



Release Notes for Cisco Configuration Professional 1.1

April 26, 2010

These release notes support Cisco Configuration Professional (Cisco CP) version 1.1. They should be used with the documents listed in the “[Related Documentation](#)” section.

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

Contents

This document contains the following sections:

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

Introduction

Cisco CP is a graphical configuration tool that allows you to create and manage router communities, and to configure LAN and WAN interfaces, routing, Network Admission Control (NAC), Network Address Translation (NAT), firewalls, the Intrusion Prevention System (IPS), Virtual Private Networks (VPNs), and many other router features. 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 enables a user to configure a LAN and WAN connection, make security settings to protect the router, and, configure a basic firewall, and Network Address Translation.

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.

Table 1 *PC System Requirements*

System Component	Requirement
Processor	2 GHz processor or faster.
Random Access Memory	1 GB. 2 GB recommended
Hard disk available memory	200 MB
Operating System	Any of the following: <ul style="list-style-type: none"> • Microsoft Windows Vista Business Edition. Microsoft recommends this operating system be installed in administrator mode. • Microsoft Windows Vista Ultimate Edition. Microsoft recommends this operating system be installed in administrator mode. • Microsoft Windows XP with Service Pack 2
Browser	Internet Explorer 6.0 or later
Screen Resolution	1024 X 768
Java Runtime Environment	JRE 1.5.0_11 or later
Adobe Flash Player	Version 9.0.124 or later, with Debug set to No
Secure Shell (SSH)	Required for secure connections with the router. Versions 1.99 and 2.0 are supported.

Router System Requirements

Router System Requirements are described in the following parts:

- [Supported Routers](#)
- [Supported Adapters, Cards and Network Modules](#)
- [Cisco IOS Releases](#)

- [Cisco IOS IPS Feature History](#)
- [Router Configuration Requirements](#)

Supported Routers

This section lists the routers that Cisco CP supports, by series.



Note

Cisco CP does not support Telco/CO router models.

Cisco 800 series:

- Cisco 815
- Cisco 851
- Cisco 857
- CISCO861-K9
- CISCO861W-GN-A-K9
- CISCO861W-GN-E-K9
- CISCO861W-GN-P-K9
- Cisco 871
- Cisco 876
- Cisco 878
- Cisco 877
- Cisco 851W
- Cisco 857W
- Cisco 871W
- Cisco 876W
- Cisco 878W
- Cisco 877W
- CISCO881-K9
- CISCO881W-GN-A-K9
- CISCO881W-GN-E-K9
- CISCO881W-GN-P-K9
- CISCO881G-K9
- CISCO881GW-GN-A-K9
- CISCO881GW-GN-E-K9
- CISCO888-K9
- CISCO888W-GN-A-K9
- CISCO888W-GN-E-K9
- CISCO888G-K9
- CISCO888GW-GN-A-K9

- CISCO888GW-GN-E-K9

Cisco CP is supported on the following Cisco 1800 series routers:

- Cisco 1801
- Cisco 1801W
- [Cisco 1801W-M](#)
- [Cisco 1801M](#)
- Cisco 1802
- Cisco 1802W
- Cisco 1803
- Cisco 1803W
- Cisco 1805 series
- Cisco 1811
- Cisco 1811W
- Cisco 1812
- Cisco 1812W
- Cisco1812J
- Cisco 1812W-J
- Cisco 1812W-P
- Cisco 1841
- Cisco 1861 Integrated Services Router

Cisco CP is supported on the following 2800 series Integrated Services Routers:

- Cisco 2801
- Cisco 2811
- Cisco 2821
- Cisco 2851

Cisco CP is supported on the following Cisco 3800 Integrated Services routers:

- Cisco 3825
- Cisco 3845

Cisco CP is supported on the following Cisco 7000 series routers:

- Cisco 7204VXR
- Cisco 7206VXR
- Cisco 7301

Supported Adapters, Cards and Network Modules

Cisco CP supports the following network modules:

- NM-4T
- NM-1FE2W-V2

- NM-1FE-FX-V2
- NM-2FE2W-V2
- NM-1FE-FX
- NM-4A/S (synchronous only)
- NM-8A/S (synchronous only)
- NM-CIDS-K9
- NM-16ESW
- NM-16ESW-1GIG
- NM-16ESW-PWR
- NM-16ESW-PWR-1GIG
- NMD-36ESW-PWR
- NMD-36ESW-PWR-2GIG

Cisco CP supports the following EtherSwitch Service Network Modules:

- NME-16ES-1G-P
- NME-X-23ES-1G-P
- NME-XD-24ES-1S-P
- NME-XD-48ES-2S-P

Cisco CP supports the following Wide Area Application Services (WAAS) modules:

- NME-WAE-502-K9
- NME-WAE-522-K9
- NME-WAE-302-K9

Cisco CP supports the following WAN interface cards:

- WIC-1T
- WIC-2T
- WIC-2A/S (Frame Relay, PPP, HDLC, no asynchronous)
- WIC-1ADSL
- WIC-1DSU-T1-V2
- WIC-1B-S/T-V3
- WIC-1AM
- WIC-2AM
- WIC-4ESW
- WIC-1SHDSL-V2
- WIC-1SHDSL-V3
- WIC 1ADSL-DG
- WIC 1ADSL-I-DG

Cisco CP supports the following high-speed WAN interface cards (HWICs):

- HWIC-4T
- HWIC-4A/S

- HWIC-4ESW
- HWIC-8A
- HWIC-8A/S-232
- HWICD-9ESW
- HWIC-16A
- HWIC-AP-G-X
- HWIC-AP-AG-X
- HWIC-ADSL-B/ST
- HWIC-ADSLI-B/ST
- HWIC-1ADSL
- HWIC-1ADSLI
- HWIC-2SHDSL
- HWIC-4SHDSL
- HWIC1-ADSL-M
- HWIC-1CABLE-D
- HWIC-1CABLE-E/J
- HWIC-1FE
- HWIC-2FE

Cisco CP supports the following advanced integration modules (AIMs):

- AIM-VPN/BP II PLUS
- AIM-VPN/EP II PLUS
- AIM-VPN/HP II PLUS
- AIM-VPN/SSL-1
- AIM-VPN/SSL-2
- AIM-VPN/SSL-3

Cisco CP supports the following voice modules:

- VWIC2-1MFT-T1/E1 (Voice Only)
- VWIC2-2MFT-T1/E1 (Voice Only)
- NM-HD-1V
- NM-HD-2V
- NM-HD-2VE
- NM-HDA-4FXS
- NM-HDV2
- NM-HDV2-1T1/E1
- NM-HDV2-2T1/E1

Cisco CP supports the following port adapters on Cisco 7000 family routers:

- PA-2FE-TX
- PA-2FE-FX

- PA-8E
- PA-4E

Cisco CP supports the following Network Processing Engines and Network Service Engines on Cisco 7000 family routers.

- NPE-225
- NPE-400
- NPE-G1
- NPE-G2
- NSE-1

Cisco CP supports the following service adapters on Cisco 7000 family routers:

- SA-VAM
- SA-VAM2
- SA-VAM2+
- C7200-VSA

Cisco IOS Releases

Cisco CP is compatible with the Cisco IOS releases listed in [Table 2](#).

Table 2 Cisco CP-Supported Routers and Cisco IOS Versions

Router Model	Earliest Cisco CP-Supported Cisco IOS Versions
Cisco 815	<ul style="list-style-type: none"> • 12.4(11)T
Cisco 860 series Cisco 880 series	<ul style="list-style-type: none"> • 12.4(15)XZ
Cisco 1801 Cisco 1802 Cisco 1803	<ul style="list-style-type: none"> • 12.4(9)T
Cisco 1805	<ul style="list-style-type: none"> • 12.4(15)XY
Cisco 1811 Cisco 1812	<ul style="list-style-type: none"> • 12.4(9)T
Cisco 1841	<ul style="list-style-type: none"> • 12.4(9)T
Cisco 1861	<ul style="list-style-type: none"> • 12.4(11)XW
Cisco 2800	<ul style="list-style-type: none"> • 12.4(9)T
Cisco 3800	<ul style="list-style-type: none"> • 12.4(9)T
Cisco 7000	<ul style="list-style-type: none"> • 12.4(9)T

Cisco IOS IPS Feature History

[Table 3](#) 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 3 *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
```

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.

Router Configuration Requirements

In order to run Cisco CP, a router configuration must meet the requirements shown in [Table 4](#).

Table 4 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 5 on page 9](#) describes the ordering options under which Cisco CP can be ordered.

Cisco Configuration Professional Express (Cisco CP Express) is a product that is shipped in router flash memory when the router is ordered with Cisco CP.

Table 5 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 5 *Cisco CP Ordering Options*

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

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 Features

Cisco CP 1.1 supports the following new features.

- Voice Support—Cisco CP enables the router to operate in the following voice modes:
 - As a Cisco Unified Communications Manager Express device.
 - As a gateway to a Cisco Unified Communications Manager. If this mode is chosen, the router can be configured as an SRST gateway as well.
- Reloading Cisco Unity Express—After you have used Cisco CP to make router configuration changes, you can reload Cisco Unity Express (CUE) from the Cisco CP interface so that CUE can read the changes in the configuration.
- Content Filtering Support—The router can be configured to use Trend Micro subscription-based category filtering, or to use Websense or Secure Computing content filter servers.
- Feedback Form—You can use the mailbox icon on the toolbar to display a web-based feedback form. When you click Submit in this form, the feedback you provided is sent to Cisco.
- Automatic collection of technical support data—You can collect technical support data whether or not Cisco CP is running, by going to **Start > All Programs > Cisco Configuration Professional > Collect Data for Tech Support**. Cisco CP automatically archives the logs in a zip file named `_ccptech.zip`, which it saves in a folder that it places on the PC desktop. The folder is named using the convention **CiscoCP Data for Tech Support YYYY-MM-DD_hh-mm-sec**. An example folder name is CiscoCP Data for Tech Support 2008-06-28_18-03-13.
- New hardware support—The following lists contain the new hardware that Cisco CP supports.

Cisco CP adds support for the following routers:

 - Cisco 851
 - Cisco 857

- Cisco 861
- Cisco 871
- Cisco 876
- Cisco 878
- Cisco 877
- Cisco 851W
- Cisco 857W
- Cisco 871W
- Cisco 876W
- Cisco 878W
- Cisco 877W
- Cisco 881

Cisco CP adds support for the following voice modules:

- VWIC2-1MFT-T1/E1 (Voice Only)
- VWIC2-2MFT-T1/E1 (Voice Only)
- NM-HD-1V
- NM-HD-2V
- NM-HD-2VE
- NM-HDA-4FXS
- NM-HDV2
- NM-HDV2-1T1/E1
- NM-HDV2-2T1/E1

Limitations and Restrictions

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

- [Cisco CP Requires Microsoft Windows Vista Be Installed in Administrator Mode](#)
- [Cisco CP Minimum Screen Resolution](#)
- [Restrictions for Cisco 7204VXR, Cisco 7206VXR, and Cisco 7301 Routers](#)

Cisco CP Requires Microsoft Windows Vista Be Installed in Administrator Mode

In order to run Cisco CP under Microsoft Windows Vista, Microsoft Windows Vista 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 Not Launch Using IP Address of SSL VPN Gateway](#)
- [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](#)

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 Not Launch Using IP Address of SSL VPN Gateway

This information provides more information about the caveat CSCek33306. When Cisco CP attempts to connect to a router with a SSL VPN gateway configured using the Cisco IOS CLI, it might not launch from the IP address used by that gateway if the CLI statements necessary for Cisco CP access are not included.

For example, if you have configured a SSL VPN connection on the interface Fe 0/0 with the gateway IP address 10.10.10.1, and the gateway name MySSLVPN, you may not be able to launch Cisco CP using that IP address.

To be able to launch Cisco CP using that IP address, add the following Cisco IOS CLI commands:

```
Router# config t
Router(config)# interface loopback next-available-loopback-number
Router(config-if)# description Do not delete - SDM SSLVPN generated interface
Router(config-if)# ip address 192.168.1.1 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# ip nat inside
Router(config-if)# exit
Router(config)# ip nat inside source static tcp 192.168.1.1 443 10.10.10.1 4443
Router(config)# router(config)# webvpn gateway MySSLVPN
Router(config-webvpn-gateway)# http-redirect port 80
Router(config) # interface FastEthernet 0/0
```

```
Router(config-if)# ip nat outside
Router(config-if)# exit
```

After adding these commands, you can launch Cisco CP by entering the following IP address and port in the browser:

```
https://10.10.10.1:4443
```

If you remove the SSL VPN gateway that was modified for Cisco CP access, you must remove the loopback interface and the Network Address Translation (NAT) rule that you created to allow access in the first place. Enter the commands shown in the description of caveat CSCek38259.

## 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
```

## Cisco Configuration Professional Is Already Running Message

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

- 
- Step 1** Press **Ctrl Alt Delete**, and click **Task Manager**.
  - Step 2** In the Windows Task Manager dialog, click **Processes**.
  - Step 3** In the Image Name column, highlight the process javaw.exe.
  - Step 4** Click **End Process**.
  - Step 5** Wait 30 seconds, and then restart Cisco CP.
- 

## Technical Support Logs Do Not Appear on Desktop

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

## Discovery Never Completes

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

- 
- Step 1** Choose **Application > Exit** to shut down Cisco CP.
  - Step 2** Go to **Start > Control Panel > Java**. The General tab is displayed.
  - Step 3** In the Temporary Internet Files box, click **Delete Files**.
  - Step 4** In the displayed dialog, leave all file types checked, and click **OK**.
  - Step 5** Click **OK** in the Java control panel to close it.
  - Step 6** Restart Cisco CP.
-



# Caveats

Caveats describe unexpected behavior in Cisco CP. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

## Open Caveats—Cisco CP 1.1

This section lists caveats that are open in Cisco CP 1.1.

- CSCsm64482

When clicking the link for configuring the WAAS NM- Central Manager in Cisco CP, the following warning message is displayed: “Are you sure want to navigate away from this page?” If you click OK, Cisco CP closes.

**Workaround:** In Internet Explorer, go to **Tools > Internet options -> Advanced**. Uncheck the “Reuse windows for launching shortcuts” option.

- CSCsm34923

Cisco CP shortcut keys do not function in Cisco CP, but perform their equivalent function in Internet Explorer.

- CSCsm93416

When Cisco CP is launched, the splash screen hides the Java applet digital signature screen. The user must click on the digital signature screen to bring it in focus so that he or she can click Run and start using Cisco CP.

- CSCsm89756

Discovery fails for a user when the user is not configured for both vty access and HTTP access using the same authentication method. For one user, the credentials for vty access and HTTP access must be the same, and the authentication method must be the same. For example, the authentication method may be authentication local, or authentication aaa, but it must be the same for both types of access.

- CSCsk51555

This caveat is caused by Cisco IOS caveat CSCsl42697. When configuring a radio interface using the Cisco CP Wireless application, QoS access commands such as max-contention and min-contention window settings are not delivered to the router.

- CSCsk88931

This caveat is caused by Cisco IOS caveat CSCsl39285. Registration with the WAAS Central Manager from the WAAS NM tab fails when the username, password, and primary interface are entered and the user clicks OK.

- CSCsl47234

When a AAA network authorization policy is being added, the delivery of IOS CLI commands to the router fails if the if-authenticated method is selected along with other methods,

- CSCsl00095

Due to a Cisco IOS 12.4(15)T1 issue, when an Easy VPN Server is configured with the split DNS option, and an Easy VPN remote client is configured on another router, the details screen on the remote client does not display split DNS details for the Easy VPN server.

- CSCsl32119

When Cisco CP is used to configure Cisco IOS IPS on a Cisco 7301 router, Cisco CP may take as much as 10 minutes to launch and correctly display Cisco IOS IPS signatures. If Cisco CP launches without delay, Cisco IOS IPS signatures are not displayed correctly, and errors can be seen when the Edit Signatures window is displayed. When the Cisco CP display is refreshed in these circumstances it may take up to 10 minutes for the signatures to be displayed correctly.

This problem has been found on 7301 routers running Cisco IOS 12.4(11)T3, when Cisco CP is run under Internet Explorer 6.0 using Java Runtime Environment 1.6.0\_03.

- CSCsk98378

Due to a Cisco IOS problem described in CSCsk67302, the output of the show running-config command will not show SSL VPN gateways associated with SSL VPN contexts. This problem has been found in Cisco IOS 12.4(15)T and 12.4(15)T1 images

- CSCsj21989

For a description of this caveat, see [Cisco CP Merge and Replace Configuration Functions Fail Under Some Conditions, page 14](#).

- CSCsh11991

Because of a Cisco IOS IPS problem, when migrating a Cisco IOS IPS configuration created using a Cisco IOS image older than version 12.4(11)T to a 12.4(11)T or later environment, user-modified signatures are not migrated.

**Workaround:** After migrating, use the Add or Edit controls in the Edit IPS window to create the signature in the new format.

- CSCsh39685

Because of Cisco IOS caveat CSCek68311, a Certificate Authority (CA) server created using the Cisco CP CA Server wizard will be shown as stopped. This problem occurs when the router is running a Cisco IOS 12.4(11)T image.

**Workaround:** Upgrade the Cisco IOS image on the router to version 12.4(11)T2.

- CSCsh41150

When the router is running a Cisco IOS image older than 12.4(11)T the Easy VPN Server Status screen in Monitoring mode displays the IP address of a client configured with a Dynamic Virtual Template Interface (DVTI) as 0.0.0.0.

- CSCsh46525

You may be unable to delete a DVTI-based Easy VPN Remote configuration using Cisco CP.

**Workaround:** Click **Refresh** in the Cisco CP toolbar and then delete the configuration.

- CSCsi03518

When a firewall is configured using Cisco CP, and then Cisco CP is used to create an SSL VPN configuration on the router, a NAT passthrough configuration is added by the SSL VPN wizard. No NAT passthrough configuration is added when creating an SSL VPN configuration using the SSL VPN edit windows.

- CSCsh44720

When Cisco CP installed on a PC is invoked in Internet Explorer 7.0 using either HTTP or HTTPS, the popup window asking for the IP address of the router appears again after the IP address has been entered in the first popup window.

When Cisco CP installed on router flash memory invoked in Internet Explorer 7.0 using HTTPS, a certification error is displayed. Cisco CP starts if you choose **Continue to this website (not recommended)**.

- CSCek38259

If the router is configured to allow Cisco CP access through a SSL VPN gateway that listens on the standard port 443, and that gateway is modified to listen on another custom port, the commands that were added for Cisco CP access are not automatically removed, and must be removed using the Cisco IOS CLI. The SSL VPN gateway may have been configured using the SSL VPN wizard, or it may have been configured manually and then modified to allow Cisco CP access by adding the commands described in [Cisco CP May Not Launch Using IP Address of SSL VPN Gateway](#).

**Workaround:**

To safely edit the SSL VPN gateway to listen to a port other than 443, do the following:

- Go to **Configure > Security > VPN > SSLVPN > Edit SSL VPN**, select the gateway and click **Edit**.
- Uncheck the **Enable secure access through IP address** checkbox is checked, uncheck it, and click **OK** to deliver the configuration change to the router.
- Click **Edit** again and enter the port number that you want the SSL VPN gateway to use.
- Remove the loopback interface that was created for Cisco CP access by clicking **Configure > Router > Interfaces and Connections > Edit Interfaces/Connections** and removing the loopback interface.
- To remove the NAT rule, click **Configure > Router > NAT > Edit NAT Configuration**, and remove the NAT rule that was added. Do not remove the NAT rule if it is being used by other parts of the configuration.

Cisco CP can now be invoked using the standard HTTPS port 443.

If you prefer to use the Cisco IOS CLI, enter the following commands to remove the loopback interface and NAT rule that were added to allow Cisco CP access. In these steps, Loopback 0 with an IP address of 192.168.1.1, and FastEthernet 0/0 with an IP address of 10.20.30.40 are used as examples.

```
Router# config t
Router(config)# no interface Loopback0
Router(config)# interface FastEthernet0/0
Router(config-if)# no ip nat outside
Router(config-if)# exit
Router(config)# no ip nat inside source static tcp 192.168.1.1 443 10.20.30.40 4443
Router(config)# exit
```



**Note** Do not enter the no ip nat inside command if other NAT translation rules are using it. If no other rules use this command, remove it.

- CSCek33306

Cisco CP may not launch from an interface with a CLI-configured SSL VPN if the CLI commands necessary for Cisco CP access have not been added. This includes SSL VPNs configured with the command **webvpn enable SSLVPNname IP-address SSLVPN**.

For more information about this caveat, see the [“Cisco CP May Not Launch Using IP Address of SSL VPN Gateway](#).

- CSCei33081

When Cisco CP is run on the PC, the Load File from PC function available from the File Management window may not work properly.

**Workaround:** With a TFTP server application on the PC, copy files to the router using the **copy tftp flash** command.

- CSCej01054

The SDM\_HIGH security policy may not block Instant Messaging (IM) applications. The application security feature blocks IM applications using the **server deny name** command. New servers may become available, and if they do, IM applications may connect to them.

**Workaround:** Complete the following steps:

- Turn on firewall logging for IM applications. The names of the servers that the IM applications connect to will be revealed in the log.
- Use the CLI to block the new servers. The following example uses the server *newserver.yahoo.com*:

```
router# config t
router(config)# appfw policy-name SDM_HIGH
router(cfg-appfw-policy)# application im yahoo
router(cfg-appfw-policy-ymsggr)# server deny name newserver.yahoo.com
router(cfg-appfw-policy-ymsggr)# end
router#
```



**Note**

- IM applications are able to communicate over nonnative protocol ports, such as HTTP, and through their native TCP and UDP ports. Cisco CP configures block and permit actions based on the native port for the application, and always blocks communication conducted over HTTP ports.
- Some IM applications, such as MSN Messenger 7.0, use HTTP ports by default. To permit these applications, configure the IM application to use its native port.

- CSCei84100

When the applications security policy blocks some Peer-to-Peer (P2P) applications, but permits others, blocked applications may be able to download files.

**Workaround:** Instead of permitting some P2P applications and blocking others, exclude the applications that you want to permit from the application security policy by unchecking the box next to the application name.

- CSCej07924

Because of a problem with the Cisco IOS NBAR feature, some Peer-to-Peer applications are able to download files even when application security is configured to block them. When the Cisco IOS NBAR feature is used to block Peer-to-Peer applications, only those applications and protocols supported by the NBAR feature will be successfully blocked.

- CSCsb26386

Because of a problem with Cisco IOS (CSCin92327), a connection between an Easy VPN Remote client and an Easy VPN Server may timeout before the user has time to enter the credentials.

**Workaround:** None

- CSCsb59200

Due to a JVM bug ([http://bugs.sun.com/bugdatabase/view\\_bug.do?bug\\_id=4110094](http://bugs.sun.com/bugdatabase/view_bug.do?bug_id=4110094)) Cisco CP IPS may crash when large Signature Definition Files (SDF) are imported. When Cisco CP is used to import large SDFs such as virtualsensor.xml or IOS-S178.zip, Cisco CP crashes when dismissing the Import Signature dialog. This problem does not always occur.

**Workaround:** Set the java heap size to -Xmx256m and try to import the file again. If you need to use Cisco CP to perform a critical operation, complete that operation before reattempting to import the file.

- CSCsa40535

VPN status in the Monitor windows do not show IPsec security association (SA) parameters for DMVPN when CLI status commands report that the crypto tunnels are up and traffic is passing through. The DMVPN tunnel is shown as established in the IKE SA tab.

**Workaround:** Use the CLI to view DMVPN status.

- CSCef43267

When the **crypto identity ca** command is used, the Loopback0 interface is shown as having no configured IP address in the Edit Interfaces and Connections window when an IP address has been configured.

**Workaround:** Disregard the IP address information in the Interfaces and Connections window. If you need to view the IP address, choose the interface and click the Edit button.

- CSCef50389

When an Easy VPN Server is configured using Digital Certificates for authentication, and an Easy VPN Remote connection is configured on another router, the client statistics for the Easy VPN server are all shown as 0 in the VPN Status window.

**Workaround:** To view client statistics, choose **Tools > Telnet**. Log in to the router, and issue the **show crypto session** command.

- CSCef63313

If an Easy VPN Remote configuration has connections to more than one Easy VPN server configured, VPN troubleshooting deactivating may report troubleshooting results for only one VPN server or give incorrect recommendations. This issue is seen only in some Cisco IOS images.

- CSCef72022

Invoking Cisco CP with a user associated with SDM\_Monitor view adds a PKI trust point and an Easy VPN profile. This behavior does not affect the running configuration.

**Workaround:** Invoke Cisco CP with a user associated with a different CLI view, or with a user of privilege level 15.

- CSCef77689

When the router is running a Cisco IOS image that does not support the **show pppoe session** command, WAN troubleshooting may not report any reasons for failure or recommended actions for PPPoE connections that are found to be down.

- CSCin54600

If a firewall is configured for an interface which already has a Management Access policy associated with it, choosing **Replace** in the Merge/Replace dialog box might prevent access to certain networks.

This occurs because choosing **Replace** causes the policy access control entries (ACEs) to be disassociated from the interface but not from the vty or HTTP line.

**Workaround:** When running Firewall wizard on an interface configured with Management Access policy, choose **Merge** option instead of **Replace** and proceed.

- CSCef73879

VPN troubleshooting may report a possible Maximum Transmission Unit (MTU) problem in the passthrough network when the tunnel is up. If the VPN interface is a dialer interface configured on an asynchronous interface, this problem may not always exist, and the displayed recommended action will have no effect.

**Workaround:** Ignore this message and the corresponding recommendation.

- CSCea89054

If you delete a WAN connection that you created, an **ip nat inside** command may still remain in a LAN interface configuration.

**Workaround:** To delete the **ip nat inside** command from the LAN interface configuration, go to Edit Interfaces and Connections, choose the LAN interface, click Edit, and delete the association in the Association tab.

- CSCin44264

Enabling AES encryption or IP compression in the Add/Edit IKE Policy or Add/Edit Transform Set windows might not work even though the Cisco IOS image running on the router supports AES encryption or IP Compression. This may happen in the following circumstances:

- Hardware encryption is enabled.
- The router has a VPN module that does not support AES encryption or IP compression.

**Workaround:** Do one of the following:

- Disable hardware encryption by adding the **no crypto engine accelerator command to the configuration file** using the CLI interface. This command tells the router to use Cisco IOS software for encryption instead of using the encryption provided by the VPN module.
- Upgrade your hardware VPN module to one that supports AES or IP compression.

For more info on VPN Modules, see the data sheet at the following link: [VPN data sheet](#).

- CSCdy80223

When Cisco CP runs with a Cisco IOS image of a release earlier than 12.3T, or earlier than Release 12.2(13)ZH, the HTTP server appends unnecessary characters to names of files it displays. As a result, when Cisco CP is started, the web browser displays the warning “Content does not match the signature.”

**Workaround:** Disregard the warning and click **Yes** to continue.

- CSCin44119

When an Easy VPN tunnel is active, using Cisco CP to apply a NAT configuration to the Easy VPN inside and outside interfaces will deliver **ip nat inside** and **ip nat outside** commands to the router, but the running configuration will not be changed. Cisco CP displays no error message when this is attempted.

**Workaround:** To apply a NAT configuration to interfaces that have been designated as Easy VPN inside or outside interfaces, complete the following steps in Cisco CP:

- Choose the Easy VPN tunnel in the VPN Connections window and click **Disconnect**. If the Connect/Disconnect button is disabled, choose the interface in the Interfaces and Connections window, open the Association tab for that connection and change the Easy VPN association to **None**.

- Open the NAT window, click **Designate NAT Interfaces**, and designate NAT inside and NAT outside interfaces.
- Select the Easy VPN tunnel, and click **Connect**. If you had to disassociate the Easy VPN tunnel from the connection, return to the Association tab, and choose the Easy VPN connection name again.

- CSCed31085

Cisco CP should not get invoked from boot images such as kboot images on 72xx routers. Such boot images are a subset of the Cisco IOS software and do not support all router functions.

**Workaround:** Boot the router with an Cisco CP-supported Cisco IOS image, and then invoke Cisco CP. See [Table 2 on page 7](#) for the Cisco IOS releases that Cisco CP supports.

- CSCed30721

Whenever any unconfigured interface contains the description \$FW\_INSIDE\$, on a router configured with a firewall, adding a new NTP server will not modify the firewall ACLs to allow NTP passthrough traffic. Instead, when the user edits the firewall's outside interface in the Interfaces and Connections window, Cisco CP prompts the user to add the NTP passthrough traffic.

**Workaround:** Use the CLI to manually remove the description \$FW\_INSIDE\$ from the unconfigured interface.

- CSCin63613

If the interface used for the primary backup connection is configured for PPPoE encapsulation, the backup connection will not function properly if the next hop address is specified during configuration. A Cisco IOS caveat (CSCin64336) has been filed for this problem. If the interface used for the primary backup connection is an Ethernet interface configured without encapsulation, the backup connection will not function properly if the next hop address is not specified during configuration.

**Workaround:** Do one of the following:

- For PPPoE connections: *Do not* provide the next hop IP address when you configure the primary backup connection.
- For Ethernet connections without encapsulation: *Do* provide the next hop IP address when you configure the primary backup connection.

- CSCin63415

If the WAN wizard is used to configure an analog modem connection as a primary backup connection, and the analog modem connection is deleted, Cisco CP may report that the interface contains unsupported configuration parameters.

**Workaround:** Click **Refresh** on the Cisco CP toolbar, and delete the connection.

- CSCed18560

The Interfaces and Connections window may display the Backup option in disabled state for asynchronous interfaces on Cisco 831 and Cisco 837 routers. This will occur when the following operations have been performed:

- The interface used for the primary backup connection is configured with an Cisco CP-supported IP address type.
- The asynchronous interface is configured as the backup for a primary interface.
- The IP address of the primary interface is changed.

When the IP address of the primary interface is changed, Cisco CP displays a Yes or No warning popup asking if you want to remove the backup configuration. If you choose **Yes**, Cisco CP removes the backup configuration, but the Interfaces and Connections window still shows the backup option as disabled, preventing you from choosing the asynchronous interface as a backup interface.

**Workaround:** Delete the asynchronous interface configuration using the Interfaces and Connections window.

- CSCin48956

When the router is configured to use PPPoE, users may not be able to download a file using FTP or display web pages from Internet hosts that they are able to ping or access using telnet. This can happen if Cisco CP is being used on a router with interfaces that Cisco CP does not support, such as Token Ring or VLAN interfaces. Cisco CP does not deliver the command **ip tcp adjust-mss 1452** to unsupported interfaces.

**Workaround:** Use the CLI to add the **ip tcp adjust-mss 1452** command to the VLAN or Token Ring interface configuration. Use Telnet to access the router and enter the following command in VLAN or Token Ring interface configuration mode:

```
Router# ip tcp adjust-mss 1452
```

- CSCed08825

Cisco CP may take several seconds to display screens in the DMVPN wizard. This latency may occur if a Java plug-in is running in the browser.

- CSCed13205

Cisco CP does not issue the **ntp update-calendar** Cisco IOS command on Cisco 7200 routers if there are no new settings to enter and if the Network Time Protocol (NTP) server was configured using the CLI, only one NTP server IP address was provided and no **ntp update-calendar** Cisco IOS command was present in the running configuration.

**Workaround:** Use Cisco CP to delete the NTP server configuration entry, click Refresh, and then re-create the entry, or make changes to the existing NTP server entry.

- CSCef89472

A download exception message may appear in the Java console when Cisco CP is launched on a PC running Japanese Windows 2000, or Japanese Windows XP. This problem does not prevent Cisco CP from starting or from being used.

- CSCso44518

Cisco CP fails to show signature details on Cisco 7204 routers running Cisco IOS IPS available before Cisco IOS 12.4(11)T. A Cisco IOS caveat (CSCso59783) has been filed for this problem.

- CSCsl00304

If an existing NAT policy is modified, and the commands delivered to the router include the **timeout xlate** command, Cisco CP delivers an unnecessary **no timeout xlate** command. This can be seen in the Deliver Configuration to Router screen. This unnecessary command does not cause any problem.

- CSCso09200

If Cisco CP is used to create a softkey template, and IP phones are associated with that template, the phones are not restarted if the template is deleted. If Cisco CP is used to modify a softkey template, and IP phones are associated with that template, the phones are not restarted when the modifications are delivered to the router.

**Workaround:** In these cases, you must issue the Cisco IOS telephony-service mode **restart all** command, as shown in the following example:



```
Router# config terminal
Router(config)# telephony-service
Router(config-telephony-service)# restart all
Router(config-telephony-service)# end
Router#
```

- CSCso66478

Because of a Cisco IOS issue, no information about the number of packets matched is reported in the Firewall Status Monitor screen on routers running Cisco IOS image c3825-adventerprisek9-mz.125-0.10.PI1.

- CSCso83037

When entering text in Cisco CP voice screens, the backspace key may not be usable. This problem is intermittent.

**Workaround:** If this problem occurs, place the cursor in front of the text that you want to remove, and press the delete key to remove all characters.

- CSCsq02323

Because of a Cisco IOS issue, Trend Micro parameter maps do not provide for the configuration of a block-page redirect URL. Only a block-page message can be configured.

- CSCsq34313

Voice features on a router may not be enabled in Cisco CP if the router enable password is different from the password used to discover the router. This is the password entered in the Create or Edit Community Entry screen.

**Workaround:** Configure the enable password to be the same as the password used to discover the router.

- CSCsq34910

When Cisco CP is used to configure a Cisco 1861, it may show more phone licenses being available than are actually available on the router.

**Workaround:** The Cisco 1861 has 12 licenses available. Do not configure more than 12 IP phones.

- CSCsq48311

When a router equipped with an internal access point is discovered, it is possible to launch multiple instances of the access point configuration program.

**Workaround:** To prevent overwriting access point configuration changes by using another instance of the application, ensure that you do not open more than one instance.

- CSCsq55593

When the Content Filter wizard is used to configure Trend-based content-filtering policy on a router with Zone Based Firewall configured, the default commands for a Trend-Micro parameter map are delivered to the router. When an attempt is made to edit the Trend Global parameter map under Content Filtering components, Cisco CP generates extraneous parameter map commands. This does not affect the functioning of the router.

- CSCsq60961

When a user clicks OK in the IPS screen to enable SDEE, extraneous commands are delivered to the router. This does not affect the functioning of the router.

- CSCsr10077

Discovery of a router with a Cisco Unity Express (CUE) factory default configuration with can take up to 15 minutes.

- CSCsr50598

When a category-based Content Filtering policy is created in the content filtering wizard, the Edit URL Filtering Policy Map Entry dialog may only the option `cptrendparacatdeny0` in the Select Parameter Name list. This list should contain the options `cptrendparacatdeny0`, and `cptrendpararepdeny0`.

**Workaround:** From the Select Parameter Type list, choose another parameter type, for example, local. Then choose trend. Both `cptrendparacatdeny0`, and `cptrendpararepdeny0` are displayed in the Select Parameter Name list.

- CSCsr50953

When a user goes to Content Filtering Components > Parameter map and chooses N2H2 or Websense, no field for the server IP address is available in the parameter map Add or Edit dialog.

- CSCsr60469

The Add button is enabled in the Router > Security > ACL Editor Unsupported Rules, Externally-Defined Rules, and Default Rules windows.

**Workaround:** Do not create an ACL rule in any of these windows. You cannot edit or delete any rule that you create in these windows. Create rules in the Access Rules, NAT Rules, IPSec Rules, NAC Rules, or QoS Rules windows.

- CSCsr76694

If a user discovers two devices with both AAA and DNS disabled, goes to the Create SSL VPN screen, and enables AAA but does not enable DNS before switching to the second device, Cisco CP may not display the Enable DNS link on the Create SSL VPN for the second device even though DNS has not been enabled.

**Workaround:** When working with two or more discovered devices, complete all prerequisite tasks on one device before switching to another discovered device.

- CSCsr79413

Users may see the message “WAAS Module Registration Failed” when registering a WAAS NM-equipped router with the WAAS Central Manager (CM), when the router has in fact registered successfully.

**Workaround:** Log on to the WAAS CM and determine if the router has successfully registered. If so, the WAAS NM can be used. If it has not, reload the WAAS NM and reregister.

- CSCsq38466

When a user is configuring a category-based Content Filtering policy and tries to download a digital certificate, the download will fail if a remote access policy that would not allow the download of the certificate is applied to the interface on which the router would receive the certificate.

**Workaround:** If you do not want to change the remote access policy, use the Cisco IOS CLI to download the certificate. Otherwise, change the permitted protocols in the policy so that it does not block the download of the certificate.

- CSCsq73364

If a router with a DOS-based file system and a router without a DOS-based file system are discovered, Cisco CP may display the file information for the DOS-based file system router when the user is viewing the Flash File Management screen for the non DOS-based file system router. This can happen if the user switches between the Flash File Management displays of both routers.

**Workaround:** View the Flash File Management information for the non DOS-based file system router before viewing that information for the DOS-based file system router.

- CSCsr15435

Cisco CP can take up to 12 minutes to discover routers with a high number of users with voice mailboxes configured. This scenario was tested on a Cisco 3845 with 240 voice mailboxes configured.

- CSCsr27018

When Cisco CP discovers multiple devices with the secure option enabled, and the user chooses a device and goes to security screens, Cisco CP may stop responding if a different device is selected from the Select Community Member list.

**Workaround:** If you find that this problem occurs, discover devices individually and configure them.

- CSCsr31992

When using Cisco CP to configure voice features on an ISR router with a large voice configuration, such as a high number of user settings, phones, extensions, mailboxes and dialplans configured, Cisco CP may take several minutes to display screens with a large amount of data, such as the Incoming Dial Plans, Outgoing Dial Plans, and Voice Mailbox screens.

- CSCsr38576

If a router has accumulated a large log buffer, Cisco CP may take more than 15 minutes to display the contents of this buffer in the Monitor > Router > Logging tabs. This problem has been observed on a router with more than 7000 entries in the buffer.

**Workaround:** Reduce the size of the buffer by going to **Configure > Router > Logging > Edit** and lowering the number of bytes in the Buffer Size field.

- CSCsr43587

When using the Flash File Management feature to load Cisco IOS images on a router, Cisco CP may display a warning message that informs you that the image you are loading is not compatible with the router model. This problem has been observed when attempting to load Cisco IOS 12.4(20)T images on SRST880 and Cisco 880 series routers.

**Workaround:** If you have verified that the image you are loading is compatible with the router, complete the copy operation.

- CSCsr50709

In the Content Filtering Components > Parameter Map > URLF-Websense and URLF-N2H2 screens, Cisco CP indicates that the selection of a source interface is mandatory.

**Workaround:** Choose a source interface.

- CSCsr51122

If two routers with WAAS modules are discovered and the user registers one router with the WAAS CM, the second router will not be able to register with the CM.

**Workaround:** Discover one router and register with the CM. Then, restart Cisco CP, discover the second router, and register with the CM.

- CSCsr56744

If a user discovers several routers in non secure mode and goes to the Security > VPN Keys Encryption page and clicks Cancel in the Enter SSH Credentials dialog for each router, the Enter SSH Credentials dialog will reappear if the user rediscovers the devices in the Community Information screen.

**Workaround:** Instead of clicking Cancel, enter the SSH credentials in the dialog.

- CSCsr57869

If a Cisco 871 is discovered along with a router that supports only legacy firewall configuration, and a user runs the Firewall wizard to configure the Cisco 871, Cisco CP attempts to deliver a Point-to-Point protocol command, for example **match protocol edonkey signature**. Command delivery fails because the Cisco 871 does not support this type of command.

**Workaround:** Discover the Cisco 871 alone and run the Firewall wizard. This problem will not occur.

- CSCsr57926

If a user configures a legacy firewall on a device that supports Zone-Based Firewall, such as a device that runs Cisco IOS version 12.4(20T, and then uses the Content Filter wizard to create a Content Filtering policy, a warning message is displayed in the Interface Configuration screen that informs the user that the Zone-pair is null or empty.

**Workaround:** In order to create a Content Filtering policy on this type of router, configure a Zone-Based Firewall policy before configuring a Content Filtering policy.

- CSCsr61142

Cisco CP may report IPSec tunnel traffic statistics after IPSec tunnels have been shut down, and may report a high number of errors for tunnels through which traffic has been passing without errors.

- CSCsr61674

If a user changes the telephony license type in the Voice > Telephony Settings window after having previously delivered telephony settings changes to the router, Cisco CP prompts the user to reset phones in order for the configuration changes to apply.

**Workaround:** In order to deliver the configuration changes to the router, click **OK** in the Reset Phones message window.

- CSCsr63144

Because of Cisco IOS caveat CSCsr63134, routers running Cisco IOS 12.4(15)T cannot be configured with NTP server information.

**Workaround:** To be able to add NTP server information to the router configuration, use a different Cisco IOS image.

- CSCsr83281

If a user right-clicks on the vertical line separating the Feature bar from the Content pane, options unrelated to Cisco CP are displayed. If the user chooses an option, the Cisco CP display may become truncated.

**Workaround:** Restart Cisco CP.

- CSCsr86353

If a user configures more than 32 blocked patterns in the Voice > Telephony Features > After Hours Tollbar screen on a router running a Cisco IOS image that supports more than 32 blocked patterns, the next time the router is discovered, it will be discovered with errors, and the After Hours Tollbar screen will be incompletely displayed. This has been found with Cisco IOS 12.4(20)T images.

**Workaround:** Do not configure more than 32 blocked patterns.

- CSCsr17365

If a user goes to the Voice > Telephony Features > Night Service Bell > Weekly Schedule or to the Voice > Telephony Features > Night Service Bell > After Hours > Weekly Schedule screen and changes the Before or the After time of any day by clicking on the arrow next to the time displayed, the change may be applied to the wrong day. This problem is intermittent.

**Workaround:** Reset the times for the day that got updated and set the times for the day you want to update.

- CSCsr65388

If a user enters an out-of-range value in the Configure > Voice > Telephony Settings Telephony License Type field, such as 999, clicks Apply, and then returns to that field and enters a value that is within range, the red border that appeared around the field when the out-of-range value was entered remains.

**Workaround:** Enter a value that is within range and click **Apply**. The value will be accepted and the field border will return to its normal color.

- CSCsr75730

If an entered voice user ID is the same as the username in the Create or the Edit Community Entry screen for the router, the configuration will not be delivered.

**Workaround:** Enter a user ID for this user that is different from the username for the router.

- CSCsr75879

When Cisco CP is closed by clicking Application > Exit, a window may appear that you must click OK to close before the Cisco CP shutdown window is displayed. This problem is intermittent.

- CSCsu18131

Due to a Cisco IOS issue, discovery of a router whose hostname contains special characters will fail. For example, if a router has the hostname Router[3845], Cisco CP will not discover it.

**Workaround:** Use the Cisco IOS hostname command to change the router name to one that does not contain special characters. For example, Router[3845] could be changed to Router3845.

- CSCsr92422

When digital signal processors (DSPs) are depleted, and a T1/E1 module is configured as a digital trunk, Cisco CP does not display an error message, and does not send the configuration to the router.

- CSCso78069

If a dial peer configured for the SIP protocol pointing to another router has been configured using the Cisco IOS CLI, and no label has been configured, the dial peer shows up in the Voice > Dial Plans > Intersite VoIP screen with no name, and no name can be added in the Edit Intersite VoIP screen.

- CSCsr55637

Messages appearing in the Discovery Details screen may be truncated.

- CSCsr99608

If users create paging numbers in both Cisco CP and the Cisco IOS CLI, and this results in overlapping numbers, the overlap is not reported in the Discovery Details screen. This may result in problems with the paging feature.

**Workaround:** Edit the paging numbers in the Voice > Telephony Features > Paging Numbers screen. Cisco CP displays error messages if paging numbers overlap.

- CSCsu06985

When an analog phone entry is created on a router with a 4 FXS DID card, an unknown phone type error message may be displayed.

**Workaround:** Rediscover the router. The analog phone entry will be displayed.

- CSCsu22579

As Cisco CP is used, the log files that record activity and that can be used for troubleshooting grow in size, and may eventually use too much hard disk memory.

**Workaround:** Go to the directory in which you installed Cisco CP, and then change the directory to ...\\CiscoCP\\logs, and delete the log files. For example, if you installed Cisco CP in the default directory, you would go to C:\\Program Files\\Cisco Systems\\CiscoCP\\logs and delete the log files.

- CSCsu07130

When a device with the “@” character in the password is discovered along with other devices in the community, the discovery status for that device is “Discovered with errors,” with the reason “Security feature disabled” given in the Discovery Details screen. If the user attempts to configure security features, the data of another discovered device will be displayed. If no other devices are in the community, an error message is displayed when the user chooses this device in the Select Community Member list.

**Workaround:** Change the password for this device to one that does not contain the “@” character.

- CSCsu30913

Currently Cisco CP supports only ad-hoc conference extension numbers that start with the letter “A” followed by digits, for example, A001. Using Cisco CP to increase the number of sessions will fail if the expected number format is not followed.

- CSCsu08777, CSCsu36808, CSCsu38230, and CSCsu38187

When a router is discovered in secure mode, an error message may be displayed when performing operations such as switching from one voice mode to another or configuring a dial plan.

**Workaround:** Rediscover the device in secure mode. If the problem persists, discover the device in non-secure mode.

- CSCsu11542

Extensive use of the Cisco CP voice feature on a PC with limited available memory may cause the application to stop functioning.

- CSCsu07155

When switching between a router with an installed G.SHDSL controller and one without such a controller, G.SHDSL controller information may be displayed in the Interfaces and Connections screen of both routers.

## Related Documentation

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

- Release Notes for Cisco Configuration Professional Express 1.1
- Cisco Configuration Professional Express 1.1 User Guide
- Cisco Configuration Professional Community User Guide
- Cisco Configuration Professional Routing and Security User Guide

These documents are available from the following link:

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

**Note**

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

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Copyright © 2008 Cisco Systems, Inc. All rights reserved.

