



## **Getting Started with Cisco Configuration Professional**

### **Americas Headquarters**

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned 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. (1005R)

#### *Getting Started with Cisco Configuration Professional*

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.



# CONTENTS

## **Preface** iii

Audience iii

Purpose iii

Related Documentation iii

Obtaining Documentation and Submitting a Service Request iv

---

## **CHAPTER 1**

### **Introduction** 1-1

Understanding Cisco Configuration Professional 1-1

Initial Setup 1-1

Initial Setup for Deployed Devices 1-2

Initial Setup for Switches 1-4

Install Cisco CP 1-5

---

## **CHAPTER 2**

### **User Interface Features** 2-1

Understanding the User Interface 2-1

Window Layout 2-1

Menu Bar 2-2

Toolbar 2-3

Status Bar 2-4

Applications Menu Field Reference 2-4

Manage Community 2-4

User Profile 2-4

Options 2-5

Templates 2-5

Offline or Demo Mode 2-6

Online Help 2-8

---

## **CHAPTER 3**

### **Device Communities and Configuration Basics** 3-1

Basic Workflow 3-1

Understanding Device Communities 3-1

Creating a Community and Adding Devices 3-2

Managing the Devices in a Community 3-4

Discovering Devices 3-5

Device Community Reference	<b>3-6</b>
Manage Community Dialog Box	<b>3-6</b>
Community View Page	<b>3-8</b>
Configuration Basics	<b>3-10</b>
Supplementary Information	<b>3-15</b>
Things to Know About Discovering Devices	<b>3-16</b>
Cisco CP Configuration Requirements	<b>3-16</b>
Wrong Secure Shell Version May Cause Discovery to Fail	<b>3-17</b>
Understanding Discovery Failed Error Messages	<b>3-18</b>
Cisco CP May Overwrite Existing Credentials	<b>3-20</b>
Proxy Server Settings Might Cause Discovery to Fail	<b>3-20</b>
Setting the Java Heap Size Value to -Xmx256m	<b>3-20</b>
Collecting Cisco CP Technical Support Logs	<b>3-21</b>
Using Cisco Configuration Professional to Run show tech-support	<b>3-21</b>

---

**INDEX**



## Preface

---

### Audience

This guide is for system administrators and network managers who want to use a graphical user interface to manage standalone network devices or groups of devices. The guide presents Cisco Configuration Professional as a solution.

### Purpose

The purpose of this guide is to help users get started with Cisco Configuration Professional. It consists of these chapters:

- Introduction—What Cisco Configuration Professional is and what it does.
- User Interface Features—Explains the user interface features.
- Device Communities and Configuration Basics—The procedures for creating communities and configuring devices.

### Related Documentation

[Table 1](#) describes the related documentation available for Cisco Configuration Professional.

**Table 1** *Cisco Configuration Professional Documentation*

Document Title	Available Formats
<i>Readme First for Cisco Configuration Professional</i>	This document is available in the following locations: <ul style="list-style-type: none"><li>• On Cisco.com.</li><li>• On the product CD-ROM in the Documentation folder.</li></ul>
<i>Cisco Configuration Professional Quick Start Guide</i>	This guide is available in the following locations: <ul style="list-style-type: none"><li>• On Cisco.com.</li><li>• On the product CD-ROM in the Documentation folder.</li></ul>

**Table 1** Cisco Configuration Professional Documentation (continued)

Document Title	Available Formats
<i>Cisco Configuration Professional Getting Started Guide</i>	This guide is available in the following locations: <ul style="list-style-type: none"> <li>• On Cisco.com.</li> <li>• On the product CD-ROM in the Documentation folder.</li> <li>• During the installation process, just before you have finished installing the product, you are provided the option to read the Getting Started guide.</li> </ul>
<i>Cisco Configuration Professional User Guide</i>	This guide is available in the following locations: <ul style="list-style-type: none"> <li>• On Cisco.com.</li> <li>• Accessible from Online help.</li> </ul>
<i>Cisco Configuration Professional Express User Guide</i>	This guide is available in the following locations: <ul style="list-style-type: none"> <li>• On Cisco.com.</li> <li>• Accessible from Online help.</li> </ul>
<i>Release Notes for Cisco Configuration Professional</i>	This document is available in the following location: <ul style="list-style-type: none"> <li>• On Cisco.com.</li> </ul>
<i>Release Notes for Cisco Configuration Professional Express</i>	This document is available in the following location: <ul style="list-style-type: none"> <li>• On Cisco.com.</li> </ul>

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



# CHAPTER 1

## Introduction

---

This chapter introduces Cisco Configuration Professional (Cisco CP) and gives you the information that you need to start using it. This chapter contains the following sections:

- [Understanding Cisco Configuration Professional](#)
- [Initial Setup](#)
- [Install Cisco CP](#)

## Understanding Cisco Configuration Professional

Cisco Configuration Professional (Cisco CP) is a GUI based device management tool for Cisco access routers. This tool simplifies routing, firewall, IPS, VPN, unified communications, WAN and LAN configuration through GUI based easy-to-use wizards.

Cisco CP is a valuable productivity enhancing tool for network administrators and channel partners for deploying routers with increased confidence and ease. It offers a one-click router lockdown and an innovative voice and security auditing capability to check and recommend changes to router configuration. Cisco CP also monitors router status and troubleshoots WAN and VPN connectivity issues.

Cisco CP is free and you can download it from: [http://www.cisco.com/en/US/products/ps9422/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps9422/prod_release_notes_list.html).

Cisco Configuration Professional Express (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 and a factory default configuration file are installed in Flash memory on routers that are shipped with Cisco CP. You can connect a PC directly to the device, and then use Cisco CP Express to configure LAN and WAN connections, a firewall, Network Address Translation, and make security settings before you place the device on the network in which it will operate. See the [Initial Setup](#) section to learn how to do this.

## Initial Setup

Devices shipped with Cisco CP have a default configuration that allows you to connect a PC to an Ethernet port on the device and start configuration immediately. This initial configuration is accomplished using Cisco CP Express. You can use Cisco CP Express to give the device an IP address

on the network in which it will operate, and the other basic configurations mentioned in the previous section. After you have configured the device and connected it to the network, you will be able to use Cisco CP to connect to the device over the network and make advanced configurations.

If the device is not connected to the network yet and you want to use Cisco CP Express to give it an initial configuration, use the procedure in this section.

**Note**

If the device is already being used on your network, and you have installed Cisco CP on your PC, skip this procedure and read [Initial Setup for Deployed Devices](#).

**Step 1**

The device default configuration file configures an IP address for one Ethernet interface, and that may configure the device as a DHCP server. Determine whether the device is configured as a DHCP server, and which Ethernet port to connect the PC to by referring to the following table.

**Note**

If the router model you want to configure does not appear in the following table, see the *Release Notes for Cisco Configuration Professional* for updated information.

Device Model	DHCP Server	Connect PC to the Applicable Ethernet Port
Cisco 815, Cisco 86x, Cisco 88x, Cisco 180x, Cisco 1805, Cisco 1811, and Cisco 1812	Yes	ACT Lnk, ETHERNET 10 BASE T, LAN, PWR Lnk, or SWITCH
Cisco 1841, Cisco 1861, Cisco 2801, Cisco 2811	No	Fast Ethernet 0/0
Cisco 28xx, Cisco 38xx	No	Gigabit Ethernet 0/0
Cisco 19xx, Cisco 29xx, Cisco 39xx	No	Gigabit Ethernet 0/0

**Step 2** Connect the PC to the device appropriate port listed in the table.

**Step 3** Configure the PC IP address by doing one of the following:

- If the device is configured as a DHCP server, ensure that the PC is configured to accept an IP address from a DHCP server.
- If the device is not configured as a DHCP server, configure the static IP address 10.10.10.2 on the PC, and use the subnet mask 255.255.255.248.

**Step 4** Open an Internet Explorer browser window, and enter the IP address 10.10.10.1 to connect to the device and start Cisco CP Express.

**Step 5** Complete the Cisco CP Express wizard to configure the device.

When you have completed initial setup and given the device an IP address on your LAN, you can use Cisco CP to connect to the device and perform additional configuration.



## Initial Setup for Deployed Devices

If the device that you want to use Cisco CP to configure is already deployed, you should ensure that the device has a configuration that supports Cisco CP. The procedure in this section shows you how to add the required configuration statements.

**Note**

The tasks that follow can also be accomplished using the **Application > Setup New Device** option in Cisco CP by connecting the PC to the console port of the device. See the topic Device Wizard in the *Cisco Configuration Professional User Guide 2.5* at [http://www.cisco.com/en/US/products/ps9422/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps9422/products_user_guide_list.html) for more details.

**Step 1** Log on to the router through an Ethernet port.

**Step 2** When the router displays the user EXEC mode prompt, enter the **enable** command, and the enable password, if one is configured, as shown below:

```
Router> enable
password password
```

**Step 3** Enter config mode by entering the config terminal command, as shown in the following example.

```
Router> config terminal
Router(config)#
```

**Step 4** Using the command syntax shown, create a user account with privilege level 15.

```
Router(config)# username name privilege 15 secret 0 password
```

**Step 5** If no router interface is configured with an IP address, configure one so that you can access the router over the network. The following example shows the interface Fast Ethernet 0 configured.

```
Router(config)# int FastEthernet0
Router(config-if)# ip address 10.10.10.1 255.255.255.248
Router(config-if)# no shutdown
Router(config-if)# exit
```

If you are going to connect the PC directly to the router, the PC must be on the same subnet as this interface.

**Step 6** Configure the router as an http server for nonsecure communication, or as an https server for secure communication.

To configure the router as an http server, enter the **ip http server** command shown in the example:

```
Router(config)# ip http server
```

To configure the router as an https server, enter the **ip http secure-server** command shown in the example:

```
Router(config)# ip http secure-server
```

**Step 7** Configure the router for local authentication, by entering the **ip http authentication local** command, as shown in the example:

```
Router(config)# ip http authentication local
```

**Step 8** Configure the http timeout policy as shown in the example:

```
Router(config)# ip http timeout-policy idle 60 life 86400 requests 10000
```

- Step 9** Configure the vty lines for privilege level 15. For nonsecure access, enter the **transport input telnet** command. For secure access, enter the **transport input telnet ssh** command. An example of these commands follows:

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# exit
Router(config)# line vty 5 15
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport output telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# transport output telnet ssh
Router(config-line)# end
```

## Initial Setup for Switches

If the device that you want to use Cisco CP to configure is already deployed, you should ensure that the device has a configuration that supports Cisco CP. The procedure in this section shows you how to add the required configuration for the switch devices: CGS-2520-24TC and CGS-2520-16S-8PC.



### Note

The tasks that follow can also be accomplished using the **Application > Setup New Device** option in Cisco CP by connecting the PC to the console port of the device. See the topic Device Wizard in the *Cisco Configuration Professional User Guide 2.5* at [http://www.cisco.com/en/US/products/ps9422/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/ps9422/products_user_guide_list.html) for more details.

- Step 1** Log on to the switch through the Console port or through an Ethernet port.
- Step 2** When the switch displays the user EXEC mode prompt, enter the **enable** command, and the enable password, if one is configured, as shown below:
- ```
Switch> enable
password password
```
- Step 3** Enter config mode by entering the **config terminal** command, as shown in the following example.
- ```
Switch> config terminal
Switch(config)#
```
- Step 4** Using the command syntax shown, create a user account with privilege level 15.
- ```
Switch(config)# username name privilege 15 secret 0 password
```
- Step 5** If IP Address is not configured, configure one so that you can access the switch over the network. The following example shows the IP Address configured on interface Vlan1.
- ```
Switch(config)# interface Vlan1
Switch(config-if)# ip address 10.10.10.1 255.255.255.248
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

If you are going to connect the PC directly to the switch, the PC must be on the same subnet as this interface.

- Step 6** Configure the switch as an http server for nonsecure communication, or as an https server for secure communication.

To configure the switch as an http server, enter the **ip http server** command shown in the example:

```
Switch(config)# ip http server
```

To configure the switch as an https server, enter the **ip http secure-server** command shown in the example:

```
Switch(config)# ip http secure-server
```

- Step 7** Configure the switch for local authentication, by entering the **ip http authentication local** command, as shown in the example:

```
Switch(config)# ip http authentication local
```

- Step 8** Configure the http timeout policy as shown in the example:

```
Switch(config)# ip http timeout-policy idle 60 life 86400 requests 10000
```

- Step 9** Configure the vty lines for privilege level 15. For nonsecure access, enter the **transport input telnet** command. For secure access, enter the **transport input telnet ssh** command. An example of these commands follows:

```
Switch(config)# line vty 0 4
Switch(config-line)# privilege level 15
Switch(config-line)# login local
Switch(config-line)# transport input telnet
Switch(config-line)# transport output telnet
Switch(config-line)# transport input telnet ssh
Switch(config-line)# transport output telnet ssh
Switch(config-line)# exit
Switch(config)# line vty 5 15
Switch(config-line)# privilege level 15
Switch(config-line)# login local
Switch(config-line)# transport input telnet
Switch(config-line)# transport output telnet
Switch(config-line)# transport input telnet ssh
Switch(config-line)# transport output telnet ssh
Switch(config-line)# end
```

## Install Cisco CP

Install Cisco CP using the instructions in the Cisco Configuration Professional Quick Start Guide. This document is found on the Cisco CP CD. If you did not receive the CD, you can obtain this document from the following link:

[http://www.cisco.com/en/US/docs/net\\_mgmt/cisco\\_configuration\\_professional/guides/CiscoCPqsg.html](http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/guides/CiscoCPqsg.html)

After you have installed Cisco CP, you can create a community, and start configuring the devices in it.





## CHAPTER 2

# User Interface Features

---

This chapter helps you understand the Cisco Configuration Professional (Cisco CP) user interface. It contains the following sections:

- [Understanding the User Interface](#)
- [Online Help](#)

## Understanding the User Interface

Cisco CP eliminates the need for multiple device managers by providing a single tool to configure and manage devices.

The following sections describe the Cisco CP user interface:

- [Window Layout](#)
- [Menu Bar](#)
- [Toolbar](#)
- [Status Bar](#)

## Window Layout

The user interface makes it easy to manage networking features. These are the main parts that define the user interface:

- [Menu Bar](#)—The row of menus across the top of the window. It offers application services, a list of open windows, and online help.
- [Toolbar](#)—The row of icons directly below the menu bar. They represent the most often used application services and most often configured networking features.
- [Left Navigation Pane](#)—The scalable panel on the left side of the content pane in which you select the features to configure and monitor.
- [Content Pane](#)—The right side of the workspace, in which windows appear. You view reports here and enter information that configures networking features.
- [Status Bar](#)—The bar at the bottom of the window. Where Cisco CP displays the status of the application.

## Menu Bar

The row of menus across the top of the window that offers application services:








**Table 2-1**      *Menu Bar*

Menu	Options
Application	<p>Contains the following options:</p> <ul style="list-style-type: none"> <li>• <b>Manage Community</b>—Allows you to create a new community or choose an existing community. See <a href="#">Chapter 3, “Device Communities and Configuration Basics.”</a></li> <li>• <b>Create User Profile</b>—Allows you to restrict users from using all of the features that are available in the left navigation pane. See <a href="#">User Profile, page 2-4.</a></li> <li>• <b>Import User Profile</b>—Allows you to import a user profile. See <a href="#">User Profile, page 2-4.</a></li> <li>• <b>Options</b>—Allows you to set user preferences such as log level, show community at startup, and show CLI preview parameters. See <a href="#">Options, page 2-5.</a></li> <li>• <b>Template</b>—Allows you to create, edit, or apply a template. See <a href="#">Templates, page 2-5.</a></li> <li>• <b>Work Offline</b>—Allows you to work with Cisco Configuration Professional in offline mode. See <a href="#">Offline or Demo Mode, page 2-6.</a></li> <li>• <b>Exit</b>—Exits the Cisco Configuration Professional application.</li> </ul>
Help	<p>Contains the following options:</p> <ul style="list-style-type: none"> <li>• <b>Help Contents</b>—Displays the online help contents, which includes online help topics and links to screencasts.</li> <li>• <b>Feedback</b>—Displays a feedback form allowing you to provide feedback on Cisco Configuration Professional.</li> <li>• <b>About</b>—Displays information about Cisco Configuration Professional such as the version number and allows you to view the end-user licence agreement.</li> </ul>

# Toolbar

Cisco CP features are available from the toolbar at the top of the window. [Table 2-2](#) describes these tools.

**Table 2-2**      **Toolbar**

Tool Icon	Description
	Home button. Click this button to display the Community View page, which summarizes the community information and allows you to add, edit, discover devices, and to view the discovery and router status of each device.
	Configure button. Click this button to display the features that you can configure on a chosen device. The features are displayed in the left navigation pane. <b>Note</b> If a feature (router, security, or voice) is not supported on a device, that feature is not displayed in the left navigation pane. <b>Note</b> If the version of Cisco IOS that is installed on the device does not support a specific feature, but an upgrade does support it, then that feature is disabled (grayed out) in the left navigation pane.
	Monitor button. Click this button to display the router and security features that you can monitor for a chosen device. The features are displayed in the left navigation pane. <b>Note</b> If a feature (router or security) is not supported on a device, that feature is not displayed in the left navigation pane. <b>Note</b> If the version of Cisco IOS that is installed on the device does not support a specific feature, but an upgrade does support it, then that feature is disabled (grayed out) in the left navigation pane.
	Manage Community icon. Click this icon to open the Manage Community dialog box where you can add a new community or edit an existing community.
	Refresh icon. Click this button to: <ul style="list-style-type: none"> <li>Rediscover the selected device in the Select Community Member drop-down menu.</li> <li>Rediscover and reload the current feature.</li> </ul> <b>Note</b> Refresh is not available for offline mode. <b>Note</b> Refresh is available only after successful discovery of one or more devices. <b>Note</b> Clicking the Refresh button refreshes the device selected in the Select Community Member drop-down menu. Selecting a device in the <b>Home &gt; Dashboard</b> page and clicking Refresh does not refresh that device.
	Provide feedback to Cisco Systems icon. Click this icon to open the Cisco Configuration Professional Feedback form, which you can use to send feedback about this product to Cisco Systems.
	Help icon. Click this button to open the help page for the active window.



## Status Bar

The status bar displays Status information about Cisco CP and selected community members.



**Note** When you are in the **Home > Dashboard > Community View** page, the padlock icon in the status bar displays the connection mode of the device that is selected in the Select Community Member drop-down list.

**Table 2-3**      **Status Bar**

Feature Icon	Feature Name	Description
	Secure Connection	The locked padlock icon indicates that Cisco CP has a secure connection with the chosen community member.
	Nonsecure Connection	The unlocked padlock icon indicates that Cisco CP has a nonsecure connection with the chosen community member.

## Applications Menu Field Reference

- Manage Community, page 2-4
- User Profile, page 2-4
- Options, page 2-5
- Templates, page 2-5
- Offline or Demo Mode, page 2-6

## Manage Community

See Chapter 3, “Device Communities and Configuration Basics.”

## User Profile

For information about how to use Cisco Configuration Professional (Cisco CP) to create or import user profiles, see the screencast at:

[http://www.cisco.com/en/US/docs/net\\_mgmt/cisco\\_configuration\\_professional/srcrst/ccpsc.html](http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/srcrst/ccpsc.html).

You must have internet access to view the screencast.



## Options

Use the Options dialog box to set the user preferences such as log level, show community at startup, and show CLI preview parameters at run time.

### How to Get to This Dialog Box

From the menu bar, choose **Tools > Options**.

### Related Links

- [Menu Bar, page 2-2](#)

### Field Reference

**Table 2-4** Options Dialog Box

Element	Description
Log Level	<p>Choose the log level that you want displayed in the log file from the drop-down list. Options are:</p> <ul style="list-style-type: none"> <li>• <b>Error</b>—Choose the Error option to display only error messages in the log file. This option is selected by default.</li> <li>• <b>Debug</b>—Choose the Debug option to display error and debug messages in the log file. Use this option when you have experienced a problem with Cisco CP, and you want to send the log files to Cisco TAC for assistance.</li> </ul> <p>After you choose the Debug option, recreate the problem that you want to log, and then use the Collect Data for TAC Support utility to send the log files to Cisco TAC. For procedure, see <a href="#">Collecting Cisco CP Technical Support Logs, page 3-21</a>. After the problem is fixed, we recommend that you change the log level back to Error.</p>
Show Community at Startup check box	<p>By default the Show Community at Startup check box is checked. When this check box is checked, the Manage Community dialog box automatically displays when you start Cisco CP. See <a href="#">Manage Community Dialog Box, page 3-6</a>.</p> <p>Un-check the <b>Show Community at Startup</b> check box if you do not want Cisco CP to display the Manage Community dialog box on startup.</p>
Show CLI Previews check box	<p>By default the Show CLI Previews check box is checked. When this check box is checked, and you enter the parameters to configure a feature, the Deliver Configuration to Router dialog box opens displaying the CLI commands to be delivered to the router.</p> <p>Un-check the <b>Show CLI Previews</b> check box if you do not want Cisco CP to display the CLI commands in the Deliver Configuration to Router dialog box before configuring a feature.</p>

## Templates

For information about how to use Cisco Configuration Professional (Cisco CP) to configure Templates, see the screencast at:

[http://www.cisco.com/en/US/docs/net\\_mgmt/cisco\\_configuration\\_professional/srcst/ccpsc.html](http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/srcst/ccpsc.html).

You must have internet access to view the screencast.

## Offline or Demo Mode

Information about how to use Cisco Configuration Professional (Cisco CP) to configure the Offline or Demo mode feature, is provided in a screencast. [Table 2-5](#) provides information about the dummy devices used in the screencast. It lists the hostnames, the corresponding hardware, and the mode used in the screencast. See [Table 2-5](#) and then view the screencast at:

[http://www.cisco.com/en/US/docs/net\\_mgmt/cisco\\_configuration\\_professional/srcrst/ccpsc.html](http://www.cisco.com/en/US/docs/net_mgmt/cisco_configuration_professional/srcrst/ccpsc.html)



**Note** You must have internet access to view the screencast.

**Table 2-5** *Dummy Device Information*

Hostname	Hardware	Mode
CISCO-877M	NM-HDV2-1T1/E1	Security-Routing
CISCO-2821-2	WIC-2AM, WIC-2T, HWIC-CABLE-D-2, WIC-1DSU-T1-V2	Security-Routing
CISCO-2811-1	WIC-1B-S/T, VWIC-2MFT-T1-DI, WIC-1ADSL, AIM-IPS-K9	Security-Routing
CISCO-3845-1	HWIC-AP-G-J, WIC-1SHDSL, WIC-1DSU-T1, NM-CIDS-K9, AIM-VPN/HPII-PLUS	Security-Routing
CISCO-2851-2	HWIC-4A/S, HWIC-4SHDSL, HWIC-1T, HWIC-1ADSLI, NME-WAE-502-K9, AIM-VPN/EPII-PLUS	Security-Routing
CISCO-2811-2	FXS-DID, T1-E1	Gateway with SRST
CISCO-2821-3	Default interfaces, no modules	Gateway with SRST
CISCO-3845-2	NME-CUE, FXS-DID, FXS, FXO, DID, T1-PRI, PVDM-32	Cisco Unified Communications Manager Express
CISCO-2821-1	PVDM, VIC2-2FXS, NM-HDV2-1T1/E1	Cisco Unified Communications Manager Express
CISCO-2851-1	VIC2-2BRI-NT/TE	Voice Gateway
CISCO-3825-1	2BRI, CUE	Cisco Unified Communications Manager Express
C1861-SRST-FK9	1861, 4FXS, 4FXO, 8xPOE	Cisco Unified Communications Manager Express
CISCO-SRST-888	Default interfaces, no modules	Gateway with SRST
CISCO-891	8 FE switch ports, 1 FE layer 3, 1 GE layer 3, 1 async, 1 wireless AP, 1 wireless-GE	Security-Routing
C1861-UC-2BRI-K9	1861, BRI, 4FXS, CUE, 8xPOE	Cisco Unified Communications Manager Express
CISCO-3945	PVDM2-32, HWIC-AP-G-E, VIC2-2BRI-NT/TE, NM-HDV2-1T1/E1	Cisco Unified Communications Manger Express
CISCO-3925	PVDM3-64, VIC2-4FXO, NM-HDV2-1T1/E1, PVDM2-48	Cisco Unified Communications Manger Express
CISCO-3845	PVDM2-32, VIC2-2FXS, NM-CUE-EC	Cisco Unified Communications Manger Express
CISCO-3825	PVDM2-48, VWIC2-2MFT-, VIC2-4FXO, NM-16ESW	Gateway with Cisco Unified SRST

**Table 2-5** *Dummy Device Information (continued)*

Hostname	Hardware	Mode
CISCO-2951/K9	PVDM2-64, VIC-4FXS/DID=, HWIC-2FE, WIC-1AM-V2, NME-IPS-K9	Cisco Unified Communications Manger Express
CISCO-2921-1	Default interface	Cisco Unified Communications Manger Express
CISCO-2911/K9	PVDM2-64, VIC2-4FXO, VIC3-4FXS/DID	Cisco Unified Communications Manger Express
CISCO-2901/K9	Default Interface	Cisco Unified Communications Manger Express
CISCO-2851	VIC2-2BRI-NT/TE, NME-APPRE-502-K9	Cisco Unified Communications Manger Express
CISCO-2821	HWIC-3G-CDMA-S, HWIC-3G-GSM, HWIC-3G-CDMA-V, EVM-HD-8FXS/DID, EM-4BRI-NT/TE, EM-HDA-6FXO	Cisco Unified Communications Manger Express
CISCO-2811	HWIC-4SHDSL, NM-HDV2-2T1/E1, PVDM2-48, AIM-CUE,	Gateway with Cisco Unified CME as SRST
CISCO-2801	AIM-VPN/EPII-PLUS, AIM-VPN/SSL-2	Security-Routing
CISCO-1941	EHWIC-D-8ESG	Security-Routing
CISCO-1861-W	PVDM2-32, VIC3-4FXS/DID, VIC2-4FXO	Cisco Unified Communications Manger Express
CISCO-1841	WIC-1SHDSL-V3	Security-Routing
CISCO876W-G-E-K9	No modules	Security Routing
CISCO1811W-AG-A/K9	2FE, Dual Band 802.11 A+B/G Radio Access Point	Security Routing
CISCO1805-D	HWIC-CABLE-E/J-2, HWIC-4ESW	Security Routing
CISCO1841	WIC-1SHDSL-V3, HWIC-16A	Security Routing
CISCO2801	AIM-VPN/EPII-PLUS, AIM-VPN/SSL-2	Security Routing
CISCO1801-M/K9	1FE ADSLoPOTS	Security Routing
CISCO877W-G-A-M-K9	No modules	Security Routing
CISCO887G-K9	No modules	Security Routing
CISCO1802/K9	1FE ADSLoISDN, ILPM-8, Dual Band 802.11 A+B/G Radio Access Point	Security Routing
CISCO1941	EHWIC-D-8ESG	Security Routing
CISCO2801	AIM-VPN/EPII-PLUS, AIM-VPN/SSL-2	Security Routing
CISCO1812/K9	No modules	Security Routing

**Note**

When a discovered device is moved to offline mode, Cisco CP sends the CLIs needed for identifying all the supported features in the device. Cisco CP sends the CLI irrespective of whether the feature is already configured on the device or not.

# Online Help

Cisco Configuration Professional provides comprehensive online help. Help gives you background information on networking features procedures for performing configuration tasks, and descriptions of each configuration screen. Some of the features have screencasts instead of online help. The links to these sceencasts are provided in the online help.



## CHAPTER 3

# Device Communities and Configuration Basics

---

Before you can configure devices using Cisco Configuration Professional (Cisco CP) you must enter the IP address or hostname, and the credentials information of the devices that you want to manage. To do this, you must first create a community, and then add devices to that community.

The following sections provide more information:

- [Basic Workflow, page 3-1](#)
- [Understanding Device Communities, page 3-1](#)
- [Creating a Community and Adding Devices, page 3-2](#)
- [Managing the Devices in a Community, page 3-4](#)
- [Discovering Devices, page 3-5](#)
- [Device Community Reference, page 3-6](#)
- [Configuration Basics, page 3-10](#)
- [Supplementary Information, page 3-15](#)

## Basic Workflow

1. Create a community.
2. Add devices to that community.
3. Discover the devices in the community.
4. Configure the devices.

## Understanding Device Communities

Before you begin using Cisco CP, you must first create a community and then add devices to that community. When you start Cisco CP for the first time, Cisco CP automatically creates a community for you, to which you can add devices.

A community is basically a group of devices (community members). A single community can contain a maximum of ten devices. You can create a community and then add the devices to it based on some common parameters. For example, you can create communities based on the location of the devices. You can create a San Jose community and add devices to it, then you can create a Bangalore community and add devices to it, and so on.

When you add a device to a community, you must specify its IP address or hostname, credential information (username and password), and other optional parameters. Cisco CP uses this information to discover the device. After you discover the device, you can configure and monitor it.

You can create and manage communities from the Manage Community dialog box. This dialog box automatically displays when you start Cisco CP. From the Manage Community dialog box, you can create communities, change the community name, delete a community, add devices to a community, export and import community information, and discover all the devices in a community.

**Note**

If you switch between communities, the status of the devices in the community from which you switched, changes to Not Discovered. To configure devices in that community, you must discover the devices again.

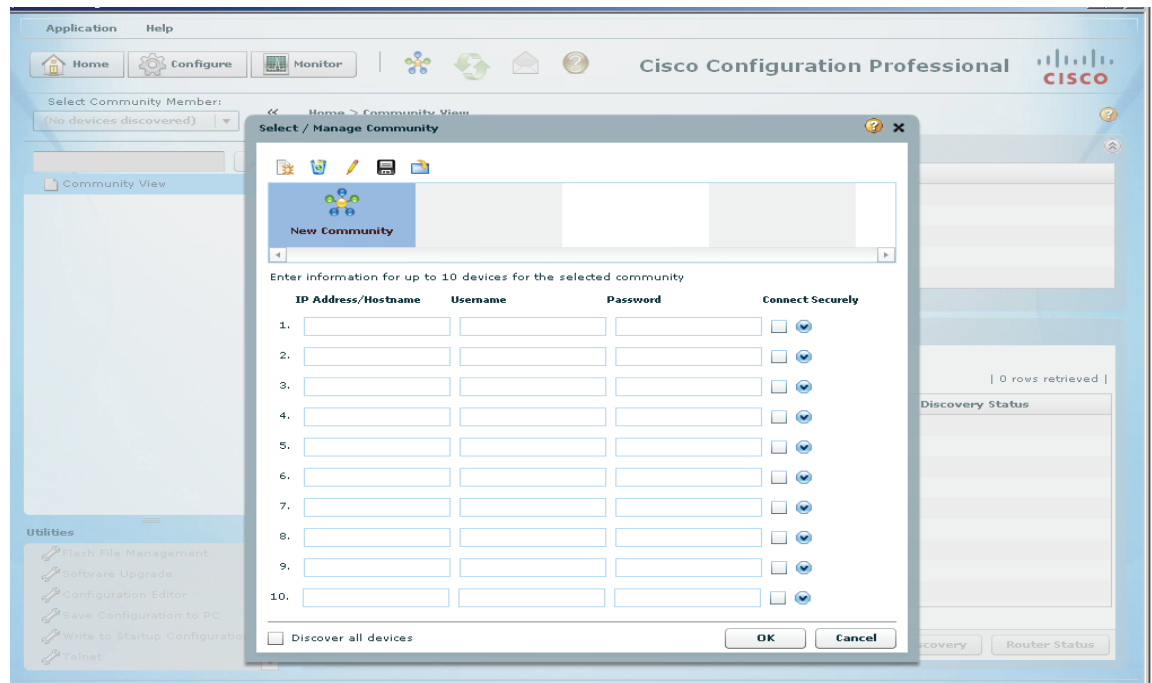
## Creating a Community and Adding Devices

### Procedure

Use this procedure to create a community, add devices to it, and discover all the devices in a community.

- Step 1** Use the Manage Community dialog box to create communities. The Manage Community dialog box automatically displays when you start Cisco CP and a community called, New Community, is created by default. See [Figure 3-1](#).

**Figure 3-1** Manage Community

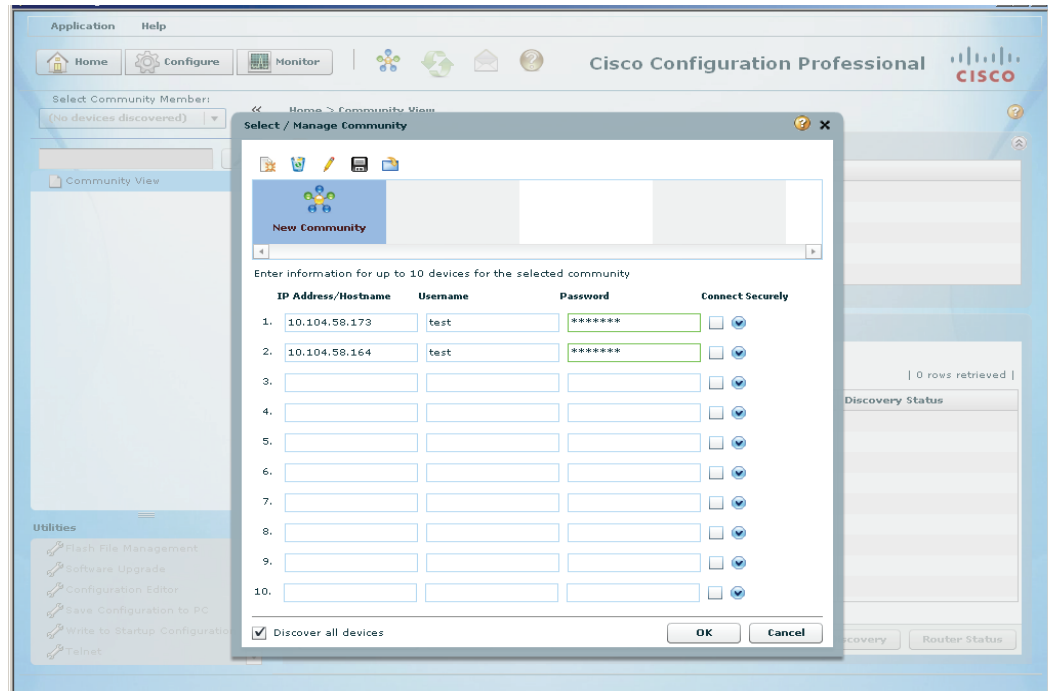


You can also open the Manage Community dialog box in the following ways:

- From the toolbar, click the **Manage Community** icon.
- From the menu bar, choose **Application > Manage Community**.

- Step 2** In the Manage Community dialog box, enter the IP address or hostname; and the username and password information for the devices that you want to configure. See example in [Figure 3-2](#).

**Figure 3-2** Manage Community With IP Address and Credentials



If you enter the default username **cisco** and default password **cisco**, the Change Default Credentials dialog box opens. For security reasons, you must change the default credentials to new credentials.

- Step 3** If you want Cisco CP to connect securely with the device, check the **Connect Securely** check box.

When you check the **Connect Securely** check box, HTTPS port 443 and SSH port 22 information is automatically added to the device. To view the port information, click the down-arrow next to the Connect Securely check box.

If you did not check the Connect Securely check box, the HTTP port 80 and Telnet port 23 information is automatically added to the device. To view the port information, click the down-arrow next to the Connect Securely check box.

- Step 4** If you want to change the default port information, click it, and then enter a new port value.

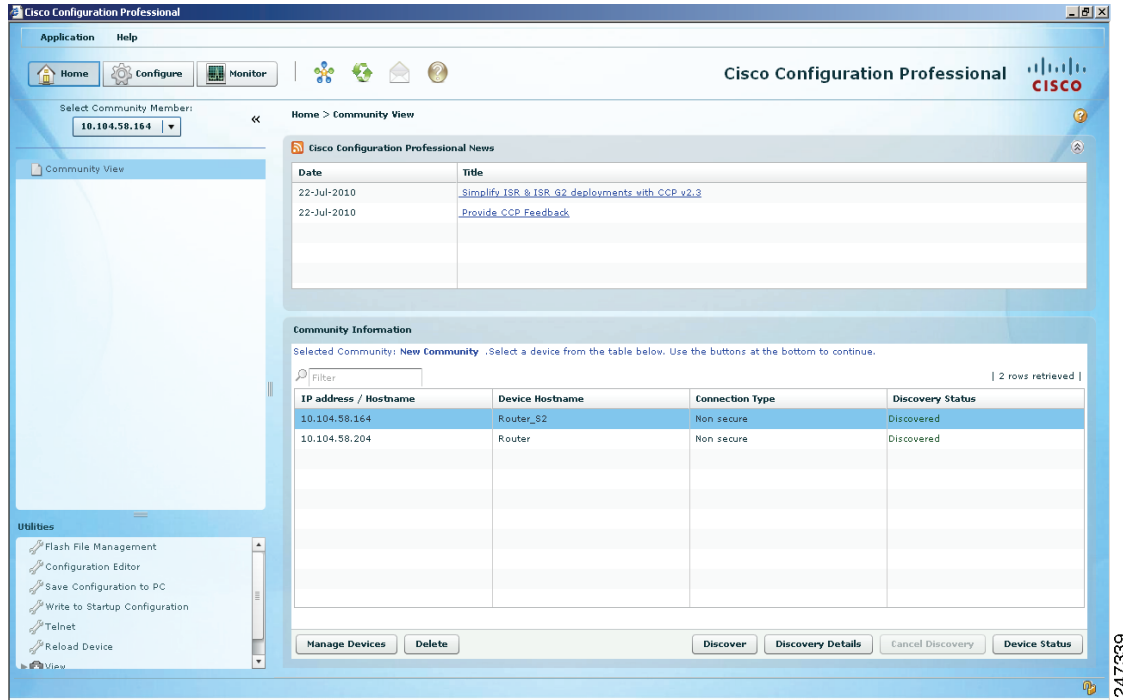


**Note** Make sure that Cisco CP can access the device at the specified secure or non-secure ports.

- Step 5** If you want Cisco CP to discover all the devices in a community, check the **Discover All Devices** check box. If you want, you can choose to discover the devices later, from the Community View page.

- Step 6** Click **OK**. The Community View page opens. It displays the information about the devices in the community. See [Figure 3-3](#).

**Figure 3-3** Community View



### Related Topics

- [Basic Workflow, page 3-1](#)
- [Understanding Device Communities, page 3-1](#)
- [Manage Community Dialog Box, page 3-6](#)
- [Community View Page, page 3-8](#)
- [Managing the Devices in a Community, page 3-4](#)

## Managing the Devices in a Community

After you create a community and add devices to it, you can view the information for that community in the Community View page (see [Figure 3-3](#)). From the Community View page, you can manage the devices (community members) in a community, such as add devices to a selected community, edit device information, delete devices, discover the devices, view information about the discovery process, and view hardware and software information about a selected device. See [Community View Page, page 3-8](#).

For details, see the *Cisco Configuration Professional User Guide*.



# Discovering Devices

In order to configure a device, you must choose the community the device belongs to, choose the device, and then discover it. Cisco CP uses the IP address or hostname, and the credential information that you specified to discover the device.

You can discover the devices in a community from the Manage Community dialog box or the Manage Devices dialog box; or you can discover the devices from the Community View page.

To discover all the devices from the Manage Community dialog box or the Manage Devices dialog box, click the **Discover All Devices** check box. All of the devices in the displayed community are discovered.

To discover specific or all of the devices in a community from the Community View page, use the procedure in this section.

## Before You Begin

Make sure that you have created a community and added devices to it.

## Procedure

Use this procedure to discover devices in a community from the Community View page.

- 
- Step 1** From the menu bar, choose **Application > Manage Community**. The Manage Community dialog box opens.
- Step 2** From the Manage Community dialog box, choose the community name in which the device you want to discover resides, and then click **OK**. The Community View page opens. See [Community View Page, page 3-8](#).
- Step 3** Do one of the following:
- To discover a particular device, select the row, then click **Discover**. A confirmation dialog box opens informing that the discovery process can take up to three minutes.
  - To discover all the devices, press the shift button on your keyboard and then select multiple rows. Click **Discover**. A confirmation dialog box opens informing that the discovery process can take up to three minutes.
- Step 4** Click **Yes** in the confirmation dialog box to continue with the discovery.
- After the discovery is complete, the discovery status information is displayed in the Discover Status column. You will see one of the following:
- Discovered—The device has been discovered and is available.
  - Discovering—Cisco CP is in the process of discovering the device.
  - Discovery failed—Cisco CP could not discover the device. See [Understanding Discovery Failed Error Messages, page 3-18](#) to determine the problem and fix it.
  - Discovery scheduled—Cisco CP has queued the discovery of the device.
  - Discovered with errors—The device has been discovered, but errors were generated during the discovery process. See [Using Cisco Configuration Professional to Run show tech-support, page 3-21](#).
  - Discovered with warnings—The device has been discovered, but some information about the device was not available. To see what warnings are given, select the row for the device and click **Discovery Details**.
  - Not Discovered—No attempt has been made to discover the device.

**Step 5** To view details about the discovery process, click **Discovery Details**.

#### Related Topics

- [Using Cisco Configuration Professional to Run show tech-support, page 3-21](#)

## Device Community Reference

The following topics describe the Device Community pages and dialog boxes used to configure device communities:

- [Manage Community Dialog Box, page 3-6](#)
- [Community View Page, page 3-8](#)

## Manage Community Dialog Box

Use the Manage Community dialog box to create a community, add devices to it, and discover all of the devices in a community.

#### How to Get to This Dialog Box

From the menu bar, choose **Application > Manage Community**.

#### Related Topics

- [Understanding Device Communities, page 3-1](#)
- [Creating a Community and Adding Devices, page 3-2](#)
- [Community View Page, page 3-8](#)
- [Community View Page, page 3-8](#)

#### Field Reference

**Table 3-1** *Manage Community Dialog Box*






Element	Description
	Add icon. Click this icon to add a new community.
	Delete icon. Click this icon to delete a selected community.
	Edit icon. Click this icon to edit the name of a selected community.

Table 3-1 Manage Community Dialog Box (continued)

Element	Description
	Export icon. Click this icon to save the community information from Cisco CP to a file on your PC.
	Import icon. Click this icon to import the community information from a file on your PC into Cisco CP. After the file is imported, Cisco CP displays the community with all its community members (devices) in the Manage Community dialog box.
IP Address/Hostname	The IP address or hostname of the device.
Username	<p>The username used to log into the router.</p> <p>If you enter the default username <b>cisco</b> and default password <b>cisco</b>, the Change Default Credentials dialog box opens. For security reasons, you must change the default credentials to new credentials.</p> <p>Cisco CP uses the new credentials that you provide to create an administrative user with a privilege level of 15. If the credentials that you enter were already configured, Cisco CP overwrites them, and gives them a privilege level of 15 when it discovers the device. If you do not want an existing user account overwritten for any reason, do not use its credentials to replace the default credentials.</p>
Password	Enter the password associated with the username that you entered.
Connect Securely check box	<p>Click this check box if you want Cisco CP to connect securely with the device.</p> <p>When you check the <b>Connect Securely</b> check box, HTTPS port 443 and SSH port 22 information is automatically added to the device.</p> <p>If you did not check the Connect Securely check box, the HTTP port 80 and Telnet port 23 information is automatically added to the device.</p>
Down arrow	<p>Click the down-arrow to view the port information that Cisco CP uses to connect to the device:</p> <ul style="list-style-type: none"> <li>• HTTP—80</li> <li>• Telnet—23</li> <li>• HTTPS—443</li> <li>• SSH—22</li> </ul> <p>You can change the default port information. Click it and then enter a new port value.</p> <p><b>Note</b> Make sure that Cisco CP can access the device at the specified secure or non-secure ports.</p>
Discover All Devices check box	Click this check box to discover all the devices in the displayed community.
OK button	Click this button to save the changes and add the community and device information to Cisco CP. When you click this button, the Community View page opens where you can view the community information. See <a href="#">Community View Page, page 3-8</a> .
Cancel button	Click this button if you do not want to save the changes that you entered.

## Community View Page

The Community View page summarizes the community information and allows you to add, edit, discover devices, and to view the discovery and router status of each device.

### How to Get to This Page

From the menu bar, choose **Application > Manage Community > Community Name > OK**.

### Related Links

- [Managing the Devices in a Community](#)
- [Configuration Basics](#)
- [Using Cisco Configuration Professional to Run show tech-support](#)

### Field Reference

**Table 3-2** Community View Page

Element	Description
<b>Cisco Configuration Professional News—Upper Pane</b>	
Date	Date the Cisco CP news was published.
Title	Links to important information about Cisco CP. The updated information is provided through RSS feeds. <b>Note</b> To view the Cisco CP news, you must have access to the Internet.
<b>Community Information—Lower Pane</b> (Displays the name of the community and summarizes the information about all the devices in the community.)	
Filter	To display only entries that contain specified text, enter the text in the Filter box. The display is updated each time you enter a character.
IP Address/Hostname	The IP address or hostname of the community member.
Router Hostname	The hostname associated with the IP address.
Connection Type	Displays one of the following: <ul style="list-style-type: none"> <li>• Non secure—The device has not been discovered, or has been discovered without using a secure protocol.</li> <li>• Secure—The device has been discovered, using a secure protocol. To ensure that the device is discovered using a secure protocol, check the Connect Securely check box in the Manage Community dialog box or the Manage Devices dialog box.</li> </ul>

Table 3-2 Community View Page (continued)

Element	Description
Discovery Status	<p>This column contains one of the following values:</p> <ul style="list-style-type: none"> <li>• Discovered—The device has been discovered and is available.</li> <li>• Discovering—Cisco CP is in the process of discovering the device.</li> <li>• Discovery failed—Cisco CP could not discover the device. See <a href="#">Using Cisco Configuration Professional to Run show tech-support</a> to determine the problem and fix it.</li> <li>• Discovery scheduled—Cisco CP has queued the discovery of the device.</li> <li>• Discovered with errors—The device has been discovered, but errors were generated during the discovery process. See <a href="#">Understanding Discovery Failed Error Messages</a>. Use the procedure in <a href="#">Collecting Cisco CP Technical Support Logs</a> to collect technical support information and send it to Cisco for analysis.</li> <li>• Discovered with warnings—The device has been discovered, but some information about the device was not available. To see what warnings are given, select the row for the device and click <b>Discovery Details</b>.</li> <li>• Not Discovered—No attempt has been made to discover the device.</li> </ul>
<b>Buttons</b>	
Manage Devices	Click the <b>Manage Devices</b> button to open the Manage Devices dialog box where you can add new devices or edit information of a specific device.
Delete	To remove a member from the community, choose the community member entry, and then click <b>Delete</b> .
Discover	To discover one or more community members, select the entry for each member that you want to discover, and then click <b>Discover</b> .
Discovery Details	To display details about the discovery of the device, select the entry for the member, and then click <b>Discovery Details</b> .
Cancel Discovery	To cancel the discovery of a device, select the row of the device being discovered, and then click <b>Cancel Discovery</b> .
Router Status	To display hardware, software, and feature details about a community member, select the entry for the member, and then click <b>Router Status</b> .

# Configuration Basics

This section illustrates configuration basics by guiding you through interface configuration screens.

To familiarize yourself with configuration basics, complete these steps:

- Step 1** Click **Configure > Interface Management > Interfaces and Connections**, and then click the **Edit Interface/Connection** tab. Cisco CP displays the configured connections (Figure 3-4). These may be connections you configured using Cisco CP Express or the Cisco IOS CLI.

**Figure 3-4** Edit Interfaces/Connections

The screenshot shows the Cisco Configuration Professional interface. The main window displays the 'Interfaces and Connections' configuration screen. The interface table is as follows:

Interface	IP	Type	Slot	Status	Description
GigabitEthernet0/0	14.15.11.1	GigabitEthernet	0	Up	
GigabitEthernet0/1	10.77.165.217	GigabitEthernet	0	Up	
Serial0/1/0	no IP address	Serial Sync/Async	0	Down	
Serial0/1/1	no IP address	Serial Sync/Async	0	Down	
Serial0/1/2	no IP address	Serial Sync/Async	0	Down	
Serial0/1/3	no IP address	Serial Sync/Async	0	Down	
Async0/2/0	no IP address	Async	0	Up	
Async0/2/1	no IP address	Async	0	Up	
Async0/2/2	no IP address	Async	0	Up	
Async0/2/3	no IP address	Async	0	Up	
Async0/2/4	no IP address	Async	0	Up	
Async0/2/5	no IP address	Async	0	Up	
Async0/2/6	no IP address	Async	0	Up	
Async0/2/7	no IP address	Async	0	Up	
ATM0/3/0	no IP address	ADSL	0	Down	

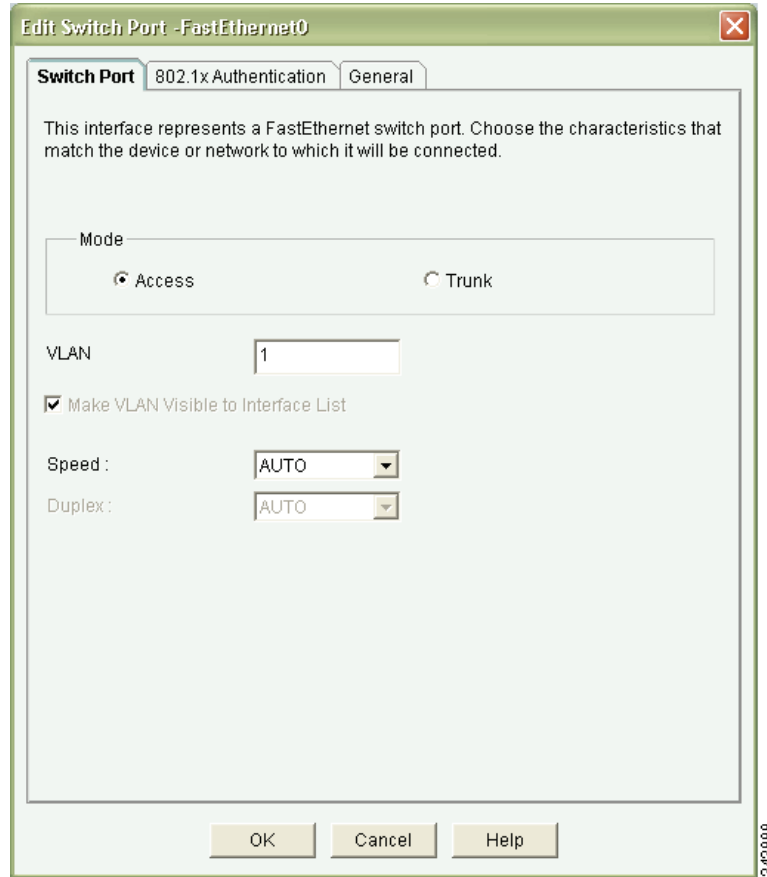
Below the table, there is a 'Details about Interface: GigabitEthernet0/0' section with the following configuration:

Item Name	Item Value
IP address/subnet mask	14.15.11.1/255.255.255.0
NAT	<None>
Access Rule - inbound	<None>
Access Rule - outbound	<None>
IPSec Policy	SDM_CMAP_1
Inspect Rule - inbound	<None>
Inspect Rule - outbound	<None>
Easy VPN Remote	<None>
QoS policy - outbound	<None>
QoS Policy - inbound	<None>

247657

- Step 2** To display a configuration dialog, choose a connection, and click **Edit**. Figure 3-5 displays the configuration dialog that enables you to edit a connection.

**Figure 3-5** Connection Dialog

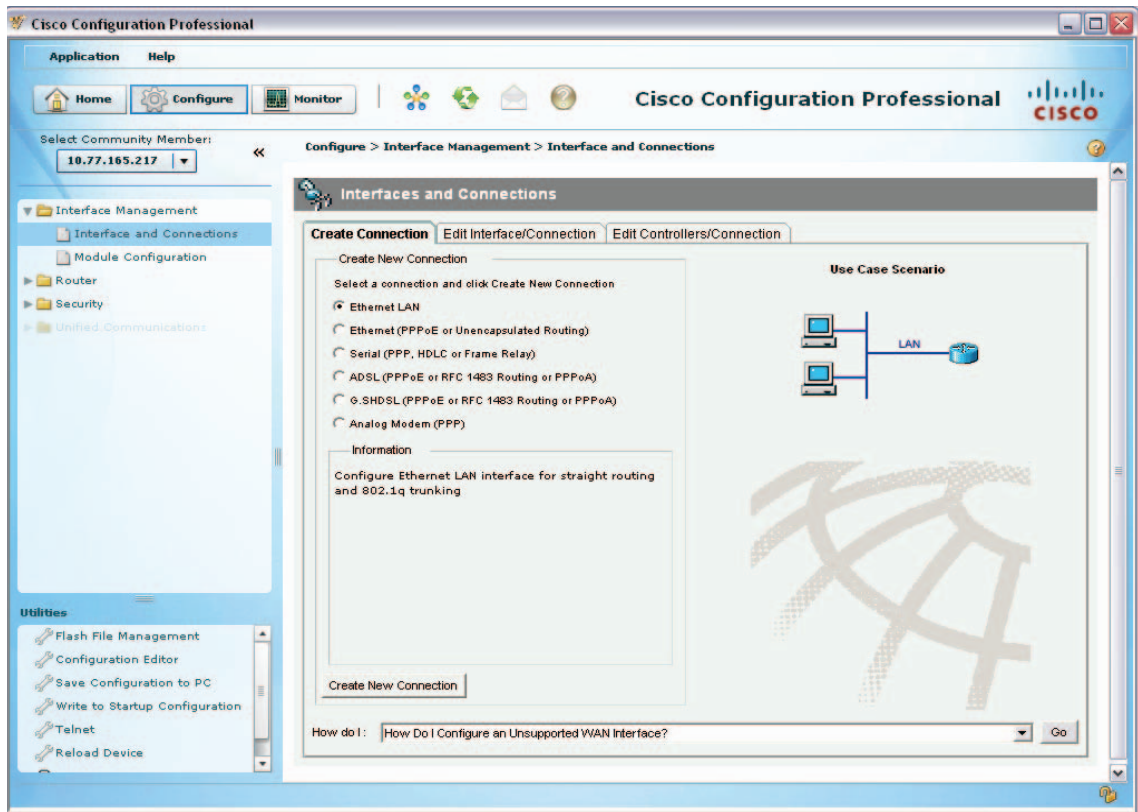


Click the other tabs in the dialog to see the other options that are available for the connection that you chose.

- Step 3** To close this dialog, click **Cancel**.

- Step 4** To see how to create a new connection, click the **Create Connection** tab. The create connection tab (Figure 3-6) enables you to choose the type of connection to create and launch a wizard that enables you to create it.

**Figure 3-6** Create Connection Tab

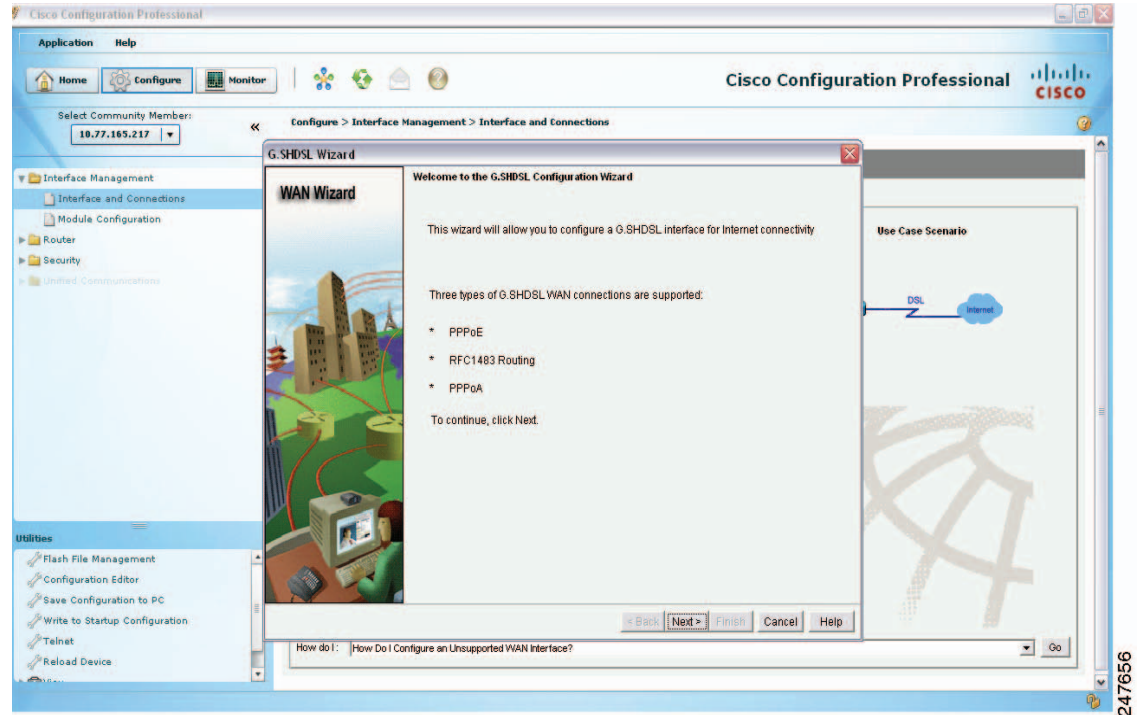


247659



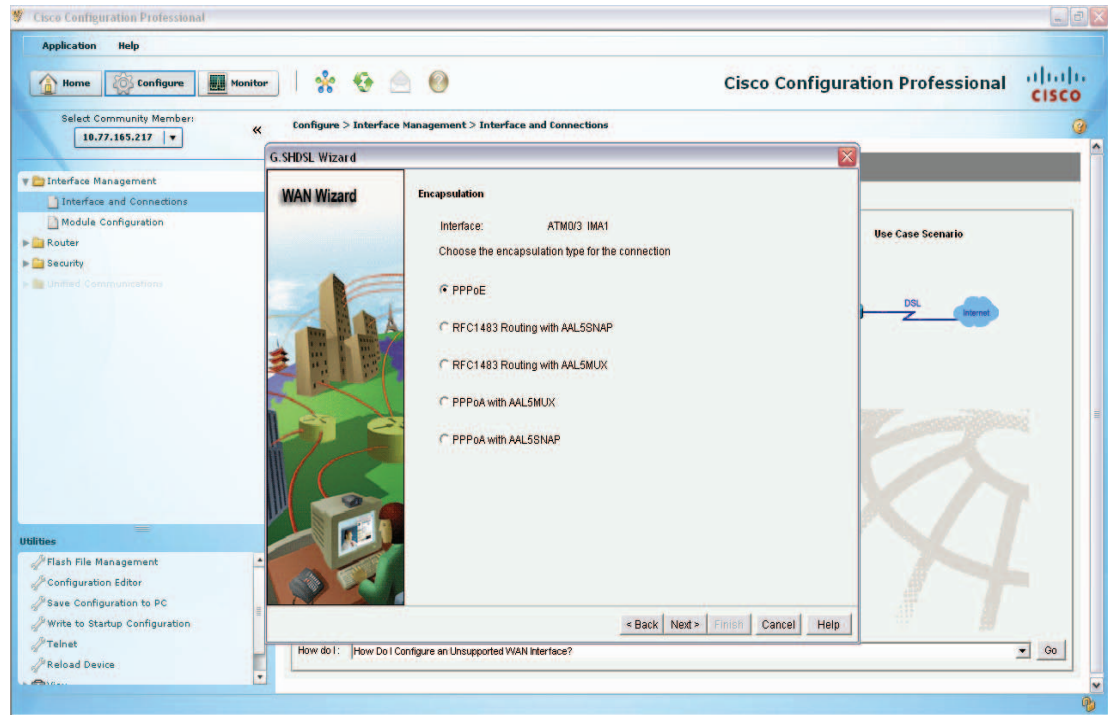
- Step 5** To launch a wizard, choose a connection type, and click **Create Connection**. Figure 3-7 shows the ADSL Connection wizard Welcome screen.

**Figure 3-7** ADSL Connection Wizard Welcome Screen



**Step 6** To begin configuration using the wizard, click **Next**. Figure 3-8 shows the ADSL Encapsulation screen, which allows you to choose the type of encapsulation to use.

**Figure 3-8** ADSL Encapsulation Screen

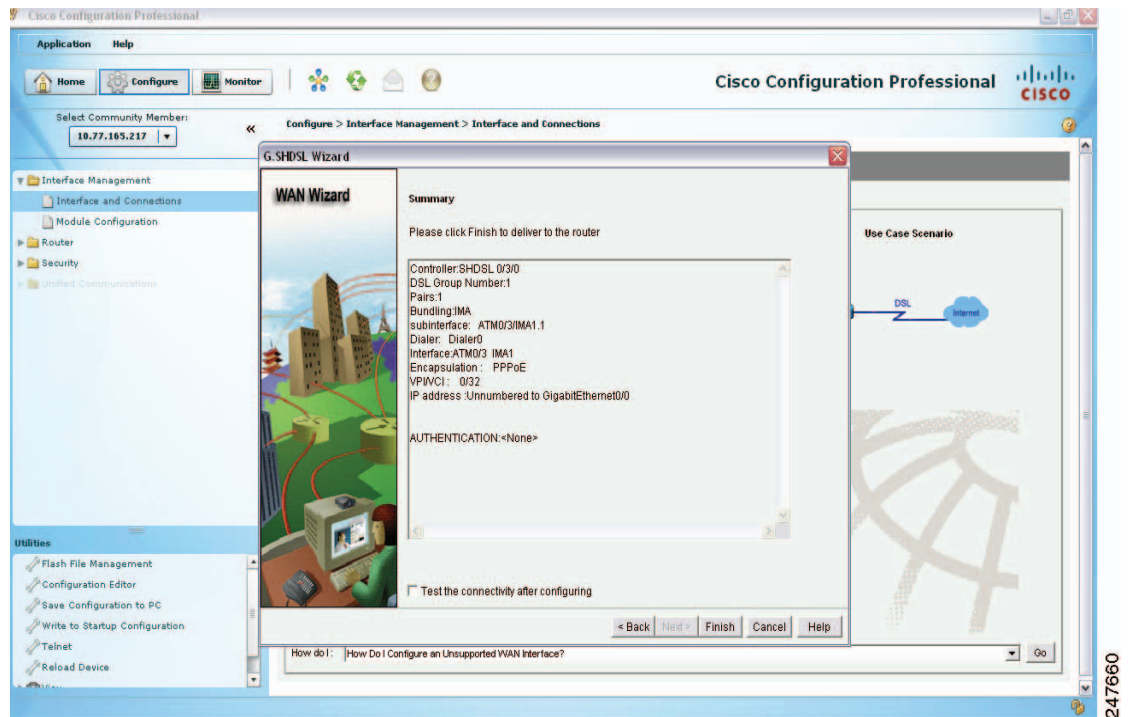


**Step 7** Choose or enter the values that the screen prompts you.

247658

- Step 8** To complete the wizard, use the Next button to move to subsequent screens and complete them. When you have entered all required values, the wizard displays the summary screen. This screen displays the values that you have entered. [Figure 3-9](#) shows the ADSL Connection Summary screen.

**Figure 3-9** ADSL Connection Summary Screen



- Step 9** Review the information. If you want to change anything, click **Back** to return to the screen in which you need to make changes, make them, and then return to the Summary screen.
- Step 10** Click **Finish** to deliver the changes to the device.

Now that you have reviewed, and perhaps performed, this procedure, you have an idea of how to configure devices using Cisco CP.

When using Cisco CP, you can click the help button at any time to get more information about the screen in which you are working.

## Supplementary Information

This section contains information that may help you use Cisco CP. It contains the following sections:

- [Using Cisco Configuration Professional to Run show tech-support](#)
- [Collecting Cisco CP Technical Support Logs](#)
- [Using Cisco Configuration Professional to Run show tech-support](#)

## Things to Know About Discovering Devices

This section gives you information to refer to if you are unable to discover a device. It contains the following sections:

- [Cisco CP Configuration Requirements](#)
- [Wrong Secure Shell Version May Cause Discovery to Fail](#)
- [Understanding Discovery Failed Error Messages](#)
- [Cisco CP May Overwrite Existing Credentials](#)
- [Proxy Server Settings Might Cause Discovery to Fail](#)
- [Setting the Java Heap Size Value to -Xmx256m](#)

### Cisco CP Configuration Requirements

Proper router configuration is required for discovery to succeed. Check the following configuration items for problems:

- Supported device—The device you are attempting to discover must be a device that Cisco CP supports. Refer to the *Release Notes for Cisco Configuration Professional* document, whose link is provided at the end of this help topic.
- Correct username and password—You must use a username and password configured on the device.
- Correct privilege level—The privilege level for the user account entered in the Add Community Member or Edit Community Member screen must be level 15.
- Cisco CP View—Cisco CP allows you to associate user accounts with CLI views, which restrict the associated user to specified actions within Cisco CP. If a user with a CLI view configured using Cisco Router and Security Device Manager (SDM) attempts to discover a device, discovery will fail. To remove an SDM CLI view from a user account and replace it with a Cisco CP CLI view, click **Router > Router Access > User Accounts/View**. Then, choose the user account to update, and click **Edit**. In the displayed dialog, choose a Cisco CP CLI view.
- Minimum Java Runtime Environment version—JRE versions minimum 1.5.0\_11 upto 1.6.0\_17 are supported.
- Correct Java heap size value—The correct Java heap size value is -Xmx256m. See “[Setting the Java Heap Size Value to -Xmx256m](#)” to learn how to set the Java heap size value.
- vty lines—A vty line must be available for each session Cisco CP establishes with the device. At least one vty line must be available for Cisco CP to connect to the device. If you use CP to launch additional applications on the device, a vty line must be available for each additional session. If a Cisco Unity Express Advanced Integration Module (AIM) is present in the device, 2 vty lines must be available to connect to the AIM.
- Transport input for vty lines—The vty transport input must be set to ssh for secure connections and to telnet for nonsecure connections.
- Security settings—The following security settings must be in place:
  - ip http server—for nonsecure access
  - ip http secure-server—for secure access
  - ip http authentication local
- Protocol and encryption settings—Verify that other settings, such as firewall, Network Access Control, and other features designed to limit access to the network are not preventing discovery.

Cisco CP configuration requirements are provided in the *Release Notes for Cisco Configuration Professional*. Additionally, the default configuration file shipped on routers ordered with Cisco CP provides a basic configuration that allows discovery to succeed.

To obtain the release notes, go to the following link:

[http://www.cisco.com/en/US/products/ps9422/prod\\_release\\_notes\\_list.html](http://www.cisco.com/en/US/products/ps9422/prod_release_notes_list.html)

In the Support box, click **General Information > Release Notes**. Find the latest release notes on the Release Notes page.

## Wrong Secure Shell Version May Cause Discovery to Fail

If the device that you are trying to discover is not using Secure Shell (SSH) version 2.0 or higher, discovery may fail, and you must update the version in order to eliminate this problem. To determine which SSH version the device is using and, if necessary, update the version and regenerate an RSA key, complete these steps:

- Step 1** Determine which SSH version the device is using, by entering the **show ip ssh** EXEC mode command. An example command entry and output follows:

```
c3845-1(config)# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
c3845-1(config)#
```



**Note** If the version shown is 1.99, there is no need to update the SSH version to 2.0.

- Step 2** To update SSH to version 2, enter the Exec mode **ip ssh version 2** command, as shown in the following example:

```
c3845-1(config)# ip ssh version 2
```

- Step 3** To generate a new RSA key, enter the Global configuration mode **crypto key generate rsa** command, as shown in the following example:

```
c3845-1(config)# crypto key generate rsa
The name for the keys will be name.domain.com
Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose
Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 768
% Generating 768 bit RSA keys, keys will be non-exportable...[OK]
c3845-1(config)# end
c3845-1# wr
```

When you complete this procedure, the configuration change is made in the running configuration, and stored to the startup configuration, and the SSH version is eliminated as a reason for discovery not succeeding.

## Understanding Discovery Failed Error Messages

Table 3-3 provides the discovery failed error messages and the conditions under which you might see them.

**Table 3-3** Discovery Failed Error Messages

Error Message	Condition
The username or password is incorrect.	<p>This error message is displayed in one of the following conditions:</p> <ul style="list-style-type: none"> <li>The username is wrong.</li> <li>The password is wrong.</li> <li>The CLI “ip http authentication local” is missing in the configuration.</li> </ul> <p>To configure local authentication for http server users, enter the following commands on the device:</p> <pre>Router&gt; <b>config terminal</b> Router(config)# <b>ip http authentication local</b></pre>
Discovery could not be completed because the security certificate was rejected.	<p>This error message is displayed when:</p> <ul style="list-style-type: none"> <li>Cisco CP connects to the device securely, but because you did not accept the security certificate, Cisco CP is unable to start discovery.</li> <li>You are not prompted to accept the security certificate at all. In this case, perform the following steps: <ol style="list-style-type: none"> <li>Clear the crypto keys using the command: <pre>Router (config)# <b>crypto key zeroize</b></pre> </li> <li>Delete the trustpoint using the CLI. For example: <pre>Router(config)# <b>no crypto pki trustpoint TP-self-signed-3248306557</b> % Removing an enrolled trustpoint will destroy all certificates received from the related Certificate Authority. Are you sure you want to do this? [yes/no]: <b>yes</b> % Be sure to ask the CA administrator to revoke your certificates. Router(config)#</pre> </li> <li>Access the router through a browser using the URL: <pre>https://&lt;ip address of the router&gt;</pre> </li> <li>Click on option 2: <p>Continue to this website (not recommended).</p> </li> <li>Launch Cisco CP and discover the device in Secure mode.</li> </ol> </li> </ul> <p>The security certificate has to be accepted within the HTTP idle timeout specified. The default value for the idle timeout is 180 seconds. For example, If the idle timeout is set to 30 seconds, you have to accept the certificate within that time. The idle timeout on the router is configured as:</p> <pre>Router(config)# <b>ip http timeout-policy idle 30</b></pre>

Table 3-3 Discovery Failed Error Messages

Error Message	Condition
	<p>If you accept the certificate after the configured time, discovery fails. However, rediscovery is successful.</p> <ul style="list-style-type: none"> <li>The router does not have SSH configured. To configure SSH: Router (config)# <b>crypto key generate rsa modulus 1024</b></li> </ul>
<p>Connection to the device could not be established. Either the device is not reachable or the HTTP service is not enabled on the device.</p>	<p>This error message is displayed in one of the following conditions:</p> <ul style="list-style-type: none"> <li>The internet connection is down.</li> <li>The IP address of the device is wrong or the device is not reachable.</li> <li>The CLI “ip route &lt;x.x.x.x&gt; &lt;x.x.x.x&gt; &lt;x.x.x.x&gt;” is missing in the configuration.</li> <li>The wrong HTTP port is provided to Cisco CP to connect to the device.</li> <li>The CLI “ip http server” is missing in the configuration for non-secure connection.</li> <li>The CLI “ip http secure-server” is missing in the configuration for secure connection.</li> </ul> <p>To configure the device as an HTTP or HTTPS server, enter the following commands:</p> <pre>Router&gt; <b>config terminal</b> Router(config)# <b>ip http server</b> Router(config)# <b>ip http secure-server</b></pre>
<p>Connection to the device could not be established. Telnet service might not be configured properly on the device.</p>	<p>This error message is displayed in one of the following conditions:</p> <ul style="list-style-type: none"> <li>The wrong telnet port is provided to Cisco CP to connect to the device.</li> <li>The CLI “login local” under vty lines is missing in the configuration.</li> <li>The CLI “transport input telnet” under vty lines is missing in the configuration.</li> </ul> <p>To configure VTY lines on the device, enter the following commands:</p> <pre>Router&gt; <b>config terminal</b> Router(config)# <b>line vty 0 4</b> Router(config-line)# <b>login local</b> Router(config-line)# <b>transport input telnet</b> Router(config-line)# <b>exit</b></pre>
<p>The hardware platform &lt;platform name&gt; is not supported.</p>	<p>This error message is displayed if the device is not supported by Cisco CP. See the <i>Release Notes for Cisco Configuration Professional</i> for a list of supported devices.</p>



## Cisco CP May Overwrite Existing Credentials

If you enter the default username cisco and password cisco when adding a device to the community, Cisco CP informs you that you must create new credentials to avoid causing a security problem. Cisco CP uses the new credentials that you provide to create an administrative user with a privilege level of 15. If the credentials that you enter were already configured, Cisco CP overwrites them, and gives them a privilege level of 15 when it discovers the device. If you do not want an existing user account overwritten, or the cisco/cisco default credentials overwritten, enter different credentials for Cisco CP to use to log on.

## Proxy Server Settings Might Cause Discovery to Fail

If you are using a proxy server for your Internet Explorer to connect to the Internet, make sure that the Internet Explorer is configured to bypass the proxy server for local addresses as well as the addresses of the devices that will be discovered by Cisco CP. Otherwise, device discovery will fail.

To resolve this issue, do the following in Internet Explorer 6.0:

- 
- Step 1** Choose **Tools > Internet Options ... > Connections > LAN Settings** button. The Local Area Network (LAN) Settings dialog box opens.
  - Step 2** Check to see if the **Use the Proxy Server for Your LAN** check box is selected. If the Use the Proxy Server for Your LAN check box is selected, select the **Bypass Proxy Server for Local Addresses** check box also.
  - Step 3** Click the **Advanced...** button. The Proxy Settings dialog box opens.
  - Step 4** In the Exceptions pane, enter the addresses of all of the devices for which you do not want Internet Explorer to use the proxy server.
  - Step 5** Click **OK** in the Proxy Settings dialog box.
  - Step 6** Click **OK** in the Local Area Network (LAN) Settings dialog box.
- 

## Setting the Java Heap Size Value to -Xmx256m

Complete the following steps to set the Java heap size to the value -Xmx256m:

- 
- Step 1** Exit Cisco CP.
  - Step 2** Click **Start > Control Panel > Java**.
  - Step 3** Open the Java Runtime Settings dialog. The location of this dialog varies by release.
    - a.** Click the **Advanced** tab. Locate the Java Runtime Settings dialog and proceed to [Step 4](#). If the dialog is not available from the Advanced tab, proceed to **b**.
    - b.** Click the **Java** tab. Locate the Java Runtime Settings dialog. Click the **View** button if necessary to display the dialog, and proceed to [Step 4](#).
  - Step 4** In the Java Runtime Parameters column, enter the value stated in the window. For example if the window states that you must use the value `-Xmx256m`, enter that value in the Java Runtime Parameters column. The following table shows sample values.



Product Name	Version	Location	Java Runtime Parameters
JRE	1.5.0_11	C:\Program Files\java\jre1.5.0_11	-Xmx256m

- Step 5** Click **OK** in the Java Runtime Settings dialog.
- Step 6** Click **Apply** in the Java Control Panel, and then click **OK**.
- Step 7** Restart Cisco CP.

## Collecting Cisco CP Technical Support Logs

Cisco CP automates the collection of the technical support logs that it generates. Cisco CP need not be running when the technical support logs are collected. If you need to send Cisco CP technical support logs to Cisco, complete the following steps:

- Step 1** Click **Start > Programs > Cisco Systems > Cisco Configuration Professional > Collect Data for Tech Support**. Cisco CP automatically archives the logs in a zip file named `_ccptech.zip`. Cisco CP saves that zip file 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.
- Step 2** Send the folder along with a description of the problem to the Cisco Technical Assistance Center (TAC).

## Using Cisco Configuration Professional to Run show tech-support

The Cisco IOS command **show tech-support** enables you to collect information about the router configuration that can be helpful in troubleshooting network problems. You can run the **show tech-support** command directly from Cisco Configuration Professional.

To run show tech-support from Cisco CP, complete these steps:

- Step 1** Discover the device for which you want to collect **show tech-support** data.
- Step 2** In the menu bar, click **View > IOS Show Commands**. Then choose **show tech-support** from the drop-down list.
- Step 3** Copy the command output and paste it into a text file.
- Step 4** Send the file to the Cisco representative who is assisting you.





## INDEX

---

### A

- About information [2-2](#)
- authentication
  - password [3-7](#)

---

### C

- community
  - adding devices [3-2](#)
  - basic workflow [3-1](#)
  - choose [2-2](#)
  - create [2-2](#)
  - creating [3-1, 3-2](#)
  - editing [3-4](#)
  - information display [3-8](#)
  - managing devices in [3-4](#)
  - understanding [3-1](#)
- community reference
  - Select/Manage Community Dialog Box [3-6](#)
- content pane [2-1, 2-2](#)

---

### D

- device
  - connection type [3-8](#)
  - discovering [3-5](#)
  - discovery details [3-9](#)
  - discovery status [3-9](#)
  - hardware, software and feature details [3-9](#)
  - hostname [3-8](#)
  - IP address [3-7, 3-8](#)
  - login [3-7](#)

- password [3-7](#)
- discover
  - devices [3-5](#)
- discovery
  - Cisco CP overwriting existing credentials [3-20](#)
  - configuration requirements [3-16](#)
  - details [3-9](#)
  - Secure Shell version problem [3-17](#)
  - status [3-9](#)
- display
  - filtering [3-8](#)

---

### F

- feature bar [2-1](#)

---

### H

- help system
  - display [2-2](#)

---

### M

- menu bar [2-1](#)
- mode
  - demo [2-6](#)
  - offline [2-6](#)

---

### O

- offline or demo mode [2-6](#)

---

## R

reference

device community [3-6](#)

---

## S

screencast

offline or demo mode [2-6](#)

user profile [2-4](#)

screens

Community Information [3-8](#)

Select / Create [3-6](#)

Status Bar [2-1](#)

---

## T

toolbar [2-1](#)

---

## U

user profile [2-4](#)