Release Notes for Cisco Configuration Professional 2.2

May 26, 2010

These release notes support Cisco Configuration Professional (Cisco CP) version 2.2. 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**, and then find the latest release notes for your release.

Contents

This document contains the following sections:

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

Introduction

Cisco CP is a GUI-based device management tool for Cisco access routers. Cisco CP simplifies router, firewall, Intrusion Prevention System, VPN, unified communications, WAN, and basic LAN configuration through GUI-based, easy-to-use wizards. Cisco CP is installed on a PC.

Routers that are ordered with Cisco CP are shipped with Cisco CP Express installed in router flash memory. Cisco CP Express is a light weight version of Cisco CP, that you can use to configure LAN and WAN interfaces and minimal IOS security features.

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 Java Runtime Error (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 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 7 - 32 and 64 bit • 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 above
Screen Resolution	1024 X 768
Java Runtime Environment	JRE versions minimum 1.5.0_11 upto 1.6.0_17 are supported.
Adobe Flash Player	Version 10.0 or later, with Debug set to No

Router System Requirements

Router System Requirements are described in the following parts:

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

Supported Routers

Table 2 and Table 3 list the routers that Cisco CP supports.

Table 2 Supported Integrated Services Routers (ISR)

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

Table 2 Supported Integrated Services Routers (ISR)

Cisco 800 Series	Cisco 1800 Series	Cisco 2800 Series	Cisco 3800 Series	Cisco 7000 Series
CISCO871-K9 CISCO871W-G-A-K9 CISCO871W-G-E-K9 CISCO871W-G-J-K9	CISCO1805-D CISCO1805-D/K9 CISCO1805-EJ			
	CISCO1811/K9 CISCO1811W-AG-B/K9 CISCO1811W-AG-C/K9 CISCO1811W-AG-N/K9			
CISCO876-K9 CISCO876W-G-E-K9	CISCO1812/K9 CISCO1812-J/K9 CISCO1812 W-AG-C/K9 CISCO1812W-AG-P/K9			
CISCO877-K9 CISCO877-M-K9 CISCO877W-G-A-K9 CISCO877W-G-E-K9 CISCO877W-G-E-M-K9	CISCO1841			
CISCO878-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			
	C1861W-SRST-C-B/K9 C1861W-SRST-C-F/K9 CISCO1861W-SRST-B/K9 CISCO1861W-SRST-F/K9 CISCO1861W-UC-2BRI-K9 C1861W-UC-4FXO-K9			

Table 3 Supported Integrated Services Routers - G2 (ISR- G2)

Cisco 800 Series	Cisco 1900 Series	Cisco 2900 Series	Cisco 3900 Series
CISCO861-K9	CISCO1905	CISCO2901/K9	CISCO3925/K9
CISCO861W-GN-A-K9		CISCO2911/K9	CISCO3925E/K9
CISCO861W-GN-E-K9		CISCO2921/K9	CISCO3945/K9
CISCO861W-GN-P-K9		CISCO2951/K9	CISCO3945E/K9
CISCO867-K9	CISCO1921		
CISCO867W-GN-A-K9			
CISCO867W-GN-E-K9			
CISCO881-K9	CISCO1941/K9		
CISCO881W-GN-A-K9	CISCO1941W-A/K9		
CISCO881W-GN-E-K9	CISCO1941W-C/K9		
CISCO881W-GN-P-K9	CISCO1941W-E/K9		
CISCO881G-G-K9	CISCO1941W-N/K9		
CISCO881GW-GN-A-K9	CISCO1941W-P/K9		
CISCO881GW-GN-E-K9			
CISCO881G-S-K9			
CISCO881G-V-K9			
CISCO881G-A-K9			
CISCO881SRST-K9			
CISCO881SRSTW-GN-A-K9			
CISCO881SRSTW-GN-E-K9			
CISCO886-K9			
CISCO886W-GN-E-K9			
CISCO886G-K9			
CISCO886GW-GN-E-K9			
CISCO887-K9			
CISCO887W-GN-A-K9			
CISCO887W-GN-E-K9			
CISCO887M-K9			
CISCO887MW-GN-E-K9			
CISCO887G-K9			
CISCO887GW-GN-A-K9			
CISCO887GW-GN-E-K9			

Table 3 Supported Integrated Services Routers - G2 (ISR- G2)

Cisco 800 Series	Cisco 1900 Series	Cisco 2900 Series	Cisco 3900 Series
CISCO887VG-K9 CISCO887VGW-GNA-K9 CISCO887VGW-GNE-K9 CISCO887VW-GNA-K9 CISCO887VW-GNE-K9			
CISCO887VSRST-K9 CISCO887VSRSTW-GNA-K9 CISCO887VSRSTW-GNE-K9			
CISCO888-K9 CISCO888W-GN-A-K9 CISCO888W-GN-E-K9 CISCO888G-K9 CISCO888GW-G-AN-K9 CISCO888GW-G-EN-K9			
CISCO888SRST-K9 CISCO888GW-G-NA-K9 CISCO888GW-G-NE-K9			
CISCO891-K9 CISCO891W-AGN-A-K9 CISCO891W-AGN-N-K9			
CISCO892-K9 CISCO892W-AGN-E-K9			

Supported Phones

Table 4 lists the phones that Cisco CP supports:

Table 4 ***Supported Phones***

Supported Phones	Supported Expansion Modules	Supported Conference Stations
6921		
6941		
6961		
7902G	7914	7935
7905	7915-12	7936
7906G	7915-24	7937G
7910G	7916-12	
7911G	7916-24	
7912G		
7920		
7921G		
7931G		
7940G		
7941G		
7941G-GE		
7942G		
7945G		
7960G – expansion module compatible (7914)		
7961G – expansion module compatible (7914)		
7961G-GE		
7962G – expansion module compatible (7915,7916)		
7965G – expansion module compatible (7915,7916)		
7970G – expansion module compatible (7914)		
7971G – expansion module compatible (7914)		
7975G – expansion module compatible (7915,7916)		
7985G		
ATA		
CIPC – Cisco IP Communicator		

Supported Network Modules

Table 5 and Table 6 list the network modules that Cisco CP supports.

Table 5 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			AIM2-CUE-K9	EM-HDA-8FXS
NM-16ESW-1GIG				EM-HDA-4FXO
NM-16ESW-PWR				EM2-HDA-4FXO
NM-16ESW-PWR-1 GIG				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
				EM3-HDA-8FXS/DID

Table 6 Supported Cisco SRE Internal Service Modules, Cisco SRE Service Modules and EtherSwitch Modules

Cisco SRE Internal Service Modules	Cisco SRE Service Modules	EtherSwitch Modules
ISM-SRE-300-K9	SM-SRE-700-k9 SM-SRE-900-k9	SM-ES2-16-P SM-ES2-24 SM-ES2-24-P SM-D-ES2-48 SM-ES3-16-P SM-ES3G-16-P SM-ES3-24-P SM-ES3G-24-P SM-D-ES3-48-P SM-D-ES3G-48-P

Supported Interface Cards

Table 7 lists the interface cards that Cisco CP supports.

Table 7 Supported Cards

WAN Interface Cards (WICs)	High-speed WAN Interface Cards (HWICs)	Voice Interface Cards
WIC-1T	HWIC-1T	VIC2-4FXO
WIC-2T	HWIC-2T	VIC2-2FXS
WIC-2A/S (Frame Relay, PPP, HDLC, no asynchronous)	HWIC-4T	VIC2-2FXO
WIC-1ADSL	HWIC-2A/S	VIC2-2BRI-NT/TE
WIC-1DSU-T1-V2	HWIC-4A/S	VIC-2DID
WIC-1B-S/T-V3	HWIC-4ESW	VIC-4FXS/DID
WIC-1AM	HWIC-4ESW-POE	VIC3-4FXS/DID
WIC-2AM	HWIC-8A	VIC3-2FXS/DID
WIC-4ESW	HWIC-8A/S-232	VWIC2-1MFT-T1/E
WIC-1SHDSL-V2	HWIC-D-9ESW	VWIC2-2MFT-T1/E1
WIC-1SHDSL-V3	HWIC-D-9ESW-POE	
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	
	HWIC-3G-GSM	
	HWIC-3G-CDMA-S	
	HWIC-3G-CDMA-V	

Table 7 Supported Cards

WAN Interface Cards (WICs)	High-speed WAN Interface Cards (HWICs)	Voice Interface Cards
	HWIC-3G-HSPA HWIC-3G-HSPA-A HWIC-3G-HSPA-G PCEX-3G-HSPA-x	

Supported Adapters, Processing Engines, and Service Engines

Table 8 lists the adapters, processing engines, and service engines that Cisco CP supports.

Table 8 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 9.

Table 9 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 861	• 12.4(20)T
Cisco 867	• 15.0(1)M
Cisco 870 series	• 12.4(9)T
Cisco 881	• 12.4(20)T
Cisco 886	• 15.0(1)M
Cisco 887	• 15.0(1)M
Cisco 888	• 12.4(20)T
Cisco 890 series	• 15.0(1)M

Table 9 Cisco CP-Supported Routers and Cisco IOS Versions

Router Model	Earliest Cisco CP-Supported Cisco IOS Versions
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(20)T
Cisco 1941 Cisco 1941W	• 15.0(1)M
Cisco 2800 series	• 12.4(9)T
Cisco 2900 series	• 15.0(1)M
Cisco 3800 series	• 12.4(9)T
Cisco 3900 series	• 15.0(1)M
Cisco 7000	• 12.4(9)T

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 10 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 10 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 89x, Cisco 180x, Cisco 1805, Cisco 1811 and 1812	Yes	Obtain an IP address automatically.
Cisco 1841, Cisco 1861, Cisco 28xx, Cisco 38xx, Cisco 29xx, Cisco 39xx	No	Static IP address from 10.10.10.2 to 10.10.10.6 Subnet Mask: 255.255.255.248

Router Configuration Requirements

To run Cisco CP, a router configuration must meet the requirements shown in Table 11.

Table 11 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 12 describes the ordering options under which Cisco CP can be ordered. Cisco CP Express is a product that is shipped in router flash memory when the router is ordered with Cisco CP.

Table 12 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

Table 12 Cisco CP Ordering Options

Ordering Options	Description
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.
ISR-CCP-CD=	Cisco CP: Shipped on CD Spare SKU: Mapped to ISR-CCP-CD
ISR-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
ISR-CCP-CD-NOCONF	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
ISR-CCP-EXP	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
ISR-CCP-EXP-NOCONF	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

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 and Changed Features
- New Hardware Support

New and Changed Features

Cisco CP 2.2 supports the following new features:

- 3G Feature Enhancements - In addition to supporting HWIC—3G—HSPA, HWIC—3G—HSPA—A, HWIC—3G—HSPA—G, and PCEX—3G—HSPA—x for 88xG series ISRs, Activation command change without SID and NID, ESN format, and PPP PDP are supported in Cisco CP 2.2
- Cisco Unity Express configuration - Cisco CP has disabled automatic initialization of Cisco Unity Express 8.x. Instead, you can use the Cisco Unity Express Configuration screen to configure Call Agent, hostname, domain name, DNS IP address, time zone, and NTP.
- Conferencing Enhancements - Earlier, Cisco CP supported configuring ad-hoc conferencing. In Cisco CP 2.2 MeetMe conferencing is also supported.
- Content Filtering Enhancements - The status of content filtering license activation and digital certificate is displayed before you launch the wizard. The two types of content filtering are category based filtering and web sense or secure computing.
- Demo Mode - Click the **Cisco Configuration Professional (Demo)** option in the Start menu to launch demo mode. The dashboard is populated with three devices. The devices supported are 800 series, ISR-G2 with licensing, and 1861 wireless. You can discover any or all of the three devices. You cannot create, edit, or delete community or add a new device to a community in demo mode.
- Dial Plan Enhancements - Earlier Cisco CP could only read dial peers created through Cisco CP. In Cisco CP 2.2, the dial plan feature can handle all types and combinations of dial plans configured by you.
- EnergyWise - The EnergyWise feature allows you to:
  - Modify power levels on specific hardware modules or components.
  - Schedule capabilities where the user can change the power level on a one-time basis or maintain a recurrent schedule.
  - Assign a device to a domain specifying EnergyWise attributes.
  - Perform interface-level power configuration.
- Firewall Enhancements
  - Support SIP/H323 Pass through

  The following enhancements are supported in Cisco CP 2.2:

  - Configuring firewall for SIP Application Inspection and configuring rate-limit feature for SIP messages. Configuring firewall for inspection of H.323v4 Annex E and Annex G packets and configuring rate-limit feature for H.323 messages. Even if firewall is configured in the device, we can delete the policies associated with the firewall and switch to the other type firewall.
  - Configuring firewall to support inspection of locally generated or locally terminated SCCP traffic.

- GUI Enhancements - Earlier, only Zone Firewall user interface was displayed if the IOS image supported Zone Firewall. In Cisco CP 2.2, it is possible to switch from Zone Firewall to Classic Firewall and vice versa. If a firewall is configured on the router, you can delete the policies associated with that firewall and switch to the other firewall. In Cisco CP 2.2 it is also possible to list the protocols in the Firewall Rule user interface by alphabet or by category.

- IOS IPS Enhancements - Cisco CP detects the status of IPS license activation and allows you to load the signature packages on the router. Cisco CP provides the URL from which to download the license and the path for the license feature.

Note Only licensed signature packages require the license to load the signature.

- Module Management Enhancements - SRE/SM support for WAN Optimization and Service Module support for Video Surveillance are provided in Cisco CP 2.2.
- Rollback Feature - Rollback feature is used to revert the entire set of CLIs executed as part of one configuration and restore the router to the state seen before executing the set of CLIs. The restore happens irrespective of whether the commands were successfully pushed to the device or not. Rollback is available for offline-online transition, template, and bulk import features. Rollback is not available for Cisco Unity Express.
- WAN Optimization Enhancements - Earlier basic discovery and configuration support was provided for WAAS modules. In Cisco CP 2.2, initial setup and application management for WAAS modules are also supported.

New Hardware Support

The new devices supported are:

- CISCO1905
- CISCO1921
- CISCO1941W-C/K9
- CISCO1941W-N/K9
- CISCO1941W-P/K9

The new interface cards supported are:

- HWIC-3G-HSPA
- HWIC-3G-HSPA-A
- HWIC-3G-HSPA-G
- PCEX-3G-HSPA-x

Limitations and Restrictions

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

- Cisco CP Minimum Screen Resolution
- Restrictions for Cisco 7204VXR, Cisco 7206VXR, and Cisco 7301 Routers
- Cisco CP and Internet Explorer 8
- JRE Settings for 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.

Cisco CP and Internet Explorer 8

In some systems (Windows XP and Windows Vista), with IE8 installed, Cisco CP may not work as expected. This is due to a reported IE 8 caching issue.

IE8 reinstall or clearing the cache does not help. Any Flash based application like Cisco CP will see this issue.

A workaround today is to create another user account with appropriate privileges and run Cisco CP in that user account.

JRE Settings for Cisco CP

The following JRE settings are needed for CCP to function properly:

Step 1 Go to **Start > Control Panel > Java**.

Step 2 Click **View** under **Java Applet Runtime Settings**.

Step 3 Select your JRE in use.

Step 4 Set the "Java runtime parameters" with the value "-Xmx256m -Dsun.java2d.d3d=false".

In addition, if JRE is upgraded to versions 1.6.0_11 or above, following settings are needed after Cisco CP installation.

Step 1 Go to **Start > Control Panel > Java > Advance**.

Step 2 Select "Java Plug-in" tree.

Step 3 Uncheck the check box for Enable next-generation Java Plug-in.

Step 4 Restart 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
- Cisco CP Merge and Replace Configuration Functions Fail Under Some Conditions
- Cisco CP Security Dashboard May Display Threats Unrelated to Your Cisco IOS IPS Installation
- Cisco CP May Lose Connection to Network Access Device
- Popup Blockers Disable Cisco CP Online Help
- Disable Proxy Settings
- Security Alert Dialog May Remain After Cisco CP Launches
- Screencasts for Cisco CP Features

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 Cisco CP 2.2 features:

- EnergyWise
- CUE settings
- Adhoc and MeetMe Conferencing
- Dial Plan

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 processes **CiscoCP.exe, CiscoCPEngine.exe, IEC2.exe**, and **SplashScreen.exe**.

Step 4 Click **End Process**.

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

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 Close all existing IE windows.

Step 3 Go to **Start** > **Control Panel** > **Java**. The General tab is displayed.

Step 4 In the Temporary Internet Files box, click **Delete Files**.

Step 5 In the displayed dialog, leave all file types checked, and click **OK**.

Step 6 Click **OK** in the Java control panel to close it.

Step 7 Restart Cisco CP.

Caveats

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

- Open Caveats, page 26
- Resolved Caveats, page 30

Open Caveats

Table 13 lists caveats that are open in Cisco CP 2.2

Table 13 Open Caveats in Cisco CP 2.2

Bug ID	Summary	Additional Information
CSCtg84311	Inconsistent Module status shown on repeated refresh.	**Symptom** Inconsistent module status shown for a module in doing repeated refresh in **Module Configuration** screen. **Conditions** It's an intermittent issue seen on refreshing the module from the **Module Configuration** screen. **Workaround** Rediscover the device using **Community Member** screen.

Table 13 Open Caveats in Cisco CP 2.2

Bug ID	Summary	Additional Information
CSCtg57954	Intermittent internal error while launching the CCP in win7 32 bit.	**Symptom** While launching CCP in win7 32 bit machine, an error message will appear: `An internal error has occurred. Cisco CP will shut down. Restart Cisco CP and discover the device again.` **Conditions** • Double click **installer.exe**. • Click on check box at the end of the installation to launch CCP. • Right click on the short cut icon and run as Administrator. **Workaround** • When you double click the **installer.exe** file, don't use checkbox at the end of the installation to launch CCP. Instead right click on the short cut icon and run as Administrator, then the CCP launch will be successful. • Right click on the **installer.exe** file and run as Administrator. Click on check box at the end of the installation to launch CCP successfully.
CSCtg55407	Refresh button is missing in some instances of module configuration.	**Symptom** Refresh button is missing in **Interface Management-> Module configuration** page. **Conditions** Refresh button is missing in **Interface Management-> Module configuration** page. **Workaround** Clear the IE cache. • Go to **Control Panel-> Java**. • In **General** tab, under temporary settings, click on **Settings** and delete temporary files present on your PC.

Table 13 Open Caveats in Cisco CP 2.2

Bug ID	Summary	Additional Information
CSCtg19665	With Log as option, CCP reads Action as drop instead of Pass.	**Symptom** If the log option is configured along with the Pass action under a policy-map, the Cisco CP reads it as Drop action. **Conditions** The problem occurs only when the log option is configured along with the Pass action under a policy-map and the device is discovered in Cisco CP. The problem does not occur when the log option is not configured with Pass Action. **Workaround** There is no workaround.
CSCtf48106	In the multi-party selection changing tab is not refreshing data.	**Symptom** On selecting multi-party conference and switching between tabs, the tab data is not getting refreshed. **Conditions** On selecting multi-party conference and switching between tabs, the tab data is not getting refreshed. **Workaround** Select **Three party Ad hoc radio** button and reselect **Multi-party ad hoc** and **meet-me** radio button.
CSCtg10629	CCP closes if OK button is clicked on SDEE subscription warning message.	**Symptom** **SDEE Subscription Warning** messages are shown while loading the IPS Signature Packages if the subscription messages have reached the limit. Upon clicking **OK** on the warning message, the Cisco CP application will either close or restart. **Conditions** This problem occurs when the **SDEE Subscription Warning** messages have reached their limit. **Workaround** The SDEE Subscription session should be cleared manually using the router CLI and rediscover the device on Cisco CP. CLI Command - clear IP SDEE subscriptions

Table 13 Open Caveats in Cisco CP 2.2

Bug ID	Summary	Additional Information
CSCtg11258	Firewall: Multiple entries created for SIP and H323 AI in the same row.	**Symptom** Adding H323 and SIP Application Inspection for self to other zone pairs using edit a rule on **edit firewall** tab leads to multiple entries(2) of the SIP and H323 Application Inspection. **Conditions** In adding SIP and H323 Application Inspection where a firewall rule exists with some other protocols selected, CCP creates double entries of the Application Inspection while on the router. The configuration is as per steps taken by the user. That is one Class map with the Application Inspection rules is added per protocol. **Workaround** There is no workaround. This is a GUI error only with no error in the configuration of the Application Inspection of any of the protocols.

CSCtf87466	SIP on in to self and vice versa leads to unreachable router.	**Symptom** Attaching/removing the management interface (in which CCP is invoked) from the zone-member security of firewall leads to unreachable router.
		Conditions Firewall configurations delivered has the configuration that tries to attach/remove the management interface (example: Gi0/0, the interface from which CCP is invoked) from the zone-security. IOS tries to reset the communication session which in return makes router unreachable and communication is lost.
		`interface GigabitEthernet0/0`
		` zone-member security in`
		` exit`
		or
		`interface GigabitEthernet0/0`
		` no zone-member security in`
		` exit`
		Workaround Rediscovering the router from CCP might work if the device is reachable. If the device is not reachable after the discovery, router is blocked by firewall through that interface IP address.

Table 13 Open Caveats in Cisco CP 2.2

Bug ID	Summary	Additional Information
CSCte49659	Replace Running Configuration does not work for devices with access point.	**Symptom**: Replace Running Configuration does not work in a router with access point module, using Cisco CP. **Conditions**: Router with access point module. In Config Editor, Replace Running Configuration does not work when the modified running configuration file is imported from the PC. **Workaround**: There is no workaround.
CSCtb33162	Only the last chat script is removed when multiple chat is configured.	**Symptom**: Only the last chat script gets removed upon clicking the delete button for the specified interface. **Conditions**: Configure multiple chat script under Dialer tab in edit mode. **Workaround**: There is no workaround.

Resolved Caveats

Table 14 lists caveats that are resolved in Cisco CP 2.2.

Table 14 Resolved Caveats in Cisco CP 2.2

Bug ID	Summary
CSCtb81205	Location to download SDM IPS packages needs to be changed.
CSCtd99143	**match-all** command not supported in IOS version 15.0.

Related Documentation

Table 15 describes the related documentation available for Cisco CP.

Table 15 Cisco Configuration Professional Documentation

Document Title	Available Formats
Readme First for Cisco Configuration Professional	This document is available in the following locations: • On Cisco.com. • On the product CD-ROM in the Documentation folder.
Cisco Configuration Professional Quick Start Guide	This guide is available in the following locations: • On Cisco.com. • On the product CD-ROM in the Documentation folder.
Cisco Configuration Professional Getting Started Guide	This guide is available in the following locations: • On Cisco.com. • On the product CD-ROM in the Documentation folder. • During the installation process, just before you have finished installing the product, you are provided the option to read the Getting Started guide.
Cisco Configuration Professional User Guide	This guide is available in the following locations: • On Cisco.com. • Accessible from Online help.
Cisco Configuration Professional Express User Guide	This guide is available in the following locations: • On Cisco. com. • Accessible from Online help.
Release Notes for Cisco Configuration Professional	This document is available in the following location: • On Cisco.com.
Release Notes for Cisco Configuration Professional Express	This document is available in the following location: • On Cisco.com.

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.

Glossary

HWIC—High-Speed WAN Interface Card

HSPA—High-Speed Packet Access

HSPA—A—High-Speed Packet Access for Americas

HSPA—G—High-Speed Packet Access for Global

PCEX—PC Express

SID—System Identification Number

NID—Network Identification Number

ESN—Electronic Serial Numbers

PDP—Packet Data Protocol (PDP)

PPP—Point-to-Point Protocol (PPP) PDP type

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