



Release Notes for Cisco Configuration Professional 1.4

August 10, 2009

These release notes support Cisco Configuration Professional (Cisco CP) version 1.4. 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:

- [Introduction](#)
- [System Requirements](#)
- [New and Changed Information](#)
- [Limitations and Restrictions](#)
- [Important Notes](#)
- [Caveats](#)
- [Related Documentation](#)



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.

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: <ul style="list-style-type: none"> • 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 up to 1.99 are supported.

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](#)
- [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	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-E/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 Routers (continued)**

Cisco 800 Series	Cisco 1800 Series	Cisco 2800 Series	Cisco 3800 Series	Cisco 7000 Series
CISCO861-K9	CISCO1805-D			
CISCO861W-GN-A-K9	CISCO 1805-D/K9			
CISCO861W-GN-E-K9				
CISCO861W-GN-P-K9				
CISCO867-W-GN-A-K9				
CISCO867-W-GN-E-K9				
CISCO871-K9	CISCO1811/K9			
CISCO871-SEC-K9	CISCO1811W-AG-B/K9			
CISCO871W-G-A-K9	CISCO1811W-AG-C/K9			
CISCO871W-G-E-K9	CISCO1811W-AG-N/K9			
CISCO871W-G-J-K9				
CISCO876-K9	CISCO1812/K9			
CISCO876-SEC-K9	CISCO1812 W-AG-E/K9			
CISCO876-SEC-I-K9	CISCO1812 W-AG-C/K9			
CISCO876W-G-E-K9				
CISCO877-K9	CISCO1841			
CISCO877-M-K9				
CISCO877-SEC-K9				
CISCO877W-G-A-K9				
CISCO877W-G-E-K9				
CISCO877W-G-E-M-K9				
CISCO878-K9	C1861-UC-4FXO-K9			
CISCO878-SEC-K9	C1861-UC-2BRI-K9			
CISCO878W-G-A-K9	C1861-SRST-B/K9			
CISCO878W-G-E-K9	C1861-SRST-C-B/K9			
	C1861-SRST-C-F/K9			
	C1861-SRST-F/K9			

Table 2 **Supported Routers (continued)**

Cisco 800 Series	Cisco 1800 Series	Cisco 2800 Series	Cisco 3800 Series	Cisco 7000 Series
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				
CISCO881SRST-K9				
CISCO881SRSTW-GN-A-K9				
CISCO881SRSTW-GN-E-K9				
CISCO886-K9				
CISCO886W-GN-E-K9				
CISCO886G-K9				
CISCO886GW-GN-E-K9				
CISCO886SRST-K9				
CISCO886SRSTW-GN-K9				
CISCO887V-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				
CISCO887-SRST-K9				
CISCO887SRSTW-GN-E-K9				

Table 2 ***Supported Routers (continued)***

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				
CISCO888SRST-K9				
CISCO888SRSTW-GN-A-K9				
CISCO888SRSTW-GN-E-K9				
CISCO891-K9				
CISCO891W-AGN-A-K9				
CISCO891W-AGN-N-K9				
CISCO892-K9				
CISCO892W-AGN-E-K9				

Supported Phones

[Table 3](#) lists the phones that Cisco CP supports:

Table 3 **Supported Phones**

Supported Phones
7906G
7911G
Expansion module (7915, 7916)
IP Conferencing station (7937)
7940G
7941G
7941G-GE
7942G
7945G
7960G
7961G
7961G-GE
7962G
7965G
7970G
7971G-GE
7975G
7985G

Supported Network Modules

[Table 4](#) lists the network modules that Cisco CP supports.

Table 4 **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				EM-HDA-8FXS
NM-16ESW-1GIG				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 5](#), lists the interface cards that Cisco CP supports.

Table 5 **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	VIC3-2FXS-EDID
WIC-1SHDSL-V2	HWIC-D-9ESW	VWIC2-1MFT-T1/E
WIC-1SHDSL-V3	HWIC-D-9ESW-POE	VWIC2-2MFT-T1/E1
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	

Supported Adapters, Processing Engines, and Service Engines

Table 6 lists the adapters, processing engines and service engines that Cisco CP supports.

Table 6 *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 7.

Table 7 *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 8 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 8 *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 9 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 9 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 10.

Table 10 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 11 on page 13 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 11 **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 1.4 supports the following new features:

- **Community GUI Enhancements** —When you start Cisco CP for the first time, Cisco CP automatically creates a community for you, to which you can add devices.
- **User Preferences** —The User Preferences feature allows you to set user preferences such as log level, show community at startup, and show CLI preview parameters at run time.
- **Voice Features**
 - **Parallel Hunt Group** — When you choose the Parallel hunt group option, the incoming call rings all numbers in the hunt group simultaneously. The Parallel hunt group type is available on Cisco Unified CME 4.3 or higher versions.
 - **Shared, Monitor, Overlay, Call Waiting on Overlay:**

Shared Extension — An extension that is shared by more than one user with the line type as Regular is called a shared extension.

Overlay—Overlaid ephone-dns are directory numbers that share the same button on a phone. Overlaid ephone-dns can be used to receive incoming calls and place outgoing calls.

Monitor—A monitor line is a line that is shared by two people. Only one person can make and receive calls on the shared line at a time, while the other person, whose line is in monitor mode, is able to see that the line is in use.

Call Waiting on Overlay—Call waiting allows phone users to know that another person is calling them while they are talking on the phone.
 - **Whisper Intercom** — When a phone user dials a whisper intercom line, the called phone automatically answers using speakerphone mode, providing a one-way voice path from the caller to the called party, regardless of whether the called party is busy or idle. The Whisper Intercom feature is supported in Cisco Unified CME 7.1 and later versions.
 - **Single Number Reach (SNR)** — The SNR feature allows users to answer incoming calls on their desktop IP phone or at a remote destination, such as a mobile phone, and to pick up in-progress calls on the desktop phone or the remote phone without losing the connection. The SNR feature is supported on routers running Cisco Unified CME 7.1 and later versions.
- **Offline or Demo Mode** — You can use Cisco CP in offline mode to demo supported features without having access to a live device. The generated CLI is not applied to the device immediately but you can view and download the configuration on the device later, after the demo operation is complete.
- **GetVPN** — GetVPN does not use traditional point-to-point tunnels. It uses "trusted" group member routers that use a common security methodology, which is independent of any point-to-point relationship.
- **Voice Security Audit** — Voice Security Audit feature adds voice audit to the existing security audit feature. This includes preventing unauthorized access of trunks and some of the other facilities which leads to toll fraud. The audit functionality is available as a wizard under "Voice Configuration". You can use this wizard to find potential issues and choose to fix them.

New Hardware Support

The new devices supported are:

- CISCO867-W-GN-A-K9

- CISCO867-W-GN-E-K9
- CISCO886-K9
- CISCO886W-GN-E-K9
- CISCO886G-K9
- CISCO886GW-GN-E-K9
- CISCO886SRST-K9
- CISCO886SRSTW-GN-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
- CISCO887-SRST-K9
- CISCO887SRSTW-GN-E-K9

The new interface cards supported are:

- HWIC-3G-GSM
- HWIC-3G-CDMA-S
- HWIC-3G-CDMA-V

The new phones supported are:

- 7975G
- 7971G-GE
- 7970G
- 7965G
- 7962G
- 7961G-GE
- 7961G
- 7960G
- 7945G
- 7942G
- 7941G-GE
- 7941G
- 7940G
- 7911G
- 7906G
- Expansion module (7915, 7916)

- IP Conferencing station (7937)
- 7985G

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](#)
- [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
```

Screenscasts for Cisco CP Features

Instead of online help, we have provided screenscasts for the following Cisco CP 1.4 features:

- Offline or Demo Mode
- GetVPN
- Voice Security Audit

These screenscasts are located at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/scrst/ccpsc.html. You must have internet access to view the screenscasts.

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 30 seconds, and then restart Cisco CP. |
-

Technical Support Logs Do Not Appear on Desktop

If the technical support logs 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 1.3](#)
- [Open Caveats—Cisco CP 1.4](#)

Resolved Caveats from Cisco CP 1.3

[Table 12](#) lists caveats that are resolved in Cisco CP 1.4.

Table 12 *Resolved Caveats in Cisco CP 1.4*

Bug ID	Summary
CSCsv96570	Cannot change the sequence number with 12.4(22)T.
CSCsx59378	Splash screen stays on when Flash Player is unavailable in Windows Vista.
CSCsx80772	ACL Object Groups: Cisco CP should not support associating OGACL for IPSec VPN.
CSCsx93982	Exception when configuring rule for traffic with OGACL.
CSCsy39505	Pushing of signature package fails.
CSCsy61239	Config enabled although telephony-service is not configured.
CSCsy74166	Wrong warning message is displayed when loading IOS image from PC in a Cisco 1861 router.
CSCsy82573	Digital signature java applet hidden behind Cisco CP application windows.
CSCsy84069	CLI commands are not removed on the router when changing from FXS to DID Cisco CP.
CSCsy91343	Cisco CP unable to discover device when using the IP Address of SSL VPN Gateway.

Open Caveats—Cisco CP 1.4

Table 13 lists caveats that are open in Cisco CP 1.4.

Table 13 *Open Caveats in Cisco CP 1.4*

Bug ID	Summary	Additional Information
CSCsl65044	Array values displayed when the mouse is placed over list in the user screen.	<p>Symptom: When the mouse is placed over a transfer box, a tool tip is given with object instances.</p> <p>Workaround: There is no workaround.</p> <p>Further Problem Description: Since this is a minor UI glitch, the tool tip information can be ignored.</p>
CSCsm91019	Security screens overlap over menu bar options and tool bar information.	<p>Symptom: Some of the menu bar options, either Tools or Help, are hidden under security screens.</p> <p>Conditions: You are in Routing or Security features screen while selecting the menu options.</p> <p>Workaround: Move to any other feature other than Routing or Security, the issue will not be seen.</p>
CSCsm95507	Cisco CP icon is changed to Internet Explorer icon after a while in the titlebar.	<p>Symptom: The icon of Cisco CP application window changes to Internet Explorer icon.</p> <p>Conditions: After the successful launch of Cisco CP, minimize the Cisco CP screen and keep it minimized for a while.</p> <p>Workaround: There is no workaround.</p>
CSCsq52996	Need to support SIP for self zone in Cisco CP.	<p>Symptom: Error message informing that any other protocols other than TCP, UDP, h323, and ICMP are not supported for inspection.</p> <p>Conditions: Only for self zone pairs.</p> <p>Workaround: There is no workaround.</p>
CSCsr65297	QoS configured in Edit QoS for DMVPN tunnel interface.	<p>Symptom: The details of QoS configured on tunnel interface is not displayed on Edit QoS policy screen when tunnel interface is selected.</p> <p>Conditions: After you have configured QoS for the tunnel interfaces, such as, Site-to-Site VPN, DMVPN, or GREoIPSec VPN, the details regarding the policy-maps and class-maps are not displayed for the tunnel interface on the Edit Qos Policy screen.</p> <p>Workaround: Identify the tunnel source interface and select that WAN interface to view the details of the QoS configured for the tunnel interface on the Edit QoS policy screen.</p>

Table 13 **Open Caveats in Cisco CP 1.4 (continued)**

Bug ID	Summary	Additional Information
CSCsw23556	Security Applet is not responding error during discovery.	<p>Symptom: Discovery of a device failed with the error Security Applet not responding.</p> <p>Conditions: This issue happens intermittently.</p> <p>Workaround: Re-launch the application.</p>
CSCsw31280	CLI Preview dialog box moves to the background.	<p>Symptom: When configuring security features, you click the Add, Edit, or other command buttons in the user interface, the dialog boxes do not open.</p> <p>Conditions: CLI Preview dialog box is not closed and is present in the background.</p> <p>Workaround: Resize or move the main Cisco CP window and complete the CLI preview dialog options that are hidden in the background to continue.</p>
CSCsw39659	Enhancement in Cisco CP for CUE post initialization.	<p>Symptom: The data fields for CUE post initialization wizard are not retained on Cisco CP if you use the back button. It is time consuming to enter all the values again.</p> <p>Conditions: This issue occurs only when any field value is invalid in the CUE post initialization wizard.</p> <p>Workaround: To avoid this situation, make sure that you enter the correct values so that you do not have to use the back button.</p>
CSCsx05868	Unable to upload CME phone load tar file.	<p>Symptom: In Cisco Configuration Professional, while trying to upload phone load tar file from the Voice > Phone Firmware feature, phone load upload might fail after some upload progress.</p> <p>Conditions: On device if exec-timeout is not set under line vty configurations or if exec-timeout is set with a smaller timeout value, then phone load upload might fail.</p> <p>Workaround: On device, under all line vty configs, set exec-timeout config with proper timeout value. Example: vty line 0 4 exec-timeout 25 0 exit</p> <p>Further Problem Description: exec-timeout is used to set the interval that the EXEC command interpreter waits until user input is detected. If no input is detected during this interval, the EXEC facility returns the terminal to the idle state and disconnects the incoming session. A big size phone load tar file might take some time to get uploaded on the device's flash. So to avoid any error during upload, exec-timeout should be set with a value greater than the time taken by upload of big tar file. If exec-timeout is set as 0 0, then vty lines may get blocked if session is not exited/closed properly.</p>

Table 13 **Open Caveats in Cisco CP 1.4 (continued)**

Bug ID	Summary	Additional Information
CSCsx57080	Cisco CP launching issue with Internet Explorer 8.	<p>Symptom: Unable to launch Cisco CP.</p> <p>Conditions: Using Internet Explorer 8 release candidate 1.</p> <p>Workaround: Downgrade to Internet Explorer 7.</p>
CSCsx72139	Cisco CP discover details should give warning in case of insufficient memory.	<p>Symptom: Voice menu folder is disabled in the Cisco CP GUI.</p> <p>Conditions: The router running IOS version 12.4(24)T or later has insufficient memory to enable telephony-service.</p> <p>Workaround: Upgrade the DRAM in the router.</p>
CSCsx75097	Unity express module discovery fails with SSH version >=2.0.	<p>Symptom: Cisco Unity Express module discovery fails with an error message stating that the device is configured with unsupported SSH version. The error messages are shown in the discovery details user interface. Due to this error message, none of the CUE features are available.</p> <p>Conditions: The device is configured with SSH version higher than or equal to 2.0.</p> <p>Workaround: Reconfigure the SSH version to lesser than 2.0, or use Telnet to communicate with the device.</p>
CSCsy06399	Error #2032 is seen on the Router Status dialog box.	<p>Symptom: This error is seen in the Router Status dialog box, when the Cisco CP application network connectivity to the router fails, or the Java applet has not started or has crashed.</p> <p>Conditions: You can verify the Java applet failure by looking at the Security and Router features in the left navigation pane. If the Security or Router features are not loaded, it indicates that the Java applet has failed or crashed. In this occurs, the Router Status dialog box displays this error message. This problem could also occur if the network connectivity to the router is lost.</p> <p>Workaround: To resolve this issue, restart Cisco CP.</p>
CSCsy49785	Service group not working for QoS, SSLVPN, NAC, and access-class.	<p>Symptom: OGACL with service group not working for QoS, SSLVPN, NAC, and access-class.</p> <p>Conditions: When associating an OGACL with service object group to QoS, SSL VPN, NAC, and access-class, the traffic does not match. This is due to an IOS issue.</p> <p>Workaround: There is no specific workaround. Use normal ACLs with these features. Once the IOS bug is fixed, this will be fixed in Cisco CP.</p>

Table 13 **Open Caveats in Cisco CP 1.4 (continued)**

Bug ID	Summary	Additional Information
CSCsy50471	Enable option should not be shown when the VDSL interface is up.	<p>Symptom: Enable option should not be shown when the VDSL interface is administratively up.</p> <p>Conditions: When the user has discovered the VDSL Controller device and navigates through Configure > Router > Interfaces and Connections > Edit Controllers/Connections, choosing the VDSL Controller, the status of the interfaces is shown as administratively up. There is no option to disable the interface. Only the Enable option is shown.</p> <p>Workaround: There is no workaround.</p>
CSCsy87964	CPU utilization at 100% when discovering devices.	<p>Symptom: After discovery of 5 devices in a community, some with secure mode, CPU shoots to 100% utilization and does not drop. CiscoCPEngine.exe CPU usage is in the range 83%-95%.</p> <p>Conditions: This problem occurs if one of the devices in the community, has high security configuration and bandwidth filters for the WAN interface. This problem does not occur in other PC environments.</p> <p>Workaround: There is no workaround.</p>
CSCsz13428	Configuration error on creating outgoing dial-plan.	<p>Symptom: Dial-plan related configuration fails saying dial-peer tag is already in use. This issue occurs occasionally when voice hunt-group is configured on the router.</p> <p>Conditions: When hunt-group is configured with pilot CLI, and the pilot number is too huge to be the dial-peer tag.</p> <p>Further Problem Description: When hunt-group is configured with pilot CLI, the router creates a dial-peer with the pilot number as the dial-peer tag. This dial-peer is not displayed in show run, and Cisco CP does not read these dial-peers (only show run is used to read in dial-peer configurations). However, these dial-peers can be seen in show dial-peer voice summary.</p> <p>In normal circumstances, the pilot number and the dial-peer tag are large numbers. This is not an issue for Cisco CP as Cisco CP always chooses the smallest tag number available to configure dial-peers and there is never any overlap of tags. However, if the pilot number is too large to be a tag for dial-peer, the router chooses the next available smallest tag number to configure the dial-peer for that hunt group. In such a situation, Cisco CP configuration for dial-plan might cause a problem because the tag that Cisco CP chooses, can overlap with the already configured hunt group related dial-peer, which results in configuration failure.</p>

Table 13 **Open Caveats in Cisco CP 1.4 (continued)**

Bug ID	Summary	Additional Information
CSCsz13759	Deleting of extensions fails if configured as Monitor/Shared.	<p>Symptom: Error while deleting multiple extensions together.</p> <p>Conditions: Create 6 extensions. For example, 1000, 2000, 3000, 4000, 5000, 6000.</p> <p>Assign extensions 1000, 2000, 3000 on button 1 of user1; and extensions 4000, 5000, 6000 on button 2 of user1. Assign extension 1000, 2000, 3000, 4000, 5000, 6000 on button1 of user2. Assign extension 1000 on button1 of user3.</p> <p>Try to delete all the extensions together.</p> <p>Workaround: Delete the extensions one by one.</p>
CSCta12755	Configuration failed when trying to deliver CLIs to the router.	<p>Symptom: Configuration failed error seen when moving from offline to online mode.</p> <p>Conditions: Configured dialplan (Dialing Restriction, Outgoing, Incoming) in offline mode on devices that are reachable while in online mode</p> <p>Workaround: Do not configure dialplan (Dialing Restriction, Outgoing, Incoming) in offline mode on devices that are reachable while in online mode</p>
CSCta31020	Whisper intercom does not throw error while editing an invalid entry.	<p>Symptom: No error message while editing invalid Whisper Intercom entry.</p> <p>Conditions: Whisper intercom dashboard should have invalid entry. Invalid entry should be created via the CLI.</p> <p>Workaround: There is no workaround.</p>
CSCta60741	Inspect rule for SSL VPN passthrough is not being configured.	<p>Symptom: Inspect rule does not get configured correctly for the SSL VPN Passthrough.</p> <p>Conditions: Configure ZBF and then configure SSL VPN. The inspect rule does not get configured correctly. This is due to an IOS bug.</p> <p>Workaround: There is no workaround.</p>
CSCta65551	DID trunk configuration is failing in Online mode.	<p>Symptom: Configuration of VIC2-DID trunk fails.</p> <p>Conditions: Edit one of the VIC2-DID, change only the description, and click OK. The configuration fails.</p> <p>Workaround: There is no workaround.</p>
CSCta77317	Analog Trunk window not closing on clicking the OK button.	<p>Symptom: Go to Configure > Voice > PSTN Trunks > Analog Trunks. The Edit screen does not close when the OK button is clicked without making any changes.</p> <p>Conditions: Go to Configure > Voice > PSTN Trunks > Analog Trunks screen. Select an entry, and then click Edit. Without making any changes, click OK. The dialog box does not close.</p> <p>Workaround: Click Cancel button.</p>

Table 13 **Open Caveats in Cisco CP 1.4 (continued)**

Bug ID	Summary	Additional Information
CSCta77454	Adhoc Conference update with SSH port blocked throws unwarranted error.	<p>Symptom: Although Discovery is successful with SSH port blocked, updates on Adhoc Conference fail as interactive commands use SSH protocol. The error message does not indicate that the SSH port is blocked.</p> <p>Conditions: Modification of Adhoc Conference parameters fail with SSH port blocked and the error message does not indicate the cause.</p> <p>Workaround: Unblock the SSH port for any transport/communication errors on Adhoc Conference.</p> <p>Further Problem Description: The Discovery process on Cisco CP is successful with SSH port blocked but features like Adhoc Conference use DSPs which interact using SSH ports. When the SSH port is blocked, all such interactions fail and hence updates on Adhoc Conference profile are not successful. The error message generated does not communicate the cause.</p>
CSCta93218	Disabling CLI view in online mode causes CLIs to be sent directly.	<p>Symptom: While moving from offline mode to online mode, clicking the View CLI button delivers the CLI to the device without a CLI preview.</p> <p>Conditions: Disable the cli preview option in the User preferences and move from offline mode to online mode. Click the View CLI button.</p> <p>Workaround: Ensure CLI preview is enabled before moving to offline mode from online mode.</p>
CSCta95721	EM-4BRI-NT/TE ports under EVM-HD-8FXS/DID not getting discovered.	<p>Symptom: When an EM-4BRI NT/TE card is installed under EVM-HDA3-8FXS/DID card, BRI ports are not seen on the GUI.</p> <p>Conditions: Install EM-4BRI NT/TE card under EVM-HDA3-8FXS/DID card.</p> <p>Workaround: There is no workaround.</p>

Table 13 **Open Caveats in Cisco CP 1.4 (continued)**

Bug ID	Summary	Additional Information
CSCta95900	Outgoing dial plan configures invalid destination pattern.	<p>Symptom: In Outgoing Dial Plan feature, during create or edit of dial plan, if the number prefix field is left blank and if variable length option is selected, Cisco CP sends the following invalid CLI: destination-pattern T</p> <p>The router displays a warning for the above command, and Cisco CP fails with an exception.</p> <p>Workaround: If variable length option is selected, make sure that the number prefix field in the Outgoing Dial Plan create or edit dialog boxes is not left blank. To configure dial plan that matches any one digit or more numbers, specify "." in the number prefix, and then select the variable length to configure the "T" destination pattern.</p> <p>Further Problem Description: Destination pattern "T" defines a match with zero or more digits and could match with an empty number also. Therefore, do not configure a dial plan with this pattern.</p>
CSCtb03710	PRI Settings voice port values are not displayed correctly.	<p>Symptom: Cisco CP does not display the ISDN Overlap Receiving and T302 timeout fields correctly while editing the T1/E1 port.</p> <p>Conditions: ISDN Overlap Receiving and T302 timeout fields under PRI settings tab should be enabled only if ISDN Switch type selected is "primary-net5" or "primary-qsig"</p> <p>Workaround: There is no workaround.</p>
CSCtb05983	Multiple delete fails in offline mode community dashboard.	<p>Symptom: Devices do not disappear from the community table immediately after deleting them.</p> <p>Conditions: Select multiple devices in the offline mode and press Delete.</p> <p>Workaround: Delete the devices one by one.</p> <p>Or</p> <p>Refresh the community table after all the devices are deleted.</p>
CSCtb07893	Acknowledge error on importing Outgoing dial plan in the offline mode.	<p>Symptom: Dial plan import fails with a Did not receive an acknowledge message error message.</p> <p>Conditions: Try to import a dial plan profile with the PSTN access digit same as the starting digit of any extension.</p> <p>Workaround: Do not import dial plan profiles with PSTN access digit same as the starting digit of any extension.</p>

Table 13 **Open Caveats in Cisco CP 1.4 (continued)**

Bug ID	Summary	Additional Information
CSCtb10599	Switching between devices in the offline mode shows incorrect data.	<p>Symptom: Incorrect left navigation pane and/or feature data shown on summary screens while switching between devices.</p> <p>Conditions: Navigate to the community screen and back while viewing a feature summary screen.</p> <p>Workaround: Use the device selected to re-select the required device and then click on the left navigation pane link for the feature.</p>
CSCtb14313	Cisco CP allows class removal with Firewall PT in GETVPN.	<p>Symptom: Connection to the device is lost when configuring GETVPN on a firewall outside interface with Cisco CP discovered through the same outside interface.</p> <p>Conditions: This occurs if Cisco CP discovered interface is a firewall outside interface and in the same interface, GETVPN is configured.</p> <p>Workaround: Rediscover the device.</p>
CSCtb14050	Cisco CP hangs when trying to upload files through SSL VPN.	<p>Symptom: Cisco CP hangs when trying to upload files through SSL VPN.</p> <p>Workaround: There is no workaround.</p>
CSCtb05571	Forward PSTN access digit not working.	<p>Symptom: In some cases, during creation or edit of Outgoing Dial Plan, forward PSTN access digit does not work as expected. Even after choosing to forward the PSTN access digit for a particular trunk, Cisco CP strips out the PSTN access digit.</p> <p>Workaround: There is no workaround to resolve this issue using Cisco CP. But you can choose to manually change the CLIs on the router to resolve this issue.</p>
CSCtb24637	Post install fails for Pano device.	<p>Symptom: After the successful discovery of Video gateway module which is in post install prompt, trying post install for video gateway module succeeds in Cisco CP screen. But, the console prompt of video gateway module is still seen in post install.</p> <p>Conditions: Router with Video gateway in post install prompt is discovered and an attempt is made to initialize the Video Gateway through Cisco CP..</p> <p>Workaround: There is no workaround. The initialization of the Video gateway has to be performed manually..</p>

Table 13 *Open Caveats in Cisco CP 1.4 (continued)*

Bug ID	Summary	Additional Information
CSCtb25590	Deleting multiple extensions throws exception.	<p>Symptom: org.hibernate.LazyInitializationException : session is not connected is seen when you try to delete extensions.</p> <p>Conditions: Selecting multiple extensions with one or more of them associated to Users and trying to delete all the extensions.</p> <p>Workaround: Delete the extensions one by one.</p>
CSCta86408	Device needs to be discovered after moving to the online mode.	<p>Symptom: The device that was discovered in online mode is shown as discovered, even after moving to offline mode and coming back to online mode.</p> <p>Conditions: The device is discovered in online mode before moving to offline mode. Changes made in the offline mode are applied to the device, then the device is moved back to the online mode. The discovery state of the device remains as discovered after moving back to the online mode.</p> <p>Workaround: Re-discover the device.</p>

Related Documentation

Table 14 describes the related documentation available for Cisco Configuration Professional.

Table 14 *Cisco Configuration Professional Documentation*

Document Title	Available Formats
<i>Cisco Configuration Professional User Guide 1.4</i>	<p>This guide is available in the following formats:</p> <ul style="list-style-type: none"> On Cisco.com. Accessible from Online help.
<i>Release Notes for Cisco Configuration Professional 1.4</i> (this document)	On Cisco.com.
<i>Cisco Configuration Professional Quick Start Guide</i>	<p>This guide is available in the following formats:</p> <ul style="list-style-type: none"> On Cisco.com from the Software download page. On the product CD-ROM. Click documents > QuickStartGuide.pdf.

Table 14 *Cisco Configuration Professional Documentation (continued)*

Document Title	Available Formats
<i>Cisco Configuration Professional Getting Started Guide</i>	On the product CD-ROM. During the installation process, just before you have finished installing the product, you are provided the option to read the Getting Started guide.
<i>Cisco Configuration Professional Express User Guide</i>	Accessible from Online help.
<i>Release Notes for Cisco Configuration Professional Express</i>	On Cisco.com.
<i>Read Me Before Configuring the Router</i>	Printed document included with your router.

**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.

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0907R)

Copyright © 2009 Cisco Systems, Inc. All rights reserved.

