTTP, SERVICE.FTP, and OTHER engines

Determining the Cisco IOS Release

To determine the release of Cisco IOS software currently running on your Cisco router, log in to the router and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the Cisco IOS release on the second output line:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) C1700 Software (c1700-k8sv3y7-mz) Version 12.2(13)ZH
```

Required IP Address Configuration Information

Table 8 provides the required IP address configuration for the PC. Use this information to complete the section "Task 4: Configure the IP Address On the PC" in the *Cisco Configuration Professional Quick Start* Guide.

Table 8 Required PC IP Address Configurations

Router Model	DHCP Server	Required PC IP Address Configuration
Cisco 815, Cisco 85x, Cisco 86x, Cisco 87x, Cisco 88x, Cisco 891, Cisco 892, Cisco 180x, Cisco 1805, Cisco 1811 and 1812	Yes	Obtain an IP address automatically.
Cisco 1841, Cisco 1861, Cisco 28xx, Cisco 38xx	No	Static IP address from 10.10.10.2 to 10.10.10.6 Subnet Mask: 255.255.255.248

Router Configuration Requirements

In order to run Cisco CP, a router configuration must meet the requirements shown in Table 9.

Table 9 Router Configuration Requirements

Feature	Requirement	Configuration Example

Secure access	SSH and HTTPS	`Router(config)# ip http secure-server`
		`Router(config)# line vty 0 4`
		`Router(config-line)# transport input ssh`

Nonsecure access	Telnet and HTTP	`Router(config)# ip http server`
		`Router(config)# line vty 0 4`
		`Router(config-line)# transport input telnet`

User privilege level	15	`Router(config)# username cisco privilege 15 secret 0 cisco`

The default configuration file meets all Cisco CP requirements. The default configuration file has the name cpconfig-*model_number*.cfg. For example, the configuration file for the Cisco 860 and Cisco 880 routers is cpconfig-8xx.cfg.

Cisco CP Ordering Options

Table 10 on page 11 describes the ordering options under which Cisco CP can be ordered.
Cisco Configuration Professional (Cisco CP Express) is a product that is shipped in router flash memory when the router is ordered with Cisco CP.

Table 10 Cisco CP Ordering Options

Ordering Options	Description
CCP-CD	Cisco CP: Shipped on CD Cisco CP Express: Shipped in router flash memory SSL Client: Shipped in router flash memory Default Configuration File: Shipped in router flash memory and in NVRAM
CCP-CD-NOCF	Cisco CP: Shipped on CD Cisco CP Express: Shipped in router flash memory SSL Client: Shipped in router flash memory Default Configuration File: Shipped in router flash memory **Note** This ordering option does not provide the default configuration file for Cisco 800 series routers.
CCP-EXPRESS	Cisco CP: Not shipped Cisco CP Express: Shipped in router flash memory SSL Client: Shipped in router flash memory Default Configuration File: Shipped in router flash memory and in NVRAM
CCP-EXPRESS-NOCF	Cisco CP: Not shipped Cisco CP Express: Shipped in router flash memory SSL Client: Shipped in router flash memory Default Configuration File: Shipped in router flash memory. **Note** This ordering option does not provide the default configuration file for Cisco 800 series routers.

New and Changed Information

This section contains new information about Cisco CP, and any information about Cisco CP that has changed.

This section contains the following parts:

- New Features
- New Hardware Support

New Features

Cisco CP 1.3 supports the following new features.

- DMVPN QoS—Dynamic Multipoint Virtual Private Network [DMVPN] QoS feature allows you to configure QoS policies on a per-tunnel basis. When you configure QoS policies on a per-tunnel basis, Cisco CP treats each security association tunnel as a separate traffic class and allows you to configure a unique policy map for each class. The configuring QoS policies per-tunnel feature is supported on routers that are running the Cisco IOS Release 12.4(22)T and later advanced security images.
- ACL Object Groups—Object group-based access control lists (ACLs) helps you to simplify the static and dynamic ACL deployments for large user-access environments on Cisco IOS routers. By using the ACL Object Groups feature, the administrator can group users, devices, or protocols into object groups and create access control entries (ACEs). Each ACE can then permit or deny a group of users access to a group of servers or services. The ACL Object Groups feature is supported on routers running Cisco IOS Release 12.4(20)T and later.
- CTCP—You can use Cisco CP to configure your router to use Cisco Tunneling Control Protocol (CTCP) to enable encrypted traffic to go through a firewall. The Enable Easy VPN Access Through Firewall feature is supported on Cisco routers that are running Cisco IOS Release 12.4(20)T and later.
- IPS Signature Download and Auto Update—The Download IPS Signature Package allows you to download a signature package from Cisco.com to your PC and then send it to the router. You can either download the latest signature package or you can specify the package that you want from a list of available packages. The Download IPS Signature Package feature is supported on Cisco routers that are running Cisco IOS Release 12.4(11)T2 and later. The Auto Update IPS Signature Package allows you to configure the router to automatically download the IPS signature package from a specified local server at periodic intervals. The Auto Update IPS Signature Package from Local Server feature is supported on Cisco routers that are running Cisco IOS Release 12.4(11)T2 and later.
- NCE Module—You can use Cisco CP to configure Network Capacity Expansion (NCE) modules. NCE modules increase the data transfer rate on a WAN link and improves the response time of remotely hosted applications. The NCE module feature is supported on routers running Cisco IOS Release 12.4(15)XY and later.
- Performance Routing—Allows you to optimize network traffic based on performance metrics of the traffic or the cost structure of network links.
- International Dial Plan—Initially, the International Dial Plan feature was available in North America only. Now it is available in UK and Spain also. In addition, it allows users to create custom templates.

New Hardware Support

Cisco CP 1.3 adds support for the following advanced integration module and network modules:

- HWIC-1DSU-T1
- HWIC-1T
- HWIC-2T
- HWIC-2A/S
- NME -IPS-K9

- HWIC-1ADSL-M
- NME -TPO
- AIM -TPO1
- AIM -TPO2
- NME -VMSS-16
- NME -VMSS-HP16
- NME -VMSS-HP32
- Cisco 891/892/887 and Annex M platforms

Limitations and Restrictions

This section describes restrictions and limitations that may apply to Cisco CP. It contains the following parts:

- Cisco CP Requirements to Run on Microsoft Windows Vista
- Cisco CP Minimum Screen Resolution
- Restrictions for Cisco 7204VXR, Cisco 7206VXR, and Cisco 7301 Routers

Cisco CP Requirements to Run on Microsoft Windows Vista

In order to run Cisco CP under Microsoft Windows Vista, Cisco CP must be installed in Administrator mode. You can do this by following the Microsoft Windows instructions to create an administrative account, and then logging on to the PC using that account name and password before installing Cisco CP. Failure to do this will require you to right-click on the Cisco CP icon or menu item, and choose “Run as administrator” each time you want to run Cisco CP.

Cisco CP Minimum Screen Resolution

Cisco CP requires a screen resolution of at least 1024 x 768.

Restrictions for Cisco 7204VXR, Cisco 7206VXR, and Cisco 7301 Routers

The following restrictions apply to Cisco CP running on Cisco 7204VXR, Cisco 7206VXR, and Cisco 7301 Routers:

- The Cisco CP Express application is not supported. You must use the Cisco IOS CLI to give the router an initial configuration that will enable you to connect to the router using a browser.
- WAN configuration is not supported. Cisco CP supports configuration of Ethernet and Fast Ethernet interfaces.
- The Cisco CP Reset feature is not available.
- No default configuration file is supplied. To run Cisco CP, you must provide a configuration that includes the commands necessary to support operation of Cisco CP.

Important Notes

This section contains important information for Cisco CP. It contains the following sections:

Cisco IOS Enforces One-Time Use of Default Credentials

To address CSCsm25466, Cisco IOS images included with recent shipments of Cisco 800, Cisco 1800, Cisco 2800, and Cisco 3800 routers, enforce the one-time use of the default user name and password provided in the Cisco CP configuration file. If you bypass Cisco CP or Cisco CP Express and use a console or Telnet connection to log into the router, the login and exec banners warn you that you must change the user name “cisco” and password “cisco” before you log off of the router. If you do not change the credentials as directed, you will not be able to log on to the router the next time that you attempt to do so.

The following Cisco IOS releases enforce the one-time use of the default credentials:

- 12.4(11)T or later
- 12.4(11)SW, 12.4(11)SW1, 12.4(11)XV, 12.4(11)XJ
- 12.4(9)T5, 12.4(9)T6
- 12.3(21), 12.3(22)

Follow the procedure in this section to secure the router by creating a new username and password, to remove the login banner and exec banner warnings, and to save the configuration changes to the router startup configuration.

Note If you login to the router using a Telnet or a console connection but do not complete the steps in this procedure, be aware of the following:

- If you do not change the default username and password, and then log off the router, you will not be able to log into the router again without entering the **reload** command. No additional warning is given before you log off.
- If you do not change the default username and password, but do enter the **write memory** command before ending the session, future logins will be disabled. In this case, you will need to follow the password recovery procedure at the following link:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml

To secure the router, remove the banner warnings and save the changes to the router startup config, complete the following steps:

Step 1 Connect the light blue console cable, included with your router, from the blue console port on your router to a serial port on your PC. Refer to your router's hardware installation guide for instructions.

Step 2 Connect the power supply to your router, plug the power supply into a power outlet, and turn on your router. Refer to your router's quick start guide for instructions.

Step 3 Use HyperTerminal or a similar terminal emulation program on your PC, with the terminal emulation settings of 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control, to connect to your router.

Step 4 When prompted, enter the username **cisco**, and password **cisco**.

Step 5 Enter configuration mode by entering the following command:

```
yourname# configure terminal
```

Step 6 Create a new username and password by entering the following command:

```
yourname(config)# username username privilege 15 secret 0 password
```

Replace *username* and *password* with the username and password that you want to use.

Step 7 Remove the default username and password by entering the following command:

```
yourname(config)# no username cisco
```

Step 8 To remove the login banner, enter the following command:

```
yourname(config)# no banner login
```

The login banner warning will no longer appear.

Step 9 To remove the exec banner, enter the following command:

```
yourname(config)# no banner exec
```

The exec banner warning will no longer appear.

Step 10 Leave configuration mode, by entering the following command:

```
yourname(config)# end
```

Step 11 Copy the configuration changes to the startup configuration by entering the following command:

```
yourname# copy running-config startup-config
```

When logging into the router in the future, use the username and password that you created in Step 6.

Cisco CP Merge and Replace Configuration Functions Fail Under Some Conditions

The problem described here is caveat CSCsj21989. If you attempt to merge configuration changes made using the Cisco CP Config Editor feature, or replace the running configuration with a configuration from the Config Editor, the router configuration will not be changed if there is a network device with a Network Address Translation (NAT) IP address, or a cache engine in the connection between the PC and the router. If you need to make changes to the router configuration that you would normally make using the Cisco CP Config Editor, use the Cisco IOS CLI instead.

Cisco CP Security Dashboard May Display Threats Unrelated to Your Cisco IOS IPS Installation

Some (or all) of the top threats you obtain using the Cisco CP Security Dashboard may not pertain to your Cisco IOS IPS installation. After you deploy the signatures applicable to the top threats displayed by the Cisco CP Security Dashboard, the dashboard may still display some (or all) top threats with a red icon because applicable signatures could not be found. Those remaining top threats are unrelated to your Cisco IOS IPS installation and not a danger to your router running Cisco IOS software.

Cisco CP May Lose Connection to Network Access Device

This note concerns the Network Admission Control (NAC) feature.

If the PC used to invoke Cisco CP returns a posture state (Healthy, Infected, Checkup, Quarantine, or Unknown) and if the group policy on the ACS server attached to the posture token assigned to the PC has a redirect URL configured, the connection between Cisco CP and the router acting as the Network Access Device (NAD) may be lost. The same problem can occur if an exception list entry attached to a policy with a redirect URL is configured with the IP address or MAC address of the PC.

If you try to reinvoke Cisco CP from this PC, you will not be able to do so because the browser will be redirected to the location specified in the redirect URL.

There are two workarounds for this problem:

- Ensure that the PC that you use to invoke Cisco CP attains a posture token which has an associated group policy on the ACS server that is not configured with a redirect URL.
- Alternatively, use Cisco CP to create a NAC exception list entry with the IP address or MAC address of the PC you use to invoke Cisco CP. Note that the exception list entry created for the PC should be associated to an exception policy which does not have a redirect URL configured in it.

For more information, see the links in the Cisco CP NAC online help pages.

Popup Blockers Disable Cisco CP Online Help

If you have enabled popup blockers in the browser you use to run Cisco CP, online help will not appear when you click the help button. To prevent this from happening, you must disable the popup blocker when you run Cisco CP. Popup blockers may be enabled in search engine toolbars, or may be standalone applications integrated with the web browser.

Microsoft Windows XP with Service Pack 2 blocks popups by default. In order to turn off popup blocking in Internet Explorer, go to **Tools** > **Pop-up Blocker** > **Turn Off Pop-up Blocker**.

If you have not installed and enabled third-party pop up blockers, go to **Tools** >**Internet Options** > **Privacy**, and uncheck the **Block popups** checkbox.

Disable Proxy Settings

Cisco CP will not start when run under Internet Explorer with proxy settings enabled. To correct this problem, choose **Internet Options** from the Tools menu, click the **Connections** tab, and then click the **LAN settings** button. In the LAN Settings window, disable the proxy settings.

Security Alert Dialog May Remain After Cisco CP Launches

When Cisco CP is launched using HTTPS, a security alert dialog box that informs you of possible security problems and asks you if you want to proceed with program launch may appear. This can happen if the router does not have the following global configuration command in the running configuration:

```
ip http timeout-policy idle 600 life 86400 requests 10000
```

Screencasts for Cisco CP Features

Instead of online help, we have provided screencasts for the following features:

- Performance Routing
- Video Surveillance
- International Dial Plan
- Outgoing Calls
- Dialing Restrictions

These screencasts are located at: http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrcst/ccpsc.html. You must have internet access to view the screencasts.

Cisco Configuration Professional Is Already Running Message

If Cisco CP has not been shut down properly, and you try to relaunch it, you may see the following message: "Cisco Configuration Professional is already running. Only one occurrence can run at a time." To correct this problem and relaunch Cisco CP, do the following:

Step 1 Press **Ctrl Alt Delete**, and click **Task Manager**.

Step 2 In the Windows Task Manager dialog, click **Processes**.

Step 3 In the Image Name column, highlight the process javaw.exe.

Step 4 Click **End Process**.

Step 5 Wait 30 seconds, and then restart Cisco CP.

Technical Support Logs Do Not Appear on Desktop

If you have followed the procedure described in New Features to create technical support logs, but the folder does not appear on the desktop, there may be installed Java applications preventing this feature from working properly. To check, go to **Start** > **Control Panel** > **Add or Remove Programs**, and scan the list for Java applications. Remove the Java applications that you can, and try again.

Discovery Never Completes

Because of Microsoft Windows Java caching issues, Cisco CP is sometimes unable to complete discovery of a device. To fix this issue, complete the following steps:

Step 1 Choose **Application** > **Exit** to shut down Cisco CP.

Step 2 Go to **Start** > **Control Panel** > **Java**. The General tab is displayed.

Step 3 In the Temporary Internet Files box, click **Delete Files**.

Step 4 In the displayed dialog, leave all file types checked, and click **OK**.

Step 5 Click **OK** in the Java control panel to close it.

Step 6 Restart Cisco CP.

Caveats

Caveats describe unexpected behavior in Cisco CP. This section contains the following:

- Resolved Caveats from Cisco CP 1.2
- Open Caveats—Cisco CP 1.3

Resolved Caveats from Cisco CP 1.2

Table 11 lists caveats that are resolved in Cisco CP 1.3.

Table 11 Resolved Caveats in Cisco CP 1.3

Bug ID	Summary
CSCsu27005	T1/E1: Displays "Configuration Failed" error message while changing time-slots, in SSH.
CSCsq60961	Unnecessary commands are delivered when enabling SDEE.
CSCsr38576	Cisco CP unable to handle UUT with large number of buffered logs.
CSCsr56744	SSH authorization dialog popup during re-discovery.
CSCsr60469	Add button should be disabled for default, unsupported, and externally defined ACL.
CSCsr75730	Users settings: improper error for phone username same as router username.
CSCsu11635	T1E1: Cisco CP unable to configure "clock source" at day two in secure mode.
CSCsw68206	T1/E1: "Configuration Failed" error when changing the clock priority in Secure mode.
CSCsr50598	TREND URL Filtering policy is not shown in URL policy map.
CSCsv36258	Not able to delete the Partial Easy VPN Remote configuration.
CSCsm89756	Router and Security should also discover algorithms supported by VPN hardware modules.
CSCin44264	Cisco CP should also discover algorithms supported by VPN hardware modules.
CSCin48956	Cisco CP does not deliver the command "ip tcp adjust-mss 1452" to unsupported VLAN1 interfaces.
CSCin54600	Replace option in Forward wizard with Management access ACLs associated blocks router access.
CSCin63415	Analog connection deleted through wizard mode shows unsupported option.
CSCin63613	Primary link fails if backup is configured with primary next hop option.
CSCed13205	Editing Network Time Protocol (NTP) server in Cisco 72xx does not deliver the NTP update-calendar.
CSCef43267	Loopback0 interface IP address is not correctly populated.
CSCef50389	The client statistics for the Easy VPN server are all shown as 0 in the VPN status window.
CSCef63313	Easy VPN client testing reports with respect to one server.
CSCef72022	Unknown commands are delivered from Router and Security in monitor view.

Table 11 Resolved Caveats in Cisco CP 1.3 (continued)

Bug ID	Summary
CSCef73879	VPN troubleshooting report for Maximum Transmission Unit (MTU) problem is misleading in certain cases.
CSCef77689	WAN troubleshooting fails to report when the Cisco IOS image does not support the show pppoe session command.
CSCef89472	A download exception message may appear in the Java console when Cisco CP is launched on a PC running Japanese Windows 2000, or Japanese Windows.
CSCsa40535	VPN status in the Monitor windows does not show IPsec security association (SA) status for DMVPN.
CSCei33081	The Load File from PC function fails when the Cache engine is present between PC and router.
CSCsb26386	Easy VPN tunnel is not coming up after entering the XAuthentication credentials.
CSCsb59200	Cisco CP crashes when dismissing the Import Signature dialog.
CSCei84100	When the applications security policy blocks some Peer-to-Peer (P2P) applications, but permits others, blocked applications may be able to download files.
CSCej01054	The security policy does not block all the Instant Messaging (IM) applications.
CSCej07924	User is able to download some of the files even though Peer-to-Peer application is blocked.
CSCek33306	Cisco CP should be launched if you enable WebVPN on same interface through CLI.
CSCek38259	Changing the port 443 to custom port does not remove NAT rule.
CSCsh39685	Certificate Authority (CA) server cannot be enabled through Cisco CP for 12.4(11)T.
CSCsh41150	Assigned IP address is shown as 0.0.0.0 in Easy VPN Server monitoring.
CSCsh46525	Not able to delete Easy VPN remote or dissociate VT.
CSCsi03518	Cisco CP access pass-through is not added in WebVPN wizard and its Edit.
CSCsj21989	Security merge configuration is not working with devices behind NAT.
CSCsk51555	Command delivery is not working in WMM Access category.
CSCsk88931	Central Manager Registration fails when entering the login credentials for Network Module.
CSCsk98378	Gateway is not associated with the context after relaunch of Cisco CP.
CSCsl00095	Split DNS details are not shown in 12.4(15)T1 image.
CSCsl32119	IPS: Takes around 15 minutes to get the IPS signature details on Cisco 7301 router.
CSCsl47234	Command delivery fails when the 'if-authenticated' is selected along with other methods.
CSCsm34923	Deactivate short cut keys to open the Internet Explorer related menus and tool bar button.
CSCsm64482	WAAS: Warning message is displayed while clicking the link for Central Manager.
CSCsm93416	Splash screen hides all the existing windows on desktop
CSCso44518	IPS: 7204VXR: Unable to view signatures.
CSCso66478	IOS Issue: Monitor traffic details are not shown for Firewall(PI1).
CSCso83037	Backspace key is not working for any text box in Cisco CP.

Table 11 Resolved Caveats in Cisco CP 1.3 (continued)

Bug ID	Summary
CSCsr43587	Flash File Management: Displays wrong message when loading 12.4(20)T images.
CSCsr61142	Wrong IPSec tunnel status is being reported.
CSCsr79413	Wrong warning message is displayed in WAAS while registering with central manager.
CSCsr76694	SSLVPN: Recommended task: Enable DSN shows wrong behavior.
CSCsr92422	Cisco CP not showing any error, incase of Configuration failure due to DSPs.
CSCsu06985	Creation of analog phone gives failure error message.
CSCsu07155	Interface G. SHDSL is listed for non supported device.
CSCsu11542	Memory leak is seen while accessing the voice screens.
CSCsu18131	Discovery fails for device with special character in hostname.
CSCsw29015	Cisco CP blank screen issue because Cisco CP was not shutdown properly.
CSCsw31280	CLI preview dialog moves to the background.
CSCsw38566	BRI trunk is not detected for Cisco 888 SRST model.
CSCed31085	Cisco CP should not load from boot images (boot images) mini IOS.
CSCdy80223	HTTP server appends unnecessary characters.
CSCea89054	Deleting a WAN connection is not removing the “ip nat insid” command from the LAN interface configuration.
CSCin44119	When Easy VPN tunnel is up, do not designate tunnel interfaces as NAT interface.
CSCed08825	DMVPN WM: Latency in displaying wizard screens with any Java Plug-in.
CSCed18560	In Cisco 837x router, auxiliary-backup connection should be deleted when backup is deleted.
CSCed30721	When dangling desc. exists, NTP Forward pass-through traffic is not added.
CSCsh11991	Migrating custom signatures.
CSCsh44720	Issues are noticed when Cisco CP is invoked in Internet Explorer 7.0.
CSCso78069	Intersite VOIP dialpeer label is not editable after RFR.
CSCsq48311	Cisco CP should not open multiple instance of Airconnect application for the same device.
CSCsr17365	Issue with Time Edit operation in Night Service and After Hours.
CSCsr27018	Security screens content does not re-paint.
CSCsr55637	Disc Details: Messages are truncated.
CSCsr65388	Red error border does not clear for mandatory field.
CSCsr75879	Cisco CP shows two instance of the closing windows to click instead of one.
CSCsq34313	Since Cisco CP does not support the specifying “enable” password, the discover function fails.
CSCsr50953	No option to enter the IP address for the Websense/N2H2.
CSCsr99608	During RFR Cisco CP does not check for overlapping numbers.

Open Caveats—Cisco CP 1.3

Table 12 lists caveats that are open in Cisco CP 1.3.

Table 12 Open Caveats in Cisco CP 1.3

Bug ID	Summary	Additional Information
CSCsz07490	Java applet not initialized and Cisco CP stuck with JRE 1.6.0_12 or 1.6.0_13.	**Symptom:** Cisco CP is stuck at the initial launch screen when trying to launch the application for the second or subsequent times. **Conditions:** JRE version 1.6.0_12 or 1.6.0_13 is installed on your PC. **Workaround:** To resolve this issue, disable Java applets to run in new JVM instances. Do the following: 1. Go to **Start > Control Panel > Java**. 2. Click on the **Advanced** tab. 3. Double-click **Java Plug-in** to expand its contents. 4. Uncheck the **Enable next-generation Java Plug-in** check box. **Further Problem Description:** In JRE versions 1.6.0_12 and 1.6.0_13, the Java applets run separate JVM instances. These JVM instance sometimes have a problem in loading the applet. When there is a failure, even after you close the Cisco CP application, the Java process continues to run in the background. Use the workaround so that the Java applet uses the same JVM instance instead of separate instances.
CSCsy91343	Cisco CP unable to discover device when using the IP Address of SSL VPN Gateway.	**Symptom:** Cisco CP is unable to discover the device when using IP address of SSL VPN gateway. **Conditions:** SSL VPN gateway (webvpn) is configured. **Workaround:** Use *one* of the following workarounds. • Change the webvpn port to something other than 443, and then make Cisco CP connect to the outside interface. • From your PC, VPN into the network, and then make Cisco CP connect to an inside interface • Add a second IP address to the outside interface using the **ip address** ***<network> <mask>*** **secondary** command and then make Cisco CP connect to it.

Table 12 Open Caveats in Cisco CP 1.3 (continued)

Bug ID	Summary	Additional Information
CSCsw39659	Enhancement in Cisco CP for CUE post initialization.	**Symptom:** The data fields for Post Initialization wizard are not retained on Cisco CP. If the user reverts back using back button, the screen displays an error message. It is an overhead to enter all values again. **Condition:** This issue occurs only when any field value is invalid on the post initialization wizard. **Workaround:** Filling in all correct values at the first instance can avoid this situation.
CSCsx52358	Not able to view the signatures in Cisco CP.	**Symptom:** You cannot configure IPS feature using Cisco CP and will not be able to view or modify signatures. **Condition:** This problem occurs only with Cisco IOS 12.4(20)T and Cisco IOS 12.4(24)T images. **Workaround:** There is no workaround.
CSCsx57080	Cisco CP launch failure with Internet Explorer 8.0.	**Symptom:** Cisco CP is unable to launch successfully when the Internet Explorer 8.0 release candidate 1 is running. **Condition:** This issue is seen only with Internet Explorer 8.0 version. **Workaround:** Downgrade the Internet Explorer 8.0 version to Internet Explorer 7.0.
CSCsx59378	Splash screen stays on when Flash Player is unavailable in Windows Vista.	**Symptom:** Cisco CP launch Splash screen does not disappear when the Adobe Flash Player is unavailable and the Splash screen overlaps with the Close screen warning window. **Condition:** When the application is started in Windows Vista platform with out flash player, launch splash screen does not disappear. **Workaround:** Install Flash Player before starting the application.
CSCsx72139	Voice folder disabled in the Graphical User Interface (GUI).	**Symptom:** Voice menu folder is disabled in the Cisco CP Graphical User Interface (GUI). **Condition:** This problem occurs when the router is running a Cisco IOS 12.4(24)T or later image and if the router memory is insufficient to enable the telephony-service. **Workaround:** Upgrade the DRAM in the router.

Table 12 Open Caveats in Cisco CP 1.3 (continued)

Bug ID	Summary	Additional Information
CSCsx74556	NCE_ Configure must be disabled for All View User.	**Symptom:** You cannot configure a Forward rule with a numbered OGACL and this feature does not work with Cisco IOS 12.4(22)T, Cisco IOS 12.4(20)T, and Cisco IOS 12.4(20)T1 images. **Condition:** When you configure Forward Rule with a numbered OGACL, the application displays exception and the command delivery fails as the numbered ACLs are not supported in Cisco IOS 12.4(22)T, Cisco IOS 12.4(20)T, and Cisco IOS 12.4(20)T1. This feature is not supported in Cisco CP. **Workaround:** Use the Cisco IOS 12.4(24)T or 12.4(22)T1 version in which the issue has been fixed.
CSCsy04507	Java control panel not shown in 64-bit Vista PC.	**Symptom:** The Java control panel is not displayed in the Windows Vista control panel on a 64-bit machine. **Condition:** When you install the JRE 6u10 b05 on a Windows Vista 64 AMD machine, the Java Control Panel (JCP) does not appear in the Windows Control Panel. **Workaround:** Launch the Java control panel from the task bar icon or by running the “javaws -viewer”.
CSCsy20018	Cisco CP's behavior when IPSec VPN with OGACL configured from CLI.	**Symptom:** Cisco CP does not support the case of IPSec VPN configurations with OGACL which is configured by using the Router CLI. **Condition:** Cisco IOS does not support OGACLs with IPSec VPN. However, the IOS allows the user to configure IPSec VPN with OGACL and does not inform the user that this an invalid configuration.Cisco CP will not handle this scenario as a valid configuration. **Workaround:** There is no workaround.
CSCsy39505	Pushing of signature package fails.	**Symptom:** When Cisco CP is used for configuring IPS this exception will be seen while uploading signatures and while getting IPS related information. **Condition:** When two applications are accessing the IPS signatures at same time this will be seen. **Workaround:** Need to close the other applications which is accessing IPS and then rediscover the device through Cisco CP.
CSCsy49785	OGACL: Service group not working for QoS, SSLVPN, NAC, and Access-class.	**Symptom:** An OGACL with Service Object group is not working for QoS, SSL VPN, NAC, and Access-class. **Condition:** The traffic is not matched when you associate an OGACL with Service object group to QoS, SSL VPN, NAC and Access-class. **Workaround:** There is no specific workaround for this problem.Use normal ACLs with these features.

Table 12 Open Caveats in Cisco CP 1.3 (continued)

Bug ID	Summary	Additional Information
CSCsy54022	Certificate not prompted during discovery in a sequence.	**Symptom:** When an IP address of the router is changed, Cisco CP does not prompt to accept the certificate during Cisco CP discover process. **Condition:** Cisco CP cannot connect back to the router in secure mode because the certificate is not accepted. This issue occurs only when the IP address by which Cisco CP is discovered is changed and rediscovery is done in a secure mode. **Workaround:** Discover the Cisco CP using non-secure mode and rediscover using secure mode.
CSCsy61239	Config enabled although telephony-service is not configured.	**Symptom:** The options such as Hunt-group, Night Service Bell, After Hours and Dialing Restrictions can be configured through Cisco CP without configuring Telephony-service. **Condition:** In absence of telephony service configuration, the user may be able to configure Hunt-group, Night Service bell, After hours or Dialing restrictions successfully via Cisco CP. These configurations are not usable until the telephony-settings are configured on the router. **Workaround:** User has to configure mandatory telephony-settings before configuring any telephony features.
CSCsy66017	Unable to deploy IPS with SDM IPS signature packages >=386.	**Symptom:** Cisco CP cannot configure and deploy IPS with Signature package S386 or later. **Condition:** This is seen when you configure the IPS with Signature package S386 or later in IPS 5x supported IOS images. **Workaround:** Do *one* of the following: • Use IOS-CLI IPS package for configuring IPS if Signature package is S386 or later. • Use Signature package first to configure which is less than S386 then use import or update through security dashboard to S386 or later.
CSCsy73163	Security dashboard empty after deploying a signature package.	**Symptom:** After updating the IPS signatures through Security dashboard in Cisco CP, the top threats listed in security dashboard becomes empty. Clicking the update threats button is not listing the threats. **Conditions:** This is seen with images supporting IPS 5x when updating with latest signature packages. **Workaround:** There is no workaround.

Table 12 Open Caveats in Cisco CP 1.3 (continued)

Bug ID	Summary	Additional Information
CSCsy80678	The order of initialization screens seems to have some issue.	**Symptom:** When the user initialize more than one module using the initialize wizard, the initialize screen fails to complete the process. **Workaround:** There is no workaround.
CSCsy82573	Digital signature java applet hidden behind Cisco CP application windows.	**Symptom:** When you enable secure connections to devices by using Cisco CP 1.3 version, the Java certificate confirmation window is hidden behind the Cisco CP application windows. The Cisco CP application fails the connection to the device after timing out on waiting for confirmation of the certificate. **Conditions:** This issue occurs when you use SSL to connect to the device. **Workaround:** Do *one* of the following: • Do not use SSL for connection. • If using SSL, upon launch of the discover process, minimize the Cisco CP windows to see the Java certificate window. After confirming, restore the Cisco CP windows to use the application. • In combination with bullet 2, choose Grant Always for the Java Certificate and this problem should not reoccur unless the certificate change
CSCsy82684	The post initialization wizard does not complete configuring in few cases.	**Symptom:** The post initialization wizard does not complete the entire IOS CLI needed for the module to be complete the session. **Conditions:** When you configure the post initialization wizard, the configuration does not complete in few cases. **Workaround:** There is no workaround.
CSCsy84069	CLI commands are not removed on the router when changing from FXS to DID Cisco CP.	**Symptom:** The Station ID and the Station Name commands are not removed from the Voice port configuration on the Router when the mode is changed from FXS to DID. **Condition**: Configure a voice port as FXS port with Description, Station ID, and Station Name through and change the mode from FXS to DID. The Station ID and Station Name commands persist on the voice port config on the Router. **Workaround**: There is no workaround.
CSCsv96570	Cannot change the sequence number with 12.4 (22)T.	**Symptom**: When the existing sequence number is changed to some other number, the package entry disappears from the user interface. **Conditions:** The issue is seen in Cisco IOS 12.4(22)T. **Workaround:** The package should be re-installed.

Table 12 Open Caveats in Cisco CP 1.3 (continued)

Bug ID	Summary	Additional Information
CSCsx20540	Java console closes and CP hangs when running tests.	**Symptom:** Java console closes and Cisco CP hangs when running the tests with JRE 1.6.0_11. **Conditions:** When you upgrade to JRE 1.6.0_11 plug-in, Java console closes andCisco CP hangs. Error message is displayed while navigating through security screen. **Workaround:** Go to **Start** > **Control Panel** > **Java** > **Java** tab > Click on **View** under Java Applet Runtime Settings > Select the JRE 1.6.0_11 > Set the 'Java runtime Parameters' with the value '-Dsun.java2d.d3d=false' >Click on **Ok.** Relaunch the Cisco CP.
CSCsx80772	ACL Object Groups: Cisco CP should not support associating OGACL for IPSec VPN.	**Symptom:** Cisco CP should not allow associating an OGACL with IPSec VPN. **Conditions:** IPsec VPN in IOS does not support OGACL. **Workaround:** Use normal ACLs with IPSec VPN.
CSCsx80787	Numbered ACLs with Object group are not shown in User Interface.	**Symptom:** When any numbered ACL's with object group is created in router, the ACL's are not populated correctly in Cisco CP. This occurs because the running configuration has some junk characters with object-group keyword. **Conditions:** This issue is seen only in Cisco IOS 12.4(20)T, Cisco IOS 12.4(20)T1, Cisco IOS 12.4(20)T2, and Cisco IOS 12.4(22)T. **Workaround:** Use the Cisco IOS 12.4(24)T, Cisco IOS 12.4(22)T1, and Cisco IOS 12.4(20)T3 versions where the issue is fixed.
CSCsx93982	Exception when configuration rule for traffic with OGACL	**Symptom:** Configuring a Forward rule with a numbered OGACL does not work with Cisco IOS 12.4(22)T, 12.4(20)T, and 12.4(20)T1. Hence this is not supported in Cisco CP. **Conditions:** When configuring FW Rule with a numbered OGACL, Cisco CP throws exception and command delivery fails as numbered ACL are not supported in IOS versions 12.4(22)T, 12.4(20)T, 12.4(20)T1. **Workaround:** Use the Cisco IOS version 12.4(24)T or 12.4(22)T1 in which the issue has been fixed. With the Cisco IOS 12.4(22)T, 12.4(20)T, 12.4(20)T1 versions, use named OGACLs.

Table 12 Open Caveats in Cisco CP 1.3 (continued)

Bug ID	Summary	Additional Information
CSCsy74166	Wrong warning message is displayed when loading IOS image from PC in a Cisco 1861 router.	**Symptom:** When you try to load an IOS image on a Cisco 1861 router through the flash file management option, "load file from PC", wrong warning message is displayed. **Conditions:** Even though you have selected the correct image for Cisco 1861 router, this warning message is displayed "This image is unsupported for this router Platform". **Workaround:** To resolve this issue, manually configure boot system flash command through CLI.

Related Documentation

Other documents with information on Cisco CP or Cisco CP Express are listed below.

- Release Notes for Cisco Configuration Professional 1.3
- Cisco Configuration Professional Quick Start Guide

These documents are available from the following link:

http://www.cisco.com/go/ciscocp

Note For information on obtaining documentation and technical assistance, product security, and additional information, see What's New, which also lists new and revised documents each month.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.