



HP ProCurve Manager 3.20

Network Administrator's Guide

© Copyright 2004, 2005, 2007, 2009, 2010 Hewlett-Packard
Development Company, LP.
All Rights Reserved.

Publication Number

5998-0573

October, 2010

Trademark Credits

Microsoft, Windows, Windows XP, and Windows Vista are registered trademarks of Microsoft Corporation.

Adobe is a trademark of Adobe Systems Incorporated.

Java is a US trademark of Sun Microsystems, Inc.

UNIX is a registered trademark of The Open Group.

Disclaimer

The information contained in this document is subject to change without notice.

The only warranties for HP products and services are set forth in the express warranty statement accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Contents

1 About ProCurve Manager

Introduction	1-2
ProCurve Manager Features	1-3
ProCurve Manager Plus Features	1-4
What's New in PCM 3.20?	1-7
Client/Server Architecture	1-8
PCM Agents	1-9
PCM Plus Optional Plug-in Modules	1-10
ProCurve PCM Plus for HP Network Node Manager	1-10
Mobility Manager	1-10
Identity Driven Manager	1-10
Network Immunity Manager	1-11
Learning to Use ProCurve Manager	1-12
ProCurve Manager Support	1-13

2 Getting Started with ProCurve Manager

Configuring PCM and Viewing Data	2-3
Adding PCM Remote Client Stations	2-4
Configuring Client/Server Access Permissions	2-4
Installing a Client	2-5
Configuring SSL for Client/Server Connections	2-7
Configuring Agents	2-8
Starting PCM Client	2-11
Server Discovery Preferences	2-12
PCM+ License Registration	2-14
Transferring PCM Licenses	2-15
Network Management Home	2-17
Network Management Dashboard	2-18
PCM Status Bar	2-27
PCM Main Menu Functions	2-27
Global Toolbar Functions	2-28
Right-Click Menu	2-29
Navigation Tree	2-30
Viewing Device Information	2-32
Filtering Information in a Tab View	2-35
Reports and Floating Windows	2-38

Network Maps	2-39
Managing User Accounts	2-40
Changing Passwords	2-40
Adding Profiles	2-41
Editing and Deleting Profiles	2-43
Adding and Removing Devices from a Profile	2-43
Adding User Accounts	2-45
Editing and Deleting User Accounts	2-47
Displaying Users	2-48
Using RADIUS Authentication	2-49
Creating SMTP Profiles	2-51
Adding SMTP Profiles	2-51
Modifying SMTP Profiles	2-52
Deleting SMTP Profiles	2-53
Configuring Automatic Updates for PCM	2-54
Automatic Update History	2-54
Using the Automatic Update Wizard	2-56
Registering ProCurve Devices via PCM	2-59
Backing Up and Restoring PCM	2-60
Manual Backup	2-61
Restoring PCM	2-64
Automatic Backup	2-65
Troubleshooting the PCM Application	2-69
PCM Services	2-69
PCM Client Permissions	2-70
PCM and Firewalls	2-70
Working With Multi-homed Systems:	2-70
Using the PCM Server for Switch Web Help	2-72
3 Configuring and Managing Agents	
How Agents Work	3-2
Agent-initiated Connections	3-5
Server-initiated Connections	3-9
Configuring Unique SSL Certificates	3-16
Changing Agent Properties and Preferences	3-19
Properties	3-20
Proxy	3-21
Discovery	3-23
Device Access Preferences	3-38
Local Agent Memory Usage	3-49
Other Agent Manager Functions	3-50

Changing Server Setup	3-51
Viewing Agent Information	3-53
Downloading Files to Agents	3-55
To Download a File to Agents	3-55
To Remove a File from Agents	3-56
Managing Remote Agents Using the Web	3-57
Troubleshooting an Agent	3-58
After PCM Reinstallation	3-58
Remove Local Agent	3-60
Method 1	3-60
Method 2	3-61
Replace an Agent	3-62
4 Discovering Devices	
How Discovery Works	4-2
Viewing Discovery Data	4-5
Updating Device Data	4-6
Using Manual Discovery	4-7
Using Re-Discover Device	4-13
Discovering a Loopback Interface	4-17
Port Classification	4-19
Displaying Port Classification Information	4-19
How Discovery Classifies Ports	4-21
Finding Nodes and Paths	4-22
Using Find Node	4-22
Using Node-to-Node Trace Path	4-26
Managing Discovery Preferences	4-28
Enabling and Disabling Discovery Processes	4-29
Changing Discovery Preferences	4-33
Excluding or Deleting Devices from Discovery	4-35
Discovery Intervals	4-39
Configuring Subnets for Discovery	4-40
Re-Classifying Unknown Devices	4-43
PCM Server Memory Usage	4-44
Importing and Exporting Discovery Data	4-45
Importing Managed Subnets	4-46
Exporting Managed Subnets	4-48
Creating an Import File for Managed Subnets	4-49
Importing Discovered Devices	4-50
Exporting Discovered Devices	4-52
Creating an Import File for Managed Devices	4-53

Troubleshooting Discovery	4-57
LLDP Problems	4-57
Remedies	4-58
Special Considerations	4-60
Slowing Down Discovery	4-60
5 Using Maps	
How Maps Work	5-2
Displaying Maps	5-4
Network Map	5-5
Agents Map	5-6
Agent Map	5-7
Subnet and VLAN Maps	5-9
Mapping Features	5-10
Map Layout Options	5-10
Map Views	5-11
Map Annotations	5-15
Map Legend	5-16
Using the Maps Toolbar Options	5-18
Viewing Network Device Information	5-19
Finding a Device in Maps	5-20
Using Background Images with Maps	5-22
6 Using the Event Manager	
Viewing Events	6-2
Restricting the Events Displayed	6-6
Filtering Events	6-6
Sorting Events	6-7
Pausing the Events Display	6-7
Managing Events	6-8
Acknowledging Events	6-8
Deleting Events	6-9
Displaying Other Event Views	6-10
Viewing Event Details	6-10
Viewing Archived Events	6-11
Viewing Aggregated Events	6-15
Setting Event Preferences	6-18
Setting Event Archive Attributes	6-19
Setting Ignored Event Preferences	6-21
Setting Throttled Events Preferences	6-23

7	Managing Network Devices	
	Using Device Manager Tools	7-2
	Rules for Configuring Device Access with PCM	7-3
	Configuring Trap Receivers	7-4
	Adding Trap Receivers	7-5
	Modifying Trap Receivers	7-6
	Deleting Trap Receivers	7-6
	Configuring Authorized Managers	7-7
	Adding Authorized Managers	7-8
	Modifying Authorized Managers	7-9
	Deleting Authorized Managers	7-9
	Configuring Friendly Port Names	7-12
	Configuring SNMP and CLI Access	7-14
	Setting Communication Parameters in Devices	7-15
	Setting Communication Parameters in PCM	7-24
	Modifying Community Names	7-34
	Using Test Communication Parameters in PCM	7-36
	Troubleshooting Device Communication Problems	7-38
	Using Global Device Access Preferences	7-40
	Setting Device Display Names	7-40
	Setting Agent-Specific Device Access Preferences	7-41
	Configuring RMON Alerts	7-42
	Adding and Modifying RMON Alerts	7-43
	Deleting RMON Alerts	7-44
	Other Device Management Tools	7-45
	Device Logs	7-46
	Using the Device Log	7-46
	Using Device Syslog	7-47
	Using the Audit Log	7-50
	Replacing Network Devices	7-54
8	Managing Modules	
	Managing ONE zl Modules	8-2
	Managing a ONE Application	8-4
	Installing a ONE Application	8-9
	Activating the License for a ONE Application	8-13
	Uninstalling a ONE application	8-16
	Troubleshooting ONE zl Module Configuration	8-18
9	Discovering Media Endpoints	
	Displaying and Reporting MED Devices	9-2

Displaying MED Devices: Agent-Group View	9-2
Displaying MED Devices: Switch View	9-4
Displaying Details about a MED Device	9-7
Importing MED Information	9-8
Displaying MED Information	9-10
Creating a MED Device Report	9-11
10 Device Access and Port Security Monitoring	
Introduction	10-2
Viewing Device Access Information	10-3
Viewing Port Information	10-6
Port Status Subtab	10-7
Port Assignment Subtab	10-8
Port Access Subtab	10-9
Modifying Port Assignments	10-14
Modifying GVRP Port Properties	10-15
Using Port Monitoring (Mirroring)	10-16
To Assign the Monitoring Port	10-17
To Assign the Ports to be Monitored	10-18
To Assign the MAC Addresses to be Monitored	10-19
To View Mirror Port Status	10-21
To View Monitored MAC Status	10-22
To View Monitored Port Status	10-23
To Disable Mirroring	10-24
Using MAC Lockout	10-25
To View MAC Lockouts	10-25
To Lockout a MAC Address	10-26
11 Monitoring Network Traffic	
Introduction	11-2
How Traffic Monitoring Works	11-2
Reviewing Traffic Data	11-3
Top Traffic Overview	11-3
Using the Traffic Tab	11-6
Reviewing Port Top Talkers	11-11
Reviewing Per-Port Traffic Statistics	11-14
Reviewing Traffic Monitor Events	11-18
Configuring Traffic Monitor	11-19
Manual Configuration of Traffic Thresholds	11-20
Manual Configuration of Traffic Monitoring	11-22
Setting Traffic Monitor Preferences	11-25

Troubleshooting Traffic Monitor	11-28
12 Managing Device Configurations	
About Configuration Manager	12-3
Performing Configuration Scans	12-4
Manual Configuration Scanning	12-4
Reviewing Device Configurations	12-10
Configurations Detail	12-11
Device Configuration History	12-12
Using Configuration Labels	12-13
Comparing Device Configurations	12-14
Updating Device Configurations	12-16
Using the Deploy Configuration Wizard	12-16
Using the CLI Wizard	12-20
Using Configuration Templates	12-26
Comparing Configuration Templates	12-27
Using IP Address Pools	12-28
Using the Configuration Template Wizard	12-32
Applying Configuration Templates to Devices	12-37
Exporting Device Configurations	12-43
Importing Device Configurations	12-45
Using the Software Licensing Feature	12-49
Using the PCM Software Unlicensing Feature	12-52
Configuration Management Preferences	12-55
Setting Preferred Switch Software Versions	12-57
Network (Proxy) Settings	12-58
Updating Switch Software	12-60
Downloading the Software Version List	12-60
Using the Software Index File Download Policy	12-60
Scheduling Automatic Updates	12-61
Using Software Image Import	12-66
Using a USB Autorun File	12-69
Managing USB Certificates	12-69
Managing Encryption Keys	12-70
Creating the Autorun File	12-70
Deploying the Autorun File	12-78
Reading a Report File	12-78
Using a Script to Manage Device Configurations	12-80
Adding a Script to Script Manager	12-82
Editing a Script	12-86
Deleting a Script	12-87

Executing a Script	12-88
Embedded Script Tags	12-95
Troubleshooting a Script Execution	12-96
Script Examples	12-97
13 Working with Custom Groups	
About Custom Groups	13-2
Rules of Custom Groups	13-2
Creating Custom Groups	13-3
Modifying Groups	13-4
Deleting a Group	13-5
Adding Devices to a Group	13-6
Removing Devices from Groups	13-8
Automatically Adding and Deleting Devices	13-8
14 Using VLANs	
About VLANs	14-2
Viewing VLAN Groups (Maps)	14-3
Creating a VLAN	14-6
Modifying VLANs	14-9
Configuring Multiple IP Addresses for VLANs	14-9
Adding a Device to a VLAN	14-10
Removing a Device from a VLAN	14-13
Making VLANs Static	14-14
Making a VLAN Primary	14-15
Deleting a VLAN	14-16
Modifying VLAN Support on a Device	14-17
VLAN Support on Wireless Devices	14-18
Port Assignments on a Device	14-22
Modifying Port Assignments	14-23
Modifying GVRP Port Properties	14-24
Using IGMP to Manage Multicast Traffic	14-25
Enabling IGMP on VLANs	14-25
IGMP Settings for Routing Switches	14-29
15 Using Virus Throttle	
Introduction	15-2
General Operation of Virus Throttle	15-3
Filtering Options	15-3
Sensitivity to Connection Rate Detection	15-4
Operating Notes	15-5

Terminology	15-6
General Configuration Guidelines	15-7
For a network operating normally:	15-7
When the network appears to be under attack	15-8
VT Configuration in PCM	15-9
VT Configuration for Blocked Hosts	15-12
Virus Throttle Log and Trap Messages	15-13
16 Using Policy Manager Features	
How the Policy Manager Works	16-2
Policy Configuration Overview	16-3
Configuring Policies	16-4
Editing Policies	16-12
Deleting Policies	16-12
Enabling/Disabling Policies	16-13
Manually Enforcing Policies	16-13
Policy History	16-14
Creating Times for Policies	16-17
Custom Groups for Policies	16-20
Defining Alerts for Policies	16-21
Creating Event-based Alerts	16-21
Creating Schedule Driven Alerts	16-26
Configuring Policy Actions	16-30
Creating an Action	16-30
Editing Policy Actions	16-38
Deleting Policy Actions	16-39
Action Type Definitions	16-40
Viewing Configuration Manager Policy Status	16-49
To Enable/Disable a Policy	16-49
To Edit a Policy	16-49
To Delete a Policy	16-50
Setting Policy Management Preferences	16-51
17 Using the Network Consistency Analyzer	
Introduction	17-2
Creating a Network Analyzer Policy	17-3
The Network Consistency Analysis Report	17-10
Network Consistency Rule by Device Type	17-11
Misconfiguration Messages	17-12

18 Using Reports

Introduction	18-2
Setting Report Preferences	18-2
Using the Report Wizard	18-4
Creating a Report Policy	18-7
Types of Reports	18-13
Asset Management Reports	18-13
Device Access Control Reports	18-14
Diagnostics Reports	18-18
Network Activity Reports	18-22

19 Using the Configurable Integration Platform

Introduction	19-2
Supporting Undiscovered Network Devices	19-3
Managing 3rd-Party Network Devices	19-8
Adding User-defined Devices	19-9
Discovering User-defined Devices	19-11
Adding Plug-in Applications	19-12
Adding User-defined Web Tabs	19-15
Decoding Third-Party Traps	19-17
Editing and Deleting CIP Definitions	19-21
Editing CIP Definitions	19-21
Deleting CIP Definitions	19-21
Troubleshooting CIP	19-22
Manually Creating CIP Files	19-23
Coding Conventions and Syntax	19-23
Supporting 3rd-Party Network Devices	19-24
Adding User-defined Devices	19-32
Adding User-defined Actions	19-36
Adding User-defined Triggers	19-38
Decoding Third-Party Traps	19-45
Troubleshooting Manual CIP Files	19-49

A Integrating PCM with NNM or NNMi

Overview	A-2
Additional References	A-2
Using PCM with NNM	A-3
Starting the PCM Client from NNM	A-4
Database User Management	A-6
Differences in PCM for NNM	A-7
Integrating PCM with NNMi	A-10

Prerequisites A-10

Integration Procedure A-10

Additional References A-11

Configuring NNMi Communication Settings A-11

Adding NNMi Subnets A-14

Differences in PCM for NNMi A-15

PCM-NNM/NNMi Synchronization A-19

 Setting Synchronization Intervals A-19

 SNMP Data Synchronization A-20

 Device Database Synchronization A-20

B Glossary

About ProCurve Manager

- Introduction** 1-2
 - ProCurve Manager Features 1-3
 - ProCurve Manager Plus Features 1-4
 - What’s New in PCM 3.20? 1-7
 - Client/Server Architecture 1-8
 - PCM Agents 1-9
- PCM Plus Optional Plug-in Modules** 1-10
 - ProCurve PCM Plus for HP Network Node Manager 1-10
 - Mobility Manager 1-10
 - Identity Driven Manager 1-11
 - Network Immunity Manager 1-11
- Learning to Use ProCurve Manager** 1-12
- ProCurve Manager Support** 1-13

Introduction

ProCurve Manager (PCM) is a Windows-based network management solution for all manageable ProCurve and third-party devices. It provides network mapping and polling capabilities, device auto-discovery and topology, tools for device configuration and management, monitoring network traffic and alerts, and troubleshooting information for ProCurve networks. PCM is included with all new ProCurve managed network devices to provide manageability out of the box.

The graphical interface in PCM provides at-a-glance Dashboards that summarize activity for nodes in network, with drill-downs for more detailed device information. PCM also provides Dashboards for licensed modules like PMM, NIM, and IDM.

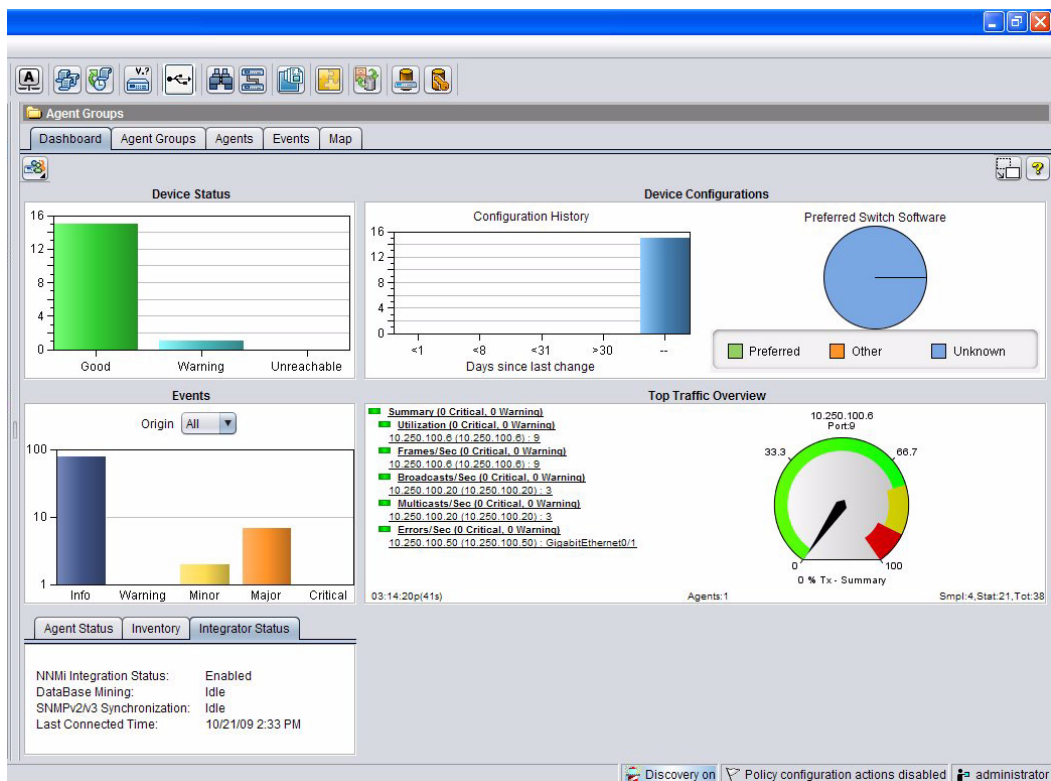


Figure 1-1. Agent Groups Dashboard

PCM also provides a simplified interface for managing and configuring the network and devices, with tools to automatically update device software and access device Web Agents and the Command Line Interface (CLI).

ProCurve Manager Features

ProCurve Manager provides an effective solution for basic monitoring and managing of network devices. PCM provides the core features of network management systems: auto discovery, network mapping, device status monitoring, and network event management. It also provides easy access to configure devices via their Web management pages or telnet access. PCM offers the basic functionality required by most IT organizations for network management, including:

Automatic device discovery: PCM is customized for fast discovery of all ProCurve and third-party manageable network devices utilizing standard SNMP MIBs. You can also define specific IP subnets and VLANs on which to perform discovery.

Network topology and mapping: Automatically creates a map of discovered network devices. Maps are color-coded to reflect device status and can be viewed at multiple levels (Agent view, physical view, subnet view, or VLAN view).

Network status summary: Upon startup, a Network Status screen displays high-level information on network devices, end nodes and events, all on one screen. From here, you can drill down on any one of these areas to get specific details.

Device monitoring: PCM provides a view of detailed device statistics and configuration information and lets you monitor devices by network, any user-defined group, or type of device.

Device management: Many device-focused tasks can be performed directly by PCM, or you can access Web and command-line interfaces with the click of a button to manage individual devices from inside the PCM Client.

Event monitoring and troubleshooting: An Events Summary displays device and PCM application events and categorizes them by severity, making it easier to track where bottlenecks and issues exist in the network. Event details provide information on the problem, even down to the specific port.

ProCurve Manager Plus Features

PCM Plus provides network administrators a powerful toolset to effectively configure, monitor, document, and troubleshoot your network. PCM Plus also provides an extensible platform that allows for the integration of other management tools, third-party devices, and ProCurve plug-in modules like Identity Driven Management (IDM), Mobility Manager (PMM), and Network Immunity Manager (NIM).

ProCurve Manager Plus (PCM Plus) is available for a 60-day trial. Thereafter, a separately purchased license key is required to use the advanced software features.

The following table compares the features provided by PCM and PCM Plus.

Feature	PCM	PCM Plus
Automatic Device Discovery	X	X
Network topology and mapping	X	X
Network status Summary	X	X
Device Monitoring and Management	X	X
Event Monitoring and Troubleshooting	X	X
Plug-in Modules - IDM, PMM, NIM		X
Switch Configuration Management		X
Security Features (e.g., VT, Mirroring, MAC lockout)		X
RADIUS Authentication of PCM Users		X
Policy-based Alerts		X
Network Traffic Analysis		X
VLAN Management		X
SNMP V3 and SSH Support		X
Device Software Updates		X
Support and Deployment for up to 10 Agents		X
Support for up to 3500 Devices		X
Automatic Device Registration		X
Custom Groups	X	X

Feature	PCM	PCM Plus
Automated Policies		X
Network Consistency Checking		X
Configurable Integration Platform		X
Inventory Report	X	X
All Reports		X
Scheduled Reports		X
Diagnostic Tools (e.g., Find Node, Path Trace)		X
Import/Export Subnet and Device Files		X
Customized Map Views		X
Network Node Manager (NNM) Integration		X

Following is a brief description of the major features provided by PCM Plus.

Network Traffic Analysis: The Traffic Manager helps you collect, measure, and analyze data about enterprise network traffic. Traffic Manager allows you to quickly identify issues, isolate problems, and optimize resource usage.

The Traffic Manager interface provides detailed information on traffic throughout the network. Leveraging enhanced traffic analysis protocols such as extended RMON and SFlow, you can define specific traffic thresholds for monitoring overall traffic levels, ports with the highest traffic, and the top users on a network port. For switches that support it, you can set thresholds and monitor both ingress and egress traffic on ports.

Optionally, you can integrate the InMon Traffic Sentinel with PCM on a device-level or system-level basis.

VLAN Management: The VLAN Manager in PCM Plus provides a single tool to create, track, and manage VLANs on your network. The VLAN management interface lets you create and assign VLANs across the entire network, without having to access each network device individually. The VLAN Manager also provides Wizards for creating VLANs, and modifying VLAN configuration, significantly reducing the likelihood of error in working with VLANs.

Configuration Management: The Configuration Manager in PCM Plus automatically tracks and logs configuration changes. Configurations can be compared over time or between two devices, with differences automatically highlighted for you.

The Configuration Manager also provides the ability to create a Device configuration template to automatically configure new ProCurve devices. A Policy can be created to automatically apply a Template to groups of devices, thus simplifying configuration and management as your network expands.

Custom Group Management: The Custom Groups feature in PCM Plus now gives you the ability to create a hierarchy of folders, each of which can contain devices or subfolders. You can create a Custom Group to match your network "locations". In addition, Groups can be defined to a port granularity, meaning that a single device may span multiple custom groups. Custom Groups become nodes in the navigation tree and has functionality similar to standard PCM device groups (e.g., ProCurve5400zl).

Automated Policy Management: With the Policy Manager you can create proactive policies that can enable immediate network action without intervention. You can create a Policy to be launched when a specific event is generated, or to take a pre-defined action at specific times. You can define the time the policy will be in effect, what devices will be included in the policy, and what actions will be taken when the policy is enacted.

Device Software Updates: The Software Version Update tool allows you to automatically update devices and obtain new ProCurve device software images from HP. You can also configure scheduled software version updates across large groups of devices—when it is most convenient for your network.

Automatic Device Registration: You can set the PCM Device Registration preference (under Registration and Licensing) to automatically register ProCurve devices with the My ProCurve portal.

SNMP V3 and SSH support: With PCM Plus you can configure PCM to support the use of SNMP V3 for device access and management, as well as the use of SSH 1 or 2 for communications between PCM and individual ProCurve devices.

Network Consistency Checking: With the Network Consistency:Network Analyzer policy you can check for configuration consistency between device connections in the network and generate a report to verify that the network is configured correctly.

Configurable Integration Platform: You can use the Configurable Integration Platform (CIP) Wizard to:

- Create and manage "User-defined devices," that is other ProCurve or non-ProCurve devices not found through auto-discovery.
- Create user-defined "Actions" and "Triggers" to launch 3rd-party applications from within the PCM Plus windows.

- Receive and process traps, and log events for non-ProCurve network devices

Schedulable Reports: The Reports scheduler lets you create a policy to schedule pre-defined PCM Plus and IDM reports at regular intervals.

Import/Export Subnet and Device Files: The Import/Export tool lets you import Device and Subnet data from a .CSV (comma delimited) file into PCM, or export Device and Subnet data from PCM to a .CSV file, so you can use it in other applications.

What's New in PCM 3.20?

The following features are new in PCM 3.20:

- Additional platforms supported:
 - Microsoft Windows 7 Professional (32/64-bit) on remote Clients only
 - Microsoft Windows Server 2008 R2 (32/64-bit)
 - VMware ESX Server 4.0
 - MS Windows Hyper-V 2008 R2
- LLDP-MED capabilities - Discover, inventory, and map LLDP-MED devices connected to LLDP-MED supported switches
- ONE zl Module application management - Install, activate, and uninstall applications on ONE zl Modules
- Script Wizard - Execute scripts (created outside of PCM) on demand or at scheduled times
- Enhanced reporting - Print reports in landscape or portrait orientation and the following new reports:
 - Device Uptime and Status Report - Provides current status of the device and percentage of time a device has been operational since it was put into service
 - MED Device Inventory - Lists pertinent information about every discovered LLDP-MED device
 - Device Configuration Change Totals - Identifies number of devices with changed software, hardware, or ROM configurations
 - Event Totals by Severity - Total number of events for each severity level at set intervals
 - Historical Event Aggregation Report - Aggregated events for each severity level at set intervals
 - Enhanced Alarms and Events

- The Last 24 Hours tab in the Dashboards' Events panel shows the number of events for each severity level at set intervals during the previous 24 hours.
 - Radio ports and control mode devices included in the Device Status History panel in Dashboards.
- SSL connection security - Unique certificates for each installation which provides added SSL connection security
 - Automatic Backup - Backup action added to Policy Manager so PCM database can be backed up automatically on demand or at specific times
 - Event IDs in Event Details - Event ID (OID) has been added to the Event Details pane shown at the bottom of the Events tab. This Event ID can be used to identify specific types of SNMP traps that should be ignored or throttled.
 - Loopback Interface - Protocols like OSPF or VRRP will always have a path because the loopback interface is accessible, even if a physical interface has failed

Client/Server Architecture

The ProCurve Manager software includes the PCM Server: A Windows host containing the ProCurve Manager Server application software that you install on your primary network management device. The PCM Server is a Java-based application that uses a data repository to store and retrieve collected network management information.

The Client component included with ProCurve Manager software is automatically installed on the PCM management Server (host). The PCM Client can be installed on other supported hosts (PCs) on the network and used to access PCM features. In addition, you can configure additional users for a Client installation, with varying levels of access (Administrator, Operator, User-view only), and restrict individual users from specific PCM functions or viewing only parts of your network.

You can install both the Server and the Client on multiple systems, providing additional redundancy and user access for network management functions.

Note:

Once you install PCM Version 3.20, you can not revert to the previously installed version. If you are uncertain if you want to upgrade to the 3.20 Version, it is best to install it on a system that does not have any earlier versions of PCM or PCM Plus installed.

PCM Agents

PCM v3's architecture lets you logically divide the network and manage devices on remote segments of large networks connected by WAN links that might or might not be behind a NAT firewall. With PCM's architecture, you can manage devices scattered geographically that were unreachable before, grant visibility and administration permissions for different parts of the network to different users, and ensure secure communication over insecure WAN links.

PCM's architecture relies on Agents deployed across the network that perform management operations on behalf of the PCM Server. A local Agent is configured on the PCM Server during installation, and up to 10 remote Agents can be installed on PCs in remote locations.

PCM Plus Optional Plug-in Modules

The following additional network management tools are bundled with the PCM software. Each of these modules is available for a 60-day trial. Thereafter, a separately purchased license key is required to enable the software features. Contact your HP representative or go to the ProCurve Web site (www.pro-curve.com) for purchasing details.

Note:

To identify the version number of PCM and the plug-in modules installed, select About ProCurve Manager from the Help menu.

ProCurve PCM Plus for HP Network Node Manager

ProCurve Manager integrates with HP Network Node Manager (version 7.5) to provide a robust solution for managing ProCurve network products in a multi-vendor environment. ProCurve Management is targeted for medium-sized enterprise networks to provide the PCM Plus functionality from the NNM interface, including ProCurve device management, network traffic monitoring, scheduled software updates, VLAN management, and policy management.

Mobility Manager

ProCurve Mobility Manager (PMM) extends the PCM monitoring and configuration tools for use with ProCurve Wireless Access Points (APs) and Wireless Services Modules (WESM). The PMM module can be used to plan wireless sites, monitor all Radios within range of the managed ProCurve APs, define Trusted Radios, and monitor and configure WLANs and SSIDs for Radios and Radio ports on ProCurve managed wireless devices.

Identity Driven Manager

The Identity Driven Manager (IDM) module for ProCurve Manager Plus automatically manages intelligent network access, applying security and performance settings to network infrastructure devices based on user, location and time. It enables central definition of policies that are then enforced at the edge by ProCurve devices. It increases network functionality and security, and is built on an existing switch platform and RADIUS standards.

Network Immunity Manager

The ProCurve Network Immunity Manager (NIM) module works with PCM Plus to gather, analyze, and interpret data from a security standpoint. Actions can be taken based upon the Network Immunity data, using the PCM Plus device management capabilities (Virus Throttle, ACLs, MAC Lockout) to mitigate or resolve existing or potential security issues. NIM can also be used to manage security devices like the ProCurve TMS zl Module.

Documentation on PCM Plug-in Modules

For information on how to configure and use PCM plug-in modules, go to <http://www.procurve.com/customercare/support/manuals/index.htm> and scroll down to "Network Management" to find links to documentation for:

HP ProCurve Identity Driven Manager

HP ProCurve Mobility Manager

HP ProCurve Network Immunity Manager

Learning to Use ProCurve Manager

The following information is available for learning about ProCurve Manager:

- This Network Administrator's Guide—helps you become familiar with using the application tools for network management.
- Online help information—provides information through Help buttons in dialog boxes, and through a table of contents with hypertext links to procedures and reference information. MS Internet Explorer version 8 is recommended.
 - We recommend you enable the "Allow active content to run in files on My Computer" Internet Explorer option (Tools > Internet Options > Advanced > Security).
- HP ProCurve Network Management Installation and Getting Started Guide—provides details on installing the application and licensing, and an overview of ProCurve Manager functionality.

ProCurve Manager Support

Product support is available on the World Wide Web at:

www.procurve.com/support

The information available at this site includes:

- Product Manuals
- Software updates
- Frequently asked questions (FAQs)
- Links to Additional Support information

You can also call your HP Authorized Dealer or the nearest HP Sales and Support Office.

Getting Started with ProCurve Manager

Configuring PCM and Viewing Data	2-3
Adding PCM Remote Client Stations	2-4
Configuring Client/Server Access Permissions	2-4
Installing a Client	2-5
Configuring SSL for Client/Server Connections	2-7
Configuring Agents	2-8
Starting PCM Client	2-11
Server Discovery Preferences	2-12
PCM+ License Registration	2-14
Transferring PCM Licenses	2-15
Network Management Home	2-17
Network Management Dashboard	2-18
PCM Status Bar	2-27
PCM Main Menu Functions	2-27
Global Toolbar Functions	2-28
Right-Click Menu	2-29
Navigation Tree	2-30
Viewing Device Information	2-32
Filtering Information in a Tab View	2-35
Reports and Floating Windows	2-38
Network Maps	2-39
Managing User Accounts	2-40
Changing Passwords	2-40
Adding Profiles	2-41
Editing and Deleting Profiles	2-43
Adding and Removing Devices from a Profile	2-43
Adding User Accounts	2-45
Editing and Deleting User Accounts	2-47
Displaying Users	2-48
Using RADIUS Authentication	2-48
Creating SMTP Profiles	2-51
Adding SMTP Profiles	2-51
Modifying SMTP Profiles	2-52

Deleting SMTP Profiles	2-53
Configuring Automatic Updates for PCM	2-54
Automatic Update History	2-54
Using the Automatic Update Wizard	2-56
Registering ProCurve Devices via PCM	2-59
Backing Up and Restoring PCM	2-60
Manual Backup	2-61
Restoring PCM	2-64
Automatic Backup	2-65
Troubleshooting the PCM Application	2-69
PCM Services	2-69
PCM Client Permissions	2-70
PCM and Firewalls	2-70
Working With Multi-homed Systems:	2-70
Using the PCM Server for Switch Web Help	2-72

Configuring PCM and Viewing Data

The following roadmap summarizes the steps required to set up your PCM.

1. Add PCM Clients (2-4).
2. Configure PCM Agents (2-8).
3. Start a Client and register PCM (2-11).
4. Set up user accounts and profiles (2-40).
5. Configure SMTP profiles for PCM e-mails (2-51).
6. Configure PCM automatic updates (2-54).
7. Configure PCM to automatically register ProCurve devices (2-59).
8. Back up the PCM configuration and database (2-60).

Once PCM is configured:

9. Learn how to monitor PCM network activity and status (2-17).
10. Learn how to view device information (2-32).

Adding PCM Remote Client Stations

When you install ProCurve Manager, both the Server and Client functions are installed on the computer. You can also install the Client function on any number of other computers in your network that have network access to the PCM Server.

Adding a Client consists of the following steps:

- Configure access permissions on PCM Server
- Install Client

Configuring Client/Server Access Permissions

Before installing remote Client stations, you must first configure the PCM Server to allow access from each new Client station.

The PCM Server maintains a list of authorized Clients that are permitted to log into the Server. By default, when the PCM Server is installed, no remote Clients are configured.

The PCM Server has a configuration file that can easily be configured to allow access to any set of actual or potential Clients. The entries in this file depend on what you know about the Clients that need to connect.

To add an entry:

1. At the PCM Server, open the **access.txt** file with a text-based editor such as Notepad or Wordpad. The default location is C:\Program Files\Hewlett-Packard\PNM\server\config.
2. Identify each Client in one of the following ways:
 - **IP address:** Type the IP address of each Client on a separate line, or configure IP addresses with wildcards by typing an asterisk (*). For example:

```
15.255.124.84
15.29.37.*
10.*.*.*
```
 - **DNS name:** Type the DNS name of each Client on a separate line, or configure DNS names with wildcards by typing an asterisk (*). For example:

```
system1.hp.com  
*.rose.hp.com
```

DNS names are useful for DHCP environments where a system's DNS name remains unchanged, although it's actual IP address may change from time to time).

- **Password:** Type a password that the Client will use to access the PCM Server. Use a password instead of an IP address or DNS name when you don't know the IP address of a potential Client (e.g., the Client comes in through a VPN where the IP address of the Client is assigned externally).

Note:

The access.txt file can contain as many addresses as needed, one entry per line, and can contain a combination of IP addresses and passwords.

3. Save and close the access.txt file. The changes will take effect immediately. It is not necessary to restart the Server.
4. If you are using passwords, you must also change an entry in the server\config\TyphoonServer.cfg file. Open this file with Notepad or Wordpad, and change the line "AUTHENTICATION=10" to:

```
AUTHENTICATION=100
```

Save the file and restart the Server (listed as "HP ProCurve Network Manager Server" in the services list).

Installing a Client

To install the Client on another computer:

1. Start a Web browser, such as Microsoft Internet Explorer, on the computer where you want to install the PCM Client.
2. In the browser address bar, type the IP address of the PCM Server followed by a colon and the port ID 8040. For example:

```
http://10.15.20.25:8040
```

3. When the ProCurve Manager page displays, click the **Download the Remote Client** link at the bottom of the page.
4. The Client installation wizard will then guide you through the Client installation.

5. On the Client, open the **Riptide.cfg** file with Notepad or Wordpad. By default the file is located at C:\Program Files\Hewlett-Packard\PNM\client\config.
6. Add the following line (substituting <yourpassword> with the password you added to the access.txt file on the PCM Server:

```
PASSWORD=<yourpassword>
```

Do not change any of the other entries in the file, as they are necessary for the correct operation of the Client.

A sample Riptide.cfg file, once edited with the password “procurve”, would look like this:

```
LEASE_LENGTH = 40000  
TRACING_PROPERTY_KEY = CoreServices.Main  
MANUFACTURER = Hewlett-Packard  
SERVICE_NAME = Typhoon  
COMPONENT_DB = config/Components.prp  
TRACING_DBFILE = config/Loggers.prp  
NETWORK_DELAY = 25000  
VERBOSE = true  
PASSWORD=procurve
```

- a. Save and close the Riptide.cfg file.
- b. Start the Client by clicking Windows Start button and selecting Programs > ProCurve Manager > ProCurve Manager Remote Client.
- c. When prompted for the PCM Server address, type the address of the Server in the Direct address field. The Client should now connect successfully to the Server.

Note

If you have multiple ProCurve Manager Servers in the network, when you install a remote Client, you will be prompted to select the Server to which you want the Client to attach. This Server will be used each time the Client program is launched. You can change the Server that is being accessed by selecting the “ProCurve Manager Server Discovery” option that was included when you installed the Client. From your computer’s Windows Start button, select Programs > ProCurve Manager > ProCurve Manager Server Discovery.

Be sure to select a PCM Server that is running the correct PCM software version.

Configuring SSL for Client/Server Connections

In connections between a remote PCM Client and the PCM Server database, SSL is used as the default encryption method.

Although SSL encryption provides significantly enhanced security in Client/Server communication, it can increase the overhead (from 30% to 50%) on both the PCM Client and Server. To avoid this impact on Client and Server performance, PCM allows you to disable SSL encryption.

To disable (or later re-enable) SSL encryption:

1. Display the SSL Connection Security window in one of the following ways:
 - Click the **Preferences** button in the toolbar and select **SSL Connection Security**.
 - Select Tools > Preferences > SSL Connection Security.
2. In the SSL Connection Security window, deselect the **Use SSL to Encrypt data on client/server Data Base connections** check box to disable SSL for unencrypted communication (improved performance) in database connections between the PCM Server and remote Clients.

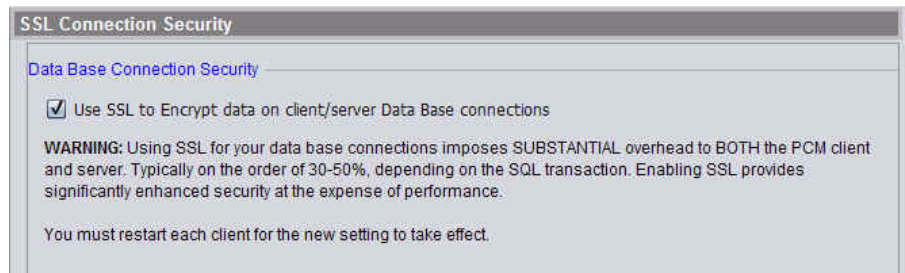


Figure 2-1. Configuring SSL for Client/Server Database Connections

Later, you may re-enable SSL encryption (impacted performance) in Client/Server database connections by re-selecting the check box.

3. Save your changes:
 - To save your changes and leave the Preferences window open, click **Apply**.
 - To save your changes and exit the window, click **OK**.
4. Restart each PCM client for unencrypted communication (disabled SSL) to take effect in Client/Server database connections.

Configuring Agents

PCM v3's architecture lets you logically divide the network and manage devices on remote segments of large networks connected by WAN links that might or might not be behind a NAT firewall. With PCM's architecture, you can manage devices scattered geographically that were unreachable before, grant visibility and administration permissions for different parts of the network to different users, and ensure secure communication over insecure WAN links.

PCM's architecture relies on Agents deployed across the network that perform management operations on behalf of the PCM Server. A local Agent is configured on the PCM Server during installation, and up to 25 Agents (including local and remote Agents) can be installed on PCs in remote locations. Geographically distributed large enterprises can be configured in multiple ways to meet user needs.

For example, a school district with 60 sites can be configured in one region managed by six remote Agents or divided into six regions with each region managed by a remote Agent, as shown in the following figure.

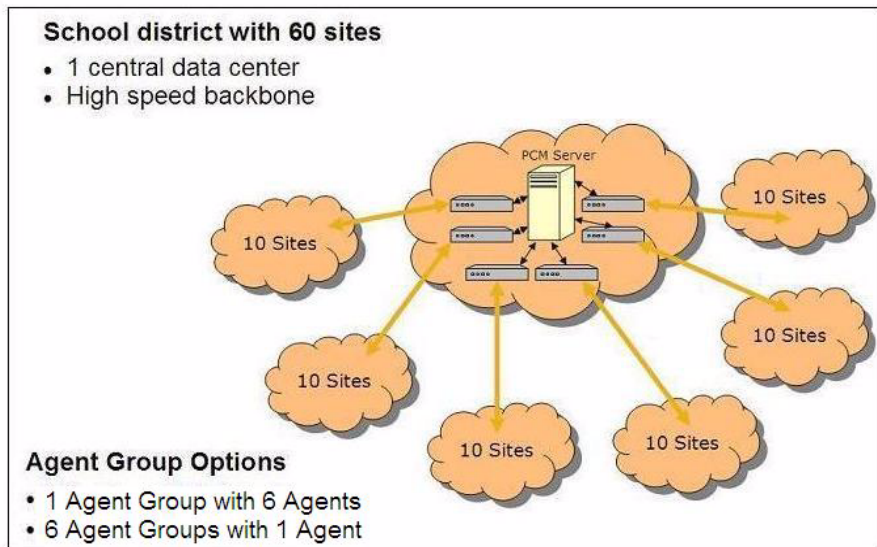


Figure 2-2. Geographically Distributed Configuration

Note:

Agents can be installed on remote networks as a Windows service by installing Agent software.

The PCM Server automatically connects to the local Agent, which is installed on the same PC as the PCM Server. The PCM Server does not automatically connect to remote Agents installed on other PCs, so you must either configure the remote Agent to initiate connections with the PCM Server or configure the PCM Server to initiate connections with the remote Agent. If a firewall or NAC appliance is between the PCM Server and a remote Agent, we recommend initiating the connection from the remote Agent behind the firewall.

Agents are placed in Agent Groups to facilitate management, which changes the navigation tree structure used in previous versions of PCM.

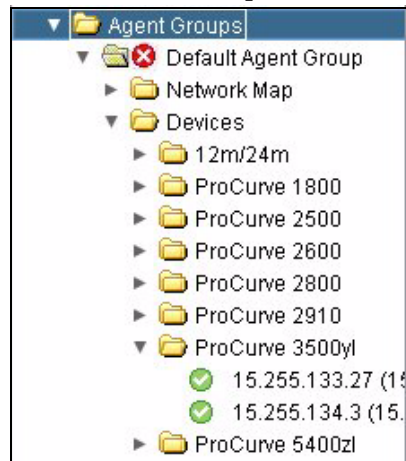


Figure 2-3. ProCurve Navigation Tree



You configure Agents by using the Agent Manager, which you open by clicking the Agent Manager button on the global toolbar. To manage an Agent, click the Agents tab and select an Agent in the navigation tree. The Agent Manager and Agents tab are described in Chapter 3, “Configuring and Managing Agents”, along with detailed instructions for all Agent-related functions listed below.

To configure an Agent (explained in detail in Chapter 3, “Configuring and Managing Agents”):

1. Install the Agent software on the remote Agent PC.
2. Configure an Agent for Agent-initiated or Server-initiated connections.
3. Identify the seed device the Agent will use to start device discovery.

Getting Started with ProCurve Manager Configuring Agents

4. If a firewall lies between PCM and the devices, configure a proxy so the PCM Clients managing those devices can bypass the firewall in a secure manner.
5. Optionally, configure new or change existing or default Discovery preferences. (Some preferences are configured during Agent installation and may not need to be configured or changed. Other default Discovery preferences are pre-defined.)
6. Customize device access settings.
7. Customize rollup status reporting thresholds.

Starting PCM Client

Before starting a PCM Client, ensure the screen resolution on the PC is set to at least 1024 x 768. Otherwise, some PCM screens may not display properly.

Start the PCM Client after you have installed the PCM Server, Client, and Agent software and set the screen resolution. Select the ProCurve Manager option from Windows Start > Programs to launch the PCM Client.

The PCM Client starts up and the Login dialog box is displayed.

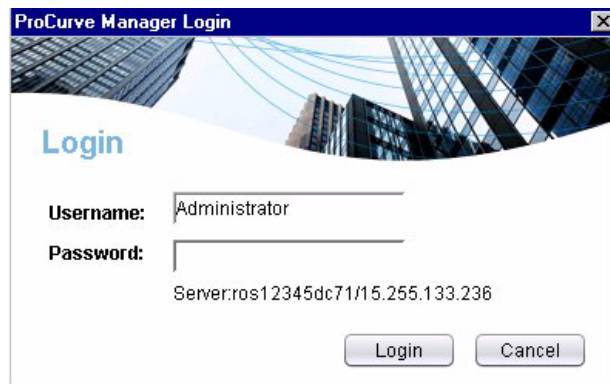


Figure 2-4. ProCurve Manager Login

If you did not enter a Username or Password during install, type the default username **Administrator**, then Click **Login** to complete the login and startup.

If you have installed the PCM Server on more than one system, the first time you start up the PCM Client you will be prompted to select a primary Server. If the original primary Server is unreachable, the Search for Servers dialog box is displayed.

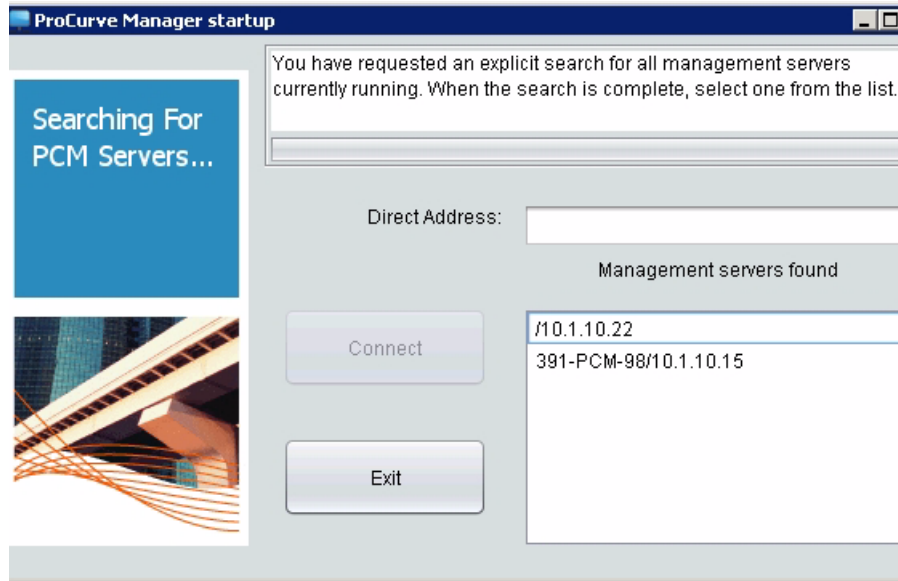


Figure 2-5. Search for Servers

Select the Server from the list on the right, then click **Connect**. The PCM Client will launch the ProCurve Manager home window.

Note:

If you are unable to launch the PCM Client, ensure the Client's access permissions are configured properly as explained in "Configuring Client/Server Access Permissions" on page 2-4. See "Troubleshooting the PCM Application" on page 2-69 for more information.

Server Discovery Preferences

When you start a PCM Client the first time, by default PCM lists all Servers that are discovered in the network as shown in figure 2-5. From the list, you select a PCM Server for the Client to access.

In some PCM networks, you may want to provide more security by limiting the display of available PCM Servers.

To limit the display of available PCM servers when a PCM Client first starts up, change the server discovery preferences as follows:

1. Open the Server Discovery window in one of the following ways:



- Click the Preferences button in the PCM toolbar and select the Server Discovery option.

- Select Tools > Preferences > Server Discovery.

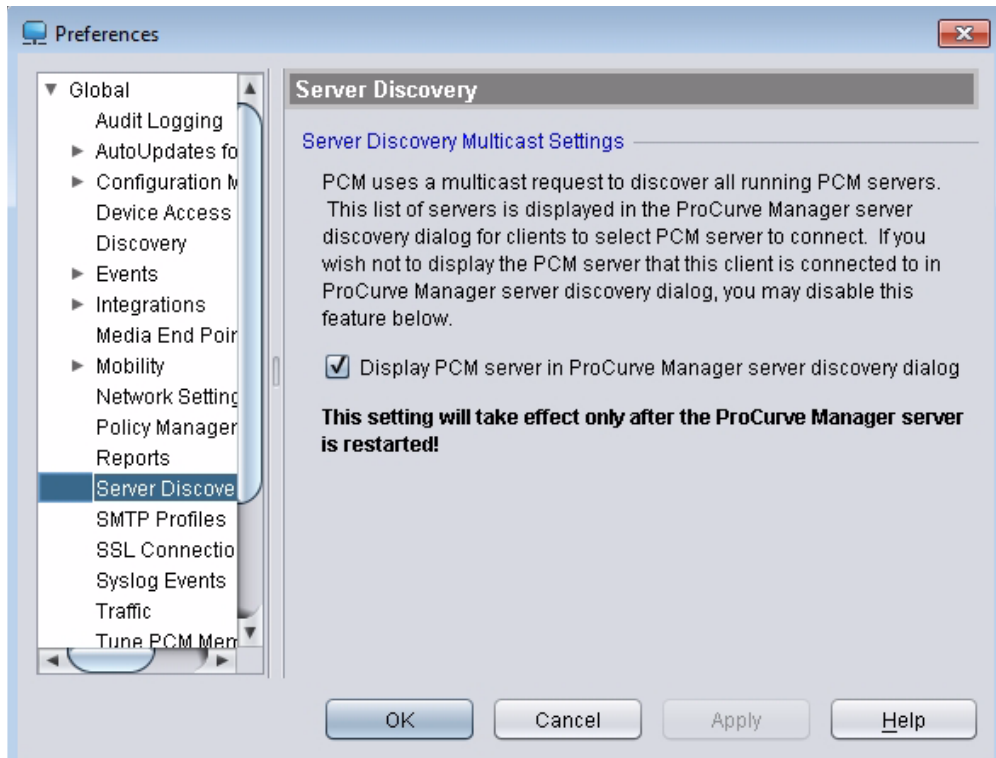


Figure 2-6. Server Discovery Preferences

2. In the Server Discovery window, do one of the following:
 - To remove the PCM Server to which the PCM Client is currently connected from the list in the Search for PCM Servers window at the first startup of a PCM Client, de-select (uncheck) the Display PCM servers in ProCurve Manager server discovery dialog check box.

Repeat this step on each PCM Client which is connected to a Server that you want to remove from the list.
 - To re-display the PCM Server to which the PCM Client is currently connected in the list when a PCM Client starts up, select (check) the Display PCM servers in ProCurve Manager server discovery dialog check box.
3. Save your server discovery setting:
 - Click **OK** to save and exit the Server Discovery window.
 - Click **Apply** to save and leave the Server Discovery window open.

PCM+ License Registration

The ProCurve Manager installation program includes a fully operable version of the PCM application, and a 60-day trial version of the PCM+ application. Until you have registered PCM, an expiring license warning will be displayed each time you log in, similar to the following.

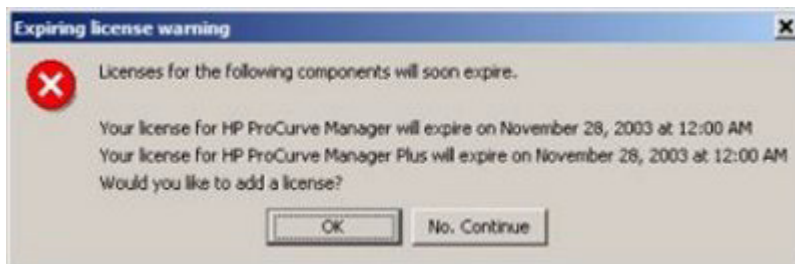


Figure 2-7. ProCurve Expiring License warning dialog box

- Click **No, Continue** to close the dialog box.
- Click **OK** to launch Licensing Administration. You can also access the Licensing window at any time to license software for PCM and its modules.

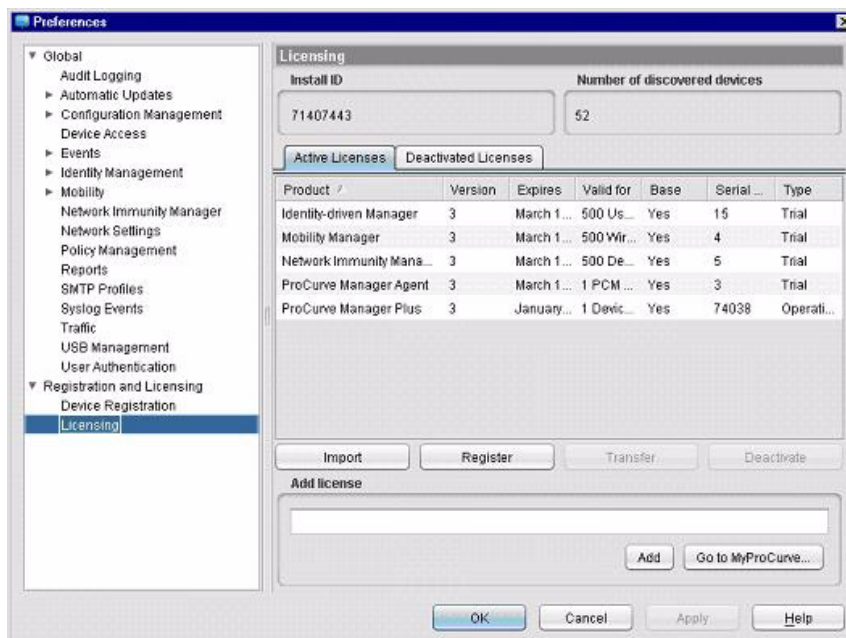


Figure 2-8. ProCurve Licensing

The Licensing window lists each of the ProCurve Management products currently installed, along with the Install ID, Serial Number, expiration date, and version.

Complete instructions for registering and licensing your PCM products are explained in the *HP ProCurve Network Management Installation and Getting Started Guide*.

Note:

If your browser uses a proxy, the proxy settings must be added to PCM Network Settings before registering or licensing your PCM products, unless you manually register and license your software through the my.procurve.com portal.

Transferring PCM Licenses

Once a license is installed, it can be transferred from one PCM Server to another PCM Server running the same software major release version (e.g., 3.0 and 3.10 both belong to major release 3.x).

1. If you have not entered your MyProCurve Credentials in PCM, enter your credentials on the Device Registration preferences window.
2. Navigate to the Licensing window:
 - a. Click the Preferences button on the global toolbar or select Preferences on the Tools menu.
 - b. In the Preferences navigation tree, expand Registration and Licensing and select Licensing.
3. Select the licenses to be transferred to another PCM Server.
4. Click **Transfer**.
5. When the confirmation prompt appears, click **OK** to confirm that you want to transfer the selected licenses and open the Transfer License wizard.
6. When the wizard Welcome window appears, click **Next** to advance to the License Selection window of the wizard.
7. In the License Selection window, check the check box in the Select column next to the licenses you want to transfer.
8. To unselect all selected licenses, check the un-Select All check box (disabled when no products are selected).
9. Click **Next**.



10. Identify the Install ID of the targeted PCM Server where the transferred license will be installed. You can find the Install ID by accessing the targeted PCM Server and selecting Tools > Preferences > Registration and Licensing > Licensing.
11. Request a new license key. To view a log of the steps taken during the process, click **View Log**.
12. Store the license bundle by selecting the location where you want to store the license bundle and typing the File Name you want to assign to it.
13. Confirm the license transfer request was processed successfully and click **Finish** to close the wizard.
14. You can then install the license(s) on the target PCM Server by using the license bundle or by using the confirmation email containing the new license key(s):
 - To use the license bundle, import the license to the targeted PCM Server.
 - a. Copy the stored license bundle to the target PCM Server.
 - b. On the Licensing window, click the **Import** button.
 - c. When the wizard Welcome window appears, click **Next** to advance to the License Selection window of the wizard.
 - d. In the Opening License File window, navigate to and select the license bundle.
 - e. Click **Next** to begin installing the license.
 - f. Monitor the installation progress and click **Next** upon completion.
 - g. Confirm the license transfer was completed successfully and click **Finish** to close the wizard.
 - To use the confirmation email, add the license to the targeted PCM Server (using the same procedure you used to initially install the license).

Network Management Home

The Network Management Home display provides a quick view of your network status in the Dashboard tab, along with overview tabs for each plug-in (IDM, PMM, NIM), a navigation tree, and access to menu and toolbar functions. You can resize the entire window, and/or resize the panes within the Network Management window frame.

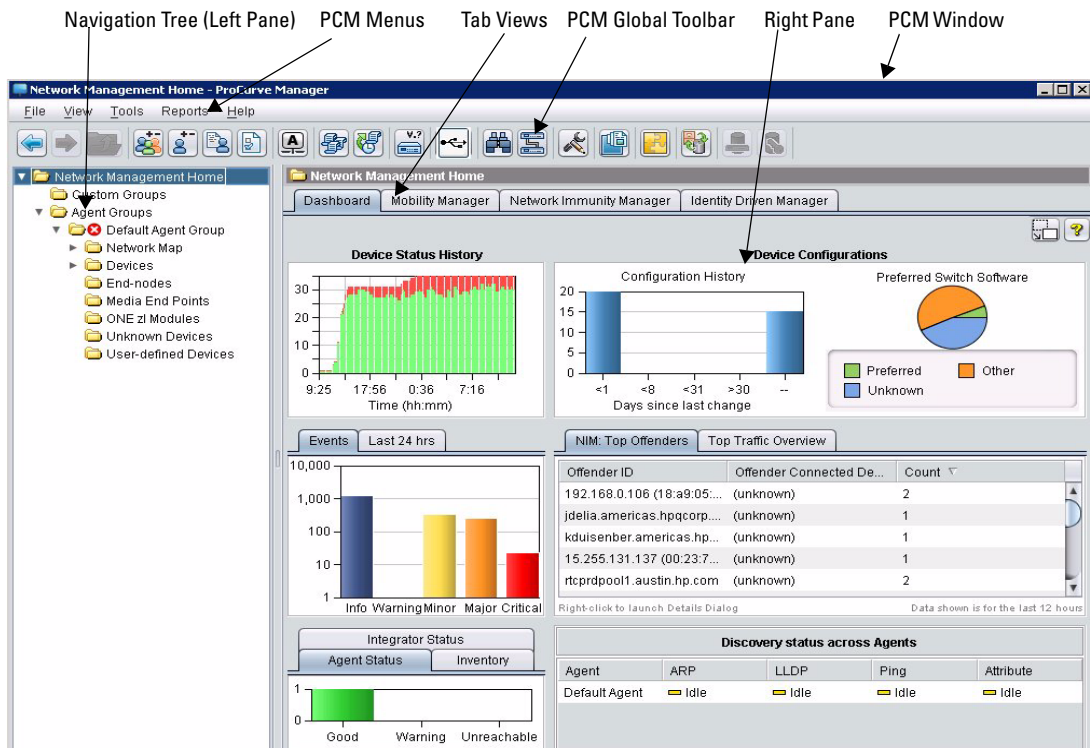


Figure 2-9. Network Management Home: Dashboard

The basics of working within the PCM Client and the Network Management Home window are described in the following sections. The function descriptions assume you are familiar with using the Windows graphical user interface.

Network Management Dashboard

When you first start PCM, the Network Management Home node is selected in the navigation tree, and the PCM Dashboard tab is displayed in the right pane, along with a dashboard tab for each installed PCM plug-in (IDM, PMM, NIM). You can return from other PCM windows to this window by selecting Network Management Home in the navigation tree.

The Dashboard tab contains the following panes of summary information for the selected node:

Device Status/Device Status History: If PMM is not installed, the Device Status panel contains a bar chart showing the number of devices with full connectivity (Good status), limited connectivity (Warning status), and Unreachable status. No history information is available.

If PMM is installed, the Device Status History bar chart is a color-coded bar chart showing the status of all wired and wireless devices, including radio ports and control mode devices, discovered during the past 24 hours:

- The green bar shows the devices that are reachable.
- The yellow bar shows the devices that have limited connectivity.
- The red bar show the devices that are unreachable.

Move the pointer over a bar to display the number of devices with each status. Click inside the Device Status History panel to display the Dashboard tab at the Agents Groups node in the navigation tree.

Device Configurations: The Device Configurations panel provides a bar chart and a pie chart. The bar chart indicates the number of devices with software configurations that have changed since the original PCM device scan, and days since the configuration changed. Moving the pointer over a bar in the bar chart displays the number of devices in that bar.

The pie chart indicates the percentage of devices with the Preferred switch software installed (set with Switch Software Preferences). Moving the pointer over a pie chart segment displays a tool tip identifying the number of devices in that segment.

Clicking anywhere in the Device Configurations panel displays the Devices Configurations tab for the associated Agent Group.

Events: On the Network Management Home dashboard, the Events tab displays a summary of events, including SNMP traps and events generated by PCM and its plug-in modules. Moving the mouse pointer over a bar in the chart displays the number of events at each severity level: critical, major, minor, warning, and information.

Use the Events tab to quickly identify the number and severity of problems in the network.

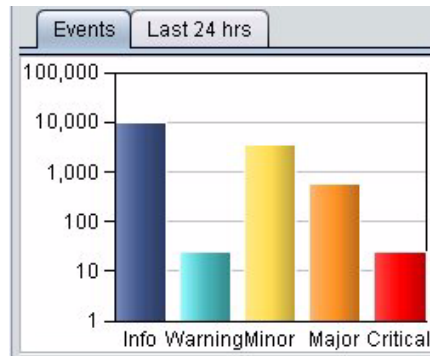


Figure 2-10. Network Management Home Dashboard: Events Tab

Notes

If you are using PCM+ for HP Network Node Manager (NNM) the display includes only events received from the NNM Events Browser.

On the Agents Group dashboard, the Events tab displays only events for:

- PCM-generated (non-device) messages
- Plug-in modules, such as Mobility Manager and Network Immunity Manager.

On all other dashboards (e.g. Custom Groups, Agent, Devices, Device Model), the Events tab includes a drop-down list that allows you to display only selected events:

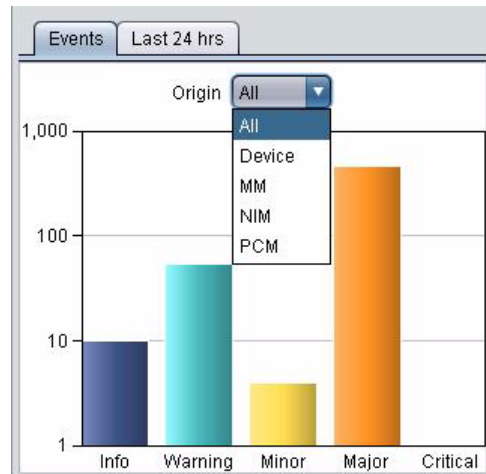


Figure 2-11. Events Tab with Drop-Down to Filter Events

To limit the display of event totals, open the Origin drop-down list and select one of the following values:

- All displays the total number of events on all devices in the PCM-managed environment.
- Device displays only events on the devices in the currently displayed dashboard group (e.g. Agent, Device Model).
- MM displays only events from ProCurve Mobility Manager for the devices in the currently displayed group.
- NIM displays only events from ProCurve Network Immunity Manager for the devices in the currently displayed group.
- PCM displays only events from ProCurve Manager core functions for the devices in the currently displayed group.

Last 24 Hours: On the Network Management Home dashboard, the Last 24 Hours tab shows a color-coded graph of the number of events that occurred in the PCM-managed network at each severity level during the last twenty-four hours or since PCM was last started (if less than 24 hours).

Use the alarm trend to quickly view the health of your network and determine the times when alarms are received. Moving the pointer over the graph displays the number of events that occurred at each severity level at a given time.

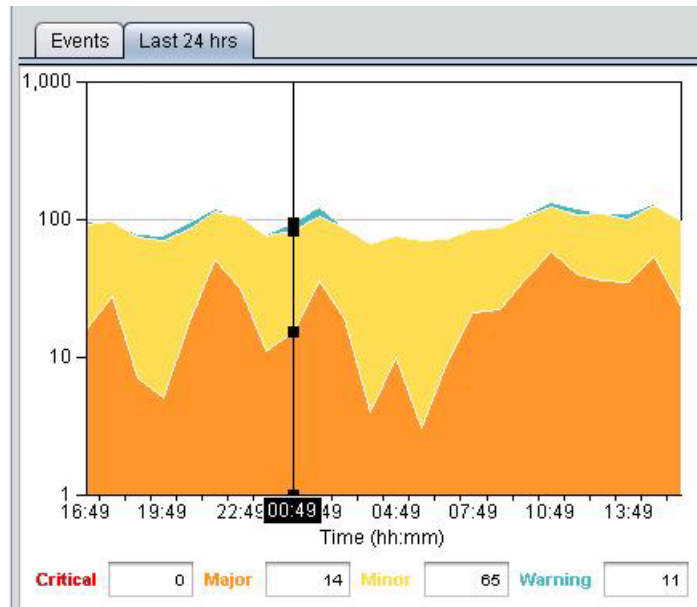


Figure 2-12. Network Management Home Dashboard: Last 24 Hours Tab

On all other dashboards (e.g. Custom Groups, Agent, Devices, Device Model), the Last 24 Hours tab allows you to display event totals by PCM plug-in module and provides threshold lines for easy event detection:

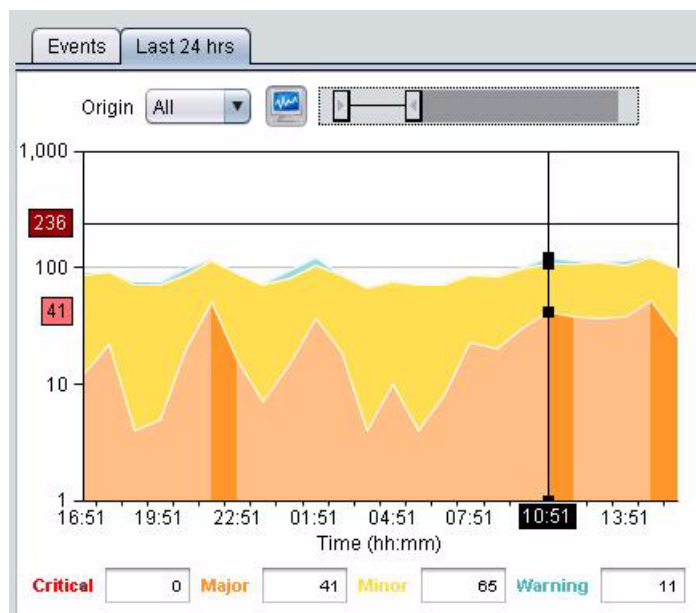


Figure 2-13. Last 24 Hours Tab with Thresholds

- To limit the display of event totals, open the Origin drop-down list box and select one of the following values:
 - All displays the total number of events on all devices in the PCM-managed environment.
 - Device displays only events on the devices in the currently displayed dashboard group (e.g. Agent, Device Model).
 - MM displays only events from ProCurve Mobility Manager for the devices in the currently displayed group.
 - NIM displays only events from ProCurve Network Immunity Manager for the devices in the currently displayed group.
 - PCM displays only events from ProCurve Manager core functions for the devices in the currently displayed group.



- Click the Threshold button to display two bars that you can drag to set an upper and lower threshold (see figure 2-13).

Use the thresholds to quickly see if events exceed the desired maximum and minimum totals, and identify the times at which the exceeded threshold values occur.

Top Traffic Overview: The Top Traffic Overview tab lists each type of traffic statistic (metric group) with a color-coded LED. The color and state of each metric-group LED is determined by comparing the values of the metric on network ports with the thresholds for the metric set on each port.

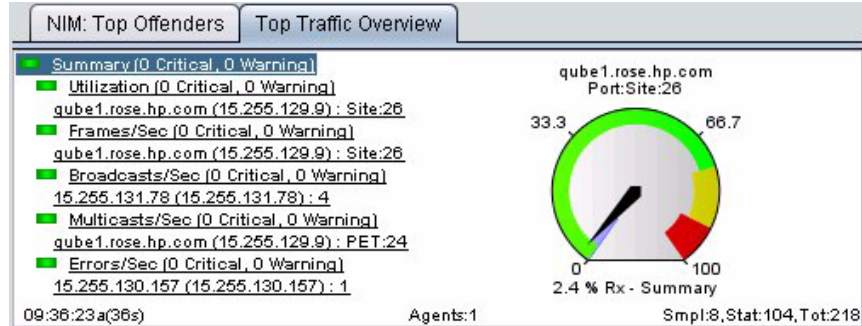


Figure 2-14. Dashboard: Top Traffic Overview

Each LED indicates the status of network traffic detected during the last minute for the metric and can be any of the following values:

- Gray (disabled): Used during initialization to indicate that the Traffic Monitor has not yet collected any data.
- Green (normal): All ports are operating normally with respect to the thresholds configured for the metric.
- Yellow (warning): At least one port has exceeded its warning threshold configured for the metric, without exceeding the critical threshold.
- Red (critical): At least one port has exceeded the critical threshold configured for the metric.

When you select a metric (for example, Utilization or Frames/Sec), the worst port measurement for the metric is displayed on the next line.

By default, the Summary of all metric groups is selected and the traffic gauge displays the status of network traffic (received during the last minute) on the worst network port.

The needle in the gauge indicates the worst metric value for the selected metric. The colors on the gauge indicate the percentage of ports whose current metric values compare to the configured thresholds for the selected metric as follows:

- Green: The current metric values fall below the configured warning thresholds.

- **Yellow:** The current metric values exceed the configured warning thresholds, but do not exceed the critical thresholds.
- **Red:** The current metric values exceed the configured critical thresholds; corrective action may be necessary.
- **Blue inner band:** High water mark, which shows the highest metric value for a port during the past 12 hours. This indicator can help you determine if there are any transient or intermittent problems for the port that may not have occurred during the last minute, even though the last completed minute shows normal activity.

Note:

If you do not have PCM installed, an unavailable message is displayed. No port selected is displayed if no devices are configured in the Traffic Monitor.

The amount of green, yellow and red displayed in the gauge corresponds to the threshold settings (set in Configure Thresholds) for the selected port and metric. For example, if the current Threshold settings for Utilization% on the selected port are as follows,

green: OK, 0-50% utilization

yellow: warning, 51-75% utilization

red: critical, 76-100% utilization

then the gauge for Utilization% would display a green area up to 50%, a yellow area from 51% to 75%, and a red area from 76% to 100%.

The text below the gauge indicates the attribute value for the current minute.

For additional details on the worst traffic segment, click inside the Worst Overview panel to display the Traffic tab for the Devices node of the navigation tree in the Agent Group that the port whose measurement was shown on the gauge resides in.

For additional information on using Traffic Monitoring, refer to Chapter 11.

Agent Status: The Agent tab uses a bar chart to show the total number of PCM Agents managed by the Server and the status of connections between the PCM Server and Agents.

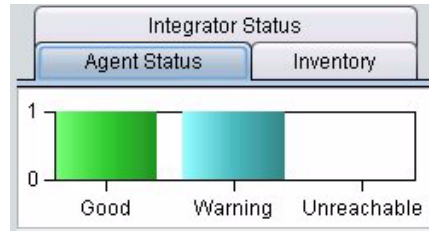


Figure 2-15. Dashboard: Agent Status Tab

The green bar represents Agents that are reachable. The blue bar represents Agents with which PCM has limited communication; for example, an agent that is restarting or not activated, or an Agent/Server connection with excessive latency. The red bar represents Agents that are not reachable.

Moving the pointer over a bar displays the number of Agents with the corresponding communication status. Clicking the panel displays the Agents tab for the Agent Groups node in the navigation tree.

Troubleshooting

If there are unreachable Agents displayed in the red bar, you can determine if the system firewall is preventing communication by temporarily disabling the firewall and rechecking the unreachable statistic in the Agent Status tab.

Inventory: The Inventory tab displays the total number of PCM Agents, network devices, end nodes, subnets, VLANs, custom groups, and LLDP-MED devices managed by PCM.

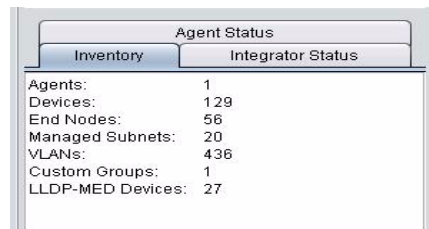


Figure 2-16. Dashboard: Inventory Tab

Note: If you use the PCM for HP NNM module, NNM provides information only for ProCurve devices. No information on end nodes is displayed in the Inventory tab

Integrator Status: The Integrator Status tab lists the integrators in the network with their status.

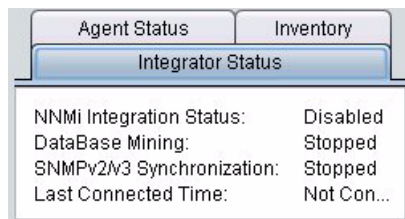


Figure 2-17. Dashboard: Integrator Status Tab

For example, the Integrator Status tab for NNMI shows:

NNMI Integration Status	Identifies whether the NNMI integrator is currently enabled or disabled
DataBase Mining	<p>Current state of database mining:</p> <p>Stopped NNMI integrator is currently disabled and database mining cannot be performed</p> <p>Idle NNMI integrator is enabled but database mining is not current running</p> <p>Running NNMI integrator is enabled and database mining is currently mining the NNMI database and updating the PCM database accordingly for all ProCurve managed devices.</p>
SNMPv2/v3 Synchronization	<p>Current state of SNMP synchronization:</p> <p>Stopped NNMI integrator is currently disabled and SNMP synchronization cannot be performed</p> <p>Idle NNMI integrator is enabled but SNMP synchronization not current running</p> <p>Running NNMI integrator is enabled and PCM is currently updating the PCM database with the SNMP Community Names defined in NNMI for all managed ProCurve devices.</p>
Last Connected Time	Time and date PCM last connected to the NNMI integrator or Not Connected if PCM has never connected to the NNMI integrator

Discovery Status Across Agents: The Discovery status across Agents tab shows whether a discovery process (e.g. ARP, LLDP, ping) on each Agent is idle or running. Information in this panel is updated every minute. Discovery processes are described in “How Discovery Works” on page 4-2.

NIM Top Offenders: The NIM Top Offenders panel lists all offenders (showing IDM users, DNS names, IP addresses, or MAC addresses for each) that evoked security alerts during the past 12 hours. The number of alerts each offender generated during that period is displayed, and by default the offenders are ordered by the number of alerts they caused.

If NIM is unable to locate an offender's point of connection to the network, a value of (unknown) will be displayed in the Offender Connected Port column of this panel. For all other offenders, whose points of connection are known, double-clicking the offender's name displays the Security Activity tab and Offenders subtab for the device that the offender was connected to at the time of their last transgression in the navigation tree. Right-clicking on an offender's row will allow the user to select Show Alert Details, which will display the Offender Details screen for the offender; this screen lists detailed information about all of the alerts portrayed in the dashboard and offers other pertinent data about the offender.

PCM Status Bar

A Status bar at the bottom of the PCM window shows the status of the Discovery process (on, off, or idle), and indicates the login account currently in use. This status bar is visible at all times.



PCM Main Menu Functions

The application menus are available at all times across the top of the PCM main window. The functions available in the menus will vary based on your login account type, and whether you are using PCM, PCM+, or other modules such as NI, PMM and IDM. Disabled functions are grayed out in the menus. Use of these application menu items are described later in this book under the processes they support.



Figure 2-18. PCM Menu Example





Global Toolbar Functions

The PCM global toolbar is available at all times across the top of the PCM main window.



Hover the mouse over a button (icon) in the toolbar to display its tool tip. Disabled functions will be grayed out.

Additional buttons appear to the right of the global toolbar of most PCM windows:





-  If it's not grayed out, click the Filter button to display filtering options, which allow you to filter the objects in the displayed pane. Detailed instructions for filtering are provided in "Filtering Information in a Tab View" on page 2-35.
-  If it's not grayed out, click the Report button to display the PCM tab contents in a separate report page layout window, where you can print the report or save it to a file.
-  If it's not grayed out, click the Floating Window button to copy the current tab or window display to a separate floating window on your desktop.
-  Click the Help button to display instructions for using the displayed window. Help opens in a new window and contains a Table of Contents and search capabilities.

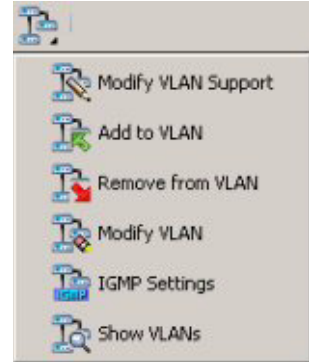
A second toolbar appears in many of the device information and configuration windows shown in the right pane. These window toolbar functions vary based on the window being displayed and the selected device type.



The functions available in the window toolbars also vary based on the profile assigned to your login, and whether you are using PCM or PCM+. The window toolbar options are described under the processes they support.

Some toolbar buttons have a small arrow in the bottom right corner, indicating there is a list of additional related options. Click the button to display the tool menu options, and select the option you want to use.

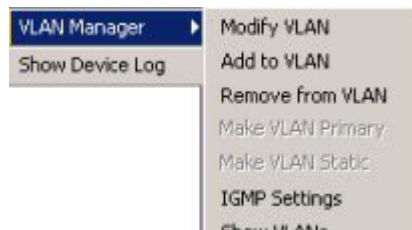
-
-  Configuration Manager
 -  Discovery Tools
 -  VLAN Manager
 -  Device Access Tools
-



Right-Click Menu

You can also access most of the component tools and commands provided with PCM via the right-click menus. To use the right-click menu, position the mouse pointer over a node in the navigation tree, and right-click to display the menu. You can also access the right-click menus when a device is selected in the Devices List and selected other windows.

An arrow (▶) next to an item in the right-click menu indicates additional sub-menu items. Click the arrow to display the sub-menu.



The options enabled in the right-click menu will vary based on the object you select, whether you are using PCM or PCM+, and your login account type. Disabled functions will be grayed out.

Navigation Tree

The navigation tree in the left pane of the PCM window provides access to network device information using a standard Windows file navigation system. Information about groups of devices and each individual device or node discovered on the network by PCM can be accessed from the navigation tree. To expand the tree, simply click the lever to the left of a node.

The status of each Agent group and device is indicated by an icon, which is updated every 30 minutes. To update the status more frequently, reduce the status polling interval.

Note:

Only the nodes and devices that are viewable by the logged-in user are displayed. You must be logged in as an Administrator to display all nodes and devices in the entire network.

The navigation tree is organized as follows:

Network Management Home: The top level of the tree provides access to information about every device in the network. Clicking Network Management Home displays the Dashboard in the right pane of the window.

- Expanding Network Management Home displays the Custom Groups and Agent Groups nodes, which can be expanded to drill down to specific groups and individual device information.
 - Custom Groups: This node is used to access information about devices in any groups you have configured. See Chapter 13, “Working with Custom Groups” for more details on creating Groups.
 - Agent Groups: The tree provides access to information about every device in the network. Clicking the Agent Groups node displays the PCM Dashboard (and its associated tabs) in the right pane of the window.
 - Expanding the Agent Groups node lists every Agent Group.
 - Expanding an Agent Group node displays the following nodes:

End Nodes: This node displays the Devices List for devices found on the network that are SNMP accessible, but do not support the bridge MIB, such as HP printers.

Media End Points: This node displays the Media Endpoint Devices (MEDs) that PCM discovered in your network. From the Media End Points tab, you can access functions to display and report on MED devices, such as Avaya, Cisco, Nortel, and Mitel Voice over IP (VoIP) phones.

ONE zl Modules: This node displays the ONE zl Modules discovered in your network. From the ONE zl Modules tab, you can access functions to install and uninstall ONE applications, activate a license, and troubleshoot ONE zl operation.

Unknown Devices: This node displays the Devices List for other devices found on the network that are not SNMP accessible, but have valid IP or IPX addresses.

If you are using PCM+ for HP NNM module, End Node and Unknown Devices will not be displayed.

User-defined Devices: This node displays any User-defined devices found on the network. Refer to “Adding User-defined Devices” on page 19-9 for more details about user-defined devices.

Network Map: This node displays the Network Map for the associated Agent Group. The Network Map node can be expanded to access The Subnets and VLANs display listings and maps for the managed subnets and VLANs.

Devices: The Devices node can be expanded to show each device group (by ProCurve switch series or third-party manufacturer) assigned to the Agent Group. The device group nodes can be expanded to access tab views for individual device information.

- The ProCurve Others node includes ProCurve devices that are SNMP accessible, but do not support LLDP, CDP or FDP. This includes older ProCurve network devices that are no longer supported, and/or newer ProCurve devices for which PCM has not yet been updated with the device drivers.
- The ProCurve Wireless Access Points node displays individual ProCurve Access Points (AP420, AP530, etc.).
- The ProCurve Wireless Services node displays individual wireless devices discovered on the network. The features available are similar to those for other (wired) ProCurve devices.
You must install the ProCurve Mobility Manager (PMM) module to use the advanced wireless configuration and monitoring features.

Viewing Device Information

There are several ways to view device information in ProCurve Manager.

- Select a node in the navigation tree, and then click the Dashboard tab. The devices reflected in the Dashboard depend on the node selected. You can also click inside some panes in Dashboard to display more detailed information.
- Select the Devices node in the navigation tree, and then click the Devices List tab to list all devices discovered on the network.
- Select a device group under an Agent Group in the navigation tree to display the Devices List for the device group. This will list all devices of that type discovered in the selected Agent Group.

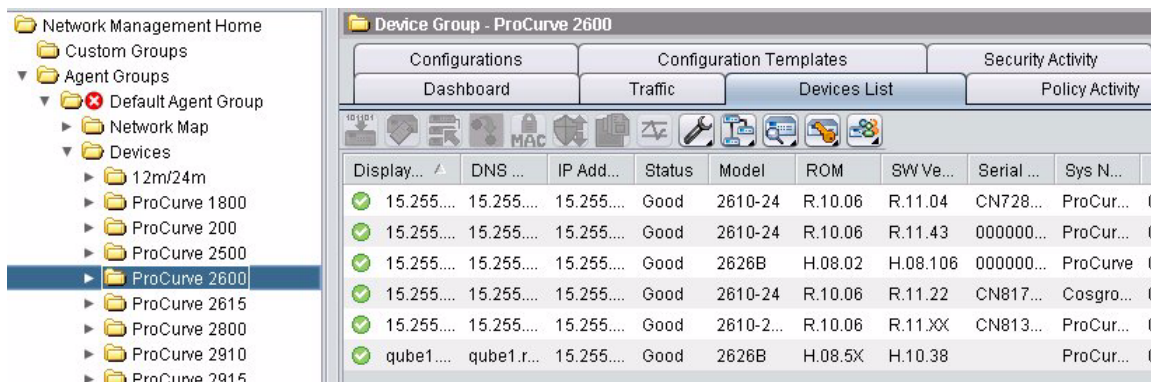



Figure 2-19. Example of the Devices List window

By default, device lists are sorted on the first column in descending order (1-10, a-z). Click the column heading to change the sort order to ascending. You can also sort the data by any of the other columns contents by clicking the column heading. An arrow  indicates the sort column, and the sort order.

Note:

The Devices window includes tabs for the Dashboard, Traffic, Devices List, Policy Activity, Events, Configurations, and Device Access. If you have a TMS zl Module installed in one of your network switches, then Security Activity, TMS-Firewall, TMS-Network, TMS-High Availability, TMS-IPS, and TMS-VPN tabs are also available.

TIP:



You can remove columns you do not want to see in the table. Simply right-click a column heading to display the list of data that can be included in the table. Checked items are displayed in the window. To hide a column, click a checked item to deselect it. The table display is refreshed and the deselected column is hidden.

From the Devices List you can select individual devices and drill-down for additional configuration details and to perform device management tasks. You can use the standard Windows selection keys Ctrl + click and Shift + click to select multiple devices in the list.

To review device properties, display the device Dashboard by double-clicking the device in a Devices List window, or clicking the device in the navigation tree.

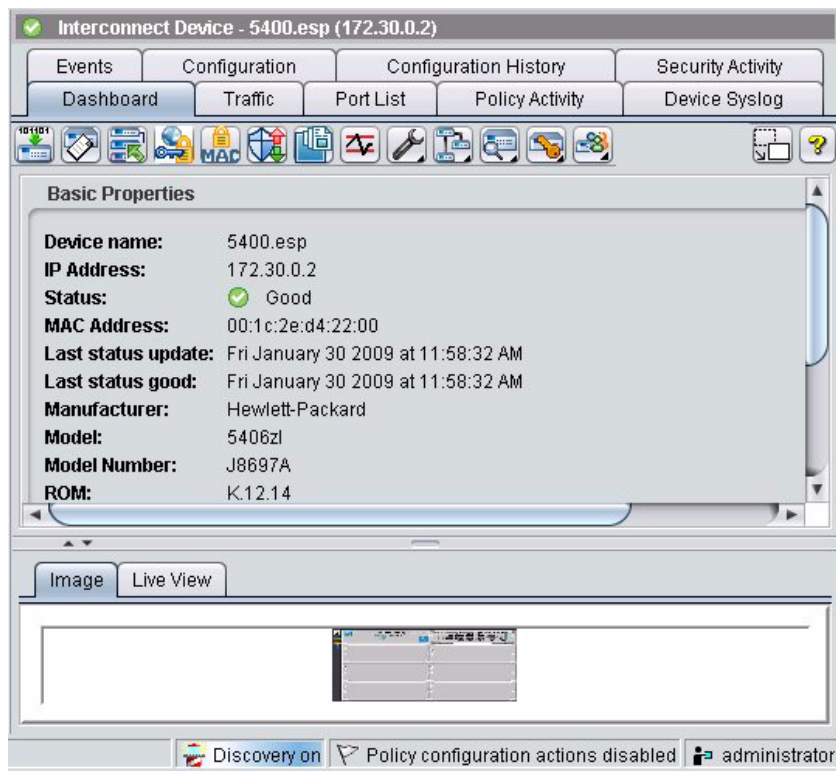


Figure 2-20. Device Dashboard

In addition to the general device properties, device name, IP Address, etc. the bottom portion of the window provides a Static view of the switch. For the models that provide WebAgent support, you can click the switch image to launch a separate window for the device's WebAgent.

Note:

If the device views do not appear in the display, it may be that you do not have the necessary JRE plug-in software. You need "J2SE Runtime Environment 5.0 (JRE)" or newer installed on your system to display the switch "live view" correctly. This software is available from Sun Microsystems Web site (java.sun.com)

For ProCurve devices that support it, you can display the Live view tab to check current port status on the switch

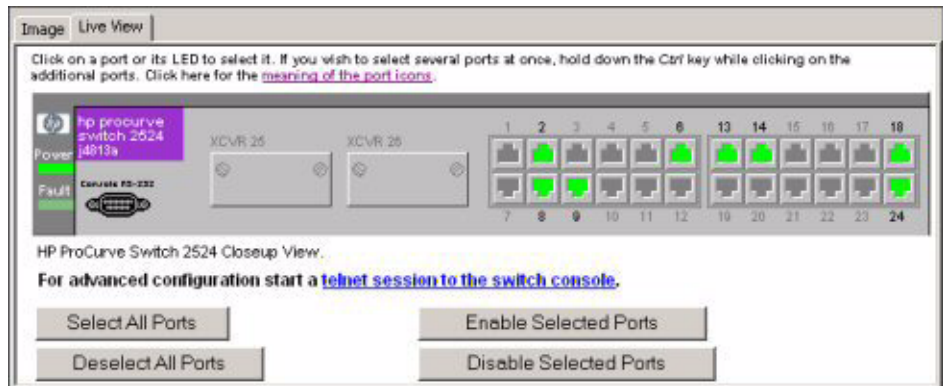


Figure 2-21. Device Properties: Live view tab

Hovering over the port with the mouse displays text below the switch image with the current port status and configuration. For example, as you mouse-over port 8 the text might be:

Port 8 is enabled, connected, and configured to Auto

You can also enable or disable a port by clicking on it, or launch a Telnet session to the switch console by clicking the telnet session to the switch console link.

Filtering Information in a Tab View

Using filtering options, you can select the information that you want to display in certain tab views, such as the Events, Security Activity, and Media End Points tabs.

To display filtering options, click the Filtering arrow at the top left side of a tab as shown in figure 2-22. The filtering criteria available for the tab view are displayed in a pane below the arrow. Filtering criteria are tab-specific.

Use the filtering options to easily locate specific information in a large display and effectively monitor network events.

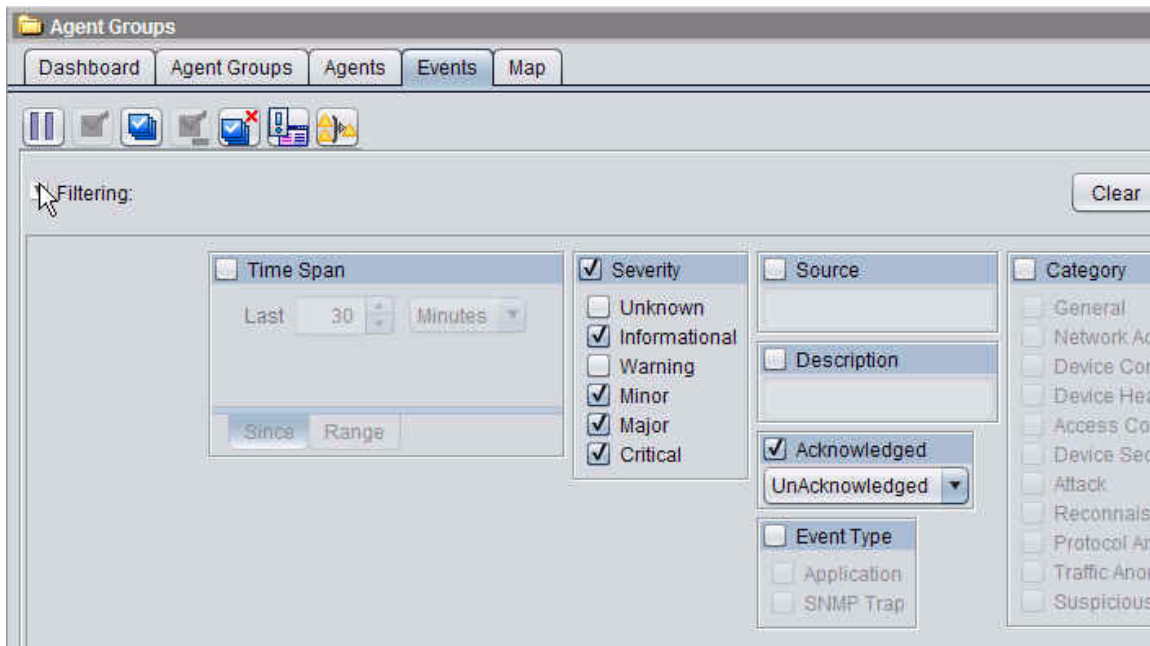


Figure 2-22. Filtering a Tab View

Any filtering criteria that are currently configured for the tab view are highlighted to the right of Filtering as shown in figure 2-23.

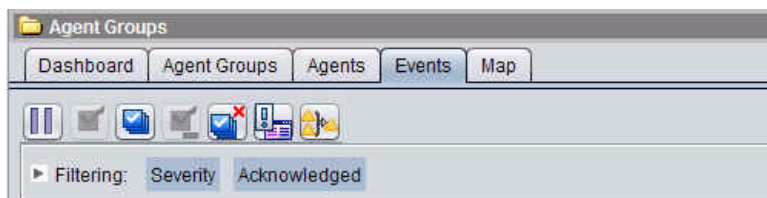


Figure 2-23. Currently Configured Filtering Criteria

When filtering the information displayed in a tab, follow these guidelines:

- When filtering events, the filter is applied against all events that are eligible for display at the current navigational tree node level instead of only the currently displayed page of event data.
- After you change filtering criteria, the tab view resets to page 1 and the first page of information that satisfies the filtering criteria is displayed.

- Filters typically affect displayed information only, so be sure to select the desired node. For example, filtering an Events window affects the selected group or device only. To change a filter for all groups and devices, display the Events tab for the Agent Groups node.
- Changing the time window affects all Event groupings of similar types. For example, changing the time filter for the ProCurve 2500 device group will also change the filter for all other specific device groups and the Devices node. Changing the time window for a specific device will change the time filter for all other specific device Events tabs.
- Some filters that allow text entry can include wild cards. For example, you can use 15.244.13 as the Source IP filter on the Events tab include view all IP addresses that include 15.244.13 such as 15.244.13.32. Wild cards are especially useful when IP addresses or names are assigned according to a specific plan.
- Do not confuse the Source filter and the Origin filter. Source is the device that caused the event, and Origin is the application or device that created the event. For example, the source might be an IP address and the origin might be PCM.

To create a filter:

1. Check a check box to activate a field. Multiple fields can be activated.
2. Select each type of information you want to display. For example, if you checked the Acknowledged check box and selected Unacknowledged from the filtering pane of the Events tab, events that have been acknowledged will be excluded from the display.
3. Click **Apply** to filter the display.
4. To save the filter, click **Save**, type the name that will be used to identify the filter, and click **OK**. The filter is added to the Load drop-down list on the Events tab, and the filter can then be activated by selecting it from the Load drop-down list.

To activate a saved filter:

1. If the Filtering pane is not displayed, click the + next to Filtering.
2. Click **Load**.
3. Select the desired filter from the drop-down list. This activates the filter and displays only events meeting the selected filter criteria.

To deactivate the current filter:

1. If the Filtering pane is not displayed, click the + next to Filtering.
2. Unselect any filters that you want to remove.
3. Click **Apply**.

To deactivate the current filter settings:

If the Filtering pane is not displayed, click the + next to Filtering. Unselect any filters that you want to remove, and click **Apply**.

To clear the current filter selection:

To clear all selections that are currently set in the filters, click **Clear**. This does not affect saved filters.

To clear unsaved filter settings:

To clear current entries in the Filters section (that have not yet been saved), click **Revert**. This does not affect saved filters.

Reports and Floating Windows

Two buttons appear in the window toolbar of most PCM windows.



If enabled, you can click the Report button to display the PCM tab contents in a separate report page layout window, where you can print the report or save it to a file.



When enabled, you can click the Floating Window button to copy the current tab or window display to a separate floating window on your desktop.

Network Maps

ProCurve Manager also provides a map feature that allows you to view your network topology. To view a map of an Agent Group's network structure, select the Network Map node under the desired Agent Group in the navigation tree.

To view a subnet map, expand the Network Map node to display the Subnets and VLANs nodes.

- Select the Subnets node to display the Subnets List view, then double-click the subnet in the list.
- Expand the Subnets node in the navigation tree to display the IP address for each of the subnets in the managed network, then select the IP address in the navigation tree.

To view a VLAN map, expand the Network Map node to display the Subnets and VLANs nodes.

- Select the VLANS node to display the VLAN List view, then double-click the VLAN in the list.
- Expand the VLANS node in the navigation tree to display all VLANs in the selected Agent Group, then select the VLAN in the navigation tree.

For additional information on working with maps, see Chapter 5, "Using Maps".

Managing User Accounts

PCM provides secure network management through user accounts and associated user profiles. User accounts define a user name and password used to log into PCM, and user profiles determine the functions that can be performed and the devices shown in the navigation tree and network maps. This prevents users from performing certain types of functions and prevents users who manage a specific Agent Group from viewing and managing devices outside their Agent Group.



To manage user profiles for PCM, click the Manage Profiles button in the PCM toolbar, or select the Manage Profiles option from the File menu. Profiles are explained in “Adding Profiles” on page 2-41.



To manage user login accounts for PCM, click the Manage Users button in the PCM toolbar, or select the Manage Users option from the File menu. User login accounts are explained in “Adding User Accounts” on page 2-45



To view users who are currently logged in and their associated profile and Client, click the Logged in Users button in the PCM toolbar as explained in “Displaying Users” on page 2-48, or select the Logged in Users option from the File menu.

Note:

The Manage Users and Manage Profiles options are not available when using the PCM-NNM module, nor are they available when logging on as a user whose profile does not have User Manager access permissions.

Changing Passwords

Use the Change Password option in the PCM File menu to change the default Administrator password or other user login passwords.

ProCurve Manager is configured with a default password for the Primary Administrator account. If you did not modify the password during installation, you should change this password after you first login.

The user name can contain 2-30 characters and must begin with a letter or an underscore.

A user password can contain 3-30 characters and can begin with any letter, underscore, or number. The password can contain lower and upper case letters from A to Z, the underscore character (_) and numbers from 0 to 9. It cannot contain any spaces or special characters other than the underscore.

Adding Profiles

PCM has three predefined profiles:

- **Administrator:** This profile has permissions to all features included in ProCurve Manager, including adding and editing user accounts.
- **Operator:** This profile has permission for all administrative functions for configuring and monitoring devices, but does not have access to the user account management functions.
- **Viewer:** This profile has permission for administrative functions for monitoring devices, but does not have access to configuration or user account management functions.

Note:

By default, all devices and custom groups are visible to these profiles.

To add a profile:

The Manage Profiles function lets you define up to 64 user profiles. To add a new profile:

1. Click the Manage Profiles button to launch the Manage Profiles window.

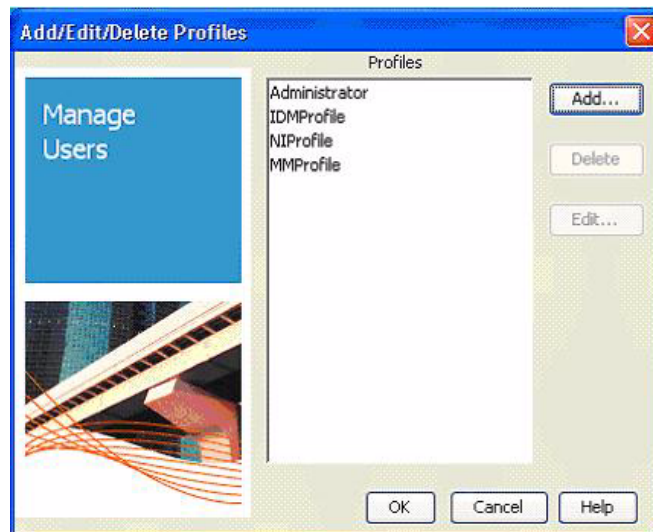


Figure 2-24. Manage Profiles

2. Click **Add** to Launch the Add Profile window.



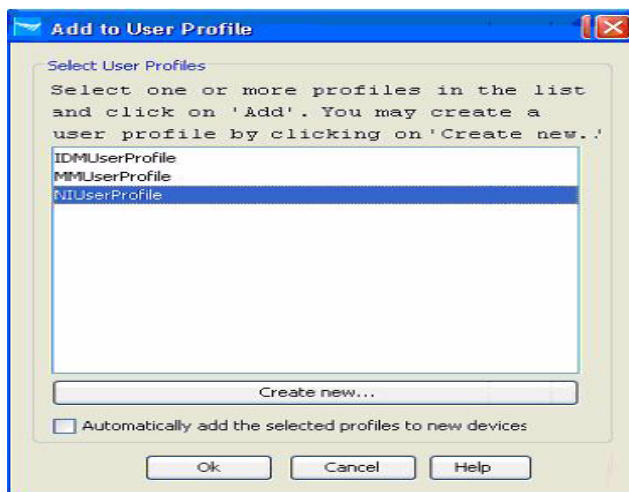


Figure 2-25. Add Profile dialog box

3. In the Profile name field, type the name used to identify the profile.
4. Check the box next to each function that users with this profile will be able to perform.
 - To select all functions in a category, simply check the category check box. For example, check the Device Manager check box to allow access to System Information, Trap receivers, and Authorized Manager.
 - To select specific functions, expand the category by clicking the lever to the left of a category and check each feature accessible by users with this profile.
5. Click **OK** to create the profile, which will be added to the list in the Manage Profiles window.

To clone a profile:



1. To create a new profile by cloning an existing profile, select the profile you want to clone and click **Clone**.

All fields are automatically filled with the values from the profile you selected.

2. Type the name of the new profile and change any other values.
3. Click **OK** to create the profile, which will be added to the list in the Manage Profiles window.

Editing and Deleting Profiles

To edit a profile:

1. Select the profile in the Manage Profiles window to enable the **Edit** and **Delete** options.
2. Click **Edit** to open the Edit Profile window, and edit the list of functions as desired. It contains the same list of functions as defined in the Add Profile window.
3. Click **Ok**. If users assigned to the profile being edited are currently logged in, the user privileges are changed immediately.

To delete a profile:

1. In the Manage Profiles window, enable the **Edit** and **Delete** options by selecting the profile to be deleted.
2. Click **Delete**. If users assigned to the profile being deleted are currently logged in, the user is automatically logged out.

Adding and Removing Devices from a Profile

An Administrator can add devices to or remove devices from a profile. Only those devices added to a profile are visible to users associated with the profile.

To add a device to a profile:



1. Right-click a device or node in the navigation tree and select Add to User Profile from the drop-down list, or select one or more devices in a device-related window, click the User Profile button, and select Add to User Profile.

Right-clicking the Agent Groups node or a specific Agent Group or device node lets you quickly add several devices to a profile.



Figure 2-26. Add Device to Profile

2. To add devices to a profile that has already been created, select one or more profiles to which the selected device or devices in the selected node will be assigned.
3. To create a new profile, click **Create new** and define the profile.
4. If you selected a group node and want to assign the selected profiles to new devices of this type, check the Automatically add the selected profiles to new devices check box.

Note:

If you do not check the Automatically add the selected profiles to new devices check box, new devices will only be visible to the Administrator.

5. Click **Ok**.

To remove a device from a profile:



1. Right-click a device or device group in the navigation tree, and select Remove from User Profile from the drop-down list. Or, select one or more devices in a device-related window, click the User Profile button, and select Remove Device(s) from User Profile.

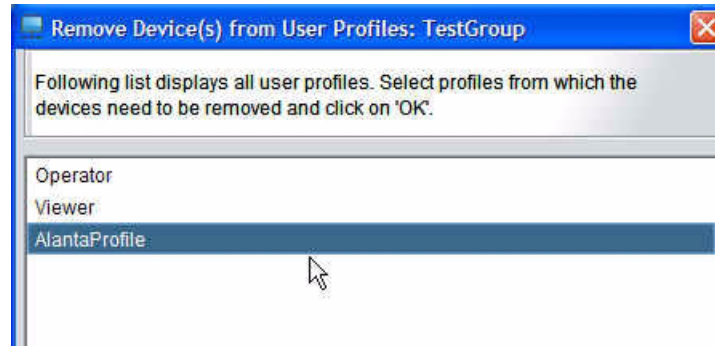


Figure 2-27. Remove Device from Profile

2. Select the profiles from which you want to remove the device(s). Use standard Windows conventions to select more than one profile.
3. Click **Remove** to remove the devices from the selected profile(s). If a user assigned to the profile is logged in, the selected devices will be removed from view.

Adding User Accounts

The Manage Users function lets you add additional login accounts with access permissions set by the profile you select for the user. To add a new user:



1. Click the Manage Users button to open the Manage Users window.

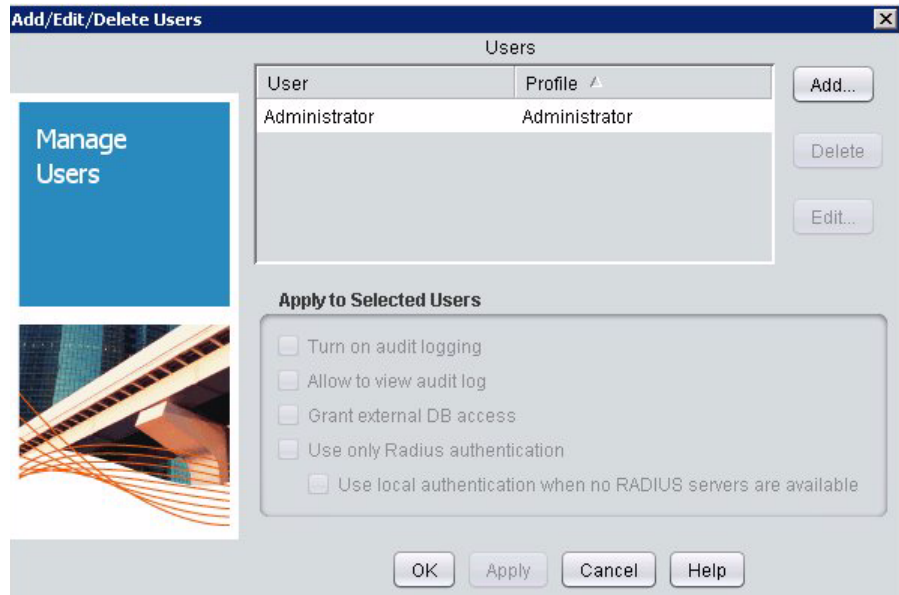


Figure 2-28. ProCurve Manage Users Wizard.

2. Click **Add** to open the Add User window.

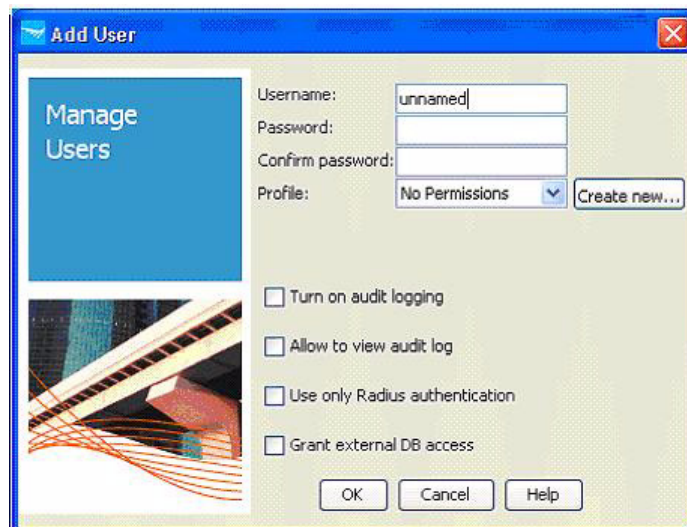


Figure 2-29. Add User dialog box

3. Enter the **Username** and **Password** for the account.
User names must contain at least 2 alphanumeric characters and cannot contain spaces or special characters. Passwords, which are optional, should conform to standard Password requirements (i.e., contain a combination of numbers, upper and lower case characters, etc.)
4. Select the **Profile** for the account. If the desired profile has not been created (is not displayed in the drop-down list), click **Create new** to create a profile.
5. Select the Turn on Audit Logging option if you want device configuration changes made by this user to be logged.
6. Select the Allow to View Audit Log option if you want to permit the user to view the audit log data. This lets the user launch the audit log browser.
7. To authenticate this user's logins via a RADIUS server instead of PCM, check the Use only RADIUS authentication check box. (The user will not be allowed to login when RADIUS authentication is disabled.) See "Using RADIUS Authentication" on page 2-49 for details.

Note:

If RADIUS authentication is configured to automatically add authenticated users to PCM and RADIUS authentication is disabled after a user is added automatically, the user cannot login until this box is unchecked.

8. To allow this user to access the PCM database from another application such as HP Network Node Manager (NNM), check the Grant external DB access check box.
The PCM database can be accessed directly using supported protocols. (JDBC, ODBC, solsql, etc.)
9. Click **Ok**. This will save the new user setup and close the Manage User window.

Editing and Deleting User Accounts

By default, only Administrators can add, edit or delete users from the ProCurve application. To edit a user account:

1. Select a user in the Manage Users window to enable the **Edit** and **Delete** option.
2. Select the **Edit** option to open the Edit Users window. It contains the same parameters as defined in the Add Users window.
3. Edit the user account parameters as desired, then click **Ok**.

To delete a user account:

1. Select a user in the Manage Users window to enable the **Edit** and **Delete** options.
2. Click **Delete**.
3. Click **OK** or **Cancel** to close the Manage Users window. (The selected user is deleted when you click **Delete**.)

Displaying Users

The Active Users list identifies all users who are currently logged into PCM, the PCM Client where the user logged in, and the login time. By default, only Administrators can view the list of users who are currently logged into PCM.

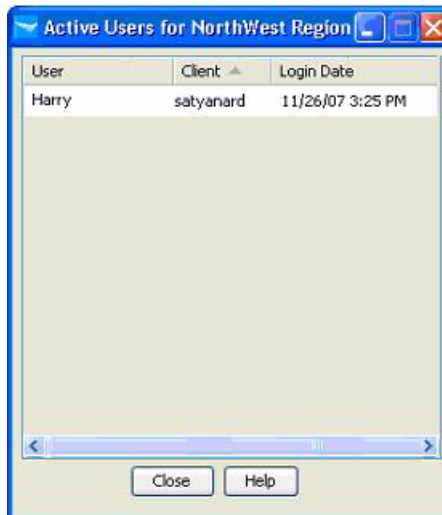


Figure 2-30. Active Users

To display users who are currently logged in:



1. Click the Active Users button on the global toolbar or select File > Logged in Users.
2. Click **Close** to close the window.

Using RADIUS Authentication

If you use RADIUS Authentication on your network, you can configure PCM user accounts to use RADIUS as the primary user authentication method. When RADIUS authentication is enabled in PCM, the user's login credentials are passed from PCM to the RADIUS server for authentication. Upon successful user authentication by the RADIUS server, PCM assigns the user profile and starts the PCM session for the user. If RADIUS does not authenticate the user, the user is denied access to PCM.

To configure PCM to use RADIUS Authentication, first make sure that the PCM Server is configured as a Client, capable of sending access request messages, to the RADIUS server. Next, select Tools > Preferences > User Authentication. This launches the Global: User Authentication window.

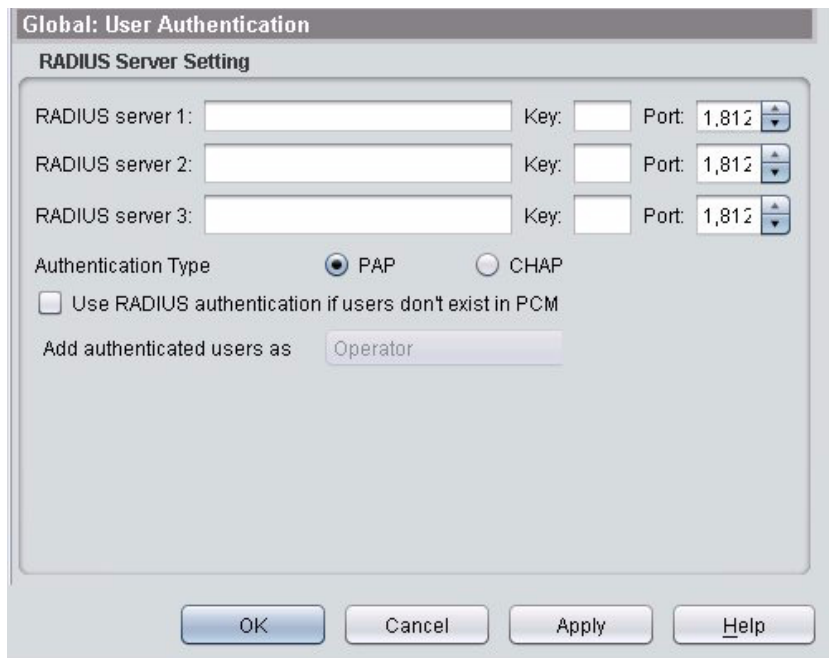


Figure 2-31. Global Preferences, User Authentication window

To enable RADIUS Authentication:

1. Configure the RADIUS server(s) by entering the IP Address of the RADIUS server, the secret key used to communicate with the server, and the port number (TCP/UDP) to use on the RADIUS server.

You can configure up to three RADIUS servers. PCM will try Server 1 first, and if it is unavailable, it will try Server 2. If server 2 is unavailable, PCM will try Server 3. If none of the configured RADIUS servers are available, you can instruct PCM to authenticate the user name and password, as explained in step 3.

2. Click the radio button to select the Authentication type, PAP or CHAP, that will be used to pass the username and password in the access request message.
3. To automatically add RADIUS Authenticated users to PCM, check the Use RADIUS authentication if users don't exist in PCM check box, then select the PCM user profile (Viewer or Operator) to apply to automatically added users.
4. Click **OK** to complete the configuration and exit the window.

Click **Cancel** to exit the window without saving the configuration.

Click **Apply** to save the configuration and keep the window open.

Creating SMTP Profiles

To use the e-mail option for PCM functions like Policy Action (Alerts) notifications and Misconfiguration Reports configure the SMTP profile to be used for e-mails.

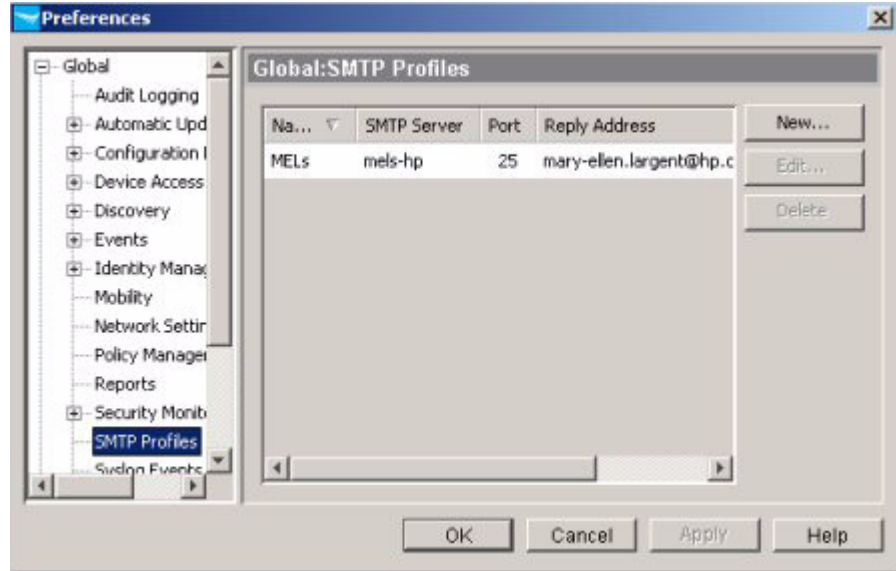


Figure 2-32. SMTP Profiles list

The SMTP Profiles window displays SMTP profiles that identify SMTP mail servers used for sending e-mail alert notifications.

Adding SMTP Profiles

To create a new SMTP profile:

1. Navigate to the SMTP profiles window by selecting **Tools > Preferences > SMTP Profiles**.
2. Click **New...** in the SMTP Profiles window to launch the New SMTP Profile window.



Figure 2-33. SMTP Profile configuration

3. Enter the SMTP Profile information in the fields provided:
 - a. In the Profile name field, enter a unique name for the SMTP profile: up to 35 characters, but not the special characters \ /) (* ? | : < > or #.
 - b. In the Server field, type the name of the SMTP server, from 1 to 35 characters. Note that this field will not be validated.
 - c. In the Port field, type the port on the server that will be used for SMTP. It can be any number between 1 and 65353.
 - d. In the Reply address field, type the email address (up to 35 characters with no spaces).
4. Click **OK** to save the profile and exit the dialog box.

The system will verify that there is an entry in the Server (name) field, that the Port is valid, and that an email address is entered. If these conditions are not met, an error message is displayed and the profile is not created.

Modifying SMTP Profiles

To modify an SMTP profile:

1. Go to Tools > Preferences > SMTP Profiles to view the SMTP profiles list.
2. Select the profile you want to change.
3. Click **Edit** to launch the SMTP Profile window.
4. Edit the SMTP profile information as described above for "Adding SMTP Profiles". Data entry fields display the current SMTP settings, which you can replace with new entries.
5. Click **OK**.

Deleting SMTP Profiles

To delete an SMTP profile:

1. Navigate to Tools > Preferences > SMTP Profiles to view the SMTP profiles list.
2. Select the profile you want to remove. You can use the standard Windows method (Ctrl and shift) to select multiple entries from the list.
3. Click **Delete**.
4. Click **Yes** in the confirmation pop-up to complete the delete process.

Configuring Automatic Updates for PCM

You can configure PCM to automatically check for application updates on the ProCurve Web site. PCM updates can include bug fixes, support for new ProCurve devices, and support for new ProCurve device software releases.

Automatic updates are downloaded to the PCM Server, which updates all Agents, as needed. An updated Agent may restart.

Note: Automatic updates to IDM Agents are not supported; you must manually update an IDM Agent.

The default configuration is set to Notify if updates are available, with a recurrence schedule that checks for updates on the first day of each week and then logs an update event in PCM.

During an automatic update, if any PCM services need to be stopped to apply the updates, PCM Clients are notified to disconnect from the PCM Server. The Auto Update function waits for a predefined time for Clients to shut down, then shuts down the PCM services. It installs the downloaded updates and restarts PCM services. An `update_history.prp` file is created on the Server with the update status information. The Auto Update function reads this file when it starts up and sends an application event to the PCM event log indicating the status of the update.

If none of the services need to be stopped for the updates to be applied, updates are applied by the Auto Update function. Upon completion of the updates, an application event is sent to the PCM event log indicating the status of the update.

Automatic Update History

To review the Automatic Update History, select `Tools > Preferences > AutoUpdates for PCM > Update History`. The Automatic Update History window displays a table containing the following PCM software update history details for the current version:

Date	Date the update was installed
Update ID	Unique ID used to identify the update
Updated by	PCM user if a user runs auto update to install updates, OR "--" if the updates were automatically applied by the PCM Server
Update mode	Identifies how the update was applied: MANUAL - Update was applied by the user with the Automatic Update Wizard. AUTOMATIC - Update was applied automatically by the system.

Automatic Update Preferences

To configure Automatic Update preferences:

1. Select Tools > Preferences > AutoUpdates for PCM to launch the Global Automatic Updates window.

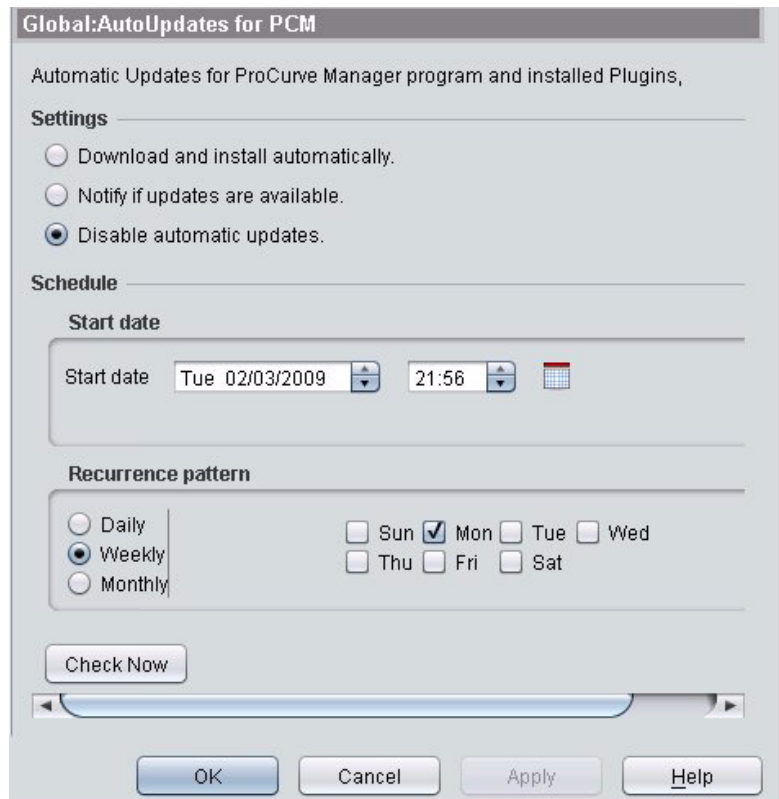


Figure 2-34. Global Preferences: Automatic Updates window

2. Select the Automatic Update option you want to use
 - Download and install automatically checks for updates at the scheduled interval, and automatically install applicable updates on the PCM Server. The update function will generate an event in the PCM events log, and in the Update History log.
 - Notify if updates are available checks for updates at the scheduled interval. When updates are found, an application event is entered in the PCM Events log. This is the default setting provided with PCM.
 - Select Disable automatic updates if you do not want to use the Automatic Update feature, then click **OK** to exit the window.
3. Configure the schedule for when updates will occur.
 - Type the Start date, or click the Calendar button to display the calendar and select a date.
 - Type the time of day (24-hour clock), or click the arrows to increase (up) or decrease (down) the time. For automatic updates, it is best to set a time when network use is low, such as night time or weekends.
4. Configure the Recurrence pattern by clicking the radio button next to the desired option, or click **Check Now** to manually launch the Automatic Update Wizard (see instructions for using the wizard below)
5. If you selected weekly or monthly, type the day of the week or month that you want the update to occur.
6. Click **OK** to save the configuration and exit the window.
Click **Cancel** to exit the window without saving any changes
Click **Apply** to save changes, and leave the window open.

Using the Automatic Update Wizard

You can check for updates at any time by using the Automatic Update Wizard. To launch the wizard:

1. You must be able to access the internet and, if you use proxies, the SOCKS proxy must be configured. Use Network Settings preferences to configure the SOCKS proxy.

To ensure the proxy server is refreshed, the proxy setting in PCM must be the same as the one set in your default browser.
2. Select Tools > Preferences > Automatic Updates to launch the Global Automatic Updates window.
3. Click **Check now** to launch the Automatic Update Wizard.

4. Select the update mode:
 - To download updates from the ProCurve FTP site, select Check for updates on the FTP Server.
 - To install updates already downloaded to the PCM server, select Check for updates in PCM's download folder. To use this feature, software update files must be placed in the /server/data/download/autoupdate folder. The default path is C:Program Files/Hewlett-Packard/PNM.

This option is especially useful in environments without internet access. The software update files can be downloaded on any PC with internet access and then transferred to the PCM server.
5. Click **Next**. Depending on your selection, PCM will check for update files in the autoupdate folder on the PCM Server or connect to the HP site and check for updates that haven't been installed on your PCM Server.
 - If no updates are found, the wizard indicates there are no updates available. Click **Close** to exit the wizard.
 - If updates are found, a list of the available updates will be displayed, similar to the following image.

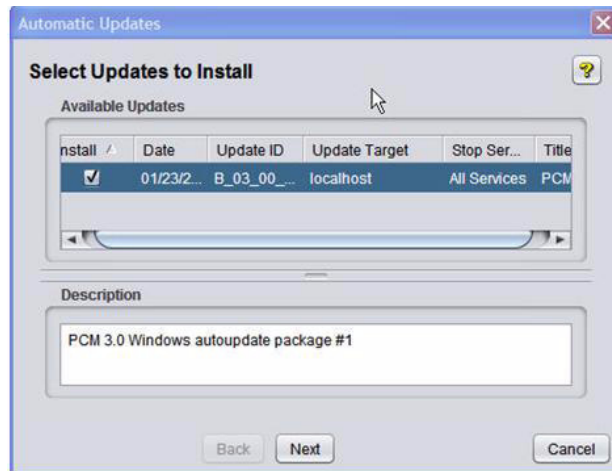


Figure 2-35. Automatic Update Wizard, Select Updates to Install

6. The Install option is selected by default. Click the Install check box to deselect any updates you do not want to install.
7. Click **Next** to install the selected update(s) on the selected Agent or Server. If updates will be downloaded, a window is displayed indicating progress of the download.

If installing the selected updates requires a restart, a message notifies you that PCM services will be shut down and the Client will be disconnected. If you are not running the Client on the same machine as the Server, a warning is displayed informing you that you may not know if the update was successful. Progress information is displayed as the updates are installed, and a message displays after the services are restarted, indicating the update results.

If the update to be installed does not require a restart of the PCM services, it is installed automatically with no warning messages. The wizard displays progress information for the update installation. When the process is complete, PCM displays a status message indicating the success or failure of the update process.

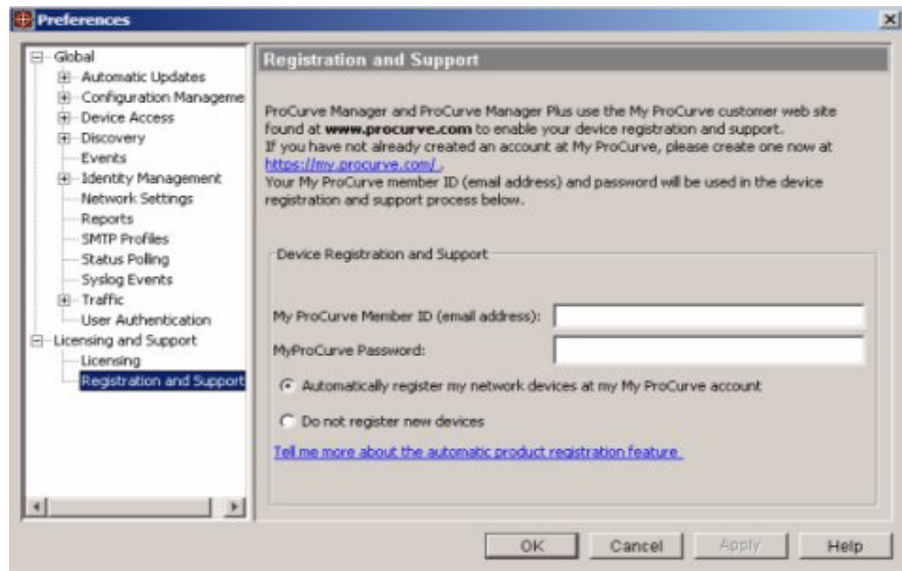
Once the update is installed, the `update_history.prp` file and Automatic Update History preferences window are updated showing the update was applied successfully.

Registering ProCurve Devices via PCM

The PCM application includes a feature that allows you to automatically register ProCurve devices with HP support when they are discovered by PCM. The Device Registration window is used to select if you want to automatically register ProCurve devices that were detected as unregistered during the Discovery process. Note that if you use HTTPS or Web proxies, you must set the SOCKS proxy in the Network Settings Preferences to use this feature.

To use automatic device registration:

1. Open the Device Registration window.
(Tools > Preferences > Registration and Licensing > Device Registration)



2. In the MyProCurve Member ID and MyProCurve Password fields, type the user name and password you received when you registered PCM.
3. Select the registration option to use with devices that PCM detects as unregistered during the Discovery process:
 - Select Automatically register my network devices at My ProCurve account to register devices automatically.
 - Select Do not register new devices if you do not want PCM to register ProCurve devices, and never want to be prompted to register devices.
4. Click **OK** to save the settings and close the window.

Backing Up and Restoring PCM

PCM allows you to manually or automatically back up all network management database files and configuration settings, including PCM plug-in modules, on the PCM Server. Traffic data is maintained on PCM Agents and is, therefore, not backed up.

To guard against catastrophic loss, it is recommended that you back up:

- After doing significant manual configuration.
- After an upgrade (e.g., PCM 2.3 to 3.0) or Automatic Update.

Note that backups can be imported to, and installed on, other operating systems.

Warning

During a backup or restore operation, all PCM services are shut down and all PCM Clients and Agents are disconnected.

Manual Backup

To manually back up all network management database and configuration files on the PCM Server:



1. Click the Backup/Restore button in the PCM toolbar to start the Backup and Restore Wizard.
2. In the Welcome window, click **Next**.

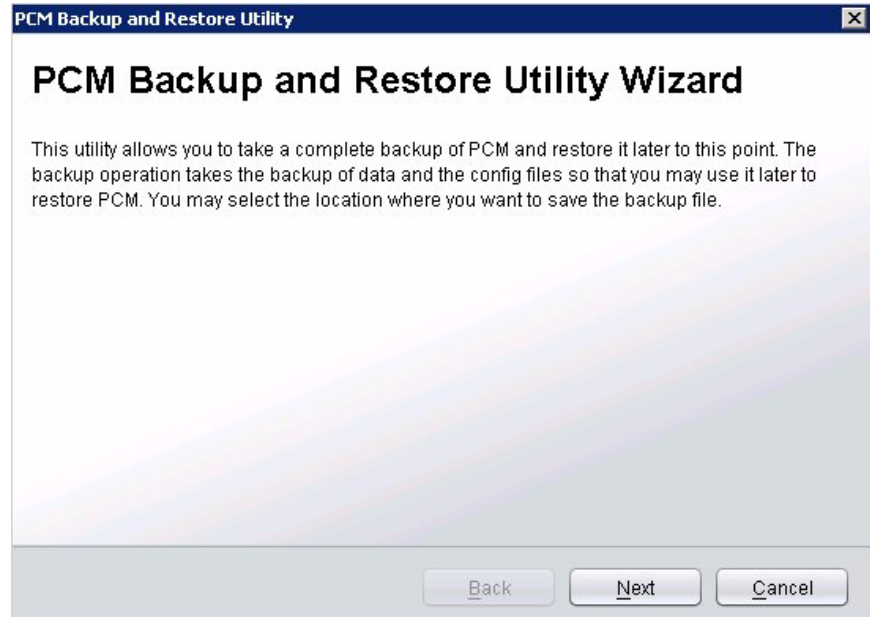


Figure 2-36. Backup and Restore Wizard: Welcome Window

3. In the Selection Step window, select Backup and click **Next**.

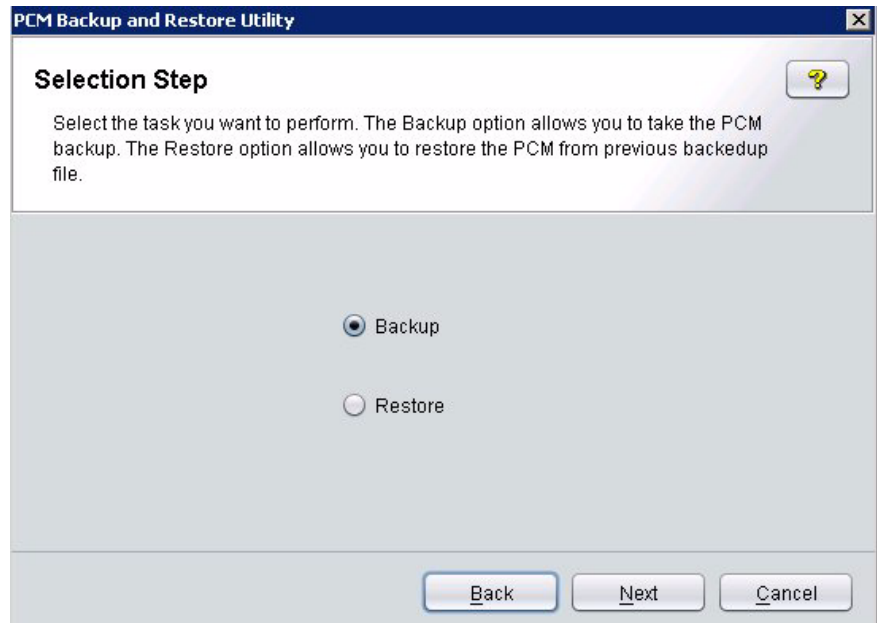


Figure 2-37. Backup Selection

4. In the Backup window, click the **Browse** button and enter the location where you want to save the backup file. Then click **Next**.

You can store the backup file at any accessible location, such as a USB removable drive or a mapped network drive. The backup file is named `PCMBBackup-dd.mm.yyyy.hh.mm.ss.zip`.

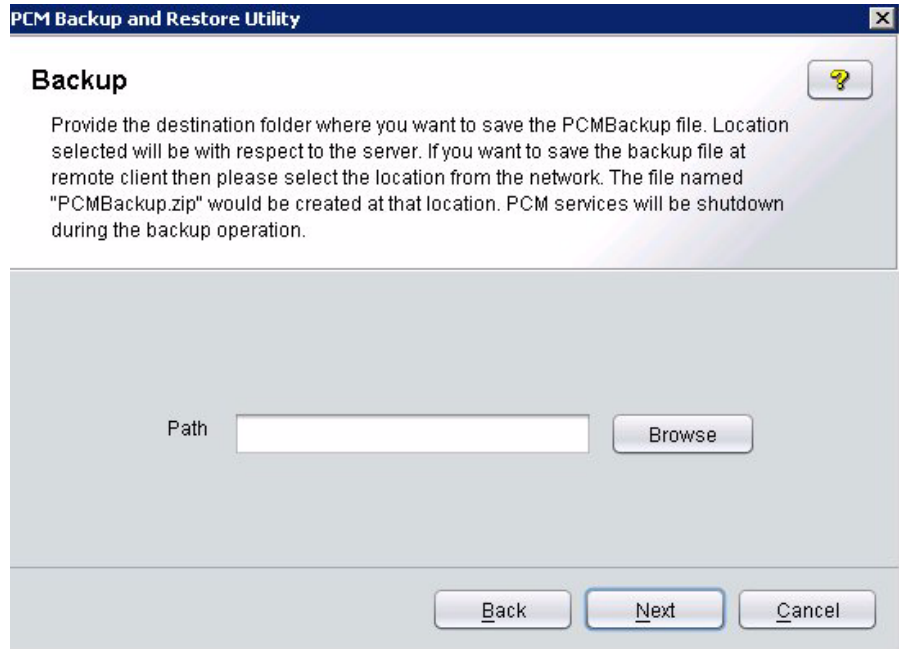


Figure 2-38. Backup Path

Note:

If you start a manual backup from a remote Client, the zipped backup file is still stored on the Server. The **Browse** button is disabled and the path you enter is used as a directory path on the Server.

In the Path field, you can also enter another Server location, a USB drive attached to the Server, or a shared folder on the remote Client. If the Client has a shared folder named "backup" (e.g., `\\Client\backup`), you can also save the backup file in the shared folder by entering the folder path.

5. When the Warning is displayed, click **OK** to start the backup process.
During the backup operation, PCM services are shut down and all Clients and Agents are disconnected.
When the backup completes, an event message indicating a successful backup is displayed.

Restoring PCM

You can restore the PCM network management database and configuration files, including PCM plug-in modules, in the event of a catastrophic loss.

Note that the PCM version that you restore must be the same version of PCM that you previously backed up.

To restore PCM:

1. Ensure that PCM has been reinstalled successfully.
2. Install licenses using the new Installation Identifier shown on the Tools > Preferences > Licensing > Support window.
3. Ensure that PCM and its plug-in modules are restored to the same automatic update as in the previous installation that you are restoring. The installed PCM and plug-in module (MM/NIM/IDM) versions and auto update numbers must match the version and auto update of the backup being restored.
4. Click the Backup/Restore button in the PCM toolbar.
5. When the Welcome window appears, click **Next**.
6. Select **Restore** and click **Next**.
7. In the Restore window, the directory path for last known successful backup file is displayed. To select another backup file, click the Browse button and enter a different pathname.



Note:

If you start a restore operation from a remote Client, the pathname you enter refers to the directory path for a backup file stored on the Server.

In the Path field, you can also enter another Server location, a USB drive attached to the Server, or a shared folder on the remote Client.

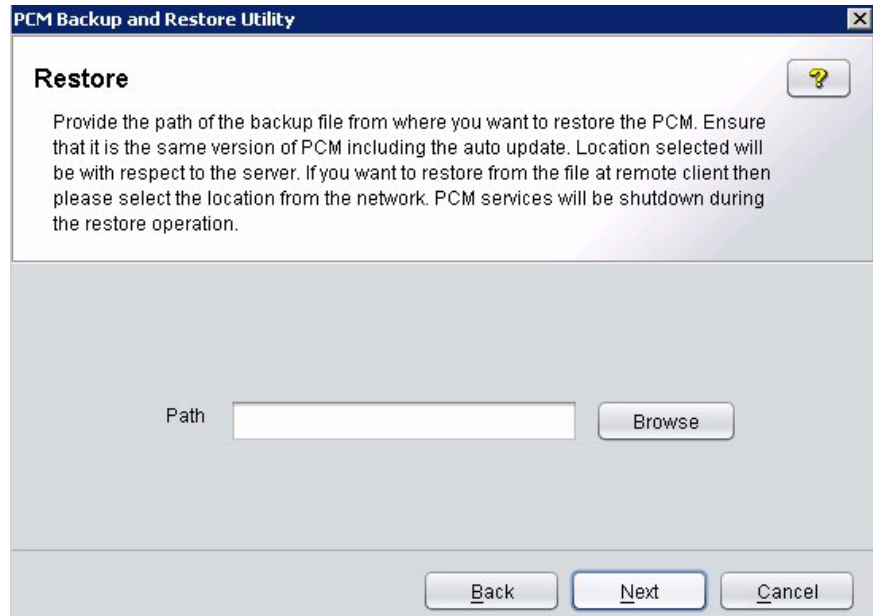


Figure 2-39. Restore Path

8. Click **Next** to begin the restore process and when the Warning appears click **OK** to begin the restore process. During restore, PCM services are shut down and all Clients and Agents are disconnected.

A restore successful event will be displayed when PCM has been restored. If the restore fails, all restore changes will be backed out.

Automatic Backup

In addition to manually backing up network management files and configuration settings on the PCM Server (see “Manual Backup” on page 2-61), you can also schedule an automatic backup as a policy action with Policy Manager.

When configured as a policy action, an automatic backup of the PCM Server is performed in response to an alert or as a scheduled action. For detailed information on how to configure policy actions, see Chapter 16, "Using Policy Manager Features".

An automatic backup functions in the same way as a manual backup:

- All PCM services are shut down.
- All Clients and Agents are disconnected.

Restriction

An automatic backup cannot be started if another backup action was performed during the last hour. An error message will be displayed.

To configure an automatic backup on the PCM Server:



1. Open Policy Manager on the PCM Server or on a Client by clicking the Launch Policy Manager button in the toolbar.
2. In the Policy Manager navigation pane, click **Actions**.
3. In the Manage Actions window, click **New**.
4. In the Create Action window:
 - a. Select **Stop and back up PCM server**.
 - b. Enter a name and an optional, text description of the backup action and click **OK**.

The name of the backup operation is added under Actions in the navigation pane and the Path Selection tab is displayed to enter a pathname.

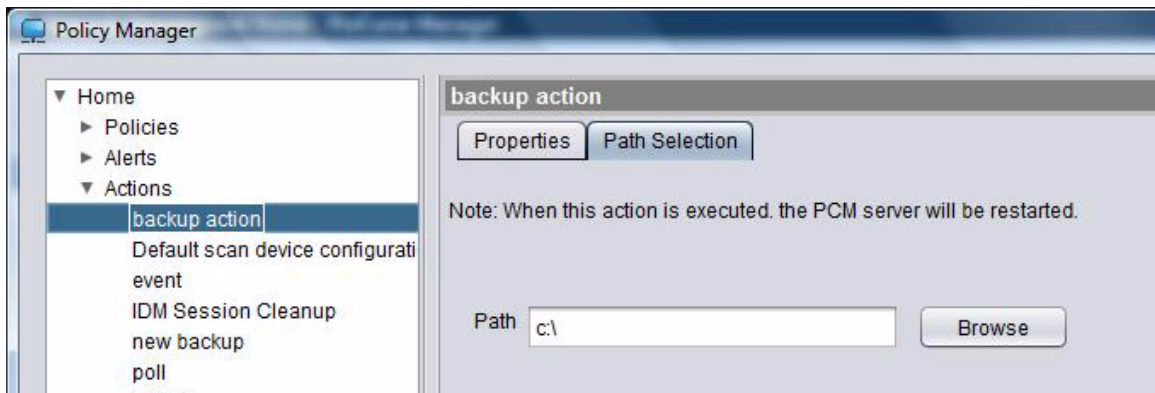


Figure 2-40. Policy Manager: Path Selection Tab

5. In the Path field, enter the pathname where you want to store the backup file.

To enter a complete directory path, click the **Browse** button and select a directory. You can store the backup file at any accessible location, such as a USB removable drive or a mapped network drive.

The backup file is named:

PCMBBackup-dd.mm.yyyy.hh.mm.ss.zip

Where *dd.mm.yyyy.hh.mm.ss* indicates the day, month, year, hour, minute, and second when the backup is performed.

Note:

If you start a manual backup from a remote Client, the zipped backup file is still stored on the Server. The **Browse** button is disabled and the path you enter is used as a directory path on the Server.

6. Save the backup configuration:
 - Click **Close** to save and exit the Backup Action window.
 - Click **Apply** to save and leave the window open.
7. Configure a policy for the automatic backup action by following the procedure in “Configuring Policies” on page 16-4. You can configure the automatic backup to be performed:
 - In response to an alert notification
 - As a regularly scheduled action that is performed at a specified time interval.

When an automatic backup operation is performed, PCM services are shut down and all Clients and Agents are disconnected.

When the backup completes, an event message indicating a successful backup is displayed.

To view the progress of a backup operation, open the lower pane of the Policies:Manage Policies > History tab in the Policy Manager as shown in figure 2-41:

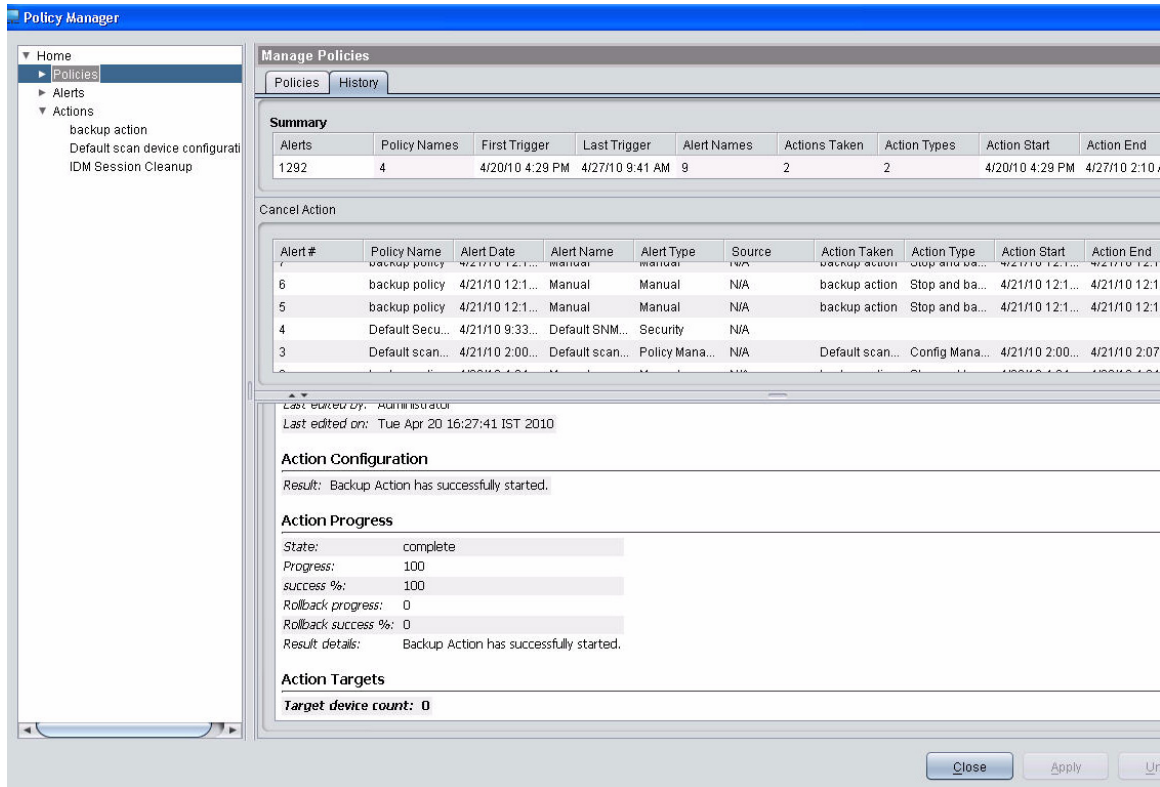


Figure 2-41. Policy Manager: Policies History Tab

Troubleshooting the PCM Application

PCM Services

If you are having trouble starting the PCM Client, or the application is not responding to commands, check to see that the PCM services are running on the PCM management Server. To access MS Windows services on a Windows XP operating system, select Start>Control Panel>Administrative Tools>Services.

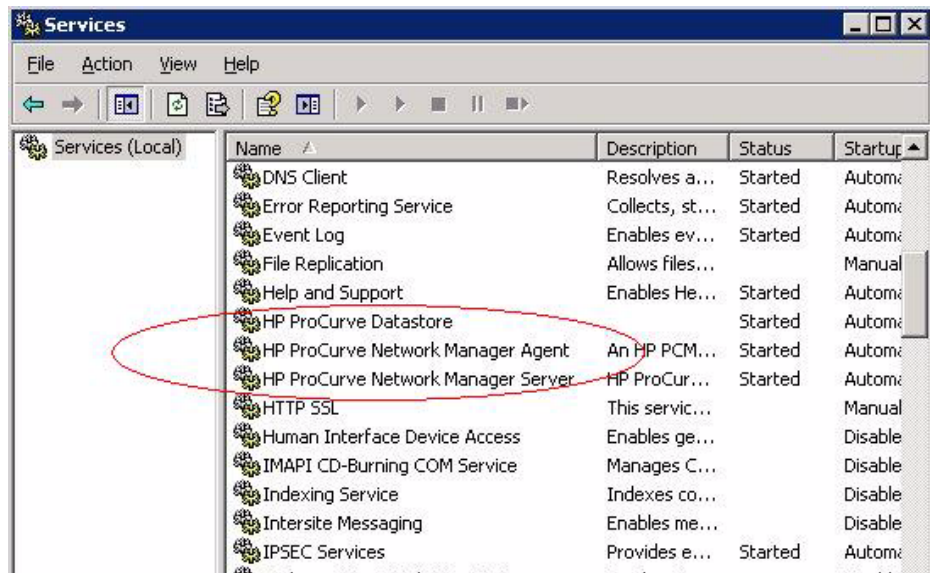


Figure 2-42. PCM Windows Services

You may need to use the Windows Administrative tools option to restart one or more of the following services:

- HP ProCurve Datastore
- HP ProCurve Network Manager Agent
- HP ProCurve Network Manager Server

PCM Client Permissions

If you can start the PCM Client, but there is no data, you may need to set the permissions for the Client. For additional information, see “Configuring Client/Server Access Permissions” on page 2-4.

1. The `access.txt` file is located on the ProCurve Manager management Server under the install directory (`/Program Files/Hewlett-Packard/PNM/server/config`). This file contains a combination of IP addresses, DNS names, and passwords that are authorized to connect to the management Server.
2. If using passwords, the password in the `access.txt` file must match the `PASSWORD = <your password>` entry in the `riptide.cfg` file located on the PCM Client in the Client directory. The default path is `C:\Program Files\Hewlett-Packard\PNM\client`.
3. If using passwords, `AUTHENTICATION=10` must be changed to `AUTHENTICATION=100` in the `TyphoonServer.cfg` file. The default path is `C:\Program Files\Hewlett-Packard\PNM\server\config`.

PCM and Firewalls

If a PCM remote Client attempts to connect to a PCM Server, and the PCM Server has a firewall turned on, it is possible that the PCM remote Client will display the message `no contexts defined` and a grey screen with no data. The firewall on the PCM Server prevents the PCM remote Client from getting the necessary connection and files from the PCM Server.

You must disable the firewall on the PCM Server to allow the PCM remote Client and the PCM Server to connect. If there is a firewall between the Client and Server, use a VPN for the connection.

Working With Multi-homed Systems:

A multi-homed system is a Server or PC that has more than one IP address. Generally this is achieved by installing more than one network card in the system, but there are other ways that a system can be multi-homed. Here are a few of the situations that meet this definition:

- A system with two or more network adaptors.
- A system with a traditional ethernet network adaptor, plus a wireless adaptor.

- A system with only one network adaptor, but that is running some network tunneling software such as a VPN client. Generally what happens in this situation, is that the system appears to have two network interfaces (each with its own IP address). But in reality the system only has one physical adaptor, and the VPN client software emulates a second adaptor (while using the original adaptor under the covers).

When ProCurve Manager (either Client, Agent, or Server) starts up, it attaches itself to the primary network interface. All network traffic between the Client or PCM Agent and Server will be directed to the selected network interface. For example, if the ProCurve Manager Client application attaches itself to the 192.3.4.5 interface, and the ProCurve Manager Server is running on the 15.255.120.25 network, the Client cannot connect successfully to the Server.

To resolve this problem PCM has a configuration file that you can change to correct this situation. To set up this file, follow these steps:

1. For a multi-homed Server, open the commIpAddr.txt file with a text-based editor (such as Notepad or WordPad). By default, the file is located in: C:\Program Files\Hewlett-Packard\PNM\server\ config. Enter the IP address of the interface you want the application to attach to and save your changes. For example for the network illustrated above, you would add the entry "15.255.120.25" (without quotes) in the first line of the file. Only the first entry is recognized, and all other entries are ignored.
2. For a multi-homed Client, perform the same steps as for the Server. By default, the file is located in: C:\Program Files\Hewlett-Packard\PNM\server\ config.
3. For a multi-homed PCM Agent, you must create the file in the C:\Program Files\Hewlett-Packard\PNM\pcm-agent directory, and then enter the IP address you want the application to attach to.

Restart the application. If this is the ProCurve Manager Client or Agent, just restart the application. If this is the ProCurve Manager Server, you must restart the PCM services (HP ProCurve -Datastore, -Network Manager Server, and -Traffic Launch Service) from the Services control panel.

Using the PCM Server for Switch Web Help

For ProCurve devices that support the "Web Help" feature, you can use the PCM Server to host the switch help files for devices that do not have HTTP access to the HP Support Web site.

1. Go to the HP Support Web site to get the Device Help files:

http://www.hp.com/rnd/device_help/

2. Copy the Web help files to the PCM Server, under:

```
C:\program files\hewlett-packard\pnm\server\
webroot\rnd\device_help\help\hpwnd\webhelp
```

3. Add an entry, or edit the existing entry in the Discovery portion of the global properties (globalprops.prp) in PCM to redirect the switches to the help files on the PCM Server. For example:

```
Global {
TempDir=data/temp
...
    Discovery{
        ...
        ...
        DeviceHelpUrlRedirect=http://15.29.37.12:8040/rnd/
device_help
        ...
    }
}
```

You will enter the IP address for your PCM Server. 8040 is the standard port number to use.

4. Restart the Discovery process for the change to be applied. Refer to "Troubleshooting Discovery" on page 4-57 for details.

Note:

Changing the Discovery global properties file will redirect the Device Help URL for all devices.

If you just want to change the DeviceHelpUrl for a particular device, go to the Configuration tab on the Web UI for that device and select the Support/Mgmt URL button. Edit the entry in the Management Server URL field for the device to point to the PCM Server; for example:

```
http://15.29.37.12:8040/rnd/device_help
```

Configuring and Managing Agents

How Agents Work	3-2
Agent-initiated Connections	3-5
Server-initiated Connections	3-9
Configuring Unique SSL Certificates	3-16
Changing Agent Properties and Preferences	3-19
Properties	3-20
Proxy	3-21
Discovery	3-23
Device Access Preferences	3-37
Local Agent Memory Usage	3-49
Other Agent Manager Functions	3-50
Changing Server Setup	3-51
Viewing Agent Information	3-53
Downloading Files to Agents	3-55
To Download a File to Agents	3-55
To Remove a File from Agents	3-56
Managing Remote Agents Using the Web	3-57
Troubleshooting an Agent	3-58
After PCM Reinstallation	3-58
Remove Local Agent	3-60
Method 1	3-60
Method 2	3-61
Replace an Agent	3-62

How Agents Work

PCM v3's architecture allows you to logically divide the network and manage devices on remote segments of large networks connected by WAN or LAN links that might or might not be behind a NAT or other firewall. With PCM's architecture you can manage devices scattered geographically that were unreachable before, grant visibility and administration permissions for different parts of the network to different users, and ensure secure communication over insecure WAN or LAN links.

PCM's architecture relies on Agents deployed across the network that perform management operations on behalf of the PCM Server. A local Agent is configured on the PCM Server during installation. Remote Agents can be installed on PCs in remote locations. Up to 25 Agents (local and remote) can be installed

Remote Agent Usage

Agents can be installed on remote segments of the network as a Windows service by installing Agent software on a PC other than the PCM Server. In networks with more than 2000 discovered devices, we recommend that all Agents be remote. See "Remove Local Agent" on page 3-60 for instructions on replacing the local Agent with a remote Agent.

You can also add a remote Agent to your network by using an HP ProCurve ONE Services zl Module (J9289A) in either of the following ways:

- The HP ProCurve PCM+ Agent with ONE zl Module (J9496A) ships with a PCM+ Agent application pre-installed on a ProCurve ONE Services zl Module.
- If you have already installed a ProCurve ONE Services zl Module, you can install a PCM+ Agent application to run on it.

Before you can use a PCM+ Agent application installed on a ProCurve ONE Services zl Module, you must first activate and configure the Agent application. For more information, refer to the *HP ProCurve PCM+ Agent with ONE zl Module: Installation and Getting Started Guide*.

The PCM Server automatically connects to the local Agent, which is installed on the same PC as the PCM Server. The PCM Server does not automatically connect to remote Agents installed on other PCs, so you must either configure the remote Agent to initiate connections with the PCM Server or configure the PCM Server to initiate connections with the remote Agent. If a firewall or NAC appliance is between the PCM Server and a remote Agent, we recommend initiating the connection from the location within the firewall.

Agents are placed in Agent Groups to facilitate management. An Agent Group consists of one or more physical Agents and allows you to logically subdivide the management of your network(s) any way you wish. This changes the navigation tree structure used in previous versions of PCM.

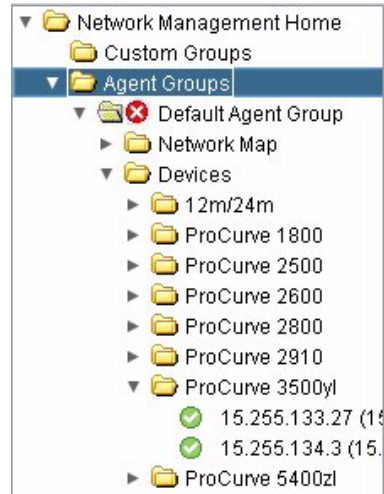










Figure 3-1. ProCurve Navigation Tree



Agents are configured with the Agent Manager, which is accessed by clicking the Agent Manager button on the global toolbar. Agents are listed on the Agents tab, which is accessed by selecting an individual Agent in the navigation tree. The Agent Manager is described on the following pages, and the Agents tab is described on page 3-53.

In addition to Agent Manager tabs, the Agent Manager also contains a toolbar of buttons at the top and the number of available Agent licenses at the bottom of the window. Toolbar buttons are used to perform the following management, diagnostic, and troubleshooting functions:

Button	Function
	The Add a new Agent button is used to configure an Agent, as explained in "To add the agent manually:" on page 3-13. Each Agent must have a unique name and IP address.
	The Clone selected Agent button is used to create an Agent using another Agent's properties as a template, as explained in "Clone Agent" on page 3-14. When cloning Agents, you must rename the new Agent and enter its IP address before activating the Agent.
	The Delete Agent button is used to remove an Agent definition that is not needed.
	The Replace Selected Agent button is used to copy the connection settings from one new healthy Agent to an old failed Agent.
	The Activate Agent button is used to enable an Agent so it can start performing PCM tasks.
	The Deactivate Agent button is used to disable the selected Agent so it cannot perform PCM tasks.
	The Move Subnets button transfers subnets from one Agent to another Agent, as explained on page 30.
	The Agent Utilities drop-down button contains the Ping, Logs, Agent File Manager, Restart, and Test Credentials functions explained in "Troubleshooting an Agent" on page 3-58.

Agent-initiated Connections

To configure an Agent to initiate communication with the PCM Server, perform the following steps.

The PCM Plus software base products (J9173A and J9174A) provide one license for the PCM Server and one license for only one PCM Agent. If you wish to use multiple PCM Agents, you must purchase an add-on incremental PCM license (J9175A) or an unlimited PCM license (J9176A or J9177A). Without a license for the additional PCM Agent, the PCM Server will not connect to the additional Agent(s).

Note:

In remote locations with firewalls, it may be easier to establish connections if the remote Agent initiates connections. If the PCM Server is configured to allow it and the entered passwords match, these Agents will automatically appear in the Agent Manager.

1. Download the Agent software from PCM Server by starting a Web browser such as Microsoft Internet Explorer on the computer where the Agent will be installed, and type the IP address of the PCM Server computer followed by a colon and the port ID 8040. For example, if the IP address of the Server computer is 10.15.20.25, enter the following URL:
`http://10.15.20.25:8040`
2. Click the **Download the Windows PCM/IDM agent** link, and click **Save** to download the file.
3. Once the download completes, close the Download window and the Web browser.

4. Double-click the downloaded file `procurve-agent-setup.exe` file to install the Agent software, and when prompted, configure the Agent as follows:

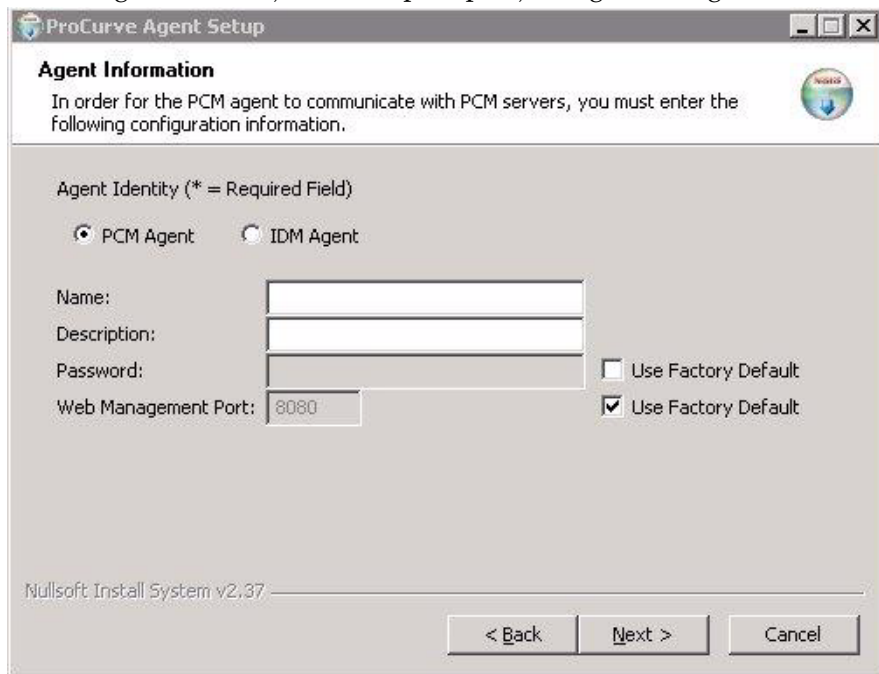


Figure 3-2. Install Agent - Agent Information

- a. Select PCM Agent.
- b. Type a Name and, optionally, a Description for the Agent.
- c. Enter a unique password or check the Use Factory Default check box to use the default password of “procurve”. This password is used for logging into the browser-based Agent UI (user name “admin”) and for authenticating with the PCM Server. The Agent entry in the Agent Manager on the PCM Server must be configured with this password.
- d. To change the default port (8080) used to open the browser-based Agent UI, uncheck the Use Factory Default check box and type the desired port number.
- e. Click **Next**.

You can change these settings at any PC with the browser-based Agent UI or at the PCM Server on the Agent Properties tab of the Agent Manager.

5. Configure the PCM Server settings as follows:

The screenshot shows the 'ProCurve Agent Setup' dialog box with the 'Server Information' tab selected. The dialog box contains the following fields and options:

- Agent-Server Connection Handling:** A section header with a horizontal line below it.
- Agent Initiates Connection:** A checkbox that is currently unchecked.
- Port:** A text box containing '51111' and a 'Use Default' checkbox that is checked.
- Encryption:** A dropdown menu showing 'SSL' and a 'Use Default' checkbox that is checked.
- PCM Server Information:** A section header with a horizontal line below it.
- IP Address:** An empty text box.
- Password:** An empty text box and a 'Use Default' checkbox that is unchecked.

At the bottom of the dialog box, there is a status bar that reads 'Nullsoft Install System v2.37' and three buttons: '< Back', 'Next >', and 'Cancel'.

Figure 3-3. Install Agent -Server Information

For the Agent to communicate with the PCM Server, these values **MUST MATCH** the values set on the PCM Server for this Agent.

- a. If the Agent will initiate connection to the PCM Server, check the Agent Initiates Connection check box. If the PCM Server will initiate a connection to the Agent, ensure this check box is unchecked.

All Agents that initiate a connection to the PCM Server must use the same port number and encryption type as configured in the Agent Manager Server Setup tab.

- b. For Port, you can change the default Port that the Agent uses to communicate with the PCM Server by unchecking the Use Default check box and enter the new port number. The default PCM Server port is 51111, which can be changed to any unused port during PCM Server installation or at the PCM Server.

Note: HP recommends that you use the default port.

- c. If you do not want to encrypt data sent to the PCM Server, uncheck the related Use Default check box and select Plain Text from the Encryption drop-down list. The default encryption method is SSL. If the PCM Server is behind a firewall, we recommend using SSL encryption.

- d. In the IP Address field, type the IP address of the PCM Server if the Agent is initiating the connection to the PCM Server. The Agent Initiates Connection check box must be checked to activate this field.
- e. Enter a unique password or check the Use Default check box to use the default password of “procurve”. This must match the password set on the Agent Manager Server Setup tab.
- f. Click **Next**.

You can change these settings at any PC with the browser-based Agent UI or at the PCM Server on the Server Setup tab of the Agent Manager.

6. In the Choose Start Menu Folder window, enter or select the folder in which you want to store PCM Agent files and click **Install**.
7. When the installation finishes, click **Next**.
8. Click **Finish** to exit the Agent Setup wizard.
9. If necessary, configure additional properties and preferences, as explained in “Changing Agent Properties and Preferences” on page 3-19.

Important: When an Agent is configured for a server-initiated connection, you **MUST** create and configure the Agent on the PCM Server using the Agent Manager.

10. If necessary, move the Agent to another Agent Group. By default, all new Agents that initiate connections are placed in the Default Agent Group.

Note:

Once an Agent is activated, it cannot be moved to another Agent Group.

11. Identify the seed device that the Agent will use as a starting point for Discovery. To do so, enter the IP address of the seed device of the General subtab on the Discovery tab of the Agent Manager.



12. Before an Agent can be used for PCM tasks, you must change the Agent's state to Active by clicking **Activate Agent** on the Agent Manager toolbar. The Agent will then be added to the Agents tab under the Agent Groups node and to the navigation tree under the appropriate Network Map node. However, only active (operational) Agents are shown in the navigation tree. If the Agent fails to connect, it will change to a state different from Active (e.g., unlicensed, wrong Agent credentials, wrong Server credentials) and be removed from the navigation tree.

Server-initiated Connections

Remote Agents can be configured during installation to initiate connections with the PCM Server or to wait for the PCM Server to initiate the connection. Perform the following steps to configure an Agent that waits for the PCM Server to initiate the connection (once the Agent is configured on the PCM Server).

Note:

In remote locations with firewalls, it may be easier to establish connections if the remote Agent initiates connections.

1. Download the Agent software from PCM Server by starting a Web browser such as Microsoft Internet Explorer on the computer where the Agent will be installed, and type the IP address of the PCM Server computer followed by a colon and the port ID 8040. For example, if the IP address of the Server computer is 10.15.20.25, enter the following URL:
`http://10.15.20.25:8040`
2. Click the **Download the Windows PCM/IDM agent** link, and click **Save** to download the file.
3. Once the download completes, close the Download window and the Web browser.

4. Double-click the downloaded file `procurve-agent-setup.exe` file to install the Agent software, and when prompted, configure the Agent as follows:

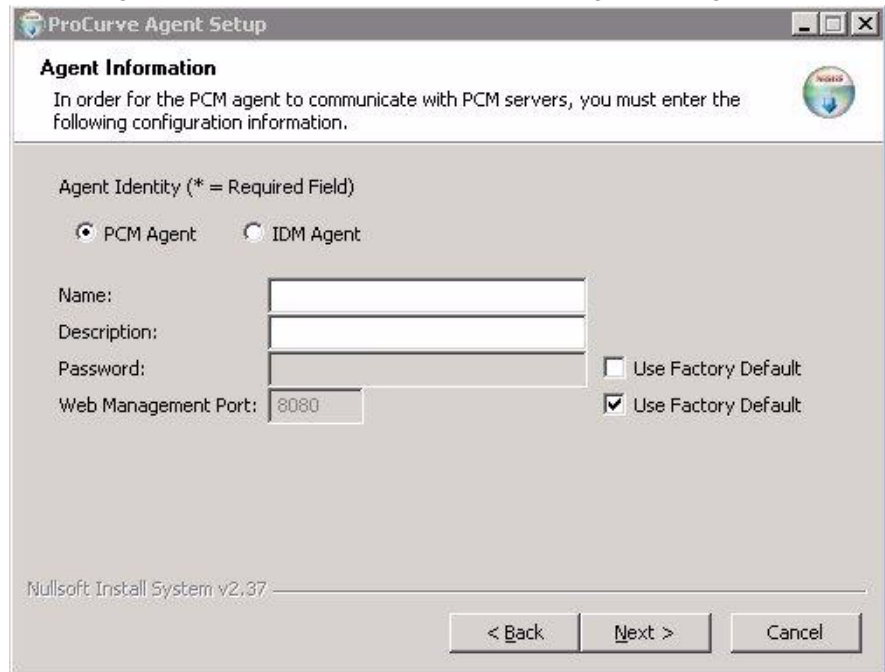


Figure 3-4. Install Agent - Agent Information

- a. On the Agent Information window, ensure PCM Agent is selected.
- b. Type a unique name that will be used to identify the Agent.
- c. Optionally, type a brief description (typically identifies the Agent location or purpose).
- d. To use the default Agent password (`procurve`) that the PCM Server uses to authenticate the Agent, check the Use Factory Default check box. To create a unique password, leave the Use Factory Default check box unchecked and type the new password.
- e. To change the default port (8080) used to connect to the Agent UI through a Web browser, uncheck the Use Factory Default check box and type the desired port number.
- f. Click **Next**.

5. Configure the PCM Agent-Server connection handling as follows:

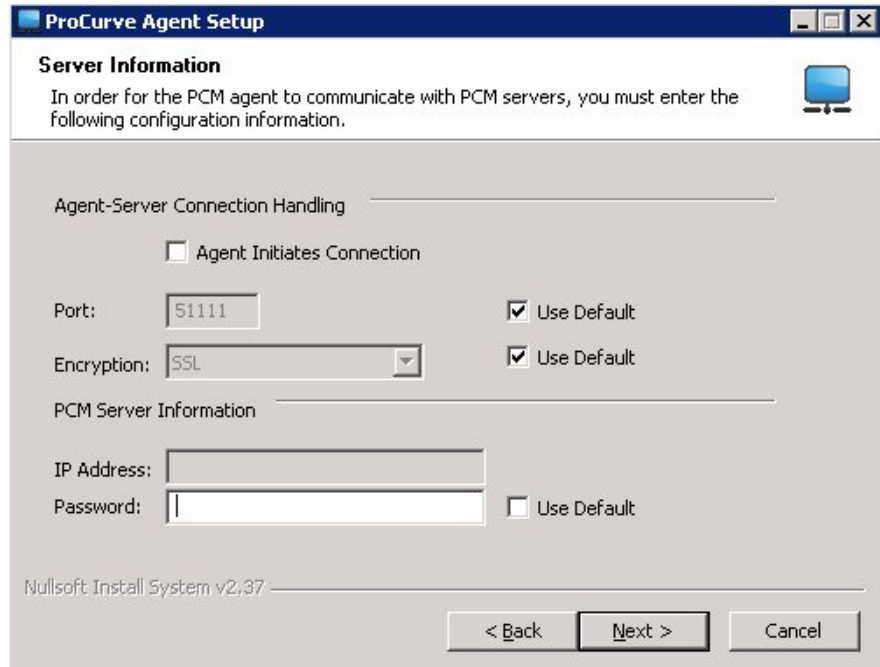


Figure 3-5. Install Agent -Server Information

- a. On the Server Information window, **DO NOT CHECK** the Agent Initiates Connections check box.
- b. If desired, uncheck the Use Default check boxes and change the port used on the PC containing the Agent and the encryption method for Agent and PCM Server connections.
- c. To use the default PCM Server password (`procurve`) to connect to this Agent, check the Use Default check box. To create a unique password, leave the Use Factory Default check box unchecked and type the new password.

You can change these settings at any PC with the browser-based Agent UI or at the PCM Server with the Agent Manager.

Record the Agent's IP address, password, port number, and encryption mode. You will need it when you open the Agent Manager to configure this Agent.

- d. Click **Next**.
6. In the Choose Start Menu Folder window, enter or select the folder in which you want to store PCM Agent files and click **Install**.

Configuring and Managing Agents
Server-initiated Connections

7. When the installation finishes, click **Next**.
8. Click **Finish** to exit the Agent Setup wizard.
9. At the PCM Server or Client, click Agent Manager on the global toolbar to start the Agent Manager:

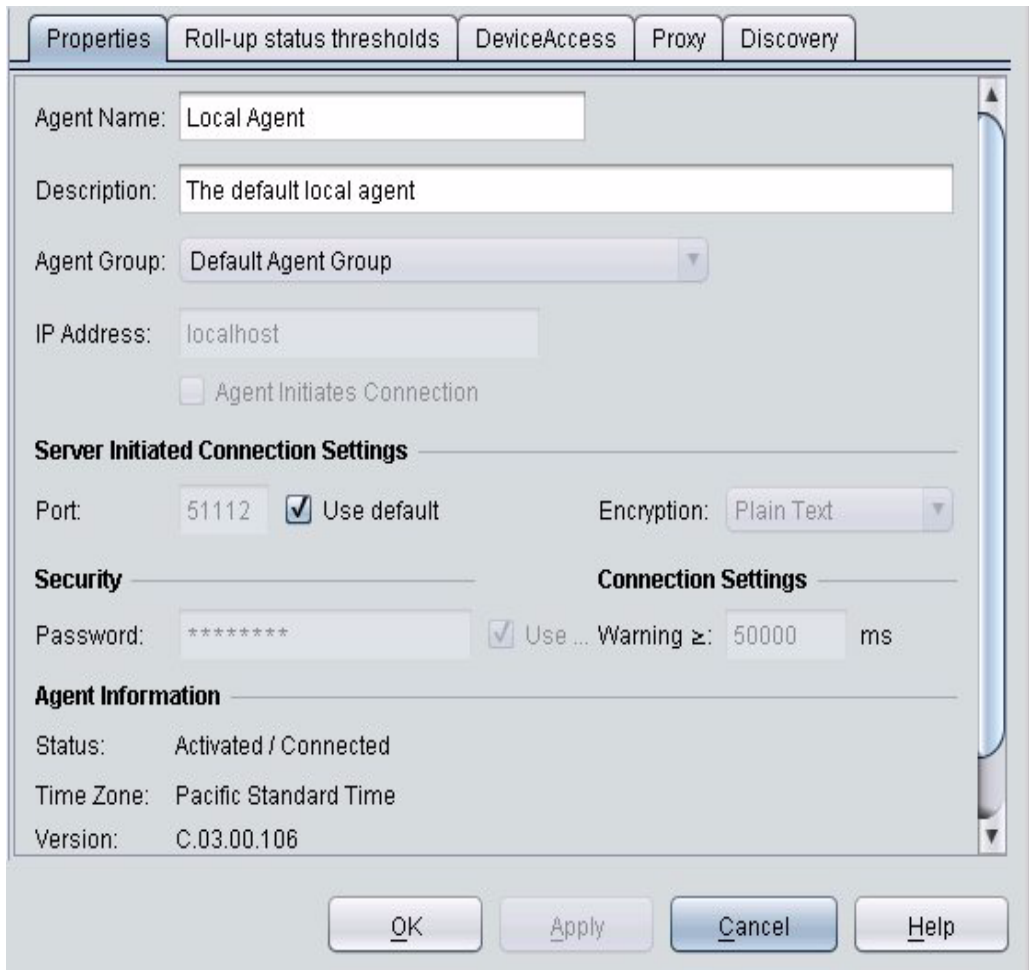


Figure 3-6. Agent Manager

10. Add the Agent manually or by cloning.

To add the agent manually:

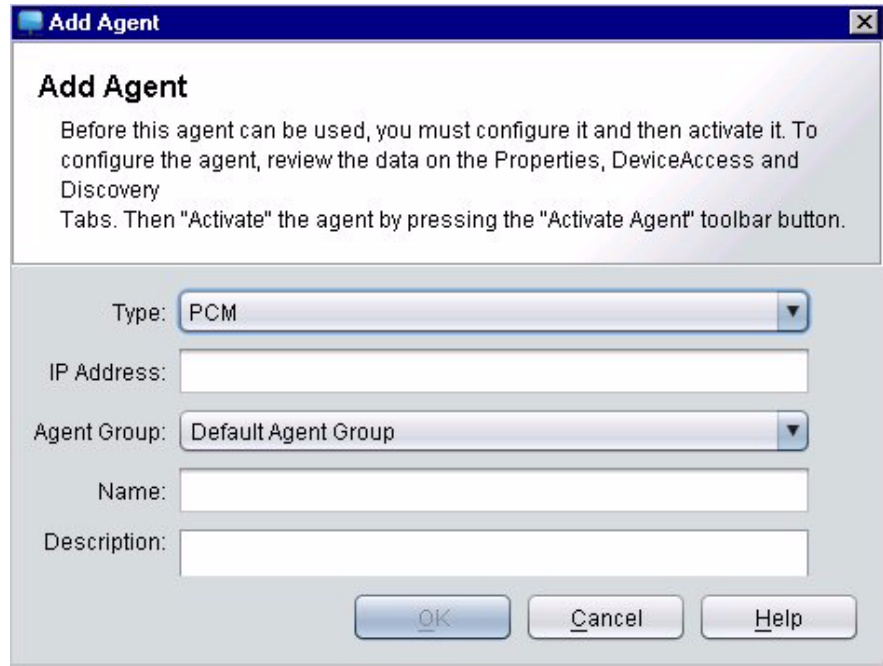


Figure 3-7. Add Agent



- a. Click the Add Agent button on the Agent Manager toolbar.
- b. Select PCM as the Type.
- c. In the IP Address field, type the IP address of the Agent.
- d. Click the Agent Group drop-down arrow and select the Agent group where the Agent will be added.

Note:

Once you activate an Agent, you will not be able to change its Agent Group.

- e. Type the name you want to assign to the Agent.
- f. Optionally, type a brief description of the Agent.
- g. Click **OK**, which closes the Add Agent window and displays the new Agent in the left pane of the Agent Manager window and all other Agent-related configuration tabs.

You can also add the Agent by cloning, which creates an Agent using another Agent's properties as a template.

To clone an existing Agent:

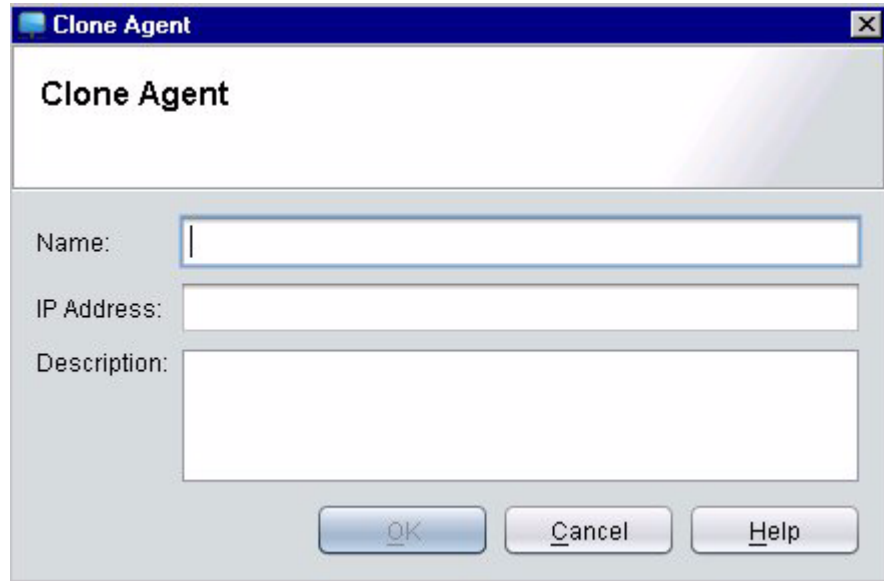



Figure 3-8. Clone Agent



- a. Select the Agent to be cloned from the Agent Manager navigation tree.
- b. Click Clone Selected Agent on the Agent Manager toolbar.
- c. In the Name field of the Clone Agent window, type the name you want to assign to the Agent.
- d. In the IP Address field, type the IP address of the Agent being configured.
- e. Optionally, type a brief description to help identify the Agent or its location.
- f. Click **OK**, which closes the Add Agent window and displays the new Agent in the left pane of the Agent Manager window and all other Agent-related windows.
- g. Optionally, change one or more Agent properties, as explained in “Changing Agent Properties and Preferences” on page 3-19.

11. The Agent is now configured. If necessary, configure additional properties and preferences, as explained in “Changing Agent Properties and Preferences” on page 3-19. For example, if there is a firewall between the PCM Client and the devices, the Server and Agent managing those devices can use a proxy to bypass the firewall in a secure manner.
12. Identify the seed device that the Agent will use as a starting point for Discovery. To do so, enter the IP address of the seed device of the General subtab on the Discovery tab of the Agent Manager.
13.  When you want the Server to connect to the Agent and start using it for PCM tasks, change the Agent's state to Active by clicking **Activate Agent** on the Agent Manager toolbar. The Agent will then be added to the PCM Agents tab under the Agent Groups node and to the navigation tree under the Network Map node. However, only active (operational) Agents are shown in the navigation tree. If the Agent fails to connect, it will change to a state different from Active (e.g., unlicensed, wrong Agent credentials, wrong Server credentials) and be removed from the navigation tree.



To disable an Agent so it cannot perform PCM tasks, select the Agent to be deactivated and click the **Deactivate Agent** button.

Configuring Unique SSL Certificates

In PCM agent-initiated and server-initiated communication, the default encryption method is SSL.

By default, the same self-signed SSL certificates are used by all Agents and the PCM Server in a PCM installation. A common certificate resides on each Agent and is used in server-initiated connections. A different certificate resides on the PCM Server and is used in all agent-initiated connections.

You can configure additional security for SSL connections so that each Agent and the PCM Server generate a unique SSL certificate for server-initiated and/or agent-initiated communication.

- After you configure the use of unique SSL certificates for *server-initiated* connections, when the PCM Server connects to a remote agent, the Agent generates a unique SSL certificate for its Agent/Server communication. The PCM Server is updated with the new Agent-specific public key and maintains a public key for each PCM Agent in the network. Server-initiated connections with the Agent from other PCM Servers will be blocked.

Warning: Configuring the use of unique SSL certificates locks an Agent to the PCM Server in server-initiated connections.

- In order for an Agent to use another PCM Server, you must restore the default SSL certificate on the Agent by using the Agent's web-based management interface.
 - If you re-install PCM on the Server, you must restore the default SSL certificate on *all* remote Agents by using the Agent's web-based management interface.
- After you configure the use of unique SSL certificates for *agent-initiated* connections, the PCM Server generates a new SSL certificate unique to the PCM installation. The new certificate's public key is automatically installed on each configured and connected remote Agent.

Warning: A new Agent or an Agent that was not connected at the time the certificate was generated will not be able to start an SSL connection with the Server until the Agent receives the new public key. You must manually install the public key on a remote Agent by using the Agent's web-based management interface.

The public key file (`agent_server_key.cert`) is stored in the `PCM_install_dir/server/config` directory on the Server. You must be able to access the public key file from the browser used to connect to the Agent's web management interface.

To generate a unique SSL certificate for use in server-initiated and/or agent-initiated connections:

1. Open the SSL Connection Security window in one of the following ways:



- Click the Preferences button in the toolbar and select SSL Connection Security.
- Select Tools > Preferences > SSL Connection Security.

2. In the SSL Connection Security window:

- To create a unique SSL certificate for each PCM Agent that is used in *server-initiated* connections, select the **Generate unique agent certificates** check box.
- To create a unique SSL certificate that PCM Agents use to connect to the Server in *agent-initiated* connections, click **Generate Now**. Only Agents that are configured and currently connected to the Server are updated.

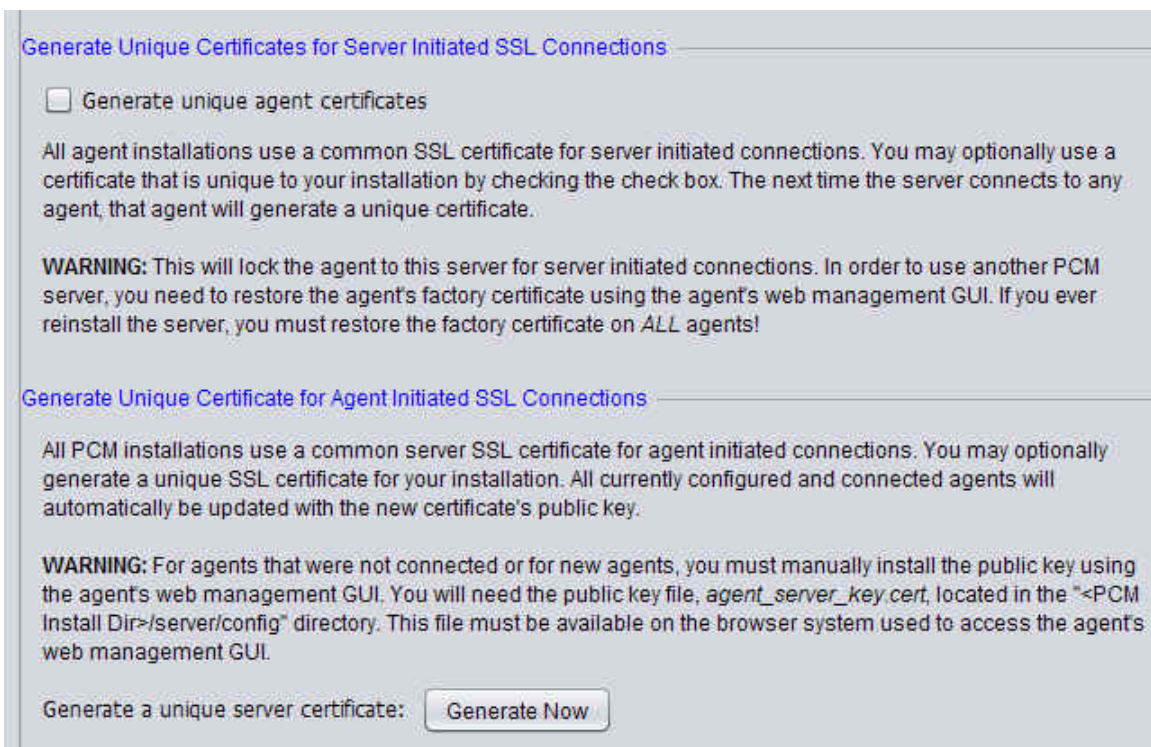


Figure 3-9. Configuring Unique SSL Certificates for Agent/Server Connections

3. Save your changes:
 - To save your changes and leave the Preferences window open, click **Apply**.
 - To save your changes and exit the window, click **OK**.

Changing Agent Properties and Preferences



Several properties and preferences can be set for Agents by using the Agent Manager tabs and toolbar. To access the Agent Manager, click the Agent Manager button on the global toolbar. To save your changes and exit the Agent Manager, click **Ok**. To save your changes and leave the Agent Manager open, click **Apply**.

The Agent Manager contains two panes. The left pane contains a PCM tab, which displays all PCM Agents detected by the PCM Server, and an IDM tab (if IDM is installed), which displays all IDM Agents detected by the PCM Server. See the *IDM User's Guide* for additional IDM information.

The right pane contains tabs of information for the PCM Agent selected in the left pane. Use these tabs to configure the following properties and preferences.

Properties

To initially configure or change one or more Agent properties, click the Properties tab in the Agent Manager and enter the following properties:

The screenshot shows a dialog box titled 'Agent Properties' with several tabs: 'Properties', 'Roll-up status thresholds', 'DeviceAccess', 'Proxy', 'Discovery', and 'NIM'. The 'Properties' tab is active. The dialog contains the following fields and sections:

- Agent Name:** Western
- Description:** (empty text box)
- Agent Group:** Default Agent Group (dropdown menu)
- IP Address:** 15.255.134.235
- Agent Initiates Connection
- Server Initiated Connection Settings:**
 - Port: 51111
 - Use default in PCM
 - Encryption: SSL (dropdown menu)
- Security:** Password: ****
- Connection Settings:** Warning ≥: 50000 ms
- Agent Information:** Status: Activated / Connected

At the bottom of the dialog are four buttons: OK, Apply, Cancel, and Help.

Figure 3-10. Agent Properties

Note:

The Agent Manager Properties tab displays all defined properties for the selected Agent and is used to edit these properties. Note that in addition to remote Agents, each PCM Server includes a predefined local Agent. Some properties for the local Agent cannot be modified.

1. Ensure the PCM tab in the left pane of the Agent Manager is selected and then select the Agent that you want to configure.
2. In the Agent Name field of the Properties tab, type the name you want to assign to the Agent. This name must match the Agent name defined on the Agent.
3. Optionally, in the Description field, type a brief description to help identify the Agent.
4. Use the Agent Group drop-down list to select the Agent group to which the Agent is assigned. The Agent group cannot be changed once an Agent is activated.

5. Type the IP address of the Agent.
6. Use the Agent Initiates Connection check box to configure whether the Server or Agent is initiating the connection. Note that the Port and Encryption fields are disabled (not used) if the Agent initiates the connection. These settings are taken from the Agent Manager Server Setup tab.
7. Check the Use default check box to use the default port (51111 for remote Agents (port 51112 is used for the local Agent).

OR

Uncheck the Use default check box and type the Port that the PCM Server will use to connect to the Agent.

8. Select the encryption type used for connections between the Agent and the PCM Server. By default, the local Agent uses Plain Text encryption, and remote Agents use SSL encryption.
 - SSL encrypts all messages in both directions.
 - Plain Text does not encrypt communication between the PCM Server and the Agent.

Note:

The Encryption, IP address, and Port fields are disabled when Agent Initiates Connection is enabled (checked). The Port field is disabled if Use default in PCM is enabled.

9. To use an authentication password other than the default, uncheck the Password Use default check box and in the Password field type the password the PCM Server will use to authenticate the Agent. The password in this field must match the password defined for the PCM Agent during Agent installation. The default password is `procurve`, which can be changed during PCM Agent installation.
10. To override the default connection thresholds for this Agent, type the Warning connection threshold (in milliseconds). The default Warning threshold is 50,000 ms. For example, if you enter a value of 50,000 ms, when the connection latency between this Agent and the Server is greater than or equal to 50,000 ms it will be categorized as Warning.

Proxy

If a firewall lies between the PCM Client and the devices, the Server and Agent managing those devices can use a proxy to bypass the firewall in a secure manner, which provides HTTP, Telnet and SSH proxy redirection. Devices then can be remotely configured via CLI (Telnet and SSH) or via a Web configuration page.

When the PCM Client and Agent are in the same network or in networks that can be reached directly with no intervening firewall, the connection to the devices via CLI or Web is performed directly. Therefore, a proxy is not needed.

To enable a proxy:

In the Agent Manager left pane, select the Agent requiring a proxy and click the Proxy tab:



Figure 3-11. Agent Proxy Tab

1. Check the Enable proxy check box.
2. To use the default proxy port (identified in the Server Setup tab), check the Use default in PCM check box. If checked, the Server will assign port numbers automatically from the Proxy port range defined on the Server Setup tab.
3. To set a specific proxy port to be used for the Agent, ensure the Use default in PCM check box is not checked and type the port number in the Proxy port field.
4. When configuring an Agent to use a proxy, you must configure your Web browser to use a Proxy auto-configuration file to be able to open device Web configuration pages. The file is located at:

`http://<server IP address>:8040/pac/pcm_autoproxy.pac`

The PCM Client should now be able to communicate with devices managed by the Agent, whether it is via Telnet, SSH or Web.

Discovery

The Agent Manager Discovery tab contains subtabs where you can configure General Discovery settings, exclude devices from Discovery, configure managed subnets, and start, stop, and schedule Discovery processes.

General Preferences

Configure the device where discovery starts, ping sweep settings, and status polling settings in the General subtab on the Agent Manager Discovery tab. You can also start and stop discovery from this tab.

To enable or disable discovery:

1. Select the Agent from the left pane of the Agent Manager, click the Discovery tab in the right pane, and then click the General subtab:

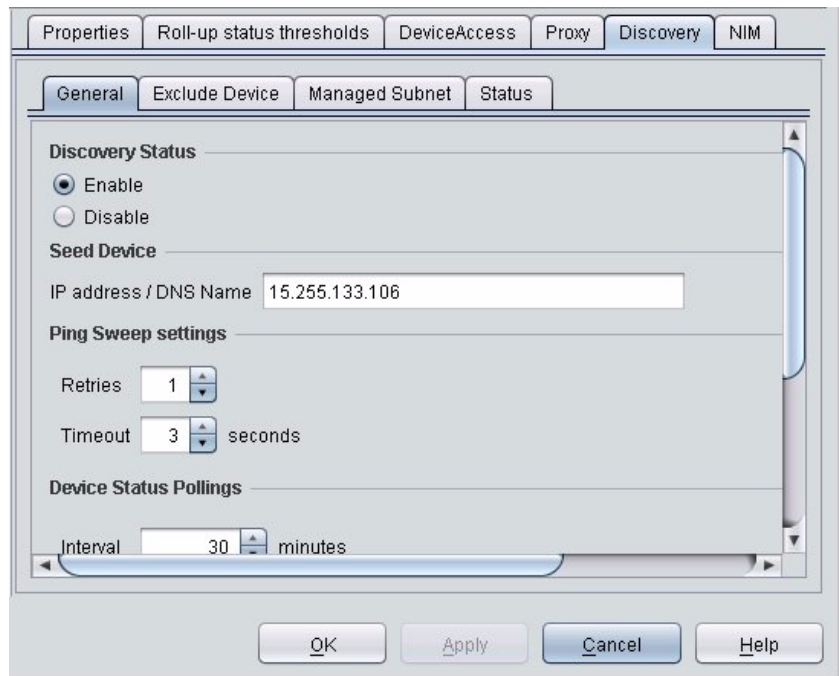


Figure 3-12. Agent Discovery - General Subtab

2. To enable the Agent to discover devices, click the **Enable** button.

Note:

Individual discovery processes can be enabled and disabled in the Status subtab of the Agent Manager Discovery tab.

3. To disable discovery, click the **Disable** button.

To change discovery preferences:

1. To change the device from which discovery starts (core ProCurve device or default gateway), type the IP address of the seed (starting) device in the IP address field of the General subtab of the Agent Manager Discovery tab. If the IP address entered is invalid or has been discovered by another Agent in the same Agent group, PCM Discovery ignores the entry and continues to use the last valid starting device.

The seed device can be any SNMP network device that is reachable from the selected Agent and has not been discovered by another Agent in the same Agent group. However, we recommend the seed device be a supported ProCurve switch (not a router or routing switch) that is a core switch (not an edge switch that is primarily connected to end nodes).

When using PCM for NNM, the starting device is the NNM server and cannot be changed. Therefore, the Starting Device option is not shown or disabled.

2. To change the number of times PCM tries (0-5 retries) to reach a device during the ping sweep phase of discovery, click the ping sweep Retries up or down arrow to display the desired number of retries. You can also type the number of retries.

If a ping response is not received from a device before timeout, Discovery will retry the ping the specified number of times before ending discovery of the device.

3. To change the number of seconds to wait for a response before the ping sweep times out, click the Timeout up or down arrow to display the desired number of seconds. You can also type the number of seconds.

Discovery will wait the specified number of seconds (1-10 seconds) for a response from the device. If a response is not received within that time, Discovery retries the ping until the specified number of ping retries is reached. If the number of retries is reached and Discovery has not received a reply, discovery of the device is ended at that IP address.

4. To change the status polling interval, click the polling Interval up or down arrow to display the number of minutes between status polling scans. You can also type the number of minutes.

Status polling monitors the status of managed devices. Setting the polling interval to 0 disables status polling.

5. To change the number of times to retry a device if a polling response is not received, click the polling Retries up or down arrow to display the desired number of retries. You can also type the number of retries.

When a polling response is not received from a device, the device state is changed to a yellow warning. If a response is not received during the next poll, the device state is changed to a red Unreachable.

6. To change the number of seconds to wait for a polling response, click the polling Timeout up or down arrow to select the number of seconds to wait. You can also type the number of seconds.
7. To automatically register the Agent as a Trap Receiver for newly discovered devices, check the Automatically register as a Trap Receiver for new devices check box.
8. If you have added user-defined devices, click the **Rescan for user-defined devices** button to launch a scan for user-defined devices and add any discovered user-defined devices to the navigation tree.

Devices Excluded from Discovery

All devices that are excluded from discovery by the Agent are shown on the Exclude Device subtab of the Agent Manager Discovery tab. A device can be excluded from all subsequent discoveries by adding a device to the Excluded Devices list for an Agent. Excluding a device removes it from the managed devices of an Agent and excludes it from all subsequent discoveries. An excluded device can be included in discoveries and become a managed device again by removing it from the Excluded Devices list.

To exclude a device from Discovery:

In the navigation tree, right-click the device to be excluded and select Exclude Device from the drop-down list

OR

In a device-related window, right-click the device to be excluded, select Discovery from the drop-down list, and then select Exclude Device from the Discovery drop-down list.

To include an excluded device in Discovery:

1. Select the Agent from the left pane of the Agent Manager, click the Discovery tab in the right pane, and then click the Exclude Device subtab:

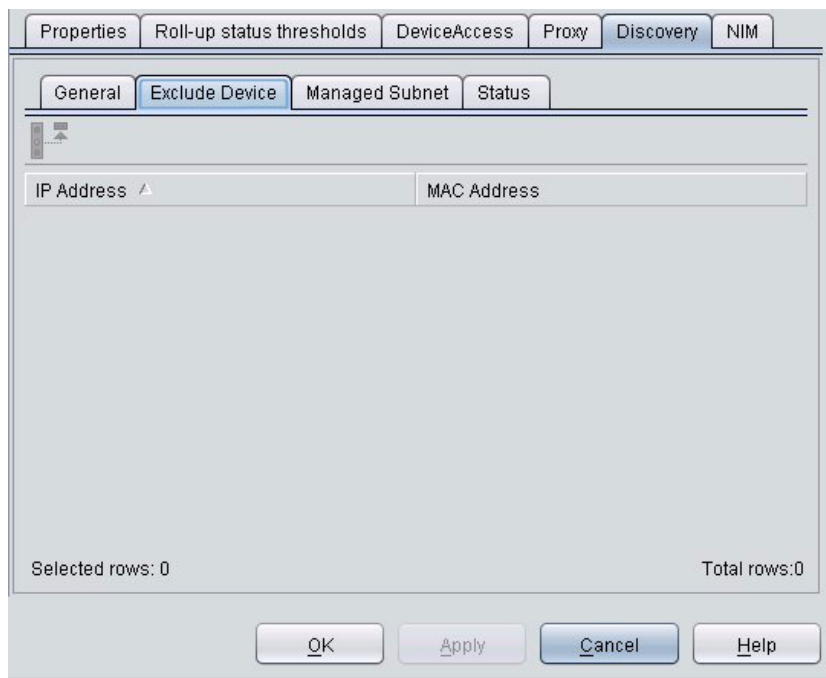


Figure 3-13. Agent Discovery - Exclude Device Subtab

2. Select the device to be removed from the Excluded Devices list and added to managed devices.

If you want to rediscover the device immediately after removing it from excluded devices, record the IP address.



3. Click the Remove from Excluded Devices List button on the Exclude Device toolbar.

The device will be discovered automatically the next time discovery runs.

4. Once the selected devices are removed from the window, click **Ok** to close the window.
5. To rediscover the device immediately without running a complete discovery, run the Manual Discovery Wizard.

Managed Subnets

From the Agent Manager Discovery tab, you can open the Managed Subnet subtab to configure the subnets you want to include and exclude in Discovery.

The subnets listed under Managed subnets are included in the Discovery process; the subnets listed under Unmanaged subnets are other subnets detected by Discovery:

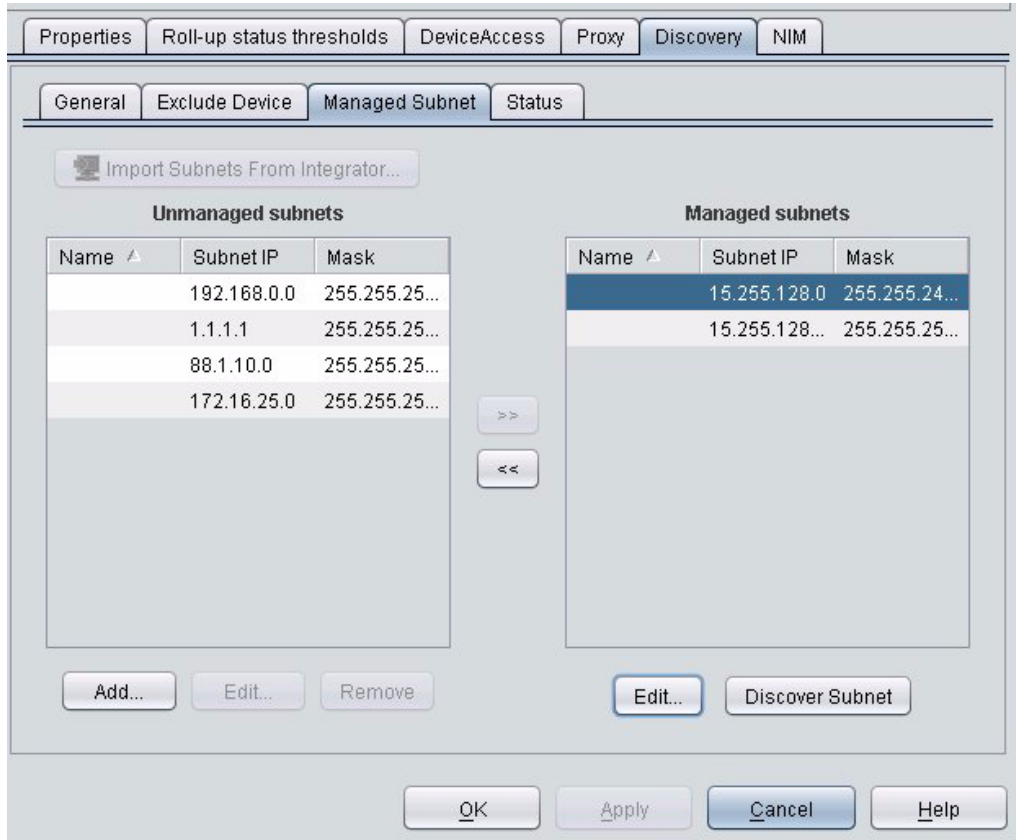


Figure 3-14. Agent Discovery - Managed Subnets Subtab

- A subnet can be managed by more than one Agent as long as the Agents belong to different Agent groups. Also, you can move subnets between Agents.

- Loopback IP addresses are sometimes listed as a managed or unmanaged subnet. Loopback IP addresses are discovered only when the IP subnet is a managed subnet for the selected Agent. If the loopback IP address is not reachable, PCM discovers the loopback IP address as a subnet and places it in the unmanaged subnets list.

To add a subnet from the local network to the discovery process:

1. In the Managed Subnet subtab, select a subnet address in the Unmanaged Subnets list and click >>.
2. Click **Apply** to save your changes.
3. Start the Discovery process to incorporate your changes by using the Status subtab, as described in “Enabling and Disabling Discovery Processes” on page 4-29.

To add a subnet from a remote network to the discovery process:

1. In the Managed Subnet subtab, click **Add**. The New Subnet window is displayed.

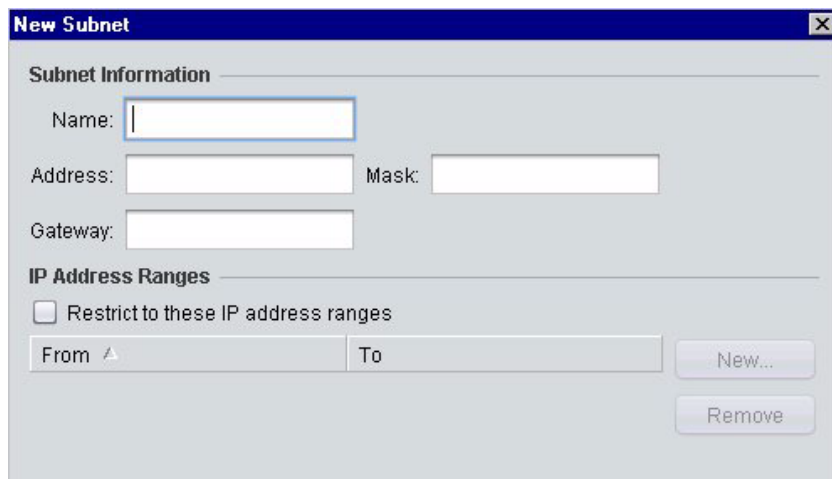


Figure 3-15. Agent Discovery - Add Subnet

- a. In the Name field, type a name to identify the subnet.
- b. In the Address field, type the network IP address to identify the subnet. A subnet can be managed by more than one Agent as long as the Agents belong to different Agent groups.
- c. In the Mask field, type the mask IP address for the subnet.
- d. In the Gateway field, type the gateway IP address used by the subnet.
- e. To discover only devices that are within an IP range:

- Check the Restrict to these IP address ranges check box and click **New**.
If Restrict to these IP address ranges is checked, you must enter at least one IP address range.
 - In the New IP Range window, type the beginning and ending IP addresses for each range in the Beginning address and Ending address fields. (Multiple IP address ranges within a subnet can be discovered.)
 - Click **OK** to save your entries and close the New Subnet window.
- f. In the Unmanaged subnets pane of the Managed Subnet subtab, select the new subnet and click **>>** to add it to managed subnets.
- Ping sweep discovery will discover all devices with the designated IP addresses.
2. To change a managed subnet to an unmanaged subnet or delete the subnet from the discovery process:
- a. Select the subnet address in the Managed Subnets list and click **<<**.
 - b. Select the subnet address in the Unmanaged Subnets list and click **Remove**.
 - c. When you are prompted that the devices which belong to the selected subnet will be removed from the PCM database, click **OK**.
3. Click **Apply** to save your changes.

To remove a subnet from the discovery process:

1. In the Managed Subnet subtab, select a subnet address in the Managed Subnets list and click **<<**.
2. Click **Apply** to save your changes.

To manually run discovery on selected subnets:

You can use the Managed Subnet subtab to discover devices on demand using a manual Ping Sweep discovery (see “Manual Ping Sweep Discovery” on page 4-3).

This feature is especially useful when you want to discover certain subnets before other subnets, which are automatically added as a result of auto-discovery, or in a large network with hundreds of managed subnets in which a discovery cycle can take several days to complete.

1. In the Managed Subnet subtab, select one or more managed subnets and click the **Discover Subnet** button.
2. When prompted to confirm the Ping Sweep discovery, click **Yes**.

A Ping Sweep discovery is performed on the selected subnets to check for new and undiscovered devices.

To move a managed subnet to another Agent:

Note:

The PCM Server must be shut down to move subnets across Agents. Therefore, we recommend you use this wizard during a low traffic period to minimize the traffic statistics lost.



1. Click the Move Subnets Wizard button on the Agent Manager toolbar, which opens the wizard, and then click **Next**.

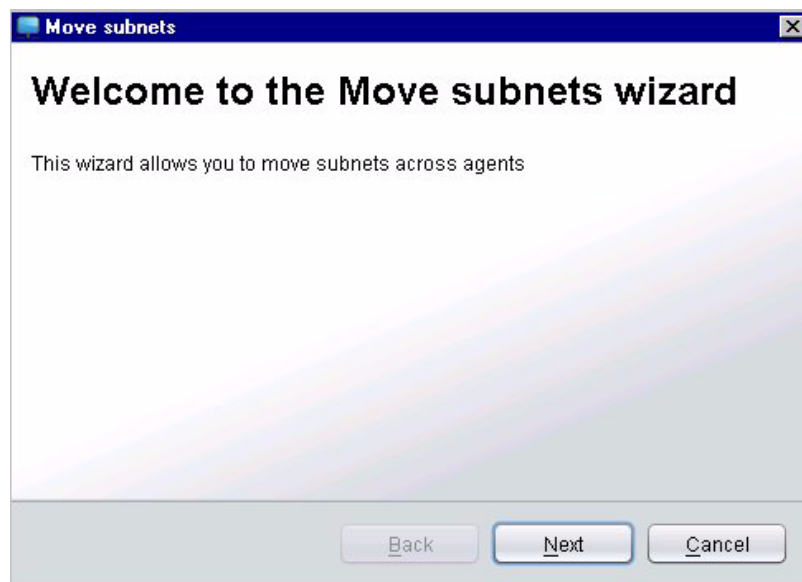


Figure 3-16. Agent Discovery - Move Subnets Wizard

2. Select the subnet to be moved and the source and destination Agents.



Figure 3-17. Agent Discovery - Move Subnets

- a. Use the **Source Agent** drop-down list to select the Agent currently managing the subnet(s) to be moved, which displays the list of subnets managed by the selected Agent.
- b. When the list of subnets currently assigned to the selected Agent is displayed, using standard Windows conventions select one or more subnets to be moved to another Agent.
- c. Use the **Destination Agent** drop-down list to select the Agent to which the selected subnets will be moved. (Agents are listed alphabetically by the Agent Group to which they belong and then by Agent name within each Agent Group.)
- d. Click **Move Subnets**.
- e. Repeat the preceding steps for all subnet movement between Agents.
- f. Click **Next**.

3. When the Confirm Subnet Movement window appears, confirm the correct subnets, source Agents, and destination Agents are shown.



Figure 3-18. Confirm Subnet Movement - Move Subnets

- a. Navigate through the subnet confirmation tree by clicking on folders to expand or minimize its contents.

You can easily identify the Subnets, Agents, and Agent Groups being changed because they are highlighted in magenta. The moved subnets are listed under the destination Agent and identify the source Agent.

- b. If you detect an error, use the **Back** button to return to the Agents and Subnets window and correct the error.
- c. After confirming the correct subnets are being moved as intended, click **Next**.

4. Optionally, configure trap receivers and authorized managers for the subnet being moved:

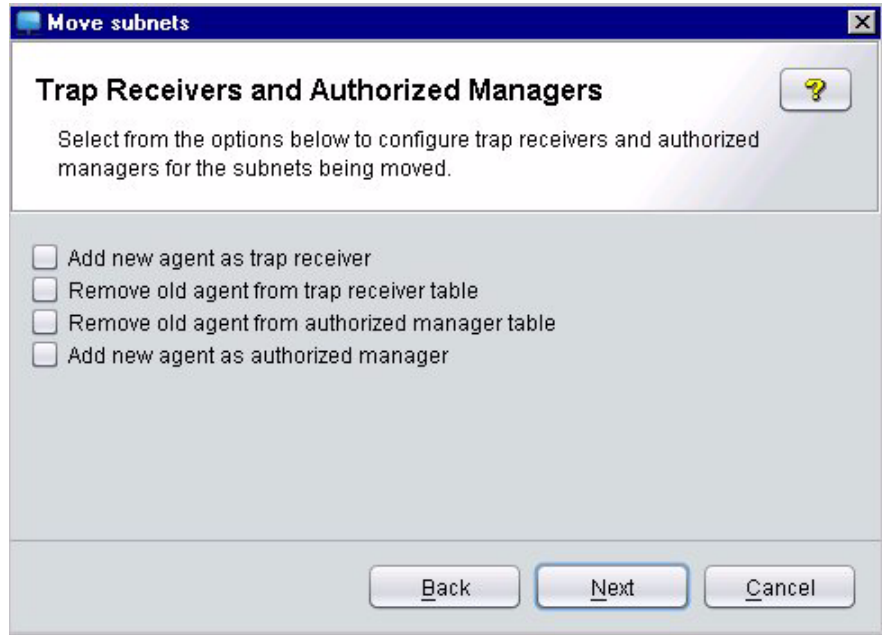


Figure 3-19. Agent Discovery - Move Subnets, Trap Receivers

- a. Check the check box next to each change you want to make to the configuration on the device.
 - b. Click **Next**.
 - c. When the confirmation prompt appears, confirm that you want to shut down PCM and click **OK**.
5. If you made configuration changes in the Trap Receivers and Authorized Managers window, select the location on the PCM Server where you want to store the configuration change results file.

This window is displayed only when trap receivers or authorized managers were configured on the previous window.

- a. Either type the complete path or use the **Browse** button to select the location.
- b. Click **Next**.

Note:

Clicking **Next** on this window will shut down the PCM Server and disconnect all Clients connected to the PCM Server.

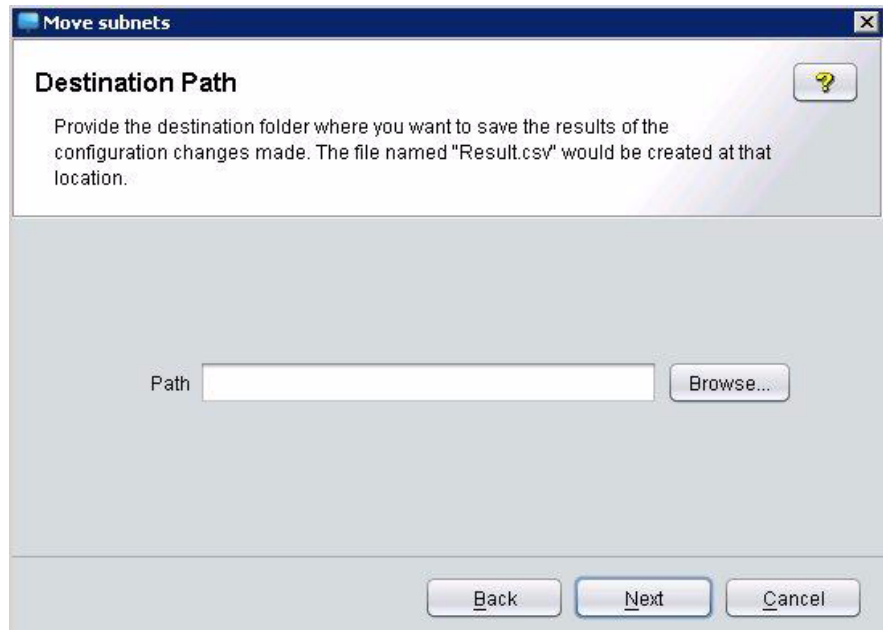


Figure 3-20. Destination Path - Move Subnets

6. Review the results to ensure you selected the subnet you want to move and the correct destination Agent.

Once the device configuration changes are completed, PCM is shut down so the subnet can be moved to the new Agent. PCM is not automatically restarted, so you must manually restart the PCM Server.

Status of a Discovery Process

Each Discovery process can be manually started, stopped, or scheduled for execution. The Status subtab of the Agent Manager Discovery tab displays the current status of each Discovery process:

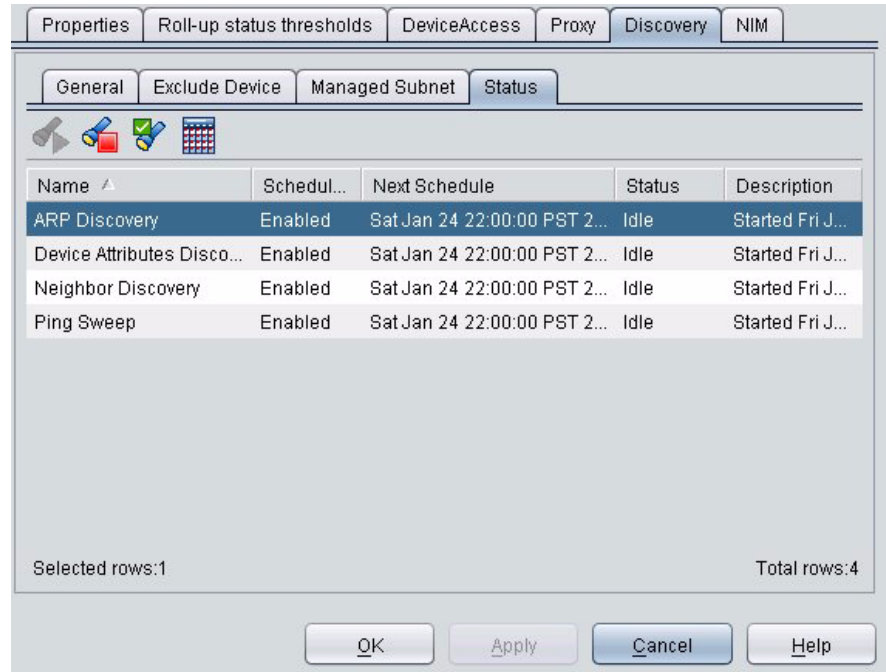


Figure 3-21. Agent Discovery - Status Subtab

By default, Discovery automatically runs when the Agent starts. PCM also provides default Discovery process schedules, which can be modified, disabled, or enabled after it has disabled.

To start, stop, or restart Discovery:

1. In the Managed Subnet subtab of the Agent Manager Discovery tab, ensure that all subnets to be discovered and managed are listed in the Managed Subnet list.
2. In the Network Settings Preferences window, ensure that network settings are correct.
3. In the General subtab of the Agent Manager Discovery tab, ensure that Discovery settings are correct.
4. Click the Status subtab of the Agent Manager Discovery tab.

5. Select the Discovery process to be started, stopped, or enabled/disabled.



6. Click the Start button. If the process is already running, the Start button will be disabled and you must first stop and then start the selected Discovery process.



7. To stop the selected Discovery process, click the Stop button.

To enable or disable a Discovery process schedule:

1. On the Status subtab of the Agent Manager Discovery tab, select the Discovery process for which you want to enable or disable the schedule.



2. To enable or disable the schedule for the selected Discovery process, click the Enable/Disable toggle button. The Enable/Disable toggle button toggles between Enabled and Disabled, depending on whether the schedule for the selected Discovery process is currently enabled or disabled.

To modify a Discovery process schedule:

1. In the Status subtab of the Agent Manager Discovery tab, select the Discovery process to be rescheduled.



2. Click the Modify Schedule button.

3. In the Start Date section of the Modify Schedule window, use the calendar or up and down arrows to schedule the next date and time to run the selected Discovery process.

OR

Check the Run at first opportunity if schedule missed check box to run the selected Discovery process immediately.

4. In the Recurrence Pattern section, define the recurrence pattern:

To run...	Do...
Never	Select Never to never run the Discovery process from a schedule.
One Time	Select One Time to run the Discovery process on the selected start date and time.
Hourly	Select Hourly and type the hours and minutes to wait between running the Discovery process. To skip Saturdays and Sundays, check the Skip Weekend check box.

Daily	Select Daily and type the number of days to wait between running the Discovery process in the Every x days field. To skip Saturdays and Sundays, check the Skip Weekend check box. The default setting is Daily for all Discovery processes.
Weekly	Select Weekly and check the boxes for the day(s) of the week you want to run the Discovery process. You can select more than one day.
Monthly	Select Monthly and then select Last day of the month to run automatic updates on the last day of each month. OR Select Monthly, select Day, and use the up or down arrow to select the day of the month.

All scheduled policies use the time zone set on the PCM Server. If the policy will be executed by a remote Agent in a different time zone, you must convert the Agent time to PCM Server time to schedule the policy for the correct Agent time. For example, the PCM Server is set to Pacific time (GMT -8 hours) and the remote Agent where the policy will be executed is set to Eastern time (GMT -5 hours). To execute a policy on the remote Agent at 6:00 P.M., set the policy schedule for 3:00 P.M.

Device Access Preferences

Configure device display names and define device access and communication preferences (CLI, SNMP, SSH, Web Agent) by using the Device Access tab in the Agent Manager. Each Agent can have different device access preferences.

Use the Global Device Access preferences explained in “Using Global Device Access Preferences” on page 7-40 to define the naming conventions used by all Agents to identify devices and ports. For example, you can select a standard naming convention or create a custom naming convention containing any combination of DNS name, IP address, and SNMP hostname. It also controls whether port names should be displayed as the interface name or the configured friendly port name.

Agent-Specific Device Access Properties

To define Agent-specific device access preferences:

1. Select the Agent from the Agent Manager navigation tree.
2. Click the Device Access tab and ensure the Device Access subtab is selected:

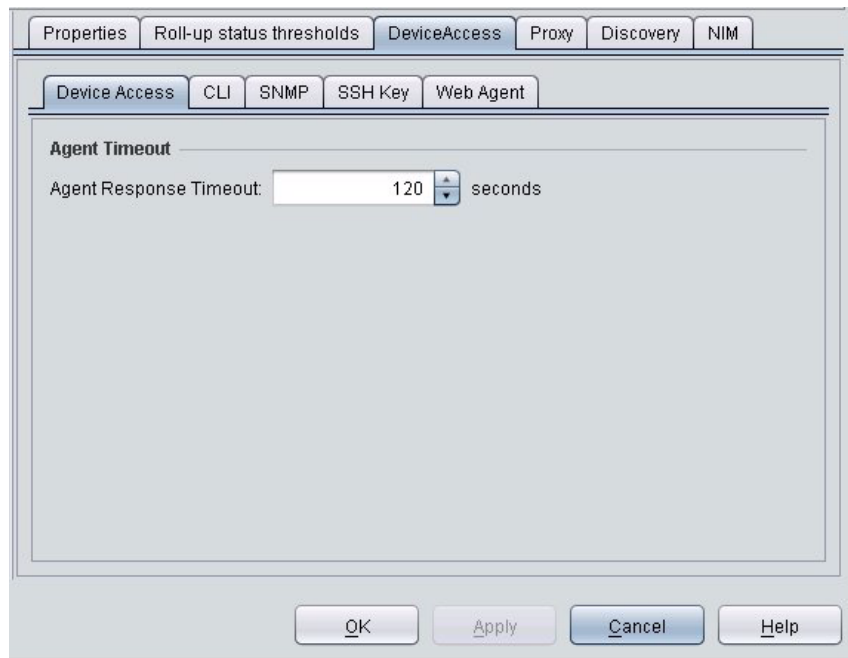


Figure 3-22. Agent Device Access

3. In the Agent Response Timeout. field, type or use the up or down arrow to set the seconds the Agent should wait for a response from devices.

CLI Settings

The CLI subtab of the Agent Manager is used to view and change the default communication parameters used by an Agent for Telnet and SSH communication with devices. The default configuration uses Telnet, with the Username and Password set to "public". However, you can change the default during installation, or at any time on this window.

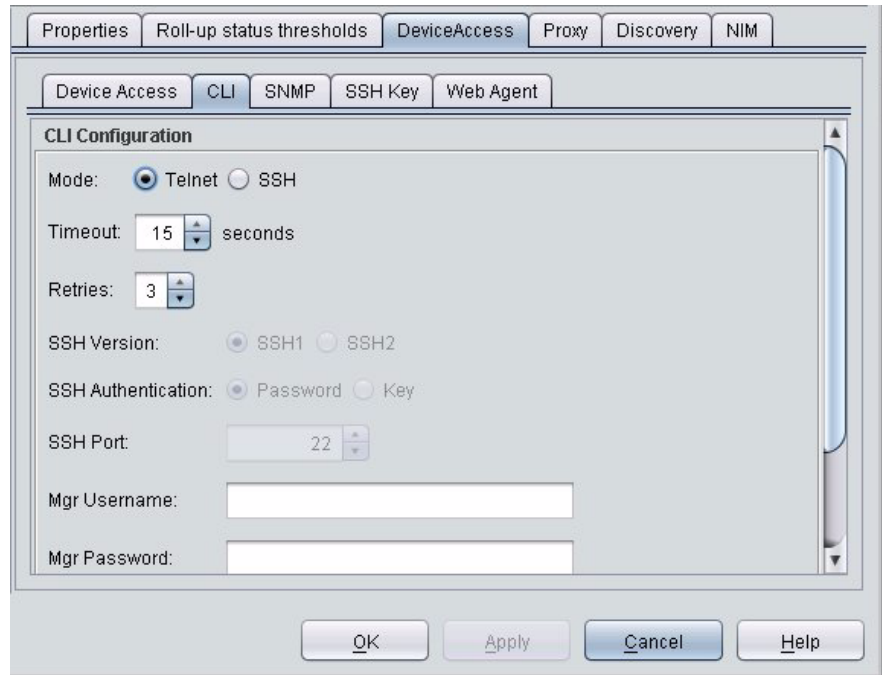


Figure 3-23. Agent Device Access - CLI

Whenever a new device is discovered, these values are updated in PCM for the device. If a new device has been discovered by PCM, but you are not getting configuration information or VLAN information (if applicable) for the device, you may need to set the Telnet username and password for the device in PCM. To change them in PCM for a specific device, use the Communication Parameters in PCM Wizard.

Note:

Use the Communications Parameters in Device Wizard to update CLI parameters in the device.

To change the CLI mode:

1. Select the Agent from the left pane of the Agent Manager window, click the Device Access tab in the right pane, and then click the CLI subtab.
2. Select the mode you want the Agent to use to communicate with devices:

Telnet	Use Telnet for CLI communication. Configure User Credentials to define Telnet parameters.
SSH	Use SSH for CLI communication. Configure SSH Credentials to define SSH parameters. If using password authentication, configure User Credentials.

3. Click the Timeout up or down arrow to set the number of seconds to wait for a response from the device. Timeout can be 1-30 seconds, with a default of 15 seconds.
4. Click the Retries up or down arrow to set the number of times to try connecting with the device. From 1-5 retries can be entered, with a default of 3 retries.

To change Telnet parameters:

1. Ensure that Telnet is selected.
2. To configure a Telnet manager login, type the new manager user name in the Mgr Username field and the associated password in the Mgr Password field.
3. To set up a Telnet operator login, type the new operator user name in the Opr Username field and the associated password in the Opr Password field.

The user names and passwords are stored in PCM for future communication, but devices are not updated. Use the Communications Parameters in Device Wizard to update CLI parameters in the device.

To change SSH parameters:

1. Select SSH as the CLI mode.
2. Click SSH1 or SSH2 to select the SSH version used by the Agent to communicate with devices that do not have specific SSH settings defined in PCM.

Key authentication for SSH1 is not supported.
3. To use SSH password authentication, click the radio button next to Password. Next, type the user credentials that SSH will use to authorize communication with devices.

4. To use SSH key authentication, select Key. (You must define the SSH key before attempting to communicate with devices using SSH key authentication.) Key authentication is used for SSH2 only.
5. Type the default port number to be used for CLI SSH communication.
If using key authentication, define the SSH2 key before attempting to communicate with devices using SSH key authentication.

SNMP Settings

SNMP preferences defined on the SNMP tab of the Agent Manager are used to access new devices during Discovery. Whenever a new device is discovered, these values are updated in PCM for the device. Use the Communications Parameters in Device Wizard to update SNMP settings in a device. You can also change the SNMP community names in PCM for specific devices with the Communication Parameters in PCM Wizard.

The default SNMPV2 version and SNMPV2 read and write Community Names (public) used by an Agent can be changed during installation or on the SNMP subtab of the Agent Manager.

Note:

Some ProCurve Network devices have SNMP disabled by default, or have public as a read-only/restricted community name. Ensure that the PCM Agent's SNMP Configuration is in sync with the device's SNMP configuration

To change Agent SNMP values:

1. Select the Agent from the left pane of the Agent Manager window, click the Device Access tab in the right pane, and then click the SNMP subtab.

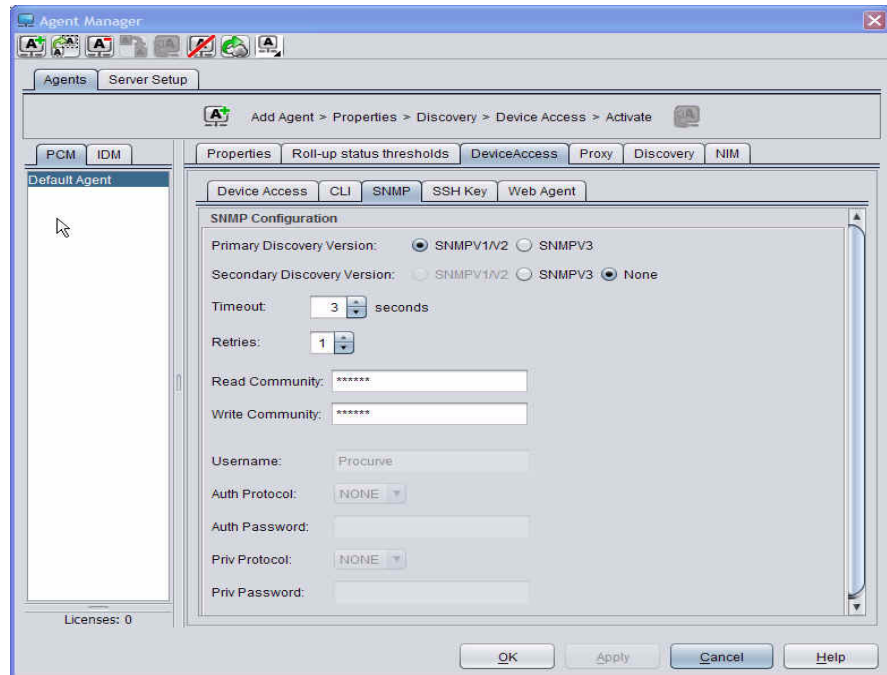


Figure 3-24. Agent Device Access - SNMP

2. Click the radio buttons next to the Primary Discovery version and Secondary Discovery version to select the version used to communicate with devices during Discovery.
3. Initially, PCM uses the Primary Discovery version. If this attempt fails, PCM uses the Secondary Discovery version. Therefore, the Primary and Secondary Discovery versions cannot be the same. You can select both versions if devices support SNMPV2 and SNMPV3.

Primary Version	Secondary Version	Description
SNMPV1/V2	None	Discovery uses only SNMPV1 or V2 to discover devices. Devices that do not support SNMPV1 or V2 will not be discovered
SNMPV3	None	Discovery uses only SNMPV3 to discover devices. Devices that do not support SNMPV3 will not be discovered.

Primary Version	Secondary Version	Description
SNMPV1/V2 or SNMPV3	SNMPV3 or SNMPV2	Discovery initially uses the SNMP version selected as the primary Discovery version to discover devices. If communications fail, Discovery attempts to communicate with the device with the secondary Discovery version. If your network contains SNMPV2 and SNMPV3 devices, you can select both SNMPV2 and SNMPV3 (one for the primary version and one for the secondary version). However, selecting both versions slows down the Discovery process. If performance is a concern, enable one version and then manually discover or import devices using the other version.

4. Click the Timeout up or down arrow to set the number of seconds to wait for a response from the device. Timeout can be set at 1-30 seconds, with a default of 5 seconds.
5. Click the Retries up or down arrow to set the number of times to try contacting the device. From 1-5 retries can be selected, with a default of 3 retries.
6. In the Read Community field, type the default Community Name used to read data on the device. The read Community Name can consist of 1-16 characters including special characters except >, <, and spaces.

When using the PCM for HP NNM module, the default SNMP read Community Name is also changed in NNM. However, devices are not updated.

PCM is shipped with the predefined SNMP read and write Community Names of public. These Community Names can be changed during Agent installation or by this SNMP function. In addition, SNMP Community Names can also be set for a specific device with the Communication Parameters in Device Wizard.
7. In the Write Community field, type the Community Name used to write data to the device. The write Community Name can consist of 1-16 characters including special characters except >, <, and spaces.

When using the PCM for HP NNM module, the default SNMP read Community Name is also changed in NNM. However, devices are not updated.
8. If you selected SNMPV3, in the Username field, type the USM user name used to communicate with the device.
9. Click the Auth Protocol drop-down arrow and select the desired authentication protocol:

MD5 Use the MD5 algorithm to produce a 128-bit fingerprint (message digest) for authentication.

SHA Use the SHA algorithm to produce a 160-bit message digest.

None Do not use any authentication protocol.

10. If you selected MD5 or SHA as the authentication protocol, in the Authentication Password field, type the password you want to use for authentication. The authentication password must contain at least 8 characters.

11. If you selected MD5 or SHA as the authentication protocol, click the Priv Protocol drop-down arrow and select the desired privacy protocol:

DES Uses a 56-bit key and block cipher method to break text into 64-bit blocks and encrypt them.

None Do not use any authentication protocol.

12. If you selected MD5 or SHA as the authentication protocol and DES as the privacy protocol, type the password you want to use in the Priv Password field.

SSH Key Preferences

The SSH Key subtab of the Agent Manager is used to view and change SSH2 key pairs. These key pairs are used by PCM for public key authentication in SSH2 communications with devices. If you select SSH key authentication for an Agent on the CLI subtab of the Agent Manager, define the key using the SSH Key subtab.

The SSH keys shown in this window are used by the selected Agent to communicate with devices when public key authentication is in force. These keys are displayed so you can copy the key and ftp it to the switch for the switch to authenticate PCM.

Note:

Key authentication for SSH1 is not supported.

To change the SSH keys:

1. Select the Agent from the left pane of the Agent Manager window, click the Device Access tab in the right pane, and then click the SSH Key subtab.

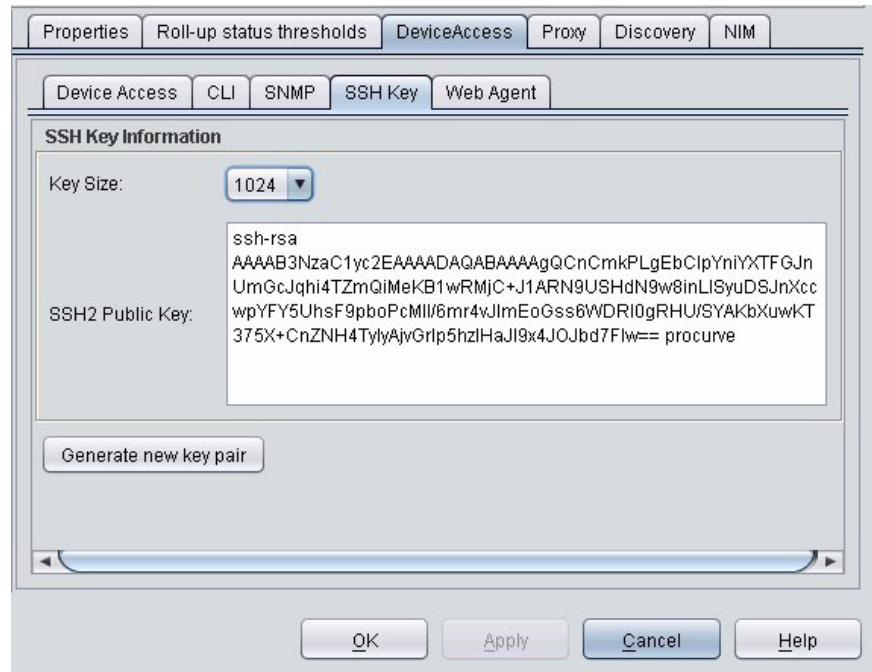


Figure 3-25. Agent Device Access - SSH Key

2. In the Key Size field, use the drop-down list to select the number of bytes contained in the key. We recommend using a key size of 768 or 1024. Otherwise, the generated key may not be valid. A small key results in faster authentication, but a large key provides greater security.
3. To generate new SSH2 keys, click **Generate new key pair**.

Generating a key in PCM causes communications with devices using the old SSH2 key to fail.

If PCM is unable to communicate with a ProCurve device using SSH key authentication, the key on PCM and the switch may be mismatched, See Device Access Problems for additional information.

WebAgent Preferences

The Web Agent subtab of the Agent Manager is used to view and change the default communications parameters used by the Agent to communicate with devices via the browser-based Web Agent. The default settings use HTTP and port 80, along with the IP address of the device. For example:

http://192.68.1.28:80

Whenever a new device is discovered, these values are updated in the Agent for the device. Use the Communication Parameters in PCM Wizard to change them for a specific device.

To change Web Agent settings:

1. Select the Agent from the left pane of the Agent Manager window, click the Device Access tab in the right pane, and then click the Web Agent subtab.

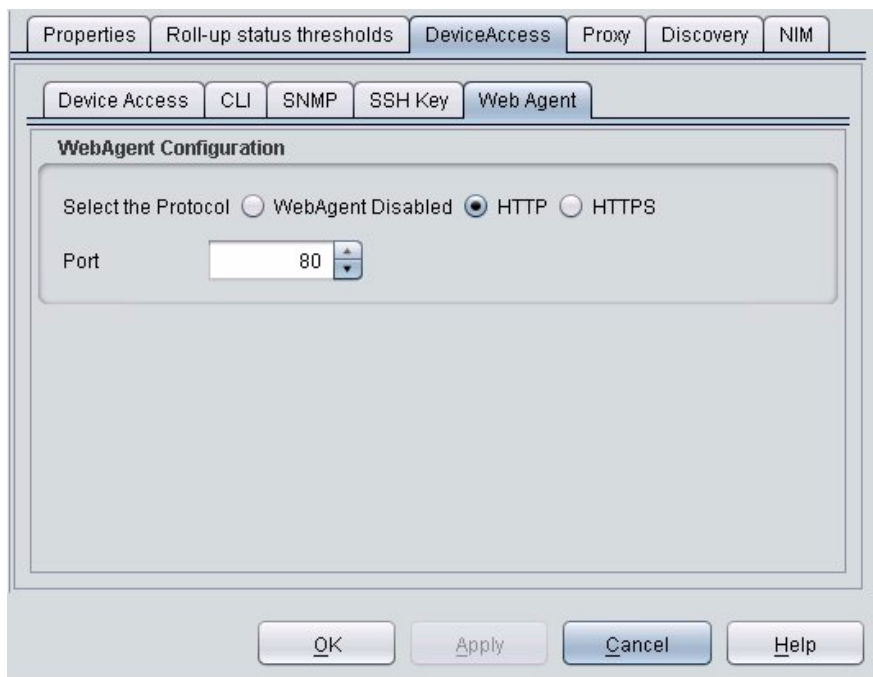


Figure 3-26. Agent Device Access - Web Agent

2. Select the mode you want to use for Web Agent communication with devices if specific Web Agent communication parameters have not been set up for the Use the less secure HTTP mode for communication. The default is HTTP.

- HTTP Use the less secure HTTP mode for communication. The default is HTTP.
- HTTPS Use the more secure HTTPS mode (HTTP over SSL) for communication.

3. In the Port field, type or use the up or down arrow to select the port on the device used for Web Agent communication. The default port is 80 for HTTP and 443 for HTTPS.

Rollup Status Reporting Thresholds

You can also configure the device thresholds for status reporting:

1. Ensure the PCM tab in the left pane of the Agent Manager is selected and then select the Agent that you want to configure.
2. Click the Roll-up Status Thresholds tab:

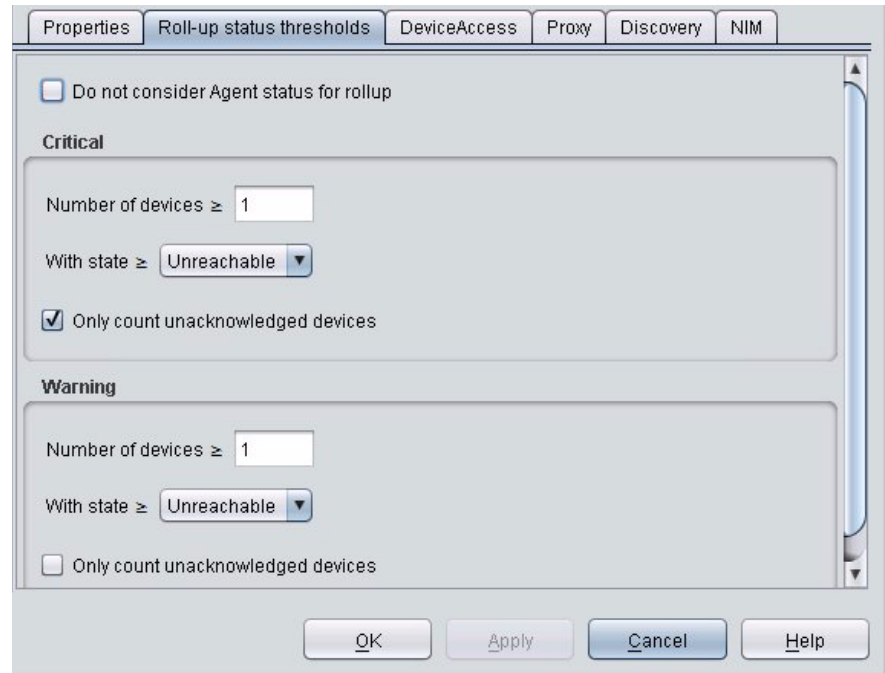


Figure 3-27. Agent Roll-up Status Thresholds Tab

3. To exclude Agents from the rollup count, check Do not consider Agent status for rollup.

4. In the Number of devices field of the Critical section, type the number of devices that must be in the selected state before the status of devices managed by the Agent is considered Critical.
5. Use the Critical With state drop-down list to select the device state used as the Critical rollup status threshold. Possible states are Warning and Unreachable.
6. To include only unacknowledged devices in the device count for the Critical threshold, check the Only count unacknowledged devices check box. Acknowledging an unreachable device (right-click the device and select Toggle acknowledged flag) removes it from the Critical count. This option is only applicable if you acknowledge devices in a warning or unreachable state.
7. In the Number of devices field of the Warning section, type the number of devices that must be in the selected state before the status of devices managed by the Agent is considered Warning.
8. Use the Warning With state drop-down list to select the device state used as the Warning rollup status threshold. Possible states are Warning and Unreachable.
9. To include only unacknowledged devices in the device count for the Warning threshold, check the Only count unacknowledged devices check box. Acknowledging an unreachable device (right-click the device and select Toggle acknowledged flag) removes it from the Warning count. This option is only applicable if you acknowledge devices in a warning or unreachable state.

Local Agent Memory Usage

If the number of managed devices in your PCM network increases and/or you are running multiple plug-in modules, you may improve performance on the local PCM Agent by allocating more memory so that it uses 2 GB RAM. The default memory usage is 1 GB.

Prerequisites: The local Agent should discover more than 1000 devices, and PCM must be running on a 64-bit operating system with at least 6GB RAM.

Warning: After you reconfigure memory usage, the local PCM Agent will restart.

To reconfigure memory usage on the local PCM Agent:

1. Open the Tune PCM Memory Usage window in one of the following ways:



- Click the Preferences button in the PCM toolbar and select the Tune PCM Memory Usage option.
 - Select Tools > Preferences > Tune PCM Memory Usage.
2. Under Tune PCM Local Agent Memory Usage, select **Large Size Configuration** and click **OK** or **Apply**.

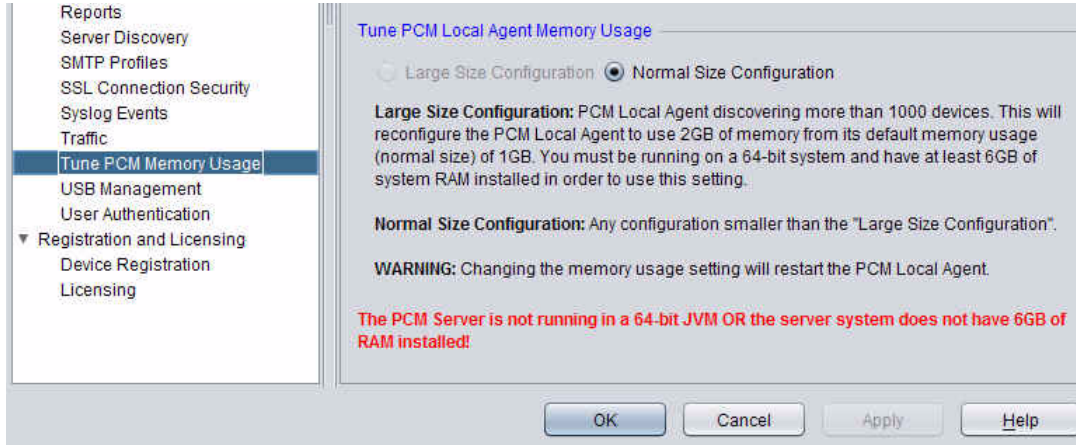


Figure 3-28. Tune Memory Usage in Local PCM Agent

Other Agent Manager Functions

A variety of Agent Manager functions may be available on tabs contributed by PCM modules (IDM/PMM/NIM) and other applications. For example, if NIM is installed the NIM tab is displayed, which allows you to customize security monitoring and analysis preferences for each Agent.

Changing Server Setup

The Server Setup tab identifies settings that the Server should use when Agents come online. Initially, these values are set during installation, but can be changed on this tab as follows:

1. Navigate to the Server Setup tab by clicking the Agent Manager button on the global toolbar and clicking the Server Setup tab in the left pane of the Agent Manager.
2. By default, passwords are shown as asterisks. To show the PCM Server, PCM Agent, and IDM Agent passwords, click the Reveal Passwords check box.
3. To change the default password used by the PCM Server to authenticate Agents, type the desired password in the Password field. By default, this password is blank, but it can be changed during installation to the default PCM password (procurve) or any user-defined password.
4. To select the default Server port and encryption type used for incoming connections from Agents, check the Enable server port check box and enter the desired Server port number and encryption type. SSL encryption encrypts all messages in both directions. By default, the Server port is 51111 with SSL encryption for remote Agents, but it can be changed during installation or on this tab.
5. To override the default connection heartbeat threshold for new Agents, type the Warning connection threshold (in milliseconds). The default Warning threshold for new Agents is 50,000 ms.

The connection heartbeat threshold setting can be overridden by setting specific values for an Agent in the Agent's Properties subtab.

6. To allow Agents that have not been detected by or defined in PCM to connect to the Server, check the Allow new Agents to connect check box and enter the Password required to connect to the Server. (The password is assigned to the Agent when it is deployed.)
7. If you choose to allow new Agents to connect, use the Template Agent drop-down list to select the default properties you want to assign to new Agents. This will save you time if you use the same device access and proxy settings. However, you must still configure the discovery seed device and subnets before the Agent can be used.

The proxy port setting can be overridden by setting specific values for an Agent in the Agent's Properties subtab.

Configuring and Managing Agents
Changing Server Setup

8. Enter the port range where the Server will listen for HTTP, HTTPS, Telnet, or SSH connections to be forwarded to Agents. A range is required when multiple Agents are configured to use a default port. By default, the proxy port range is 49200 through 49300, but it can be changed on this tab.

Note:

During installation, all Agents that initiate a connection to the PCM Server must be configured with the same port number and encryption mode set in this tab.

Viewing Agent Information

Use the Agents tab to view information about Agents. Select the Agent Groups node or a specific Agent group in the PCM Server's navigation tree to display the Agents tab, which lists all Agents assigned to the selected Agent Group.

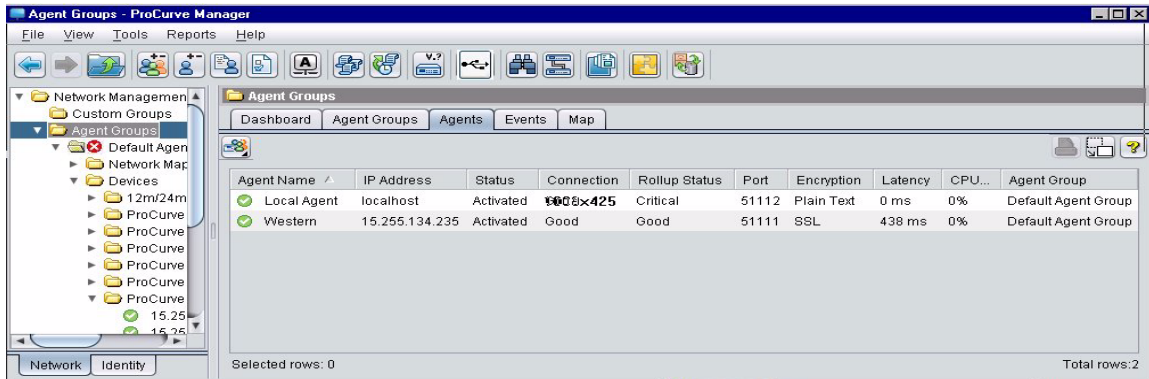


Figure 3-29. Agents Tab

The Agents tab contains the following Agent information:

Agent Name	Name of the Agent along with a color-coded icon showing the operational status of the connection between the PCM Server and the Agent: Green Operational with good link speed Yellow Either operational slow link or unconfigured good link Red Either unreachable or unauthorized good link
IP Address	IP address of the Agent
Status	Operational state of the Agent. Possible values are: Activated: Fully operational, licensed and configured properly Activation Needed: Agent has not been configured. Configure the Agent and mark it as active. Agent password mismatch: The Agent passwords on the Agent and the PCM Server do not match. Authentication has failed. You must reconfigure the Agent password on either the Server or the Agent. Both sides connecting error: Both the Agent and the Server have been configured to initiate the socket connection. This operation is mutually exclusive: only one side can initiate a connection. Use the Agent's web-management interface to reset the SSL certificate to the factory default. Downloading Packages: The PCM Server is downloading or updating the agent code on the Agent. This is an informational status message. Executing Commands: Scripts are being run for packages that need to be customized prior to use. This is an informational status message.

Status (Continued)	<p>Extracting Packages: Packages that have been downloaded to the Agent are being installed for use. This is an informational status message.</p> <p>Loading Components: Agent components are being prepared for execution. The next status displayed is usually "Activated".</p> <p>Restarting: The Agent is restarting. This is normal operation after an auto-update, the first time that the Agent connects to the Server, or after certain types of configuration changes. This is an informational status message.</p> <p>Server password mismatch: The PCM Server passwords on the Agent and the Server do not match. Authentication has failed. You must reconfigure the Server password on either the Server or the Agent.</p> <p>Unauthorized: Agent credentials or PCM Server credentials are not correct, Agent and PCM Server cannot communicate.</p> <p>Unlicensed: Agent is not licensed and cannot connect to PCM Server.</p>
Connection	State of the connection (Good, Warning, or Unreachable)
Port	Port used by the Agent to listen for connections
Encryption	Whether the Agent is using unencrypted plain text or SSL to communicate with the PCM Server
Latency	Link latency
CPU%	Percentage of the Agent's CPU being used
Agent Group	Agent group to which the Agent belongs (displayed only when the Agent Groups node is selected)

Downloading Files to Agents

The Agent File Manager is used to manually download files to Agents. Primarily, this tool is used to download CIP files (trap decoders and device OID files). These Agent files are individual files, created either directly or via some wizard, that need to be deployed to Agents. Packages deployed via the standard download protocol consist of entire archive .zip files and are usually put on the PCM Server when PCM is installed or an auto update is received.

The Agent Manager keeps track of every Agent ad hoc file that needs to be downloaded to Agents. Each time an Agent connects to the PCM Server, the Agent receives this list of files and verifies that it has the same version of all files on the list. If the Agent doesn't have the file or has a different version, the file is automatically downloaded to the Agent during the initial download protocol step.

The Files to Send list is maintained long-term, because new Agents can be installed at any time, and when new Agents first connect, all files in the Files to Send list are downloaded to the Agent.

This window also contains a Files to Remove tab, which is used to remove files from Agents.

To Download a File to Agents



1. Click the Agent Manager button on the global toolbar to open the Agent Manager.



2. Click the Agent Utilities button on the Agent Manager toolbar and select Agent File Manager from the drop-down list.

3. On the Agent Ad hoc File Manager window, click **Add** (shown below the File List on the Files to send tab).

4. When the Open window appears, select the file you want to add, and click **Open**. You can also type a new file name in the File Name field. The selected file is added to the File List in the Agent File Manager.

5. Select the file from the File List and, optionally type a description of the file.

6. In the Destination field, type the destination directory relative to the Tornado container folder (folder named with the install ID of the Typhoon server it is connected to). For example, type `config/devConfig/`

`extern` if you want the file to be copied to the `config/devConfig/extern` directory. Do not include a trailing slash or the file name (just the path to the folder).

7. To force an immediate update to Agents, click **Synchronize Agents now!** at the top of the window.

Files are not immediately downloaded to the Agents unless you click the Synchronize Agents now! button. Otherwise, files are downloaded the next time an Agent connects and resynchronizes with the PCM Server.

8. Click **OK** to close the Ad Hoc File Manager window.

To Remove a File from Agents



1. Click the Agent Manager button on the global toolbar to open the Agent Manager.



2. Click the Agent Utilities button on the Agent Manager toolbar and select Agent File Manager from the drop-down list.
3. On the Files to Send tab of the Agent File Manager window, select the file to be removed from the File List.
4. Click **Remove**, which moves the file to the File List on the Files to Remove tab.

Thereafter when Agents are synchronized, files listed on the Files to Remove tab are removed from the Agent as well as downloading files in the Files to Send tab.

Once that happens, the files stay on the “Files to Remove” list because we cannot be sure that there aren’t other Agents that perhaps are down or offline at the moment.

5. Once you are sure a file has been removed from all Agents, it can be removed from the Files to Remove list by selecting the file and clicking the Remove button below it.
6. Click **OK** to close the Agent File Manager.

Managing Remote Agents Using the Web

The following types of Agent information and features can be accessed through the browser-based Agent UI:

- Agent connection
- Agent credentials
- Agent identity
- Managing SSL certificates
- Troubleshooting

To access the Agent Web Management UI:

1. Open a browser, such as Internet Explorer.
2. If a firewall is between the PC you are using and the Agent, identify the proxy in your browser. For example, to configure a proxy in Internet Explorer:
 - a. On the Internet Explorer menu, select Tools > Internet Options > Connections.
 - b. Click the LAN Settings button on the Connections tab.
 - c. Check the Use a proxy server for your LAN check box.
 - d. Type the proxy server IP address and port number used during installation of the Agent.
 - e. Click **OK**.
3. In the address bar, type the https URL:
`https://<Agent IP address>:<Port>/`
4. Replace <Agent IP address> with the IP address of the Agent, and replace <Port> with the Web port configured during installation (default 8080).
5. When the Agent UI Login screen appears, click Login and type the User Name and Password. The default user name is "admin" and the password is the same as the Agent password (default "procurve", if used).

See the Agent UI online help for information about the each feature.

Troubleshooting an Agent

If the Agent is not communicating with the PCM Server or is not operating as expected, use the following Agent Manager tools to troubleshoot the Agent.

After PCM Reinstallation

If PCM is reinstalled on the Server after remote PCM Agents are upgraded (e.g., by auto update), PCM Agents are downgraded to the PCM Agent version on the Server.

To test a link:

Use the Ping button to initiate an ICMP ping to an Agent from the PCM Server.



1. Click the Agent drop-down button.
2. Select **Ping** from the drop-down list.
3. Review the displayed information to ensure the Agent can communicate with the pinged device.
4. Click **OK** to close the window.
5. If necessary, revise the Agent properties.

To test credentials:

The Test Agent Credentials function is used to ensure the PCM Server and Agent have the other's credentials (passwords) configured correctly. This function is available only for Agents configured for Server-initiated connections and can only be used when the Agent is disconnected.



1. Select the Agent for which you want to test credentials.
2. Click the Agent Utilities button on the Agent Manager toolbar.
3. Select **Test Credentials** from the drop-down list.
4. Review the displayed summary to ensure the PCM Server can communicate with the Agent and that their credentials are correctly configured on each side.
5. If the PCM Server cannot communicate with the Agent, ensure the Agent is installed, ensure Agent credentials are configured correctly on the PCM Server, ensure PCM Server credentials are configured correctly on the PCM Server.

To display a log:

Use log files to track occurrences during troubleshooting.



1. Click the Agent drop-down button.
2. Select **Logs** from the drop-down list.
3. To view all logs, check the **Select All Log Files** check box and click **View Log Files**.
4. To view a specific log, select the desired log and click **View Log Files**.
5. To save all logs to a .zip file, click **Save All Logs to Zip**, select the destination location, and click **Save**.

To restart an Agent:

Use the **Restart** button to restart the Agent when necessary. You should not use this function unless instructed to do so by HP Support.






1. Click the Agent drop-down button.
2. Select **Restart** from the drop-down list.

Remove Local Agent

In networks with more than 1200 discovered devices, we recommend that all Agents be remote. This requires moving the local Agent to a remote Agent on another PC, which can be done in either of two ways. The procedure you use depends on whether you want to retain data (config scan, events, VLANs, traffic, etc.) from the local Agent and the time it takes to return to complete a discovery cycle.

Method 1

With this method all devices managed by the local Agent are managed by the new remote Agent. However, VLAN data and traffic data for devices previously managed by local Agent are not moved. Discovery, in its next cycle, discovers VLAN data at the new remote Agent, Traffic sampling must be manually enabled at the remote Agent, and all traffic data is sampled anew.

1. Install a remote Agent on a different PC, and connect this Agent to the PCM sever, as explained at the beginning of this chapter.
2.  Move subnets from the local Agent to the new remote Agent, as explained on page 3-30.
3.  Deactivate the local Agent by selecting the local Agent in the left pane and clicking the Mark Inactive button.
4.  Delete the local Agent by selecting the local Agent in the left pane and clicking the Delete Agent button.

Method 2

With this method all data at the new remote Agent is rebuilt over a period of time, just as it was done initially with the local Agent. Data is completely coherent, does not have any dependency on original data of the local Agent, and, therefore, is up to-the-minute. The only drawback is this takes time to complete an entire discovery cycle. Also, all old data (e.g., config scans, events, etc.) is lost.



1. Deactivate the local Agent by selecting the local Agent in the left pane and clicking the Mark Inactive button.



2. Delete the local Agent by selecting the local Agent in the left pane and clicking the Delete Agent button.
3. Install a remote Agent on a different PC, and connect this Agent to the PCM Server, as explained at the beginning of this chapter.
4. Set the seed device for the new remote Agent to the same seed device that was used by the local Agent. To do so, select the new remote Agent in the left pane and enter the IP address of the seed device on the General subtab of the Discovery tab in the Agent Manager.
5. Using the managed Subnets subtab of the Discovery tab in the Agent Manager to assign the subnets that were earlier managed by the local Agent to the new remote Agent.

Replace an Agent

When the system where an Agent is installed suffers an unrecoverable failure and new Agent software is installed on a new system to replace the one that failed, use the Agent Manager to replace the failed Agent with the new Agent. The Agent Manager achieves replacement by copying the connection settings of the new healthy Agent to the connection settings of the failed Agent, so the new Agent can assume the identity and responsibilities of the old Agent. The original entry in the database for the new Agent is deleted afterwards.

To replace an Agent:

1. Click the Agent Manager button on the global toolbar to open the Agent Manager.
2. Select the Agent to be replaced (Agent that failed).



Click the Replace Agent button on the Agent Manager toolbar, which opens the Replace Agent window.

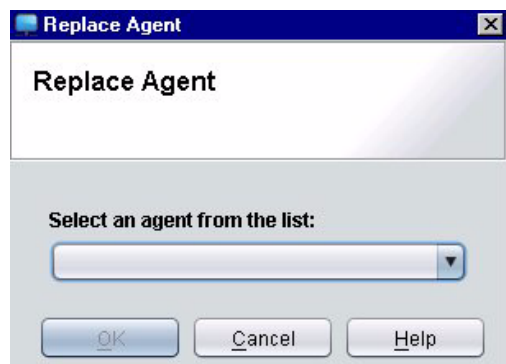


Figure 3-30. Replace Agent

The Replace Agent button is available only for disconnected PCM Agents that initiate connections to the PCM Server. It is not available for IDM Agents.

3. In the Replace Agent window, use the drop-down list to select the Agent that will replace the selected Agent.

Only Agents that have never been activated are displayed in the list.

4. When the confirmation prompt appears, ensure the correct Agent is displayed and click **Yes**.

To delete an Agent:

Use the Delete Agent button to delete an Agent, which removes it from the Agent Manager list and all other Agent-related windows. All devices discovered by the Agent are also deleted from PCM.

1. In the left pane of the Agent Manager, select the Agent to be removed.
2. Click the Delete Agent button.
3. When the confirmation prompt appears, click **OK**.



Discovering Devices

How Discovery Works	4-2
Viewing Discovery Data	4-5
Updating Device Data	4-6
Using Manual Discovery	4-7
Using Re-Discover Device	4-13
Discovering a Loopback Interface	4-17
Port Classification	4-19
Displaying Port Classification Information	4-19
How Discovery Classifies Ports	4-21
Finding Nodes and Paths	4-22
Using Find Node	4-22
Using Node-to-Node Trace Path	4-26
Managing Discovery Preferences	4-28
Enabling and Disabling Discovery Processes	4-29
Changing Discovery Preferences	4-33
Excluding or Deleting Devices from Discovery	4-35
Discovery Intervals	4-39
Configuring Subnets for Discovery	4-40
Re-Classifying Unknown Devices	4-43
PCM Server Memory Usage	4-44
Importing and Exporting Discovery Data	4-45
Importing Managed Subnets	4-46
Exporting Managed Subnets	4-48
Creating an Import File for Managed Subnets	4-49
Importing Discovered Devices	4-50
Exporting Discovered Devices	4-52
Creating an Import File for Managed Devices	4-53
Troubleshooting Discovery	4-57
LLDP Problems	4-57
Remedies	4-58
Special Considerations	4-60
Slowing Down Discovery	4-60

How Discovery Works

Discovery is the process used by ProCurve Manager to automatically find all the devices in the managed subnets and determine the devices' relationships to each other (topology). The discovered devices are displayed in the Devices List and Network Maps, and added to PCM's device information database. Discovery collects only the basic device and connectivity (port and VLAN) information. (The Configuration Manager Scan function collects detailed device configuration information.)

ProCurve Manager can discover any devices within the managed network (subnets), that are SNMP accessible with valid read Community Names (SNMPv1/2) or USM user names (SNMPv3), depending on the protocols enabled in the SNMP subtab of the Agent Manager Device Access tab. Such devices include:

- HP's ProCurve series of manageable switches and routers that support LLDP (Link Layer Discovery Protocol 802.1AB), CDP (Cisco Discovery Protocol - read-only), or FDP (Foundry Discovery Protocol).
- Other ProCurve devices that are SNMP accessible, but do not support LLDP, CDP, or FDP.
- Other HP network devices that are SNMP accessible and support the bridge MIB.
- Devices on the network (end nodes) that are SNMP accessible, but do not support the bridge MIB, such as HP printers.
- Other devices on the network with valid IP addresses, including third-party devices that support SNMP.

Discovery is a resource-intensive process and may take some time. To speed up discovery in the new architecture, a discovery engine is used for each Agent. This allows you to divide the discovery process between Agents which reduces overall discovery time, and set different access credentials, policies, and schedules for each Agent. And, devices discovered by an Agent are viewable only by authorized users.

Note:

PCM v3's new architecture is the next-generation management of user-defined management domains. This new architecture enables secure extensibility of management from a large campus site to geographically dispersed remote sites with thousands of LAN and WLAN devices.

Each Agent uses a multi-phase process, working from the IP address of the seed device with the SNMP read community name specified during the installation process, to find and map devices in the network. In PCM 3.0, the seed device and SNMP community name can be unique for each Agent, and devices are mapped by the Agent.

- Neighbor discovery is the fastest discovery process, where PCM looks for all LLDP, CDP, and FDP-enabled devices in the neighbor tables on the device.

LLDP and CDP are Layer 2 protocols implemented by various switches for the purpose of informing their neighbors of their existence and connection, and to learn about their own immediate neighbors. Once switches have learned of the connections to their neighbors, they make that information available to management applications that choose to interrogate the switch appropriately. CDP is used on 8000, 1600, 4000, 2400, 2424, and 6108 ProCurve devices. FDP, similar to CDP, is available on the 9300 devices with software version 7.6 or later.

- The second discovery process is ARP discovery, which looks for other active network devices in the ARP cache on discovered switches and on the devices found in the discovered switch neighbor table. For more information, refer to the *Advanced Traffic Management Guide* or the *Management and Configuration Guide* for your ProCurve switch.
- Device Attributes discovery is another discovery process that uses SNMP to collect information related to device port status, port speed, port security, port authType, etc.) and VLANs configured on each device found on the network.
- The Ping Sweep discovery process is used to locate all devices connected to the network. This process takes the longest time to run because it will ping all addresses in a subnet and is subject to time-out delays.

Manual Ping Sweep Discovery

During scheduled discovery runs, a PCM ping sweep pings every IP address in each subnet managed by an Agent. In a large network with a large number of subnets (greater than 200), PCM may take several days to complete a discovery cycle. Because of the delay in completing the discovery, PCM may not discover some devices that are added later or that become unreachable during the ping sweep.

To ensure that new and undiscovered devices are included in Discovery, you can manually start a ping sweep discovery on selected subnets on a per-agent basis by clicking the **Discover Subnet** button as described in “Managed Subnets” on page 3-27.

From the seed device specified during PCM Server installation and Agent configuration, Discovery propagates through each of the devices listed in the neighbors table and ARP discovery looks for active network devices for each IP address in the table. At the same time, the Ping Sweep discovery process starts looking for active network devices in the Managed subnet.

For each device found in the network using LLDP, ARP, and Ping sweep, Discovery performs the following process:

- Log an entry to the Device Log, accessed via the Device Log button on the Devices List, indicating the device has been created (an entry added to the PCM database)
- If AutoTrap is configured, add the Agent station as a trap receiver on the device, and log an entry to the Device Log and Events monitor table indicating either success or failure.
- Classify the device model for grouping in the navigation tree.
- Device Attributes - Retrieve and update the device properties, such as ports, VLAN configurations, software versions, sysContact, sysLocation, etc.

Note:

When using the PCM for HP's Network Node Manager (NNM) module, PCM reads the NNM device database to get initial ProCurve device information, then the PCM discovery process retrieves the network properties for ProCurve devices. ARP and Ping Sweep discovery functions are provided via the NNM discovery process.

The Discovery process also registers the NNM server as a trap receiver for each ProCurve device, and all device and PCM application events are logged to the NNM Events database.

Initially, discovery works only for devices on the same subnet as the Discovery seed device. Discovery polls the seed device for the subnet mask and computes the subnet address from the IP address. Discovery then defines the subnet as the default managed subnet. Once you have started PCM, you can add subnets and devices on your network to the Discovery list for each Agent.

Discovery uses the default SNMP read community name specified during the install process to discover new devices on the network. Once a device is discovered, you can change the SNMP read community name for that device in PCM using the Communication Parameters Wizards (See Chapter 7, "Managing Network Devices" for details).

When Discovery is first started, it launches status polling to poll the discovered network devices for operational status at prescribed intervals. The polling results are used to display device status in the Devices List. The interval for

running each Discovery component can be altered in the Discovery settings for each Agent. (See “Managing Discovery Preferences” on page 4-28 for details.) Note that even if Discovery is stopped, status polling continues to run and check the status of devices on the network.

Viewing Discovery Data



The Status bar in the bottom PCM window frame includes an indicator for Discovery status, either on or off. This allows you to check the Discovery process status at all times.

Discovery Process Status



You can also review the current status of each Discovery process for an Agent in the Status subtab of the Agent Manager Discovery tab. Access this tab by clicking the Agent Manager button on the global toolbar or selecting Tools > Agent Manager > Discovery > Status. The Status subtab of the Agent Manager Discovery tab displays the current status of each Discovery process. This window is also used to start, stop, and schedule Discovery processes.

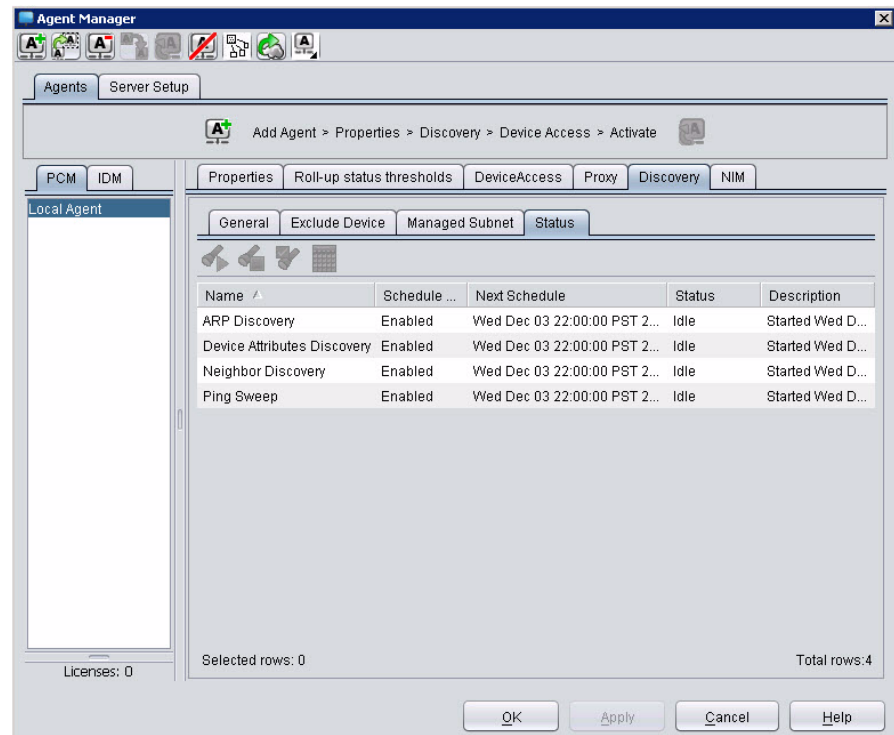


Figure 4-1. Agent Manager, Discovery Status subtab

Dashboard Inventory Pane

The Dashboards for the Agent Groups node, Devices nodes, and specific Agent groups provide a summary of the items discovered on the network (in the Agents you are allowed to view) in the Inventory pane.

Inventory	
Agents:	1
Devices:	18
End Nodes:	34
Managed Subnets:	2
VLANs:	12
Custom Groups:	0

Figure 4-2. Dashboard Inventory pane provided by Discovery

Note:

When using the PCM+ for NNM module, the Inventory data refers only to ProCurve network devices. End nodes inventory will always be 0. This is because PCM+ only gets information on ProCurve devices from NNM, thus is unable to determine end nodes or unknown devices.

Devices Lists

Click the Devices node in the navigation tree to display a list of all devices discovered by the Agent, or click a device group to display a list of all devices of a specific type that have been discovered by the Agent.

You can also use Subnet and VLAN maps to view network topology maps showing devices and their connections, as explained in Chapter 5 “Using Maps”.

Updating Device Data

If you do not find a device in the Devices List and you know its IP address, use the Manual Discovery process to check for the device, as explained in “Using Manual Discovery” on page 4-7. You can also re-discover a device to update device data. For example, if you change the location of a device, and do not want to wait until the next scheduled scan to see the changes in PCM, you can re-discover the device, as explained in “Using Re-Discover Device” on page 4-13. A device must be re-discovered to update PCM with changes due to any of the following:

- the device was disconnected, then reconnected to another port or device
- a module has been removed or added to the device

- configuration changes are made to the device, such as STP, trunk connection, etc.
- connections shown for the device in the Network Maps are incorrect.

Note:

Discovery and Re-discovery do not collect and store device configuration information. Discovery is used only to update the device’s network properties and connections. To get device configuration data, you must use the Configuration Manager Scan, described in Chapter 12, “Managing Device Configurations”.

Using Manual Discovery

You can manually discover a device on the network at any time using the Manual Discovery Wizard. The Manual Discovery Wizard is also used to re-discover a device, however some screens will differ as explained in “Using Re-Discover Device” on page 4-13.

1. Select Manual Discovery from the Tools menu,



Figure 4-3. Manual Discovery Wizard, Welcome

2. Click **Next** to display the Device Information window.

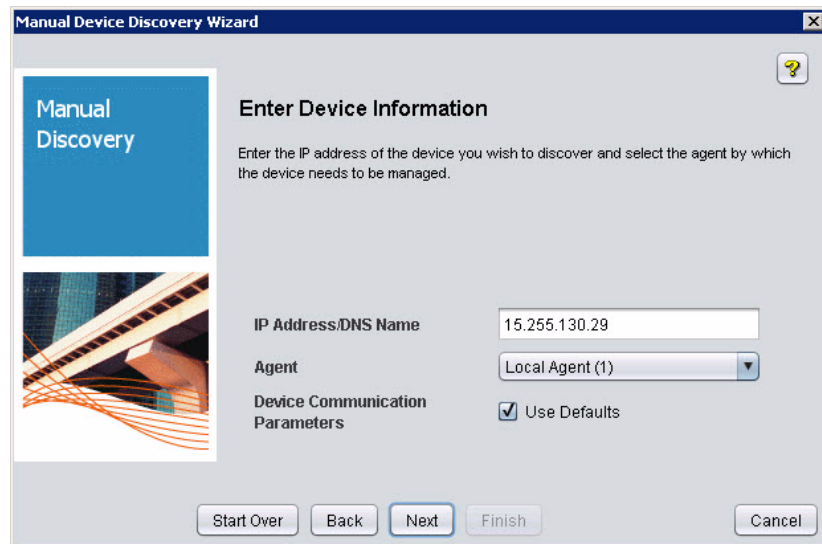


Figure 4-4. Manual Discovery Wizard, Device Information

3. In the Device IP Address field, type the IP address or DNS name of the device to be discovered.
4. In the Agent field, use the drop-down list to select the Agent that will discover the device.
5. Check the Device Communication Parameters Use Defaults check box to use the SNMP and Telnet/SSH defaults defined in PCM.

OR

Uncheck the check box to manually define the communications parameters. If you do not use communication parameter defaults, the wizard displays additional screens where you will define the communications parameters.

6. Click **Next**.

Discovery checks if the device has been discovered by another Agent or belongs to a subnet managed by another Agent. If the device IP address belongs to a subnet not managed by any Agent in the Agent Group, a new managed subnet will be added to the selected Agent.

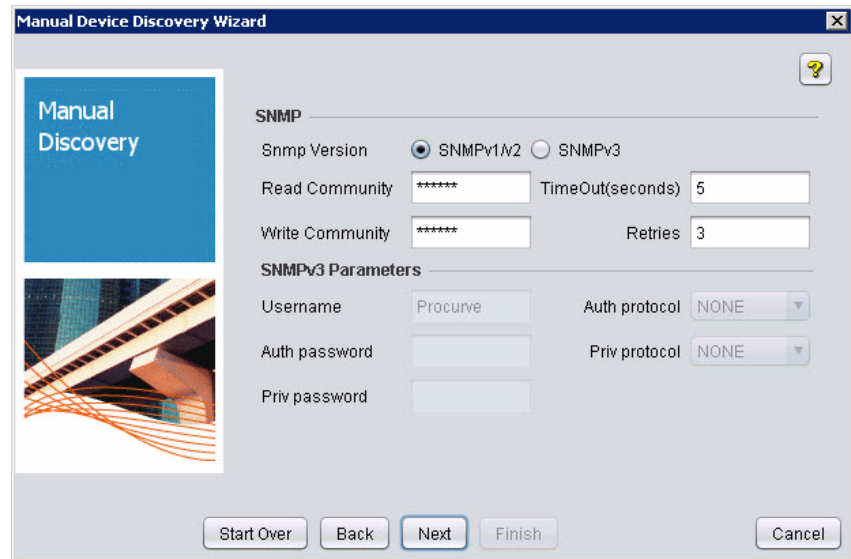


Figure 4-5. Manual Discovery Wizard, SNMP

7. To select the SNMP version(s) used by PCM, select SNMPv1/v2 and/or SNMPv3. If you selected a single device, the SNMP version(s) currently enabled on the device is selected (checked) automatically.
8. To change the SNMPv1/v2 communication parameters used for manual discovery:
 - a. In the **Read Community** field, type the SNMP Read Community Name used to communicate with the device.
 - b. In the **Write Community** field, type the SNMP Write Community Name used to communicate with the device.
 - c. In the **TimeOut** field, type the communication timeout period (in seconds) for manual discovery.
 - d. In the **Retries** field, type the number of device communication retries for manual discovery.
9. To change SNMPv3 communication parameters used for device discovery:
 - a. Click the radio button to select **SNMPv3**, which enables the SNMPv3 fields in the window.
 - b. Enter the **USM Username** used to access the device.
 - c. If the device uses an authentication protocol, select it from the **Auth Protocol** drop-down menu:

None - Do not use an authentication protocol.

MD5 - Use the MD5 algorithm to produce a 128-bit fingerprint (message digest) for authentication.

SHA - Use the SHA algorithm to produce a 160-bit message digest.

- d. If you selected MD5 or SHA, in the Auth Password field, type the password used for authentication. The password must contain at least 8 characters.
- e. If you selected the MD5 or SHA authorization protocol and the device uses privacy protocol, click the Private Protocol drop-down arrow and select DES privacy protocol or None.
 - DES uses a 56-bit key and block cipher method to break text into 64-bit blocks and encrypt them.
 - Select None if you do not want to use a privacy protocol.
- f. If the device uses the DES Privacy Protocol, select it from the Priv Protocol drop-down menu. DES uses a 56-bit key and block cipher method to break text into 64-bit blocks and encrypt them.
- g. If you selected DES, type the Private Password used to communicate with the device. The password must contain at least 8 characters.
- h. Click **Next** to continue to the Telnet parameters window.

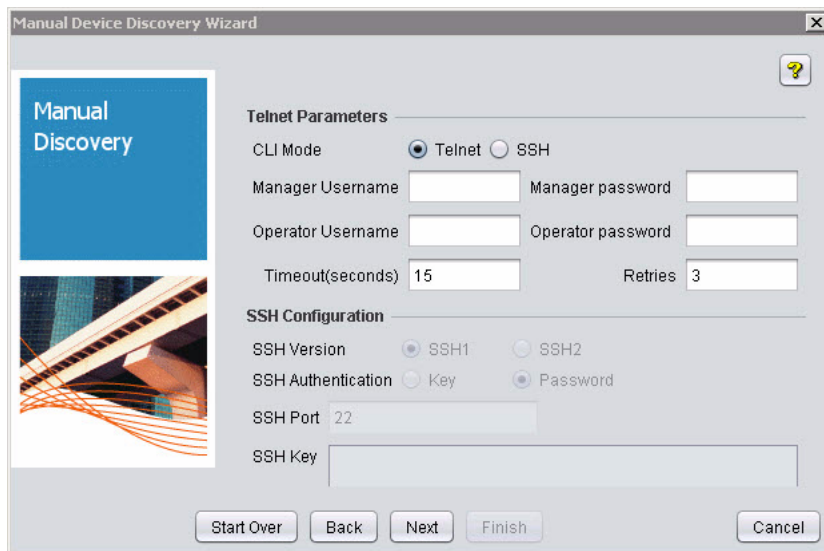


Figure 4-6. Manual Discovery Wizard, Telnet Parameters

10. To change the CLI mode, click the radio button next to the mode you want PCM to use to communicate with devices: Telnet or SSH.
11. If you selected Telnet, change telnet parameters:
 - a. To configure the telnet manager login, type the new manager user name in the Manager Username field and the associated password in the Manager Password field.
 - b. To configure a telnet operator login, type the new operator user name in the Operator Username field and the associated password in the Operator Password field.
12. If you selected SSH, change SSH parameters:
 - a. Click the radio button to select the SSH version used by PCM to communicate with the device: SSH1 or SSH2.
 - b. Click the radio button to select the Authentication method: Password or Key (SSH2 only).
 - If you selected Password, in the Manager or Operator Password field at the top of the screen, type the user credentials that SSH will use to authorize communication with the device.
 - If you selected Key, type the key in the SSH Key field.

You must define the SSH2 key before attempting to communicate with devices using SSH key authentication. Key authentication is used for SSH2 only.
 - c. In the SSH Port field, type the default port number to be used for CLI SSH communication.
13. Click the Timeout up or down arrow to set the number of seconds to wait for a response from the device. Time-out can be 1-30 seconds, with a default of 15 seconds.
14. In the Retries field, type the number of times to try connecting to the device. From 1-5 retries can be entered, with a default of 3 retries.

15. Click **Next** to discover the device and display the Connection Status window.

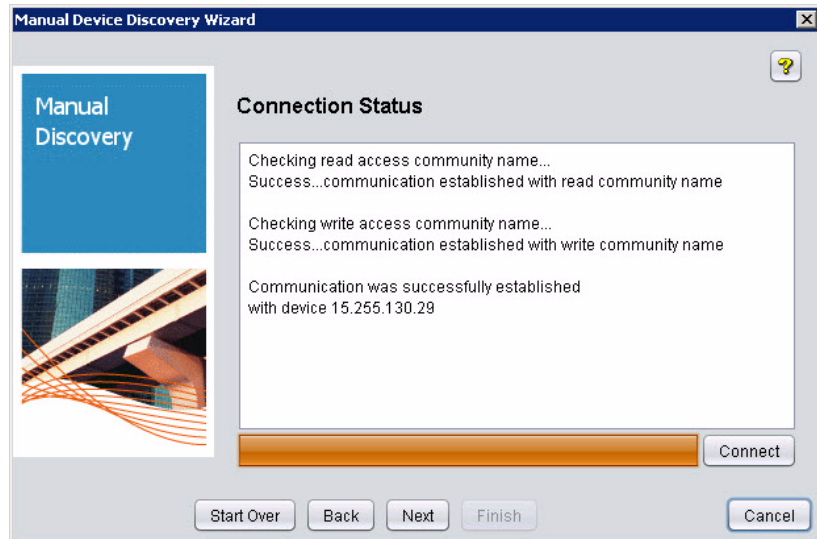


Figure 4-7. Manual Discovery Wizard, Connection Status

PCM attempts to verify the device information and establish a connection with the device using the values you entered. Discovery progress displays in the Connection Status window.

Note:

If the device subnet is already managed by another Agent in the same Agent group, a failure message is displayed and device discovery is stopped.

16. If the IP address or SNMP community is not found, a failure message is displayed. In this case, go back and re-enter the device information and retry.
17. If the device IP has already been discovered, a dialog box displays with the message Device already exists, do you want to delete and re-discover? Click **Yes** to delete the device from the PCM database and re-discover. Click **No** to cancel the manual discovery and the Finished screen will display.
18. Click **Next** to continue the manual discovery process and display the Discovery Status window.

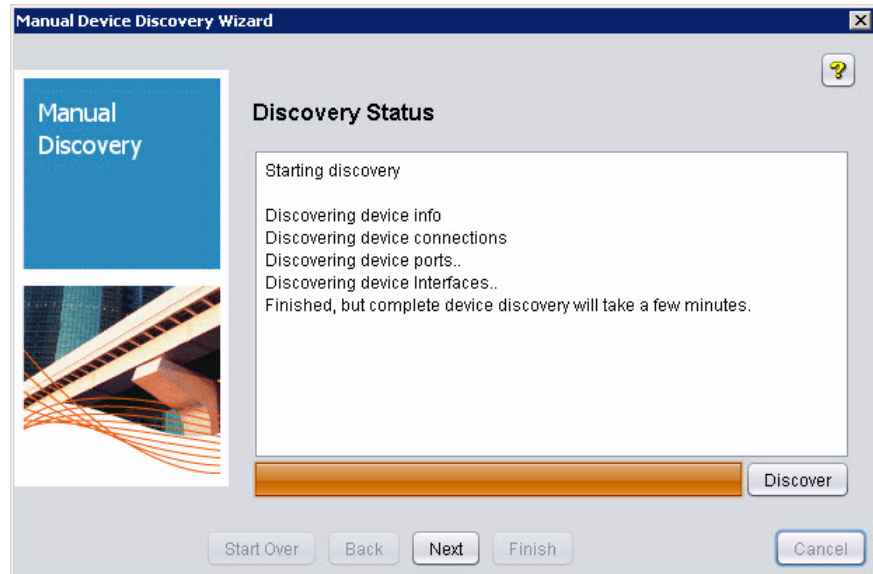


Figure 4-8. Manual Discovery Wizard, Discovery Status

19. Click **Next** to go to the Discovery Finished window.
20. Click **Finish** or **Close** to exit the wizard.

OR

Click **Start Over** to return to the start of the wizard and discover another device.

Using Re-Discover Device

A device must be re-discovered to update PCM data with changes due to any of the following:

- The device was disconnected, then reconnected to another port or device.
- A module has been removed or added to the device.
- Configuration changes are made to the device, such as STP, trunk connection, etc.
- Connections shown for the device in the Network Maps are incorrect.

The Re-Discover Device feature also uses the Manual Discovery Wizard to re-discover a device and update the device attributes stored in PCM. Therefore, example screens have not been included for Re-Discover Device. To re-discover a device:

1. Right-click a device in the navigation tree and select Re-Discover Device from the right-click menu.

This displays the Device Discovery Wizard welcome dialog box.

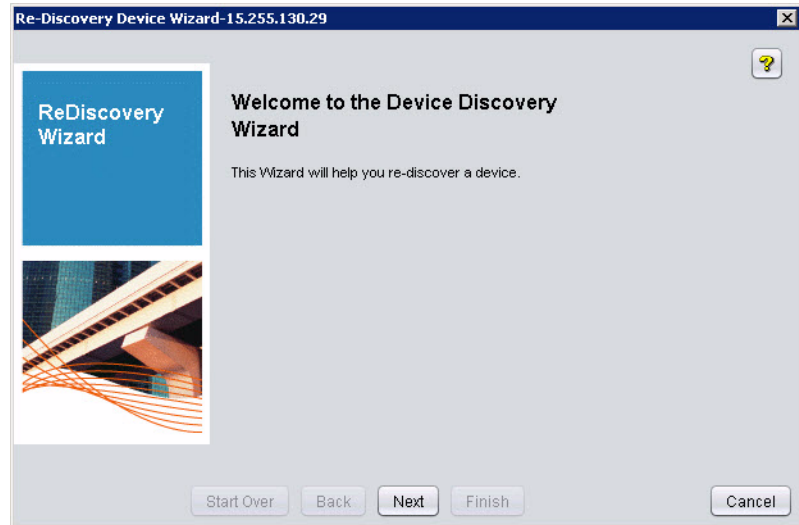


Figure 4-9. Manual Re-Discovery Wizard, Welcome

2. Click **Next** to go to the Device Information window
3. To use the default communication parameters defined in PCM, ensure the Use Device Defaults check box is checked and click **Next**.

PCM attempts to verify the device information and establish a connection with the device. The progress displays in the Connection Status window.

4. If the device connection is successful, click **Next** to continue to the Select Attributes to Rediscover screen. If the device connection fails, return to the Device Information window and perform the following steps.
 - a. Unselect Use Device Defaults by clicking its check box.
 - b. Click **Next** to continue to the windows used to configure the device communication parameters. (Refer to step 8, step 9, and step 10 beginning on page 4-9.)
 - c. When you have set the communication parameters, click **Next** to continue to the Connection Status window.

5. The Select Attributes to refresh window lets you select the device attributes you want to refresh in the discovery database. The default option is to refresh All Attributes.

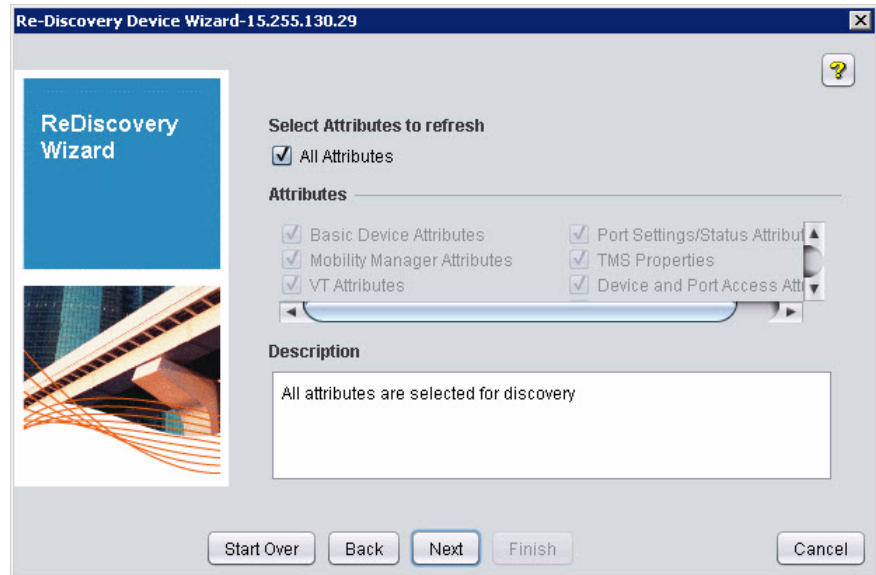


Figure 4-10. Manual Re-Discovery Wizard, Attributes

- a. To refresh all attributes, check the All Attributes check box.
- b. To refresh only selected attributes, uncheck the All Attributes check box and check the check box next to each attribute you want to refresh.
- c. Click **Next** to continue the Re-Discovery process.

The Discovery Status window displays the re-discovery status. When successful, PCM deletes the old selected device attribute and collects and stores the new device attributes in the PCM Discovery database.

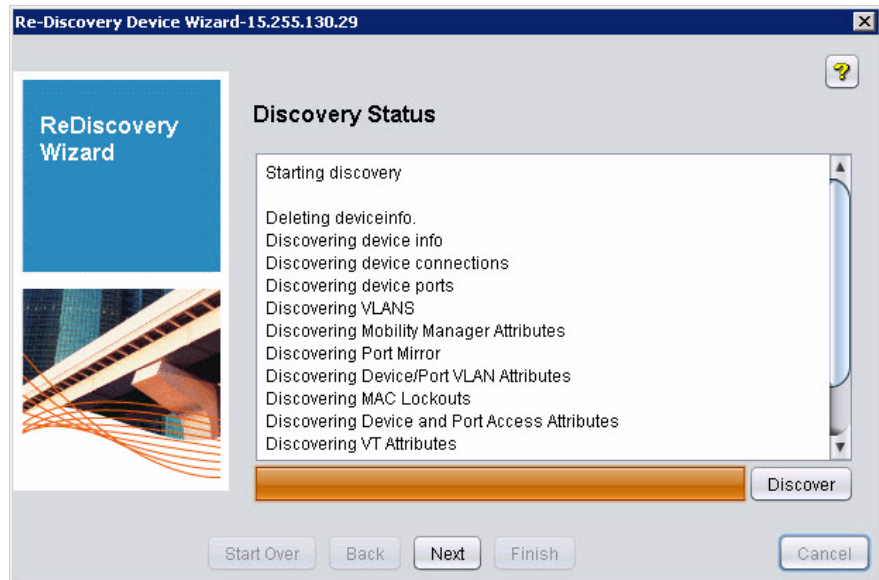


Figure 4-11. Manual Re-Discovery Wizard, Status

Remember, Discovery collects only the basic device and connectivity (port and VLAN) information. To collect detailed device configuration information, Scan the device configuration as described in Chapter 8, "Managing Device Configurations".

Discovering a Loopback Interface

A loopback interface is an interface defined on a Layer 3 device that can be reached from every interface on the router (regardless of VLAN) because it is always routed.

A loopback interface ensures that Layer 3 protocols, such as OSPF and VRRP, always have an open path even if a physical interface fails.

Example: Loopback Discovery

This section provides an example of how a loopback interface is discovered. A device configured with several VLANs and a loopback interface is shown in figure 4-12.

```
3500-Core# show IP
Internet (IP) Service
IP Routing : Enabled
Default TTL      : 64
Arp Age         : 20
Domain Suffix   :
DNS server      :
VLAN            | IP Config  IP Address      Subnet Mask
-----+-----+-----+-----
DEFAULT_VLAN   | Disabled
VLAN31         | Manual     172.16.31.2     255.255.255.0
VLAN100        | Manual     172.16.100.1    255.255.255.0
VLAN200        | Manual     172.16.200.1    255.255.255.0
VLAN220        | Manual     172.16.220.1    255.255.255.0

Loopback Interface
 Loopback      | IP Config  IP Address      Subnet Mask
-----+-----+-----+-----
lo0           | Manual     172.16.31.101   255.255.255
```

Figure 4-12. Sample Loopback Configuration

In this example, VLAN 100 is managed by PCM. The discovery process follows these steps:

1. PCM discovers the device with the IP address 172.16.100.1.
2. PCM checks to see if a loopback interface is configured and discovers the loopback interface 172.16.31.101.

3. If the loopback IP address is reachable (can be pinged) from the PCM server and the subnet to which the loopback IP address belongs is managed by the Agent:
 - PCM replaces the device IP address 172.16.100.1 with the loopback address 172.16.31.101 in PCM maps and on the navigation pane.
 - PCM communicates with the device through its loopback interface.

Note

After the loopback IP address is discovered, at first both the device and loopback IP address are displayed for the device in PCM maps. When implicit groups in PCM memory are refreshed (an internal operation), the device IP address 172.16.100.1 is replaced by the loopback IP address 172.16.31.101.

You must restart the PCM Client in order for the loopback interface to be displayed in the PCM navigation tree.

Loopback Restrictions

The following restrictions apply to loopback interfaces in the discovery process:

- If the seed device is configured with a loopback IP address, PCM does not discover the loopback IP address. Another non-loopback IP address is used to represent the device in PCM.
- PCM does not discover the loopback IP address if the IP subnet is not managed by an Agent.
- For PCM to manage a device using its loopback IP address, PCM must be able to reach the loopback IP address.
- If the loopback IP address is not reachable, PCM discovers the loopback IP address as a subnet and places it in the unmanaged subnets list (Agent Manager > Discovery > Managed Subnet subtab) for the Agent.
- In order for PCM to use a loopback IP address to manage a device, one of the following conditions is required:
 - The device must be discovered manually using the loopback IP address.
 - The loopback IP address must belong to a subnet managed by the Agent, which allows auto-discovery to use the loopback IP address to communicate with the device.
- If a device has multiple loopback IP addresses, any loopback address can be selected from the list in the discovery process.

Port Classification

To support the Access Management and Security functions, the PCM discovery process collects and provides Port Classification information for network devices.

Displaying Port Classification Information

To display port classification information for a device, do one of the following:

- Right-click a device in the navigation tree and select **Port Classification** from the menu.
- Right-click a device in the Devices List tab and select **Discovery > Port Classification** from the menu.

Port Na...	Port Type	Override Port Type	Remote IP ▲	Remote MAC	Remote Device Type	Remote P...
B7	Infrastruct...	Use Discovery Type	172.16.100.7	00:01:E7:A5:B8:C0	2424M	2
B16	Infrastruct...	Use Discovery Type	172.16.100.8	00:1C:2E:8D:4E:5B	7102dl	eth 0/2
B2	Infrastruct...	Use Discovery Type	172.16.100.68	00:0F:61:08:E5:9E	MSM320R	eth1
ADP	Infrastruct...	Use Discovery Type	172.16.100.125	00:12:79:8C:12:FE	Wireless_Serv_zl_Mod	dnlink
AUP	Infrastruct...	Use Discovery Type	172.16.100.125	00:12:79:8C:12:FE	Wireless_Serv_zl_Mod	uplink
CDP	Infrastruct...	Use Discovery Type	172.16.100.126	00:12:79:8C:12:CE	Wireless_Serv_zl_Mod	dnlink
CUP	Infrastruct...	Use Discovery Type	172.16.100.126	00:12:79:8C:12:CE	Wireless_Serv_zl_Mod	uplink
B23	Infrastruct...	Use Discovery Type	172.16.100.150	00:13:21:57:19:C1	2608-PWR	1
F2	Edge	Use Discovery Type	172.16.100.202	00:23:47:7A:06:E3	end node	
F1	Unknown	Use Discovery Type				
B9	Unknown	Use Discovery Type				

Buttons: Refresh, Apply, Close, Help

Figure 4-13. Port Classification

The Port Classification window displays:

- Port Name (port number) on the selected device that is connected to another device on the network.
- Port Type, one of the following:
 - Infrastructure Port, indicates connection to another switch in the network. This is also referred to as inter-switch ports in other areas of PCM
 - Edge Port, indicates connection to an end node device, such as a printer, PC, or Server.
- Override Port Type, one of the following manual classifications:
 - Use Discovery Type (default), indicates that the port classification is assigned by PCM's methodology
 - Infrastructure, indicates the port is connected to another device in the network
 - Edge, indicates the port is connected to an end node device, such as a printer, PC, or Server
 - Unknown, indicates PCM is not able to determine accurately whether the port is infrastructure or edge port.
- Remote IP, the IP address of the attached device (or device port)
- Remote MAC, the MAC address of the attached device (or device port)
- Remote Device Type, the network device type (e.g., 2848) or end node that is connected.

How Discovery Classifies Ports

To classify infrastructure ports the following methodology is used:

1. For links discovered during the "neighbor" discovery, the ports associated with this link are classified as infrastructure ports.
2. When the port classification process determines that the device port is forwarding traffic for only one MAC address that belongs to a switch, the port is classified as an infrastructure port.

To classify operational edge ports the following methodology is used (for ports whose operational status is up):

1. For each port, check the entries in the address forwarding table on the switch (bridge MIB).
2. If the forwarding table for the switch port contains only one MAC address, and if it is associated to a ProCurve or managed switch, then this port is assumed to be connected to an end-node and is classified as an edge port.
3. If the forwarding table for a port has more than one MAC address and that port is not an infrastructure port, the port is ignored and has an UNKNOWN status.
4. If a single MAC address is found in the device port forwarding table, check the ARP table for IP address and MAC address. Use information found in the ARP table to perform a SNMP query to determine if connection is a host or ProCurve device. If the system responds to SNMP and indicates it is a host, the port is classified as an edge port.
5. If the attached device does not respond to SNMP, the device is pinged. If the device is reachable, PCM classifies the port as an edge port.

Finding Nodes and Paths

PCM contains two discovery tools that help you identify:

- Neighboring devices are connected to a network node.
- The path a Layer 2 packet takes to reach a destination address.

Using Find Node

Use the Find Node feature to discover all the neighboring devices connected to the selected network node. A network node can be a switch or a host, such as a PC, server, or printer.

If a switch is specified as the node, Find Node displays all the neighboring devices connected to that switch. If a host is specified as the node, Find Node uses information in the bridge MIB of the switches belonging to the same subnet as the host to find the switch and port number to which the host is connected.

To identify switches connected to the specified switch, Find Node queries the CDP/FDP/LLDP information on the switch. To identify the hosts, Find Node retrieves the ARP and bridge MIB cache on the switch and determines whether each device in the ARP table is directly connected to the specified host. Therefore, only active hosts will be identified.

CLI communication and SNMP read and write access are required for Find Node to provide the correct results.

Note:

If the device is connected to an unmanaged device, the closest managed device is displayed, along with the Unable to find connected device message.

To use Find Node:

1. Ensure that PCM can communicate with the node by testing communication parameters in PCM (right-click device and select **Device Access**>**Communication Parameters** in PCM).
2. Click the **Find Node** button in the global toolbar or select **Tools** > **Diagnostic tools** > **Find Node**.



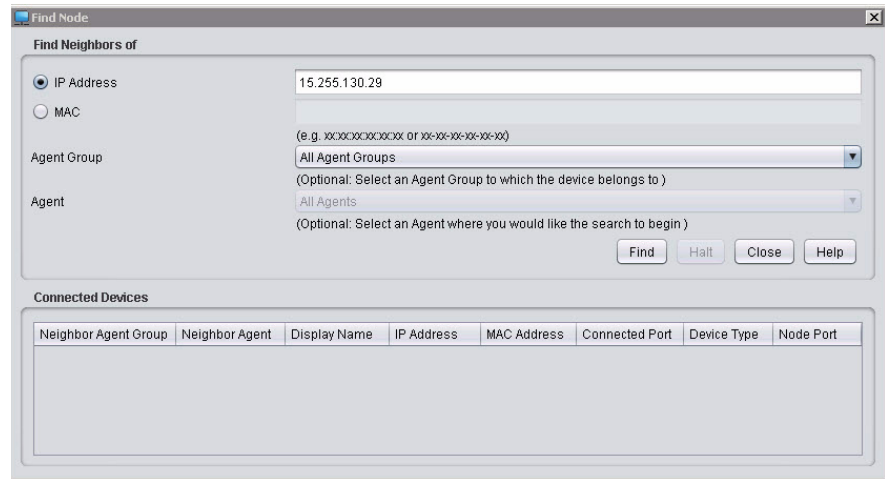


Figure 4-14. Find Node

3. Select IP Address or MAC. The device must be managed (discovered) and reachable by PCM.
 - a. For IP Address, type the IP address or DNS name of the host or switch in the IP Address field
 - b. For MAC, type the MAC address (format **xx:xx:xx:xx:xx:xx**) of the switch in the MAC address field. The MAC address can only be used to specify switches.
4. Use the Agent Group drop-down list to select the Agent group that the node belongs to. You can also select All Agent Groups if you're not sure where the node is located, however searching all Agent groups can take a long time.
5. Optionally, use the Agent drop-down list to select the Agent where the search should begin.

- Click **Find** to run the Find Node process. The DNS name for the specified address will be displayed in the Find Node window and the status of the Find Node process is shown in the status bar above the column headings.

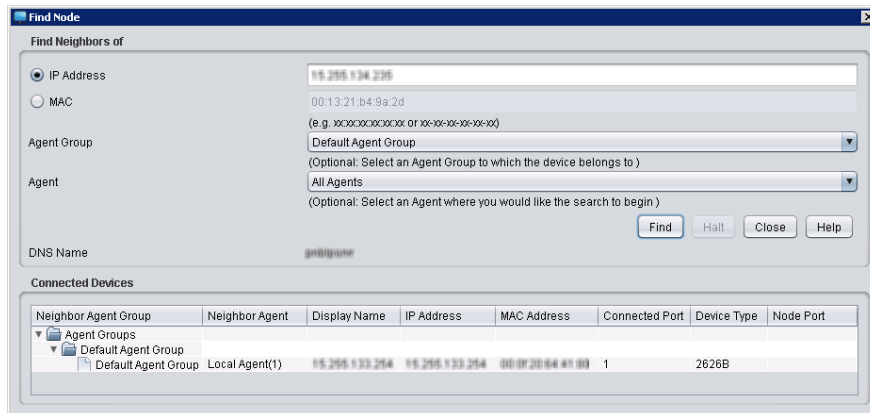


Figure 4-15. Result for a Host

Information for the devices to which the switch is connected is returned, including:

Neighbor Agent Group	Agent group to which the host belongs.
Neighbor Agent	Agent to which the host belongs.
Display Name	Display name or friendly name used in PCM for the switch to which the host is connected. (Naming conventions are defined in Device Access.)
IP Address	IP address of the switch to which the host is connected.
MAC Address	MAC address of the switch to which the host is connected.
Connected Port	Port on the switch where the host is connected.
Device Type	Type of device (Switch/End Point/Access Point/Gateway) that is connected.
Node Port	Node Port is not applicable to End Point nodes, so the field is blank.

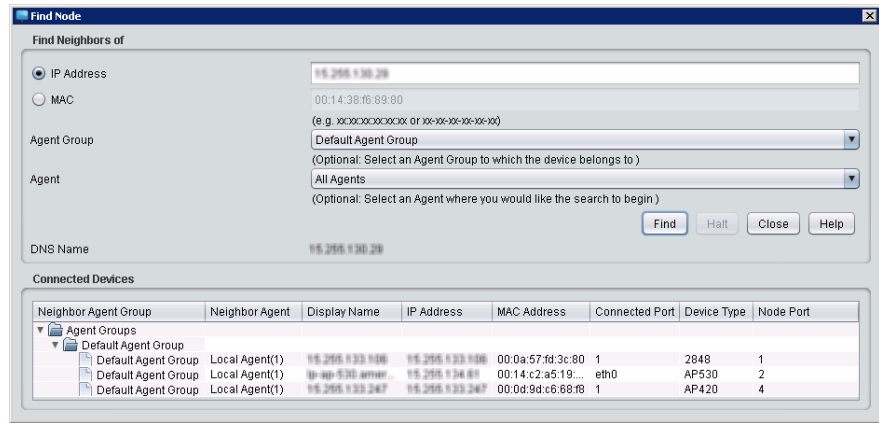


Figure 4-16. Find Node Result for a Switch

If you specified a Switch Node, information for all devices connected to the specified switch is displayed in the Find Node window, including:

Note:

You must click the lever next to the display name to display this field.

Neighbor Agent Group	Agent group to which the switch belongs. Click the lever next to the Agent group to display additional information about the switch. A separate line of information is shown for each port on the selected switch.
Neighbor Agent	The Agent to which the switch belongs.
Display Name	Display name or friendly name used in PCM for the device connected to the switch. (Naming conventions are defined in Device Access.)
IP Address	IP address of the neighboring device to which the specified switch is connected.
MAC Address	MAC address of the neighboring device to which the specified switch is connected.
Connected Port	Port on the neighboring switch to which the specified switch is connected
Device Type	Type of device using the IP address or MAC address that you entered.
Node Port	Port number or friendly name on the specified switch used to connect to the neighboring device.

Using Node-to-Node Trace Path

To help determine the actual connections between devices on the network, you can use the Trace Path function. This feature detects and displays the path a Layer 2 packet takes to reach a destination address. This feature is especially useful when troubleshooting a network with connectivity problems.



1. Click the Trace Path button in the global toolbar or select Tools > Diagnostic tools > Trace Path.

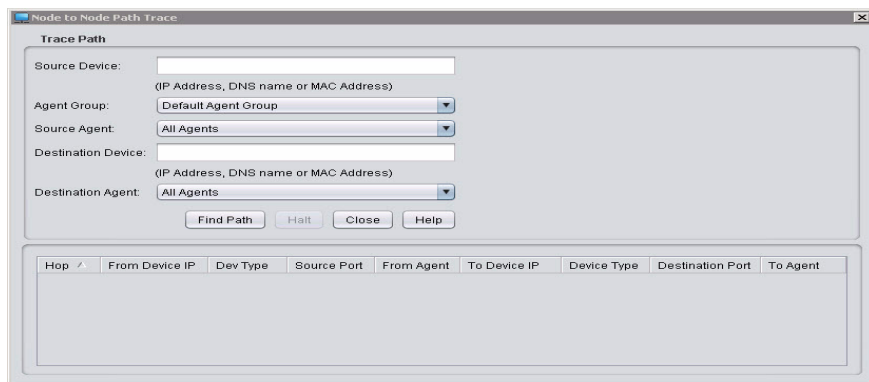


Figure 4-17. Node to Node Trace Path

2. Define the **Source Device** by typing its IP Address, DNS Name, or MAC Address of the device where the packet will originate.
3. In the **Agent Group** field, choose the Agent group where the path search is to be done. This choice is used as a filter to populate the **Source Agent** and **Destination Agent** fields.
4. In the **Source Agent** field, choose the Agent in where the source device was discovered. If you are not sure which Agent to choose, choose **All Agents**.
5. In the **Destination Device** field, type the IP address, MAC address, or DNS name of the intended destination device.
6. In the **Destination Agent** field, choose the Agent where the source device was discovered. If you are not sure which Agent to choose, choose **All Agents**.
7. Click **Find Path**.

The results are returned, listing the devices and hops (connections) between the specified source and destination devices, as shown in figure 4-18.

The screenshot shows a window titled "Node to Node Path Trace" with a "Trace Path" section. The configuration fields are as follows:

- Source Device: 15.255.130.29 (with a note: (IP Address, DNS name or MAC Address))
- Agent Group: Default Agent Group
- Source Agent: All Agents
- Destination Device: 15.255.133.119 (with a note: (IP Address, DNS name or MAC Address))
- Destination Agent: All Agents

Buttons at the bottom of the configuration section are "Find Path", "Halt", "Close", and "Help".

Below the configuration is a table with the following data:

Hop	From Device IP	Dev Type	Source Port	From Agent	To Device IP	Device Type	Destination Port	To Agent
1	15.255.130.29	2608-PWR	1	Local Agen...	15.255.133.106	2848	1	Local Agen...
2	15.255.133.106	2848	1	Local Agen...	15.255.130.29	2608-PWR	1	Local Agen...
3	15.255.130.29	2608-PWR	1	Local Agen...	15.255.133.106	2848	1	Local Agen...

Figure 4-18. Trace Path Results

Managing Discovery Preferences



Use the Discovery tab in the Agent Manager to change the Discovery seed (starting) devices, and configure preferences for each Agent, such as the Ping Sweep and Device Status Polling scans.

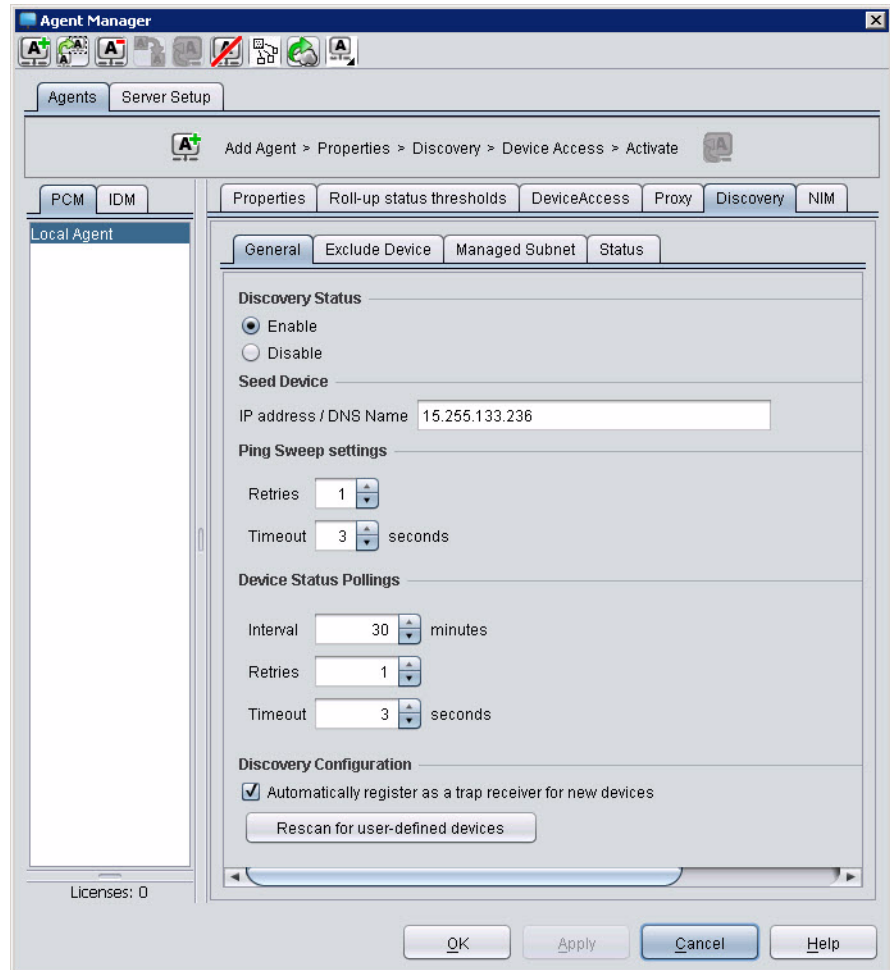


Figure 4-19. Agent Manager, Discovery tab

The Discovery tab in the Agent Manager contains the following subtabs for each Agent:

- The General subtab (explained below) is used to start and stop discovery, and change the seed device, ping sweep settings, and status polling settings.
- The Exclude Device subtab lists all device IP addresses that have been excluded from the Agent and is used to remove device IP addresses from the Excluded List, which enables Discovery to discover the IP address.
- The Managed Subnet subtab is used to add/edit subnets managed by the Agent and remove subnets from those managed by the Agent.
- The Status subtab displays the status of each Discovery component and is used to stop, start, and schedule these components.

Enabling and Disabling Discovery Processes

By default, PCM automatically starts all discovery processes when an Agent starts. However, you can enable/disable discovery or specific Discovery processes and schedule processes for a set time.

To enable or disable all Discovery processes:

1. Select the Agent from the left pane of the Agent Manager, click the Discovery tab in the right pane, and then click the General subtab.
2. To enable the Agent to discover devices, click the **Enable** button (shown in figure 4-19).

Individual discovery processes can be enabled and disabled in the Status subtab of the Agent Manager Discovery tab.

3. To disable discovery, click the **Disable** button.

The default preference for Discovery Status is Enable, indicating that all discovery processes will run as scheduled.

To enable or disable a specific Discovery process:

1. Select the Agent from the left pane of the Agent Manager, click the Discovery tab in the right pane, and then click the Status subtab.

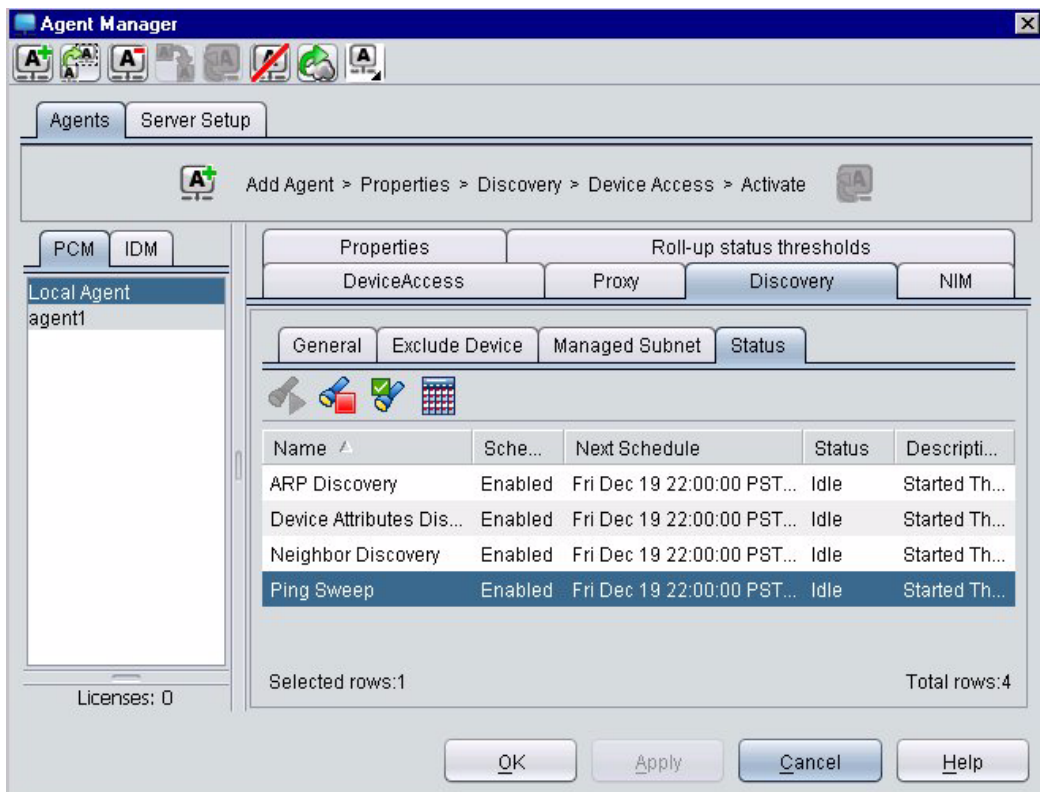


Figure 4-20. Agent Manager, Discovery Status tab

2. Select the Discovery process to be started, stopped, or enabled/disabled.
3. To start the selected Discovery process immediately, click the Start button. If the process is already running, the Start button will be disabled and you must first stop and then start the selected Discovery process.
4. To stop the selected Discovery process, click the Stop button.
5. To save your changes and leave the window open, click **Apply**.

OR

To save your changes and exit the window, click **OK**.

To enable or disable a Discovery process schedule:

1. Select the Agent from the left pane of the Agent Manager, click the Discovery tab in the right pane, and then click the Status subtab.
2. Select the Discovery process for which you want to enable or disable the schedule.
3. To enable or disable the schedule for the selected Discovery process, click the Enable/Disable toggle button. The Enable/Disable toggle button toggles between Enabled and Disabled, depending on whether the schedule for the selected Discovery process is currently enabled or disabled.
4. To save your changes and leave the window open, click **Apply**.



OR

To save your changes and exit the window, click **OK**.

To modify a Discovery process schedule:

By default, Discovery processes are scheduled to run daily at 10:00 P.M. However, the schedule can be modified for each process.

1. Select the Agent from the left pane of the Agent Manager, click the Discovery tab in the right pane, and then click the Status subtab.
2. Select the Discovery process to be rescheduled.
3. Click the Modify Schedule button.



Modify Schedule

Start date

Start date Thu 12/04/2008 22:00

Run at first opportunity if schedule missed (e.g., server down)

Recurrence pattern

Never

Onetime

Hourly

Daily

Weekly

Monthly

Every 1 Day(s)

Skip weekend

OK Cancel

Figure 4-21. Modify Discovery Process Schedule

- In the Start Date section of the Modify Schedule window, use the calendar or up and down arrows to schedule the next date and time to run the selected Discovery process.

OR

Check the Run at first opportunity if schedule missed check box to run the selected Discovery process immediately.

- In the Recurrence Pattern section, define the recurrence pattern:

Never	Select Never to never run the Discovery process from a schedule.
One Time	Select One Time to run the Discovery process on the selected start date and time.
Hourly	Select Hourly and type the hours and minutes to wait between running the Discovery process. To skip Saturdays and Sundays, check the Skip Weekend check box.
Daily	Select Daily and type the number of days to wait between running the Discovery process in the Every x days field. To skip Saturdays and Sundays, check the Skip Weekend check box. The default setting is Daily for all Discovery processes.
Weekly	Select Weekly and check the boxes for the day(s) of the week you want to run the Discovery process. You can select more than one day.
Monthly	Select Monthly and then select Last day of the month to run automatic updates on the last day of each month.

OR

Select Monthly, select Day, and use the up or down arrow to select the day of the month.

Note:

All scheduled policies use the time zone set on the PCM Server. If the policy will be executed by a remote Agent in a different time zone, you must convert the Agent time to PCM Server time to schedule the policy for the correct Agent time. For example, the PCM Server is set to Pacific time (GMT -8 hours) and the remote Agent where the policy will be executed is set to Eastern time (GMT -5 hours). To execute a policy on the remote Agent at 6:00 P.M., set the policy schedule for 3:00 P.M.

- To save your changes and exit the window, click **OK**.

Changing Discovery Preferences

You can change the seed (starting) device, ping sweep settings, and status polling parameters for each Agent.

To change the Seed Device for an Agent:

1. Select the Agent from the left pane of the Agent Manager, click the Discovery tab in the right pane, and then click the Status General subtab.
2. To change the Discovery Seed Device (core ProCurve device), type the IP address of the seed (starting) device in the IP address field. If the IP address entered is invalid or has been discovered by another Agent in the same Agent group, PCM Discovery ignores the entry and continues to use the last valid seed device.

The seed device can be any SNMP network device that is reachable from the selected Agent and has not been discovered by another Agent in the same Agent group. However, we recommend the seed device be a supported ProCurve switch and not an edge switch.

Note:

When using the PCM for OV-NT NNM module, the seed device is the NNM server and cannot be changed, so the Seed Device option is not shown in the Discovery Settings window.

To change Ping Sweep settings:

1. Select the Agent from the left pane of the Agent Manager, click the Discovery tab in the right pane, and then click the General subtab.
2. To change the number of times PCM tries (0-5 retries) to reach a device during the ping sweep phase of discovery, click the ping sweep Retries up or down arrow to display the desired number of retries. You can also type the number of retries.

If a ping response is not received from a device before timeout, Discovery will retry the ping the specified number of times before ending discovery of the device.

3. To change the number of seconds to wait for a response before the ping sweep times out, click the Timeout up or down arrow to increase or decrease the interval (1-10 seconds).

4. Discovery will wait the specified number of seconds (1-10 seconds) for a response from the device. If a response is not received within that time, Discovery retries the ping until the specified number of ping retries is reached. If the number of retries is reached and Discovery has not received a reply, discovery of the device is ended.

To change Status Polling settings:

Status polling monitors the status of managed devices.

1. To change the status polling interval, click the polling Interval up or down arrow to display the number of minutes between status polling scans. You can also type the number of minutes.

Setting the polling interval to 0 disables status polling.

2. To change the number of times to retry a device if a polling response is not received, click the polling Retries up or down arrow to display the desired number of retries. You can also type the number of retries.

When a polling response is not received from a device, the device state is changed to a yellow warning. If a response is not received during the next poll, the device state is changed to a red Unreachable.

3. To change the number of seconds to wait for a polling response, click the polling Timeout up or down arrow to select the number of seconds to wait. You can also type the number of seconds.

To register as a trap receiver:

To automatically register the Agent as a Trap Receiver for newly discovered devices, check the Automatically register as a Trap Receiver for new devices check box.

If you have added user-defined devices, click the Rescan for user-defined devices button to launch a scan for user-defined devices and add any discovered user-defined devices to the navigation tree.

To scan for User-Defined Devices

If you have added user-defined devices, click the Rescan for user-defined devices button to launch a scan for user-defined devices and add any discovered user-defined devices to the navigation tree.

For more information on User Defined Devices, refer to “Adding User-defined Devices” on page 19-9.

Excluding or Deleting Devices from Discovery

Excluding a device stops it from being discovered in all subsequent discoveries and adds it to the Excluded Devices list for the Agent managing the device. Deleting a device removes it from the currently managed devices. The device must also be excluded or it will reappear in PCM and be added to managed devices if detected in subsequent discoveries.

Excluding Devices

Excluding a device removes it from the managed devices of an Agent and excludes it from all subsequent discoveries. An excluded device can be included in discoveries and become a managed device again by removing it from the Excluded Devices list.

To exclude a device:

1. In the navigation tree, right-click the device to be excluded and select Exclude Device from the drop-down list

OR

In a device-related window, right-click the device to be excluded, select Discovery from the drop-down list, and then select Exclude Device from the Discovery drop-down list.

The Select Action window of the Exclude/Delete Device Wizard displays with the selected device IP address in the Devices to Delete list and the Exclude option selected.

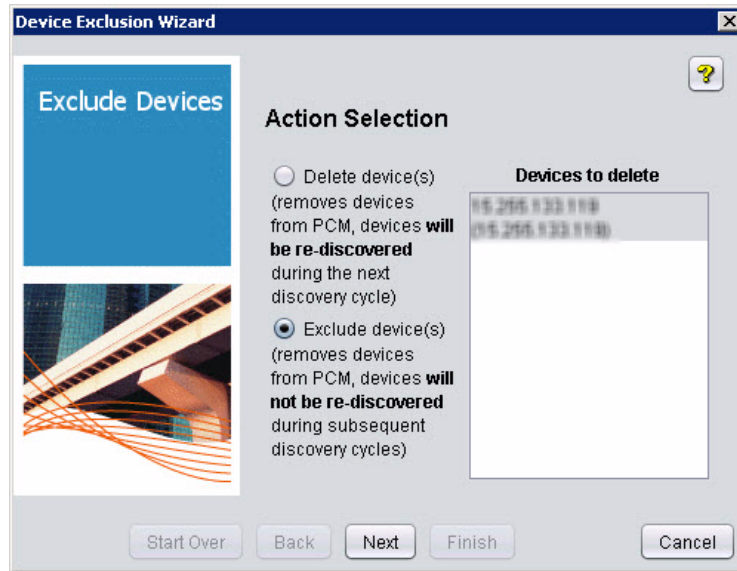


Figure 4-22. Exclude/Delete Device Wizard, Select Action

2. Click **Next** to exclude the device and continue to the Removal Status window. A message is displayed that the device has been deleted. Click **OK**.

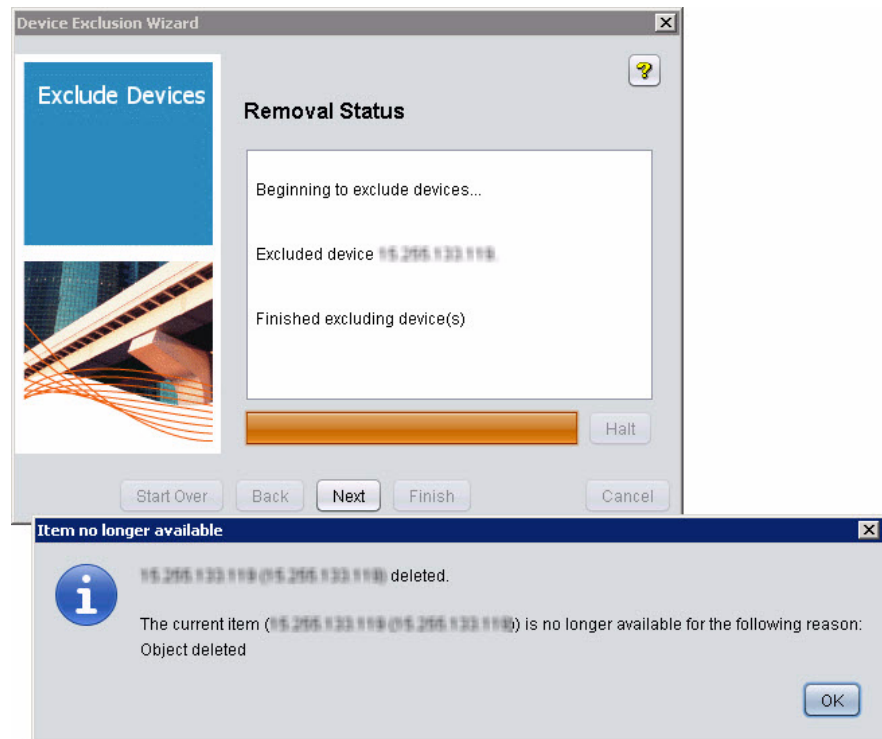


Figure 4-23. Removal Status, and 'Item no longer available' message

3. Click **Next** to continue to the Finish window.
4. Click **Finish** or **Close** to exit the wizard.

When you select the Delete Device option, the same wizard is launched, and the Delete Device option is selected when the wizard opens. Otherwise, the delete process is the same as the exclude process.

To include an excluded device in Discovery:

1. In the left pane of the Agent Manager, select the Agent that manages the device to be excluded, click the Discovery tab in the right pane, and then click the Excluded Device subtab. This tab displays a list of all devices excluded from discovery by the Agent.

Discovering Devices Managing Discovery Preferences

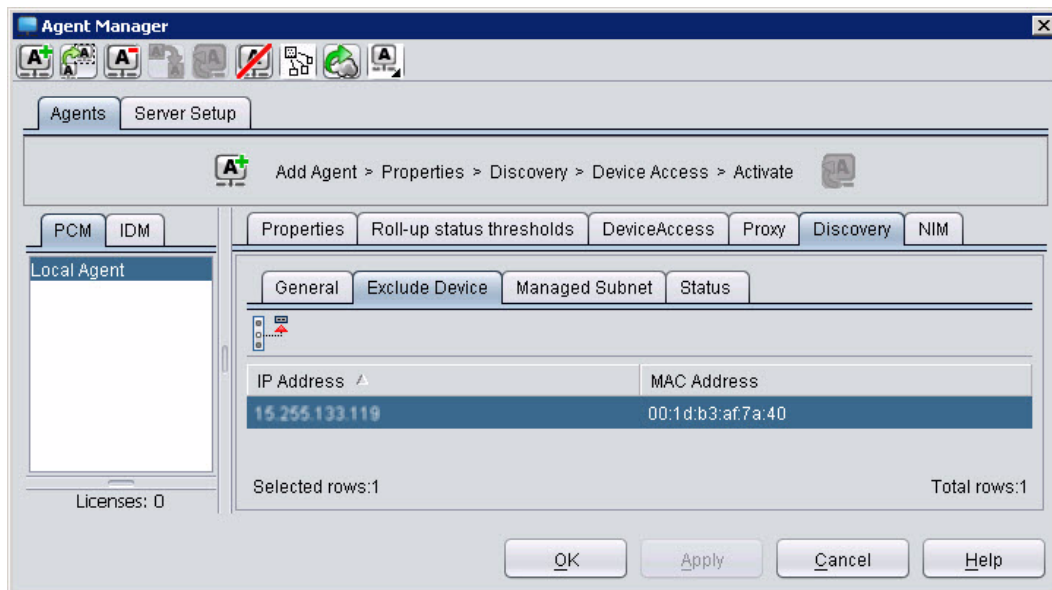


Figure 4-24. Agent Manager, Exclude Device from Discovery

2. Select the device to be removed from the Excluded Devices list and added to managed devices.
3. If you want to rediscover the device immediately after removing it from excluded devices, record the IP address.
4. Click the Remove from Excluded Devices List button on the Exclude Device toolbar. The device will be discovered automatically the next time discovery runs.
5. Once the selected devices are removed from the window, click **OK** to close the window.
6. To rediscover the device immediately without running a complete discovery, run the Manual Discovery Wizard.



To delete a device from Discovery:

Deleting a device removes it from the currently managed devices. The device must also be excluded or it will reappear in PCM and be added to managed devices if detected in subsequent discoveries.

Use the Exclude/Delete Device Wizard to delete devices. Following the Exclude Device instructions except select **Delete Device** from the right-click menu.

Discovery Intervals

In general, the less frequent the discovery intervals, the lower the demands on the CPU of the PCM Server and the less network traffic will be generated for the purposes of discovery.

The fundamental trade-off you should consider when configuring discovery intervals is that less frequent discovery processes result in longer times (on average) before changes in the network are reflected in PCM. So you should start out by asking the following questions:

- How stable is your network? That is, how frequently are devices being added or removed, and how often are sections of the network being re-wired with a different topology? If your network is highly fluid you will want to configure discovery to run more frequently (being aware that it will increase network traffic slightly). On the other hand, if the network is very stable, you might choose to run less frequently, and only at times when there is little other traffic on the network competing for network resources.
- How quickly do you want to see changes in the network reflected in the PCM user interface? If you are willing to tolerate a delay between when a new device is added to the network and when it shows up in PCM, then you can use a longer discover interval.

Configuring Subnets for Discovery

You can configure the subnets to be included in the Discovery process using Managed Subnet subtab of the Agent Manager Discovery tab.

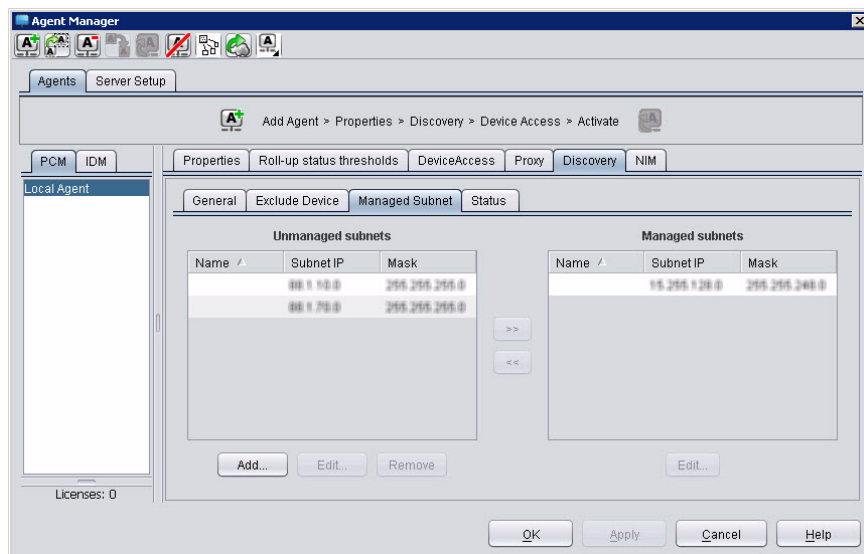


Figure 4-25. Agent Manager, Discovery Subnets

The Managed Subnet subtab lists the subnets that are included in the Discovery process for the selected Agent and all other unmanaged subnets found by the Discovery processes of the Agent.

Note:

Subnets managed by other Agents are not listed. To move a subnet from one Agent to another, see “Managed Subnets” on page 3-27.

To add a subnet to the Managed Subnets list, select the Subnet address in the Unmanaged subnets pane and click >> to move it under Managed Subnets, then click **OK** or **Apply**.

The Inventory pane in the Dashboard reflects the change in number of subnets and devices.

Adding and Modifying Subnets

To add a new subnet to the list of subnets in the Subnets tab of the Agent Manager, click **Add** to launch the New Subnet dialog box.

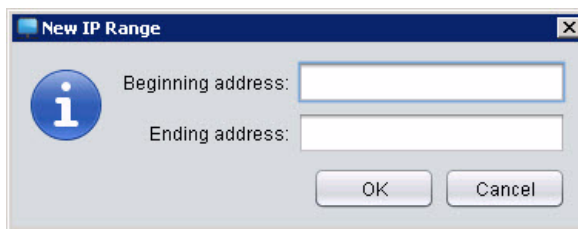
The screenshot shows a dialog box titled "New Subnet". It contains the following elements:

- Subnet Information** section:
 - Name: [Text Input Field]
 - Address: [Text Input Field] Mask: [Text Input Field]
 - Gateway: [Text Input Field]
- IP Address Ranges** section:
 - Restrict to these IP address ranges
 - From: [Text Input Field] To: [Text Input Field]
 - New... [Button]
 - Remove [Button]
- Bottom buttons: OK [Button], Cancel [Button], Help [Button]

Figure 4-26. Add New Subnets dialog box

1. Enter the Subnet information:
 - a. In the **Name** field, enter the "friendly" subnet name
 - b. In the **Address** field, enter the IP Address of the subnet
 - c. In the **Mask** field, enter the Subnet Mask number,
 - d. In the **Gateway** field, enter the IP Address of the Gateway for the subnet.

2. Select the Restrict to these IP Address Ranges option to restrict discovery on the Subnet to the selected IP addresses.
 - a. Click **New...** to add IP address ranges to the available list.



- b. Type the From (starting), and the To (ending) IP addresses to be included in the IP Address range, then click **OK**.

The IP addresses will be validated. If they are not valid, an error message appears. Otherwise, the new IP address range appears in the New Subnet dialog box.

3. When you have entered the Subnet information click **OK**. The new Subnet Address appears in the Unmanaged subnets list.

To remove a subnet:

1. Select the address in the Unmanaged subnets list
2. Click **Remove**. The Subnet address no longer appears in the Managed Subnet tab. When the subnet is removed, all devices in the subnet are also deleted.

You cannot remove a Managed Subnet. Therefore, you must move Managed Subnets to the Unmanaged Subnets list before removing them.

To modify a subnet:

1. Select the Subnet address in the Unmanaged Subnets or Managed Subnets list in the Subnets tab.
2. Click **Edit...** under the list.
3. This displays the Edit Subnet dialog box, similar to the Add Subnet dialog box. Make the desired changes, then click **OK**.

You need to restart the discovery process for the subnet changes to take effect.

Re-Classifying Unknown Devices

In some instances Discovery will be unable to classify an ProCurve device, generally due to a mismatch in the SNMP Management community name settings. This Unknown Devices node contains a list of any devices discovered in the network that are not SNMP accessible but have a valid IP or IPX address

Note:

This feature is not applicable for users of PCM for NNM because there are no "Unknown" devices.

To reclassify an unknown device as an end node:

1. Click the Unknown Devices node in the tree.
2. Select the device to be moved from the Unknown node to the End Node group.
3. Click the Reclassify Device as End Node button.
4. When the confirmation prompt appears, click **Yes** to complete the process.



Note:

Once you reclassify a device as an end node, you cannot change the device classification unless you manually delete and rediscover the device.

To manually reclassify an unknown device:

1. Delete the device from Discovery, as explained in “Excluding or Deleting Devices from Discovery” on page 4-35.
2. Obtain the communication parameters for the device.
3. Manually discover the device, as explained in “Using Re-Discover Device” on page 4-13.

PCM Server Memory Usage

If the number of managed devices in your PCM network increases and/or you are running multiple plug-in modules, you may improve performance on the PCM Server by allocating more memory so that it uses 3 GB RAM. The default memory usage is 1.25 GB.

Prerequisites: The PCM Server should discover more than 3000 devices or at least 2000 devices if multiple plug-in modules are installed. Also, PCM must be running on a 64-bit operating system with at least 6 GB RAM.

Warning: After you reconfigure memory usage, the PCM Server will restart.

To reconfigure memory usage on the PCM Server:

1. Open the Tune PCM Memory Usage window in one of the following ways:



- Click the Preferences button in the PCM toolbar and select the Tune PCM Memory Usage option.
 - Select Tools > Preferences > Tune PCM Memory Usage.
2. Under Tune PCM Server Memory Usage, select **Large Size Configuration** and click **OK** or **Apply**.

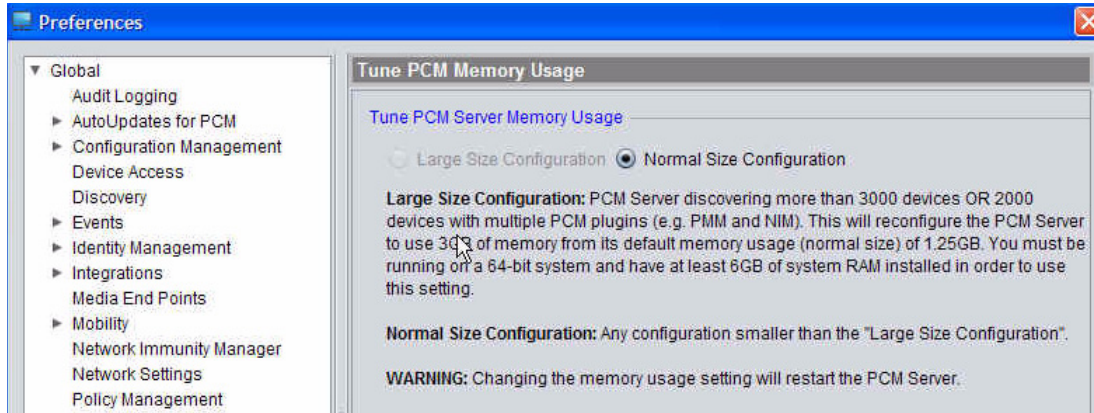


Figure 4-27. Tune Memory Usage in Local PCM Agent

Importing and Exporting Discovery Data

PCM is designed to automatically discover subnets and devices in your network. However, in certain circumstances, you may want to minimize the added network traffic that PCM discovery creates by turning off discovery and importing a list of the subnets and devices that you want PCM to manage.

Similarly, you can export a list of managed subnets and devices from the PCM database in order to:

- Maintain a record of managed subnets (by Agent) and devices.
- Create an asset inventory.
- Use the list as input to other network management applications so that they work with the same set of managed subnets and devices as PCM.

PCM provides the following **Import** and **Export** functions from the Tools menu:

Import subnets	Imports a list of managed subnets or devices from a local file in CSV (comma-separated values) format that is stored on the PCM Client from which you start the import operation.
Import devices	
Export subnets	Exports a list of managed subnets or devices taken from the PCM database to a local file on the PCM Client from which you start the export operation.
Export devices	

Prerequisite for Importing Subnets and Devices: Before you import a file containing a list of subnets and devices to be managed by PCM, you must first create the file in CSV format (one row for each subnet/device) and store it in a local directory on the PCM Client you use to import the file. For information on the valid file format to use, see:

- “Creating an Import File for Managed Subnets” on page 4-49
- “Creating an Import File for Managed Devices” on page 4-53

Note: The format used to create an imported subnet/device file is the same format used in the subnet/device file exported from the PCM database.

Importing Managed Subnets

To import a list of managed subnets from a CSV file on the PCM Client:

1. Create a file of listed subnets as described in “Creating an Import File for Managed Subnets” on page 4-49, and store it locally on the PC on which the PCM Client (from which you start the import operation) is running.
2. Select Tools > Imports > Import Subnets.
3. In the Import Subnets window:

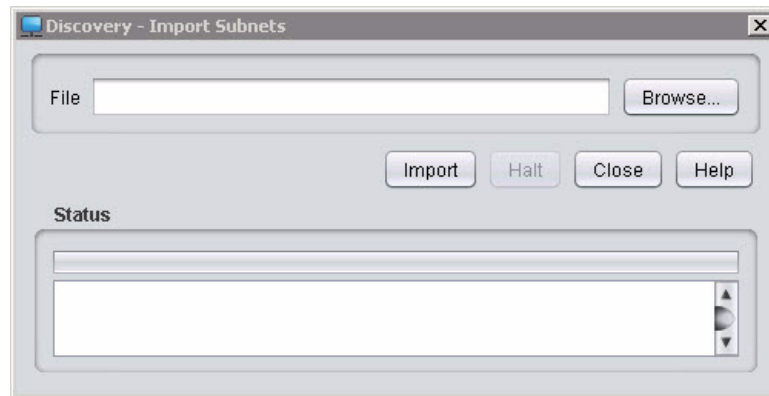


Figure 4-28. Import Subnets

- a. In the File field, type the pathname of the file to import or click the **Browse** button to enter a file stored on your system.
- b. Click **Import**.

The progress of the Import Subnets operation is displayed in the Status field. The Subnet entries in the file are displayed as they are imported into PCM as shown in figure 4-29.

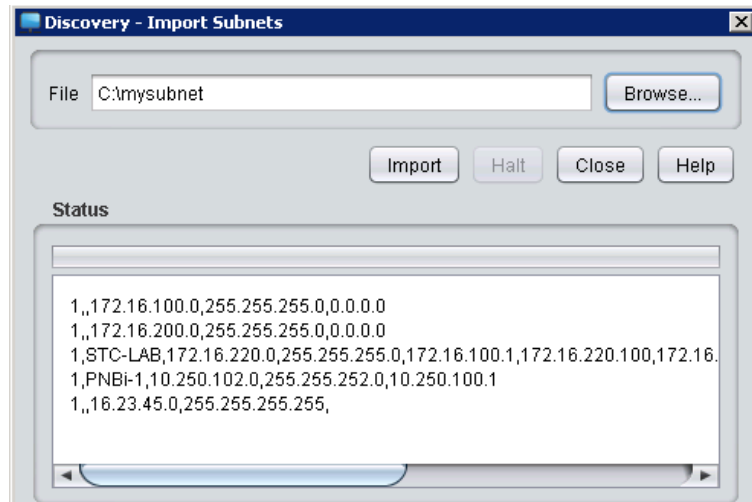


Figure 4-29. Importing Subnets: Status Window

**Notes on
Importing a
Subnet File**

Data for unmanaged subnets cannot be exported from a PCM Client.

When PCM imports the file, it first parses the import file to check for proper syntax. If no syntax errors are found, PCM imports the data into the PCM database.

Exporting Managed Subnets

To export a list of managed subnets to a local file from the PCM database:

1. Select Tools > Exports > Export Subnets.
2. In the Export Subnets window:

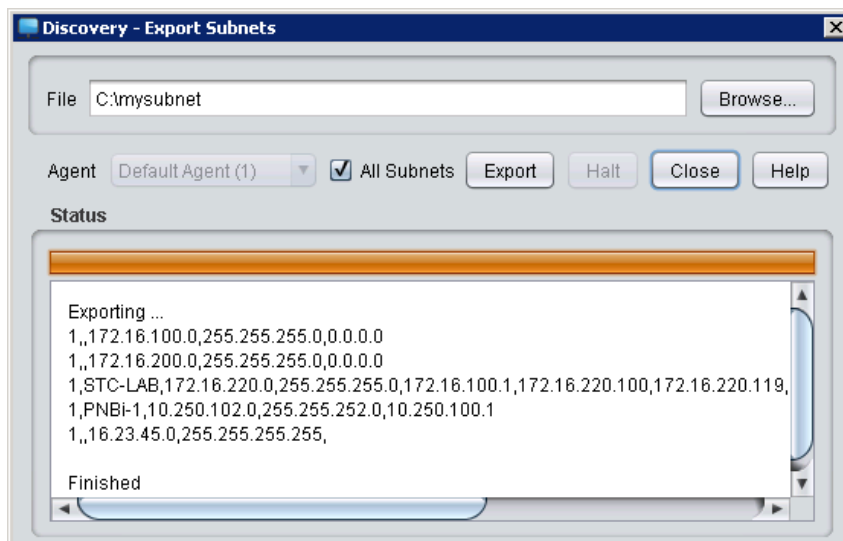


Figure 4-30. Export Subnets

- a. In the File field, type the path and filename of the export file or click the **Browse** button to enter an existing file on your system that you want to overwrite.
- b. By default, the All Subnets check box is selected so that PCM exports a list of all subnets managed by all Agents. To limit the list of subnets to only those managed by a specified Agent, select an Agent from the Agent drop-down list.
- c. Click **Export**.

The progress of the Export Subnets operation is displayed in the Status field as shown in figure 4-30. The subnet file is stored at the specified location on the PCM Client from which you started the export operation.

Creating an Import File for Managed Subnets

To import a list of managed subnets, you must first create a file in CSV format using the following guidelines:

- Enter each subnet on a separate line in the file.
- Be sure to type each entry in the exact CSV format described below. PCM will display an error message if a subnet entry cannot be imported into the database.
- When you finish, store the import file on the PCM Client from which you import the file.

AgentID, Name, Subnet IP address,subnet mask,default gateway,start address,end address,start address,end address,[start address,end address],...

Where:

AgentID is the ID (for example, 1 or 2) of the PCM Agent that manages the subnet.

Name (optional) is the name of a subnet.

Subnet IP address (required) is the network IP address of the subnet.

subnet mask (required) is the network mask of the subnet.

default gateway (required) is the default gateway IP address used by the subnet.

start address (optional) is the start address for a restricted range of subnet addresses; end address (optional) is the end address for a restricted range of subnet addresses.

You can optionally repeat the [start address,end address] parameters to specify an additional range of IP addresses of imported subnets managed by the Agent.

An example of the CSV format used in an import subnet file is shown in figure 4-31. (The same format is generated for an export subnet file.)

```
1,,172.16.100.0,255.255.255.0,0.0.0.0
1,,172.16.200.0,255.255.255.0,0.0.0.0
1,STC-LAB,172.16.20.0,255.255.255.0,172.16.1.1,172.16.20.100,172.16.20.119,172.16.20.20,172.16.20.50
1,PNBi-1,10.250.102.0,255.255.252.0,10.250.100.1
1,,16.23.45.0,255.255.255.255,
```

Figure 4-31. Sample Import Subnet File

Importing Discovered Devices

By using the Import Devices feature, you can quickly configure PCM to discover additional devices. You can include both ProCurve and third-party devices in the import list.

Notes on Importing a Device File

If Discovery is turned off, you can use the Import Devices feature to import a list of the devices that you want to manage with PCM.

PCM uses the agent information in the imported CSV file to configure the Agent that will be used to discover and manage each device.

When PCM imports a device file it first parses the import file to check for proper syntax. If no syntax errors are found, PCM imports the device data into the PCM devices database. Only devices that can be accessed with the specified read community name or the default community name configured in the Device Access preferences can be created in the database.

To import a list of managed devices from a CSV file on the PCM Client:

1. Create a file of listed devices that use SNMPv2 and/or SNMPv3 to communicate with PCM as described in “Creating an Import File for Managed Devices” on page 4-53. Store the file locally on the PC on which the PCM Client (from which you start the import operation) is running.
2. Select Tools > Imports > Import Devices.
3. In the Import Devices window:

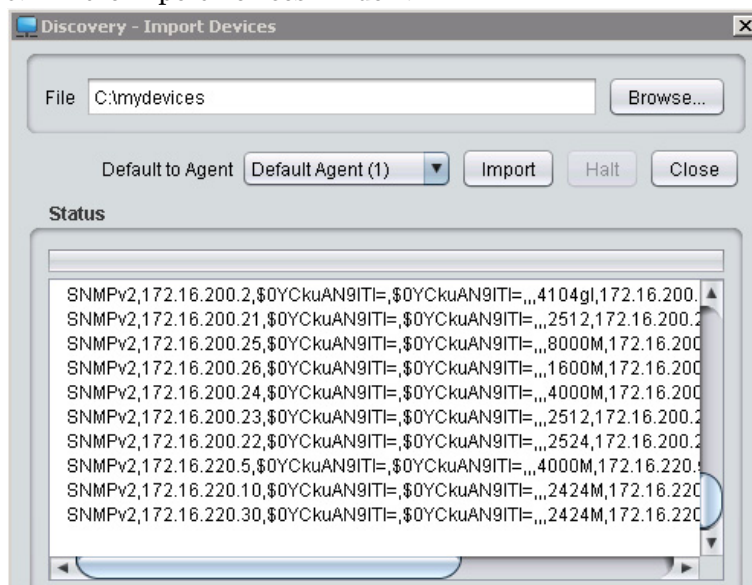


Figure 4-32. Import Devices

- a. In the File field, type the pathname of the file to import or click the **Browse** button to enter a file stored on your system.
- b. (Optional) If no agent information is included in the import file for a device (for example, if the file was created in PCM version 2.3 and no agent information is available), select the Agent that currently manages the device from the Default to Agent drop-down list.

If you import a CSV device file created on PCM version 3.*xx*, the file contains the managing Agent ID for each device. These Agents must be already installed for the devices to be imported into the Agent. In this case, do not select a value from the Default to Agent list.

- c. Click **Import**.

The progress of the Import Devices operation is displayed in the Status field. The device entries in the file are displayed as they are imported into PCM as shown in figure 4-32.

Note that the information on imported devices specifies the version of SNMP used to communicate with the device. See “Creating an Import File for Managed Devices” on page 4-53 for more information.

Exporting Discovered Devices

To export a list of discovered devices to a local file from the PCM database:

1. Select Tools > Exports > Export Devices.
2. In the Export Devices window:

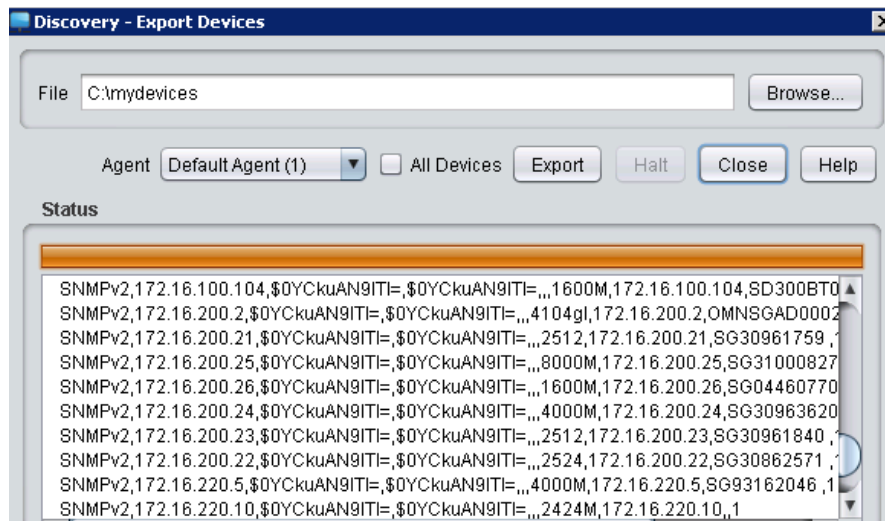


Figure 4-33. Export Devices

- a. In the File field, type the path and filename of the export file or click the **Browse** button to enter an existing file on your system that you want to overwrite.
- b. By default, the All Devices check box is selected so that PCM exports a list of all devices discovered/managed by all Agents. To limit the list of discovered devices to only those managed by a specified Agent, select an Agent from the Agent drop-down list.
- c. Click **Export**.

The progress of the Export Devices operation is displayed in the Status field as shown in figure 4-33. The device file is stored at the specified location on the PCM Client from which you started the export operation.

Note that the information on exported devices specifies the version of SNMP used to communicate with each device. See “Creating an Import File for Managed Devices” on page 4-53 for more information.

Creating an Import File for Managed Devices

To import a list of managed devices, you must first create a file in CSV format using the following guidelines:

- Enter each device on a separate line in the file.
- Be sure to type each entry in the exact CSV format described below. PCM will display an error message if a device entry cannot be imported into the database.
- Note that a different CSV format is used according to whether an imported device supports SNMPv2 or SNMPv3 management.

You can use both SNMPv2 and SNMPv3 formats for imported devices in the same import file or store them in different files

- When you finish, store the import file on the PCM Client from which you import the file.

SNMPv2 Devices

When importing a list of managed devices that use SNMPv2, you must create a CSV file in which each device is described in the following format:

SNMPv2,IP address,read community name,write community name,telnet password,telnet user,AgentID

Where:

SNMPv2 (required) indicates that the device uses the SNMPv2 protocol.

IP address (required) is the IP address of the device or the DNS name; for example, nmdev01.rose.hp.com.

Read community name (optional) is the SNMP read community name configured on the device. If the read community name is not specified, the default read community name specified in the PCM Global Preferences for Device Access will be used.

Write community name (optional) is the SNMP write community name configured on the device. If write community name is not specified, the default write community name specified in the PCM Global Preferences for Device Access will be used.

Telnet password (optional) is the telnet password configured on the device. Some PCM components, such as Configuration Manager, need this information in order to execute CLI commands on the device. If the telnet password is not specified, the default telnet password in PCM Global Preferences for Device Access will be used.

Telnet user — Optional if the device is not configured with a telnet user name. If the device is not configured with a telnet user name, this parameter is required. If the telnet user name is not specified, the default telnet user name in PCM Global Preferences for Device Access will be used.

An example of the CSV format to use to describe SNMPv2 devices in an imported file is shown in figure 4-34.

```
SNMPv2,172.16.100.1,$OYCkuAN9ITI=,$OYCkuAN9ITI=,$z9z3Y8MmjdVTs/ECu9TBbQ==,  
admin,3500yl-PWR,172.16.100.1,SG815TF02F,1  
SNMPv2,172.16.100.2,$OYCkuAN9ITI=,$OYCkuAN9ITI=,$z9z3Y8MmjdVTs/ECu9TBbQ==,  
admin,4108gl,lab201r.tandem.com,SG30961453 ,1  
SNMPv2,172.16.100.101,$OYCkuAN9ITI=,$OYCkuAN9ITI=,$z9z3Y8MmjdVTs/ECu9TBbQ==,  
admin,4000M,172.16.100.101,SG95060151 ,1  
SNMPv2,172.16.100.5,$OYCkuAN9ITI=,$OYCkuAN9ITI=,$z9z3Y8MmjdVTs/ECu9TBbQ==,  
admin,2524,172.16.100.5,SG30862576 ,1  
SNMPv2,172.16.100.12,$OYCkuAN9ITI=,$OYCkuAN9ITI=,$z9z3Y8MmjdVTs/ECu9TBbQ==,  
admin,2626,172.16.100.12,,1  
SNMPv2,172.16.100.100,$OYCkuAN9ITI=,$OYCkuAN9ITI=,$z9z3Y8MmjdVTs/ECu9TBbQ==,  
admin,5308xl,172.16.100.100,,1  
SNMPv2,172.16.100.14,$OYCkuAN9ITI=,$OYCkuAN9ITI=,$z9z3Y8MmjdVTs/ECu9TBbQ==,  
admin,2900-24G,172.16.100.14,LP626KI00J,1  
SNMPv2,172.16.100.20,$OYCkuAN9ITI=,$OYCkuAN9ITI=,$z9z3Y8MmjdVTs/ECu9TBbQ==,  
admin,8212zl,172.16.100.20,SG727BY036,1
```

Figure 4-34. Sample Import File: SNMPv2 Devices

SNMPv3 Devices

When importing a list of managed devices that use SNMPv3, you must create a CSV file in which each device is described in the following format:

SNMPv3, IP address,USM user name,authentication protocol,authentication password,privacy protocol, privacy password,telnet password,telnet user,AgentID

Where:

SNMPv3 (required) indicates that the device uses SNMPv3 protocol.

IP address (required) is the IP address of the device or the DNS name, for example, nmdev01.rose.hp.com.

USM user name (optional) is the user name used to communicate with the device. If the user name is not specified, the default user name specified in the Global Preferences for Device Access will be used.

Authentication protocol (optional) is the authentication protocol used to access the device. Allowed values include MD5, SHA, or NONE. If the Authentication protocol is not specified, the default Authentication Protocol specified in the Global Preferences for Device Access will be used.

Authentication password (optional) is the authentication password set on the device. If an authentication password is not specified, the default authentication password in Global Preferences for Device Access will be used.

Privacy protocol (optional) is the privacy protocol used. Allowed values are DES and NONE. If the privacy protocol is not specified, the default privacy protocol specified in the Global Preferences for Device Access will be used.

Privacy password (optional) is the privacy password configured on the device. If the privacy password is not specified, the default privacy password in Global Preferences for Device Access will be used.

Telnet password (optional) is the telnet password configured on the device. Some PCM components such as Configuration Manager, need this information to execute CLI commands on the device. If the device is configured with a telnet password, this information is needed. If the telnet password is not specified, the default telnet password in Global Preferences for Device Access will be used.

Telnet user (optional) is the telnet user configured on the device. Some PCM components such as Configuration Manager, need this information in order to execute CLI commands on the device. If the device is configured with a telnet user name, then this information is needed. If the telnet user name is not specified, the default telnet user name in Global Preferences for Device Access will be used.

Agent ID identifies the Agent that should manage the device. If importing from PCM 2.xx, the Agent ID is optional. If importing from PCM 3.xx, the Agent ID will be used to import devices. The PCM environment where the devices are being imported must contain an Agent with this ID.

The # (optional) is used for comment

An example of the CSV format to use to describe SNMPv3 devices in an imported file is shown in figure 4-35.

```
SNMPv3,172.16.100.1,Procurve
SNMPv3,172.16.100.2,Procurve,MD5,$Q/YRtzEbQ1bDZQFHrTj0QA==
SNMPv3,172.16.100.12,Procurve,MD5,$Q/YRtzEbQ1bDZQFHrTj0QA==,DES,$Q/YRtzEbQ1bDZQFHrTj0QA==
SNMPv3,172.16.100.100,Procurve,MD5,$Q/YRtzEbQ1bDZQFHrTj0QA==,DES,$Q/YRtzEbQ1bDZQFHrTj0QA==,
$z9z3Y8MmjdVTs/ECu9TBbQ==,admin
SNMPv3,172.16.100.14,Procurve,MD5,$Q/YRtzEbQ1bDZQFHrTj0QA==,DES,$Q/YRtzEbQ1bDZQFHrTj0QA==,
$z9z3Y8MmjdVTs/ECu9TBbQ==,admin,2900-24G,172.16.100.14,LP626KI00J,1
SNMPv3,172.16.100.20,Procurve,MD5,$Q/YRtzEbQ1bDZQFHrTj0QA==,DES,$Q/YRtzEbQ1bDZQFHrTj0QA==,
$z9z3Y8MmjdVTs/ECu9TBbQ==,admin,8212zl,172.16.100.20,SG727BY036,1
```

Figure 4-35. Sample Import File: SNMPv3 Devices

For more information on how to configure Device Access preferences for SNMP, see “Using Global Device Access Preferences” on page 7-40.

Troubleshooting Discovery

Because Discovery uses SNMP, if a device is not SNMP enabled, or if the SNMP Community Names are changed, Discovery may be unable to properly classify and map the device.

If Discovery is not finding or classifying a known device on the network, it may be due to temporary problems on the network or on the device. Try using Manual Discovery. If the Device is found, but is not classified in the correct product group, delete the device and manually discover it or wait until automatic discovery discovers the device.

LLDP Problems

The following LLDP problems can result in Discovery and mapping errors:

- The switch does not appear in the LLDP Neighbors table of an adjacent LLDP device, which may be due to any of the following:
 - Either the port connecting the switch to the adjacent device is not a member of an untagged VLAN, or any untagged VLAN to which the port belongs does not have an IP address.
 - If there is more than one physical path between the switch and the other LLDP device and STP (Spanning Tree Protocol) is running on the switch, then STP will block the redundant link(s). In this case, the switch port on the remaining open link may not be a member of an untagged VLAN, or any untagged VLANs to which the port belongs may not have an IP address.
 - The adjacent device's LLDP Neighbors table may be full. View the device's Neighbors table to determine whether it is full.
- One or more LLDP neighbors appear intermittently or not at all in the switch's LLDP Neighbors table. This may be caused by more than 60 neighboring devices sending LLDP packets to the switch. Exceeding the 60-neighbor limit can occur, for example, where multiple neighbors are connected to the switch through non-LLDP devices such as hubs.
- The same LLDP switch or router appears on more than one port in the LLDP Neighbors table. Where LLDP is running, a switch or router that is the STP root transmits outbound LLDP packets over all links, including redundant links that STP may be blocking in non-root

devices. In this case, the non-root device shows an entry in its LLDP Neighbors table for every port on which it receives a LLDP packet from the root device.

Remedies

If a device is not discovered, try the following remedies:

1. Make sure the device is in a managed subnet. If not, manually discover the device and the device subnet will be automatically added to the managed subnet list in PCM. Furthermore, all connected devices on this new managed subnet will be discovered.
2. If a device belongs to a managed subnet that has not discovered, make sure PCM is configured with the correct read & write SNMP community names for the device.
3. Check the IP authorization table on the device. If the PCM Server IP address is not in the list, add it or clear all entries in the table.
4. When PCM detects a device in the network, PCM tries to communicate with the device using configured SNMP community names. If the community names configured in PCM do not match the device, the device will be listed under the Unknown Device node. After you configure the PCM with the correct SNMP community, delete this device from the Unknown Device node and manually discover the device or wait for PCM discovery to discover the device in the next discovery cycle.
5. PCM discovers networks by looking at the device LLDP/CDP table and the ARP cache. Occasionally, if a device ARP cache contains too many entries the PCM ARP discovery process slows down the PCM discovery capability. Because other discovery processes are blocked by the ARP process. When manually discovering the device with a large number of ARP entries, it appears that the manual discovery wizard is hung.
6. Sometimes the Manual Discovery Wizard freezes because it encounters an exception/error. To ensure there are no errors, check the client/Cs-err.log file for any exception caused by a discovery component. If there is an exception, close the wizard and relaunch the Manual Discovery Wizard for the same device. Report the error to ProCurve Networking.
7. The seed device should be a CORE/MAIN switch in your network, because the fastest method of discovery is LLDP/CDP discovery.
8. If devices in the network are not discovered by the LLDP/CDP or ARP process, PCM depends on the Ping Sweep process. It is important that the subnet mask for the seed device is set correctly. For example, assume that all of your devices are in 10.1.98.0 and 10.1.99.0. If the subnet mask for the

seed device 10.1.98.0 is set to 255.255.0.0, PCM Ping Sweep process starts discovering your network by pinging from 10.1.0.1 to 10.1.254.254. PCM Ping Sweep discovery process will take a long time to start discovering the devices on your network which are in 10.1.98.0 and 10.1.99.0 subnets. In this case you can manually edit the subnet mask in PCM or add the managed subnet in which most of your devices are connected. This will help PCM to discovery all devices in your network quickly.

9. A large number of unnecessary VLANs can also slow down the PCM discovery process. This is especially true when there is an unnecessarily large number of VLANs on the seed device, and can result in the Manual Discovery Wizard appearing to be frozen.
10. When you have a large number of subnets with fewer devices in each subnet and if you choose one the devices as your seed device, PCM only discovers the devices that belong to the subnet of the seed device. Even though PCM finds many devices in the CDP/LLDP table on these discovered devices, they are dropped because they do not belong to the managed network. In this type of network configuration, you must manually add all subnets to PCM. For example, if your network has over 300 subnets and less then 10 devices per subnet, most devices will not be discovered until you add all 300 subnets to the PCM managed subnet list. To avoid this lengthy process, enable PCM to discover all devices and add their subnet to the PCM managed subnet list by add the appropriate subnet mask and mask.

For example, assume you have subnets ranging from 10.1.1.0 to 10.1.150.0. In this case, manually adding a managed subnet with a 16-bit subnet mask like 10.1.0.0 and a mask of 255.255.0.0 enables PCM not to drop/ignore any devices that belong to 10.1.0.0 network.

11. If a routing-enabled switch has two interfaces (e.g., 10.1.50.0 and 10.1.51.1) and each interface is managed by a different Agent, only one Agent can discover the switch.
12. When PCM pings a device and the device does not respond, the device will not be discovered until the next discovery cycle. Disabling and re-enabling discovery for each Agent causes discovery to search for new devices on the network.
13. The SNMP EngineID must be unique for devices. Otherwise, only one device will be discovered.

Special Considerations

- PCM cannot discover the ProCurve Secure Router 7000dl unless the SNMP Agent is enabled on the router (with the `ip snmp agent` CLI command).

Slowing Down Discovery

On a large network OR when there are too many events and traffic data processed by the PCM, discovery, traffic and event PCM components compete with each other for CPU cycles. If this occurs, slow down discovery by change

1. Discovery's Device Attributes Discovery, which by default is scheduled to run daily, requires many CPU cycles because it processes all device attributes and performs many SNMP calls. Schedule this discovery thread to run once a week on Friday night at 22:00 hours OR once every few days. This will help other PCM components to run more efficiently.

Change the schedule on Agent Manager > Discovery > Status.

2. To minimize the discovery attribute thread contribution for any kind of CPU utilization issue on the PCM Agent, set the secondary discovery thread priority and number of secondary threads that get created on the PCM Agent by modifying the following lines in `pcm_agent\xxx\config\DiscoveryAgent.scp`:

```
SECONDARY_THREADS=3 (change it to 1 for one thread)
```

```
SECONDARY_THREADS_PRIORITY=5 (change to 3 or 1)
```

3. Stop and restart the Device Attributes Discovery component on Agent Manager > Discovery > Status. (The Agent does not need to be restarted.)

Using Maps

How Maps Work	5-2
Displaying Maps	5-4
Network Map	5-5
Agents Map	5-6
Agent Map	5-7
Subnet and VLAN Maps	5-9
Mapping Features	5-10
Map Layout Options	5-10
Map Views	5-11
Map Annotations	5-15
Map Legend	5-16
Using the Maps Toolbar Options	5-18
Viewing Network Device Information	5-19
Finding a Device in Maps	5-20
Using Background Images with Maps	5-22

How Maps Work

When ProCurve Manager is started, the Discovery process automatically finds the devices on your network. The Mapping tool uses the information provided by the Discovery Topology scan to create network topology maps. The Mapping tool will automatically create a map of the entire network, and separate maps for the Agents, Subnets, or VLANs you have configured.

During the Neighbor (LLDP) discovery cycle, PCM will generate or update network topology maps to reflect the physical layout of devices in the network, based on the connections found in the Neighbor tables on devices in the network. Discovery also maps wireless devices such as the AP420 and 520wl Access Points, and the 700 series Access Control devices.

All forms of network topology mapping rely on LLDP or CDP. (Devices that do not support LLDP/CDP/FDP, such as AP420, AP520, and WESM modules, cannot detect information about their neighbors.) Therefore, discovery can only map LLDP-enabled devices and ProCurve wireless devices, including:

- LLDP-supported devices
- CDP-supported devices
- FDP-supported devices
- ProCurve Access Points
- ProCurve Wireless Edge Services Modules

All other devices, such as ProCurve 4100gl switches running in router mode, are shown as unmapped devices in maps.

LLDP Mapping Requirement

For mapping to work correctly, LLDP must be enabled for both transmit and receive.

On the ProCurve 2500 Series devices, you must upgrade the switch software to version F.05.60 to enable LLDP transmit and receive. Earlier versions of switch software support only LLDP transmit and did not map correctly.

Agent, Subnet, and VLAN maps, which are subsets of the Agents map for an Agent Group, are created when the VLAN discovery cycle is completed.

To create the Agent maps, PCM identifies all Agents in each Agent Group and all devices and links in each Agent. PCM also identifies all links between Agents in an Agent Group.

To create the Subnet map, Discovery extracts all the links (a connection between two devices) for all devices in the Agent map. For each link it determines if the connected devices belong to the subnet being mapped. If the devices for the link belong to the subnet being mapped, they are added to the Subnet map.

To create the VLAN map, for each link extracted from the Agent map, Discovery will determine if the connected ports for the link belong to the VLAN being mapped. If the ports for the link belong to the same VLAN ID, then Discovery adds the link to the VLAN map.

In addition to these maps, you can use the Find Node feature to get information about connections between network nodes. See “Finding Nodes and Paths” on page 4-22 for details.

Displaying Maps

To display all available maps for an agent group, click on the Agent's Network Map node in the PCM navigation tree. Click an entry under Agents, Subnets, or VLANs to display its map.

Each map provides a graphical view of the specified area of the network. The view differs according to the node level you select:

- The Network Map provides a graphical view of the physical layout of a managed network and displays the connectivity and status of devices discovered in the network, including third-part devices.
- The Agents Map provides a graphical view of the physical layout of all Agents (local and remote) defined in the selected Agent Group.
- The Agent Map provides a graphical view of the physical layout of all devices managed by the Agent and displays the connectivity and status of these devices.
- The Subnet Map provides a graphical view of all devices in the selected subnet.
- The VLAN Map provides a graphical view of all devices using the selected VLAN.

Each map is described in detail in this section. From a map window, you can access map-related features, such as changing the view, adding a background image, and finding a device in the map. See “Mapping Features” on page 5-10 for more information.

Refreshing a Map

Maps are refreshed and redrawn at the completion of each discovery cycle (LLDP discovery process).



In addition, you can perform a manual refresh of a Network, Subnet or VLAN map by clicking the Refresh a Map button in the toolbar.

A manual refresh is sometimes necessary if, after PCM completes the initial discovery, a map does not display all links between connected devices. Without a manual refresh, the missing links may not be added until a later discovery cycle completes.

Status information is based on the status of the device (available, not available, etc.) when the last Status Polling discovery was performed on the device.

Network Map

Clicking the Network Map node in the navigation tree displays the Network Map window, which provides a graphical view of the physical layout of a managed network. Maps display the connectivity and status of devices discovered in the network, including third-party devices.

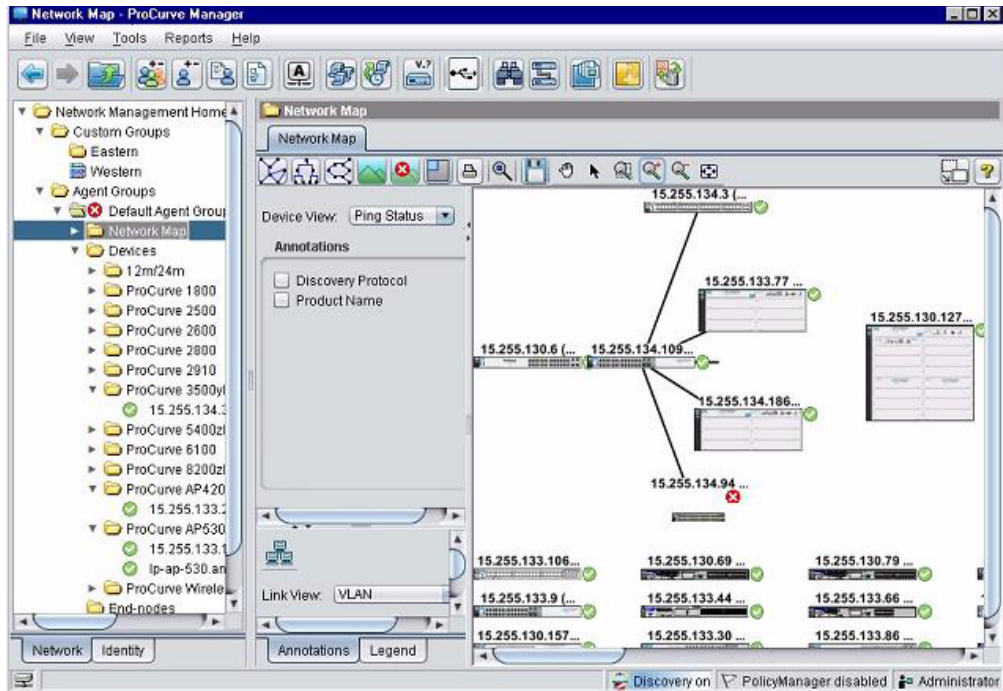


Figure 5-1. Network Map

A device label is displayed next to each device in the map. The format used to label a device is configured with the Device Display Name value in the Device Access Preferences window.

Mousing over a device or its label displays additional information. You can view device properties by double-clicking a device or right-clicking a device and selecting View. The right-click menu also provides access to other PCM functions, such as the Go to Map function described in “Finding a Device in Maps” on page 5-20.

You can display additional link information by selecting options in the Annotations pane at the left of the map, as described in “Mapping Features” on page 5-10. Available annotations can vary based on the device and ProCurve applications in use on your network.

The Legend tab at the left of the map identifies the colors and symbols used to identify the device, security, traffic, and link status shown in the map.

Devices that have been discovered, but cannot be mapped (because they are not LLDP, or CDP enabled) are displayed without connections to the rest of the network.

Double-clicking an icon on the map displays the device's Dashboard, and right-clicking a device provides access to standard right-click functions and the Go to Map function explained in "Finding a Device in Maps" on page 5-20

Agents Map

Click the Agents node under the Network Map node in the navigation tree to display the Agents Map.

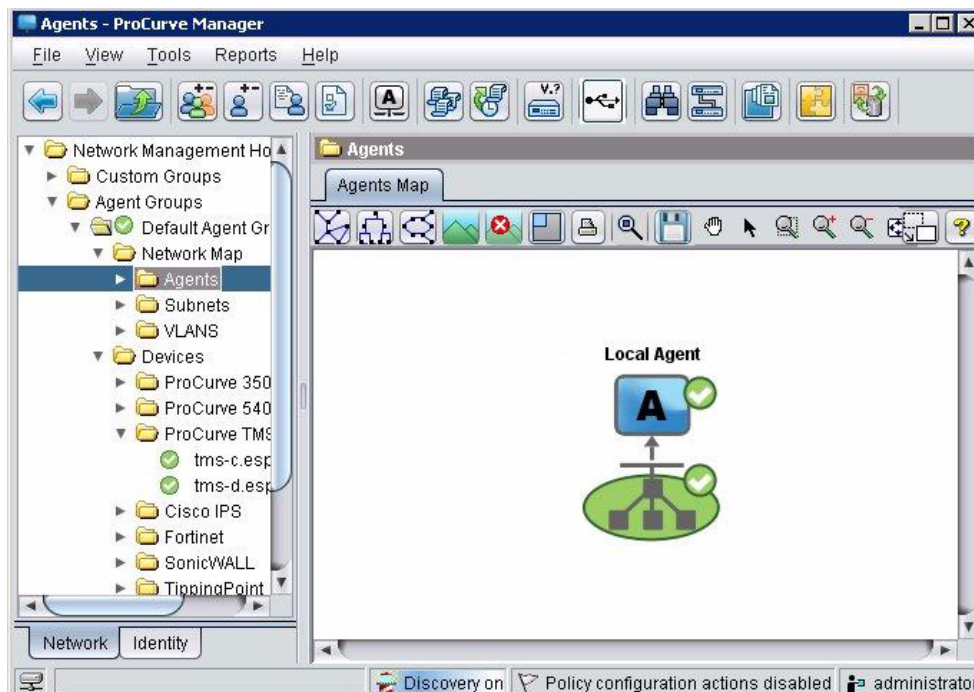


Figure 5-2. Agents Map

The Agents Map provides an overview of the physical layout of all Agents (local and remote) in the selected Agent Group. There are six possible Agent states:



Agent up, devices are reachable.



Agent up, at least one device is in warning state.



Agent up, at least one device is unreachable.



Agent down, devices were reachable when Agent went down.



Agent down, at least one device was in warning state when Agent went down.



Agent down, at least one device was unreachable when Agent went down.



Double-clicking an Agent on the map displays the devices managed by the Agent.

The Annotations and Legend tabs are not available for Agents maps.

Agent Map

Click a specific Agent node under the Network Map node in the navigation tree to display the Agent Map.

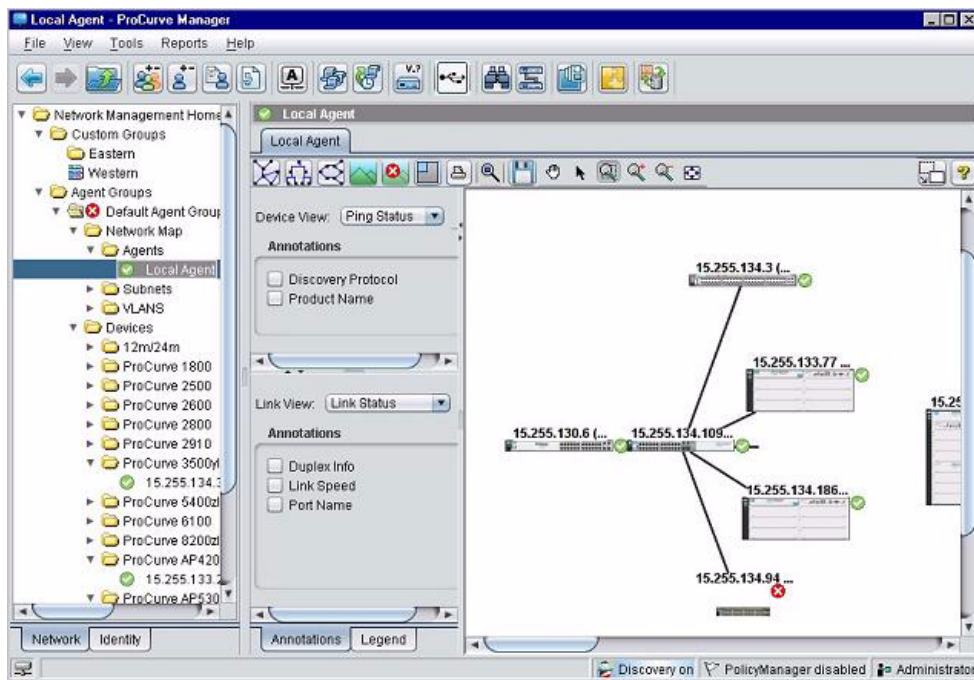


Figure 5-3. Map for a Specific Agent

The Agent Map provides an overview of the physical layout of all devices managed by the Agent and displays the connectivity and status of these devices. Green device icons indicate that all devices managed by the Agent are reachable, red device icons indicate that at least one device managed by the Agent is unreachable, and yellow device icons indicate that at least one device is in a warning state.

A device label is shown next to each device in the map. These device labels are based on the Device Display Name selected in the Device Access Preferences. You can display additional link information by selecting options in the Annotations pane at the left of the map, as explained in “Mapping Features” on page 5-10. Available annotations can vary based on the device and ProCurve applications in use on your network.

The Legend tab at the left of the map identifies the colors and symbols used to identify the device, security, traffic, and link status shown in the map.

Devices that have been discovered, but cannot be mapped (because they are not LLDP, or CDP enabled) are displayed without connections to the rest of the network.

Double-clicking an icon on the map displays the device's Dashboard, and right-clicking a device provides access to standard right-click functions and the Go to Map function explained in "Finding a Device in Maps" on page 5-20

Subnet and VLAN Maps

Maps are also available that show the devices in a managed subnet or VLAN. Subnet and VLAN maps contain the same layout options as the Network Map.

To view the map for a specific subnet or VLAN, expand the Agents node in the navigation tree, then expand the Subnets or VLANs node to display individual subnet addresses and VLAN IDs. Click the subnet address or VLAN ID to display the related map.

Definition:

Managed Subnet: A subnet within the Network Infrastructure that has been added to the ProCurve Manager's managed device list.

In PCM+, the VLANs map window also contains a Port Properties tab, which you can use to review the VLAN's port configurations. For more information on configuring and managing VLANs, refer to Chapter 9, "Using VLANs".

Mapping Features

Map Layout Options

Note:

Customized map layouts and background images are lost when upgrading to PCM 3.x.

The map layout default uses the "physical" map layout. That is, it reflects the physical wiring or layout. Map layout options are disabled when a background image is used.

The Mapping tool provides the following other options for map layout. When another layout is selected, all subsequently discovered devices are arranged in this layout.



Radial Tree Layout- Arranges the nodes in a tree radially, with branches determined by device link. Nodes are partitioned into levels, and levels are arranged in circles or ellipses around the root. This is the PCM default layout type when the map is displayed for the first time.



Tree Layout - Arranges nodes at each level horizontally, connected vertically to other levels, starting with the root node at the top.



Hierarchical - Arranges the nodes hierarchically by level (top to bottom and left to right), so that the majority of links point in the same direction.



UniformLengthEdges - Arranges the nodes hierarchically with all edges of uniform length.

In the above layouts, the device positions are not preserved. Rather, the layout type is preserved.

User Defined Layout - You can manually arrange nodes on the map and then click the **Save** button on the Map toolbar to save your changes. After saving the layout, device positions are fixed and the layout is preserved, even after the Client is restarted. If a new device is discovered, it is placed below the discovered devices.

The First four layouts are ideal when discovery is running since it produces a clutter-free map. The User defined layout is ideal once discovery has almost completed.

Note:

If a new device is discovered or the Client is restarted, the current layout is applied to the entire map and the old layout is lost.

If you save manual changes in one layout and later save a different layout, the initial changes are lost. If you save manual changes in one layout and later select a different layout type, PCM assumes you want newly discovered devices to be in the new layout type, so the changes saved in the first layout type are lost.

Map Views

You can select a variety of device and link views that provide special annotations in a map.

Ping Status Device View

Selecting Ping Status as the device view for a map lets you display the Discovery Protocol used to discover each device in the map and the Product Name. When Discovery Protocol is selected, labels appear next to each device, indicating the LLDP, CDP, or FDP protocol in use and whether it is on or off. When Product Name is selected, labels appear next to each device, indicating the product name (e.g., 5408).

The ping status of each device is shown by color-coded device icons next to the device, as described in the Legend tab.

To enable Discovery Protocol or Product Name:

1. Navigate to the Network, Subnet, or VLAN Map window by selecting the desired node in the navigation tree.
2. Click the Device View drop-down arrow in the Annotations tab of the left pane and select **Ping Status**.
3. Check the Discovery Protocol and/or Product Name check boxes.

Security State Device View

Selecting Security State as the device view of a map lets you display the number of security alerts reported by NIM during the configured time interval for offenders connected to each device in the map. Depending on the options you select, a label appears below each device indicating the category and/or severity of all alerts received for the device. The time span encompassing the alert totals and the refresh interval for the security state can also be set for Security State totals.

The Security state of each device is shown by color-coded device icons, as described in the Legend tab, and is based on the most severe security alert from offenders connected to the device in the configured time window.

1. Navigate to the Network or Subnet Map window by selecting the node in the navigation tree.
2. Click the Device View drop-down arrow in the Annotations tab of the left pane and select **Security State**.
3. Check any combination of the following check boxes:

Security Totals by Category: Display the number of alerts reported by External and ProCurve sources which pertain to offenders that are connected to each device.

Security Totals by Severity: Display the number of minor, major, warning, and critical alerts which pertain to offenders that are connected to each device.

1. To change the time span encompassed in the totals, in the Time Window fields, select 1-9000 minutes or hours. For example, setting this value to 2 hours shows the number of security alerts reported by NIM for all devices during the previous 2 hours. The default is 60 minutes.
2. To change how often the totals are updated, in the Update Rate fields, select 1-60 minutes or hours. The default is 5 minutes.
3. Click **Apply**.

Link Status View

The Link Status annotation displays the status of each link and optionally displays duplex information, link speed, and name of the port being used for the connection. When selected, labels containing the selected information appears on the appropriate link(s).

The link status of each device is shown by color-coded lines, as described in [the Legend tab](#).

To display link status:

1. Navigate to the Network, Subnet, or VLAN Map window by selecting the node in the navigation tree.
2. Click the Link View drop-down arrow in the Annotations tab of the left pane.
3. Select **Link Status**.

4. To display duplex information for the links between network switches, check the Duplex check box. If duplex mode is configured, a label appears next to the link connector, indicating the duplex mode configured at each end of the link:

HDx/HDx : Half duplex/Half duplex

FDx/HDx: Full duplex / Half duplex (and vice versa)

FDx/FDx: Full duplex / Full duplex

To display the link speed configured on connected devices shown in the map, click the Link Speed check box to display the link speed. A label appears next to each link, indicating the connection speed for each end of the link (e.g., 100/100Mbps, or 1000/1000Mbps).

To display the port names used for the device connections, check the Port Name check box. A label appears next to each link, identifying the port on the device at each end of the connection (e.g., 6/49, or A1/F1).

VLAN Link View

The VLAN link view displays color-coded VLAN(s) and optionally displays duplex information, link speed, and name of the port being used for the connection. When selected, a label containing the selected information appears next to each device. You can view up to three VLANs at once, with all links in a VLAN color-coded the same.

Note:

The VLAN link view is not available on a Subnet map or VLAN map.

The link status of each VLAN is shown by color-coded lines, as described in the Legend tab.

To display VLAN link status:

1. Navigate to the Network Map window by selecting the Network Map node in the navigation tree.
2. Click the Link View drop-down arrow in the Annotations tab of the left pane.
3. Select **VLAN**.
4. Select the VLAN by clicking the Select VLAN button and selecting the desired VLAN(s).



5. To display duplex information for the links between network switches, check the Duplex check box. If duplex mode is configured, a label appears next to the link, indicating the duplex mode configured on the VLAN:

HDx/HDx	Half duplex/Half duplex
FDx/HDx	Full duplex / Half duplex (and vice versa)
FDx/FDx	Full duplex / Full duplex
6. To display the link speed configured on connected devices shown in the map, click the Link Speed check box to display the link speed. A label appears next to each link, indicating the connection speed for each end of the link (e.g., 100/100Mbps, or 1000/1000Mbps).
7. To display the port names used for the device connections, check the Port Name check box. A label appears next to each link, identifying the port on the device at each end of the connection (e.g., 6/49, or A1/F1).

Traffic Link View

Selecting Traffic Link View displays color-coded links identifying traffic conditions and optionally annotations that identify the source and destination devices and ports.

If separate Transmit and Receive statistics are available, the Traffic Link View displays two dashed link lines representing the worst measurement going into and out of the device. Note that each measurement could be from different metrics.

The Traffic Link View annotation displays the status of each link and optionally displays traffic violations. The link status of each device is shown by color-coded lines, as described in the Legend tab. This lets users trace link utilization and traffic on all links, and gives them a broad view of network utilization so they can diagnose problem areas when utilization exceeds the limits.

To display traffic link status:

1. Navigate to the Network, Subnet, or VLAN Map window by selecting the node in the navigation tree.
2. Click the Link View drop-down arrow in the Annotations tab of the left pane.
3. Select **Traffic**.
4. To display an annotation for ports with traffic violations, check the Show Violation Ports check box.

Selecting this option displays the port name when a critical or warning traffic threshold is exceeded for the port.

Map Annotations

Available annotations vary based on the device and ProCurve applications in use on your network.

You can view device properties by double-clicking a device or right-clicking a device and selecting *View*. The right-click menu also provides access to other PCM functions.

Maps are refreshed automatically when devices and links change. Status information is based on the status of the device (available, not available, etc.) when the last Status Polling discovery was performed on the device. When the Security State device view is selected, the status is based on the most severe security alert from offenders connected to the device in the configured time window.

Discovered devices that are not LLDP/CDP/FDP enabled are shown below the connected devices, and devices excluded from Discovery are not shown. For example, ProCurve 4100gl switches running in router mode are not shown on maps.

Operating Notes for annotation labels:

- The port labels appear at the end of the link nearest to their corresponding ports.
- A port can have only one label. If the user selects multiple check boxes in the Annotations pane on the left side of the map, the values get appended to the displayed label instead of adding one more label.

Map Legend

Clicking the Legend tab at the bottom of some map windows displays a legend identifying the symbols used in map.

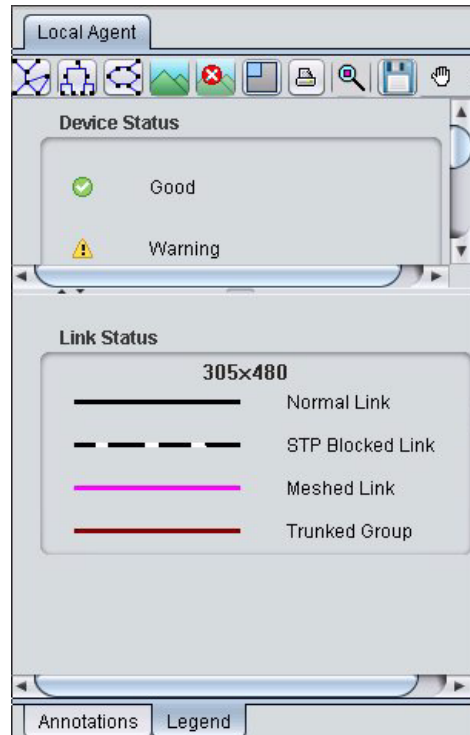















Figure 5-4. Map legend

The displayed legend varies depending on the Device View and Link View selected in the Annotations tab. Legend options are:





Device Ping Status:

-  Good (device up)
-  Warning state
-  Unreachable
-  Unknown (no status available)
-  Good, Agent Unreachable
-  Warning, Agent Unreachable
-  Unreachable, Agent Unreachable
-  Unknown, Agent Unreachable
-  Warning, Acknowledged
-  Unreachable, Acknowledged
-  Unknown, Acknowledged





Security State:

-  Normal (device up)
-  Warning
-  Minor
-  Major
-  Critical

Link Status:

-  Normal link, which indicates the link between devices is up
-  STP blocked link, which is any redundant physical path to serve as a backup (blocked) path in case the existing active path fails
-  Meshed link, which indicates a group of meshed switch ports exchanging meshing protocol packets.
-  Trunked group, which indicates a trunked port connection. Refer to the configuration manuals that came with the switch for details on port trunking.

Traffic Status:

-  Normal (no violation)
-  Warning threshold violation
-  Critical threshold violation
-  No Data Available

VLAN:

Shows a different color for each VLAN and the VLAN number

Using the Maps Toolbar Options

In addition to map layout options, the Toolbar in the Maps windows includes buttons for changing the map background, and map viewing functions. Each tool (button) is described below in the order in which it appears in the toolbar, reading from left to right.



Figure 5-5. Maps toolbar

Note:

Map Layout options are described in “Map Layout Options” on page 5-10



Map Overview: Launches a separate sub-window on top of the main map. The overview shows the entire topology related to the network in the main window, with any selected devices or network area highlighted. This is useful when you have zoomed in on a specific area of the network in the main window, and want to refer to its location in the overall network without losing the zoom focus.



Print Map: Lets you print a copy of the selected map using the standard Windows print functionality.



Locate Device in Map: Lets you locate the node or device in the map by using the IP address. Click the button to display the Locate a device in Map dialog box. Enter the IP address of a device, then click OK. If the device exists on the map it will be selected. This Locate function will also search VLAN IP interfaces for a device.



Save Layout: Saves device positions in the map, so the same view is displayed whenever the map is opened. Saved layouts are local to the PCM Client where Save Layout is executed.



Panner: Click and drag with the hand to center the map in a different part of the window. This is useful for scrolling to view parts of the network that do not fit in the window.



Select: Click the 'pointer' button to select a device or node in the map. You can click and drag a device using the pointer to position devices on a background image added to the map. When you move a device, the device will retain the position you set. Note that as discovery adds new devices to the map, distortions may occur in the device layout you created.

You can also click the pointer to return the cursor to normal operation after using Panner or Zoom options.



Zoom in Rectangle: Magnifies the selected area of the map. Click this button and drag the crosshair to select the area of the map you want to magnify.



Zoom In: Magnifies the entire map.



Zoom Out: Reduces the magnification of the map.



Fit to View: Adjusts the map to display the entire network in the window.

Viewing Network Device Information

If Ping Status is selected as the device view, mousing over a device displays the device name, IP address, and device type. Mousing over a link displays various information (e.g., link from/to devices and link speed), depending on the view. You can double-click devices in the Network Map to view the device Dashboard or right-click the device to access PCM functions.

You can double-click devices in a map to view the device properties and configuration, or you can select the device in the map and then use the right-click menu to view the device properties and access PCM functions.

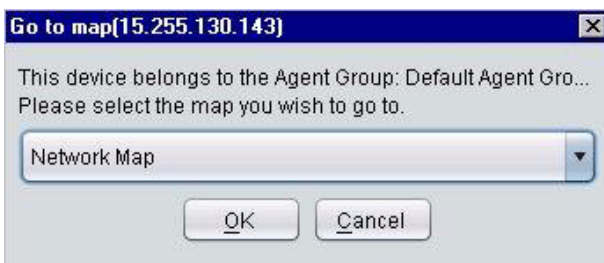
Note:

Devices running routing mode, such as the ProCurve 4100gl switches, do not appear in the map.

Finding a Device in Maps

Use the Go to Map feature to find a single device in the Network, Agent, Subnet or VLAN map.

1. Select the device node in the navigation tree or a map.
2. Use the right-click menu, and select the Go to map option. The Go to map dialog box displays.



3. Network Map is the default map selection. Use the drop-down menu to select the Agent, Subnet, or VLAN map to display.
4. Click **OK**. This displays the selected network map, with the focus zoomed in to the selected device.
5. To view the selected device location in the entire network, click the Map Overview button in the toolbar.

This launches the Map Overview sub-window on top of the map main window. The entire network is displayed, and the selected device is highlighted in the network, as shown in the following example.

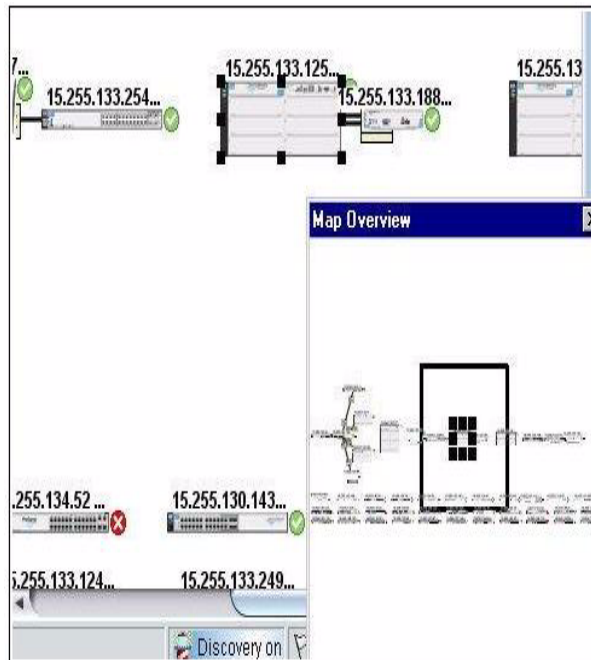


Figure 5-6. Example of Map Overview used with Go to map feature.

You can move the Map Overview window to any area on the screen, but it remains linked to the Go to map, map display. When you close the main map window, the Map Overview is closed automatically.

Using Background Images with Maps

You can add a background image to the Map views to help differentiate between network and subnet maps at a glance.

Note:

Customized map layouts and background images are lost when upgrading to PCM 3.x.

To add a background image to a map:

1. Open the map window.
(click the map node in the navigation tree).
2. Click the Set Background Image button in the maps toolbar.



The Set Background Image dialog box displays.

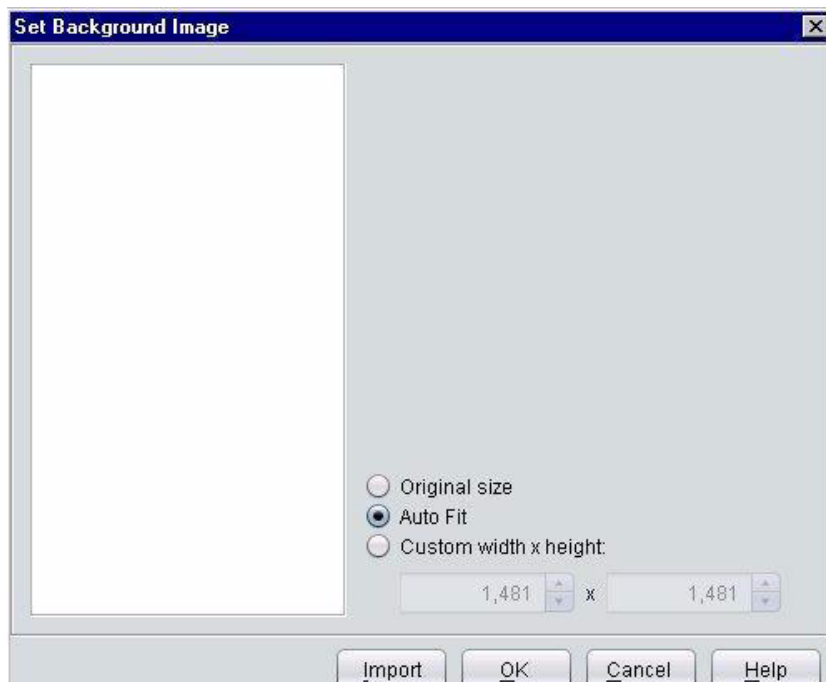


Figure 5-7. Set Map Background dialog box

3. To import a graphic, click the **Import** button and locate the image file to use as the map background. You can browse and select .jpg, .jpeg, .gif, or .png files stored on local or network devices.

When you import an image, the image file name displays in the list in the left pane of the Set Background Image window.

4. In the left pane, select the file to use as the map background.

All image files available in the client\config\maps\background directory are listed in the left pane, including some standard images that come with PCM.

5. Select one of the following size options for the background:
 - Original Size: Center the graphic in the map without changing the size of the graphic
 - Auto Fit: Automatically expand or reduce the graphic to cover all devices in the map. Otherwise, the background will remain at the initial auto-fit size when newly discovered devices are added and new devices will be positioned below the background image.
 - Custom width x height: Expand or reduce the graphic to a specific width and height in pixels.
6. Optionally, drag devices to any position on the background. This is especially useful when the background image is a map or floor plan.
7. Click **OK**.

The image now appears as the background of the map. It remains as the associated map background until you clear the image from the map, or select a different image to use for the map background.

To remove a Map Background Image:

1. Select the map node to display the map with its associated background image.
2. Click the Clear Background Image button in the map toolbar.



The background image is replaced by the default PCM background. Although the background is removed from the map, the device icons remain where they were positioned and the image file is retained in the client\config\maps\background directory.

3. To delete an image file and remove it from the list of available images in the Set Background Image window, right-click the image in the list and select **Remove**.

Using the Event Manager

Viewing Events	6-2
Restricting the Events Displayed	6-6
Filtering Events	6-6
Sorting Events	6-7
Pausing the Events Display	6-7
Managing Events	6-8
Acknowledging Events	6-8
Deleting Events	6-9
Displaying Other Event Views	6-10
Viewing Event Details	6-10
Viewing Archived Events	6-11
Viewing Aggregated Events	6-15
Setting Event Preferences	6-18
Setting Event Archive Attributes	6-19
Setting Ignored Event Preferences	6-21
Setting Throttled Events Preferences	6-23

Viewing Events

Events collected from devices and applications are reported in two ways: the Events pane in Dashboards, and Events tabs for Agent groups and devices.

The Events pane in Dashboards helps you quickly identify the number and severity of problems in the network, indicated by SNMP traps and application events received. For additional information about Dashboards, see “Network Management Dashboard” on page 2-18.

For more in depth information, use the Events tab to view and manage application events and SNMP traps generated by network devices. This tab helps you quickly identify problems for a device, device group, Agent, or Agent group (depending on the node you select in the navigation tree).

You can perform the following functions from Events tabs:

- View events
- View Event Details
- Sort events
- Filter events
- Acknowledge events
- Delete events
- Pause/Resume event reception
- View Aggregated events
- View Archived events

To display the Events tab view:

- Select a device, device group, Agent, or Agent group in the navigation tree and click the Events tab, or
- Click the Events pane in the Dashboard for a device, device group, Agent, or Agent group.

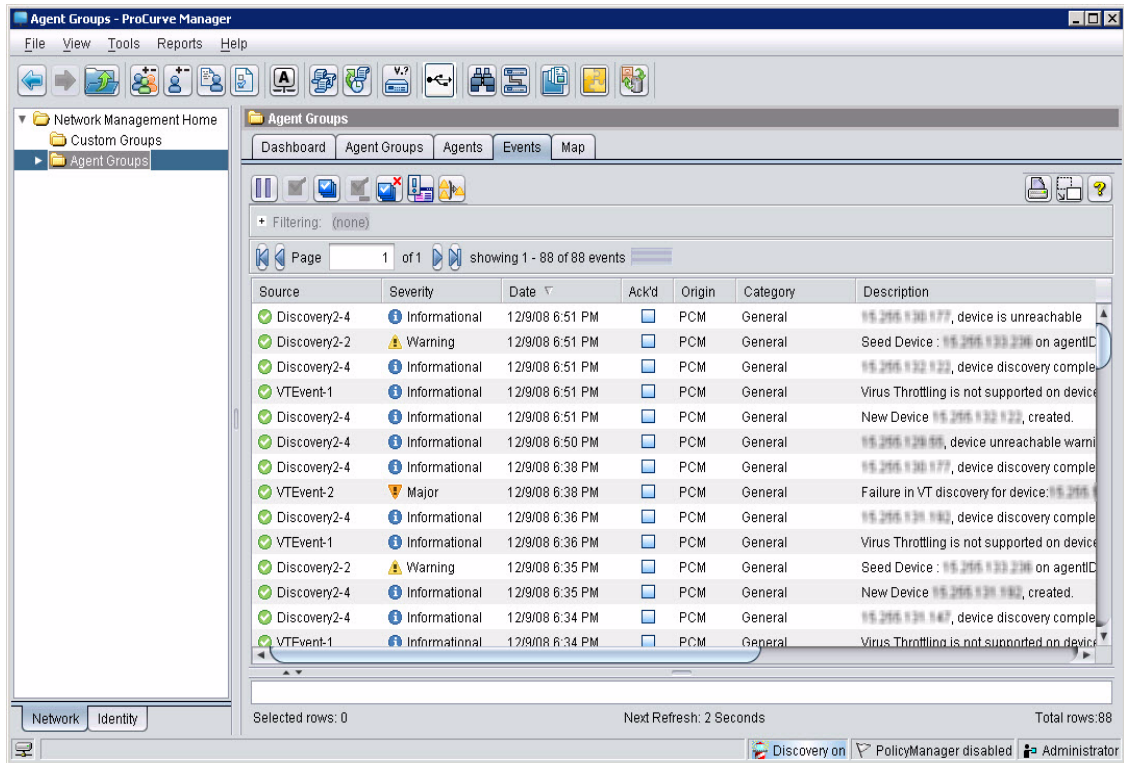


Figure 6-1. PCM Agent Groups Events tab

The Events tab lists common events and SNMP traps contained in the database for the selected node. Each event is categorized by the level of severity. Common switch events are described in the Management and Configuration Guide for your switch, and common NIM events are described in the *NIM Security Administrator's Guide*. PCM Traffic Monitor alarms are also displayed in the Events tab.

The types of events displayed depend on the node selected in the navigation tree:

- The Agent Groups node Events tab displays only PCM Server events (not associated with a specific Agent).





The Events tab for the Agent Groups node or a specific Agent group may show unassociated events, depending on the user profile (ProCurve Manager > Event Manager > View Unassociated Events). Unassociated events are not associated with a managed device and typically originate in the

PCM application, PCM modules, or an undiscovered device (e.g., undiscovered devices that are sending unsolicited SNMP traps to Agents within the Agent Group).

- An Agent Group Events tab displays all events received from devices managed by Agents in the Agent Group.
- A Devices node Events tab displays all events received from devices managed by Agents associated with the parent Agent Group. Events shown at this level differ from events shown at the Agent Group level, because the Devices node Events tab only shows events from discovered devices.
- A device group Events tab displays all events received from devices managed by the Agents associated with the parent Agent Group and of the selected device type.
- A device Event tab displays all events generated by the device. If a device is moved to a different Agent Group, device events generated while part of the original Agent Group will no longer be visible. However, it can still be viewed from the old Agent Group Events tab.






Events tabs contain the following sortable columns of information for each event:

Source: This column identifies the device or application that generated the event. Use the Origin and Description columns to further identify the source. This column also contains color-coded icons that indicate:

-  Connected
-  Warning
-  Unreachable
-  From unknown device

This column is not displayed when you select the Events tab for a device.

Severity: The Severity column shows the severity of each event. Events are categorized into five levels of severity:

-  Informational - Routine events
-  Warning - Unexpected service behavior
-  Minor - Switch error that may impact performance
-  Major - Switch error with potential of inhibiting switch operations
-  Critical - Severe switch error with the potential of halting all switch operations.

Traffic Monitor Critical alarms appear as Major events, and the event will indicate which port generated the threshold alarm. Severity for events received from third-party devices is derived from the severity assigned by the device.

Date: The Date column identifies the date and time when the event occurred. The date is shown in the Month-Day-Year hh:mm AM/PM format. Time is shown in the 24-hour clock format hh:mm:ss followed by the time zone.

Ack'd: The Ack'd column identifies whether the event has been acknowledged. A check in the box indicates that the event has been acknowledged, and an empty box indicates that the event is not yet acknowledged.

If the Events configuration is set to auto-delete acknowledged events, the Ack'd column will show only unacknowledged events. See “Setting Event Preferences” on page 6-18 for additional information.

Origin: The Origin column identifies the application or device that produced the event (e.g., PCM, NIM including NBAD engines, IDM, PMM, Device, or Unknown Device).

Category: The Category column identifies the type of event.

Agent: The Agent column identifies the Agent that received the event. This column is displayed on Events tabs for the Agent Group, Devices, and Device Group nodes.

Description: The Description column provides a short description of the event. The description is derived from a list of predefined event type descriptions included with the PCM application.

Three additional columns are not visible by default: Origin Type, Vendor, and Activity Type. To display these columns, right-click any displayed column heading and use the drop-down list to select (check) the columns you want to show. To remove a column from the display, select (uncheck) the column heading.



Clicking an event description scrolls the screen to the right. Mousing over a tooltip icon in the Description column displays the entire description in a tooltip.

Restricting the Events Displayed

The events shown on this tab are restricted to events from the devices that you are allowed to view (based on your user profile and the Agent receiving the event). Additionally, the Events tab can be customized to include only the types of events you want to view at any given time. Certain types of events can always be excluded from the list by using Ignored Event and Throttle Event Preferences or temporarily excluded by Filtering. Functions that determine which events displayed in the Events tab are:

- User Profile
- Events Browser Preferences
- Ignored Event Preferences
- Throttled Event Preferences
- Devices Excluded from Discovery
- Devices Excluded from Security Monitoring
- Filtering

The event-related tasks you can perform are also governed by your user profile.

Filtering Events

The events shown in the Events tab can be filtered, as explained in “Filtering Information in a Tab View” on page 2-35, to show only specific types of events. When filtering events, the event filter criteria is applied against all possible events, not just the current visible page of event data. Therefore, the current page resets to page 1, and currently selected events are unselected and may no longer be displayed. In addition to common filters, the Events tab contains the following filters:

- Origin is the entity that generated the event.
- Categories identifies the type of event.
- Source is the IP address contained in the Source field of events.

Sorting Events

Events in the Events tab can be sorted by any column heading, such as Severity. Click the desired column heading to sort events in descending order. Click the column heading again to sort events in ascending order. By default, events shown in the Event Browser are sorted by Event Date in descending order (with the newest events at the top).

A down pointer appears next to the column heading when events are sorted in descending order, and an up pointer appears next to the column heading when events are sorted in ascending order.

When sorting by column, all events that match the current selection criteria are sorted, not just the current page of event data that is visible. Therefore, the current page resets to page 1, and currently selected events are unselected and may no longer be displayed.

Pausing the Events Display



By default, events in the Events tab are refreshed every 30 seconds, displaying any new events received by PCM during the previous 30 seconds. However, you can click the Pause/Resume toggle button to temporarily suspend refreshing displayed events in the Events tab.



Click the Pause/Resume toggle button again to resume refreshing event data. Refreshing event data also can be paused and resumed by right-clicking an event (any field except Source) and selecting Pause/Resume Event Reception.

Note:

Event data refresh is also suspended when one or more events are selected.

For example, you might want to pause events when you are viewing selected events. You can also detach paused view, resume events on the original tab so you can see new events.

Managing Events

Acknowledging Events

Acknowledging an event indicates that you are aware of the event but it has not been resolved and changes the status of the event in the Events tab. You can configure the Events browser to automatically delete acknowledged events from the Events tab, in which case the event will be removed from the list.

Events can be acknowledged by selecting specific events or by acknowledging all events currently available in the Event Log.

To acknowledge a specific event:

1. Using standard Windows conventions, select the events that you want to acknowledge.
2. Click the Acknowledge Event button on the Events tab toolbar.



To acknowledge filtered events:

1. Create a filter for the events you want to acknowledge, as explained in Filtering. For example, to acknowledge all informational events create a filter for Informational severity.
2. Ensure the displayed events are the ones you want to acknowledge.
3. Click the Acknowledge All Events for Filtered Set button on the Events tab toolbar.



Deleting Events

Deleting an event has the following effects:

- Removes the event from the SNMP Traps window.
- Removes the event from the count on the SNMP Traps Summary subpanel in Dashboards.
- Removes the event from the database directly without archiving them. This option is not recommended and instead we recommend archiving handle aging events.
- and moves it to its archive file.

To delete specific events from an Events tab:

1. On an Events tab, select the events that you want to delete.
2. Click the Delete Event button in the Events toolbar.



Events can also be deleted by right-clicking an event and selecting Delete Selected Event.

To delete filtered events:

1. Create a filter for the events you want to delete, as explained in Filtering. For example, to delete all informational events create a filter for Informational severity.
2. Ensure the displayed events are the ones you want to delete.
3. Click the Delete All Events for Filtered Set button on the Events toolbar.



Displaying Other Event Views

Viewing Event Details

Clicking an event in the Events tab displays the details for that event in the bottom section of the Events tab. In addition, information identifying possible causes and actions to resolve the problem is available for Fault Finder events. Click the link in the Event Details to access this additional information.

Note:

The link and additional window are available only for events defined in the switch Fault Finder application.

The Event Details pane, which can be resized by dragging the top bar of the pane, contains the following information in addition to the information shown in the list of events.

Event Type: The Event Type identifies the source of the event (e.g., from the switch, PCM, Traffic Manager).

Received from: The Received from line lists the IP address and name (if available) of the device the event was received from, or the name of the PCM component that generated the event (e.g. Discovery, Traffic Monitor, etc.).

Date received: The Date received line identifies the date and time when the event occurred. The date is shown in the Month-Day-Year hh:mm AM/PM format. Time is shown in the 24-hour clock format hh:mm:ss followed by the time zone.

Date acknowledged: The Date acknowledged line indicates whether the event has been acknowledged and the date and time of acknowledgement.

Severity: The Severity description shows the severity of the event and any additional identifying information, such as the device generating the event or the offender and victim IP addresses and ports.

Event Description: For events generated by PCM, the Description provides a brief description of the event.

For events received from NIM and security devices, the Description provides additional information about the event, such as the scan that detected the attack and vendor-specific data.

Viewing Archived Events

The Archived Events window lists details for each event in the Archive Log, which contains events that have been deleted. The events displayed can be filtered by the date the event was generated and by any event filter created in the Events window. The Archived Events window also lets you generate an Archived Events Report that can be saved to disk or printed.

Note:

The Archive Events window shows all archived events, including events that you may not be able to view on the Events tab (e.g., because of user profile restrictions). Therefore, you may want to limit some user profiles from viewing archived events.

Events are moved from the database to the Archive file when the database exceeds 500,000 events. The order in which events are moved to the Archive file is determined by configurable Event Preferences. In addition, archiving of SNMP and PCM events can be disabled on the Event Preferences window. Therefore, the Archived Events window and report may not contain any events or only SNMP or PCM events.



Click the Event Archive button in the Events tab toolbar to display the Archived Events window:

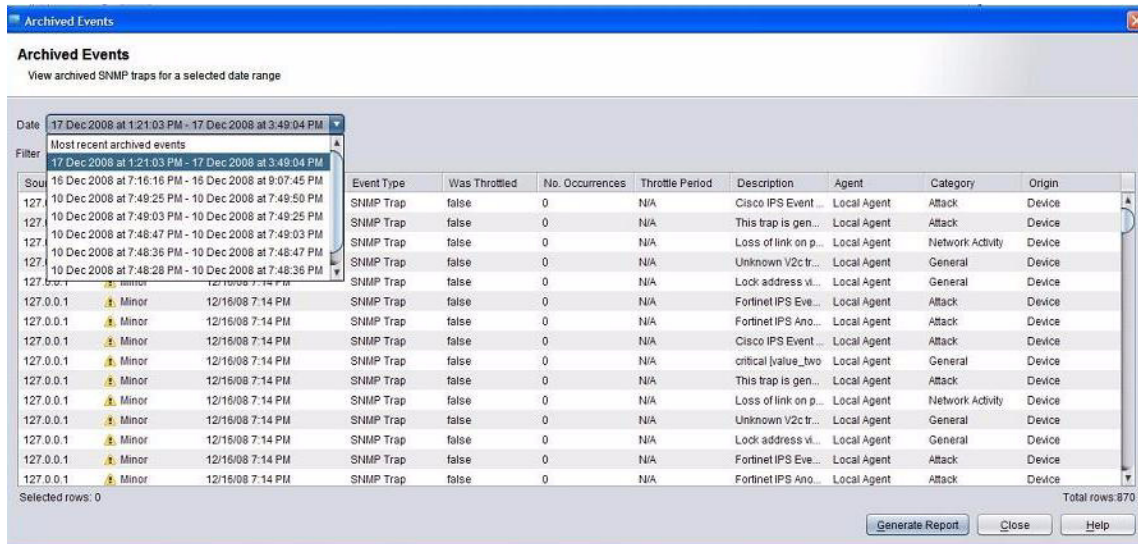


Figure 6-2. Archived Events

The Archived Events window provides the following information for each event:

Source	IP address of the device that caused the event
Severity	Severity level of the event: Informational, Warning, Minor, Major, Critical (listed in order of severity from lowest to highest)
Date Received	Time and date the event was received.
Type	Type of source that generated the event: SNMP trap, PCM event, or Syslog event
Was Throttled	Whether the event was created because of Virus Throttling. Possible values are: true, false, and not supported (device does not support Virus Throttling)
No. Occurrences	Number of times the event occurred during the selected reporting period (most recent reporting period is since last PCM restart)
Throttle Period	Length of time the device was throttled by Virus Throttling
Description	Descriptive information contained in the event
Agent	Agent that sent the event to the PCM Server
Category	Category of the event. An event can be classified as a single category or a combination of categories, represented as a comma separated list. General Network Activity Device Configuration Device Health Access Control Device Security Attack Reconnaissance Protocol Anomaly Traffic Anomaly Suspicious
Origin	Application or device that created the event

You can select the date range for displayed events by clicking the Date drop-down arrow and selecting the desired date range from the drop-down list. A new date range begins when PCM is restarted.

To further filter archived events, in the Filter field type the text of the filter you want to use. The display will list only events containing the filter text in any of the data fields.

To generate a report from the Event Archive:

To generate a report that can be printed or saved to disk, click **Generate Report**. This will create and display a report with the data from the Archive Event view.

To display the next page, click the > button in the bottom left corner. Or, to display the previous page, click the < button.



To print the report, click the print button and complete the standard Windows print screen.



To save the report to an .htm or .html file, click the save (disk) button, and complete the standard Windows save screen. Be sure to include the .htm or .html file extension in the filename. By default the saved file location is Program Files/Hewlett-Packard/PNM/client.

To close the window, click the Windows X button in the upper right corner.

To archive log files:

The Archive Log Files function creates a zip archive of all log files in the selected log directories and transfers them to the selected location on the Client.

Navigate to Archive Log Files by selecting Tools on the menu bar and selecting Archive Log Files.

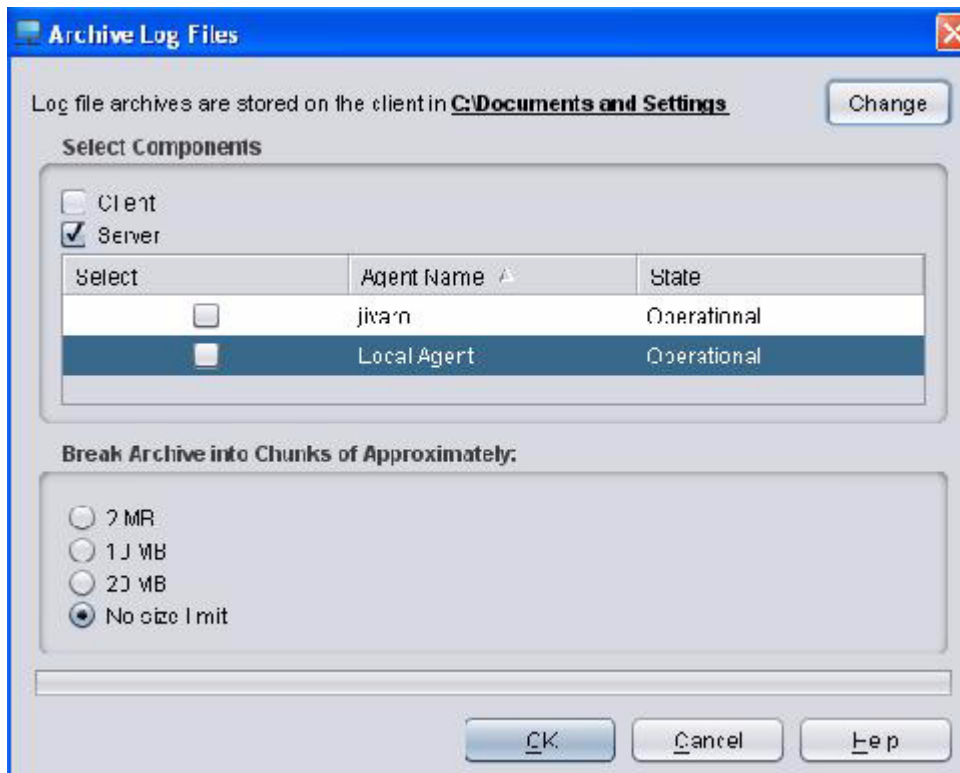


Figure 6-3. Archive Log Files

1. To store the archive files in a location other than C:Documents and Settings, click **Change** and select the desired destination.
2. Check the Client check box to archive all log files contained in the /PNM/ client directory.
3. Check the Server check box to archive all log files contained in the /PNM/ server directory.
4. Check the check box next to the Agent for which you want to archive log files.
5. To limit the size of the zip file, select 2 MB, 10 MB, or 20 MB. The default is No size limit.
6. Click **OK** to create the zip file and transfer them to the selected location.

Viewing Aggregated Events

By default, the Aggregated Events window shows the number of events and the most recent occurrence for each severity level. However, you can filter the display by event type, event source, event origin, and time interval.

Aggregation (Severity)	Event Occurrence Count	Most Recent Occurrence
Warning	11269	12/20/08 9:23 AM
Informational	369	12/19/08 3:04 PM
Minor	359	12/19/08 5:31 PM
Major	93	12/19/08 11:24 AM
Critical	3	12/18/08 11:38 AM

Figure 6-4. Aggregated Events



Click the View Aggregated Events button on the Events toolbar to display the Aggregated Events window.

Double-click any row in the Aggregated Events window to display a window listing all events in the selected severity.

To filter by time:



1. Select the group or device you want to display from the navigation tree, device-related window, or group-related window.
2. Click the Events tab for the selected group or device.
3. Click the View Aggregated Events button on the Events toolbar, which displays the Aggregated Events window.
4. Check the Time Span check box to activate the time fields.
5. To display only events received after a specific time, click the Since tab at the bottom of the Time Span panel and select the reporting period. For example, selecting 12 Hours displays events received during the previous 12 hours.
6. To display only events received during a specific time range, click the Range tab at the bottom of the Time Span panel and select the From and To dates and times.
7. To save the time setting and filter the display by time, click **Apply**.
8. Optionally, change the aggregated event type as explained below.

To filter by aggregated event type:

1. Select the group or device you want to display from the navigation tree, device-related window, or group-related window.
2. Click the Events tab for the selected group or device.
3. Click the View Aggregated Events button on the Events toolbar, which displays the Aggregated Events window.
4. Check the Aggregated Event check box and use the drop-down list to select the type of aggregation you want to display:



Severity	Filter by event severity level (default)
Origin	Application or device that produced the event (e.g., PCM, NIM including NBAD engines, IDM, PMM, Device, or Unknown Device).
Source	Component within the product that produced the event (e.g., Discovery). Source is derived from event and can vary based on the origin.
Type	Type of event (SNMP trap, Syslog Trap, or Application)
Application Provided	Licensed PCM modules and ProCurve security devices that supply application-specific Aggregation Filter settings

5. To save the aggregated event setting, click **Apply**.
6. To save the aggregated event setting and time setting, click **Save**.
7. To categorize events by the previous setting, click **Revert**.
8. To load a saved filter, click Load and select the filter from the popup window.
9. To close the window, click the Windows X in the upper right corner.

Setting Event Preferences

In addition to the event filters, you can use the Events option in the Preferences menu to customize the Events tab display and event archiving attributes.

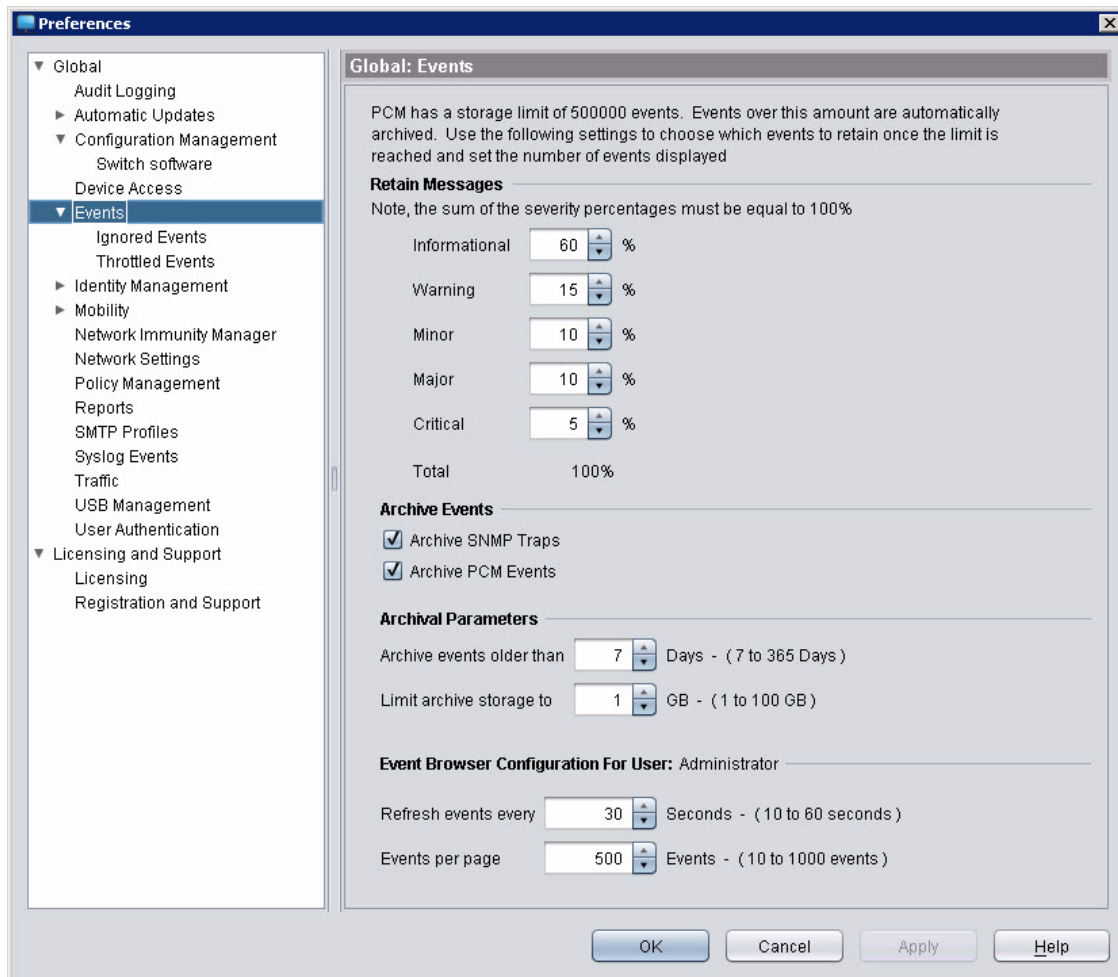


Figure 6-5. Global:Events Configuration Preferences window.

Setting Event Archive Attributes

1. Open the Preferences window and select the Events option to display the Global:Events (browser) configuration window (Tools > Preferences > Events).
2. Use the fields in the Retain Messages section to set the percentage of event types you want to save in the Events database and display in the Events tab. These percentages are based on the overall size set in the Max number of events field, and must equal 100 percent. If the maximum events is exceeded, the first type of event to get archived will be Informational, then Warning, then Minor, and so on as needed to maintain the maximum number of events shown in the display. For example,

Retain Messages

Note, the sum of the severity percentages must be equal to 100%

Informational	60	%
Warning	10	%
Minor	10	%
Major	10	%
Critical	10	%
Total	100%	

Figure 6-6. Setting Event Preferences: Severity Percentages

As shown in the above example, the maximum number of events is set to 1000 and Informational events is set to 60 percent. When timed trimming triggers and the total events exceed 1200 (1000 x 120%) and there are more than 720 (1200 x 60%) Informational events, the oldest Informational events are archived and then deleted from the corresponding table.

To ensure you maintain all Critical and Major events, set the total of the two types to 100 percent (e.g., 60 and 40), and set the other severity types to 0 percent.

3. To archive SNMP traps in the Event Log, check the SNMP Traps check box.

OR

To stop archiving SNMP traps in the Event Log, uncheck the SNMP Traps check box.

If SNMP trap archiving is enabled, all SNMP traps and PCM events are archived under <install dir>/server/data/events/[CommonArchive|SyslogArchive|IDMArchive] with filename prefixes of EVT-. The default installation directory is:

/Program Files/Hewlett-Packard/PNM

4. To archive PCM events in the Event Archive Log, check the Archive PCM Events check box.

OR

To stop archiving PCM events in the Event Log, uncheck the Archive PCM events check box.

5. To change how long events are held before being archived, select the Archive Events Older Than number of days. By default, events are moved to the archive file after 7 days. This setting affects both SNMP traps and PCM events.
6. To change the amount of disk storage that can be consumed by the Event Archive file, select Limit archive storage to and set the space (in gigabytes) available for storage. By default, PCM event archive space is limited to 1 gigabyte. This storage size is used for both SNMP trap archives and PCM event archives.
7. To change how often the Events tab is refreshed, select the desired seconds (10-60) using the Refresh events every up or down arrows or type the value. By default, the Events tab is refreshed every 30 seconds.
8. To change the number of events shown on each page of the Events tab, select the number of events (10-1000) using the Events per page up or down arrows or type the value. By default, the Event Tab displays 500 rows of event data.
9. Optionally, set the Ignored Event and Throttled Event preferences, as described on the following pages.
10. To save your changes and leave the Preferences window open, click **Apply**.

OR

To save your changes and exit the window, click **Ok**.

Setting Ignored Event Preferences

The Ignored Events Preferences window is used to exclude specific event types from the Events tab of all Agents. Events can be excluded for a specific device or all devices.

Open the Ignored Events Preferences window (Tools > Preferences > Events > Ignored Events).

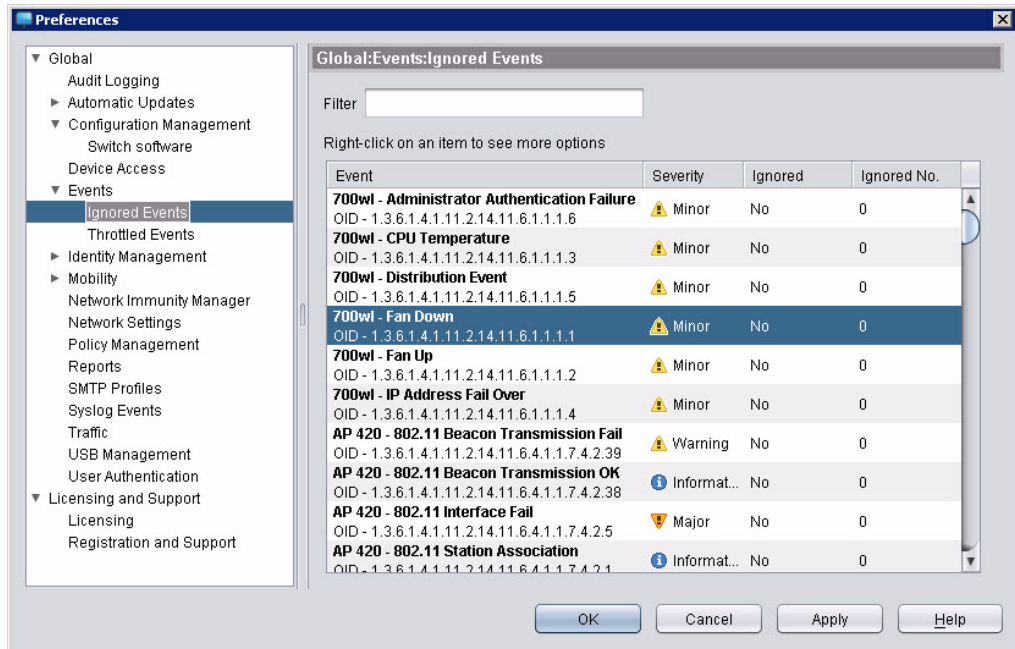


Figure 6-7. Global Preferences: Ignored Events window

This window lists the following information for each event:

Event	Event ID. If an SNMP trap, the friendly name of the trap and OID are displayed. If a PCM application event, the friendly name of the event and software component responsible for the event are displayed.
Severity	Assigned severity for the event
Ignored	Indicates which events are set to be ignored by PCM
Ignore No.	Number of devices on which the event is ignored (0 if event is not ignored, N/A for application events)

The default sort order is by friendly name in ascending order. Click any column heading to change the sort order of the list. Click the column heading again to reverse the sort order.

Configuring Ignored Events

1. Right-click the event and select **Ignore** or **Select devices to ignore from**. Selecting **Ignore** excludes the selected event type from all devices, and selecting **Select devices to ignore from** opens the **Ignore Traps** window so you can select specific devices from which to ignore events.

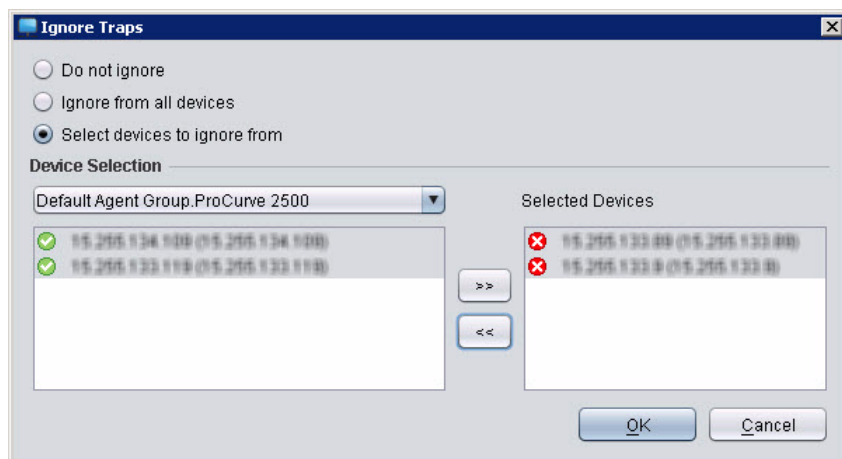


Figure 6-8. Event Preferences, Ignored Events

2. If you selected **Select devices to ignore from**, in the **Ignore Traps** window ensure **Select devices to ignore from** is selected and use the **Select Device Group** drop-down menu to select the device type, which lists all devices in the selected group in the selection box on the left.
3. Select the devices from the list in the left box, and click **>>**, which moves the selected devices to the **Selected Devices** box. Select multiple devices in a group by using standard Windows selection keys **ctrl+click** and **shift+click**.
4. Click **OK** to save the settings and close the dialog box.

Restoring Ignored Events

To restore monitoring of an ignored event from all devices:

1. Right-click the event and select **Do not ignore**.

To restore monitoring of an ignored event from specific devices:

1. Right-click the event and select **Select devices to ignore from**.
2. To remove a selected device, select the device from the **Selected Devices** box and click <<. Select multiple devices by using standard Windows selection keys ctrl+click and shift+click.
3. Click **OK** to save the settings and close the dialog box.

Setting Throttled Events Preferences

You can use the Throttled Events preferences to suppress specific event types from the event display for a specified time period from one to 60 minutes. You can configure Throttled Event traps for a specific device or all devices.

Note:

Do not confuse throttled events with events created by virus throttling. Throttled events are common events that are suppressed (throttled).

Open the Preferences window and select **Events > Throttled Events** to display the **Global:Events:Throttled Events** configuration window.

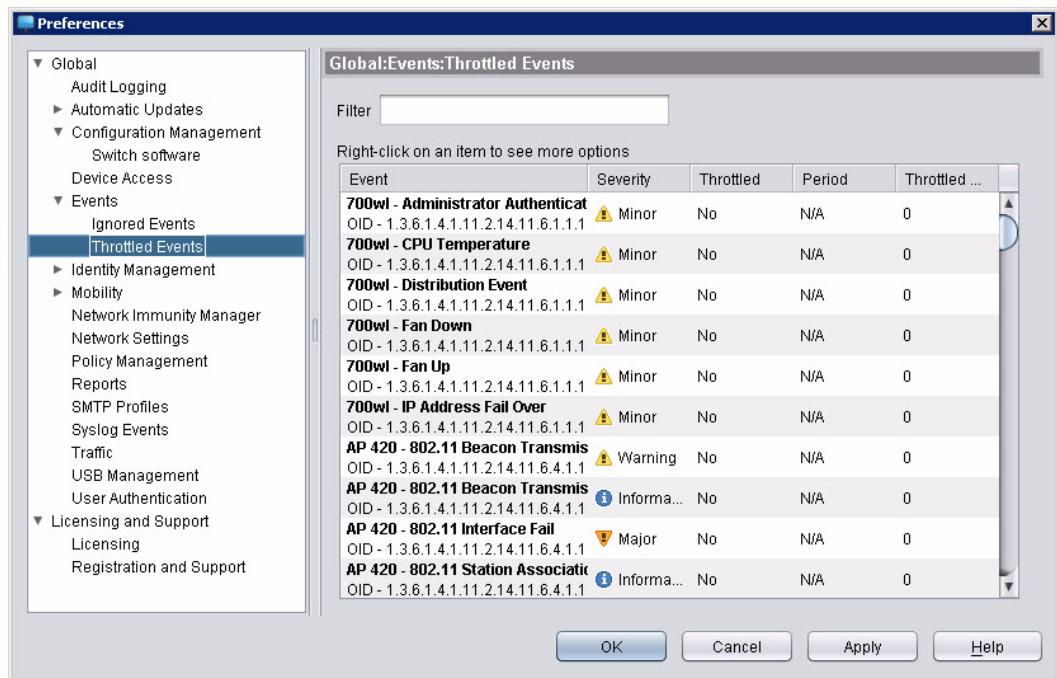


Figure 6-9. Global Preferences: Throttled Events window

The columns in the event listing provide the following information for each event:

- **Event:** The event ID. In the case of an SNMP trap, the friendly name of the trap and the OID is listed.
- **Severity:** The assigned severity for the event.
- **Throttled:** Indicates which events are set to be throttled by PCM.
- **Period:** Indicates the time period for which the event is throttled.
- **Throttle No.:** Indicates the number of devices on which the event is throttled. (0 if event is not throttled, N/A for application events).

The default sort order is by friendly name in ascending order. You can click any of the column headings to change the sort order of the list.

Configuring Throttled Events

To throttle an event on a specific device:

1. Right-click the event and select **Throttle** or **Select devices to throttle from**. Selecting **Throttle** suppresses the selected event type from all devices, and selecting **Select devices to ignore from** opens the **Throttle Traps** window so you can select specific devices from which to suppress events.

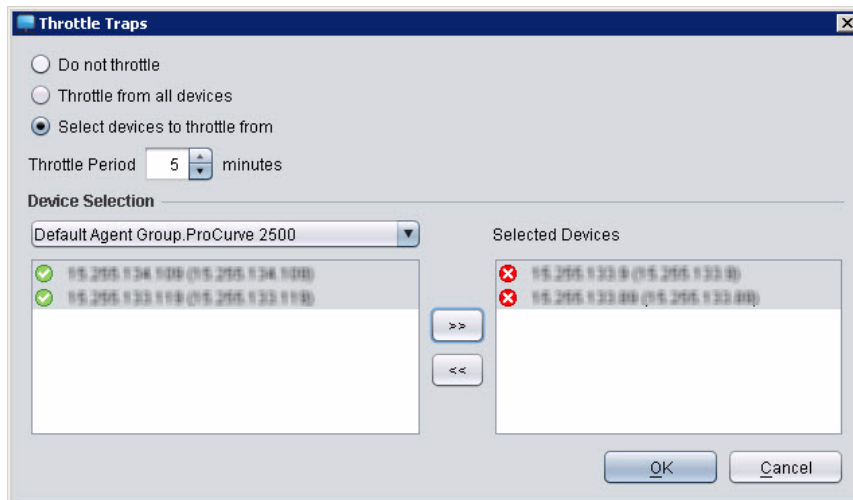


Figure 6-10. Event Preferences, Throttled Events

Note:

PCM application events are generated by the application, not devices; thus the Select devices to throttle from option, and access to the Throttle Traps dialog is disabled for application events.

2. If you selected Select devices to throttle from, in the Throttle Traps window ensure Select devices to throttle from is selected and use the Select Device Group drop-down menu to select the device group you want to throttle, which lists all devices in the selected group in the selection box on the left.
3. Select the devices from the list in the left box, and click >>, which moves the selected devices to the Selected Devices box. Select multiple devices in a group by using standard Windows selection keys ctrl+click and shift+click.
4. Use the Throttle Period drop-down list to select the number of minutes to throttle events.
5. Click **OK** to save the settings and close the dialog box.

Restoring Throttled Events

To restore monitoring of a throttled event from all devices:

Right-click the event and select Do not throttle.

To restore monitoring of a throttled event from specific devices:







1. Right-click the event and select Select devices to throttle from.
2. To stop throttling a selected device, select the device from the Selected Devices box and click <<. Select multiple devices by using standard Windows selection keys ctrl+click and shift+click.
3. Click **OK** to save the settings and close the dialog box.

Managing Network Devices

Using Device Manager Tools	7-2
Rules for Configuring Device Access with PCM	7-3
Configuring Trap Receivers	7-4
Adding Trap Receivers	7-5
Modifying Trap Receivers	7-6
Deleting Trap Receivers	7-6
Configuring Authorized Managers	7-7
Adding Authorized Managers	7-8
Modifying Authorized Managers	7-9
Deleting Authorized Managers	7-9
Configuring Friendly Port Names	7-12
Configuring SNMP and CLI Access	7-14
Setting Communication Parameters in Devices	7-15
Setting Communication Parameters in PCM	7-24
Modifying Community Names	7-34
Using Test Communication Parameters in PCM	7-36
Troubleshooting Device Communication Problems	7-38
Using Global Device Access Preferences	7-40
Setting Device Display Names	7-40
Setting Agent-Specific Device Access Preferences	7-41
Configuring RMON Alerts	7-42
Adding and Modifying RMON Alerts	7-43
Deleting RMON Alerts	7-44
Other Device Management Tools	7-45
Device Logs	7-46
Using the Device Log	7-46
Using Device Syslog	7-47
Using the Audit Log	7-50
Replacing Network Devices	7-54

Using Device Manager Tools

The Device Access tools in PCM provide the basic functions to configure communication parameters for ProCurve network devices including:

 Device Manager	- Configuring trap receivers on a device.
 Telnet to device	- Setting Authorized managers.
 Connect to WebAgent	- Telnet (using SSH) to device to use CLI.
 Communication Parameters in PCM	- Connect to Device's Web Agent.
 Communication Parameters in Device	- Set Communication Parameters for SNMP, Telnet, and CLI.
 Test Communication Parameters in PCM	- Test communication parameters for device.



To access the Device Manager, select the device to be managed in the Devices List or the Navigation Tree then click the Device Access button in the toolbar to display the Device Access Tools menu; or, you can right click the device and select Device Access → Device Manager from the menu.



Figure 7-1. Device Manager window, default display.

The Device Manager window uses a tabbed display for the device management functions supported. The default display shows the System Information tab, with the system name, contact, and location if available. The availability of the remaining tabs (Trap Receivers, Authorized Manager, and Port Names) will vary based on the network device type and configuration. For example, ProCurve 420 wireless devices show only the System Information and Trap Receivers tab.

Rules for Configuring Device Access with PCM

PCM uses the following default settings to access ProCurve Network devices:

- CLI access via Telnet, using SSH1 with Password Authentication enabled, and no Manager Username defined.
- SNMPv1/v2, with a Community name of “public” for read and write access. User is set to Procurve, and no authentication protocol is set.
- SSH key: (1024 default)
- WebAgent access using HTTP on port 80.

This will work for all ProCurve devices discovered by PCM if:

- No IP Authorized Managers are configured on the devices. (or SNMP Authorized Managers on ProCurve 4000 Series)
- Devices have an SNMP community name of public, with Read and Write access set to Unrestricted.

Note:

Some ProCurve Network devices have SNMP disabled by default, or have public as a read-only/restricted community name. Ensure that the PCM Agent's SNMP Configuration is in sync with the device's SNMP configuration

To improve security you can alter the PCM default settings in Global Preferences, or the Device access settings using the "Communication Parameters" functions available in the PCM Device Manager menu, keeping in mind the following rules:

- When you change the Global Preferences for Device Access, it changes the parameters PCM uses to communicate with devices. This will work for all devices configured to use the "PCM default" in the Communications Parameters in PCM Wizard. If you are not using the PCM defaults for a device, changes in Global Preferences for Device Access will not be applied.
- If you set SSH or SNMPv3 security, or other device access settings using the *Communications Parameters in Device* feature, then the default PCM Device Access parameters will no longer work. You will need to use the *Communications Parameters in PCM* to match settings you changed on the Device. (any change in a device's SNMP, CLI, or WebAgent access or security settings should be matched in the PCM Communication Parameters for the device.)
- When you use the *Communications Parameters in PCM* to set the PCM device access, it overrides the Device Access settings in the Global Preferences for the selected devices only.
- When in doubt, use the Test Communications Parameters in PCM to check if PCM is able to access the device.

Configuring Trap Receivers

The PCM management station is automatically registered as the default trap receiver for switches discovered on the network; however, you can change this using Global Preferences. Refer to “Managing Discovery Preferences” on page 4-28 for details. Use Device Manager option in the Device Access menu to configure additional trap receivers.

The Trap Receivers tab displays the list of IP Addresses (devices) that the selected device will send traps to. You can also add, delete or modify the Trap receivers configured for the device.



Figure 7-2. Device Manager: Trap Receivers tab

The listing shows the IP Address of the trap receiver, and the Event filters in place for event types to be forwarded to the trap receiver.



You can refresh the display to check for changes in the Trap Receivers configuration by clicking the Retrieve button in the toolbar.

Note:

PCM receives traps irrespective of the community name. However, if a trap receiver is added in PCM, the community name will always be "public". The modify option in PCM cannot override other community names set in the device. For PCM-NNM, the Network Node Management (NNM) server is set as the default trap receiver, instead of the PCM Server.

Adding Trap Receivers

Use Device Manager option in the Device Access menu to configure additional trap receivers for a selected device.



1. Click the Add Trap Receiver button in the toolbar to display the Add Trap Receiver dialog.

The screenshot shows a dialog box titled "Add Trap Receiver". It contains two input fields: "IP Address:" with an empty text box, and "Event log filter:" with a dropdown menu currently set to "NOT INFO". Below the fields are "Ok" and "Cancel" buttons.

2. Enter the **IP Address** of the device to receive traps.
The IP address must be in the proper format. You cannot use 0.0.0.0, 255.255.255.255, the multicast address, loopback address, or subnet broadcast address of the device.
3. Use the **Event Log Filter** drop-down menu to select the type of events you want to include in the Event Log:

NONE	Do not use the Event Log
NOT INFO	Include all events except information events
CRITICAL	Include critical events only
ALL	Include all events
DEBUG	Include debug events only

If you are using the PCM-NNM module, events are logged in NNM.

Not all devices support Event log filters (such as wireless). When setting trap receivers for such a device, the Event log filter field is disabled.

4. Click **Ok**. A check will be performed to ensure the IP address is valid.
 - If it is a valid IP address the Add dialog is closed and the Trap Receivers list is updated with the new entry.
 - If the IP address is invalid you will get an "Invalid IP address" error, and the Add dialog remains open so you can enter the IP address.

You will also get an error when trying to add a trap receiver in any of the following cases:

- If the IP is a duplicate of an trap receiver already set for the device.
- If the maximum number of trap receivers for the device is exceeded.

- If the SNMP credentials are incorrect. Check communication parameters for the device to verify.
- If the device is unreachable, either the connection or device is down.

Note:

When PCM (Server) starts up, it binds to port number 162, which is the port that all incoming traps arrive on. If another process is already bound to that port, PCM cannot receive traps. Make sure no process is bound to port 162. Examples of applications that bind to port 162 are the Windows SNMP Trap Receiver Service, HP OpenView, MG-Soft MIB Browser Trap Ringer, etc.

If another process is bound to port 162, simply terminate the process and restart the PCM Server. To restart the PCM Server (in Windows):

- Go to Control Panel > Administrative Tools > Services.
 - Double click the ProCurve Network Manager Server, click the Stop button, and then click the Start button.
-

Modifying Trap Receivers



To modify a Trap Receiver, select it from the list, then click the Modify Trap Receiver button in the toolbar to display the Modify Trap Receiver dialog.

The Modify Trap Receivers dialog is displayed with the IP Address of the selected trap receiver. Edit the IP address or Event log filter as needed then click **OK**. The IP address will be validated (as described for adding a trap receiver).

Deleting Trap Receivers



To delete a Trap Receiver, select the entry from the list, then click the Delete Trap Receiver button in the toolbar. A confirmation pop-up will be displayed.

Click **Yes** to complete the process.



You can delete all trap receivers at the same time by clicking on the Delete All button in the toolbar.

Configuring Authorized Managers

For devices that support IP-based Authorized Managers, you can use the PCM Device manager to configure Authorized Managers. The Authorized Managers feature uses IP addresses and masks to determine which stations (PCs or workstations) can access the switch through the network. This covers access through the following means:

- Telnet and other terminal emulation applications
- The switch's Web browser interface
- SNMP (with a correct community name)

Also, when configured in the switch, the Authorized Managers feature takes precedence over local passwords, TACACS+, RADIUS, Port-Based Access Control (802.1X), and Port Security. This means that the IP address of a networked management device must be authorized before the switch will try to authenticate the device using other access security features. Thus, with authorized managers configured, the station attempting to access the switch must be included in the switch's Authorized Managers list, as well as having the correct username and passwords.

Click the Authorized Managers tab in the Device Manager window to view a list of Authorized Managers on a device.



Figure 7-3. Device Manager: Authorized Managers tab

The Authorized Managers list gives the IP address, IP Mask, and Access permissions for the device's authorized managers.



Click the Retrieve button in the toolbar to refresh the display and check for any changes to the device's Authorized Managers settings.

Note:

If you add an Authorized Manager for a device without adding PCM as an Authorized manager, or if you change the Management Community name on a device using the CLI or WebAgent, you will not be able to manage the device using PCM.

Adding Authorized Managers



To add an Authorized Manager, click the Add button in the Authorized Managers toolbar. This will display the Add Authorized Managers dialog. Up to ten authorized managers can be added to the device.

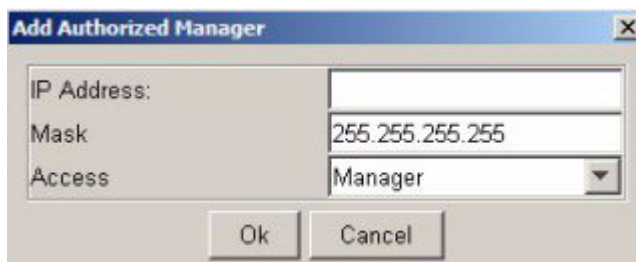


Figure 7-4. Add Authorized Manager dialog.

When using the Authorized Managers feature, the PCM Server must be configured as an Authorized Manager for the device. The process for adding other authorized managers is similar to adding your PCM Server, shown below.

1. Enter the **IP Address** of the management station. (For PCM, the station must have the PCM application installed).
2. Enter the **IP Mask** address.
 - The default IP Mask is 255.255.255.255 and allows switch access only to a station having an IP address that is identical to the Authorized Manager IP parameter. (“255” in an octet of the mask means that only the exact value in the corresponding octet of the Authorized Manager IP parameter is allowed in the IP address of an authorized management station.)
 - You can alter the mask and the Authorized Manager IP parameter to specify ranges of authorized IP addresses. For example, a mask of 255.255.255.0 and any value for the Authorized Manager IP parameter allows a range of 0 through 255 in the 4th octet of the authorized IP

address, which enables a block of up to 256 IP addresses for IP management access. A mask of 255.255.255.252 uses the 4th octet of a given Authorized Manager IP address to authorize four IP addresses for management station access.

3. Select the **Access** level for the station.
 - **Manager:** Enables full access (read and write) to device configuration functions.
 - **Operator:** Enables read only functionality to device configurations.
4. Click **Ok** to complete the process.

The IP address will be validated. You will get an error message if it is invalid. Otherwise, the Authorized Managers list is updated with the new information.

Note

The access levels for SSH and SNMPv3 can be set using the Communication Parameters in Device Feature from the Device Access Menu. You can also add additional Community Names and edit the Management Community settings using this feature.

Modifying Authorized Managers



To modify an Authorized Manager, click the Modify button on the Authorized Managers toolbar. This will open the Modify Authorized Manager dialog, which has the same inputs as the Add Authorized Managers dialog. Edit the existing entries, then click Ok.

Deleting Authorized Managers



To delete an Authorized Manager, select the entry in the Authorized Managers list, then click the Delete button in the Authorized Managers toolbar.



You can also use the Delete All button to delete all the authorized manager entries, without first having to select the entries.

Setting SNMP Authorized Managers on 1600m, 4000m and 8000m Devices

Because the 1600m, 4000m, and 8000m Devices support both SNMP and IP authorized manager, the process for setting authorized managers on these device types using PCM is different than for other devices. In the Device Manager window for 1600M, 4000M and 8000M devices, you will see:

Managing Network Devices Configuring Authorized Managers

- An Authorized Manager tab to use for setting SNMP authorized managers. The SNMP Authorized Managers uses a station's IP address with the SNMP Community Name, to restrict access to the specified management stations.
- An IP Authorized Manager tab to use for setting IP authorized managers. The IP Authorized Manager on these devices are used to authorize which stations can:
 - Access the switch's Web browser interface
 - Telnet into the switch console interface
 - Perform TFTP transfers of configuration files and software updates on the switch

Setting the IP Authorized Manager is the same as described under "Adding Authorized Managers" on page 7-8.

To set the SNMP authorized manager:

1. Select the Authorized Manager tab.

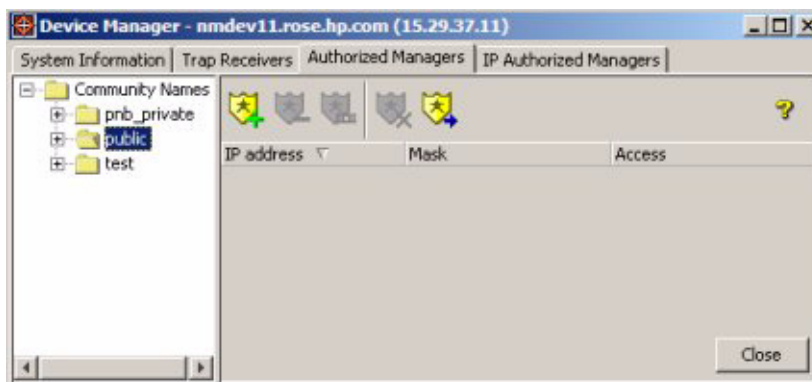


Figure 7-5. Authorized Manager tab for 1600M, 4000M, and 8000M devices

2. Select the associated SNMP Community Name from the list in the left pane of the window. The list will vary based on what is currently configured on the device. Use the Communications Parameter in Device feature in the Device Access menu to add SNMP Community names.
3. Click the Add button to display the Add Authorized Manager dialogue.
4. Enter the **IP address** of the PCM Server to be added as an authorized manager.



The IP address must be in the proper format, it can not be 0.0.0.0, 255.255.255.255, or the multicast address, loopback address or subnet broadcast address of the device.

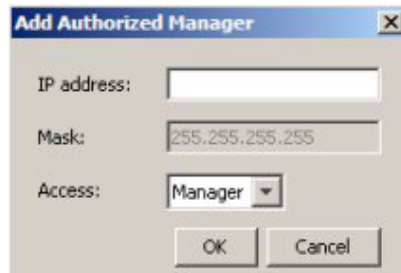


Figure 7-6. Add Authorized Manager dialog

5. Enter the **IP Mask**. In PCM 3.0, this field is disabled for 1600m and 4000m devices and is 255.255.255.255 by default.

The mask allows a range of IP addresses to be recognized as authorized managers. The default IP mask is 255.255.255.255, which allows switch access only to a management station with an IP address identical to the authorized manager IP address. To specify ranges of authorized IP addresses, set the fourth octet to indicate the number of authorized managers. For example, a mask of 255.255.255.252 will allow four IP addresses for management station access.

6. Select the **Access** level for the management station. In PCM 3.0, this field is disabled for 1600m and 4000m devices and is set by PCM depending on the community write access (restricted or unrestricted).
 - **Manager**: Enables full access (read and write) to device configuration functions.
 - **Operator**: Enables read only functionality to device configurations.
7. Click **Ok** to complete the process.

The IP address will be validated. An error message is displayed if it is invalid. Otherwise, the Authorized Managers list is updated with the new information.

Note:

Deleting or changing the management community named "public" may prevent access by PCM to the device. If security for network management is a concern, ProCurve recommends you change the Write access on the device to "Restricted" using the Communication Parameters in Device feature from the Device Access menu, rather than changing the management community name.

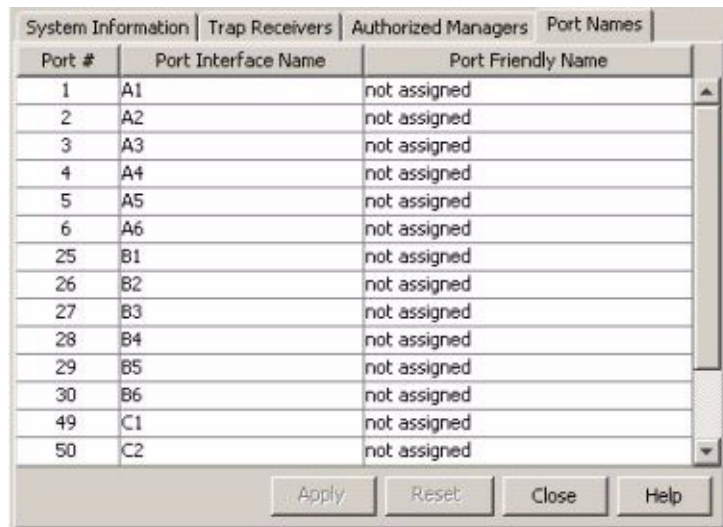
Configuring Friendly Port Names

The Device Manager also provides a way to assign "friendly" port names to assist in tracking port configurations throughout the network. When the Use Friendly Port Names option in the Global Preferences for Device Access is enabled (see page 7-40), the following areas of PCM will display the friendly port name (if available) instead of the interface name:

- The traffic configuration windows.
- The "Port Assignment Table" tab for a device.
- The "Port Properties" tab for a VLAN under "network map".
- Ports shown in the "Find Node" and "Node to Node Path Trace" results.
- Ports shown in the Modify VLAN Wizard.
- The tool tips for network links on the maps.

To assign friendly port names:

1. Select the device in the Devices List or Navigation tree, then select the Device Manager option in the toolbar, or using the right-click menu (Device Access > Device Manager).
2. Click the Port Names tab in the Device Manager window.



The screenshot shows a window titled "Device Manager" with several tabs: "System Information", "Trap Receivers", "Authorized Managers", and "Port Names". The "Port Names" tab is active, displaying a table with three columns: "Port #", "Port Interface Name", and "Port Friendly Name". The table contains 15 rows of data, all with "not assigned" in the "Port Friendly Name" column. At the bottom of the window are four buttons: "Apply", "Reset", "Close", and "Help".

Port #	Port Interface Name	Port Friendly Name
1	A1	not assigned
2	A2	not assigned
3	A3	not assigned
4	A4	not assigned
5	A5	not assigned
6	A6	not assigned
25	B1	not assigned
26	B2	not assigned
27	B3	not assigned
28	B4	not assigned
29	B5	not assigned
30	B6	not assigned
49	C1	not assigned
50	C2	not assigned

Figure 7-7. Device Manager: Port Names tab

3. Click to select the port to which you want to apply a Friendly Name.
This will enable the Port Friendly Name field so you can type the name.
4. Type the Friendly Name you want to use.
5. Repeat the process for each port that you want to assign a friendly name.
6. Click Apply to update the port names for the Device.
Click Reset to return the Port Name to the previous setting.
Click Close to exit the window without applying the new Port Names.

Configuring SNMP and CLI Access

PCM provides a default device access configuration designed to work with ProCurve devices. The default SNMP community names are set when you install PCM. To provide support for newer ProCurve devices in more complex network configurations using SNMP-V3, and SSH for CLI access, you can also set the PCM device access parameters for individual devices using the Device Manager Menu.

- Use the Communication Parameters in Device option to create and change the Access settings for SNMP and CLI (Telnet and/or SSH) on individual devices. You can also use this option to set or change the Management Community Name on a device. Changes made to the device using this option will also update the Device Access settings for that device in PCM.
- Use the Communication Parameters in PCM option is to set access parameters that PCM uses to communicate with a device via SNMP, CLI, and the Web Agent. You would use this wizard if the device access settings on a device (community name or SNMP) are changed using Telnet or the WebAgent (not using the PCM interface wizards). Parameters set in this wizard can also be used to override the settings in the (Global) Preferences for Device Access that PCM uses to communicate with new discovered devices.
- Use the Test Communication Parameters option to compare SNMP and CLI communication parameters stored on the device with those stored in PCM, and verify that PCM can communicate properly with the device.

Setting Communication Parameters in Devices

The Communication Parameters in Device Wizard is used to create and change SNMP and CLI parameters in devices. These parameters are changed in the selected device(s) and in PCM.

PCM can use SNMP (SNMPV2 or SNMPV3), telnet, or SSH to communicate with devices. SNMPV2 uses the traditional community name and read and write access permissions for communication. SNMPV3 provides a secure communication that requires PCM to use a username (governed by its assigned security level) to communicate with the device.

If you launch the wizard for multiple devices, the wizard does not display any information. However, if you launch the wizard for a single device, the wizard displays the SNMP and CLI configurations for the selected device.

Tip: You can also use the "Device Management: Communication Parameters" Action in the Policy Manager to reconfigure SNMP and CLI settings on devices.



1. Select the device(s) in the Devices List, then select the Communication Parameters in Device option from the Device Manager menu to launch the Wizard.
2. Click **Next** in the Welcome window to display the "Configure the settings" window.

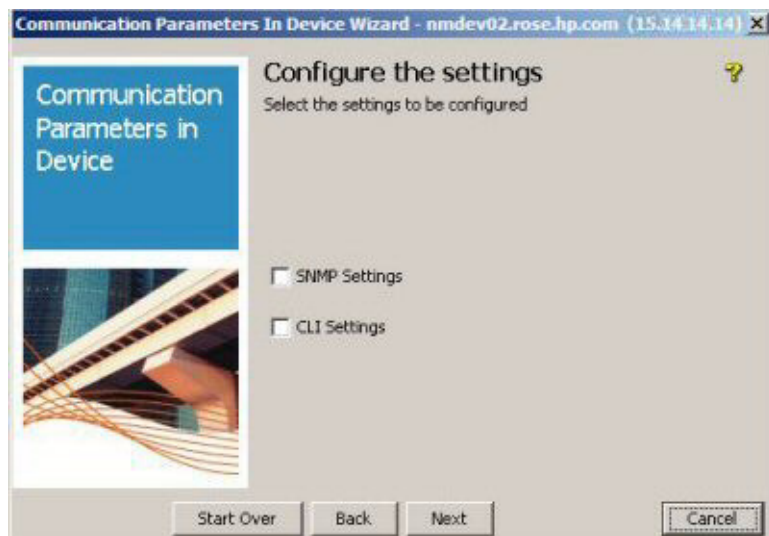


Figure 7-8. Communication Parameters in Device: Settings selection

3. Select one or both of the settings to be configured, then click **Next**.

The following instructions describe the process if both options are selected.

Note:

If you are using the PCM-NNM module, NNM listens for SNMP Community Name "events" from PCM, and uses the event data to update its own database to match the changes made in PCM.

If you change the SNMP community name for the device and update the NNM database using NNM's SNMP configuration window, the new configuration is uploaded to the PCM device database at the next discovery or device scan.

When SNMP Settings are selected, the wizard displays the Configure SNMP settings window next.

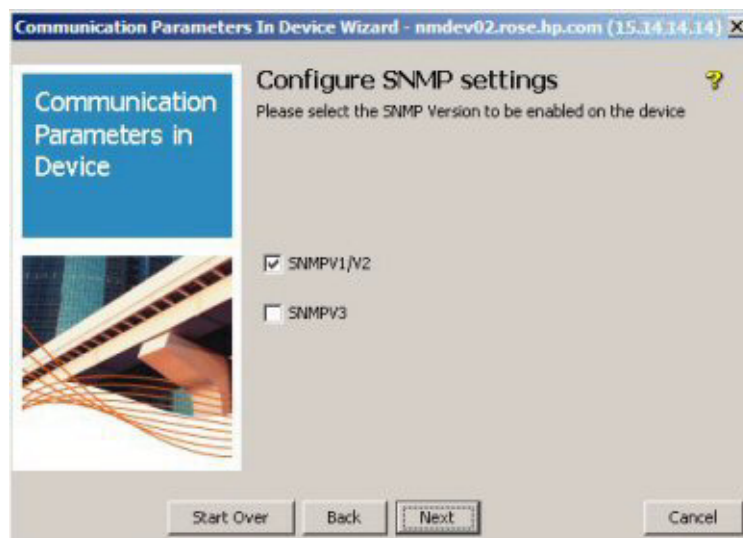


Figure 7-9. Communication Parameters in Device: SNMP Settings selection

4. Click to select the SNMP versions you want to configure, then click **Next**.
An unselected SNMP version will be disabled on the device.
5. If you selected SNMPV2, the V2 Credentials Configuration window displays.

The V2 Credentials Configuration window is used to configure community names for access to devices using SNMPV2. Each community can have different read and write access permissions. The management community name is used by PCM to communicate with the selected device. Up to five

community names can be configured on the switches. Only two community names can be configured on a wireless device; one for the read community name and one for write community name.

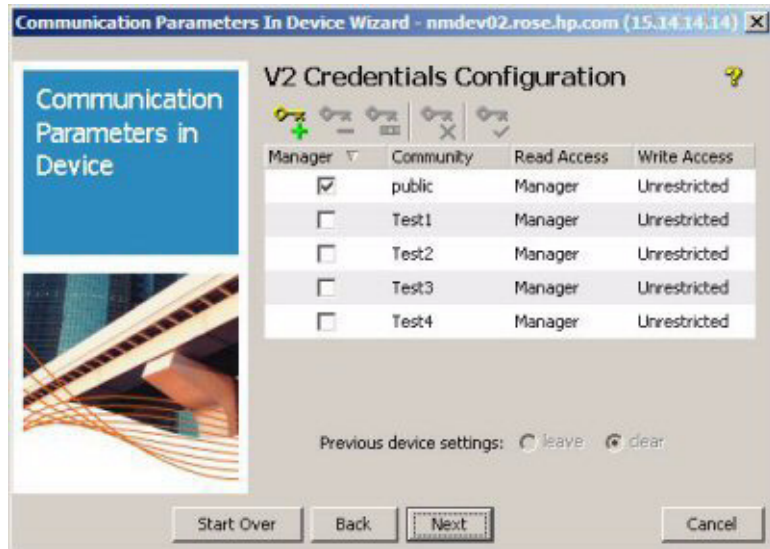


Figure 7-10. Communication Parameters in Device: SNMP V2 credentials

When this window is launched by selecting a single device, the information for all SNMPV2 community names currently configured in the device are displayed. However, community names configured in wireless, 9315, 9308, 9304, 6308, and 6304 devices are not displayed, even when a single device is selected. You can add new community names for these devices, but you cannot modify or delete existing community names for these devices.

When you access this window by selecting more than one device, this window does not display any information. You can add community names for all the selected devices, but you cannot modify or delete community names currently configured on individual devices.



6. Click the Add Names button in the toolbar. This will display the Add Community Names dialog.



Figure 7-11. Device Communication Parameters: SNMPv2 Community name

- a. Type the SNMP Community Name to be added, up to 16 characters. The characters "<" and ">" cannot be used.
- b. Click the Read Access drop-down arrow and select the level of permissions for read access:
Manager level provides access to the entire MIB
Operator level provides access to a restricted portion of the MIB.
- c. Click the Write Access drop-down arrow and select the level of permissions for write access:
Unrestricted provides read and write access to the MIB.
Restricted provides read only access to the MIB.

Note:

Wireless devices (AP -420, -520, and 530) and 9100 switches have only two community names. The read and write community, with Manager restricted and Manager unrestricted.

- d. Click to select the Use this as the management community? option. This will set this community name as the management community on the device.
- e. Click **OK** to save the changes and return to the V2 Credentials Configuration window.

The entry will be validated to ensure the community name format, and that the limit for community names on the device has not been exceeded. If the community name is invalid, you will get an error message. Otherwise, the V2 Credentials Configuration dialog is updated with the new entry.

Up to five community names for each device can be defined through PCM.

A maximum of two community names can be configured on a wireless device. One is used as the read community name, and another is used as the write community name. The community name added as manager restricted is set as the read community, and the one added as manager unrestricted is set as the write community on the device.

Click **Next** in the V2 Credentials Configuration dialog to continue.

If you selected only SNMP settings, and the SNMP V2 option, the procedure is finished at this point.

7. If you selected SNMP V3, the SNMP V3 Credentials window displays. Use this window to view and change SNMP V3 USM users configured on the selected device.

SNMPV3 provides a secure communication that requires PCM to use a username (governed by its assigned security level) to communicate with the device.



Figure 7-12. Communication Parameters in Device: SNMP V3 credentials

If you selected more than one device before launching the wizard, the credentials columns will be blank. You can add a USM users for all selected devices, but you must select devices individually in order to modify or delete USM user information.

USM users allow access to devices using SNMPV3. When configured, PCM will use the management USM user to communicate with the selected device. Up to five USM users for each device can be defined.



- a. Click the Add Names button in the toolbar. This will display the Add USM User dialog.

Figure 7-13. Device Communication Parameters: SNMP V3 Add USM user

Enter the USM User information:

- In the Username field type the USM user name you want to create. A USM user name must be unique and cannot contain the > or < character.
- Select the desired Authentication Protocol from the drop-down menu.
- In the Auth Password field, type the password you want to use for authentication.
- Select the desired Protocol from the Priv Protocol drop-down menu.
- In the Priv Password field, type the password you want to use.
- Click to select the Use this as the management USM User? option. This will set the USM user as the management USM user.
- Click **OK** to save the changes and return to the V3 Credentials Configuration window.

The entry will be validated to ensure the USM user name and password format. If the USM user name or password is invalid, you will get an error message. Otherwise, the V3 Credentials Configuration dialog is updated with the new USM User entry.

Note:

The username and password length requirements vary between device types. If you do not match the requirements for the selected device the configuration will fail.

- b. Click **Next** in the V3 Credentials Configuration dialog to continue.

If you selected only SNMP settings and the SNMP V3 option, the procedure is finished at this point.

8. If you selected CLI Settings in the Configure Settings window, the CLI Settings Configuration window displays.

Select Telnet or SSH, then click **Next** to continue.



Figure 7-14. Device Communication Parameters: CLI mode selection

If an option is not selected, that option will be disabled on the switch.

Currently SSH configuration is not supported on 420 wireless devices, 9315, 9308, 9304, 6308, and 6304 switches.

9. If you selected Telnet, the User Credential Configuration window displays.



Figure 7-15. Device Communication Parameters: Telnet User Credentials

- a. Check the Leave the existing settings checkbox, and then click **Next** to continue,

OR

Check the Enable Password Protection checkbox and then:

- To set up a manager login, type the new manager user name in the Mgr Username field and the associated password in the Mgr Password field.
 - To set up an operator login, type the new operator user name in the Opr Username field and the associated password in the Opr Password field.
- b. Click **Next** to continue.

10. If you selected SSH in the CLI Settings Configuration, the SSH Configuration window displays.



Figure 7-16. Device Communication Parameters: SSH Configuration

11. Select the SSH version, and the Authentication type, then click **Next**

Note:

Key authentication for SSH1 is not supported.

If you selected Password Authentication, the User Credentials Configuration window displays. This is the same window as used for setting Telnet User Credentials. Follow the procedure described for Step 10 on page 7-22.

If you selected Key Authentication, after you click Next the Summary window displays.

12. When you have finished setting the Communication Parameters, the Results window displays, indicating if the communication parameter settings for the Device are successfully configured. If not, you will see a message in the Results pane indicating the configuration was not completed.

Setting Communication Parameters in PCM

The Communication Parameters in PCM Wizard is used to view and change the CLI, SNMP, and WebAgent parameters used by PCM to communicate with a device. Changes made in this window are stored in PCM, but not in the selected device. Use the Communication Parameters in Device Wizard to update CLI and SNMP parameters in PCM and the device.

If you launch the wizard by selecting multiple devices, the fields in the wizard are empty. If you launch the wizard by selecting a single device, the wizard displays values stored in PCM for the selected device.

To override the Global Preferences that PCM uses for Device Access via SNMP, CLI, and WebAgent on selected devices:

1. Select the device (or devices) in the Devices List or the Navigation Tree then click the Device Access button in the toolbar to display the Device Access Tools menu; or, you can right click a device and select Device Access →Communication Parameters in PCM from the menu.

This launches the Communication Parameters in ProCurve Manager Wizard.

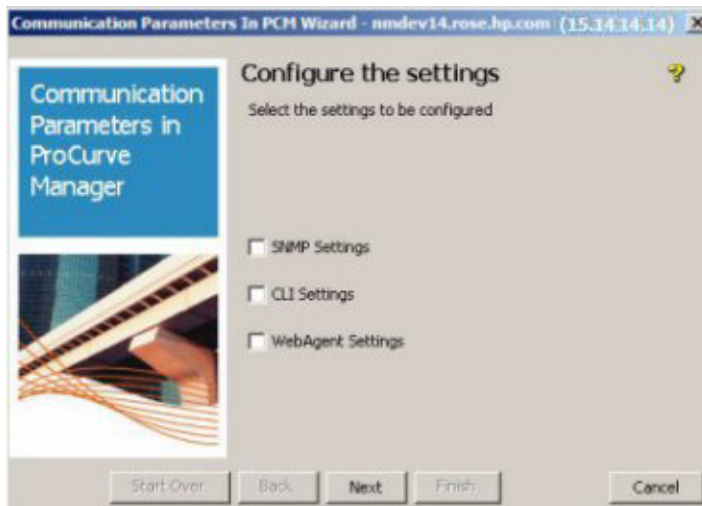


Figure 7-17. Communication Parameters in PCM

2. Select any one, or combination of the check boxes (defined below), then click **Next**.

SNMP Settings	Change the settings PCM uses for SNMP communication
CLI Settings	Change the settings PCM uses for telnet or SSH communication
Web Agent Settings	Change the settings PCM uses to launch the system's default Web browser and target the device's Web Agent

Instructions for setting configuration parameters follow, in the order they would appear if all three options are selected.

3. If you selected the SNMP settings, the Configure SNMP Timeout and Retries window displays.

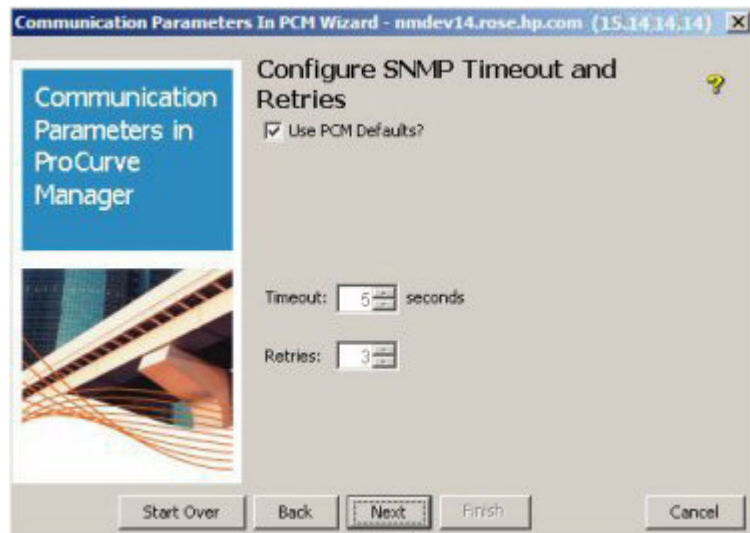


Figure 7-18. Communication Parameters in PCM: SNMP configuration

4. Click **Next** to continue, and accept the PCM defaults, or
 - a. Click the check box to de-select **Use PCM Defaults**,
 - b. Set the **Timeout** and **Retries** intervals as needed.

Click the up or down button to increase or decrease the number of seconds before a timing out the connection, and the number of times to retry connecting when a Timeout occurs.

- c. Click **Next** to continue to the Configure SNMP Version window.

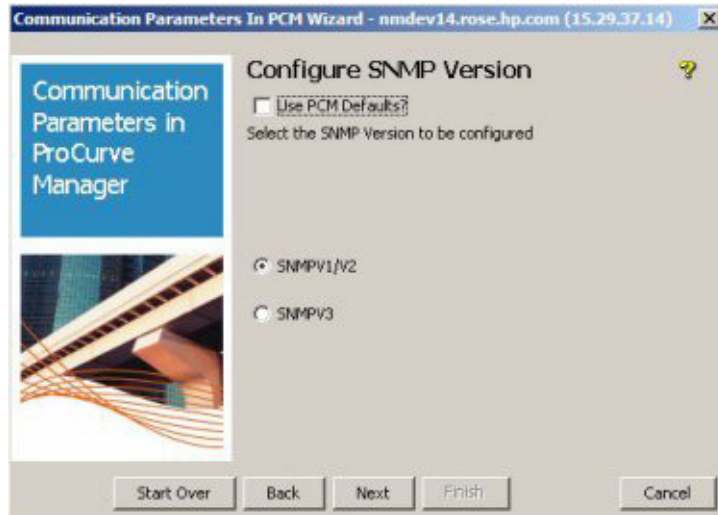


Figure 7-19. Communication Parameters in PCM: SNMP version

5. Click **Next** to continue, and accept the PCM default (SNMPV2), or
 - a. Click the check box to de-select **Use PCM Defaults**,
 - b. Click to select the version (SNMP V2 or SNMP V3) you want PCM to use with the selected device.

If the device does not support SNMP V3, the button is disabled.

If multiple devices are selected, and one of the selected devices supports SNMP V3, the button is enabled; however, the SNMP V3 settings will only be applied to the device or devices that support it. It will be ignored on devices that do not support SNMP V3, and SNMP V1/V2 remains the version used for device access.

- c. Click **Next** to continue to the Configure SNMP Credentials window.
6. For SNMP V2, the next window is the "Configure SNMP V2 Credentials"

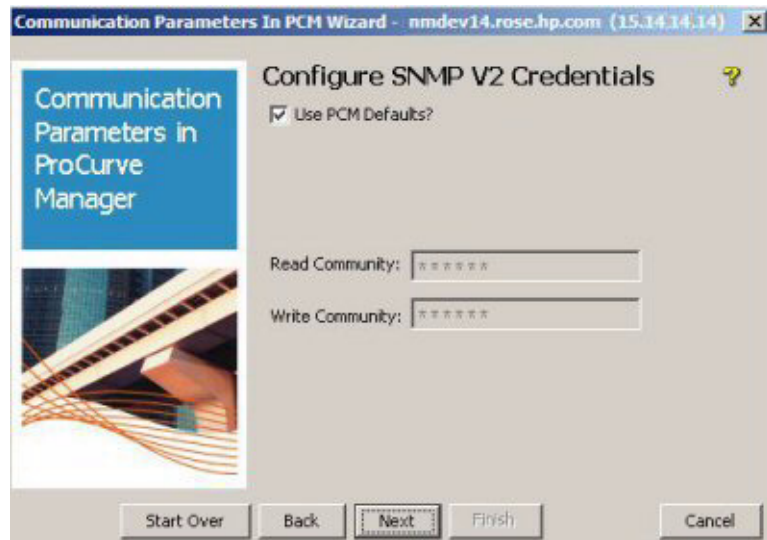


Figure 7-20. Communication Parameters in PCM: SNMP V2 Credentials

7. Click **Next** to continue, and accept the PCM defaults, or
 - a. Click the check box to de-select **Use PCM Defaults**,
 - b. Type the SNMP **Read Community** name and **Write Community** name that PCM will use with the device. This will override the Preferences setting for the selected device.

Note:

PCM uses the default SNMP community name of "public" for both Read and Write Community Names. These community names can be changed during installation, or on the Discovery tab in Agent Manager.

If you change the SNMP Credentials used by an Agent for device access, use the Test Communication Parameters in PCM feature to verify PCM's ability to access the device.

8. For SNMP V3, the next window is the "Configure SNMP V3 Credentials"

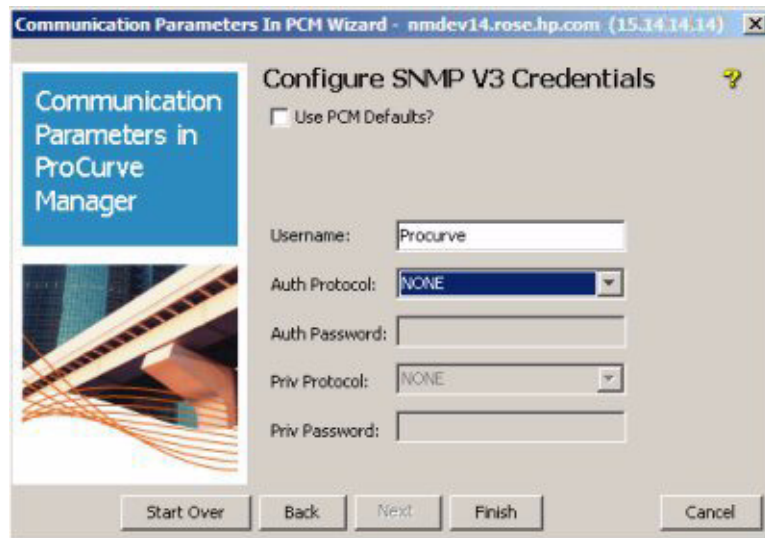


Figure 7-21. Communication Parameters in PCM: SNMP V3 Credentials

9. Click **Next** to continue, and accept the PCM defaults, or
 - a. Click the check box to de-select **Use PCM Defaults**,
 - b. Type the **Username**.
 - c. Select the **Authorization Protocol** if used, and type the **Authorization Password**.
 - d. Select the **Privacy Protocol** if used, and type the **Privacy Password**.
 - e. Click **Next** to continue.

If you are changing only the SNMP parameters, you would finish the procedure at this point.

10. If you selected the CLI Settings, the Configure CLI Timeout and Retries window displays.

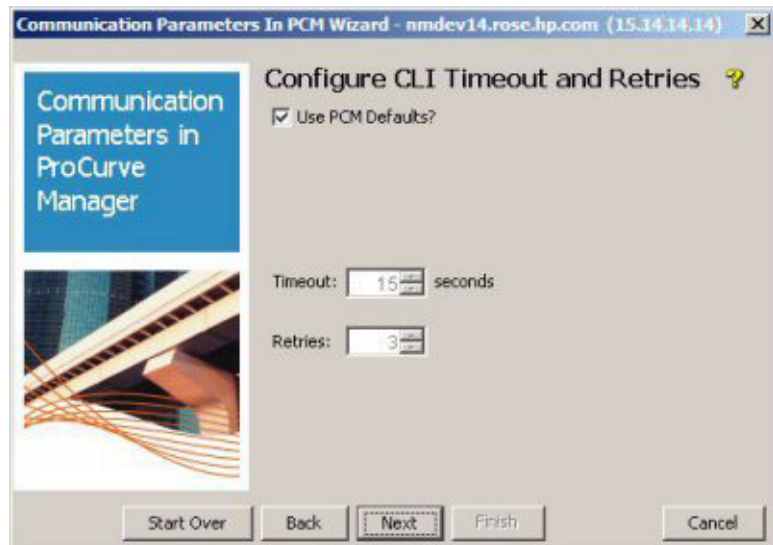


Figure 7-22. Communication Parameters in PCM: CLI configuration

11. Click **Next** to continue, and accept the PCM defaults, or
 - a. Click the check box to de-select **Use PCM Defaults**,
 - b. Set the **Timeout** and **Retries** intervals as needed.

Click the up or down button to increase or decrease the number of seconds before a timing out the connection, and the number of times to retry connecting when a Timeout occurs.

- c. Click **Next** to continue to the Configure CLI Mode window.

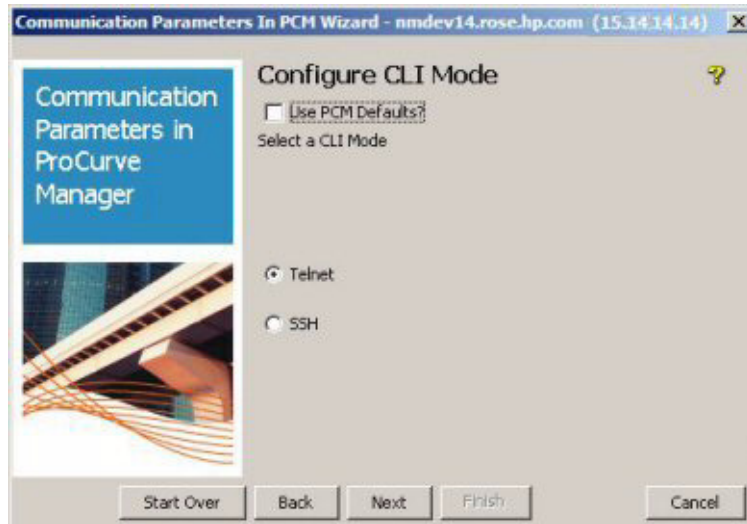


Figure 7-23. Communication Parameters in PCM: CLI Mode selection

12. Click **Next** to continue, and accept the PCM default (Telnet), or
 - a. Click the check box to de-select **Use PCM Defaults**,
 - b. Click to select the CLI mode to use with the selected device.
 - c. Click **Next** to continue
13. If you select Telnet, the Configure CLI User Credentials window displays.



Figure 7-24. Communication Parameters in PCM: CLI Credentials

14. Click **Next** to continue, and accept the PCM defaults, or
 - a. Click the check box to de-select **Use PCM Defaults**, and enable the Username and Password fields.
 - b. In the **Mgr UserName** field, type the new manager user name.
 - c. In the **Mgr Password** field, type the Manager password.
 - d. In the **Opr UserName** field, type the new Operator user name. (optional)
 - e. In the **Opr Password** field, type the Operator password.

The user and password entries are not required to continue;
 - f. Click **Next** to continue.
15. If you selected SSH, the Configure SSH Credentials window displays.

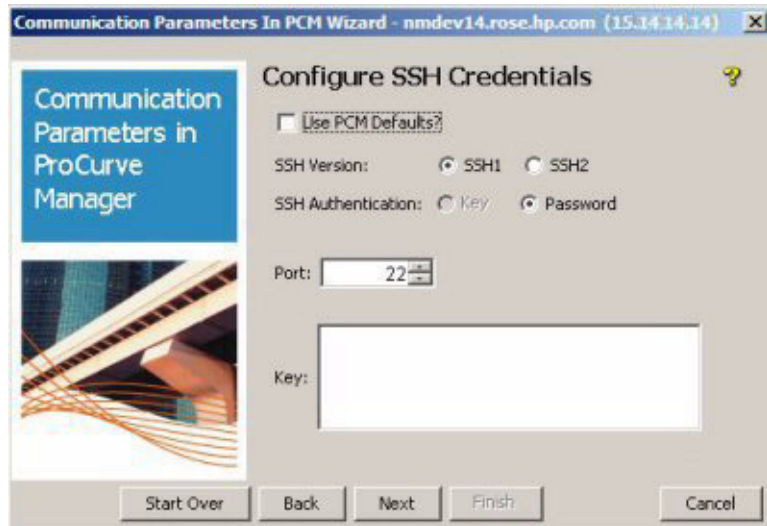


Figure 7-25. Communication Parameters in PCM: SSH Credentials

16. Click **Next** to continue, and accept the PCM defaults, or
 - a. Click the check box to de-select **Use PCM Defaults**,
 - b. Click the radio button to select the **SSH version** used by the device: SSH1 or SSH2.
 - c. For SSH 2, click the radio button to select the **SSH Authentication** method to use: Key or Password authentication.
 - d. For SSH1, Password is automatically selected and Key is disabled.

e. For SSH 2 using Key authentication:

- Enter the Port number PCM will use to connect with the device.
- Enter the Key that PCM will use to authenticate with the device.

To get the public fingerprint key of the device, on the Device CLI execute the command:

```
show crypto host-public-key fingerprint
```

Copy the version specific finger print. For SSH2 you would copy only the second line.

```
<Command: show crypto host-public-key fingerprint >  
896 a5:d4:f0:a5:7c:93:76:61:42:f2:25:6e:96:91:86:28 host_ssh1  
896 c9:36:ae:bc:8d:33:94:3b:3e:b6:31:5e:91:17:6d:11 host_ssh2.pub
```

"Paste" the device's public-key finger print in the Key field in the PCM wizard.

- f. If you selected SSH 1, or SSH 2 with Password authentication, click **Next** to continue to the Configure CLI User Credentials window. These entries are the same as described for step 14 on page 7-31.
- g. If you selected SSH2 with Key authentication, click Finish to save the configuration and exit the wizard.

If you selected only CLI settings to configure, you would finish the procedure at this point.

17. If you selected Web Agent settings, the Configure WebAgent Credentials window displays.



Figure 7-26. Communication Parameters in PCM: Web Agent Credentials

18. Click **Next** to continue, and accept the PCM defaults, or
 - a. Click the check box to de-select **Use PCM Defaults**,
 - b. Click one of the radio buttons to select the WebAgent protocol to be used (Http or Https) or to Disable WebAgent.
 - c. Select the **Port** that PCM will use to communicate with the device.
 - d. Click **Finish** to complete the procedure.

Modifying Community Names

The PCM Management Community Name is set at installation. If you do not specify one, PCM will use a default Management Community name of "public," with full read and write privileges to the device. This is used by PCM for auto-discovery, traffic monitoring, SNMP trap generation and threshold setting. If security for network management is a concern, it is recommended that you change the write access for the "public" community to "restricted."

Note:

If you are using the PCM-NNM module, the default Community Names are provided by NNM. You can still modify the Management Community names using the procedure below. The data will be passed to NNM from the event generated by PCM when you apply the change to the device.

To modify a Community Name for a Device,

1. Select the device in the Devices List, then launch the Device Access > Communication Parameters in Device Wizard
2. Select the **SNMP Settings**, then the **SNMP** version (SNMPV1/V2 or SNMPV3).
3. In the Credentials Configuration window, select the Community name you want to use as the Management Community, then click the Modify button in the toolbar. This will display the Modify Community Names dialog, similar to the Add Community Names dialog.



If the Community Name you want to use is not found, add the Community Name and select it as the management community. When you click OK, a validity check on the community name will be performed. If it is valid, the Community Names list will be updated with the new entry.

4. To set the name as the Management Community, select **Use this as the Management Community?**, then click **OK** to save the change and close the dialog.
5. When you return to the Credentials Configuration window, the changes will be reflected in the Community Names listing.

The name selected as the Management community appears at the top of the list and the Manager check box is selected.

Deleting Community Names

To delete a Community Name:

1. Select the device in the Devices List, then launch the Device Access > Communication Parameters in Device Wizard
2. Select the **SNMP Settings**, then the **SNMP** version (SNMPV1/V2 or SNMPV3).
3. In the Credentials Configuration window, select the community name you want to delete, then click the Delete button in the toolbar. A confirmation dialog will be displayed.
4. Click **Yes** to complete the delete process. If you have selected the Management Community Name, you will get an error notice telling you are not allowed to delete the Management Community Name.



To delete all the currently configured Community Names for the device, select the Delete All button in the toolbar.



Using Test Communication Parameters in PCM

The Test Communication Parameters in PCM window is used to compare SNMP and CLI communication parameters stored on a device and those stored in PCM for the device. If the values match, the test succeeds and PCM can communicate with the device using the SNMP or CLI communication parameters defined in PCM.

The Test Communication Parameters window displays the following information for selected devices:

Device	Identifies the devices being tested by IP address and/or DNS name
CLI Mode	Displays Telnet or SSH, depending on the mode used by PCM to communicate with the device
CLI Manager	Displays Success if PCM was able to login to the device through CLI as the manager, or displays Failure if PCM could not login to the device through CLI as the manager.
CLI Operator	Displays Success if PCM was able to login to the device through CLI as the operator, or displays Failure if PCM could not login to the device through CLI as the operator.
SNMP Version	Identifies SNMPV2 or SNMPV3, depending on the SNMP version used by PCM to communicate with the device
SNMP Read Community	If using SNMPV2, displays Success if PCM was able to read data from the device or No Access if PCM was unable to read data from the device
SNMP Write Community	If using SNMPV2, displays Success if PCM was able to write data in the device or No Access if PCM was unable to write data in the device
SNMPV3	If using SNMPV3, displays Success if PCM was able to communicate with the device or Unsuccessful if PCM was unable to communicate with the device
Status	Current status of the test

Device	CLI Mode	CLI Mana...	CLI O...	SNMP Ver...	SNMP Read...	SNMP Write...	SNMPV3	Status
ros59441la...	Telnet	Failed: Log...	Success	SNMPV2	Success	No Access	-	Completed
hummer-sw...	Telnet	Failed: Inc...	Failed: Inc...	SNMPV2	Success	Success	-	Completed

Figure 7-27. Test Communication Parameters results window

To test communication parameters:

1. Navigate to the Test Communication Parameters in PCM window.
2. In the navigation tree, right-click the device or device group to test.
3. Select Device Access from the drop-down list.
4. Select Test Communication Parameters in PCM from the Device Access drop-down list.

Alternately, you can:

1. In a device-related window, select one or more devices to be tested.
2. Click the Device Access button on the toolbar.
3. Select Test Communication Parameters in PCM from the Device Access drop-down list.

Check the results in the Test Communication Parameters window to ensure that all communications were successful.

If the test failed, change the communication parameters in PCM. Refer to “Troubleshooting Device Communication Problems” on page 7-38 for additional information.

To abort testing at any time, click Halt, which stops the test process without closing the window, or click Close, which exits the process and closes the window.

4. Click Close to exit the Test Communications Parameter Wizard.

Troubleshooting Device Communication Problems

If PCM is unable to communicate with a ProCurve device on your network, it may be caused by one or more of the following problems:

- The default switch configuration is set to Menu instead of CLI. Use the Setup command on the switch CLI to change the Login Default to CLI.
- The Primary SSH login is not set as the "Public Key" on the switch.
- The Client Public Key is incorrectly copied into PCM.
- The SSH version set in PCM is mismatched with the SSH version supported on the switch.
- The SSH key size for the key generated on PCM is mismatched with the key size set on the switch.
- Some of the switches support only a specific version of SSH. If you generate a key on PCM, both SSH ver1 and ver2 keys are generated. Be sure to copy the correct key to the switch.

Note:

When the SSH key is regenerated on PCM, all device communications between the Agent and devices using the old key will fail until the new Key has been copied to the device. Similarly, if the SSH key is regenerated on a device, communications with PCM will fail until the key is copied to PCM.

You can use the following procedures to check SSH related configurations.

For SSH with Password Authentication:

1. Select a switch that supports SSH
2. Use the Test Communication Parameters Wizard to check that the switch and PCM are in sync with each other.
3. Telnet to switch and run the following commands:

```
$ ip ssh key-size 1024
$ crypto key generate ssh rsa
$ ip ssh
```
4. Use the Communication Parameters in PCM Wizard for the device. Modify the CLI options to configure the SSH (Password) settings to match the switch.

For SSH with Key Authentication:

1. Go to Agent Manager > Device Access > SSH
2. Set the key-size as **1024** and click **Generate new key pair**.
3. Verify the SSH version installed on the switch.
4. Copy the `procurveSSH2.pub` file from the `PNM/server/config` directory to the `PNM/pcm-agent/data/download` directory, and then telnet to the device and execute the command:

```
copy tftp pub-key-file <ip address> procurveSSH<n>.pub manager
```

where *ip address* is the IP address of the Agent and *<n>* is the SSH version number.

5. Get the finger-print of the "host-public-key" from the switch:

```
$ show ip host-public-key fingerprint
```

Note: Copy only the line for the SSH key type needed (SSH1 or SSH2). This is what you will "paste" into the Key field in the PCM wizard.

6. Use the Communication Parameters in PCM Wizard for the device. Modify the CLI options to configure the SSH (Key Authentication) settings to match the switch.

This should allow for launching the SSH terminal after Authentication.

Using Global Device Access Preferences

In addition to the Device Manager functions, PCM provides Global Preferences for device access, including SNMP and Telnet access information preferences.



To change the Global Device Access settings, click the Preferences button in the PCM toolbar, then expand the Device Access node in the menu to display the available options.

Setting Device Display Names

Use the Global:Device Access window to set the Device Display Name and Port Name displays in PCM.

1. Select Device Access in the Preferences menu.

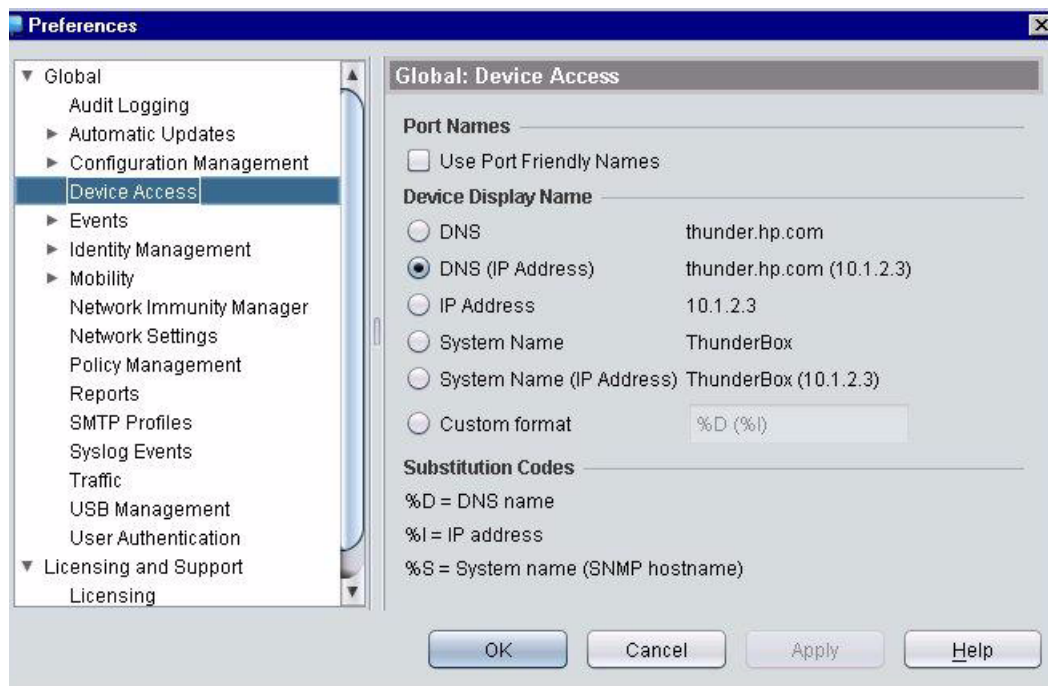


Figure 7-28. Preferences, Global:Device Access window

2. To display port friendly names on PCM screens instead of the port interface name (e.g., A1, B2), check the Use Port Friendly Names check box.

If a friendly name for a port has not been configured, PCM displays the port interface name. If a PCM feature allows you to enter a port name as input, PCM will continue to display the port interface name even when the Use Port Friendly Names check box is checked.

3. To use a standard naming convention, select the desired device display name in the Device Display Name section.
4. To use a custom naming format, select Custom Format, and type the text and/or codes you want to include in device names. Possible codes are:

%D	DNS name
%I	IP address
%S	SNMP hostname

For example, type %S SNMP hostname to display Thunderbox SNMP hostname.

5. Click OK to save the Display Name settings and close the window.

Setting Agent-Specific Device Access Preferences

The following Device Access preferences can be customized for each Agent:

- Device Access Agent Response Timeout
- CLI (Telnet and SSH)
- SNMP (SNMPv1/v2 and SNMPv3)
- SSH Keys
- WebAgent Protocol and Port

These preferences are described in “Configuring and Managing Agents” in chapter 3.

Configuring RMON Alerts

The RMON Manager (Remote Monitoring) feature in PCM provides an interface you can use to configure RMON alert thresholds for monitoring "ethernet statistics" on a device port or VLAN. When an RMON threshold is exceeded on a monitored device an alert is sent to all trap receivers configured for the device.



To review or configure the RMON alert thresholds set for a device, select the device in the Devices List then click the Launch RMON Manager button in the toolbar. The RMON Manager window displays with a list of currently configured alert thresholds for the selected device.

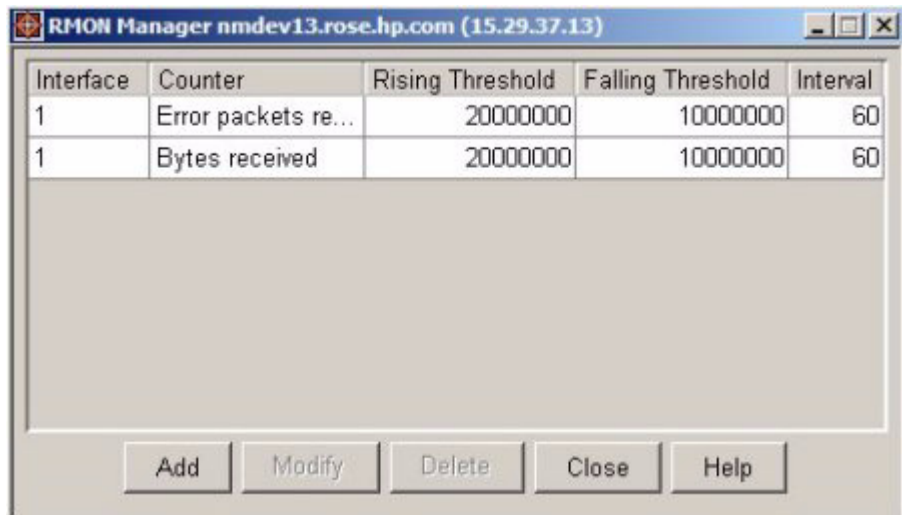


Figure 7-29. RMON Manager main window.

(Refer to RFC 2819 for details on implementation of RMON and use of RMON Statistics in the MIB)

Adding and Modifying RMON Alerts

To set a new RMON alert, click **Add** to display the RMON Thresholds dialog. To modify an existing alert, select it on the list of thresholds, then click Modify.

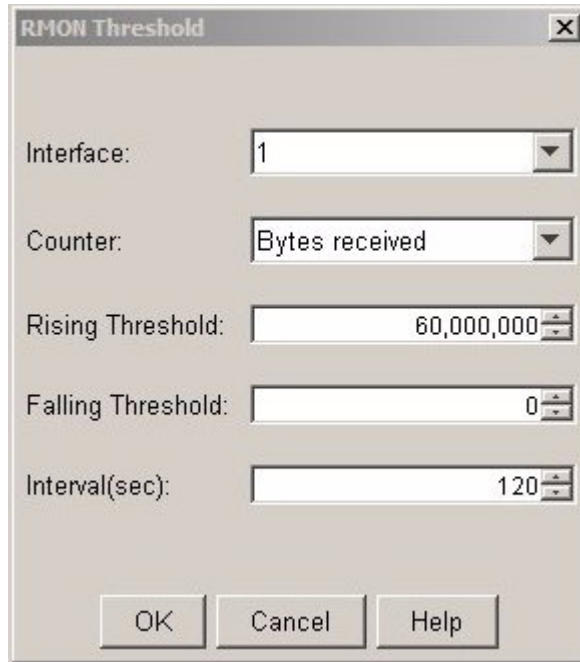


Figure 7-30. Add/Modify RMON Thresholds dialog

RMON alerts are composed of five elements: interface, counter, rising threshold, falling threshold, and interval, defined as follows:

Interface	Specifies the port on the target device on which to configure the RMON alert. Select from the available ports using the drop down menu. You can also select a VLAN interface from the list to measure traffic to and from the VLAN on any port on the switch configured for that VLAN.
Counter	This defines the specific RMON variable to monitor. A trap is sent to all listed trap receivers if the counter variable crosses the rising or falling threshold values. Select the Counter type from the drop down menu.
Rising Threshold	This numeric value defines the upper limit for the monitored variable. Should the variable exceed this limit a trap will be sent. Use the up and down buttons to increase or decrease the threshold value, or type the desired value.

Falling Threshold	This value defines the lower limit for the monitored variable. Should the variable drop below this value a trap will be sent. Use the up and down buttons to increase or decrease the threshold value, or type the desired value.
Interval	This value specifies the variable sample rate in seconds. Use the up and down buttons to increase or decrease the threshold value

Click **OK** to complete the add or modify process and close the dialog. The RMON Manager alert threshold listing will be updated with the new settings.

The RMON Manager has a built in mechanism to prevent multiple events from being generated should the sampled value oscillate around one of the threshold values. Thus, in order for a rising threshold event to occur the sampled variable must first go below the falling threshold value. Conversely, before a falling threshold event can occur, the sampled variable must first exceed the rising threshold value.

For example, if the sampled variable exceeds the rising threshold value, a Rising threshold alert will occur. If the sampled value drops back below the rising threshold and then rises above the rising threshold, an alert will not occur. In order for another Rising alert to occur, a Falling threshold alert must first occur.

Sample Rising Alert message in the PCM events (SNMP Traps) tab display:

%2 is above threshold %5; value = %4. (Sample type = %3; alarm index = %1)

Where:

%2 = the counter being monitored

%5 = the threshold level the user set

%4 = the value of the counter when the trap was generated

%3 = the sample type used (absolute or delta, represented as numeric values defined in the MIB)

%1 = the alarm

Deleting RMON Alerts

To delete an RMON Alerts from the device, select the alert in the list in the RMON Manager window, then click **Delete**. The alert is removed from the list in the RMON Manager window.

Other Device Management Tools

In addition to the functions provided by the PCM Device Manager, you can also access the Web Agent for the switch, or launch a telnet session to the Menu Interface for the switch from within the PCM display.

To access the Web Agent for a device, select the device in the Devices List or in the navigation tree, then open the "right click" menu and select the Connect to Web Agent option. This will launch the Web Agent browser, with the Status tab displayed.

To Telnet to a device, select the device in the Devices List or in the navigation tree, then open the "right click" menu and select the Telnet option. This will open a Telnet session to the device and launch the Main Menu Interface.



You can also select devices in the Devices List, then select the CLI button from the Device Configuration options menu in the toolbar to launch the CLI Wizard. See "Using the CLI Wizard" on page 12-20 for more information.

For details on using the Web Agent, Menu Interface, and CLI, refer to the Configuration Management manuals that came with the switch device.

Device Logs

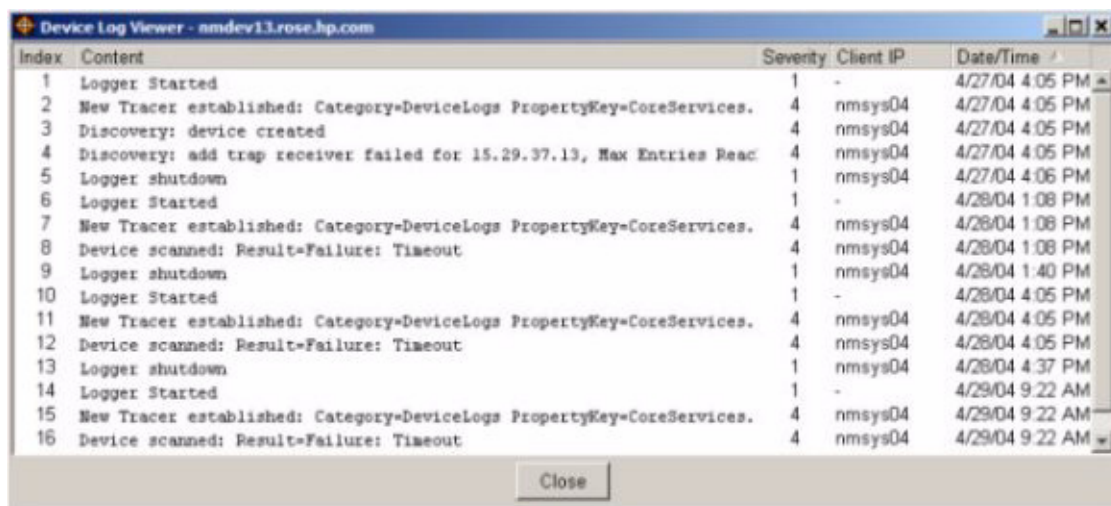
This section describes the tools provided with this release of PCM that you can use to assist in finding and resolving problems that occur in individual devices on the network. For more detailed information on troubleshooting device problems, refer to the "Management and Configuration Guide" that came with your switch device.

Using the Device Log



The PCM application provides a Device Log viewer you can use to check the log entries created for a device by PCM. Select a device in the Devices List, then click the Device Log Viewer button in the toolbar to display the Device Log Viewer window.

The Device Log Viewer shows a list of log entries for actions performed by PCM on the device. It will list the type of log entry, when it was created, and the log file name, along with additional details on data stored in the log file. You can drag the window pane separator to increase the detail section of the Device Log Viewer window. You can also copy and paste the device log entries to another application (such as notepad or MS Word) if desired.



Index	Content	Severity	Client IP	Date/Time
1	Logger Started	1	-	4/27/04 4:05 PM
2	New Tracer established: Category=DeviceLogs PropertyKey=CoreServices.	4	nmsys04	4/27/04 4:05 PM
3	Discovery: device created	4	nmsys04	4/27/04 4:05 PM
4	Discovery: add trap receiver failed for 15.29.37.13, Max Entries Reac	4	nmsys04	4/27/04 4:05 PM
5	Logger shutdown	1	nmsys04	4/27/04 4:06 PM
6	Logger Started	1	-	4/28/04 1:08 PM
7	New Tracer established: Category=DeviceLogs PropertyKey=CoreServices.	4	nmsys04	4/28/04 1:08 PM
8	Device scanned: Result=Failure: Timeout	4	nmsys04	4/28/04 1:08 PM
9	Logger shutdown	1	nmsys04	4/28/04 1:40 PM
10	Logger Started	1	-	4/28/04 4:05 PM
11	New Tracer established: Category=DeviceLogs PropertyKey=CoreServices.	4	nmsys04	4/28/04 4:05 PM
12	Device scanned: Result=Failure: Timeout	4	nmsys04	4/28/04 4:05 PM
13	Logger shutdown	1	nmsys04	4/28/04 4:37 PM
14	Logger Started	1	-	4/29/04 9:22 AM
15	New Tracer established: Category=DeviceLogs PropertyKey=CoreServices.	4	nmsys04	4/29/04 9:22 AM
16	Device scanned: Result=Failure: Timeout	4	nmsys04	4/29/04 9:22 AM

Figure 7-31. Device Log Viewer window

The Client IP is the address of the PCM console from which the action (command) was sent to the device.

Using Device Syslog

Syslog is a logging tool that allows a "client" switch to send event notification messages to a networked device operating with the Syslog Server software.

To enable the Device Syslog function in PCM, you need to set the PCM Server as the Syslog server. You can use the CLI functionality in PCM to do this, entering the command:

```
config logging <syslog-ip-addr>
```

where *syslog-ip-addr* is the IP address of the PCM Server. For additional information refer to the section on "Syslog Operation" in the "Management and Configuration Guide" for your switch.

Performance of the system can be jeopardized by collecting syslog from too many devices. Therefore, we recommend that you enable the Device Syslog function on a limited number of key devices or send syslog events to another server.

To review the Device Syslog in PCM, double-click the device node in the tree or Devices List to display the Device Properties window, then click the Device Syslog tab.

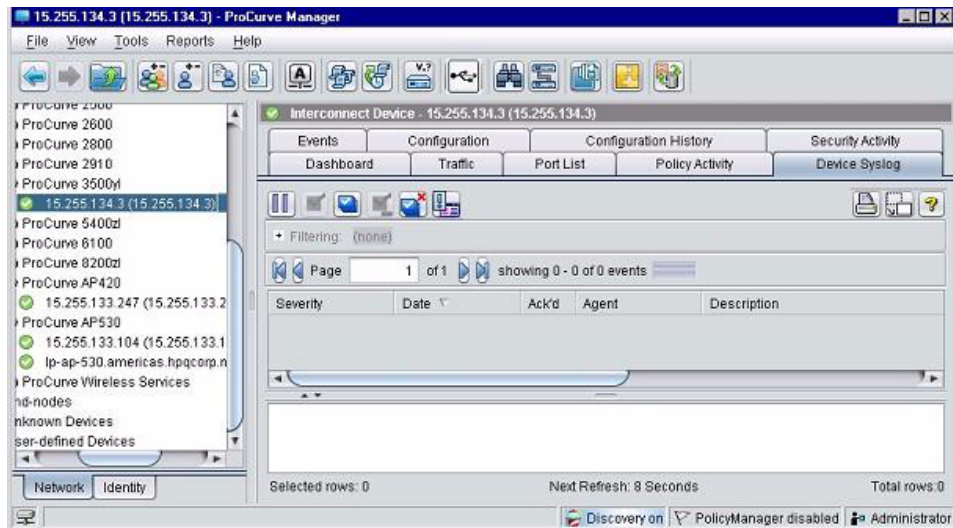


Figure 7-32. Device Syslog window.

The information in the Device syslog is similar to data found in the Events tab.

Severity: The Severity column shows the severity of each event, one of:

- Informational - Routine events
- Warning - Unexpected service behavior
- Minor - Minor switch error that may impact performance
- Major - Major switch error with potential of inhibiting some switch operations
- Critical - Severe switch error with the potential of halting all switch operations

Status: The Status column identifies whether the event has been acknowledged. A green asterisk indicates that the event has been acknowledged, and a red asterisk indicates that the event is new and has not been acknowledged.

Date: The Date column identifies the date and time when the event occurred. The date is shown in the Day of Week-Month-Day-Time-Year format. Time is shown in the 24-hour clock format hh:mm:ss followed by the time zone.

Description: The Description column provides a short description of the event. The description is derived from a list of predefined event type descriptions included with the PCM application.

Filtering Syslog Events

Use the Filter field at the bottom of Device Syslog window to enter text to search for within the event "Description". Just type the word(s) you are searching for, then click Apply Filter. The listing will be resorted so that all events in which the filter text is found are at the top of the list.

Acknowledging Syslog Events

Acknowledging an event indicates that you are aware of the event but it has not been resolved.



To acknowledge an event, select the event(s) to be acknowledged in the list then click the Acknowledge button below the list.

The "Acknowledge Event" action will set the selected event(s) as acknowledged, update the Syslog file, and update the event status in the list to reflect the change.

Deleting Syslog Events



To delete an event select the events that you want to delete, then click the Delete Event button below the events list.

Deleting a Syslog event will remove the event from the Syslog file and the Device Syslog display.

Managing Syslog Size

The PCM Syslog server can hold a maximum of 1500 events. You can use the Syslog Events option in the Global Preferences to reduce the number of events the Syslog will hold, and the rate at which the Syslog file will be automatically trimmed (cleared) of excess files.

1. Select the Syslog Events option in the Preferences menu to open the Global:Syslog Events window.

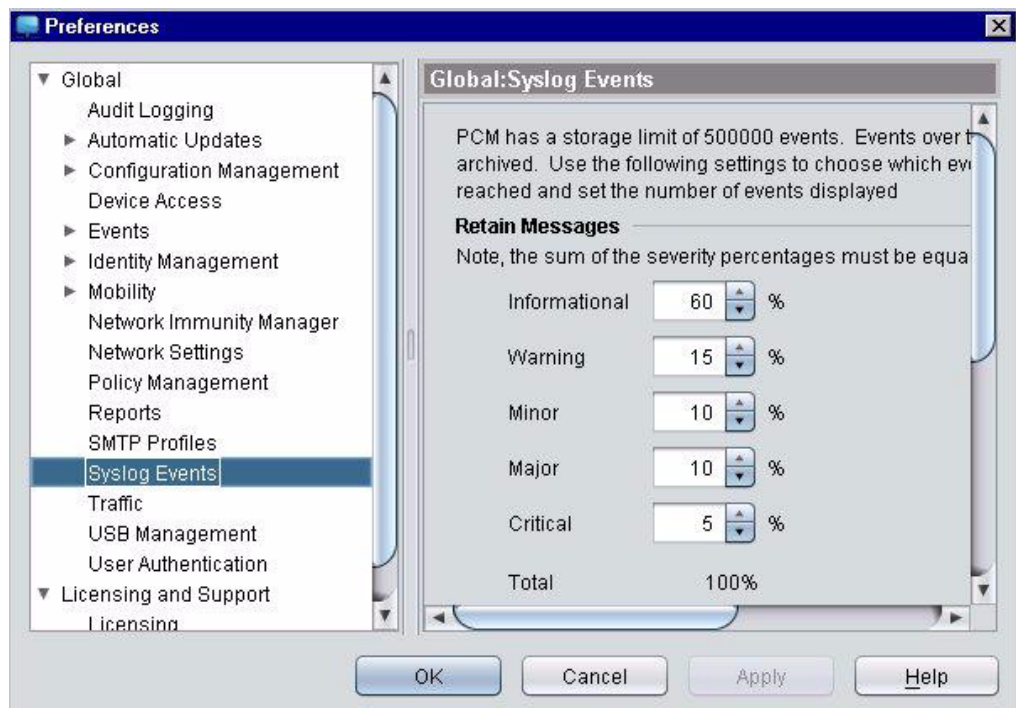


Figure 7-33. Global Preferences: Syslog Events options

2. For the **Number of Syslog events per device**: type the number of events or use the buttons to increase or decrease the number of events.
3. For **Trim Syslog messages every**: type the interval (number of hours) that you want to wait before trimming the Syslog file to the maximum number of entries, or use the buttons to increase or decrease the trim interval.

If a device is generating many events in the Syslog, the log will hold the events over maximum, but operations with Syslog will be impacted, and eventually the device operation may be impacted.

4. Click **OK** to apply the preferences and close the window.

Using the Audit Log

You can use the Audit Log functions in PCM to assist in compliance with IT auditing and governmental regulations for IT systems security. When Audit Logging is enabled, a log of any changes or actions made to the managed network devices is made. You can generate a report of the Audit Logs to help meet audit requirements.



To review the Audit Log for all devices, click the Audit Log button in the global toolbar. To review the Audit Log for selected devices, select the device nodes in the navigation tree, or select the devices in the Devices list. Use the right-click menu to select the Audit Logs option, or click the Audit Log button in the toolbar.



Figure 7-34. Example of the Audit Log display

The PCM Audit Logging feature allows you to configure PCM to log all changes made via PCM to network devices by any PCM user. During normal run-time operation, each time that a user that is enabled for audit logging performs a configuration change to a device, PCM places a record in the audit log file. Each record contains the following information:

- the user that made the change,
- the Client IP where the change was made,
- the IP address of the device,
- the port that was affected (if any),
- the PCM module that was used,
- the date and time of the change,
- the context/operation performed (for example, "Port Friendly Name changed"), and
- the actual data used in the operation (e.g. the new friendly port name, the device configuration file, etc.).

The audit log can later be examined and filtered in a manner similar to the existing event browser functionality.

The PCM administrator can configure the Audit Log options for each user, using the Turn on audit logging and Allow to view audit logs options, as described for “Adding Profiles” on page 2-41.

Audit Logging Preferences

You can override the Audit Logging settings for users, and restrict access using the Audit Logging Preferences window. Go to Tools > Preferences > Audit Logging.



Figure 7-35. Global Preferences: Audit Logging window

The Global Preferences window for Audit Logging contains three parameters.

- **Turn on Audit Logging** - allows the Administrator to quickly enable or disable all audit logging. If you are experiencing performance problems or working to diagnose abnormal behavior in PCM, you may need to turn off functionality that could be contributing to abnormal behavior. This parameter lets you turn audit logging on or off without affecting the audit logging configuration for individual user accounts.
- **Force Audit Logging for all users** - allows the Administrator to force audit logging regardless of who the user is. If the Administrator is finding that some unknown person is changing device configurations without permission or perhaps a common configuration action is causing an unwanted side affect, this allows all device configuration changes to be temporarily monitored without having to manually

modify the audit logging configuration for each user. When the issue has been isolated, the Administrator can then uncheck the option to resume the normal audit logging functions.

Note that if a device configuration change is due to an automated action (arrival of a security event, for example), it will always be logged regardless of the user who setup the original policy. That is, as long as audit logging is turned on.

- **Audit Log only viewable by Administrator** - allows the Administrator to enhance security of the audit logging feature. This option, when enabled, allows only the Administrator to view the audit log files without having to modify the audit logging configuration for each ProCurve Manager user.

Replacing Network Devices

When replacing a discovered device with another device using the same IP address, rediscovering the new device does not update basic attributes and other dependent data structures in PCM.

Perform the following steps to replace a device:

1. Delete the old device from PCM, as explained in “To delete a device from Discovery:” on page 4-39.
2. Use the Manual Discovery Wizard to discover the new device, as explained in “Using Manual Discovery” on page 4-7.

Managing Modules

Managing ONE zl Modules	8-2
Managing a ONE Application	8-4
Installing a ONE Application	8-9
Activating the License for a ONE Application	8-13
Uninstalling a ONE application	8-16
Troubleshooting ONE zl Module Configuration	8-18

Managing ONE zl Modules

PCM supports the deployment and management of HP ProCurve Switch ONE zl (Open Network Ecosystem) Modules and compatible applications that run on the ONE Service Operating System. ONE zl Modules and installed applications are automatically discovered when PCM discovers a switch containing a ONE zl Module.

To display the ONE zl Modules installed in ProCurve network devices, click the ONE zl Modules folder under an Agent group in the PCM navigation tree. The discovered ONE zl Modules are listed in the ONE zl Modules tab.

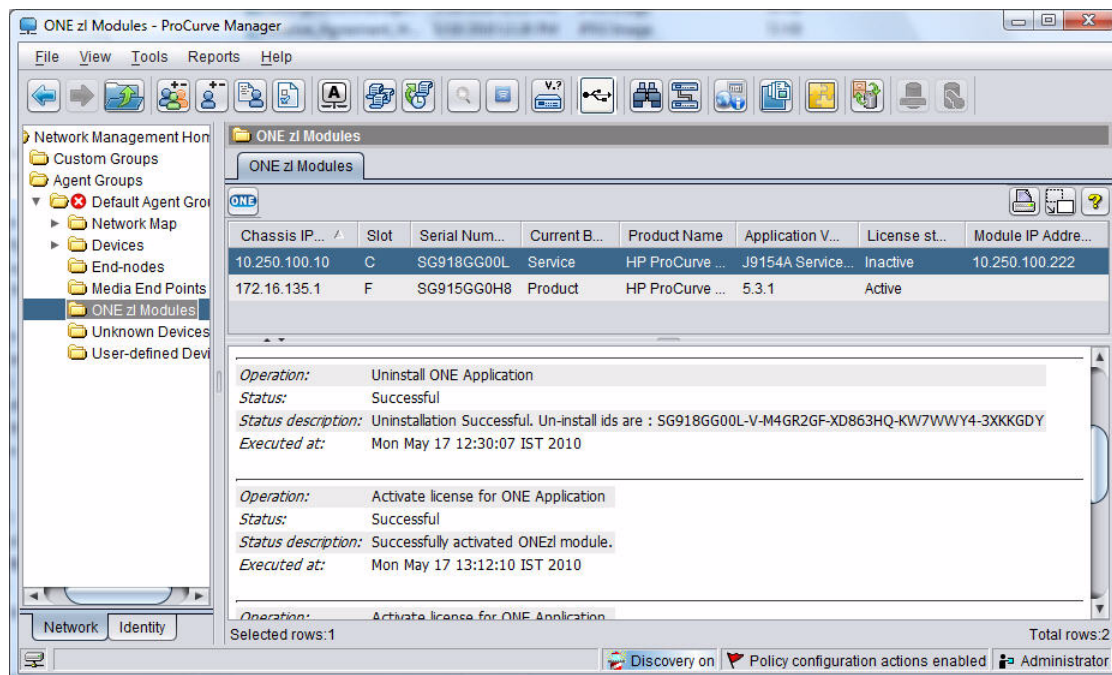


Figure 8-1. ONE zl Modules Tab

From the ONE zl module list, you can access PCM features to deploy and manage ProCurve ONE zl Modules and supported applications, such as PCM Agent and Threat Management Services (TMS).

The following information is displayed for each ONE zl Module:

Chassis IP Address	IP address of the switch in which the ONE zl Module is installed
Slot	Switch slot in which the ONE zl Module is installed
Serial Number	Serial Number of the ONE zl Module
Current Boot	Whether the ONE zl Module is currently booted from the Service Operating System or an installed software application (Open Architecture product), such as PCM Agent
Product Name	The application currently installed on the ONE zl Module. This column is blank if no product is installed.
Application Version	Version number of the Operating System service or application used to boot the ONE zl Module
License Status	Status of the license for the application installed on the ONE zl Module: Active Application and license are installed. Inactive Neither the application nor license are installed. Installed License key is still installed for an application that has been uninstalled. Unknown The application is not installed and the license state is unknown.
Module IP Address	IP address of the Service OS if the module is booted into the Service OS, or IP address of the application if the module is booted into the Product OS

For more information about ONE zl Modules, refer to the *Installation and Getting Started Guide for the HP ProCurve Switch ONE zl Module* at <http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm>.

Troubleshooting ONE zl Modules

To display a history of the configuration operations performed on a ONE zl Module, click on an entry in the ONE zl Modules tab (see figure 8-1). The history is shown at the bottom of the tab, and describes each action performed with the ONE zl Module Management Wizard since the module was last discovered by PCM.

You can enlarge or shrink this history pane by dragging its top bar or by clicking the up or down arrow on the left side of the top bar. For more information, see “Troubleshooting ONE zl Module Configuration” on page 8-18.

Managing a ONE Application

You can manage the software applications on a ONE zl Module in the following ways:

- Install an application.
- Activate the license for an installed application.
- Uninstall an application.
- Uninstall an application and license.

To manage a ONE software application on a ONE zl Module:

1. Start the ONE zl Module management wizard in one of the following ways:
 - Select Tools > ONE zl Module Management Wizard.
 - Click the ONE zl Modules folder under an Agent group in the navigation tree. In the ONE zl Modules tab, select a module and click the ONE button or right-click the module and select ONE zl Module Management Wizard.
2. In the Welcome window, click **Next**.
3. Enter information about the switch in which the ONE zl Module is installed and the Agent that manages the module in the ONE zl Module Chassis Information window.

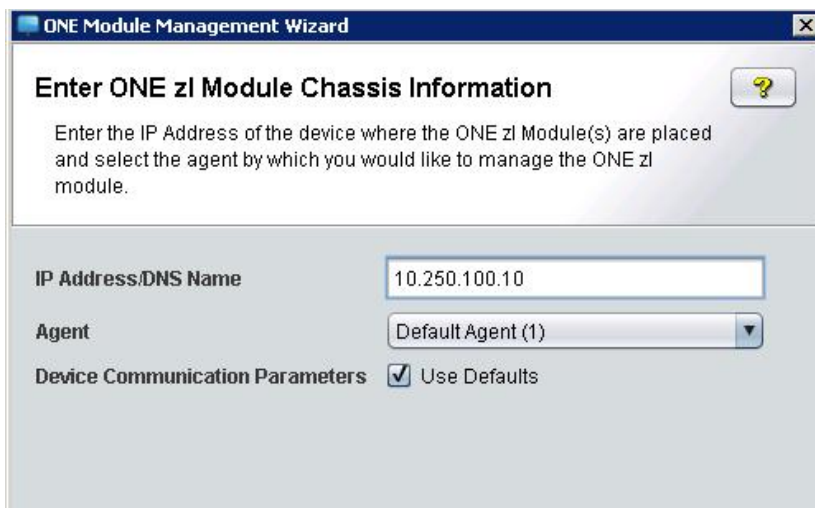


Figure 8-2. ONE zl Module Chassis Information

- a. Enter the IP address or DNS name of the switch in which the ONE zl Module is installed. (If you opened the wizard by selecting a module from the ONE zl Modules tab, this field is greyed out and the switch IP address is automatically entered.)
- b. Select the Agent that manages the module from the drop-down list. (If you opened the wizard by selecting a module from the ONE zl Modules tab, this field is greyed out and the agent is automatically entered.)
- c. To communicate with the switch using the SNMP and CLI communication parameters configured in PCM, select the Use Defaults check box. See “Setting Communication Parameters in PCM” on page 7-24 for more information.

To configure different SNMP and CLI settings to communicate with the switch, uncheck the Use Defaults check box.

- d. Click **Next**.

If you unchecked the Use Defaults check box, follow Steps a and b below to configure new SNMP and CLI settings to communicate with the switch:

- a. Select the SNMP version to use and enter new SNMP communication parameters. Then click **Next**.

Ensure that the new SNMP configuration supports the SNMP settings used by the PCM Agent that manages the module. See “SNMP Settings” on page 3-41 for more information.

- b. Select the communication protocol (Telnet or SSH) to use and enter the necessary parameters. Then click **Next**.

Note that SSH1 does not support key authentication. You must first define an SSH2 key before PCM can communicate with a switch using SSH key authentication.

4. In the Connection Status window, verify that the SNMP and CLI settings establish communication with the switch in which the ONE zl Module is installed. Then click **Next**.

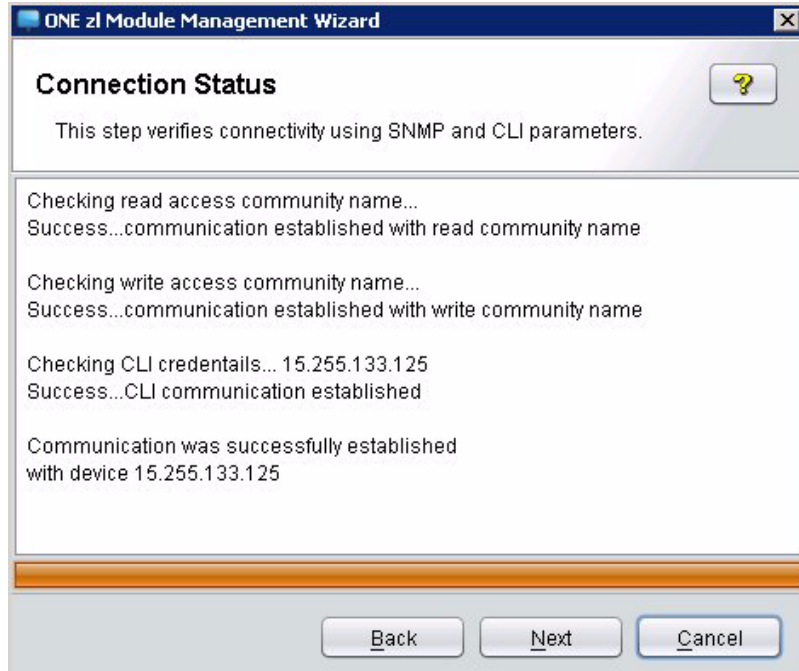


Figure 8-3. ONE zl Connection Status Window

If the IP address, SNMP community, or CLI credentials are not valid or not found, an error message that describes the failure is displayed. In case of a failed communication, click **Back** and re-enter the correct device information.

5. If you opened the wizard by selecting Tools > ONE zl Module Management Wizard and entered an IP address, the ONE zl Module Discovery window is displayed with a list of the ONE zl Modules discovered on the device.

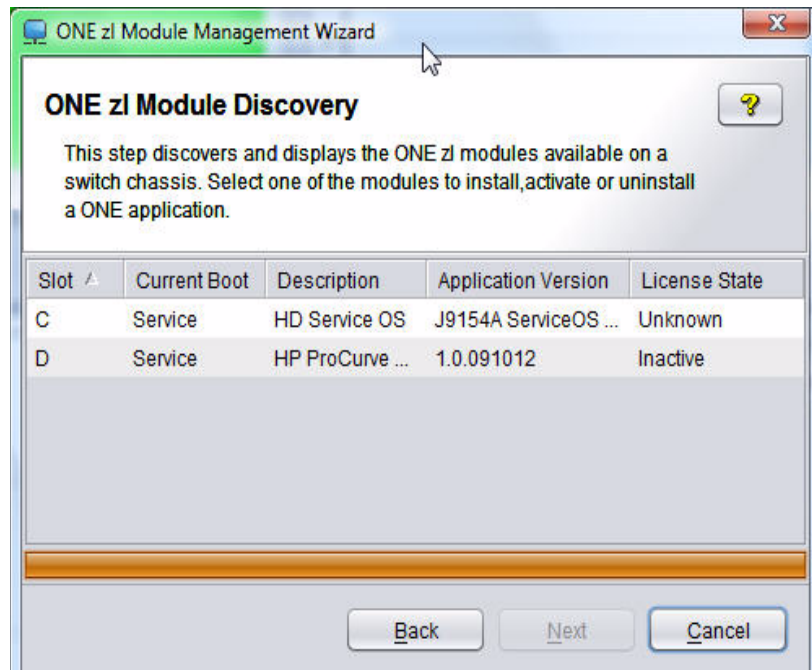


Figure 8-4. ONE zl Module Discovery

Select the module on which you want to install, activate, or uninstall a ONE application and click **Next**.

6. In the Configure ONE zl Module window, select the configuration task that you want to perform and click **Next**.

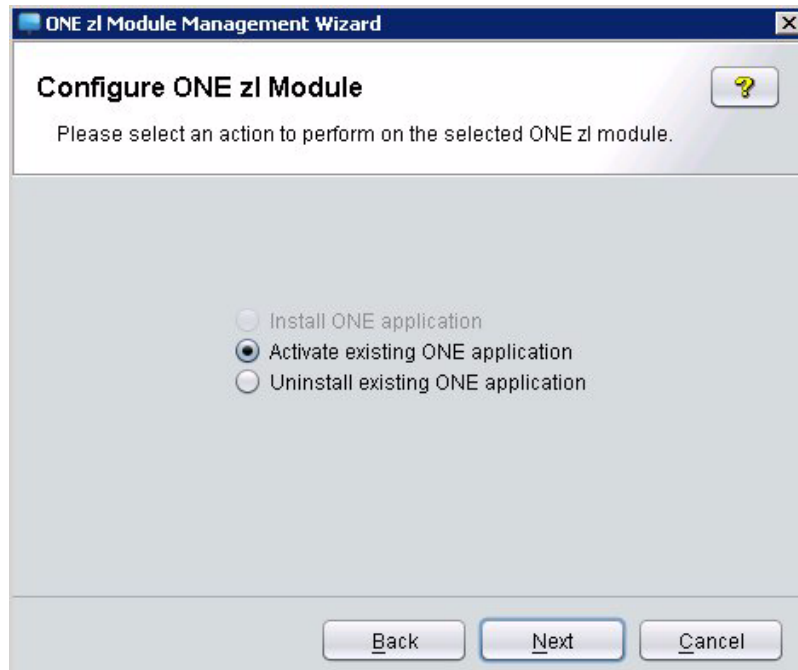


Figure 8-5. ONE zl Module Configuration

Follow the steps described in the following sections to install, activate the license, or uninstall a software application on a ONE zl Module:

- “Installing a ONE Application” on page 8-9
- “Activating the License for a ONE Application” on page 8-13
- “Uninstalling a ONE application” on page 8-16

Note that the Install ONE application option is grayed out (not available) if an application is already installed on the selected ONE zl Module.

The Activate existing ONE application option is grayed out if you have already activated the license.

Installing a ONE Application

To install an application on a ONE zl Module:

1. Ensure that the application software resides in one of the following locations:
 - On the ONE zl Module
 - In a directory on the PCM Server.
2. Follow the steps in “Managing a ONE Application” on page 8-4 to display the Configure ONE zl Module window.
3. Select Install ONE application and click **Next**.
4. In the Image Source for ONE zl Module window, enter the source location of the software to be installed.



Figure 8-6. ONE zl Module Image

- If the application software has already been copied to the ONE zl Module, select the ONE zl Module radio button. (No other action is required in this window.) Then click **Next**.
- If the application software resides on the PCM Server, select the PCM Server radio button and click the **Browse** button to enter the directory path where the software is stored. Then click **Next**.

Note: If you select PCM Server, ensure that an IP address has already been assigned to the ONE zl Module so that the PC where the managing PCM Agent resides can communicate with the ONE zl Module. By default, no IP address is configured when a ONE zl Module is installed in a switch chassis.

5. Do one of the following:
 - If you selected to install an application stored on the ONE zl Module, select one from the list of discovered images and click **Next**.

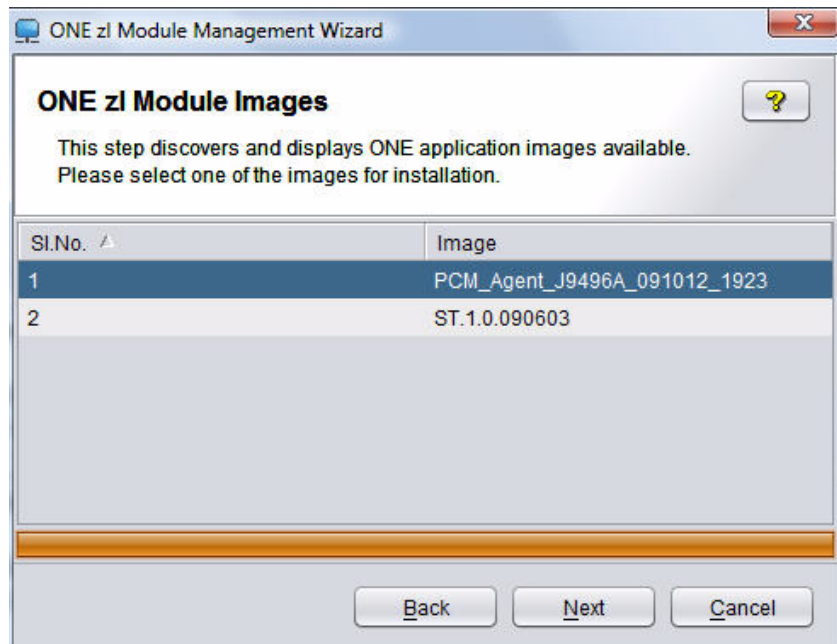


Figure 8-7. ONE zl Module Images

- If you selected to install an application image stored on the PCM Server, PCM discovers the IP address of the ONE zI Module and enters the address in the IP Address field. To change the IP address, simply type a new IP address in the field. Then click **Next**.

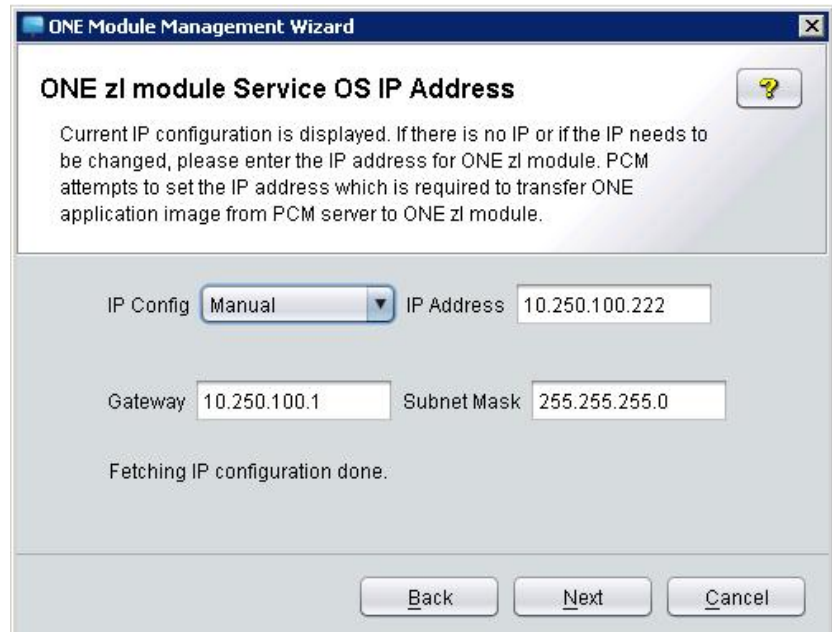


Figure 8-8. ONE zI Module: Service OS IP Address

The ONE zI Results window is displayed to show the status of the installation.

Note: Installing an Open Architecture application on a ONE zI Module may take several minutes.

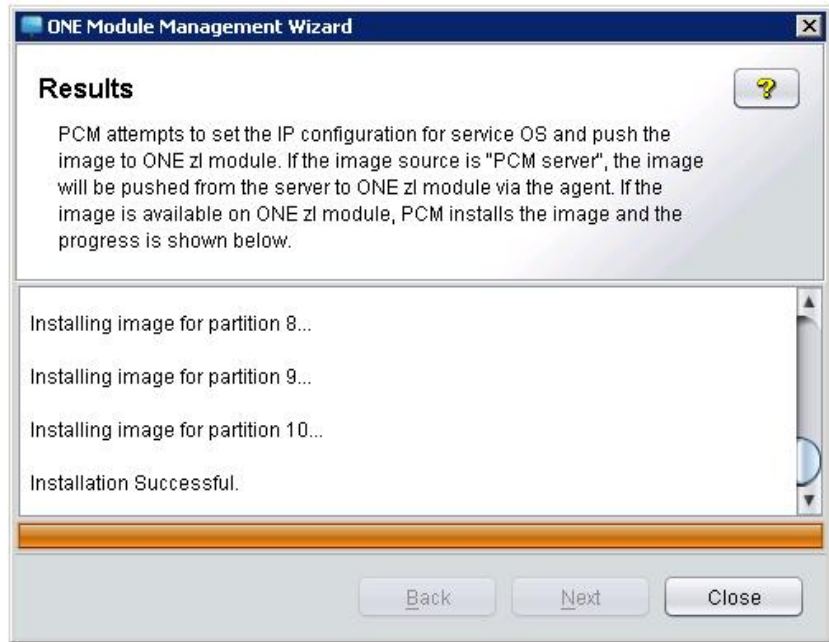


Figure 8-9. ONE zI Module: Management Wizard Results

6. Click **C**lose when the installation completes.

In the ONE zI Modules tab (figure 8-1), the module entry is updated with the application name and software version number.

Activating the License for a ONE Application

To activate (install) the license for the application installed on a ONE zl Module:

1. Ensure that PCM can communicate with My.ProCurve.com.

PCM needs external Web access to retrieve the latest file with an activation license key from the My.ProCurve.com web site. If necessary, configure the required proxy settings in the Network Settings Preferences window as described in “Network (Proxy) Settings” on page 12-58.

To automatically register the ProCurve switch on which the ONE zl Module is installed with My.ProCurve.com when it is discovered by PCM, follow the procedure in “Registering ProCurve Devices via PCM” on page 2-59.

2. Follow the steps in “Managing a ONE Application” on page 8-4 to display the Configure ONE zl Module window.
3. Select **Activate** existing ONE application and click **Next**.

Note that the **Activate** option is grayed out (not available) if a license key has already been activated for an installed application on the selected ONE zl Module.

4. Use the ONE zI Registration/Uninstall ID window to activate the license for the ONE zI Module service operating system.

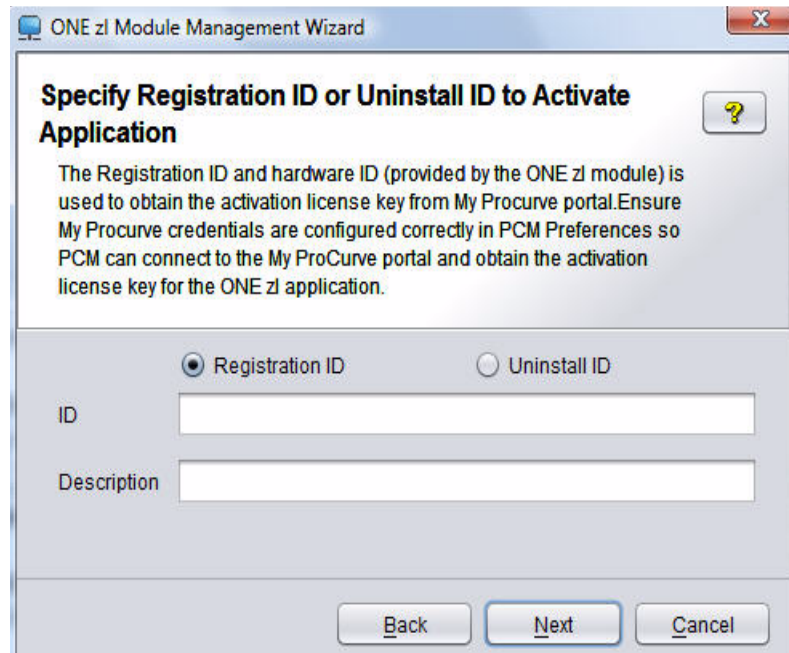


Figure 8-10. ONE zI Activation - Registration/Uninstall ID

Do one of the following:

- If you are activating the license for the first time, select **Registration ID**, enter the registration ID that you received when you purchased the ONE zI Module, enter an optional text description, and click **Next**.
- If you are re-installing a license that was previously uninstalled, select **Uninstall ID**, enter the uninstall ID that you received when you uninstalled the ONE zI Module service operating system, enter an optional text description, and click **Next**.

If you need to redisplay the uninstall ID, enter the show licenses uninstalled command at the services-module level of the ONE zI Module Service operating system.

The ONE zI Activate Results window displays the activation progress. Using the registration ID or uninstall ID that you entered in the ONE zI Activation window and the hardware ID obtained from the device, PCM contacts the My ProCurve portal to get the license key.

The license key activates an application installed on the ONE zI Module and boots the ONE zI Module from the application.

5. In the ONE zI License window, read through the legal notice and license agreement. To accept the agreement, select the I accept all of the above terms check box and click **Next**.

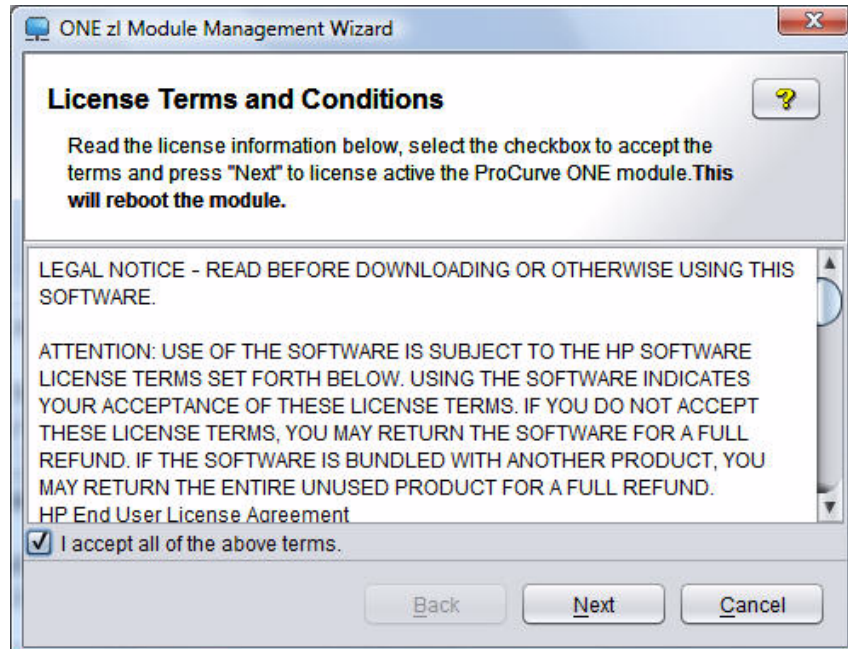


Figure 8-11. ONE zI Activation - License Terms

Uninstalling a ONE application

To uninstall a ONE application and (optionally) its license key:

1. Ensure that the application to be uninstalled is running on a ONE zl Module.

To display the current status of all ONE applications installed on ONE zl Modules, click the ONE zl Modules folder in the navigation pane.

2. Follow the steps in “Managing a ONE Application” on page 8-4 to display the Configure ONE zl Module window.
3. Select Uninstall existing ONE application and click **Next**.

Note that this option is available only if an application is installed on the selected ONE zl module.

4. Use the ONE zl Uninstall window to uninstall a ONE application and (optionally) its license key.

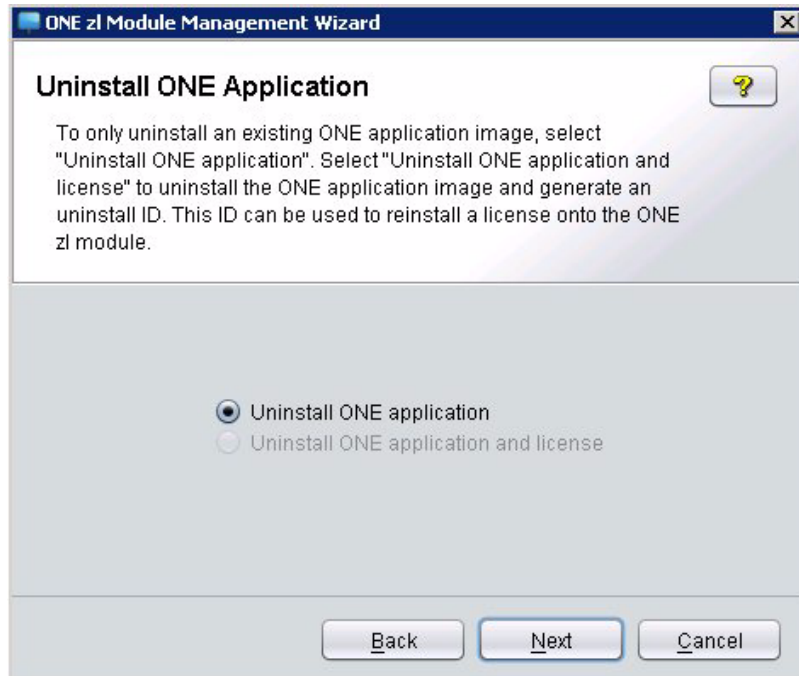


Figure 8-12. ONE zl Uninstall

Do one of the following:

- To uninstall a ONE zl Module application and its license key, select Uninstall ONE application and license and click **Next**. (This option is available only if an application license has been installed.)
- To uninstall only an unlicensed ONE zl Module application, select Uninstall ONE application and click **Next**. (This option is available only if an application is unlicensed.)

The ONE zl Uninstall Results window is displayed to show the uninstall progress. If the module is operating in Product mode, PCM boots the module into Service mode and then uninstalls the application.

If you also uninstalled the license, the Uninstall ID is displayed and the PCM database is updated.

Important

Be sure you record the Uninstall ID when it is displayed. You will need the uninstall ID to reinstall the license.

If you misplace the uninstall ID, you can redisplay it in either of the following ways:

- Enter the `show licenses uninstalled` command at the services-module level of the ONE zl Module Service operating system.
 - As shown in figure 8-1, click the ONE zl Modules folder under an Agent group in the PCM navigation tree. Then click the module listed in the ONE zl Modules tab. Scroll through the configuration history in the bottom pane of the tab to find the uninstall ID.
-

Troubleshooting ONE zl Module Configuration

When you use the ONE zl Module Management Wizard to install, activate, and uninstall ONE software applications on a ONE zl Module, you can:

- Monitor the status of an ongoing operation.
- Check the status of completed operations.

To monitor the configuration of a ONE zl Module:



1. Click the Configuration Management Status button in the global toolbar.
2. Click the ONE Configuration Status tab.

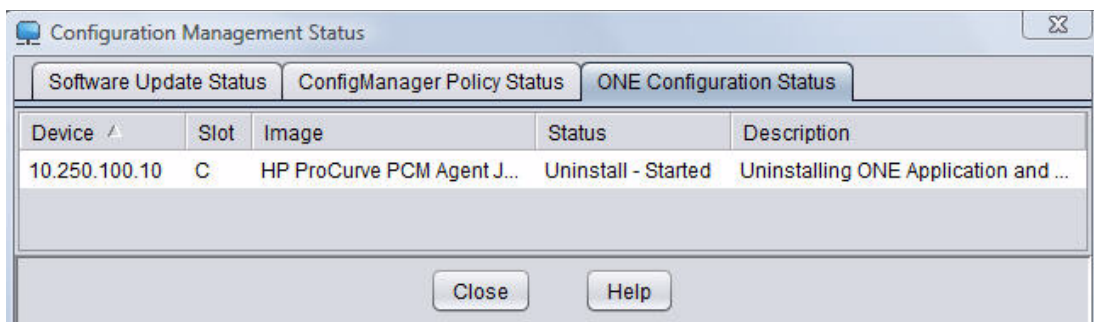


Figure 8-13. ONE Configuration Status Tab

The ONE Configuration Status tab displays the following information about an ongoing configuration operation:

Device	IP address of the switch in which the ONE zl Module is installed
Slot	Switch slot in which the ONE zl Module is installed
Image	Software application that was installed, activated, or uninstalled on the ONE zl Module.
Status	Type of configuration task performed and whether it completed successfully
Description	Text description of the configuration task and its completion status

The configuration entry is removed once the operation is completed.

To view the status of completed configurations on a ONE zl Module:

1. Click the ONE zl Modules folder under an Agent group in the PCM navigation tree.
2. Click the module entry in the ONE zl Modules tab (see figure 8-1).

The history of configuration operations on the module is displayed at the bottom of the tab.

Discovering Media Endpoints

Displaying and Reporting MED Devices	9-2
Displaying MED Devices: Agent-Group View	9-2
Displaying MED Devices: Switch View	9-4
Displaying Details about a MED Device	9-7
Importing MED Information	9-8
Displaying MED Information	9-10
Creating a MED Device Report	9-11

Displaying and Reporting MED Devices

PCM supports the discovery and reporting of Media Endpoint Devices (MEDs) in your network. PCM discovers MED devices using the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) protocol that runs between edge switches and LLDP-MED-enabled media endpoints, such as Avaya, Cisco, Nortel, and Mitel Voice over IP (VoIP) phones.

PCM provides different views and detailed information on discovered MED devices, such as an IP phone inventory with Power over Ethernet (PoE) and QoS priority information.

PCM uses SNMP and CLI interfaces to retrieve LLDP-MED MIB data from HP ProCurve ProVision switches. The LLDP-MED data is used to display information on media endpoints (such as IP phones) in windows, maps, and reports in PCM.

Note

PCM does not manage MED devices directly; PCM retrieves and displays MED information from switches, which are connected to host devices or directly to MED devices, such as IP phones.

The following HP ProCurve ProVision ASIC-based switches support the LLDP-MED protocol and MED discovery:

2520 Series Switch	3500yl Series Switch	6600 Series Switch
2600 Series Switch	4200 Series Switch	8206zl Series Switch
2600 -PWR Series Switch	5400zl Series Switch	8212zl Series Switch
2900 Series Switch	6200 Series Switch	

Displaying MED Devices: Agent-Group View

To view a listing of all the IP phones and other MED devices discovered by an Agent group:

1. In the navigation tree, click the Agent Groups folder to open it.
2. Click an Agent Group folder.
3. Click the Media End Points folder in the Agent group.

Model Name	IP Address	MAC Address	Manufa...	SW Revisi...	Connected IP	C...	Device
MITEL 5330 DM	172.16.135.232	08:00:0f:41:f...	Mitel Corpor...	Main 01.04....	172.16.100.20	A4	End Po
MITEL 5324 IP	172.16.103.152	08:00:0f:40:f...	Mitel Corpor...	Main 02.00....	172.16.103.11	3	End Po
CP-7975G	10.250.100.22	04:fe:7f:69:4...	Cisco Syste...	SCCP75.8-...	172.16.100.20	A2	End Po
9620			Avaya	ha96xxua3_...	172.16.103.11	5	Not Def
	172.16.135.253	00:24:b5:f6:...			172.16.135.23	A2	End Po

Figure 9-1. MED Device Discovery: Agent-Group View

In the Media Endpoints tab, information on all MED devices discovered by the Agent group is displayed, including the IP address of each MED and the host device to which the MED is connected.

A MED device may belong to the following device classes:

- Class I: Does not support IP media or act as an end-user communication appliance (e.g., IP Communication Controllers)
- Class II: Has IP media capabilities but may or may not be associated with a specific end user (e.g., Voice/Media Gateways or Conference Bridges)
- Class III: Acts as an end-user communication appliance supporting IP media (e.g., IP Phones or PC-based soft phones)

The Custom Attribute columns (not shown in figure 9-1) display data on the second and third attributes from an imported data file. If no LLDP-MED information has been imported, the columns are blank. See “LLDP-MED Import MEDs” on page 9-9 for more information.

Use the Agent Group view of MED devices in the Media End Points tab to search or filter the list for selected devices.

- To filter the display to show only a selected group of devices, click the Filtering arrow, select the check box next to one or more filtering criteria (IP address, Manufacturer, and so on), enter specific parameters in any of the filtering fields, and click **Apply**.

- To save current filtering settings in a file that you can later retrieve and apply, click **Save** and enter a file name.
- To revert back to the previously saved settings, click **Revert**.
- To load previously saved settings, click **Load** and enter a file name.
- To sort the list of MED devices, click on any of the column headings (Model Name, IP address, etc).
- To print a report of only the MED devices listed in the currently displayed Media Endpoints tab, click the **Print** button.

You can also generate a report on discovered MED devices by following the steps in “Create a Report: MED Device Inventory” on page 9-11.

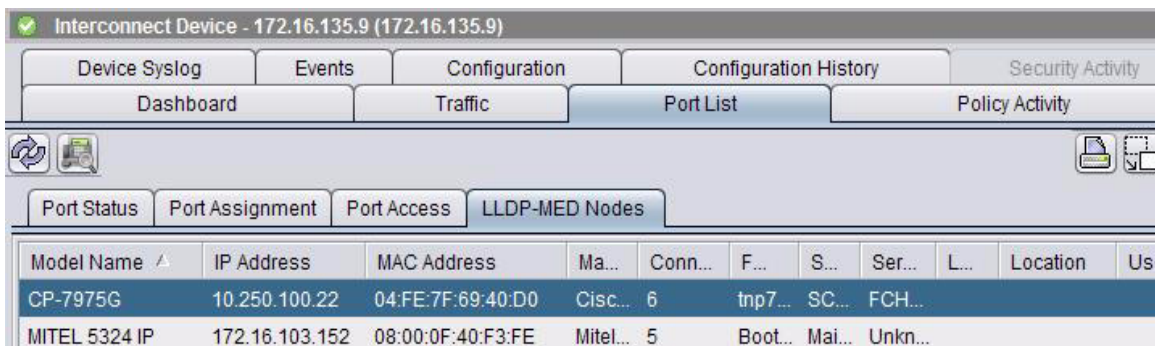
Displaying MED Devices: Switch View

You can display the MED devices discovered by a switch through a tab listing or a graphical map of host devices with connected MEDs.

Tab Listing

To display a list of MED devices that are discovered by a switch:

1. In the navigation tree, open the Devices folder under an Agent group, click a device model, and click a switch name or IP address.
2. In the Interconnect Device window, click the Port List tab and then click the LLDP-MED Nodes subtab. A list of the MED devices discovered by the selected switch is displayed.



Model Name	IP Address	MAC Address	Ma...	Conn...	F...	S...	Ser...	L...	Location	Us
CP-7975G	10.250.100.22	04:FE:7F:69:40:D0	Cisc...	6	tnp7...	SC...	FCH...			
MITEL 5324 IP	172.16.103.152	08:00:0F:40:F3:FE	Mitel...	5	Boot...	Mai...	Unkn...			

Figure 9-2. MED Device Discovery: Switch-level View



Click the **Refresh** button in the toolbar to perform a manual rediscovery of MED devices. The list in the LLDP-MED Nodes tab is refreshed with newly discovered MEDs and with changes in the attributes of existing MEDs.



To display detailed information about an individual MED device, select a device in the LLDP-MED Nodes subtab and click the **MED Device Details** button. See “Displaying Details about a MED Device” on page 9-7 for more information.

Graphical Map

To display a graphical view of the MED devices discovered by a switch:

1. In the navigation tree, open the Devices folder under an Agent group, click a device model, and click a switch name or IP address.
2. In the Interconnect Device window, click the Dashboard tab and then click the LLDP-MED and End Host Map button.
3. From the LLDP-MED and End Host Map view, you can display specific information about MED and end host devices by selecting any of the check boxes under **Annotations** or double-clicking a device in the map.



For example, figure 9-3 shows a sample view in which all annotations are selected to display information on:

- Discovery protocol
- Product name
- Properties
- Port number
- Location
- User name

The following IP addresses and port numbers identify the MED devices and end hosts connected to the switch at 172.16.135.1:

- LLDP-MED-enabled device (IP Phone) at 172.16.135.232
- PC connected to IP phone at 172.16.135.11
- End hosts (172.16.135.15, 172.16.135.22, and 00:24:a8:1d:65:f4)
- End host with authenticated user (172.16.36.1)
- Users on port A2

To display device-specific information, move the mouse pointer over a MED or end host device on the map. For example, moving the pointer over Users displays user names and the type of authentication (MAC address, web-based, 802.1x) used to access the device.

Discovering Media Endpoints Displaying and Reporting MED Devices



Note: You can display a map overview of the MED devices discovered by a switch (as shown in the lower right-hand corner of figure 9-3) by clicking the Map Overview button. The overview is useful when a large number of discovered MED devices and end hosts are connected to a switch and cannot be displayed in one window.

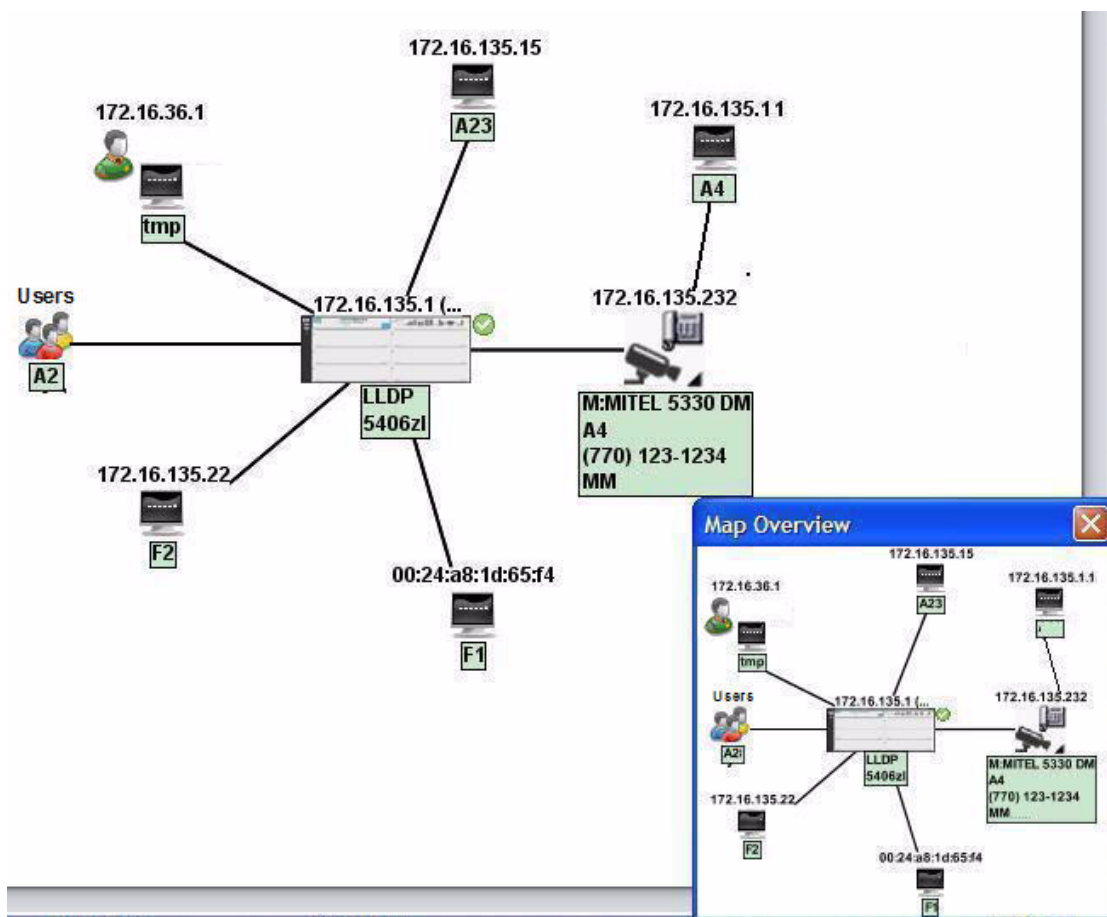


Figure 9-3. MED Device and End Host Discovery: Map View

Displaying Details about a MED Device

From a list of discovered MED devices, you can display detailed information about a selected device:

1. Do one of the following:



- From the list of discovered MED devices in an agent-group view (figure 9-1) or switch-level view (figure 9-2), select a device and click the **MED Device Details** button.
 - From an LLDP-MED and End Host map (figure 9-3), double-click a MED device on the map.
2. In the MED Device Details window, click a tab in the window to display detailed information on:
 - Power over Ethernet (PoE) requirements and device type
 - Location of the device
 - VLAN and QoS policy configuration for network traffic to and from the device
 - LLDP system information



Figure 9-4. MED Device Details

Importing MED Information

You can import additional data about discovered MED devices into the information displayed in PCM tab lists and maps. Additional MED data is imported from a file created by a PCM user.

Importing MED information allows you to view information about MED devices that PCM cannot discover directly. For example, by merging imported IP phone data with PCM-discovered data in a MED Device Inventory report, you can search for an IP phone by user name or phone number.

Prerequisite: Text File in CSV Format

To import new MED data, you must first create an ASCII text file with the data in a comma-separated value (CSV) format. Commas, semicolons, or tabs are supported as delimiters; for example:

```
<MED_mac-address>,<custom_field_1>,[custom_field_2]  
<MED_mac-address>;<custom_field_1>[custom_field_2]  
<MED_mac-address> <custom_field_1> [custom_field_2]
```

Where:

<MED_mac-address> is the MAC address of the MED device.

<custom_field_1> is an undiscovered device attribute.

<custom_field_2> is an optional, second undiscovered device attribute.

For example, to import the user names and locations of IP phones into PCM MED displays, you could start with a data file from your PBX and create a text file in CSV format in which rows of data are listed in the format:

```
<ip_phone_mac-address>,<user_name>,<phone_number>
```

After you import the CSV file, PCM automatically updates the Custom Attribute 1 and 2 fields in MED displays in PCM windows and reports, such as the rightmost columns in figure 9-8. The new headings and IP phone-specific information (user names and phone numbers) are now displayed.

Importing Additional MED Information

To import a text file in CSV format that contains additional information on discovered MED devices:

1. Create a CSV file that you can access from a PCM Client using data about MED devices. You must enter data in the CSV file in the formats described in “Prerequisite: Text File in CSV Format” on page 9-8.

Note: Lines that contain less than two fields or more than three fields are ignored by the Import MEDs Info Wizard.

2. Open the Import MED Info wizard from the Tools menu by selecting Import > Import MED info.

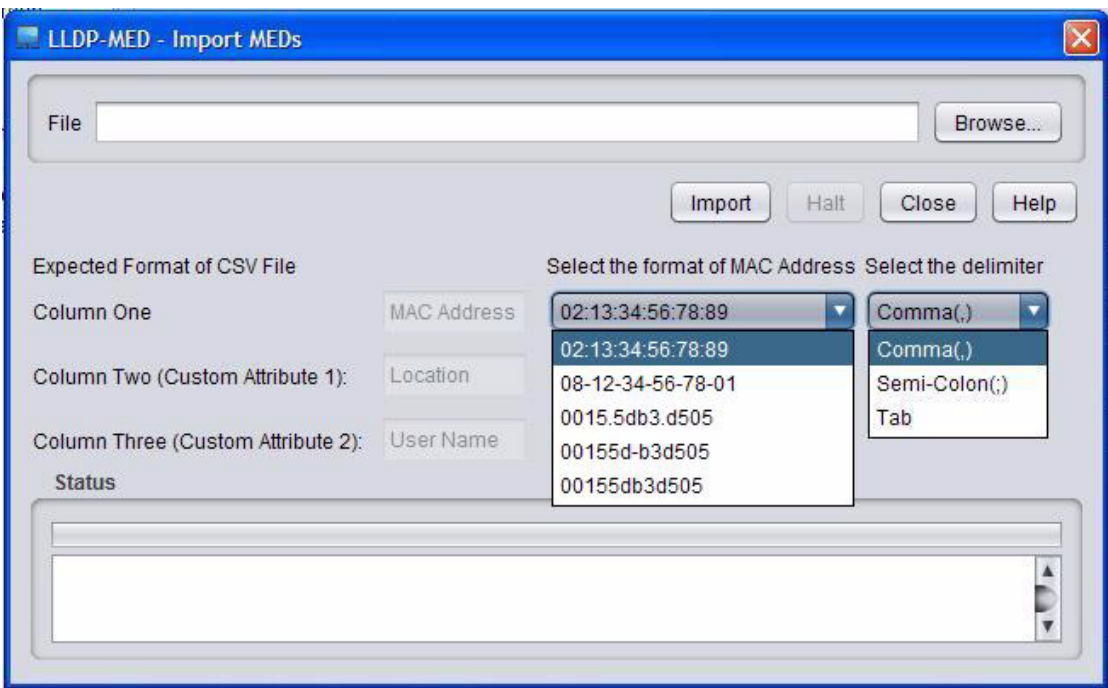


Figure 9-5. LLDP-MED Import MEDs

3. In the LLDP-MED Import MEDs window, enter the following information:
 - a. In the File field, use the **Browse** button to enter the CSV file to import.
 - b. Next to the Column One field, select the MAC address format used for MED devices, and the delimiter used to separate columns of data in the CSV file. Valid delimiters are: comma (,) semicolon (;), or tab.
 - c. The Column Two and Column Three fields are read-only and display the names used as headings in the report for the imported MED information in the second and third columns in the CSV file.

These names are configured in the Media Endpoint Preferences window (see “Displaying MED Information” on page 9-10).

The default names (Custom Attribute 1 and Custom Attribute 2) are shown in parentheses.

- d. Click **Import** to import the contents of the CSV file.
- e. Monitor the import progress in the Status pane and ensure that the file is imported successfully.

After the CSV file is imported and processed, a summary report of the operation is displayed in the Status pane. Imported information on MED devices automatically updates PCM windows and reports.

- f. Click **Close** to close the window.

Displaying MED Information

You can customize the way in which the MED information is displayed in PCM windows and reports. For example, you can specify the number of rows of MED data to be displayed on each page of the Media Endpoints tab (figure 9-1), and the heading used to describe each column of imported data.

To configure your preferences for the display of MED information:

1. From the Tools menu, select Preferences > Media End Points to display the Media End Points Preferences window.

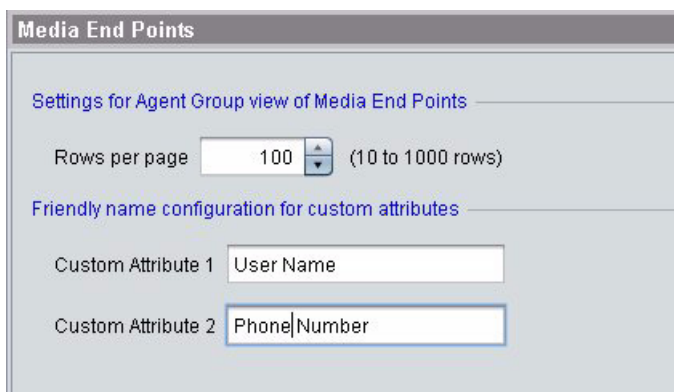


Figure 9-6. Media End Points: Preferences

2. Enter the following information:
 - a. In the Rows per page field, enter the maximum number of rows (10-1000) to be displayed on each page. Limiting the number of rows per page reduces the time required to display a page and improves readability.
 - b. In the Custom Attribute 1 field, type the user-friendly name you want to use to describe the imported data in column 2 of the CSV file.
For example, typing `User Name` will display "User Name" in PCM displays and reports of MED information.
 - c. In the Custom Attribute 2 field, type the user-friendly name you want to use to describe the imported data in column 3 of the CSV file. If the CSV file does not contain a second custom field, this name is ignored.

- d. Click **OK** to save your changes and close the window; click **Apply** to save your changes without closing the window.

The headings in the displays of MED information in PCM windows and reports are automatically updated with the changes.

Creating a MED Device Report

The MED Device Inventory Report lists each MED device discovered in the selected Agent group and provides detailed information about each device. This report is useful when determining the topology, software, and power requirements of your MED devices.

To generate a MED Device Inventory Report:

1. From the Reports menu, select Asset Management > MED Device Inventory.
2. In the Create a Report window, select the group of MED devices to be included in the report and click **Finish**.

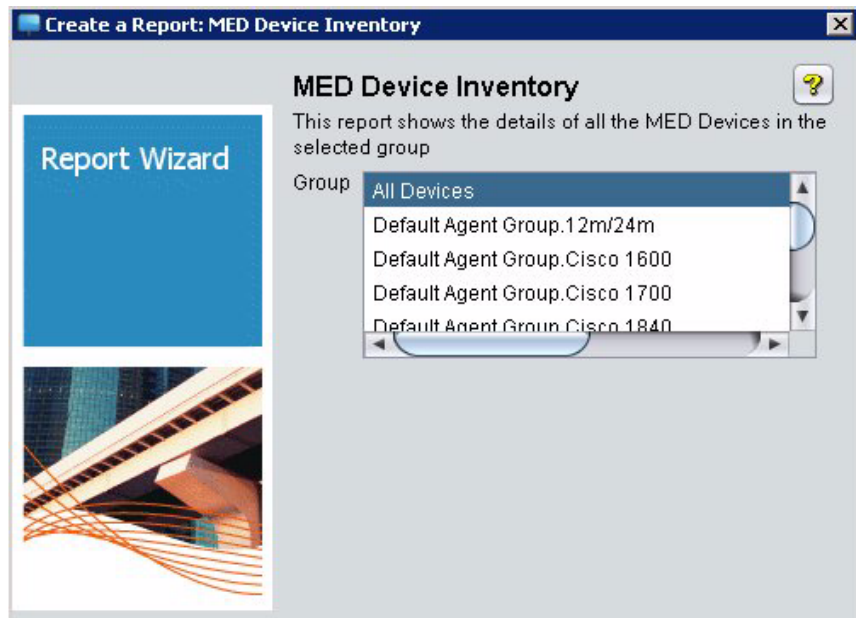


Figure 9-7. Create a Report: MED Device Inventory

3. The MED Device Inventory Report is displayed with information about each LLDP-MED device in the selected group.

LLDP MED Devices									
Model Name	IP Address	Connected Device (Port)	Manufacturer	FW Revision	VLAN ID	802.1p Priority	PoE Power Req (Watts)	Custom Attribute 1	Custom Attribute 2
CP-7975G	10.250.100.22	172.16.100.20(A2)	Cisco Systems, Inc.	tnp75.8-3-4-16BN01 bin	0	4	12.0		
MITEL 5330 DM	172.16.135.232	172.16.100.20(A4)	Mitel Corporation	Boot 01.04.02.10	3	3	4.7		

Figure 9-8. MED Devices Report

Note that the Custom Attribute 1 and 2 columns contain MED information imported from a CSV file on an end-host device (see “Importing MED Information” on page 9-8). These columns are blank if no additional MED information has been imported.

- To page through the report, click the > and < arrows at the top of the report window. Other toolbar icons let you display the first or last page, a specific page number or change the page size and magnification.
- To print the report, click the Print icon and complete the standard Windows print screen.
- To save the report to a file, click the Save icon. Then enter a filename and directory path, and click **Save**. Be sure to include the appropriate file extension in the filename; for example, .htm, .html, .pdf, .odt, .rtf, .xls, or .csv.

By default, the report is saved in the /My documents directory.

Device Access and Port Security Monitoring

Introduction	10-2
Viewing Device Access Information	10-3
Viewing Port Information	10-6
Port Status Subtab	10-7
Port Assignment Subtab	10-8
Port Access Subtab	10-9
Modifying Port Assignments	10-14
Modifying GVRP Port Properties	10-15
Using Port Monitoring (Mirroring)	10-16
To Assign the Monitoring Port	10-17
To Assign the Ports to be Monitored	10-18
To Assign the MAC Addresses to be Monitored	10-19
To View Mirror Port Status	10-21
To View Monitored MAC Status	10-22
To View Monitored Port Status	10-23
To Disable Mirroring	10-24
Using MAC Lockout	10-25
To View MAC Lockouts	10-25
To Lockout a MAC Address	10-26

Introduction

The Device Access and Port List tabs let you monitor device access and port settings for managed network devices, including port-based access and security configuration.

There are several different levels of access and security referred to in this chapter.

Device Access: This refers to the general access to a switch. The Device Access tab lets you easily verify if Console, Telnet or SSH Access security is configured on a switch. You can configure device access and authentication methods using the PCM Device Manager options (“Configuring SNMP and CLI Access” on page 7-14) or the switch CLI, as described in the *Access and Security Guide* for your switch.

Port Access: Refers to the use of port-based access control. For ProCurve switches that support port-based access control, you can use the switch CLI to configure individual ports for authentication of clients trying to access the network across that port.

Port Security: Refers to the configuration of MAC addresses allowed to access the network through a given port on the switch. This includes configuring the number of authorized MAC addresses allowed on the port, as well as how the port acquires authorized addresses. When a connect attempt is received from an unauthorized MAC address, an SNMP trap is sent.

The level of access and security configured on the device generally reflects its operation within the network. Devices being used to route network traffic between switches, subnets, and VLANs need to provide higher throughput. These infrastructure devices may use only minimal Device Access controls, as there is less risk of unauthorized traffic across infrastructure ports. Devices at the network edge, those that Clients can connect to directly to access the network, are more likely to use port-based access and security configuration to reduce unauthorized access to the network.

The Port List tab provides a high level view of the status of port configuration, Port (VLAN) Assignments, and Port Access and Security settings applied to individual ports on a switch. You can use the Port List tab features to monitor the port access and security settings, and more efficiently manage client access to the network.

Viewing Device Access Information

The Device Access tab display provides a summary view of the access control settings for individual devices, along with an indicator of the percentage of ports on the device that have Port Access and Port Security configured.

To display the Device Access tab, select the Devices node or device group in the navigation tree and then click the Device Access tab.

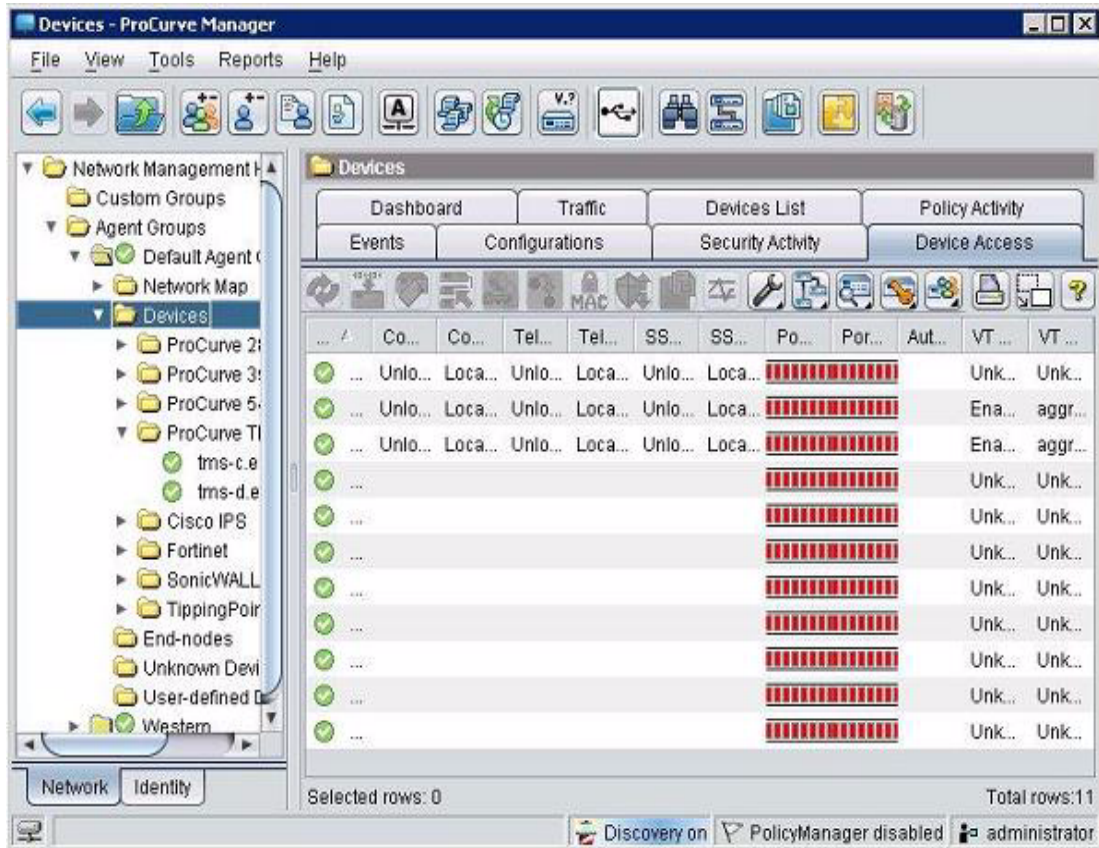


Figure 10-1. Device Access tab display

Device Access and Port Security Monitoring

Viewing Device Access Information

The Device Access tab provides the following information for each device in the group:

Device	The device identifier within PCM. (DNS name, IP Address, etc.)
Console Access	Either Locked meaning console access requires a login password, or Unlocked, no password required.
Console Authentication	Indicates the primary Authentication method used with the console login password. Possible values are: Local, RADIUS (ChapRadius or EapRadius), and TACACS.
Telnet Access	Either Locked meaning Telnet access to the device requires a login password, or Unlocked, no password required.
Telnet Authentication	Indicates the primary Authentication method used with the Telnet login password. Possible values are: Local, RADIUS (ChapRadius or EapRadius), and TACACS.
SSH Access	Either Locked meaning SSH access to the device requires a login password, or Unlocked, no password required.
SSH Authentication	Indicates the primary Authentication method used with the SSH login password. Possible values are: Local, Radius (ChapRadius or EapRadius), and TACACS.
Port Access	A bar graph (0-100 percent) indicating the percentage of ports that have port-access configuration requiring authentication of the client or device connecting to the port. Green indicates secured, red means no port-access security.
Port Security	A bar graph (0-100 percent) indicating the percentage of ports that have port security configuration that limits port connections based on MAC addresses. Green indicates port security is enabled, red means no port security is enabled.
Authentication Server(s)	The IP address of the RADIUS or TACACS server configured for authorization on the device.
VT Status	Indicates if Virus Throttle (connection rate filtering) is Enabled on the device. Other values are Disabled, and Not Supported.
VT Sensitivity	Indicates the Virus Throttle sensitivity setting when VT is enabled. See "Using Virus Throttle" on page 15-1 for details on using the Virus Throttle feature.

If the Access and Authentication columns in the display are blank it may be due to one of the following:

- Device attributes have not yet been discovered, and the information is not available yet.
- Passwords are set on the device, but corresponding communication parameters have not been set in PCM for that device. Use the Test Communication Parameters in device feature to verify, and if needed use the Communication Parameters in PCM Wizard to configure the CLI settings.
- The feature is not supported by PCM for the device (for example, wireless, 7000, 8100, 9400). See the PCM Supported Devices matrix for a complete list of supported features:

http://cdn.procurve.com/training/Manuals/PCM_Supported_Devices.pdf

The information for device access fields is based on data derived from the `show authentication` CLI command and, in case of certain device software (e.g., K.13.xx or greater), the information comes from HP MIBs. The Port Access information is derived using the `show port-access` CLI command and, in case of certain device software versions (e.g., K.13.xx or greater), the information comes from HP MIBs. Port Security is derived from the `hpSecure-PortTable` MIB.

Viewing Port Information

The Port List tab provides additional details related to port status, VLAN assignments, and access and security settings applied to individual ports on a switch.

The Port List tab is available for individual devices.

1. Select a device in the navigation tree or in the Devices List.
2. Click the Port List tab to display the tab contents.

Index	Port	Status	Speed Mbps	Virus Filter Action	Monitoring	Monitored By
1	1	■	100	Not Configured	Not Configured	
2	2	■	10	Not Configured	Not Configured	
4	4	■	10	Not Configured	Not Configured	
5	5	■	10	Not Configured	Not Configured	
6	6	■	10	Not Configured	Not Configured	
7	7	■	10	Not Configured	Not Configured	
8	8	■	10	Not Configured	Not Configured	
9	9	■	10	Not Configured	Not Configured	
10	10	■	10	Not Configured	Not Configured	

Selected rows: 0 Last update: 2/12/09 3:21:53 PM Total rows: 24

Discovery on Policy configuration actions disabled Administrator

Figure 10-2. Device Port List tab, Port Status subtab

Port Status Subtab

The default display within the Port List tab is the Port Status subtab.

The Port Status subtab provides basic information on the individual ports on the device including:

Index	Port index number
Port	Port identifier, which may be the same as the port Index, or the port name if friendly port names are used.
Status	Indicates current status of the port, either Green indicating the port is up; or grey, indicating the port is down.
Speed Mbps	Current status of the port's speed
Virus Filter Action	Indicates if Virus Throttle is in use on the port. See Chapter 15, "Using Virus Throttle" for more information.
Monitoring	Indicates if port is configured to monitor (mirror) another port. Lists the monitored port and device IP if actively monitoring. See "Using Port Monitoring (Mirroring)" on page 10-16 for details.
Monitored By	Indicates if the port is being monitored, gives the port name and device IP of the port set to monitor (mirror) this port. See "Using Port Monitoring (Mirroring)" on page 10-16 for details.

You can click the column headings to change the sort order in the table.

There are no right-click menu functions on the individual ports listed in the table; however, you can configure Port Mirroring (Monitor ports and Mirror ports) using the Port Monitoring tool menu. See "Using Port Monitoring (Mirroring)" on page 10-16 for details.

Port Assignment Subtab

To review the current port assignments for the device, click the Port Assignments subtab in the Port List tab.

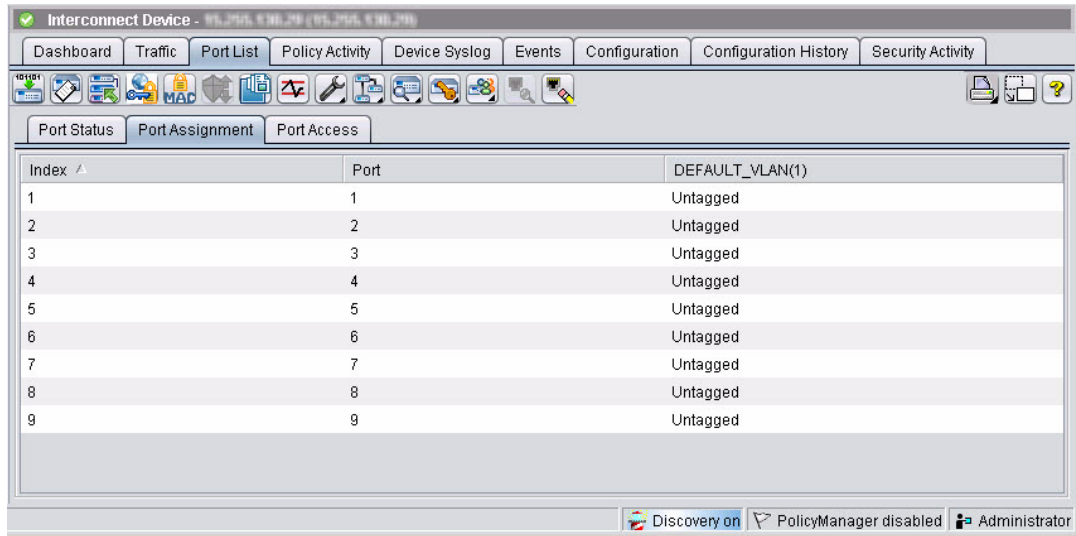


Figure 10-3. Port List Tab: Port Assignments subtab

The subtab lists each of the VLANs to which a port is assigned and the current configuration of the port VLAN support (tagged, untagged, etc.).


Note:

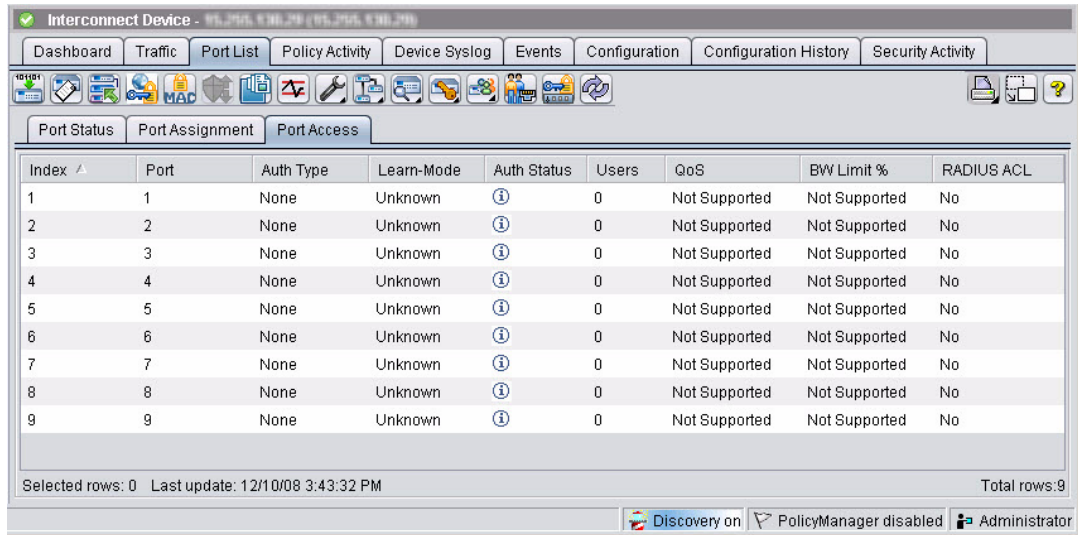
Because the Port Assignments subtab is device specific, it is not shown when a custom group is selected.










The Port Assignment subtab contains toolbar buttons used to modify port assignments as explained in “Modifying Port Assignments” on page 10-14, and GVRP properties as explained in “Modifying GVRP Port Properties” on page 10-15.

Port Access Subtab

The Port Access subtab provides details on security, authentication, and access controls configured on individual ports. Click the Port Access subtab to view the Port Access data.

To update the Port Access information display, click the Refresh  button in the toolbar.



Index ^	Port	Auth Type	Learn-Mode	Auth Status	Users	QoS	BW Limit %	RADIUS ACL
1	1	None	Unknown		0	Not Supported	Not Supported	No
2	2	None	Unknown		0	Not Supported	Not Supported	No
3	3	None	Unknown		0	Not Supported	Not Supported	No
4	4	None	Unknown		0	Not Supported	Not Supported	No
5	5	None	Unknown		0	Not Supported	Not Supported	No
6	6	None	Unknown		0	Not Supported	Not Supported	No
7	7	None	Unknown		0	Not Supported	Not Supported	No
8	8	None	Unknown		0	Not Supported	Not Supported	No
9	9	None	Unknown		0	Not Supported	Not Supported	No






Selected rows: 0 Last update: 12/10/08 3:43:32 PM Total rows: 9

Discovery on PolicyManager disabled Administrator

Figure 10-4. Port List Tab, Port Access subtab

The Port Access subtab provides information on the access and security settings for individual ports on the device including:

Index	Port index number
Port	Port identifier, which may be the same as the port Index, or the port name if friendly port names are used.
Auth Type	<p>Authentication method, if configured. Possible values are:</p> <ul style="list-style-type: none"> 802.1x - 802.1x Port Access Security used to authenticate devices. MAC Auth - MAC address used to authenticate devices Web Auth - User name and password must be entered to authenticate devices. None - No authentication is configured <p>Auth Type may display multiple authentications per port on devices that support that feature.</p>


Learn-Mode	<p>Learn-Mode setting used on secured ports; that is, how the port acquires authorized addresses. Possible values are:</p> <p>Continuous: Port learns addresses from inbound traffic from any connected device. This is the default setting.</p> <p>Limited-Continuous: A fixed limit (1 - 32) to the number of learned addresses allowed per port.</p> <p>Static: A fixed limit on the number of MAC addresses authorized for the port, with some or all of the authorized addresses specified. (If only some of the authorized addresses are specified, the port learns the remaining authorized addresses from the traffic it receives from connected devices.)</p> <p>Configured: All MAC addresses authorized for the port are specified. The port is not allowed to learn addresses from inbound traffic.</p> <p>Port Access: Allows only the MAC address of a device authenticated through the switch's 802.1X port-based access control.</p> <p>Unknown: The Learn-mode cannot be determined or is not set.</p>
Auth Status	<p>Indicator showing the current authentication status of the port: Possible values are:</p> <ul style="list-style-type: none"> Secured port, open and authenticated Secured port, authenticating Secured port, closed and no logged in user Secured port, closed Unsecured port, status unknown
Users	Number of current (authenticated) user logins on the port.
QoS	<p>Quality of Service level assigned for traffic across the port (if QoS control is supported). Values range from 1-7, where:</p> <ul style="list-style-type: none">6, 7 indicates high priority (get first priority)4, 5 indicates medium priority (get second priority)0, 3 indicates normal priority (get third priority)1, 2 indicates low priority (gets last priority) <p>An asterisk (*) indicates IDM override of switch QoS.</p>
BW Limit %	Bandwidth (Rate) limit configured on the port, if any. Values are given in percentage from 1 - 100%. An asterisk (*) indicates IDM override of switch bandwidth limits.
RADIUS ACL	Indicates if any RADIUS ACLs (IDM Access Control Lists) are applied to the port. Possible values are Yes or No.

Parameters displayed in the Port Access subtab are derived from the following CLI commands:

- show port-access [authenticator], [mac-based], [Web-based]
- show port-security
- show rate-limit
- show qos port-priority

User Sessions Details

To drill down to review additional details on the current user sessions on a port:

1. In the Port Access subtab, select a port that has current users who have been authenticated, indicated by a .
2. Click the User Sessions button in the toolbar to display the User Sessions window.

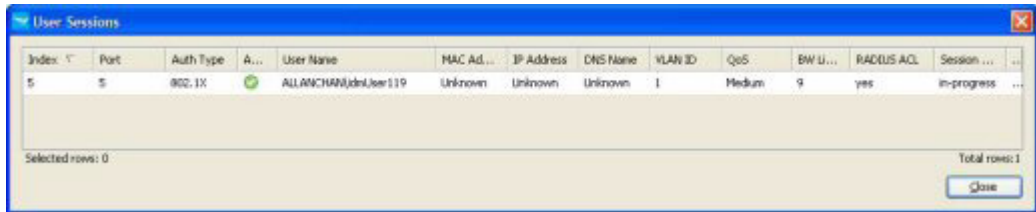








Figure 10-5. User Sessions Window

The User Sessions window provides the following information about users for the selected port:

Index	Index number associated with the port
Port	Port number (which may be the same as the port Index) or the port name if friendly port names are used
Auth Type	Authentication method used: 802.1x - 802.1x Port Access Security used to authenticate devices MAC Auth - MAC address used to authenticate devices Web Auth - User name and password must be entered to authenticate devices None - No authentication is configured
Auth State	Authentication icon showing current authentication status of port:  secured port, open and authenticated  secured port, authenticating  secured port, closed and no logged in user  secured port, closed, unknown  unsecured port, security issue  unsecured port, unknown session status
User Name	Number of authenticated users currently logged in through the port
MAC Address	MAC address of the computer where the user connected to the port
IP Address	IP address of the computer where the user connected to the port

Device Access and Port Security Monitoring
Viewing Port Information

DNS Name	DNS name of the computer where the user connected to the port
VLAN ID	VLAN being used. The displayed VLAN value is the effective VLAN applied to the user on this port, either the static VLAN configured on the switch or the VLAN override value from IDM.
QoS	Quality of Service level assigned to the port. Levels range from 1-7, with 1 being the lowest priority and 7 being the highest priority. The displayed QoS value is the effective QoS applied to the user on this port, either the static QoS configured on the switch or the QoS override value from IDM.
BW Limit %	Port bandwidth limit, shown as a percentage (1-100%). The displayed BW limit is the effective bandwidth limit enforced for the user on this port, either the static BW limit configured on the switch or the BW limit override value from IDM.
ACL	Whether RADIUS ACL (access control list) is applied to the port. Possible values are Yes or No.
Session Status	Current status of authentication (e.g., in progress, authenticated)
Session Time	Length of time user has been logged in

IDM is not required for this window. However, User Sessions information is available only for authenticated users.

ACL Details

The ACL Details window can be displayed when an ACL is used for the port. It identifies access rules and packet hits of the applied ACL.

To drill down to review additional details on the current ACLs configured on a port:

1. In the Port Access subtab, select a port that uses ACL.
2. Click the ACL details button in the toolbar, which displays the ACL Details window.

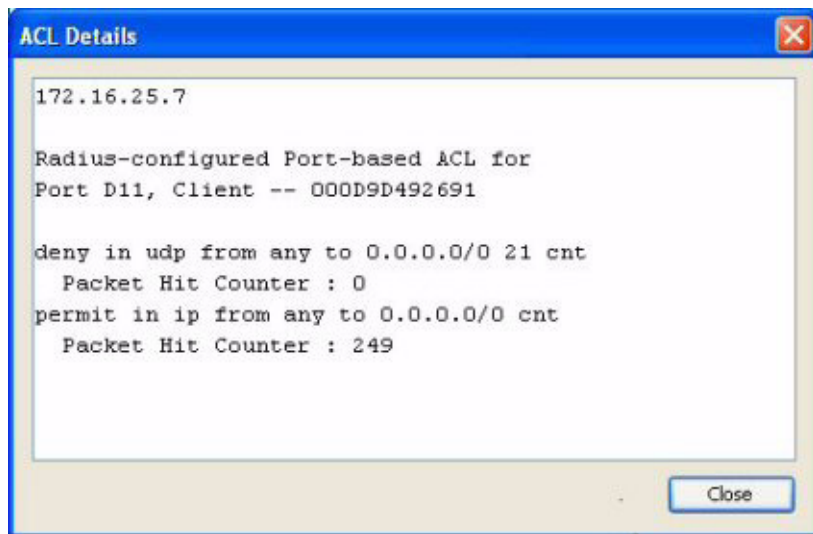


Figure 10-6. Port Access, ACL Details

Modifying Port Assignments



Click the Modify Port Assignments button in the toolbar of the Port Assignment subtab to change the VLAN port assignments. This launches the Modify Port Assignments window.

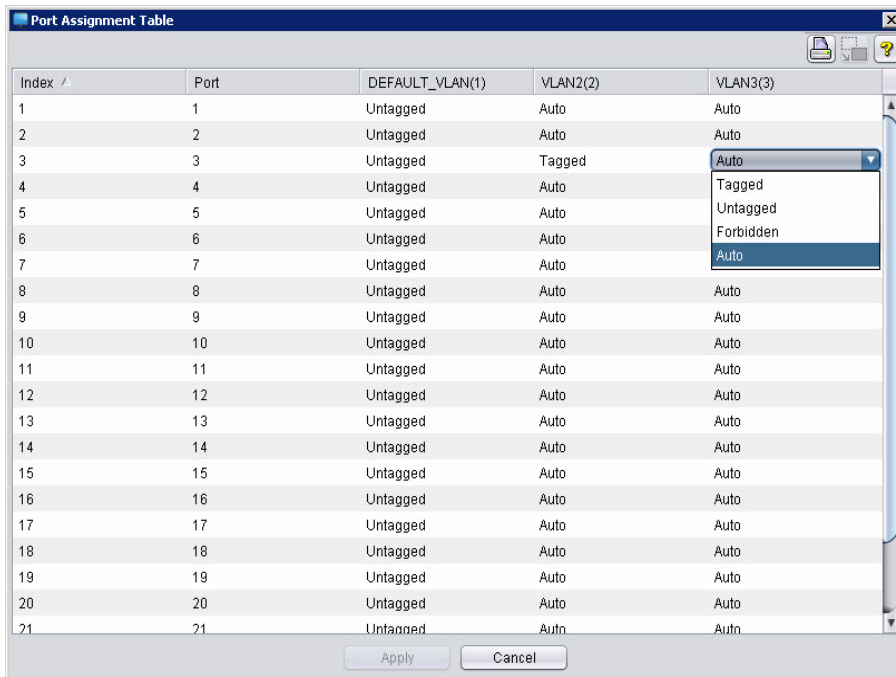


Figure 10-7. Modify Port Assignments window

To modify port assignments:

1. Click the VLAN table cell to be modified, which then displays a hidden drop-down menu you can use to select the Property you want to have for the port in that VLAN. The VLAN port options are:

Tagged	Port can be included in multiple VLANs.
--------	---

Untagged	Port can be included in only one untagged VLAN.
----------	---

Forbidden	Port cannot be included in this VLAN.
-----------	---------------------------------------

No	Port is not included in this VLAN.
----	------------------------------------

2. Change the port properties as needed, then click **Apply** to save the changes and close the window.

Modifying GVRP Port Properties

To modify VLAN support by individual port on a device that supports GVRP:



1. Click the Modify GVRP Port Properties button in the Port Assignment subtab toolbar.

Index	Port	GVRP Status	Ingress Filtering	Acceptable Frame Type
2	2	Learn	Enabled	All

Figure 10-8. Device Properties: Port Properties

2. Select the GVRP status for the port: Blocked, Learn, or Disabled.
3. Select whether the Ingress Filtering for the port is Enabled or Disabled.
4. Select the Acceptable Frame Type: All or Tagged.
5. Click **Apply** to update the Port Properties display, then click **OK** to close the dialog.

Using Port Monitoring (Mirroring)

Many ProCurve switches support the use of port monitoring (mirroring). You can designate monitoring of inbound and outbound traffic on:

- **Ports and static trunks:** Allows monitoring of individual ports, groups of contiguous ports, and static port trunks.
- **Meshed ports:** Allows traffic monitoring on all ports configured for meshing on the switch.
- **Static VLANs:** Allows traffic monitoring on one static VLAN.
- **MAC addresses:** Allows monitoring of MAC addresses.

The switch monitors network activity by copying all traffic inbound and outbound on the specified interfaces to the designated monitoring port, to which a network analyzer can be attached.

Note:

VLANs, a switch mesh, and port trunks cannot be used as a monitoring port.

The switch can monitor static LACP trunks, but not dynamic LACP trunks.

It is possible, when monitoring multiple interfaces in networks with high traffic levels, to copy more traffic to a monitor port than the link can support. In this case, some packets may not be copied to the monitor port.

If you use "remote mirroring" (with Network Immunity Manager), ProCurve recommends using jumbo frames on 1/10 GB ports. Otherwise, data may be lost if switches between the monitored port and remote mirror do not support jumbo frames.

Use the following configuration sequence to configure port monitoring using PCM:

1. Assign a monitoring (mirror) port.
2. Designate the port(s) to monitor.

To Assign the Monitoring Port

1. Select the device node in the navigation tree, or select the device in the group Devices List.
2. Click the Port List tab to display the Port Status subtab.
3. In the Port Status subtab, select the port you will use as the monitoring (mirror) port.
4. Select the Configure Mirror Port option from the toolbar pull-down menu. The Configure Mirror Port dialog displays, with the selected port ID.

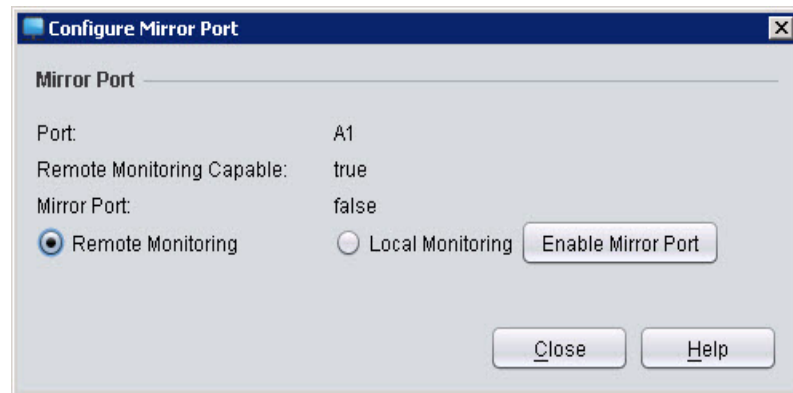


Figure 10-9. Configure Mirror Port dialog

5. Click the radio button to select Remote Monitoring or Local Monitoring.
 - Use remote monitoring to monitor activity of a port on another (remote) device.
 - Use local monitoring to monitor activity of another port in the same device.
6. Click the **Enable Mirror Port** button.

The MirrorPort field changes to true, and the button changes to **Disable Mirror Port**.

Click **Close** to save the mirror port setting, or click **Disable Mirror Port** to return the port to the default state.

In the Port Status subtab, the Monitoring column for the configured port is now blank.

To Assign the Ports to be Monitored

1. Select the device node in the navigation tree, or select the device in the group Devices List.
2. Click the Port List tab to display the Port Status subtab.
3. In the Port Status subtab, select the port you want to monitor. You can use shift+click, or ctrl+click to select multiple ports.
4. Select the Monitor Port option from the toolbar pull-down menu.



The Select Mirror Port window displays, listing the ports and devices configured as mirror (monitoring) ports.

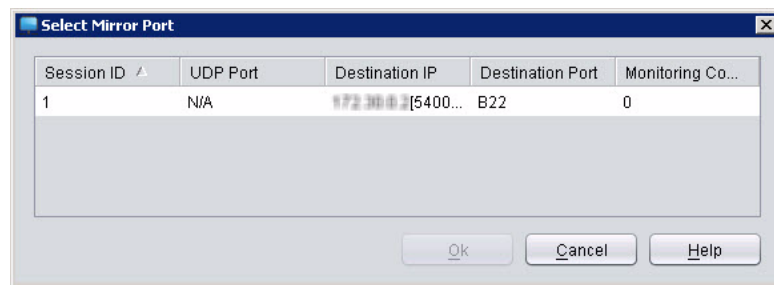


Figure 10-10. Select Mirror Port display

5. Click the port you want to use for monitoring, then click **OK**.

The Select Mirror Port window closes, and the mirror port information appears in the Monitored By column for the port being monitored.

To Assign the MAC Addresses to be Monitored

1. Select the device node in the navigation tree, or select the device in the group Devices List.
2. Click the Port List tab to display the Port Status subtab.
3. Select the Monitor MAC option from the toolbar pull-down menu, which opens the MAC Monitor Wizard.
4. Select the session you want to monitor the MAC address and click **Next**.

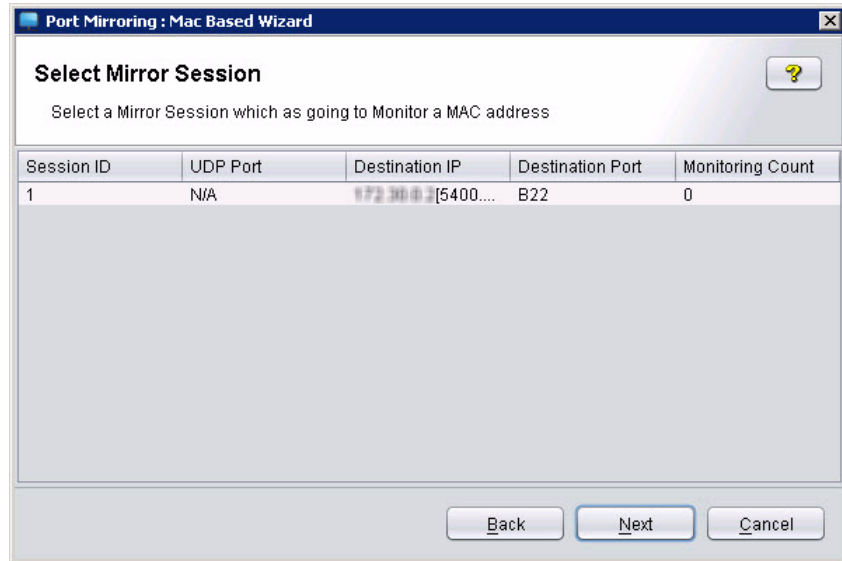


Figure 10-11. MAC Monitor Wizard, Select Mirror Session

5. In the Monitoring Sources window, click **Add** to add the MAC addresses to be monitored. Click **Remove** to remove a wrongly added MAC while adding a MAC.

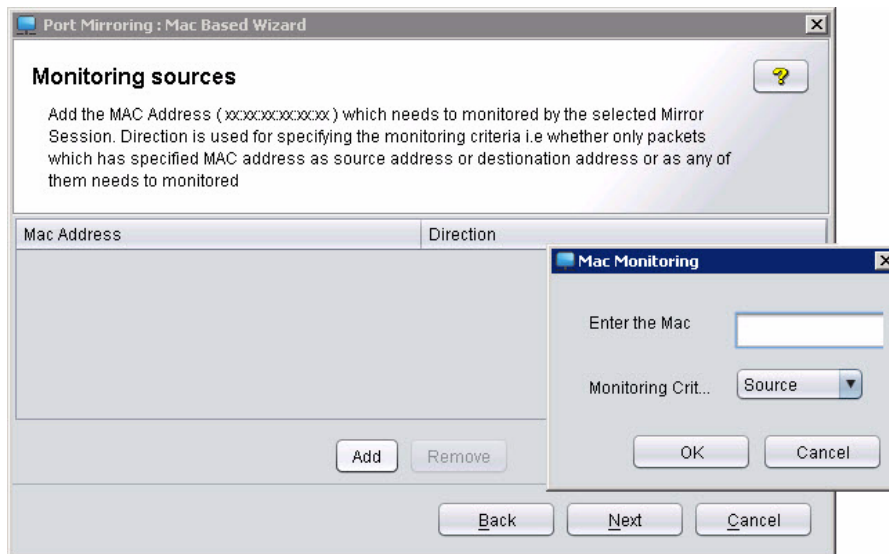


Figure 10-12. MAC Monitor Wizard, Add MAC Address

- a. In the Enter the MAC field, type the MAC address that you want to monitor. Type the MAC address as six groups of two hexadecimal digits, separated by colons (:).
 - b. Use the Monitoring Criteria drop-down list to select packets based on:
 - Source: MAC address is contained in the Source field of the packet
 - Destination: MAC address is contained in the Destination field of the packet
 - Both: MAC address is contained in either the Source or Destination fields of the packet
 - c. Click **OK** to save your entries and close the dialog.
 - d. Click **Next**.
6. When the Finish Step window of the MAC Monitor Wizard appears, confirm that the MAC mirroring operation completed successfully and click **Finish** to close the wizard.

To View Mirror Port Status

1. Select the device node in the navigation tree, or select the device in the group Devices List.
2. Click the Port List tab to display the Port Status subtab.
3. In the Port Status subtab, select the Monitoring port.
4. Select the View Mirror Port Status option from the toolbar pull-down menu.



The View Mirror Port Status window displays.

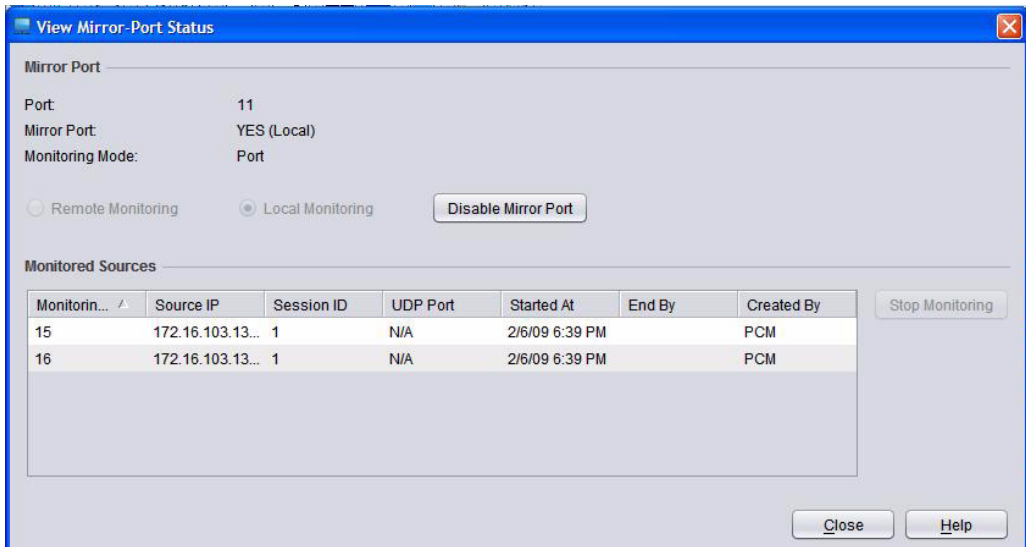


Figure 10-13. Mirror Port Status

The display lists the mirror port information along with the list of ports or MAC (with Device address) that are being monitored by this port.

To View Monitored MAC Status

1. Select the device node in the navigation tree or group Devices List.
2. Click the Port List tab to get to the Port Status subtab display.
3. In the Port Status subtab, select the Monitoring port.
4. Select the View Monitored Mac Status option from the toolbar pull-down menu, which displays the View Monitored Mac Status window.

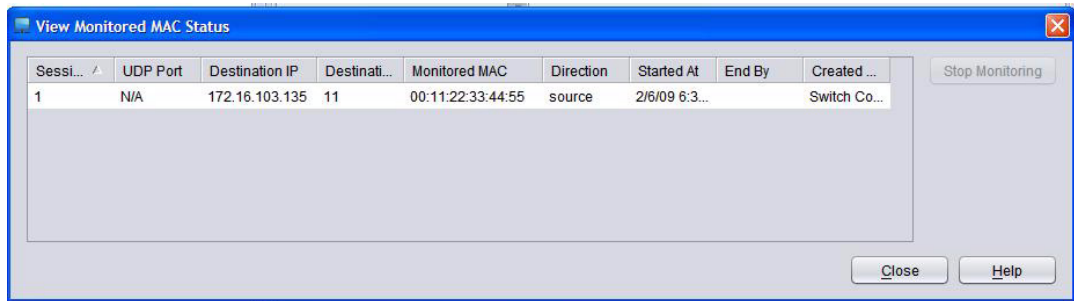


Figure 10-14. View Monitored Mac Status

The display lists the mirror port information along with the list of ports (with Device address) that are being monitored by this port.

5. To end monitoring, select a MAC address and click **Stop Monitoring**. When the confirmation prompt appears, click **Yes**.

To View Monitored Port Status

1. Select the device node in the navigation tree or in the group Devices List.
2. Click the Port List tab to get to the Port Status subtab display.
3. In the Port Status subtab, select the "Monitored By" port.
4. Select the View Monitored Port Status option from the toolbar pull-down menu.



The View Monitored-Port Status dialog displays.

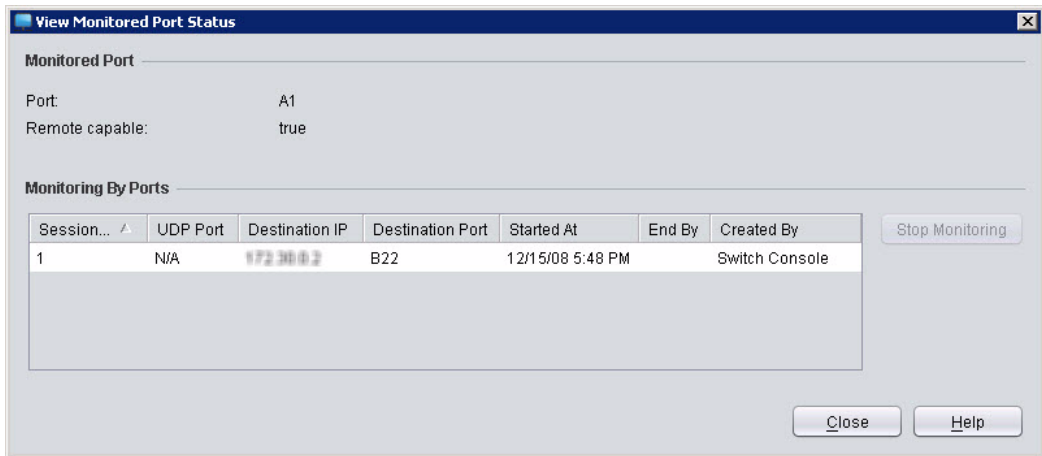


Figure 10-15. Monitored Port Status

The information on the monitoring (mirroring) port, and the monitoring start and end times is provided.

5. Select a port and click Stop Monitoring to end monitoring of the port. Click **Yes** in the confirmation pop-up.

The monitoring information is cleared from the View Monitored Port Status dialog. When you click **Ok**, the dialog closes, and the entry in the "Monitored By" column for the port is blank.

To Disable Mirroring

1. Select the device node in the navigation tree or in the group Devices List.
2. Click the Port List tab to get to the Port Status subtab display.
3. In the Port Status subtab, click to select the Monitoring port.
4. Select the View Mirror Port Status option from the toolbar pull-down menu.
5. To turn-off monitoring of one or more ports or MACs, select the monitoring source in the Monitoring Ports list, then click **Stop Monitoring**.



Click **Yes** in the confirmation pop-up dialog.

The port is removed from the Monitoring Ports list, and when you close the dialog, the mirror port entry in the Monitored By column for the affected port is removed.

6. To stop port monitoring completely, click **Disable Mirror Port**.

The Mirror Port status changes to false, and when you close the dialog the Monitoring entry for the disabled mirror port is removed, as are mirror port entries in the Monitored By column for the ports that were being monitored.

Using MAC Lockout

You can use the MAC Lockout feature to select ProCurve switches to block traffic from a specific MAC address on that switch. When used, all traffic to or from the specified MAC address is dropped.

To View MAC Lockouts

1. Navigate to the MAC Lockout window.
 - a. In the navigation tree, select the switch to be locked out.
 - b. Click the MAC Lockout button on the toolbar.

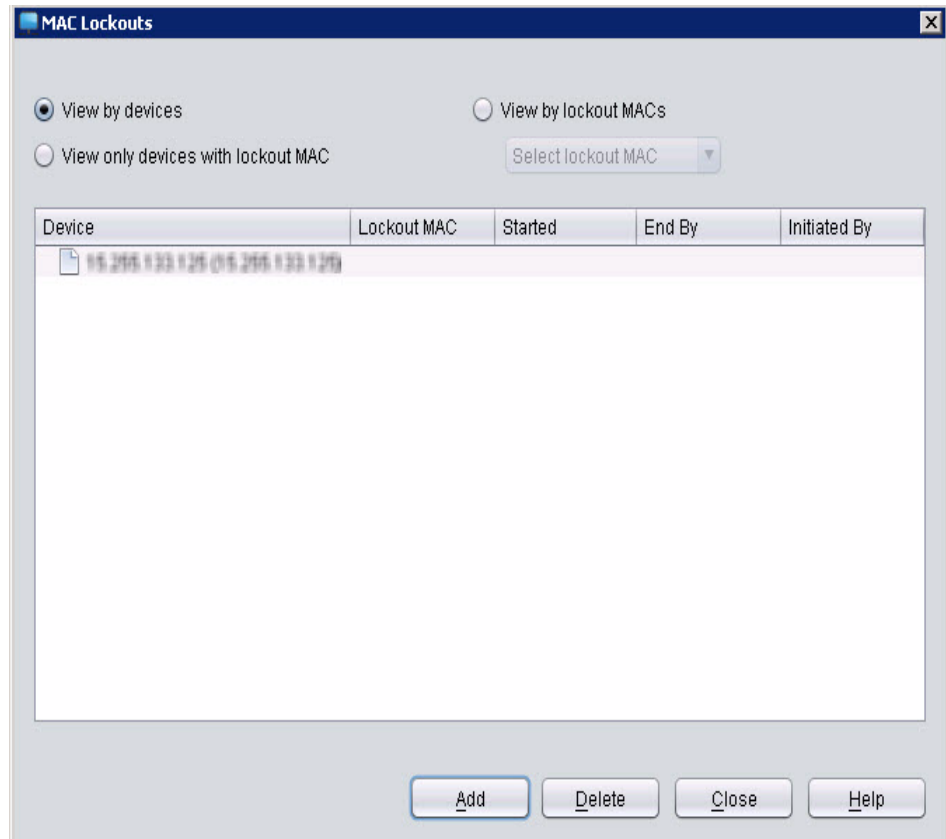


Figure 10-16. MAC Lockouts window

2. Select the view:
 - Select the View by devices radio button to view all discovered switches that support MAC Lockout regardless of their current MAC lockout configuration.
 - Select the View only devices with lockout MAC radio button to view all discovered devices that currently have MAC lockout configured and list them by their IP address.
 - Select the View by lockout MACS radio button to view all discovered devices that currently have MAC lockout configured and list them by their MAC address.

The Mac Lockouts list includes when a MAC lockout was initiated, and when it is scheduled to end (roll back).

To Lockout a MAC Address

1. Navigate to the MAC Lockout window.
 - a. In the navigation tree, select the switch to be locked out.
 - b. Click the MAC Lockout button on the toolbar.
2. Click **Add**. This launches the Add Lockout MAC dialog.



Figure 10-17. Add Lockout MAC dialog.

3. Type the MAC address of the device you want to lock out. Enter the MAC address as six sets of two-digit values separated by colons (e.g., xx:xx:xx:xx:xx:xx).
4. Click **OK** to lockout the specified MAC address and close the window, or Click **Cancel** to exit the window without saving your changes.

To remove a MAC lockout:

1. Navigate to the MAC Lockout window.
 - a. In the navigation tree, select the switch to be locked out.
 - b. Click the MAC Lockout button on the toolbar.
2. In the MAC Lockouts window, select the device from which MAC lockout should be removed.
3. Click **Delete**.
4. Click **OK** in the confirmation dialog to remove the lockout from the selected device and close the window.

Click **Cancel** to exit the window without saving your changes.



Monitoring Network Traffic

Introduction	11-2
How Traffic Monitoring Works	11-2
Reviewing Traffic Data	11-3
Top Traffic Overview	11-3
Using the Traffic Tab	11-6
Reviewing Port Top Talkers	11-11
Reviewing Per-Port Traffic Statistics	11-14
Reviewing Traffic Monitor Events	11-18
Configuring Traffic Monitor	11-19
Manual Configuration of Traffic Thresholds	11-20
Manual Configuration of Traffic Monitoring	11-22
Setting Traffic Monitor Preferences	11-25
Troubleshooting Traffic Monitor	11-28

Introduction

The Traffic Manager in PCM provides a traffic monitoring facility that delivers minute-by-minute views of the volume and even the content of traffic at specified points within your ProCurve network.

Traffic monitoring is set to run automatically, with the capability for simultaneously performing statistics polling and sFlow sampling. Traffic Manager uses sampling and statistics polling to monitor five key metrics that summarize network activity on the port: utilization and per-second rates for total frames, broadcast frames, multicast frames, and errors. The Top Traffic Overview pane in Dashboards and the Traffic tab displays the current, worst measurement in the entire network for each measured metric group.

How Traffic Monitoring Works

The statistics polling used by Traffic Manager consists of retrieving standard counters at a fixed, repeated interval (1 minute); the difference in counter values and period between retrievals is used to calculate a rate for each of the Traffic monitor metrics. For most ports these counters are extracted from the Interfaces Group of MIB II (RFC 2233), though for some older devices other MIBs are used. Polling statistics from a port allows PCM to report the volume of traffic on the port, but does not provide any information as to the content of the traffic seen on the port.

The traffic sampling collection utilizes a standard called sFlow (RFC 3176) in which frame headers are sampled randomly from each port on which traffic sampling is enabled, then bundled together with snapshots of the corresponding port counters and sent to PCM. The traffic "samples" are used to reconstruct the volume of traffic on the monitored port (using differences measured over time much like statistics polling) and the actual traffic content via statistical estimation.

Traffic Manager employs a default configuration for automatically selecting and configuring ports on which to monitor traffic. You can manually override the automatic statistics sampling to disable traffic monitoring on specific ports, or to have statistics and/or sampling always enabled on specific ports. You can also tune the threshold settings for each measured metric to suit your specific network requirements.

Reviewing Traffic Data

Traffic data can be found on Dashboards and the Traffic tab for devices and device groups.

Top Traffic Overview

When traffic monitoring is enabled, the Top Traffic Overview pane on Dashboards displays data for egress or transmitted (Tx) traffic, and ingress or received (Rx) traffic, for the metric groups that the data collector monitors:

- Utilization, in bytes per second, given as a percentage of total available.
- Frames per second,
- Broadcasts per second,
- Multicasts per second, and
- Errors per second.

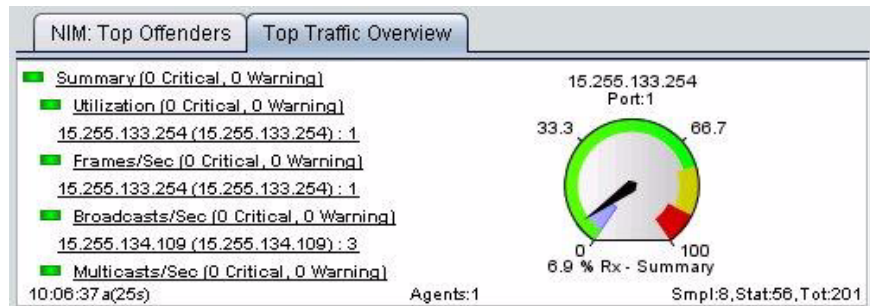


Figure 11-1. Traffic Overview Pane on Network Management Home Dashboard

The Top Traffic Overview panel lists each metric group (type of traffic statistic), a color-coded LED for each metric group indicating the state of the worst port with regard to that metric group, and a Traffic Gauge. The metric group LED takes its state from the worst port in the network as measured by the ports' values for the indicated metric group with respect to the metric thresholds set on each port. The LEDs indicate the network traffic status for the latest update (most recently elapsed minute) with each LED indicator showing one of the following states:

LED	State	Utilization	Description
Gray	Disabled	-	Used during initialization to signify that the Traffic Monitor has not yet collected any data
Green	Normal	0-74%	All ports are within the normal range for the metric group as measured relative to their respective thresholds.
Yellow	Warning	75 - 89%	At least one port has exceeded the warning threshold defined for it in the metric group, but it has not exceeded the critical threshold defined for it.
Red	Critical	90% or greater	At least one port has exceeded the critical threshold defined for it in the metric group.

Reading the Traffic Information Gauge

By default, when the summary of metric groups is selected, the traffic gauge displays network traffic information on the worst port for the current minute. When a metric group is selected, for example Utilization (0 Critical, 1 Warning), the worst measurement on a port in that metric group is displayed for the most recently completed minute.

The needle moves around the gauge to indicate the measured value for the selected metric group. The colors on the gauge indicate the state of the measured value relative to the port's thresholds that are defined for the selected metric group:

- Green: The measured value falls below the warning threshold defined for the indicated port and metric group.
- Yellow: The measured value has exceeded the warning threshold defined for the indicated port and metric group, but has not exceeded the critical threshold defined for the port and metric group.
- Red: The measured value has exceeded the critical threshold defined for the indicated port and metric group and corrective action may be warranted.
- Blue inner band: High water mark, which shows the highest value measured for the indicated port and metric group during the past 12 hours. This indicator can help you determine if there are any transient or intermittent problems for the port that may not have occurred during the last minute, even though the last completed minute shows normal activity.

Note:

If you do not have PCM installed, an unavailable message is displayed. No port selected is displayed if no devices are configured in the Traffic Monitor.

The amount of green, yellow and red displayed in the gauge corresponds to the threshold settings (set in Configure Thresholds) for the selected port and metric. For example, if the current Threshold settings for Utilization% on the selected port are as follows,

green: OK, 0-50% utilization

yellow: warning, 51-75% utilization

red: critical, 76-100% utilization

then the gauge for Utilization% would display a green area up to 50%, a yellow area from 51% to 75%, and a red area from 76% to 100%.

The text below the gauge indicates the attribute value for the current minute.

For additional details on the worst traffic segment, click inside the Worst Overview panel to display the Traffic tab for the Devices node of the navigation tree in the Agent Group that the port whose measurement was shown on the gauge resides in.

Trend Graph Displays

For additional details on the worst traffic segment, click the port listed under the metric to change the display from the traffic gauge to a trend graph.

The trend graph displays the measured values for the metric group over a span of 12 hours (720 intervals). As new points are added, the bars in the graph shift left. The x-axis displays the timestamps of the range of data in the window. For ports that support separate Rx (received or ingress) and Tx (transmit or egress) traffic data, two graphs are displayed. When only Rx-Tx combined data is available, one graph is displayed.

Horizontal threshold indicators (graph lines) display for the warning threshold value (yellow), critical threshold value (red) and maximum (high water mark) value (blue). The warning and critical threshold indicators are not editable from this pane. You can mouse-over on each bar to display its value, timestamp and threshold values.

Using the Traffic Tab

The Traffic tab provides a traffic monitoring facility that delivers minute-by-minute views of the volume and the content of traffic at specified points within your ProCurve network. Only the devices/ports in the selected device or device group are displayed. When the Devices node is selected all monitored device ports are displayed. Traffic monitoring is set to run automatically, with the ability to simultaneously perform statistics polling and sFlow sampling.

Click the Traffic tab to display traffic details for devices in the node selected in the navigation tree.

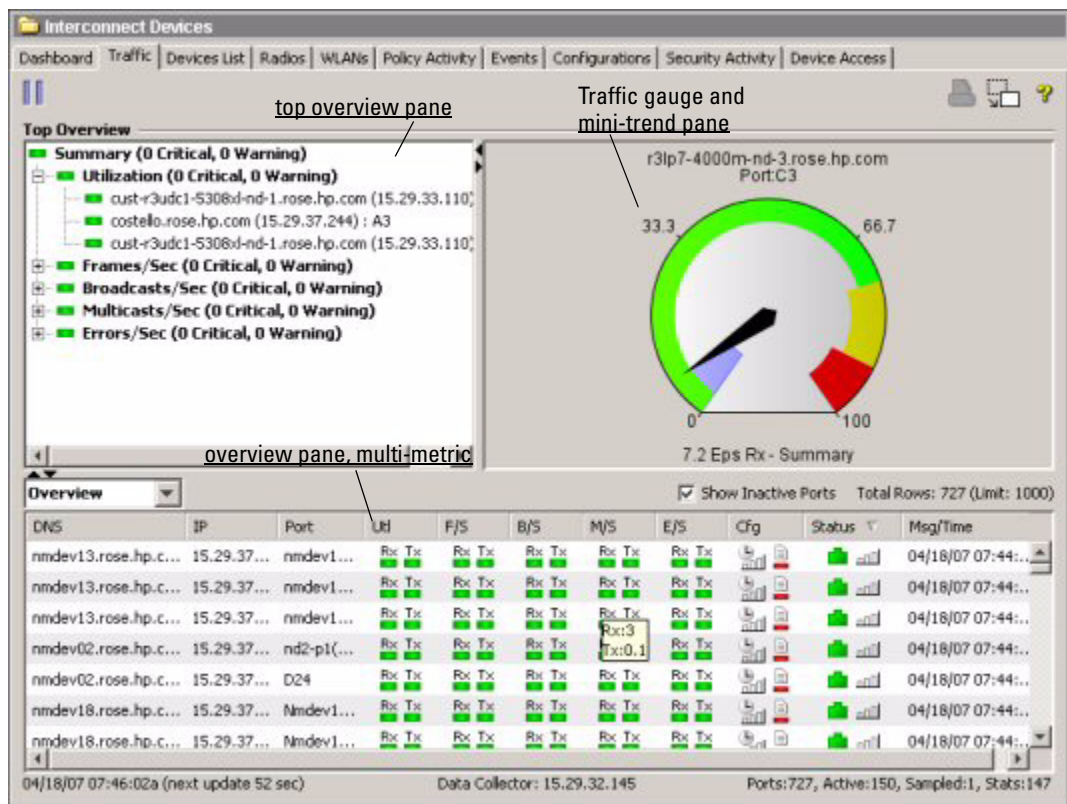


Figure 11-2. Traffic Tab

The Traffic tab is divided into three separate panes.

Top Traffic Overview Pane: Displays the worst measures for each metric group, and the number of ports that have reached critical or warning thresholds in the last interval. Click the + to show the worst ports for that metric. The number of device ports for each metric group can be set in the traffic preferences (default is 3).

Each row contains a leading LED (icon) indicator that shows one of the following states:

- Disabled (gray), used during initialization to signify that the Traffic Monitor server has not received any data yet.
- Normal (green), metric is within the normal range.
- Warning (yellow), metric has exceeded normal range, but is not critical.
- Critical (red), a threshold violation for the metric has occurred.

The metric group row LED takes its state from the worst case in the metric group (or is disabled). The LEDs display the network traffic information for the latest update (or current minute). The color of the LED (green, yellow or red) corresponds to the threshold settings for that port. Using the default thresholds for utilization, the LED colors can be interpreted as follows:

green: OK, 0-74% utilization

yellow: warning, 75 - 89% utilization

red: critical, 90% or greater utilization

Traffic Gauge and Mini-Trend Pane: : When you first open the Traffic tab, the Traffic Gauge displays, with the pointer set for the worst port in the current minute. When a heading row is selected, for example Utilization (0 Critical, 1 Warning), the worst metric in that group is selected. Note that the Critical and Warning notation indicates the number of ports for which the threshold was exceeded in the last interval.

Click a port under the Metric in the Top Traffic Overview pane to display the Mini-Trend pane (bar graph) for that port. The trend graph displays the measured values for the selected metric and port over a span of 12 hours (720 intervals). As new points are added, the bars in the graph shift left. The x-axis displays the timestamps of the range of data in the window. For ports that support separate Rx (received or ingress) and Tx (transmit or egress) traffic data, two graphs are displayed. When only Rx-Tx combined data is available, one graph is displayed.



Figure 11-3. Traffic Trend Graph display

Horizontal threshold indicators (graph lines) display for the warning threshold value (yellow), critical threshold value (red) and maximum (high water mark) value (blue). The warning and critical threshold indicators are not editable from this pane. You can mouse-over on each bar to display its value, timestamp and threshold values.

Overview Pane (multi-metric mode): This pane displays a table with the device/ports for the selected device or device group in the navigation tree. Because of the potentially large number of ports in a given network, the number of devices/ports displayed is limited to 1000. This limit is shown in the Total Rows field at the upper right of the Overview panel and can be modified in Traffic Preferences. Each column can be sorted in descending or ascending order by clicking the column heading. The sort is first performed on the Agents, and the results are merged on the Server up to the limited number of rows.

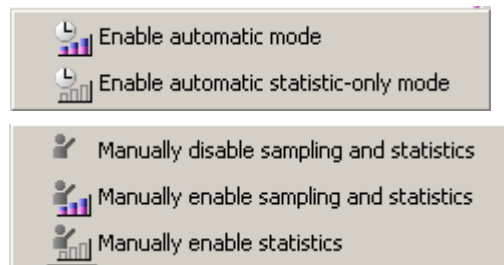
Note:

Some ports will be missing LEDs in certain columns; specifically wireless radios and WAN ports. This happens when a port does not support the counters than can be used for that metric. The remaining metrics - those that LEDs appear for - will function correctly for such ports.

Some ports have only one LED in each column rather than two LEDs. When counters are available to support ingress/egress traffic breakout, two LEDs are used.

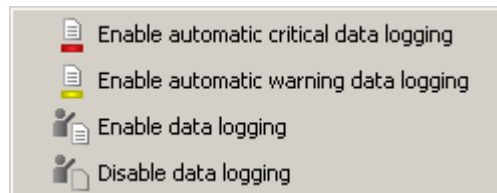
The following information is provided in the table columns:

- Device: displays the device name in the form "DNS Name (IP Address)" and can be sorted alphabetically (alpha-numerically if numbers are used)
- Port: displays the port in the form "Friendly Port Name (Port Name)" and can be sorted alphabetically (alpha-numerically)
- Metric group type: displays the name of the selected metric group, and LEDs (icons) as described in the Top Traffic Overview section above. If separate Rx and Tx data is available, two LEDs are displayed. If only Rx-Tx combined data is available, one LED is displayed. The metric groups can be sorted based on the threshold violations. The default is to sort from highest (critical) to lowest (normal or disabled), thus all critical violations are sorted before warning violations, warning violations are sorted before normal ports and so on. In the case of separate Rx and Tx data, the worst of the two measures will be used to determine sort order.
- Cfg (Monitor): displays two icons indicating the current traffic configuration on the port. The icons correspond to the configuration options available in the right-click menus.
 - Automatic or Manual Sampling (enabled or disabled)



Note that only one sampling method can be used at a time. When you enable automatic mode, manual sampling is disabled, and vice versa.

- Data Logging (Auto-critical, Auto-warning, enabled or disabled)



Monitoring Network Traffic

Reviewing Traffic Data

- Status: displays the current status for the port. The status value will be one of the following:
 - A colored bar chart indicates sample data received in the last interval/minute
 - Gray outline bars indicate statistics only data received in the last interval/minute
 - If no bar chart appears, no sample or statistics data was received
- Msg/Time: displays the timestamp for the last time stats were collected for the port and descriptive information regarding the state of the port with respect to data collection.

Overview Pane (single-metric mode): is similar to the multi-metric mode but only displays one of the metrics for each port allowing for more detail. Switching between multi-mode and single-mode is accomplished from the drop-down menu above the table. There is a single-metric mode for each metric group. For example selecting Utilization in the menu will change the table to display a single metric column titled Utilization with data similar to the following figure:

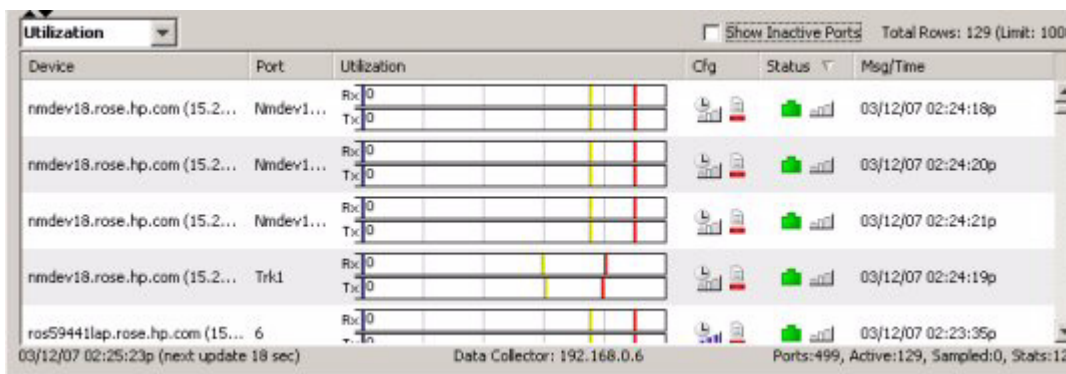


Figure 11-4. Overview Pane "Single-metric" mode display

When separate Rx and Tx measurements are not available, a single Rx-Tx graph is displayed. The color of the bar reflects the threshold violation status. Separate color bars indicate threshold settings and "high water mark" for the port. This column can be sorted similarly to the Metric Group column.

Status Bar: The Status Bar at the bottom of the Traffic tab displays:

- The last update from the data collector and estimated time until the next update (left).
- The data collector status (middle), displays the PCM Server IP address.

- Data collector administration data (right): Sampled = number of ports providing statistics in last minute, Stats= number of ports providing sample data in last minute, Total = total ports in the query.

Mousing over the right text displays a break down of the information for each Agent.

Reviewing Port Top Talkers

Right-click a single port in the Traffic tab, then select the Port Top Talkers... option from the right-click menu to display the Traffic-Port Top Talkers window.

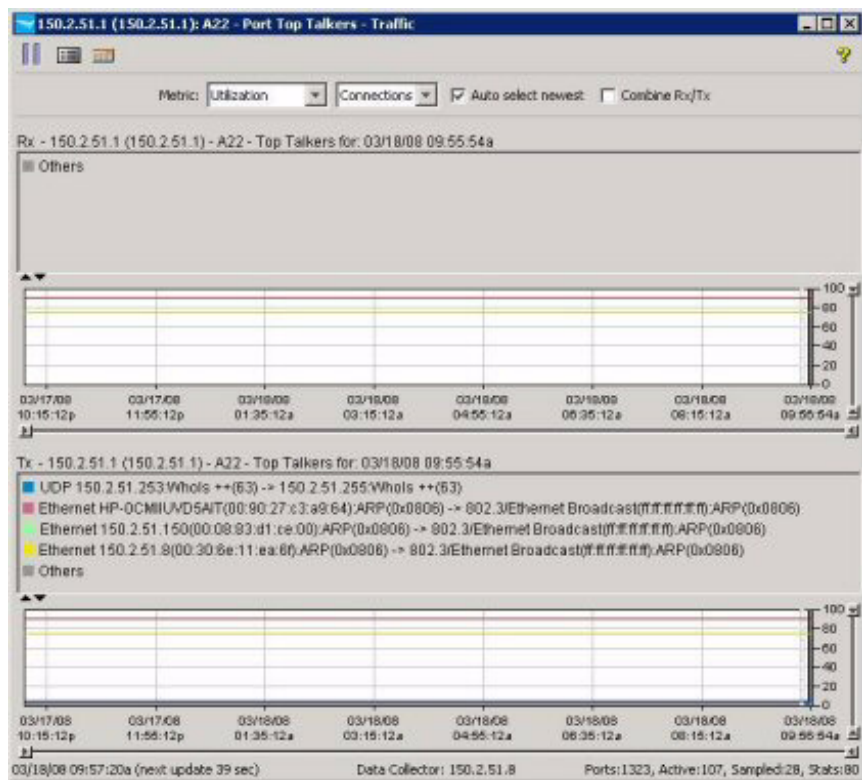


Figure 11-5. Traffic, Port Top Talkers window

The Port Top Talkers window helps answer the question, “Who is causing the problem (who are the top talkers) on a given port?” by displaying a graph identifying the top nodes causing the network activity on the port for the selected minute. If the port is not sampling-capable, the only data displayed

is “Others”. Note that with sampled (sFlow) data, PCM is able to determine the traffic content and volume. With just polling statistics, PCM can only determine traffic volume.

Top Talker View Options

The Top Talker View has two menu selections. The options of each are described in the following table. You can display a graph of the Top Talkers for each of the measured metrics, for received (Rx) and transmitted (Tx) traffic, by selecting the options for the metric and the attribute to display:

Menu Item	Function
Metric	Displays a new graph for each metric: <ul style="list-style-type: none">• Utilization%• Frames/sec• Broadcasts/sec• Multicasts/sec
Top Talkers	Selects the traffic type displayed for the selected metric: <ul style="list-style-type: none">• Connections• Destinations• Sources• Protocols

Top Talker data is given for Rx (received) and Tx (transmitted) traffic. The Top Talker data consists of a legend showing the Top Talkers for the selected interval and a bar chart displaying the data from the current and previous intervals. The legend displays each entry's percentage contribution of the total counts for the interval displayed in the graph. The total counts are displayed under the percentages. When you hover over the bar corresponding to the legend entry in the stacked bar chart of a minute, the contribution from a top talker legend entry displays the timestamp of the minute being hovered on, and the contribution of the legend entry and total of the metric value for the minute hovered over are shown below the timestamp.

Note:

The Top Talker graphs are designed to show data at one minute intervals for the last 12 hours. The data display starts on the right and moves to the left over time.

The yellow and the red horizontal lines on the background of the graph represent the warning and critical values, respectively, for the selected port. These lines only appear when the graph scale is high enough.

The selection of a bar inside either Rx or Tx graph is synchronized so that a selection in one will automatically select the corresponding bar in the other (for the same interval). The scroll bar at the bottom of the region is tied to both graphs and will scroll the x-axis. The scroll bar at the right of the graphs will scroll the Y axis.

The information provided by the legend includes:

- The source address, destination address, or both depending on the attribute being viewed.
- The network protocol or service being used for the communication path. That is, the highest network protocol decoded by PCM for the applicable attribute is displayed.
- The direction of data flow (the source and destination nodes)

There are a maximum of 5 Top Talker entries for Rx and Tx measures. You can visually trace the data across the graph to see trends in activity over the past 12 hours.



You can also use the right click menu on the graph. This menu is available in the mini-trend graph as well and allows the user to change to “Fixed max scale”, default is “Auto Scale” as well as unzoom. You can click-drag a rectangle in the charts to zoom in. You can right-click drag to pan the data.

Reviewing Per-Port Traffic Statistics

Right-click a single port in the Traffic tab, then select the Port summary... option from the right-click menu to display the Port Summary - Traffic window.

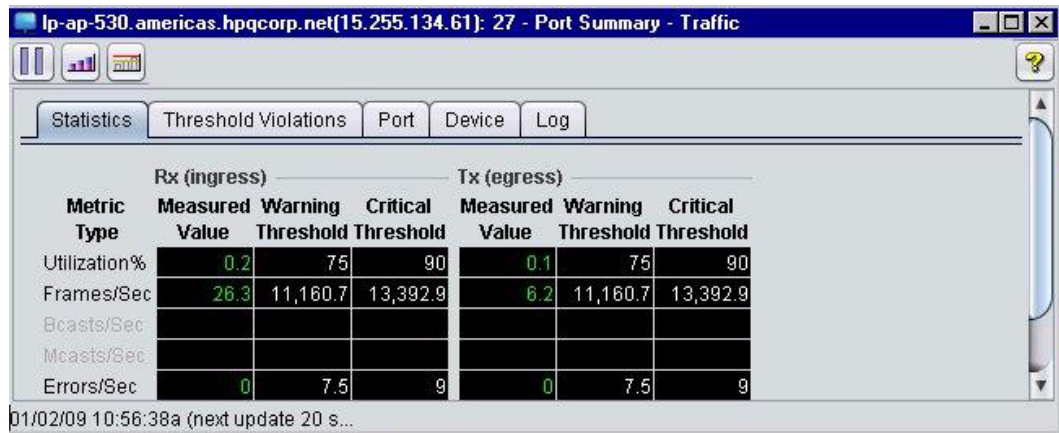


Figure 11-6. Port Summary, Statistics tab display

The Port Summary - Traffic window uses a tabbed display to provide the summary traffic information for the selected port, as described below:

Statistics Tab: The default display, this tab provides a table that lists the summary details for each traffic metric for the port, including:

- Measured Value: The current value (at last update) for the metric.
- Warning Threshold configured for the metric.
- Critical Threshold configured for the metric.

Threshold Violations: Click the tab to display a table with data on threshold violations for each metric on the selected port for both ingress and egress traffic.

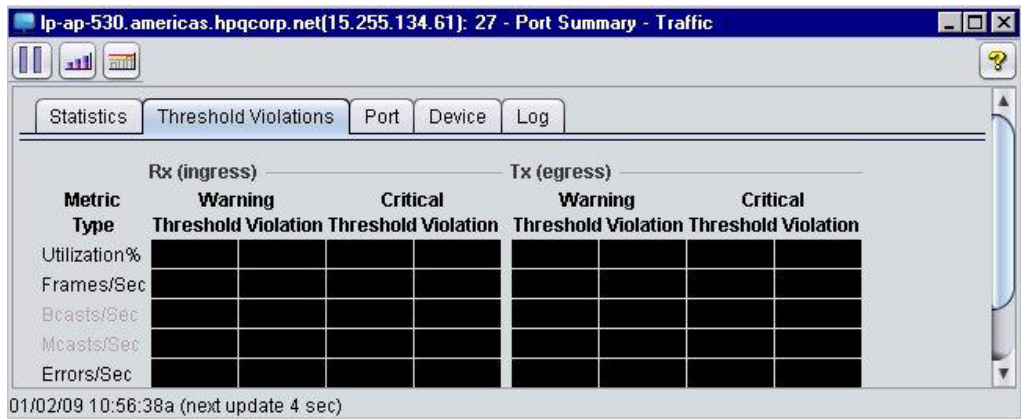


Figure 11-7. Port Summary, Threshold Violations tab display

- Warning Violation indicates when the port is in violation of the warning threshold value. This means the port's metric value has crossed the warning threshold and has not stayed below the warning threshold for 3 minutes.
- Critical Violation indicates when the port is in violation of the critical threshold value.

Port: The Port tab provides port attributes

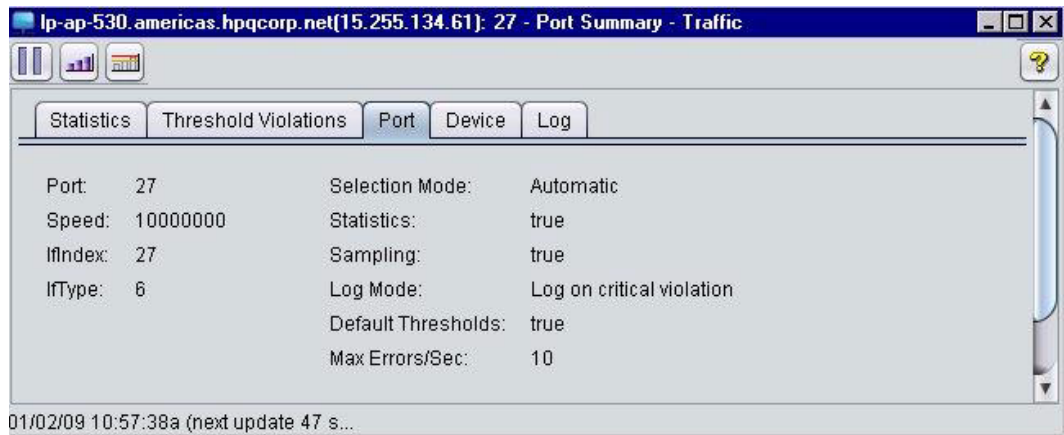


Figure 11-8. Port Summary, Port tab display

The left column lists the:

- Port - Port name or ID.
- Speed - the port's operating speed
- Active - If the port is currently active (true or false),
- IfIndex, IfType - The interface index and interface type from MIB-2.

The right column lists the traffic configuration on the port, including:

- Mode indicates if sampling is set to Auto or Manual mode.
- Collect Statistics Data (if supported) indicates whether the Agent should attempt to collect statistics if the device supports this feature.
- Collect Sampling Data (if supported) indicates whether the Agent should attempt to collect sampling data (sFlow) if the device supports this feature.
- Log Mode displays the current log mode for the port. The valid modes are:
 - Auto-Crit: logging of the port traffic data will start/stop during critical violations
 - Auto-Warning: logging of the port traffic data will start/stop during warning violations
 - Manual-On: logging of the port traffic data is always on
 - Manual-Off: logging of the port traffic data is always off
- Default Thresholds indicates if default traffic thresholds are used, yes or no.

- Max Errors/Sec indicates maximum errors per second based on line speed of the port.

The Device tab lists the IP Address and Product Description of the device the port belongs to.

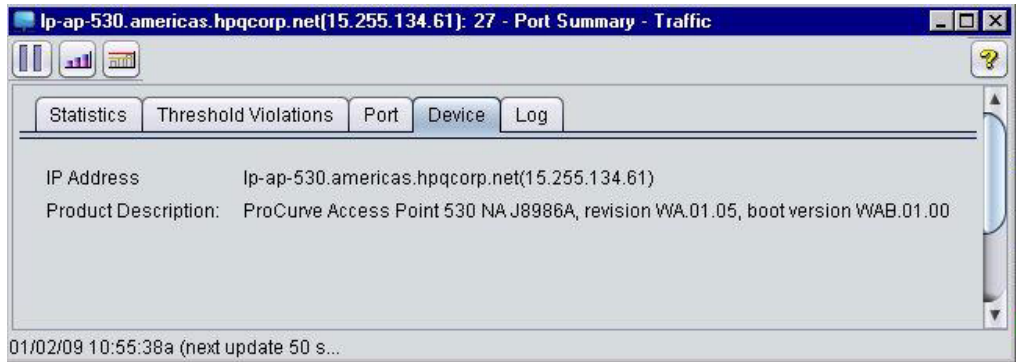


Figure 11-9. Port Summary, Device tab

Log: This tab displays timestamps for the latest received traffic updates. It is essentially a history of the contents of the Traffic tab's Msg/Time column.



Figure 11-10. Port Summary, Log tab

Reviewing Traffic Monitor Events

Traffic Monitor "alarms" can be reviewed in the Event browser. In the Events browser, "Critical threshold" alarms have an event severity of Major, and Warning threshold alarms have an event severity of Warning. The threshold violation event will indicate which port generated the threshold alarm.

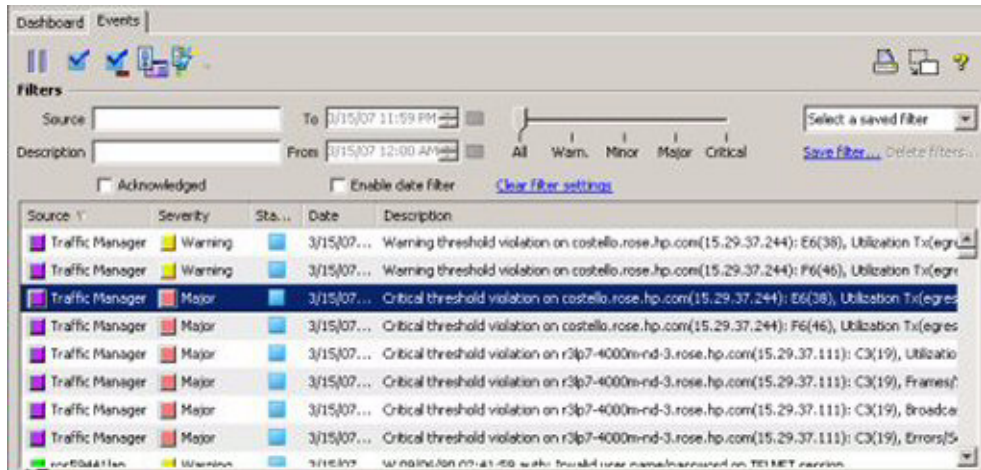


Figure 11-11. Example of Traffic Monitor events

Only one threshold violation event will be sent and the port is put in a "violation" state. This can be monitored by the Port Summary Threshold Violation tab. The port must remain below both thresholds (warning and critical) for 3 minutes for the port to be removed from the violation state.

Configuring Traffic Monitor

Traffic Manager employs a default configuration for automatically selecting and configuring ports on which to monitor traffic.

You can manually override the automatic statistics sampling to disable traffic monitoring on specific ports, or to have statistics and/or sampling always enabled on specific ports. You can also tune the threshold settings for each measured metric to suit your specific network requirements.

Manual Configuration of Traffic Thresholds

To configure the traffic thresholds for Warning and Critical:

1. Select the device or group where you want to configure Traffic monitoring, then open the Traffic tab display.
2. Click to select the ports on the devices that you want to configure thresholds for traffic monitoring. Use shift-click or Ctrl+click to select multiple ports.
3. Select the Configure Thresholds option from the traffic right-click menu to display the Traffic- Threshold Configuration dialog. (see figure 11-12 on the next page.)

Thresholds can be set for each metric on Rx or Tx. If the port only supports combined Rx and Tx data, only one bar will be shown. The threshold parameters can be set as follows:

1. Click the check box to indicate that a Warning event should be sent to the Events browser.
2. Enter the Warning threshold value (any number from 0%-100%, and less than the critical threshold setting).
3. Click the check box to indicate that a Critical event should be sent to the Events browser.
4. Enter the Critical threshold value (any number from 0%-100%, and greater than the warning threshold setting).

Note:

The threshold percentage is valid for the utilization only where it is measured in percent. The other metrics are based on the maximum frames per second for the speed. However, you can specify the maximum errors per second (see “Changing Line Speeds” on page 11-22).

5. Repeat the process to set threshold values for each metric measured by Traffic Monitor. When you are done, click the **OK** button to save the changes and close the Threshold Configuration dialog.

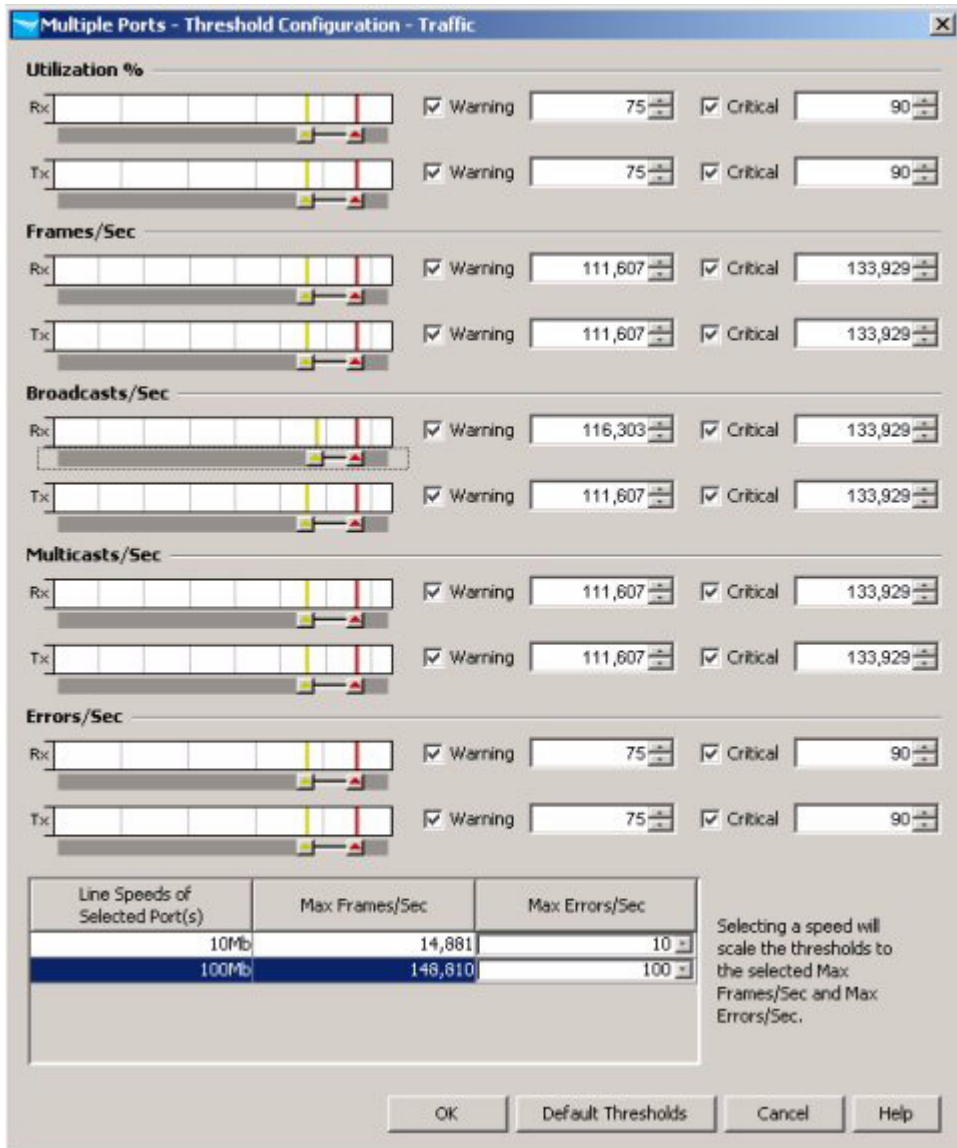


Figure 11-12. Traffic Monitor: Thresholds Configuration dialog

You can also change the threshold settings by moving (click+drag) the colored threshold indicators in the bar graph. For example, moving the yellow bar will change the Warning threshold in the graph, and the numeric (%) field. Similarly, when you enter a number in the % field, the related bar in the graph will move to indicate the new setting.

Changing Line Speeds

In multiple port selections, multiple line speeds for the selected ports are shown in the table in the bottom of the dialog, along with the relative metric/Sec, and Max Errors allowed for that line speed.

The relative Max Error counts for a port can be modified as follows:

1. Select the line speed that you want to change.
2. Use the Set Max Errors pull-down menu to select the maximum errors. The number is set as indicated for the selected line speed, and converted to the appropriate number for all other line speeds. For example, if Max Errors for 1Gb line speed is set to 100, and you have a second port with a line speed of 10Gb, the Max errors will automatically be scaled to 1000, and so on.

The Max errors number controls the maximum value displayed in the thresholds configuration sliders, as well as on the traffic Gauges and in the Errors/Sec view in the Traffic tab display.

Changing the threshold ranges to better represent your network's normal activity will be a relative decision. It is recommended that you use the default threshold values first and adjust them to fit the traffic patterns on your network. By fine tuning the threshold levels, you can find the optimum operating conditions for each port on your network, which makes it easier to see problems as they occur.

Manual Configuration of Traffic Monitoring

To display the traffic monitoring configuration tools menu, right click the row of a selected port in the Overview metrics table in the Traffic tab:

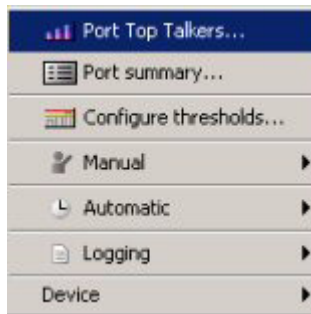


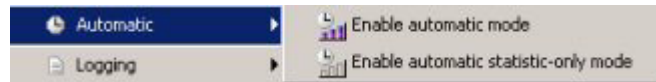
Figure 11-13. Traffic Manager tools menu (right-click menu)

Select the Manual sub-menu to enable or disable Manual configuration of polling and sampling.



Click an option to turn it on. The icon for that monitoring option will appear in the Cfg column of the selected port on the Overview table in the Traffic Tab display. (refer to figure 11-2 or figure 11-4)

Use the Automatic options to enable or disable automatic traffic sampling and statistics.



Note that only one monitoring mode can be in use on a port. Selecting a different monitoring option will automatically disable the previous setting. For example:

If the Manually enable statistics mode is in use on a port, when you select Enable automatic mode, the manual mode is disabled on the port, and the automatic mode icon appears in the Cfg column.

The Logging sub-menu provides options for configuring traffic data logging.



The following table describes the available traffic configuration functions:

Traffic Menu Option	What it does...
Manual: Manually disable sampling and statistics	Turns off all traffic monitoring on the selected ports.
Manual: Manually enable sampling and statistics	Turns on traffic sampling and statistics for the selected ports. Traffic monitoring is in effect until disabled, or switched to automatic mode.
Manual: Manually enable statistics	Turns on traffic statistics monitoring for the selected ports. Statistics monitoring is in effect until disabled, or switched to automatic mode.
Automatic: Enable automatic mode	Turns on automatic traffic monitoring. Traffic manager will do statistics polling and/or sFlow sampling as indicated by traffic levels on the selected ports.
Automatic: Enable automatic statistics-only mode	Turn on automatic traffic statistics monitoring for the selected port. No sFlow sampling will be performed.
Logging: Enable automatic critical data logging	Automatically logs data if port traffic violates a critical threshold setting (logs only critical threshold violations).
Logging: Enable automatic warning data logging	Automatically logs the data for the port if the port is in violation of the warning threshold.
Logging: Enable data logging	Set data logging on the selected port to Manual On mode, which logs all Traffic Monitor data for the selected port(s).
Logging: Disable data logging	Set data logging on the selected port to Manual off mode, which turns off all traffic monitor data logging on the selected port(s).
Configure Thresholds...	Launches the Traffic: Threshold Configuration window for the selected port(s). See "Manual Configuration of Traffic Thresholds" on page 11-20 for details.
Port Top Talkers...	Launches the Traffic: Port Top Talkers window, with data for the selected port(s). See "Reviewing Port Top Talkers" on page 11-11 for details.
Port summary...	Launches the Traffic-Port Summary window for the selected port. (If more than one port is selected, only the last port selected is displayed). See "Reviewing Per-Port Traffic Statistics" on page 11-14 for details.
Device	Launches the PCM device right-click menu, for access to Configuration Manager, Device Manager, etc.

The data log files include essentially everything that is in the Top Talkers legend for each minute that you have logging enabled on a port. The log files are located in: <PCM-agent-install>\<server-id>\data\traffic\data\log

Setting Traffic Monitor Preferences

You can enable automatic configuration of the Traffic Monitor features and configure the Traffic "view settings" using the Preferences, Traffic options.

The automatic configuration feature uses the Discovery process to automatically configure the Traffic Monitor ports based on the Default Port Monitoring preference.

View settings and customize the row table limits in the Traffic tab.

To enable the automatic Traffic configuration on discovered ports:

1. Select Tools > Preferences > Traffic to display the Global:Traffic preferences window.

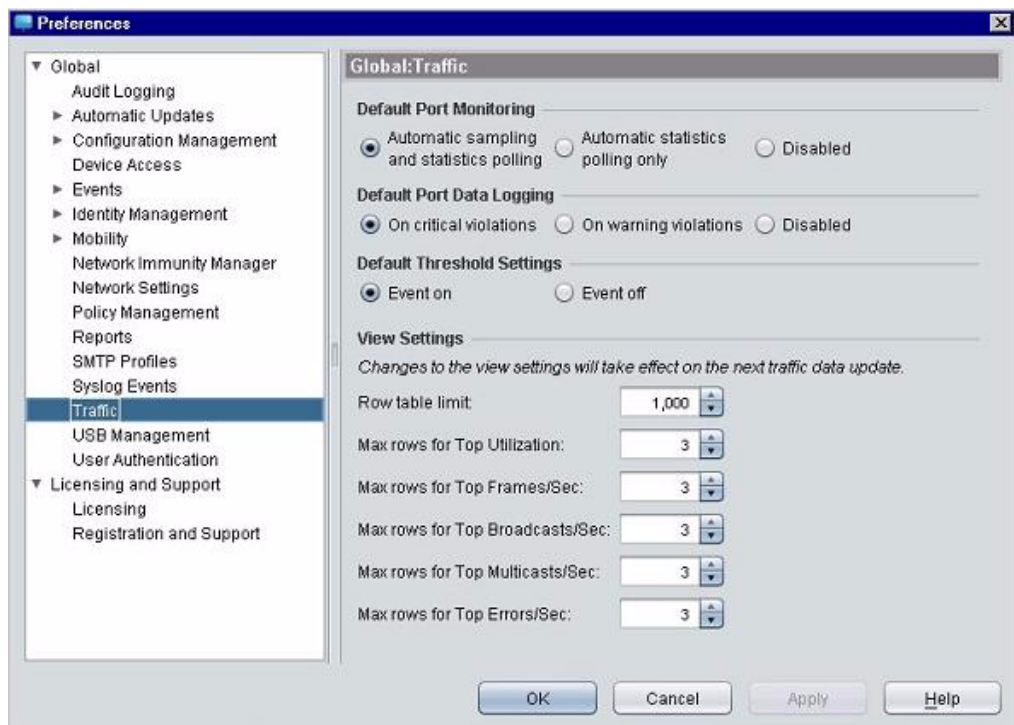


Figure 11-14. Preferences, Global:Traffic window

Monitoring Network Traffic

Setting Traffic Monitor Preferences

2. Select the desired Default Port Monitoring option by clicking the radio button.
 - **Automatic sampling and statistics polling:** Configures automatic traffic monitoring with sampling and statistics on any newly discovered port. You can override the mode in the Traffic tab views.
 - **Automatic statistics polling only:** Configures automatic traffic monitoring with statistics polling only on any newly discovered port. You can override the mode in the Traffic tab views.
 - **Disabled:** Traffic monitoring will not be configured for any newly discovered port, unless set manually in the Traffic tab views.
3. Select the desired Data Log option from the pull-down menu.
 - **On critical violations:** All newly discovered ports are configured to automatically log data if the port has violated the critical threshold.
 - **On warning violations:** All newly discovered ports are configured to automatically log data if the port has violated the warning threshold.
 - **Disabled:** All newly discovered ports are configured to not allow data logging.
4. Select the desired Default Threshold Settings option by clicking the radio button.
 - **Event On:** All newly discovered ports will send threshold violation (Warning or Critical) events to the event browser and the PCM automation can act on the event.
 - **Event Off:** Events are not sent, but they will be included in the threshold violation count.

Note that this value can be overridden in the Threshold Configuration dialog (Warning/Critical check boxes)

Note:

Changes made to the preferences for Default Port Monitoring Mode, Data Log Mode, and Default Threshold settings apply only to newly discovered switches and ports. It does not apply to traffic monitoring on existing devices or ports on the network.

5. The **View Settings** options customize the row table limits in the Traffic tab displays. Set the row limits using the increase or decrease buttons.
 - **Row table limit:** Sets the maximum number of rows (100-1000 in increments of 10) allowed in the Overview table in the bottom panel of the Traffic tab. The default is 1000.
 - **Max rows for Worst *metric*:** Max rows that will be displayed for each metric in the Top Traffic Overview table at the top of the Traffic tab. The range is 0 - 10 with a default of 3.
6. Click **Ok** to save Traffic Preference changes and exit the window.
Click **Apply** to save changes without exiting the window.
Click **Cancel** to exit the window without saving the Traffic Preferences configuration changes.

Troubleshooting Traffic Monitor

There may be times when your Traffic Monitor graphs are not registering any data, or one or more LED displays may go gray. Some of the reasons this may occur are:

- **Data Not Current**—If the data is not current, the graphs and LED displays will not have information.
- **Too Little Traffic on Network**—If your network is carrying very little traffic at this time, the graphs may not indicate any traffic for sFlow data. You will get statistical polling on devices no matter how little traffic exists on the port. If there is no traffic, the reported values will be "0".
- **One port (Port) is Gray**—There may be a problem with this particular port. The data sampler may not be working, there may not be enough traffic on that port, or a device may have been disconnected from that port.
- **Machine is Very Busy**—The CPU may not be able to process the data because it is too busy.
- **Switch is Very Busy**—When an interconnect device becomes overloaded, it may stop responding to traffic monitoring requests in order to execute its primary function of handling network traffic.

You can also look in the Log tab on the Traffic-Port Summary window, or the PCM Event Browser to get additional information on specific devices that may be having problems, or for "Traffic Manager" events indicating there is a problem with Traffic Monitor's ability to access the device.

For sFlow to function properly the traffic data collector must be allowed to receive traffic on port 6343. Some firewalls may block this port by default, and you will need to reconfigure the firewall in order to use PCM traffic monitoring.

If you are using PCM-NNM, make sure that the SNMP Write Community name is set in NNM, and that the Write Community names in PCM and NNM are the same.

Remember that you only need to select one side of a network connection for traffic monitoring. Selecting both sides results in unnecessary overhead on the network.

Managing Device Configurations

About Configuration Manager	12-3
Performing Configuration Scans	12-4
Manual Configuration Scanning	12-4
Reviewing Device Configurations	12-10
Configurations Detail	12-11
Device Configuration History	12-12
Using Configuration Labels	12-13
Comparing Device Configurations	12-14
Updating Device Configurations	12-16
Using the Deploy Configuration Wizard	12-16
Using the CLI Wizard	12-20
Using Configuration Templates	12-26
Comparing Configuration Templates	12-27
Using IP Address Pools	12-28
Using the Configuration Template Wizard	12-32
Applying Configuration Templates to Devices	12-37
Exporting Device Configurations	12-43
Importing Device Configurations	12-45
Using the Software Licensing Feature	12-49
Using the PCM Software Unlicensing Feature	12-52
Configuration Management Preferences	12-55
Setting Preferred Switch Software Versions	12-57
Network (Proxy) Settings	12-58
Updating Switch Software	12-60
Downloading the Software Version List	12-60
Using the Software Index File Download Policy	12-60
Scheduling Automatic Updates	12-61
Using Software Image Import	12-66
Using a USB Autorun File	12-69
Managing USB Certificates	12-69
Managing Encryption Keys	12-70
Creating the Autorun File	12-70
Deploying the Autorun File	12-78

Reading a Report File	12-78
Using a Script to Manage Device Configurations	12-80
Adding a Script to Script Manager	12-82
Editing a Script	12-86
Deleting a Script	12-87
Executing a Script	12-88
Embedded Script Tags	12-95
Troubleshooting a Script Execution	12-96
Script Examples	12-97

About Configuration Manager

The Configuration Manager component in PCM allows you to scan ProCurve Switches in your network and store records of the switch configurations (SW, HW, and Switch Software [OS] configurations) in a database. This information can then be used to:

- Identify when a device configuration has been changed.
- Roll back or forward configurations on a device or devices.
- Send CLI command(s) to one or many devices.

The Configuration Manager scan process can be done on demand or as a scheduled process. This helps you manage device configurations in your network by providing notification whenever any configuration (software or hardware) changes on a ProCurve device in the network.

The Configuration Manager includes the following features:

- Scanning device configurations (manually or at scheduled intervals)
- Viewing device configurations
- Viewing configuration history for a device
- Comparing two device configurations
- Restoring or deploying a configuration to a device
- Creating a configuration template for a device type, and using the template to automatically configure new devices as they are connected to the network
- Importing and exporting device configurations
- Licensing switch software
- Scheduling automatic software updates
- Creating and executing an autorun file from a USB drive
- Running scripts against selected devices on demand or as policy-based actions

Performing Configuration Scans

A configuration scan must be performed on your ProCurve devices before any configuration information is available in the PCM display. A default policy is provided that automatically scans devices on the network to collect device status and configuration information once each day. You can also perform a manual scan at any time.

While Config Scan stores the device configuration in the database, PCM does not interpret this configuration. Performing a config scan does not update device attributes in PCM (e.g., VT settings, STP state, VLAN settings etc.). Discovery gathers the attributes of the devices and their states and updates the device configuration in PCM. Certain components like Port Access and VT also provide a refresh toolbar button to fetch the attributes from the switch on demand and update PCM's repository.

Manual Configuration Scanning

To manually scan a device or group of devices:

1. Select the device or devices in the Devices List display,
2. Select the Scan option from the Device Configuration toolbar menu. Alternately, you can right-click the device in either the navigation tree, or the network map, then select Config Manager > Scan from the right-click menu. Either action will launch the Scan Wizard.



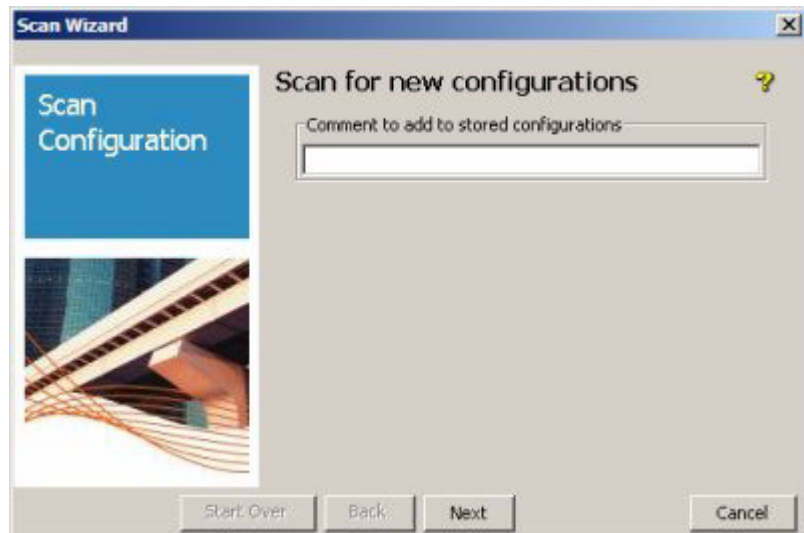


Figure 12-1. Configuration Manager: Scan Wizard, Comment dialogue.

You can enter a Comment that will be stored in the database along with the configuration record, or just click **Next** to continue with the scan process.



3. Select the file transfer method to use for transferring the configuration text from the device to PCM:

- The default is Use TFTP for configuration file transfer.

The default method for configuration file transfer is based on what is defined in Global Preferences for Configuration Management. At initial PCM installation, the default is "Use TFTP for configuration file transfer".

- You can change the mode of transfer for this particular run of the Scan Wizard by selecting "Use Secure Copy for configuration file transfer". Secure Copy (SCP) works with SSH v1 and SSH v2 to provide a more secure file transfer method between PCM and the managed switch. Make sure that SSH is enabled on the device and SSH is the preferred CLI mode in "Communication Parameters in PCM" wizard if SCP is selected as the method for transfer of configuration file.

If you are unsure whether all the devices in your network support the use of SCP, select the Allow TFTP if Secure Copy is not supported, and Allow TFTP if Secure Copy Fails options. If Allow TFTP failover options are not set, the scan configuration operation will report errors if SCP is not supported on the target device.

Enabling SCP modifies the device's configuration the first time it is scanned. The option to use TFTP as a failover mode of configuration scan applies to one single run of the scan wizard. However, if you use this feature, every switch between TFTP and SCP subsequently modifies the configuration again.

4. Click **Next** to begin the actual configuration scan.

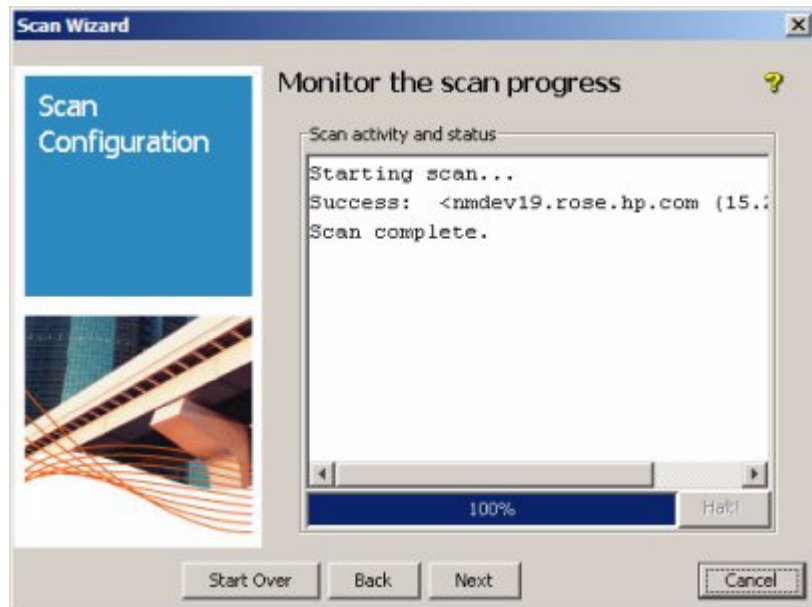


Figure 12-2. Configuration Manager: Scan Wizard, Monitor dialogue.

If the device is not supported by the Configuration Manager, the scan process returns a failure notice in the Monitor dialogue. The scan process will also fail if the correct Write Community Name, SSH parameters and CLI passwords are not configured on the device. Otherwise, the scan proceeds and the "View results" dialogue is displayed.

Note:

On 9300 series devices, if the switch has the super-user password configured, there must be a write community with the same value. For PCM to be able to collect configuration information on your 9300 device, you need to:

- Delete the global super-user password, or
- Set the community name to match the global super-user password.
 - Set the password from a telnet session:
enable super-user-password <password>
 - Set the SNMP Read/Write community name to the same value:
snmp-server community <password> rw

If you selected multiple devices to scan, you can click the **Halt!** button to stop the scan process after it starts. The scan will complete on the device currently being scanned, then the process is stopped. In the case of a single device being scanned, once the scan is started, clicking **Halt!** will have no real effect.

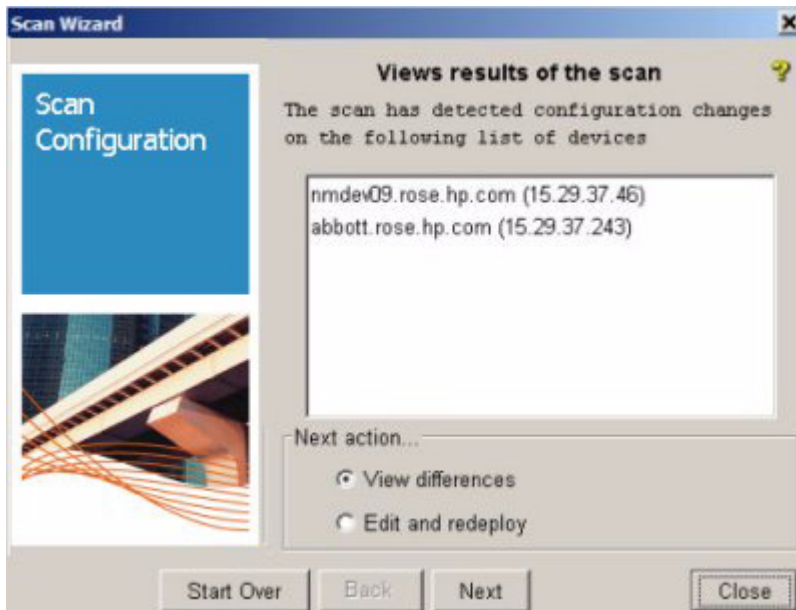


Figure 12-3. Configuration Scan Wizard, View results dialogue.

5. To view differences found between scanned configurations, select the **View differences** option, then click **Next**. The View differences dialogue is displayed.

Note:

If this is the first time the device has been scanned, the "View differences" options will not work, since the system is unable to detect changes until more than one configuration has been scanned.

6. To edit the changed configuration, select the device in the "View results of scan" listing, select the **Edit and redeploy** option, then click **Next**. The Deploy Wizard: Edit dialogue is displayed (see Figure 12-11).

Refer to the instructions for using the Deploy Wizard to update configurations, starting on page 12-16.

If there are no changes detected, the scan results box is empty.

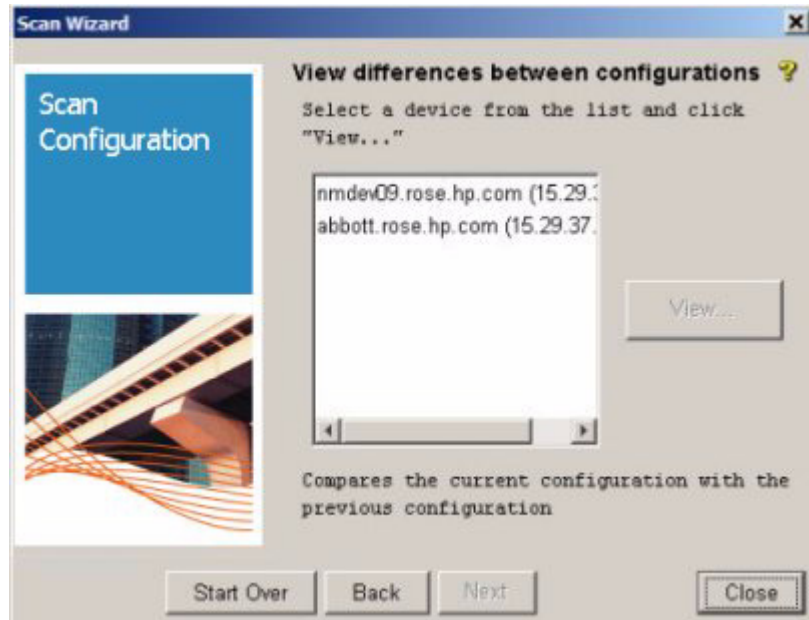


Figure 12-4. Configuration Scan Wizard, View differences dialogue

7. In the "View differences" dialogue, select the device, then click **View...** The "Configuration Difference Viewer" is launched showing the current and previous configuration scan information (see Figure 12-9)
8. When you have completed the configuration scan process, click **Close** to exit the Scan Wizard.

Scheduling Configuration Scans

PCM provides a pre-defined policy to perform configuration scans at regular intervals. You can adjust the policy schedule and target devices, or create separate configuration scan policies to meet your network management requirements. Refer to Chapter 16, "Using Policy Manager Features" for details.

Reviewing Device Configurations

The Configurations pane in Dashboards provides a quick review of overall network device configurations. For a more detailed display, click the Configurations tab.

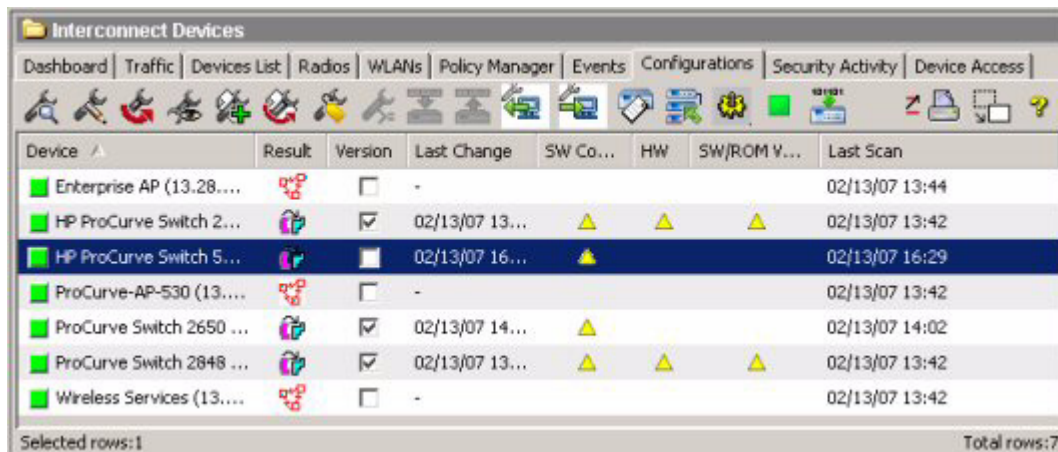


Figure 12-5. Device Configurations listing

The Configurations display provides a summary view of devices configuration, and latest configuration changes. It gives the following information for each device:

Device	DNS name or IP address of the device
Result	Icons indicating the result of the last scan, one of: <ul style="list-style-type: none"> Changed Login failure Device not supported Scan timed out Device never scanned Network error prevented scan
Version	A check indicates the device has the preferred version of the software, as set in the Configuration Manager Preferences. The default Preference setting is the latest available version.
Last Change	Date of the most recent configuration change.

SWConfig	Yellow triangle indicates the software configuration changed on the date shown in the Last Change column.
HW	Yellow triangle indicates the hardware configuration changed on the date shown in the Last Change column.
SW/ROM Ver	Yellow triangle indicates the ProCurve Switch Software and/or Boot ROM changed on the date shown in the Last Change column
Last Scan	Most recent date that a device scan was attempted.

You can sort the list on any of the columns. For example, click the SW column and/or Last Change column heading. This will re-sort the list with devices that have software changes at the top.

Configurations Detail

To view detailed configuration information for a device, double-click the device in the Configurations tab, or select a device in the navigation tree. This displays the Properties tab in the Configuration pane, as described under “Viewing Device Information” on page 2-32. Click the Configuration tab to view the device configuration detail.

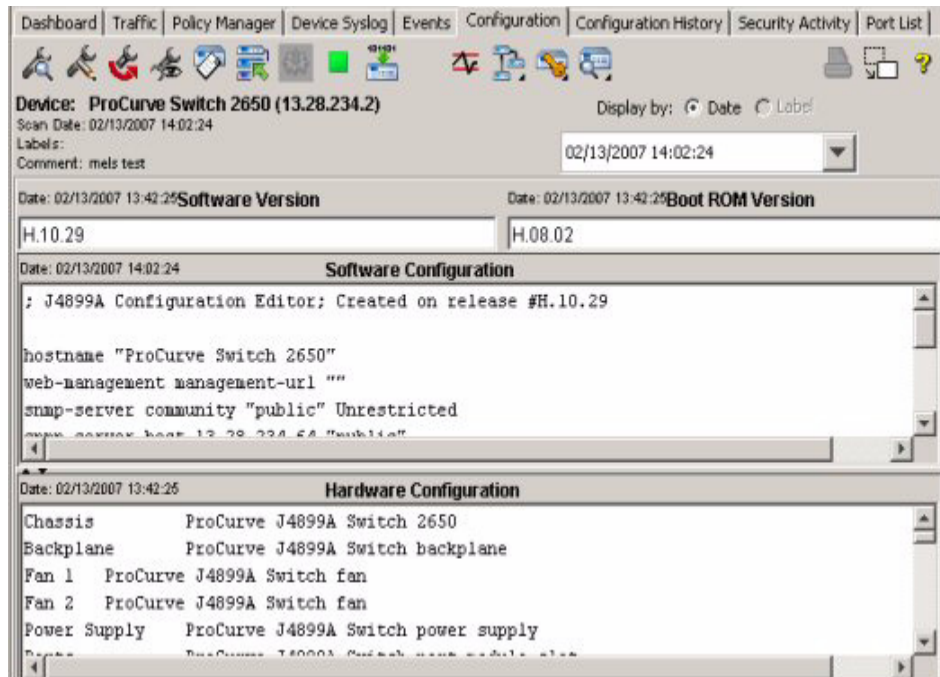


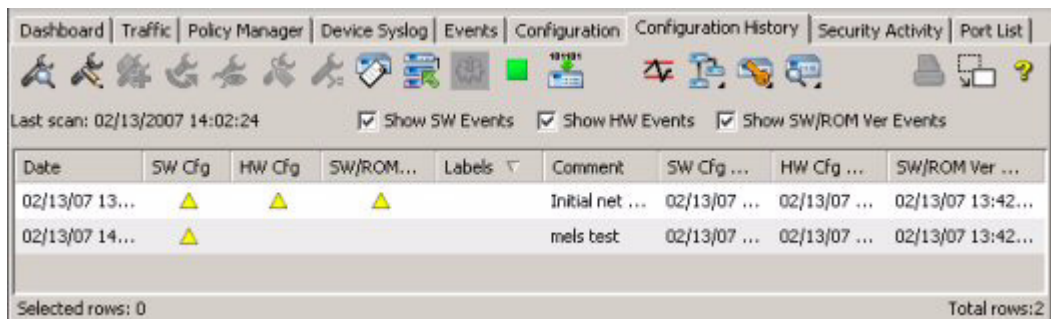
Figure 12-6. Device Configuration detail

If the configuration for the device has changed, you can use the **Display by** option to review the configuration details from previous scans, either by **Date** of the scan, or by configuration **Label** (if used).

Configurations are collected for the ProCurve Wireless access points (420wl, 520wl), but the format is binary proprietary (machine readable only). You can still label and re-deploy wireless configurations as needed.

Device Configuration History

Click the Configuration History tab to view a history of configuration changes for the device.



Date	SW Cfg	HW Cfg	SW/ROM...	Labels	Comment	SW Cfg ...	HW Cfg ...	SW/ROM Ver ...
02/13/07 13...	▲	▲	▲		Initial net ...	02/13/07 ...	02/13/07 ...	02/13/07 13:42...
02/13/07 14...	▲				mels test	02/13/07 ...	02/13/07 ...	02/13/07 13:42...

Figure 12-7. Device Configuration History display

The Configuration History window displays a list of all past configurations* stored for the device. This information can be used to determine when and how configurations have changed.

- The Sw Cfg, Hw Cfg, and SW/ROM Ver columns are marked with a yellow triangle to indicate if the given configuration had changed when that configuration scan was stored.
- The Labels field lists any labels applied to a given configuration.
- The Comments field lists comments entered on the scan event.
- The remaining Sw Cfg Date, Hw Cfg Date and SW/ROM Ver Date columns are provided to help sort the configuration data by the date changes occurred. You can filter out the display of Sw, Hw, or Sw/ROM events by unchecking the "Show" events at the top of the list.

* The number of stored configurations and how long they are saved is controlled by the Configuration Management preferences.

Using Configuration Labels

You can apply labels to a device configuration to help identify known good configurations or other special configurations in the Configurations and Configuration History displays.



To apply a configuration label, select the device configuration in the Configurations or Configuration History display, then click the Label button in the toolbar. The **Apply a Label to device configurations** dialogue will be displayed.

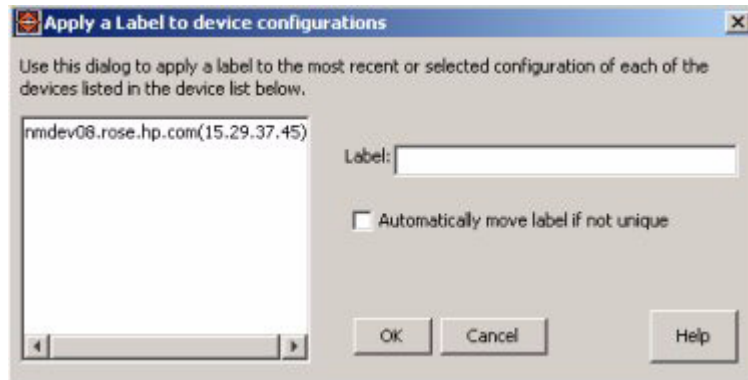


Figure 12-8. Apply Label to Device Configuration dialogue

Note that when accessed from the Configuration History, the device name pane is not shown. Also, if multiple devices are selected in the Configurations listing, each of the devices will be listed in the dialogue.

Enter a **Label** for the device (software) configuration, then click **OK**. The device configuration record will be updated with the new Label.

If you are not sure if the label is unique—that it has not been used before for the selected device, check (click) the **Automatically move label** option. This moves the label to the selected configuration, from a configuration on which it was previously used.

You can apply multiple labels to any given configuration, but each label must be unique. Once a label is applied, the label cannot be edited or removed from that configuration.

Comparing Device Configurations

The Configuration Manager allows you to compare configurations between devices, or two separate configurations on the same device.



To compare device configurations between two separate devices, in the Devices List or the Configurations tab, select two devices in the list, then click the Compare button in the toolbar. In the confirmation pop-up dialogue, click **Compare** to continue with the comparison.

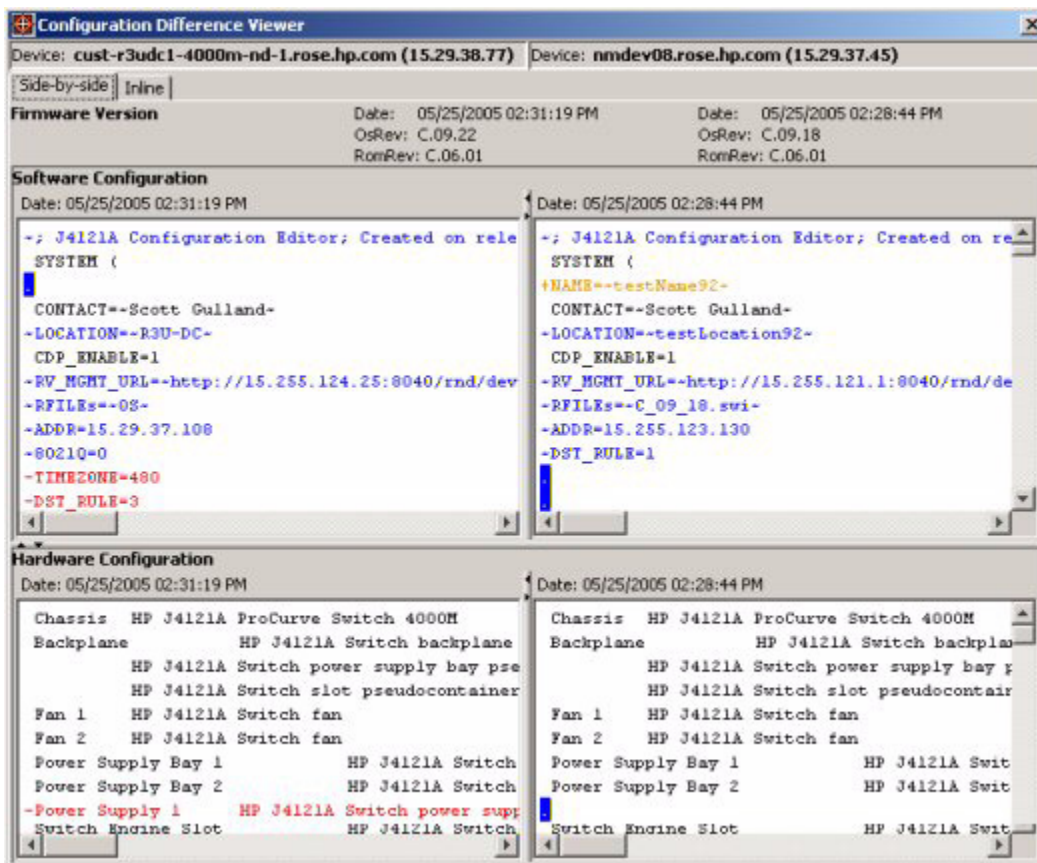


Figure 12-9. Configurations Difference Viewer, default display

The default display is Side-by-side, that is with one device configuration in the right side and the other on the left. Differences in the software configuration are highlighted with different colored text.

If you want to view the differences between the two configurations, click the Inline tab. This displays one pane of configuration commands on top of the other, with additional configuration parameters marked with a plus sign and deleted or missing parameters marked with a minus sign.

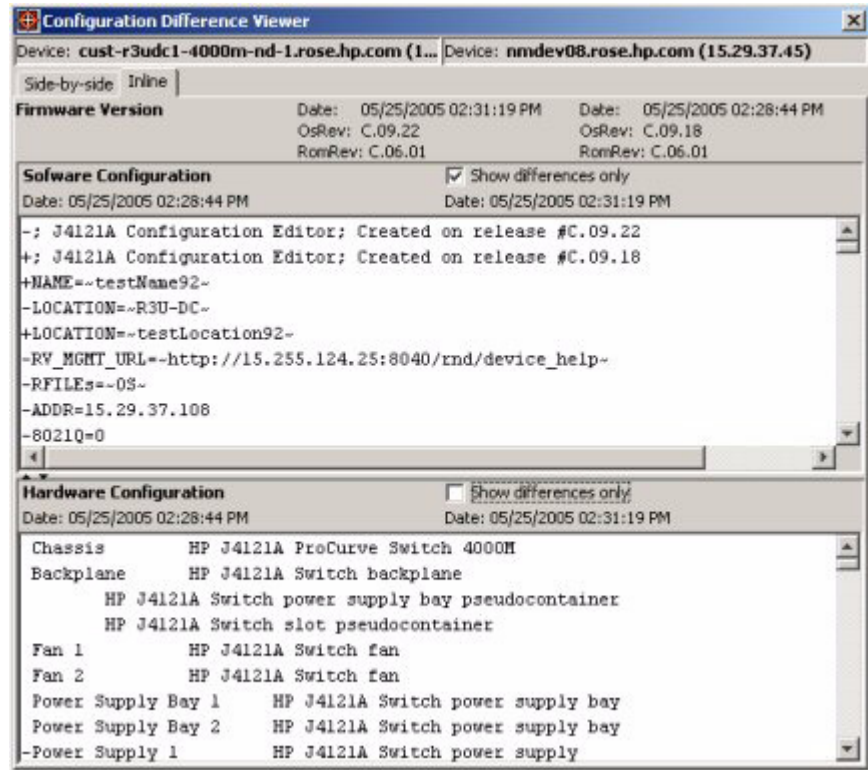


Figure 12-10. Configuration Difference Viewer, Inline display

To view only the differences between the two configuration files, click to check the **Show differences only** option. The inline display will list the first device type, software release, and device name. Then the second device is listed, with the differences in configuration from the first device listed. No other colors or indicators are used to highlight differences between the two configurations.

Updating Device Configurations

After reviewing your network device configurations, you can use the Deploy Wizard to edit the software configuration and deploy it to a device (commit to flash). The Deploy Wizard will perform a total replacement of the software configuration on the target device and then reboot the device and capture the new configuration information. Deployment is useful when you capture a known good configuration and want to restore that configuration in its entirety, or apply the configuration to other devices.

Tip: Use the Device Manager for simple tasks like changing the host name, community names, and authorized managers. Use the CLI Wizard, Telnet, or Web Agent for more complex configuration changes.

Using the Deploy Configuration Wizard



To deploy a known good configuration to a device,

1. Go to the Configuration History window for the device and select the configuration to be deployed, then click the Deploy Configuration button in the toolbar to launch the Wizard.

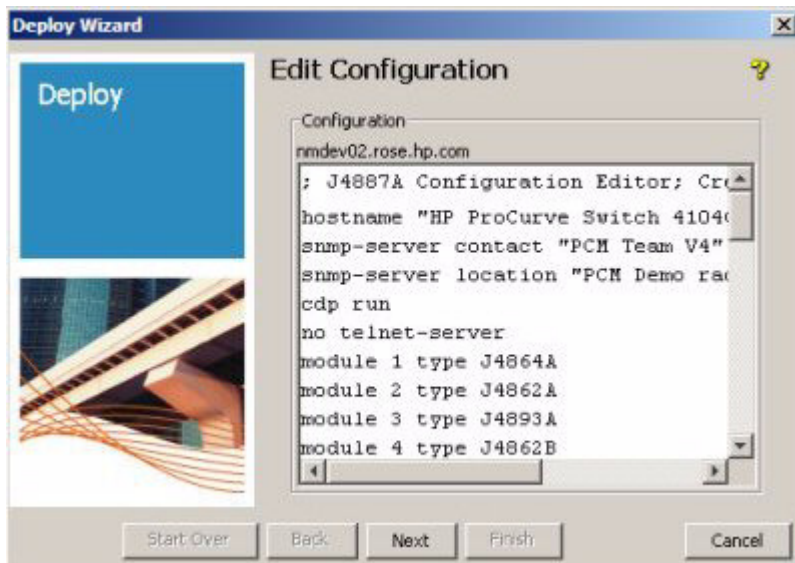


Figure 12-11. Deploy Wizard, Edit Configuration dialogue

Note:

For most ProCurve devices the CLI commands for the configuration display in readable text form. For the 8000, 4000, 2400, and 1600 series devices, the configuration is shown and edited in record format.

If you have selected a known good configuration, no edits should be needed. However, you can click in the configuration display and edit the configuration. PCM does no parsing or interpretation of text entered in the Deploy Wizard. For details on using device configuration (CLI) commands, see the *Management and Configuration Guide* for the device.

Click **Next** to continue.



Figure 12-12. Deploy Wizard, file transfer settings dialog

2. Select the file transfer method to use for transferring the configuration text from the device to PCM:

- The default is Use TFTP for configuration file transfer.

The default method for configuration file transfer is based on what is defined in Global Preferences for Configuration Management. At initial PCM installation, the default is "Use TFTP for configuration file transfer".

- You can change the mode of transfer for this particular run of the Scan Wizard by selecting "Use Secure Copy for configuration file transfer". Secure Copy (SCP) works with SSH v1 and SSH v2 to provide a more secure file transfer method between PCM and the managed switch.

- If you are unsure whether all the devices in your network support the use of SCP, select the Allow TFTP if Secure Copy is not supported, and Allow TFTP if Secure Copy Fails options. If Allow TFTP failover options are not set, the scan configuration operation will report errors if SCP is not supported on the target device.

Enabling SCP modifies the device's configuration the first time it is scanned. The option to use TFTP as a failover mode of configuration scan applies to one single run of the scan wizard. However, if you use this feature, every switch between TFTP and SCP subsequently modifies the configuration again.

Click **Next** to continue.

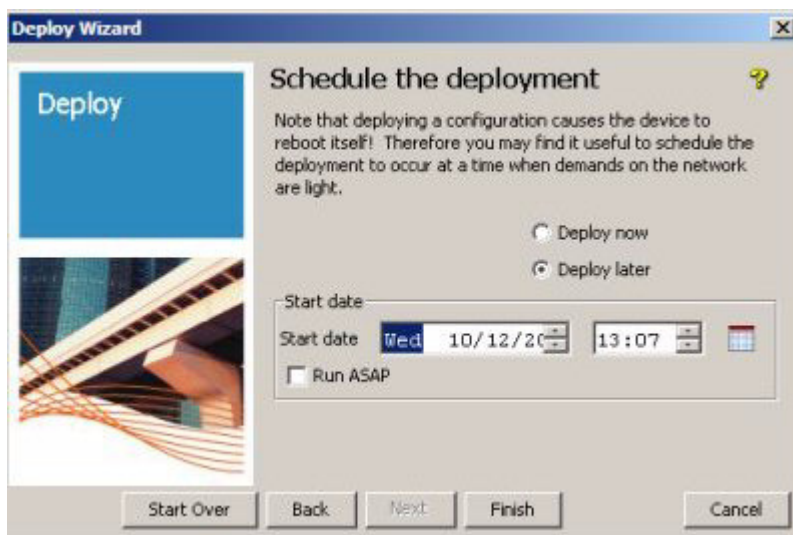


Figure 12-13. Deploy Wizard, Schedule deployment dialogue.

3. Click to select the deployment schedule option:
 - Select **Deploy now** if you need to deploy the configuration immediately to correct a problem in the device. The configuration will deploy as soon as you click the **Next** button.
 - Select **Deploy later** to deploy the configuration at the date and time that you specify in the **Start date** fields.

If you selected the Deploy later option, click **Finish** to save the configuration deployment schedule and exit the wizard.

4. If you selected the Deploy now option, when you click Next the deployment status displays:

- Successful - The configuration deployed successfully.
- Deployment Failed - The configuration was not deployed due to a bad connection, nonexistent or invalid file, or invalid permissions.

Tip: Make sure that SSH is enabled on the device and SSH is the preferred CLI mode using the Communication Parameters in PCM wizard if SCP is selected as the method for transfer of configuration files.

- Configuration files identical - No changes are made because the configuration file on the device is identical to the configuration deployed.

Click **Close** to exit the Deploy Wizard.

Tip: To apply a known good software configuration from one network device to another, you can copy the software configuration text from the Configuration detail display, then paste the copied text in the "Deploy Wizard: Edit" dialog.

Using the CLI Wizard

The CLI Wizard feature in the Configuration Manager lets you issue a configuration command to multiple devices at the same time. In this way you use a "batch process" to update the configuration on all devices at once, instead of having to update each device separately.

To issue a command to multiple devices using the CLI Wizard,

1. Select the devices in the Devices List or Configurations list display.
2. Select the CLI option from the Device Configuration toolbar menu to launch the CLI wizard.

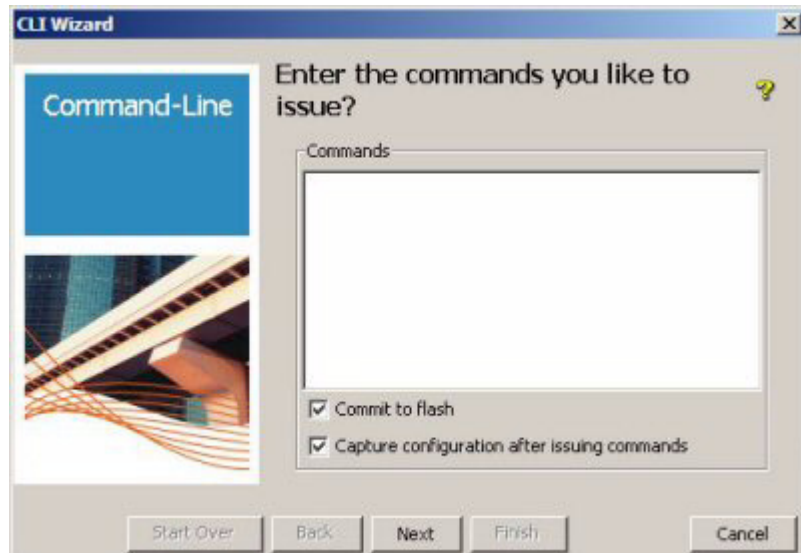


Figure 12-14. CLI Wizard, Commands dialogue

3. Click in the text box and type the configuration **Commands** you want to apply.

You can enter any mixture of commands or "show" commands. The commands will be executed in the order entered. Care should be taken when issuing commands that change an IP address or commands that will cause a device to reboot.

4. The **Commit to flash** option is essentially a "write memory" command that will commit commands to the startup configuration.

The **Capture configuration...** option tells Configuration Manager to automatically scan the device to capture the configuration after the commands are issued. This option also issues a "write memory" command.

Click the check box to deselect these options. A check mark indicates the options are enabled.

5. Click **Next** to continue.:

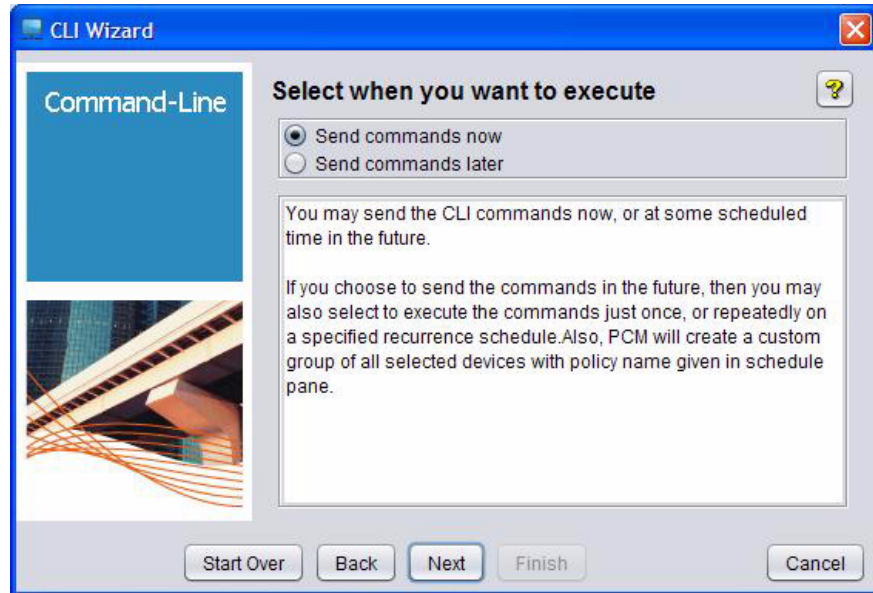


Figure 12-15. CLI Wizard, Select when to execute dialogue

6. Select when you want to execute the CLI commands:
 - Select **Send commands now** if you want to execute the commands immediately to repair a problem or improve performance.
 - Select **Send commands later** to send commands at a time when the impact to network performance will not be a problem.
7. Click **Next** to continue.

If you selected the Send commands now option, the CLI Wizard will display a monitor of the command status. You can enlarge the monitoring window by clicking the white square.

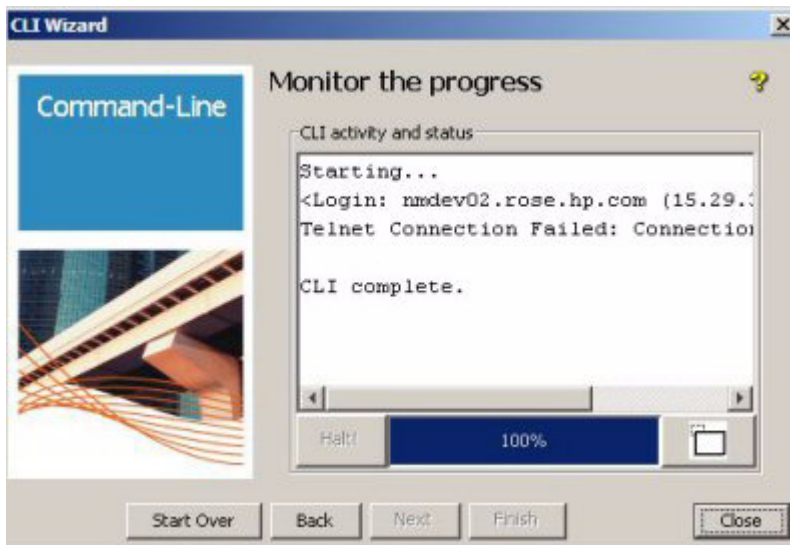


Figure 12-16. CLI Wizard, Monitor dialogue

In the Monitor dialogue, click **Halt** to stop the CLI command action. Otherwise, the monitor will display the results of each command. To view the output in an enlarged window, click the Enlarge Output Window button.

Note:

If you issue commands to multiple devices using the CLI Wizard, it issues the commands to five devices at a time, in parallel, until all devices are configured. You can alter the number of devices with the Performance Tuning parameters in the Global Preferences for Configuration Management. See page 12-55 for details.

If you selected the Send commands later option, when you click **Next** a scheduling dialogue is displayed.

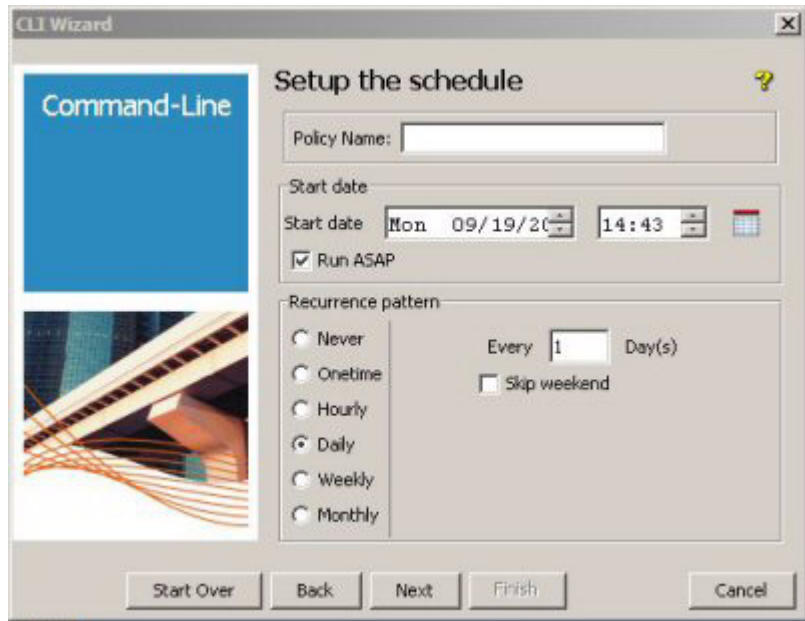


Figure 12-17. CLI Wizard, Schedule setup dialogue

8. Type a **Policy Name** under which the CLI commands will be stored.

Enter the **Start date** and time, and the recurrence pattern if you want to repeat the commands at scheduled intervals.

- | | |
|----------|---|
| Never | No further action is required (Policy definition is saved, but will not be enforced). |
| One time | No further action is required (the currently scheduled time is used with no recurrences). |
| Hourly | Type the number of hours and minutes to wait between executing commands. If you do not want the commands executed on Saturdays and Sundays, check the Skip weekend check box. |
| Daily | Type the number of days to wait between enforcements. If you do not want the commands enforced on Saturdays and Sundays, check the Skip weekend check box. |

9. Click **Next** to continue.

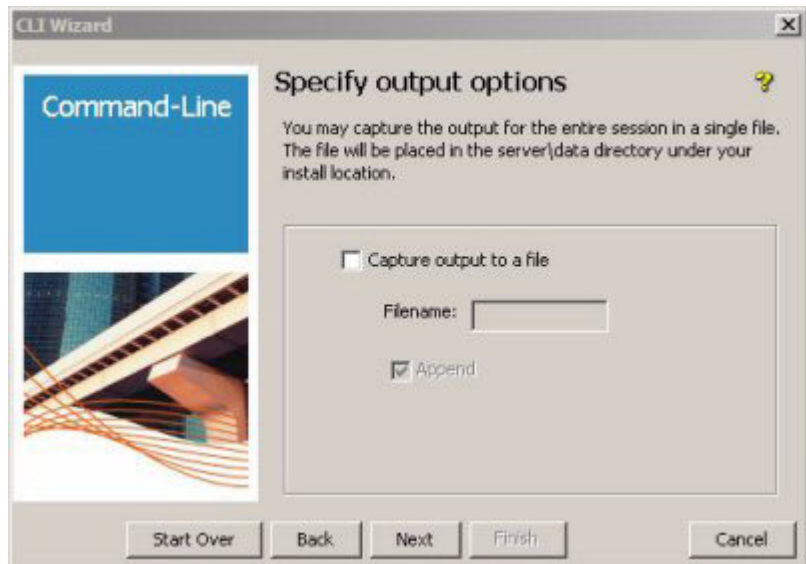


Figure 12-18. CLI Wizard, Output Options dialogue

10. Select the Session Output options:
 - a. If you do not want to capture the output for the session, click **Next** to close the "Specify Output Options" window.
 - b. Click the **Capture output to a file** check box to capture the output for the session.
 - c. Type the **Filename** in which to store the output.
 - d. Click the **Append** check box to append the next session output to previous output if the file already exists.

To overwrite an existing file, ensure that the Append check box is not checked.
 - e. Click **Next**. The Show Selected devices dialogue is displayed, with the list of devices to which the CLI commands will be applied.

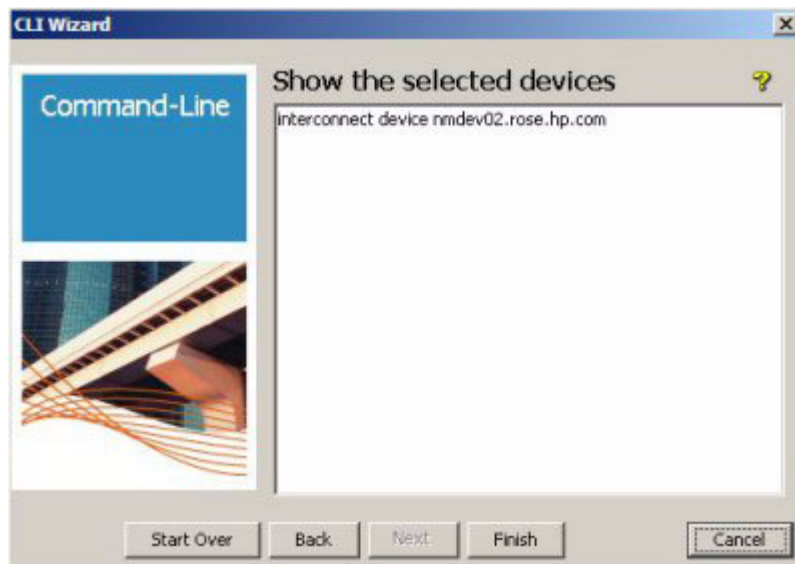


Figure 12-19. CLI Wizard, Show Selected Devices dialogue

11. Click **Finish** to exit the CLI Wizard, or **Start Over** to return to the Commands dialogue and issue additional commands.

Using Configuration Templates

The Configuration Templates tab displays an overview of configuration templates. These templates can be deployed to a single device, or to a predefined or custom group of devices of the same type. You can also apply configuration templates using a Policy to automatically configure all devices that use the same configuration syntax. For example 1600m, 2400, 2424, 4000m and 8000m models use a common configuration file syntax.

For information on using Configuration Templates to automatically configure newly discovered devices, refer to “Using the Deploy Configuration Wizard” on page 12-16.

The Configuration Templates tab displays the templates associated with the selected device Group, with the following information:

Template Name	Name assigned to the template
Description	Brief description of the template
Policies	Number of policies currently using the template

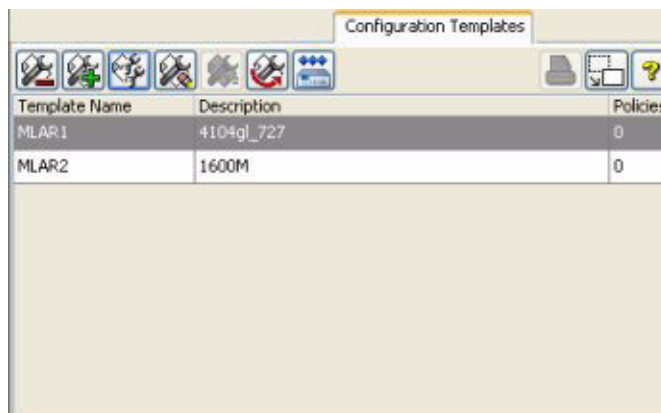


Figure 12-20. Configuration Templates tab view

You can access the following functions from the Configuration Templates tab.

- Open the Configuration Template Wizard (with no default values) to create a new device configuration template.
- Open the Configuration Template Wizard with values copied from another template so you can easily create a template similar to another template
- Modify configuration templates. See "Using the Configuration Template Wizard" for additional information.
- Manage IP Pools (See below)
- Delete configuration templates.
- Compare configuration templates
- Deploy a configuration template to a device or group of devices.

Comparing Configuration Templates

The Compare Configuration Templates function is used to compare software configuration templates. It works similarly to the Compare Device Configurations function described on page 12-14.

To compare two configurations templates:

1. Select a device group in the navigation tree to display the Devices window, then click the Configuration Templates tab.
2. Select two configuration templates from the listing in the Configuration Templates display.
3. Click the Compare Templates button in the window toolbar.
4. Ensure that the configuration templates listed in the Template Difference Viewer are the ones that you want to compare, then click **Compare!**
5. The default display is Side-by-side, that is with one configuration template in the right side and the other on the left. Differences in the software configuration are highlighted with red and blue text.



As with Device configurations, you can change to the Inline View, and set the display to view only the differences between the two configuration templates.

Using IP Address Pools

If you plan to deploy a configuration template to multiple devices, a static IP address cannot be used in the template. Instead, you must use an IP_POOL statement to assign IP addresses to devices configured by the template.

The syntax for the IP_POOL statement is

```
<IP_POOL=PoolName, ADDRESS, "User Comment" >
```

Where:

PoolName

Is the name of the IP address pool you want to use, or a question mark (?). You can also leave the first field blank.

The pool name is limited to alphanumeric characters (a-Z and 0-9) and the underscore (_). Other special characters and spaces are not allowed.

Type a question mark or leave the first field blank to assign an IP address pool in a later wizard step, which is especially helpful when the IP address pool will be created in a later step.

User Comment

Is a descriptive comment, enclosed in quotation marks. There is no restriction on the length of a comment, however the comment cannot contain embedded quotation marks and the statement must fit on one line.

An IP_POOL statement can contain blank spaces between elements. However, the entire statement must be a single line. That is, the opening "<" must be on the same line as the closing ">."

You can use the IP Pool Manager and IP Pool Configuration functions to create and manage IP Pools for use in configuration templates.

IP Pool Manager

Use the IP Pool Manager to review IP Pool information used for configuration templates, and to access the functions for creating, modifying or deleting IP Pools. An IP address pool provides a list of IP addresses that are used to automatically assign IP addresses to devices when configuration templates are deployed. This is especially helpful when new devices are discovered.



Click the IP Pool Manager button in the Configuration Templates toolbar to launch the IP Pool Manager window.

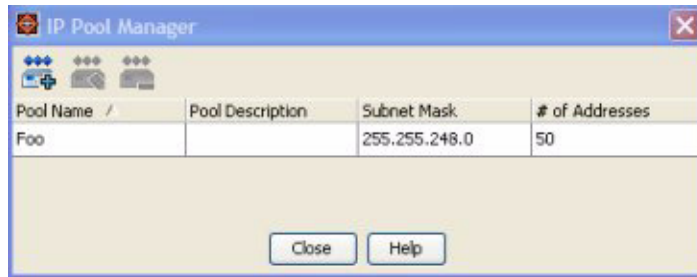


Figure 12-21. IP Pool Manager display

This IP Pool Manager window provides the following information for each defined IP pool:

Pool Name	The name assigned to the IP address pool
Pool Description	: A brief description of the IP Pool
Subnet Mask	The Subnet Masked used for all IP addresses in the pool.
# of Addresses	The number of unassigned IP addresses in the IP pool. When configuration templates that use the pool are deployed, this number decreases as unique IP addresses are taken out of the pool and added to software configuration files. A second entry will appear in the list for the remaining available IP addresses in the pool.

When the number of available IP addresses in a pool drops below 10, a warning event is issued. When the number of available IP addresses in a pool drops below 3, a major event is logged.

Configuring IP Address Pools

To add an IP Pool:



1. Click the Add IP Pool button in the IP Pool Manager toolbar to launch the IP Address Pool Configuration window.

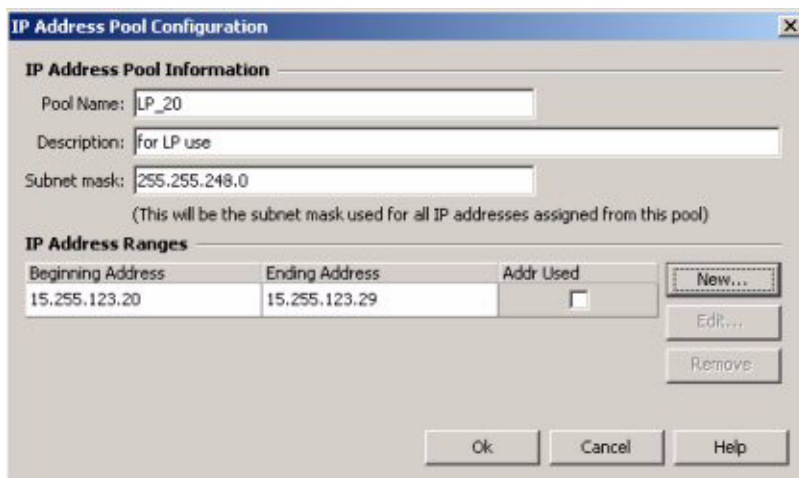


Figure 12-22. IP Pool Manager, Address configuration

The IP Address Pool Configuration can also be launched from within the Configuration Template Wizard.

The IP Address Pool Configuration window is used to create or modify an IP address pool. This window also identifies whether the IP addresses in a Pool have been assigned to devices. When the check box in the Address Used column next to an IP address range contains a check, then the IP addresses in that range are already in use. This can result in the original IP address range being split into two lines, one for the IP addresses already in use, and one for IP addresses in the pool that are still available to be assigned.

Note:

You can change an IP address from available to unavailable by checking the Addr Used check box.

2. In the **Pool Name** field, type the name you want to assign to the pool.
3. Type a **Description** identifying how the pool of IP addresses will be used. An entry in this field is optional.
4. Type the **Subnet mask** that will be used with the IP Addresses in the pool. IP address ranges cannot cross the subnet boundary defined by the subnet mask.
5. To enter the IP addresses to be included in the pool, click the **New** button. This launches the Configure IP address range dialogue.



Figure 12-23. IP Pool Manager: Configure IP address range.

- a. In the **Beginning IP Address** field type the lowest IP address in the range,
- b. In the **Ending IP Address** field type the highest IP address in the range.
- c. To assign a single IP address to the pool, type the IP address in the Beginning address field. (Leave the Ending address field blank.) All IP addresses you enter must be within the subnet mask range.
- d. Click **Ok** to close the dialogue. The new IP range displays in the list in the IP Pool configuration window.

Repeat the process if you want to use more than one range of IP addresses in the Pool.



6. To modify an IP address range, select the range in the list, then click the Edit button to launch the Configure IP address range dialogue and change the desired value.



7. To delete an IP address range, select the address or address range and click the Delete button.
8. When you are finished configuring the IP addresses pool, click **OK** to save the IP pool configuration and close the window.
9. The new IP Pool appears in the IP Pool Manager window, and will be available in the IP Pools listing in the Configuration Template Wizard.

Using the Configuration Template Wizard

To assist you in creating device configuration templates, PCM provides a Configuration Template Wizard. The method used to launch the Wizard is based on how you want to create the template.

- To create a template based on an existing device configuration:



- Select the Device in the Navigation Tree or the Devices list.
- Select Config Manager > Create Template from the toolbar, or using the right-click menu.

Note:

A successful configuration scan must be performed on the device in order to use it for creating a Configuration Template.

- To create a new template based on an existing configuration template:



- Select the Device group node to display the Device Group window, then select the Configuration Templates tab.
- Select the Template in the list displayed, then click the Create template by Copying button in the toolbar.

- To create a completely new template, simply click the Create Template button in the Template Configuration toolbar.

The following steps define the template configuration process using the wizard.

1. Click **Next** in the Welcome window to go to the Template Name window.

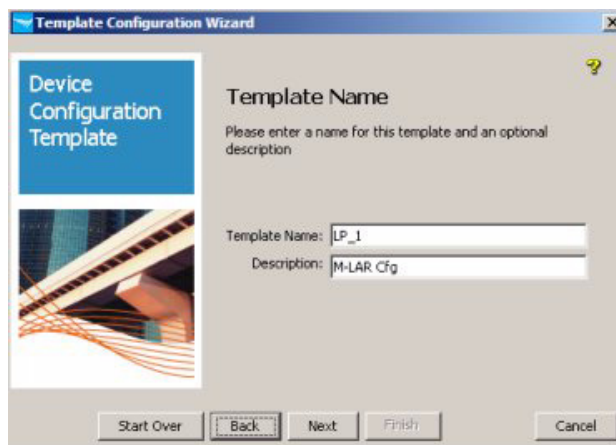


Figure 12-24. Device Configuration Template, assign name

2. Type a **Template Name** for the Configuration Template, and if desired, enter a brief **Description** for the template.
3. Click **Next** to continue to the Template Configuration window.

The contents in the window will vary based on the configuration method you selected.

- If you are creating a template from a selected device configuration, or using "Copy from Existing Template" function, the configuration for the selected device or template will be displayed.
- If you are creating a new template, the configuration pane will be blank.

The Template Configuration Data window in the Wizard lets you enter or modify the configuration. Except for IP addresses, entries must conform to the syntax and semantic rules for the target class of device. See "Comparing Configuration Templates" on page 12-27 for details on IP Address statement syntax and creating IP Pools for use in configuration templates.

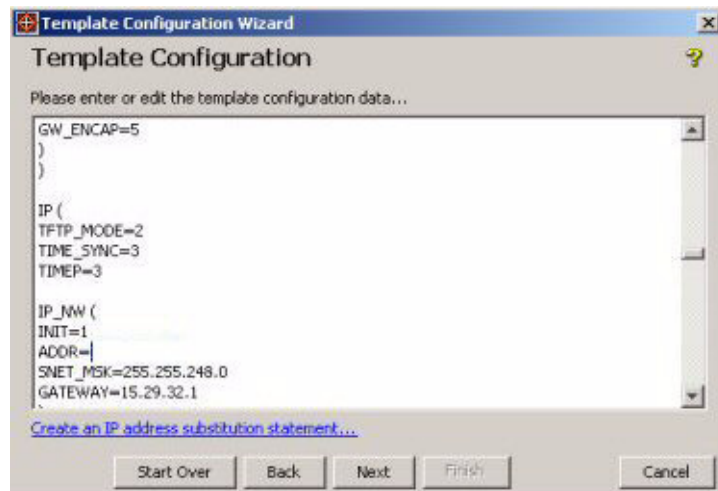


Figure 12-25. Device Configuration Template, template configuration

4. Modify the existing configuration data as desired, or
Type the configuration details for the template.

5. To insert an IP address substitution statement in the template, place your cursor in the configuration window where the IP Address statement should go, then click the link. This will launch the IP Address Substitution dialogue.



Figure 12-26. Configuration Template, IP Address substitution

- a. Select the **IP Pool Name** from the drop-down menu, then enter a comment if desired. The **Comment** is included in the IP Address statement in the configuration file.
- b. If the IP Pool is not found in the drop-down menu, you can click the link to **Create a new IP address Pool**. This will launch the IP Pool Configuration window, described on page 12-29.
- c. Click **OK** to close the Address Substitution dialogue and return to the Configuration window. The substitution statement appears in the configuration template, similar to the following example.

```
ADDR=<IP_Pool=FOO, ADDRESS, "Use of IP Pool Example">
```

Repeat Step 5 for each IP Address substitution needed in the template.

6. When the configuration data is complete, click **Next** to continue.
 - If you did not include an IP address substitutions in the template, the Summary Window displays. Go to step 8 for details.
7. If you included an IP address substitution, the Review IP Address Pools window displays.



Figure 12-27. Configuration Template, Review IP address pool

The review window shows the Pool Name, number of IP Addresses available in the pool, and any Comment entered for the IP address substitution. Review the information to make sure you are using the correct IP address pool for each statement. If any are incorrect, use the drop-down list to select the correct pool name.

- Click the **Create a new IP Address pool** link to launch the IP Address Pool Configuration window. (See page 12-29 for details on using this window.)
 - Click the **Show IP address pools** link to launch the IP Pool Manager window to review other possible IP pools.
8. Click **Next** to continue. The Summary window displays.

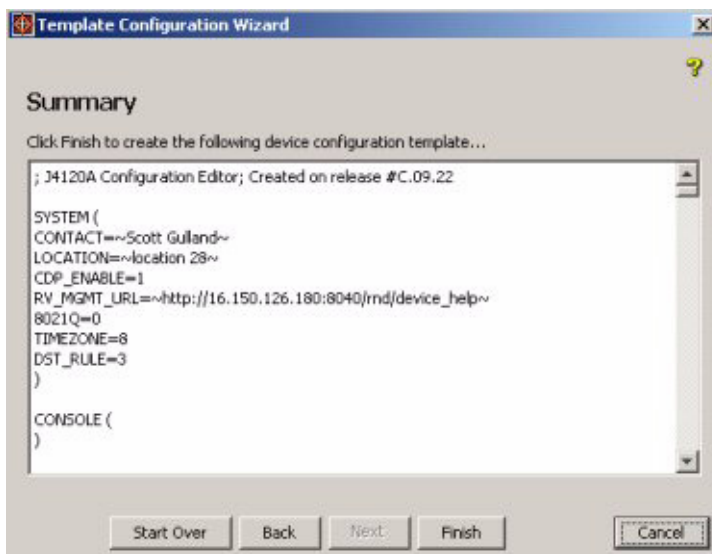


Figure 12-28. Configuration Template Summary display

9. Review the configuration template to ensure it is correct, then click **Finish** to save the template and exit the Wizard.

Click **Cancel** to exit the Wizard without saving the template.

Click **Back** to return to the previous window in the Wizard.

Click **Start Over** to return to the start of the Wizard, without cancelling the configuration.

To modify a configuration template:

1. Select a device group in the navigation tree to display the Devices window, then click the Configuration Templates tab.
2. Click the Modify template button in the toolbar to launch the Configuration Template Wizard and edit the configuration as needed. See “Using the Configuration Template Wizard” on page 12-32 for details.



To delete a configuration template:

1. Select a device group in the navigation tree to display the Devices window, then click the Configuration Templates tab to see the templates associated to the selected device group.
2. Select the Template from the list, then click the Delete template button in the Configuration Templates toolbar.



Applying Configuration Templates to Devices

A powerful feature of configuration templates is the ability to automatically configure new devices as they are discovered by PCM. To use this feature:

1. Create a configuration template for the class of devices (device group) that you want to have configured automatically when they are added (and discovered) on the network.
2. Before connecting the new device to the network, set the Contact or Owner field on the device to the following:

<PCM_Template=templatename>

Where templatename is the name of template you created in step 1 above.

3. Set up minimal connectivity information using DHCP or a temporary static IP address and connect the device to the network. When a device is discovered, PCM will automatically deploy the configuration template on the device.

Using the Deploy Template Wizard

You can also apply a configuration template to device(s) on the network at any time using the Deploy Template wizard.

1. Select the device in the Navigation tree or the Devices list.
2. Using the toolbar buttons or right-click menu, select Config Manager > Deploy Template to launch the Deploy Template Wizard.

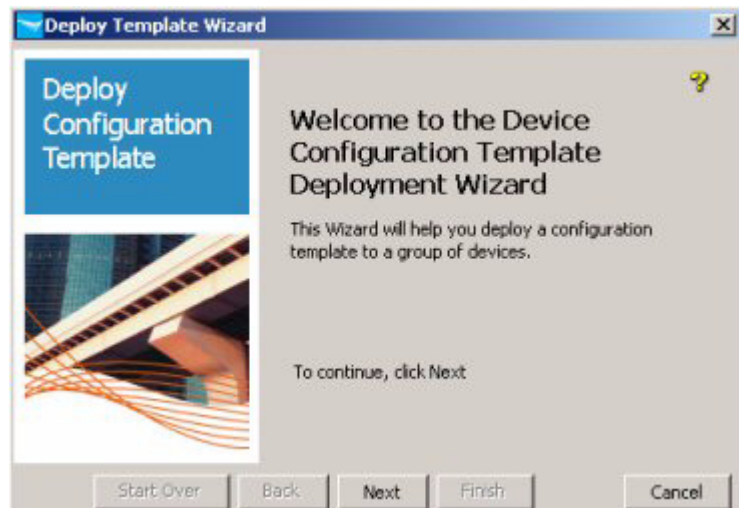


Figure 12-29. Deploy Configuration Template wizard

3. Click **Next** to continue to the template selection.

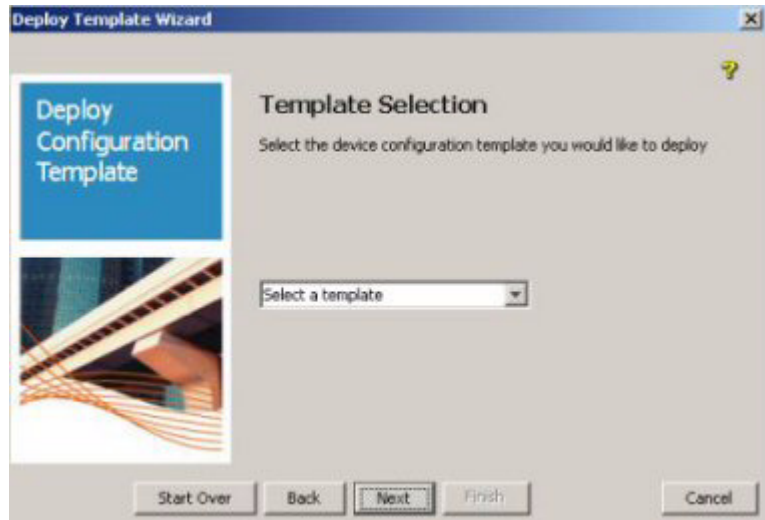


Figure 12-30. Deploy Configuration, template selection

4. Select a configuration template to deploy from the pull-down menu.
Click **Next** to continue to the deployment schedule selection.



Figure 12-31. Deploy Configuration, select deploy time

5. In the When would you like to deploy? dialog:
 - If you select **Deploy Now**, the configuration template will be applied to the device immediately. (after the file transfer method is selected)
 - If you select **Deploy Later**, you need to set the date and time (schedule) for when the template will be applied to the device.

Deploying a configuration template causes the device to reboot. Use Deploy Later if you do not want the device rebooted at the current time.

In the Set Policy Info and Deploy Schedule dialog, enter a Policy name and the Start date (date and time) you want to deploy the configuration.



Figure 12-32. Deploy Configuration, Set schedule for deployment

6. Click **Next** to continue to the configuration file transfer selection.

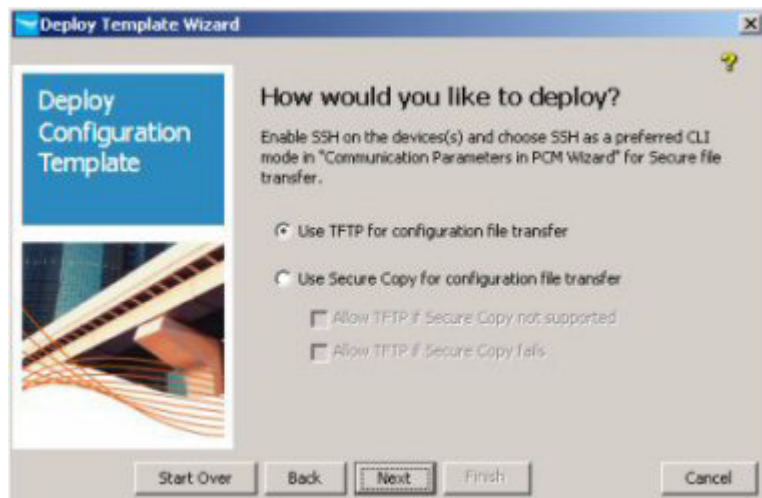


Figure 12-33. Deploy Configuration Template: file transfer selection

7. Select the file transfer method to use for transferring the configuration text from the device to PCM:
 - The default method for configuration file transfer is based on what is defined in Global Preferences for Configuration Management. At initial PCM installation, the default is "Use TFTP for configuration file transfer".
 - You can change the mode of transfer for this particular run of the Scan Wizard by selecting "Use Secure Copy for configuration file transfer". Secure Copy (SCP) works with SSH v1 and SSH v2 to provide a more secure file transfer method between PCM and the managed switch.
 - If you are unsure whether all the devices in your network support the use of SCP, select the Allow TFTP if Secure Copy is not supported, and Allow TFTP if Secure Copy Fails options. If Allow TFTP failover options are not set, the scan configuration operation will report errors if SCP is not supported on the target device.

Enabling SCP modifies the device's configuration the first time it is scanned. The option to use TFTP as a failover mode of configuration scan applies to one single run of the scan wizard. However, if you use this feature, every switch between TFTP and SCP subsequently modifies the configuration again.

Note: If a switch is configured to use either RADIUS or TACACS+ for authenticating a secure SSH session on the switch, you cannot enable SCP. The switch displays an error message if there is an attempt to configure either option when the other is already configured.

8. Click **Next** to continue.

If you chose to Deploy Now (or set the Deploy Schedule for ASAP) a confirmation dialog displays.

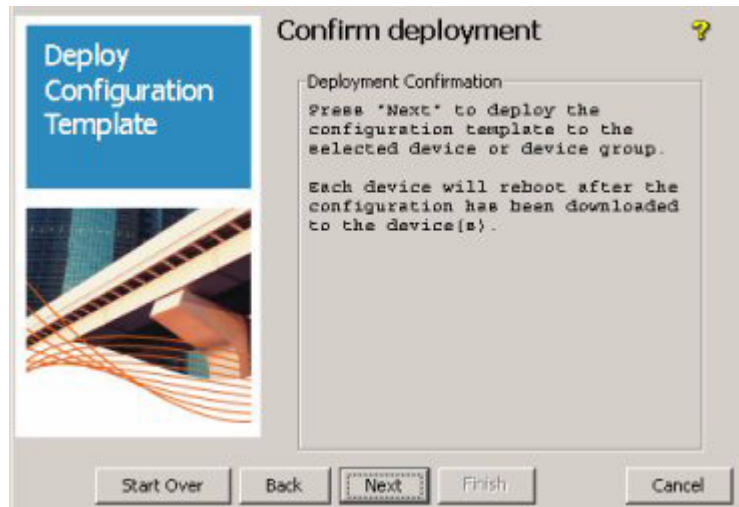


Figure 12-34. Deploy Configuration Template, confirmation dialog

9. Click **Next** to continue to the Review screen.

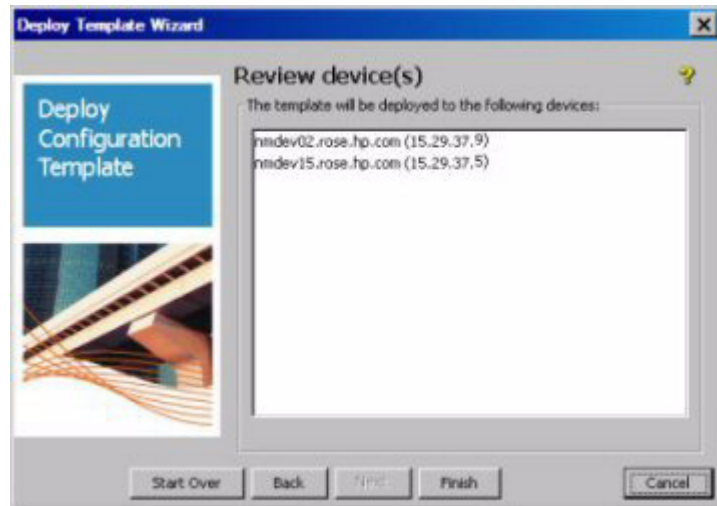


Figure 12-35. Deploy Configuration Template, target device review

10. Click **Finish** to complete the configuration template deployment.

A status window displays the progress of the deployment.

- Successful - The configuration deployed successfully.
- Deployment Failed - The configuration was not deployed due to a bad connection, nonexistent or invalid file, or invalid permissions.
- Configuration files identical - No changes are made because the configuration file on the device is identical to the configuration deployed.

Click **Close** to exit the Deploy Wizard.



An alternate method for deploying a configuration template is to go to the Configuration Templates tab, select the template to be deployed, then click the Deploy Template button in the toolbar to launch the wizard.

Exporting Device Configurations

To help you document network device configurations, you can use the Export Configurations feature in the Configuration Manager. The Export Device Configurations wizard will save a text copy of any configuration information found in the configuration history for a device. The exported files are stored in the `<install_directory>/server/config/devConfig/export` directory with a file extension of `.cfg`. You can then read and print the ASCII files using a simple text editor such as NotePad.

To export device configuration files:

1. Click the Device group node, or individual device node in the navigation tree, or select the device(s) in the Devices List tab.
2. Select the Export Configurations option in the Configuration Manager toolbar menu, or from the Configuration Manager menu off of the right-click menu.

This launches the Export Device Configurations wizard, with the list of selected devices.



Figure 12-36. Export Device Configuration Wizard, Review devices

3. Review the list of devices to be included in the configuration export, then click **Next** to begin the export operation.

Click **Cancel** to exit the wizard if you do not want to continue with the configuration export, or if the devices list is incorrect.

4. The wizard displays the status of the configuration file export process.

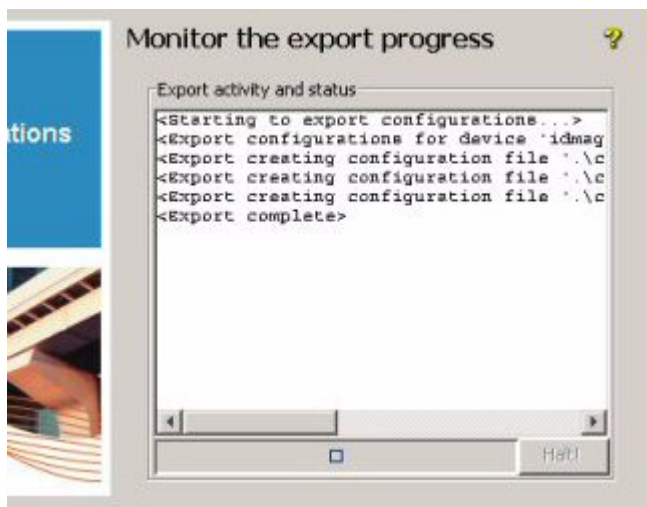


Figure 12-37. Export Configuration, export status display

You will see three files created for each device configuration:

- HwCfg.cfg: contains the device hardware configuration, including installed modules, switch fans, ports, etc.
- SwCfg.cfg: contains the switch software configuration, including SNMP settings, VLANs, port settings, etc.
- OsCfg.cfg: contains a list of the Switch OS and boot ROM versions that are installed on the device.

The exported files are stored in the `<install_directory>/server/config/devConfig/export` directory with a file extension of `.cfg`. The file names are a concatenation of the device IP address, file scan date and time, and file type. If there is more than one configuration for the device found in the configuration history, a separate file is created for each configuration.

5. After the `<Export complete>` message displays, click **Close** to exit the wizard.

Importing Device Configurations

You can save the exported configuration files to another system as part of a DRP (disaster recovery plan) or use the files to document network device configurations for audit purposes. You can also use an exported configuration as a template to create configurations for new ProCurve devices of the same type. You can import a configuration through PCM to apply the configuration to a new device, or to restore an existing device's configuration.

The Import Device Configurations wizard lets you import an ASCII text file for a device configuration into the PCM configuration history database. The configuration files to be imported must use the standard configuration file naming conventions:

```
IPAddr_Date_Time_Type.cfg
```

where:

- `IPAddr` = the IP address for the device, with the "." replaced by an underscore "_".
- `Date` = The date the configuration was captured or created, given in YYYYMMDD format.
- `Time` = The time the configuration was captured or created, given in HHMM format. Hours (HH) uses a 24 hour clock, with digits 00 to 23.
- `Type` = The Configuration file type, one of the following:
 - `HwCfg`: contains the device hardware configuration, including installed modules, switch fans, ports, etc.
 - `SwCfg`: contains the switch software configuration, including SNMP settings, VLANs, port settings, etc.
 - `OsCfg`: contains the Firmware revision code, ROM revision code, and finally the OS revision code (not used) The file must give this information in three lines, in the order listed here. (Firmware, ROM, OS)

All files must have the .cfg file extension. The .cfg files to be imported must be copied to the `<install_directory>/PNM/server/config/devConfig/import` directory.

The contents of each file is expected to contain the device's configuration data as ASCII text, although binary data will be accepted. The maximum data size of an import configuration file is 4MB.

To import the .cfg files from the import directory into the PCM configuration history database:

1. Click a node in the navigation tree to display a tab containing the Configuration Manager menu button.
2. Select the Import Configurations option in the Configuration Manager toolbar menu, or from the Configuration Manager menu off of the right-click menu.

This launches the Import Device Configurations wizard, with the list of selected devices.



Figure 12-38. Review Import devices dialog

3. Review the list of devices to be included in the configuration import, then click **Next** to continue to the Select Import Options dialog.

Click **Cancel** to exit the import wizard if the list of devices is incomplete or incorrect.

4. In the Select Import Options dialog, click the check box to select the Delete existing device scan configurations option.

This will delete all of the preexisting scanned configurations for a device prior to importing new configuration data from the import directory. This allows you to avoid the case where you want to import a configuration, but that system has a configuration (via configuration scan) that is newer than the configuration being imported, which would prevent the import of the configuration data. The device's preexisting scanned configurations are only deleted if one or more import files are found for the device.



Figure 12-39. Select Import Options dialog

5. Click **Next** to continue the configuration import.

The wizard displays the status of the configuration file import process.

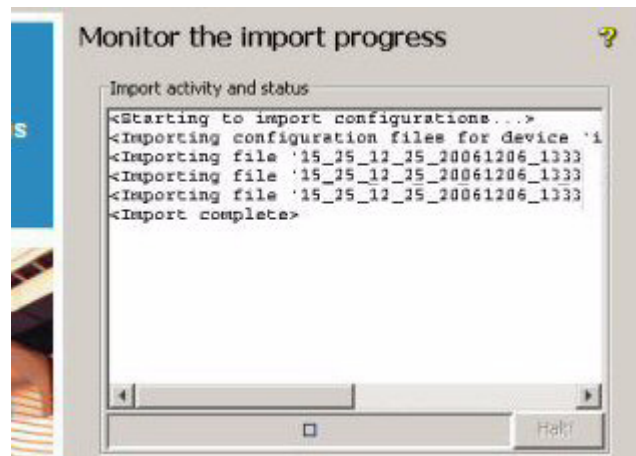


Figure 12-40. Import Configuration Wizard: import status dialog

When the import operation is launched, PCM will look for files in the `<install_directory>/server/config/devConfig/import` directory that have a matching IP address in their name. PCM sorts the device files by date and time and reads them in from oldest to newest, storing each file's data as the configuration for the device and using the date and time information for the imported file as the scan time and date.

You will see up to three files imported for each device configuration:

- `HwCfg.cfg`: contains the device hardware configuration, including installed modules, switch fans, ports, etc.
- `SwCfg.cfg`: contains the switch software configuration, including SNMP settings, VLANs, port settings, etc.
- `OsCfg.cfg`: contains a list of the Switch OS and boot ROM versions that are installed on the device.

PCM will only import the file if its date is newer than the latest configuration information stored in the PCM database. If the date of the import files are older than the last configuration a failure message is displayed for the file import.

6. After the `<Import complete>` message displays, click **Close** to exit the wizard.

When reviewing the device configuration history, the Comment column will show that the configuration file is "imported".

Using the Software Licensing Feature

For those ProCurve Devices that support the use of premium software that requires registration of the software license, you can use the License Software wizard to automatically register the switch software license on the "My ProCurve" Web site.

To use the PCM Software Licensing feature:

1. Right-click the device in the Devices List, or the device Node in the Navigation tree.
2. Select Config Manager > License Software. This launches the License Software Wizard.



Figure 12-41. Premium Switch Software Licensing wizard

3. Click **Next** to continue to the Enter Your License Information window.



Figure 12-42. Switch Software License Information

4. Enter the License information:
 - a. Select a **Package** from the pull-down menu.
 - b. Type (or paste) the **Registration ID** that you received when the software was purchased.
 - c. Type a brief **Description** for the license, which will appear in the "My ProCurve" portal window. This is optional, not required.
 - d. Click the check box if you want to **Save device configuration changes** before the device is rebooted. (When the License information is updated, the device is rebooted and any configuration changes are saved in the device's flash memory).
5. Click **Next** to continue to the license confirmation window.

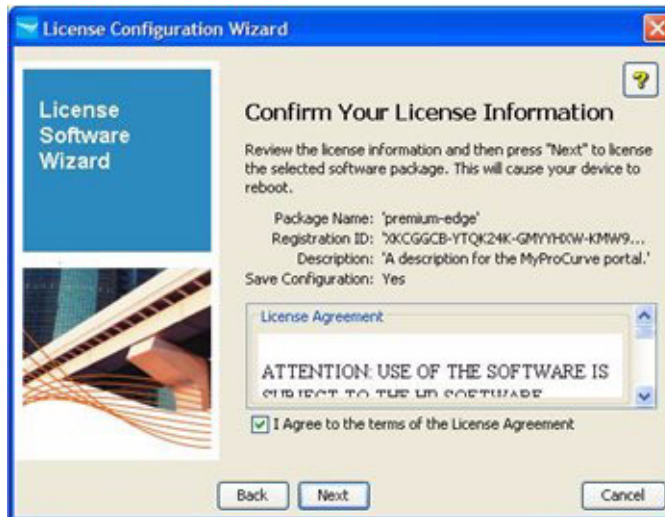


Figure 12-43. Switch Software License Confirmation

6. Review the Registration ID and License Agreement, then click the check box to indicate **I agree to the terms of the License Agreement**.
7. Click **Next** to continue to the Monitor license deployment window.



Figure 12-44. Switch Software Licensing, deployment status display

8. The window displays the progress as the license is deployed to the device. When Licensing is complete, click **Finish** to exit the wizard.

Using the PCM Software Unlicensing Feature

Over time, you may need to move your licensed software from one device to another. In order to do this, you need to first "unlicense" the software on the device where it was originally installed.

1. Right-click the device in the Devices List, or the device Node in the Navigation tree.
2. Select Config Manager > Unlicense Software. This launches the Unlicense Software Wizard.

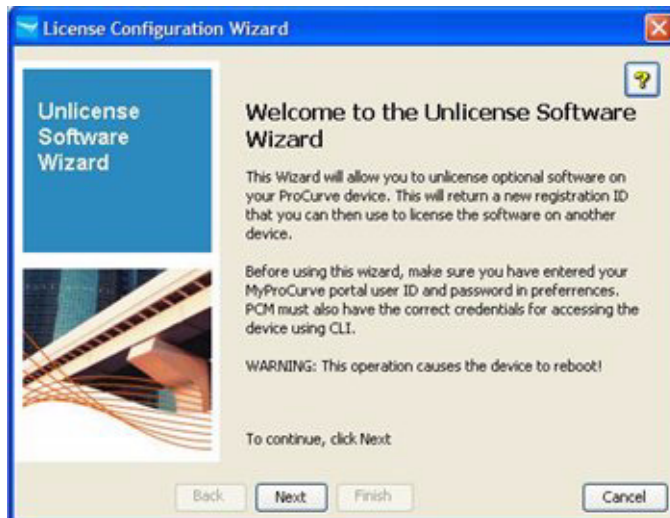


Figure 12-45. Premium Switch Software, Unlicense Software wizard

3. Click **Next** to continue to the Enter Your Unlicense Information window.

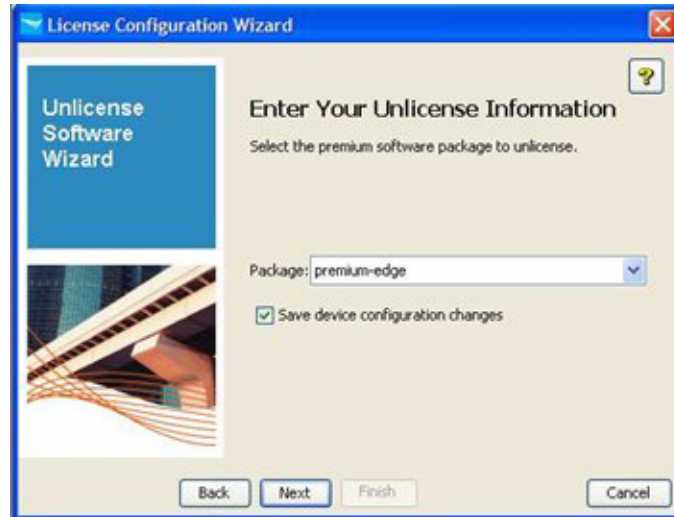


Figure 12-46. Switch Software Unlicense Information

4. Enter the Unlicense information:
 - a. Select a **Package** from the pull-down menu.
 - b. Click the check box if you want to **Save device configuration changes** before the device is rebooted. (When the License information is updated, the device is rebooted and any configuration changes are saved in the device's flash memory).
5. Click **Next** to continue to the Unlicense confirmation window.

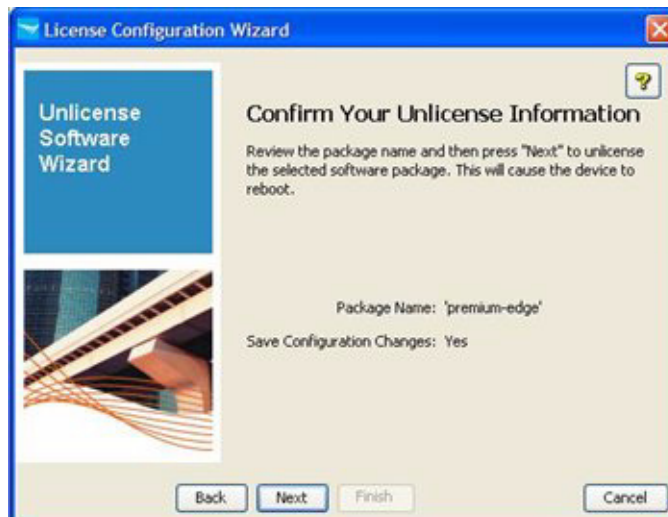


Figure 12-47. Switch Software, Unlicense Confirmation

6. Click **Next** to continue to the Monitor unlicense progress window.

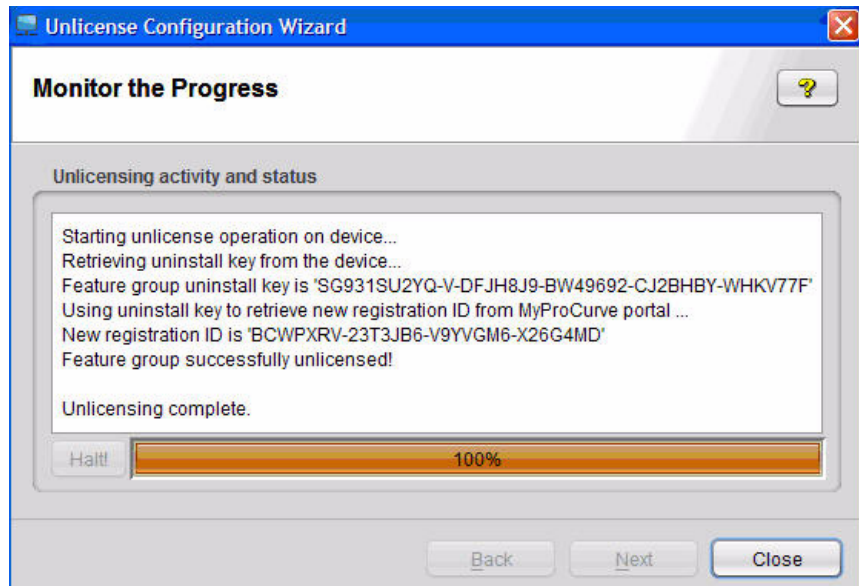


Figure 12-48. Monitor Progress of Software Unlicensing

7. The window displays the progress as the unlicensing operation is performed on the device. When Unlicensing is complete, click **Close** to exit the wizard.

Configuration Management Preferences



To set the Configuration Manager preferences, click the Preferences button in the global toolbar, then select (click) the Configuration Management option in the Global menu.

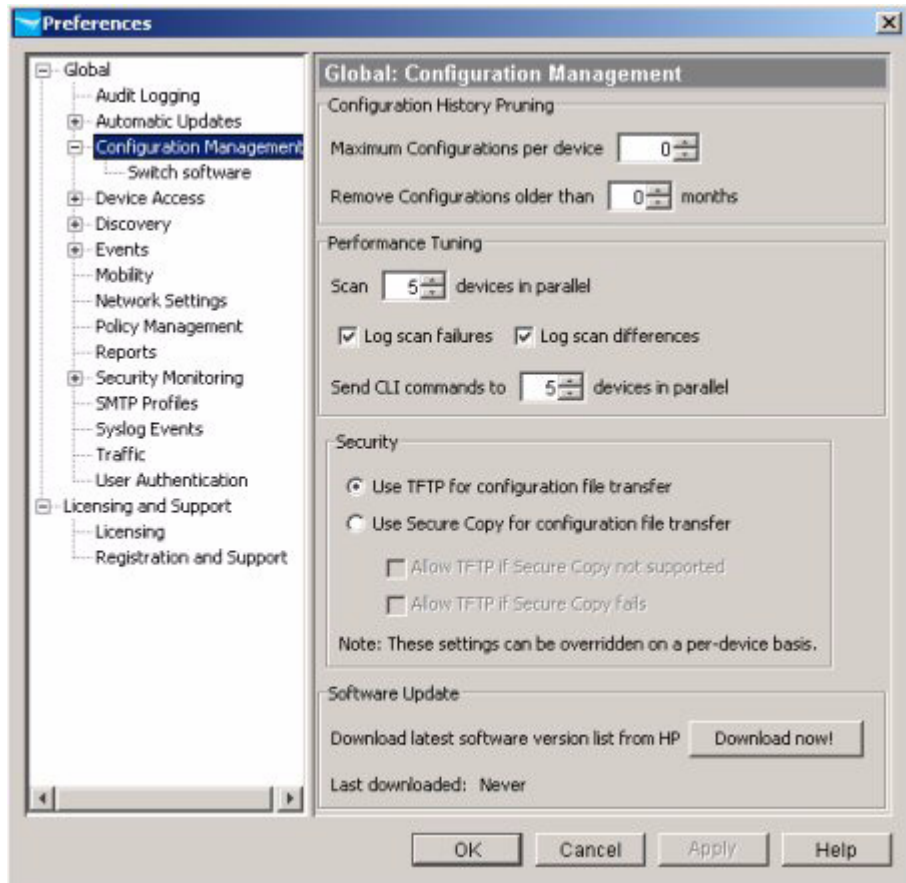


Figure 12-49. Global Preferences:Configuration Management settings

- You can type changes to the Configuration History Pruning and Performance Tuning parameters, or use the buttons to increase or decrease the parameters.

The default entry for **Maximum Configurations** is 0, which allows an unlimited number of configuration. If you set a non-zero value, an attempt is made once per day to reduce the number of saved configurations to the specified value by deleting the oldest configurations.

The **Remove Configurations** default of 0 indicates that no configurations will be removed.

The **Log scan failures** option is used to log an entry in the Events browser when a configuration scan fails. The event source is Configuration Manager, and severity is Informational. The **Log scan differences** option is used to log an entry in the Events browser whenever a device configuration changes.

The **Send CLI commands to** option indicates the maximum number of devices to which CLI commands can be deployed at the same time. The default is **5**. Use the buttons to increase or decrease the allowed number of devices.

- The Security section lets you select the default file transfer method you want to use for transferring sensitive switch configuration files between the switch and PCM.

The default preference is **Use TFTP for configuration file transfer** to transfer configuration files between the switch and PCM.

Click to select the **Use Secure Copy for configuration file transfer** option to make Secure Copy (SCP) the default configuration file transfer method. SCP is an implementation of the BSD `rep` (Berkeley UNIX remote copy) command tunneled through an SSH connection. SCP works with SSH v1 and SSH v2 to provide a more secure file transfer method.

Note:

If a switch is configured to use either RADIUS or TACACS+ for authenticating a secure SSH session on the switch, you cannot enable SCP. The switch displays an error message if there is an attempt to configure either option when the other is already configured.

If you are unsure whether all the devices in your network support the use of SCP, select the **Allow TFTP if Secure Copy is not supported**, and **Allow TFTP if Secure Copy Fails** options. If Allow TFTP failover options are not set, the configuration scan and deploy operations will report errors if SCP is not supported on the target device.

- The Software Update section lets you get the latest switch OS versions by clicking the **Download now!** button. PCM will go out to the ProCurve support Web site and download a listing of the latest switch software versions. The Last Downloaded field will display the most recent download date and time.

Setting Preferred Switch Software Versions

The Switch Software window lets you select the software configuration version you want to use for each device type. In a preferred version is not identified, the most recent switch software version is used for software updates.

To set the preferred software configuration version:

1. Navigate to the Switch Software window.
(Tools > Preferences > Configuration Management > Switch Software)

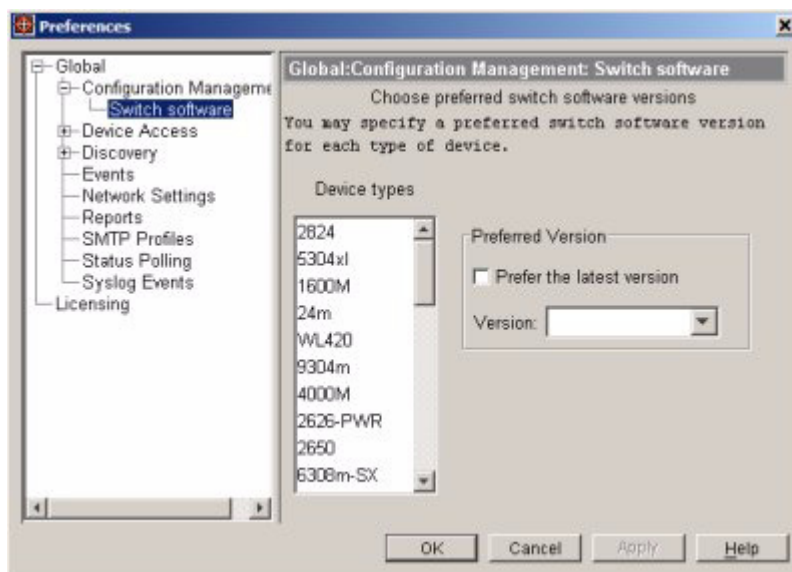


Figure 12-50. Global Preferences: Switch Software settings window

2. Scroll down the Device Types list and select the device type you want to set.
3. To use the most recent software configuration to update devices, check the **Prefer the latest version** check box.

To use a specific version, use the up and down arrow keys to select the desired version from the **Version** field.

4. Click **OK** to save the settings and close the Switch Software window.

Network (Proxy) Settings

PCM needs external Web access to retrieve the latest switch software files for ProCurve network devices from the ProCurve Web site. If the HTTP proxy was not configured at installation, or if the proxy server has changed, use the Network Settings Preferences to configure the Proxy settings.

Note:

If a firewall lies between the PCM Client and devices, the Server and Agent managing those devices can use a proxy to bypass the firewall in a secure manner. This type of proxy is configured with the Agent Manager.

1. Select Tools > Preferences > Network Settings.

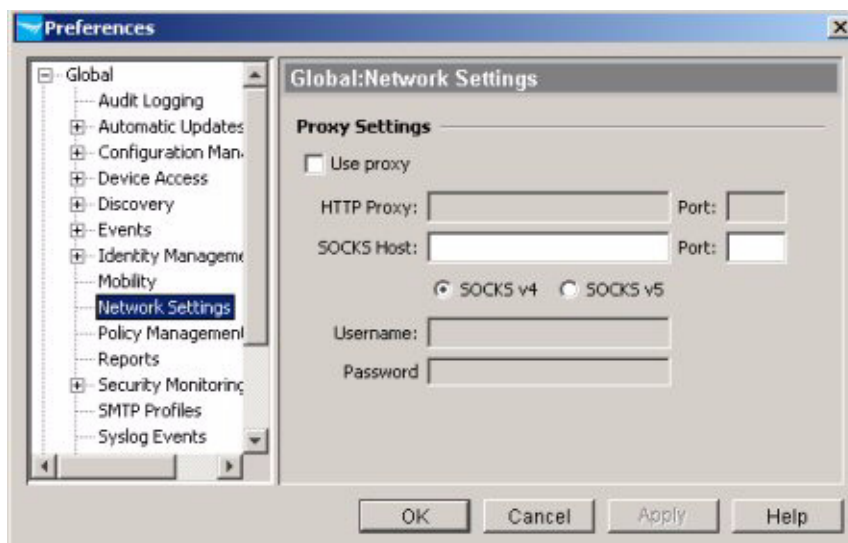


Figure 12-51. Global Preferences: Network Settings window

2. Click the **Use proxy** check box, if it is not already selected.
3. For HTTP proxy:
 - a. In the **HTTP Proxy** field, type the DNS name or IP address of the proxy server for the subnet.
 - b. In the **Port** field, type the port number used to access the proxy.

4. For SOCKS proxy:
 - a. In the **SOCKS Host** field, type the SOCKS server (host) name.
 - b. Enter the **Port** number used to access the SOCKS server.
 - c. Click to select the SOCKS version to use. (**SOCKS v4** or **SOCKS v5**).
 - d. For SOCKS v5 enter the **Username** and **Password** used to access the SOCKS host.
5. Click **OK** to save the network settings and close the window.

Updating Switch Software

HP provides periodic software updates for ProCurve switches via the ProCurve Support Web site. You can use the Software update feature in PCM to automatically download and apply updates to devices at scheduled times.

Downloading the Software Version List

When you review the Configurations listing, the "Version" column in the display indicates whether the device is running the preferred switch software version (by default the most recent version of the software). This is done by comparing the current software version found in the MIB during the configuration scan to the current software listing and the option set in the Preferences.

To download the latest listing of ProCurve Switch Software versions:

1. Select the Configuration Management option in the Preferences menu (see Figure 12-49 on page 12-55).
2. Click the **Download now!** button in the Software Update section of the window.

This will download a listing of the current switch software revisions from the ProCurve Web site to the PCM Server.

(server/data/download/procurve_firmware.prp).

You can also sign up for the driver update notification at:

<https://my.procurve.com>

Using the Software Index File Download Policy

You can create a Policy to check for software updates, on the ProCurve Web site at scheduled intervals, and automatically download updates to the PCM Server. See Chapter 16, "Using Policy Manager Features" for details.

Scheduling Automatic Updates

To schedule devices for automatic software updates, or to edit an existing software update schedule:

1. Select an Agent Group node or Device Group node in the navigation tree
2. Select the device or devices in the Devices List or Configurations tab display.
3. Click the Software Update button in the toolbar to launch the Software Update Wizard.

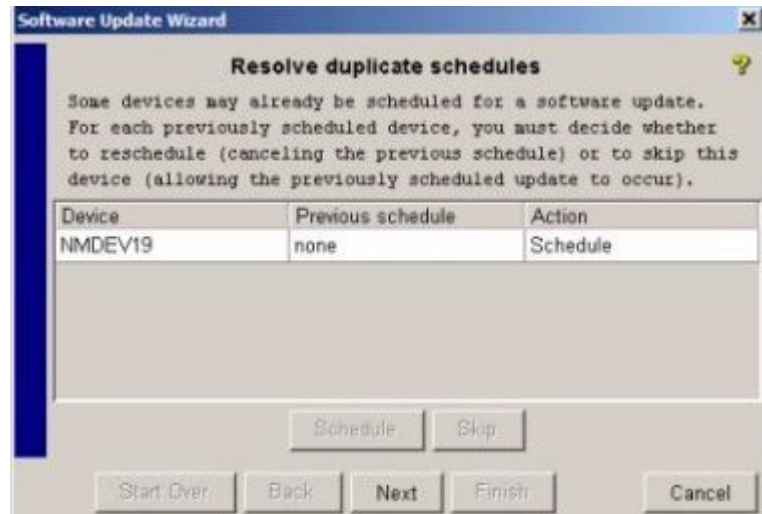


Figure 12-52. Software Update Wizard, schedule dialogue

4. Click in the dialogue to enable the Schedule and Skip buttons, then set the **Action** to Schedule or Skip (exclude) for each device.

If the devices were not previously scheduled, the Action defaults to Schedule and you can continue with no other action set up.

If you set the Action to Skip for all devices in the list, there is no other setup required. Click **Cancel** to exit the Wizard.

5. Click **Next** to display the Scan devices dialogue.

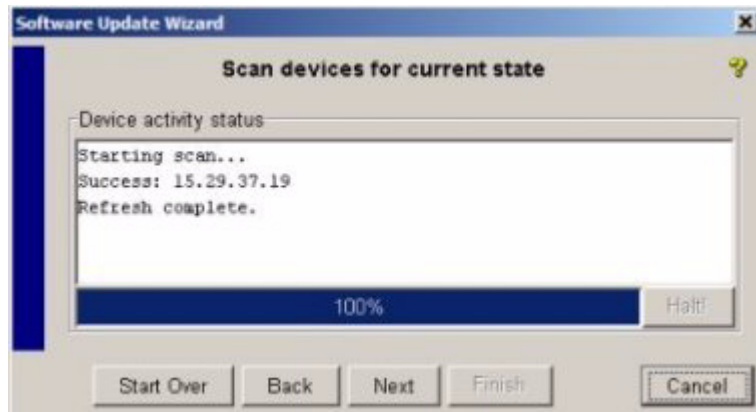


Figure 12-53. Software Update Wizard, Scan devices dialogue

The wizard will scan to get the current software state for each device.

6. When the scan (Refresh) is complete, click **Next** to display the Select Version dialogue.

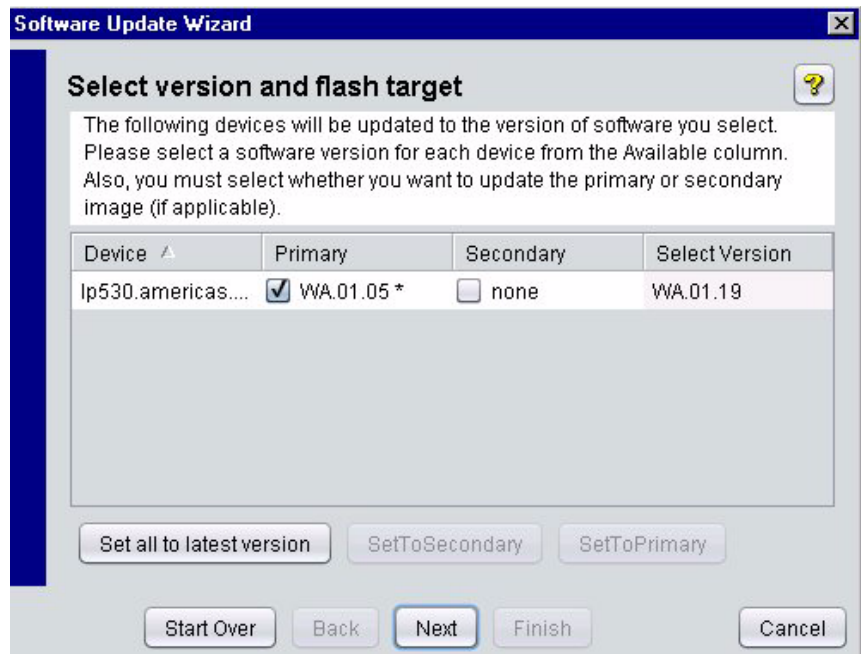


Figure 12-54. Software Update Wizard, Select version

The Primary column lists the primary software image (primary flash) found on the device. The Secondary column lists the secondary software image (secondary flash) found on the device, if any. An asterisk (*) next to the software version indicates the software image that is currently running, or "boot flash". In some cases you may use the Secondary image until you have determined compatibility between newer software versions and your existing device configuration. Note that secondary images are only available in dual image devices.

7. Click the check box to select which software image you want to update on the device, **Primary** or **Secondary**.

To update the Primary software image on multiple devices, click **Set to Primary Version**. To update the Secondary software image on multiple devices, click **Set to Secondary Version**.

8. Click the **Select Version** box to enable the software version pull-down menu, then select the version you want to upload to the device. The pull-down menu lists all software versions currently available for the device.

To update all devices to the newest software available, click **Set all to latest version**.

9. PCM will check to make sure the current switch configuration meets all prerequisites for installing the newest software version.

If the prerequisite software was found on the PCM Server but is not installed on the switch, a pop-up dialogue appears, informing you what prerequisites (BootROM version and Firmware) must be met before you can install the newest switch software version, as well as the current software version on the switch.

Click **Yes** to select and install the prerequisite software, needed before you can install the newest switch software version.

Click **No** if you do not want to update the switch software at this time.

If the software image was not found on the PCM Server, a pop-up informs you what prerequisites (BootROM version and Firmware) are needed, what the currently installed software version is, and that the pre-requisite software needs to be acquired from HP.

Click **OK** to close the dialogue.

If you selected the Set all to latest version option, any prerequisite software will be installed and the latest version will be applied to the switches.

10. Click **Next** to display the Setup dialogue.

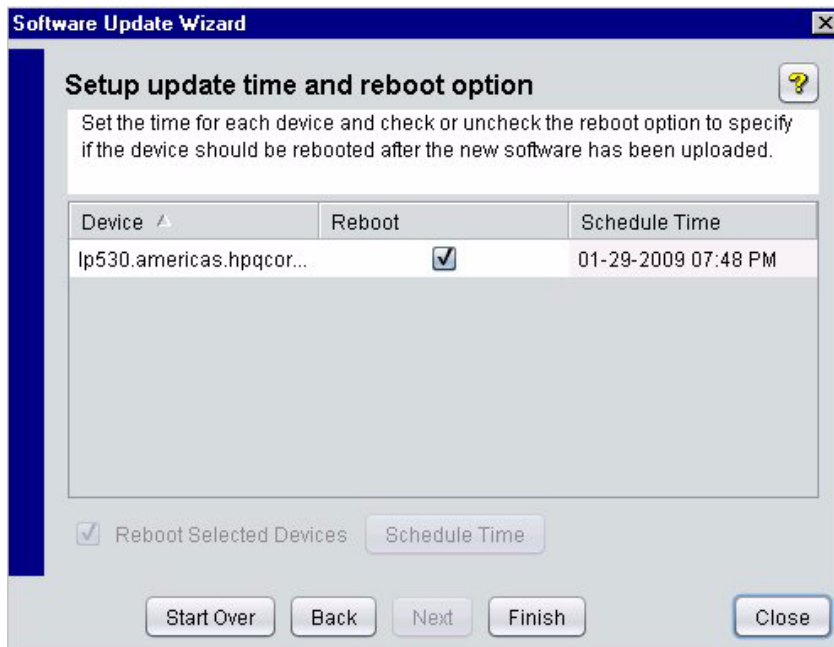


Figure 12-55. Software Update Wizard, Setup update time

11. The software update Setup will have the **Reboot Selected Devices** option selected (checked) by default. This indicates that the system should be automatically rebooted after the software is updated. If you do not want the system to be rebooted, uncheck the Reboot check box next to the device.
12. Set the **Schedule Time** that you want the software update to be performed. You can type the date, or use the buttons to increase or decrease the entries for date and time. To set the same schedule time for multiple devices, use the **Schedule Time** button.

Caution:

If you enter a time that is earlier than the current date and time, and there is a more recent software update, PCM will attempt to perform the update and reboot the switch immediately.

The system will be rebooted on the currently running software. If you selected to update the Secondary software image, and the Primary software image is the currently running version on the device, the device will be rebooted using the Primary image, not the updated software version. To reboot the device using the updated software version, you will need to do a manual reboot with the Secondary software image.

- Click **Finish** to save the Software Update schedule and exit the Software Update Wizard.

Reviewing Software Update Status



To review and delete scheduled switch software updates, click the Configuration Management Status button in the global toolbar.

Device	Image	Version	Reboot	Scheduled	Status
lp530.americas...	Primary	WA.01.14	<input checked="" type="checkbox"/>	Mon Mar 29 19:19:00 PDT 2010	Waiting

Figure 12-56. Switch Software Update Status

The Software Update Status dialogue displays the devices currently set up in the software update schedule with the following information:

Device	Name or IP address of the device to be updated.
Image	The software image to be updated, primary or secondary.
Version	The version number of the software to be loaded on the device.
Reboot	A check mark indicates that the device will reboot automatically after the software is updated.
Scheduled	Date and time the software update is scheduled to occur.
Status	Current status of the software update. Possible status types are: Waiting, Updating, Completed, Error (update failed), Retrieving, Reboot, Unknown (can't communicate with Agent). An event is created for an Updating or Error status.

Deleting Scheduled Software Updates

To delete a device from a scheduled software update:

1. Select the device in the Software Update Status dialogue.
2. Click **Delete**.
3. Click **OK** in the confirmation pop-up to complete the process. The device will be removed from the software update schedule and the Software Update Status dialogue will be updated.

To delete an entire Software update schedule, use the Software Update Status window to delete each device included in the schedule.

Use the Software Update Wizard if you want to exclude (skip) a device from a scheduled software update without deleting it from the schedule.

Using Software Image Import

The Software Image Import Preferences window lets you add, edit, and delete premium software for MSM devices. This feature eliminates the need to manually add an entry to the `procurve_firmware.prp` file and initiate a software update when you purchase premium software for an MSM device.

You can also use this feature to select the preferred software version for a device type.

Note:

Software updates via PCM require that the `procurve_firmware.prp` file be updated appropriately. This file acts as the source of information about the software image available for upgrade and is updated in PCM automatic updates for non-premium devices.

To add entry for manually imported image to PRP file:

1. Download the software image file from the manufacturer's Web site, and place it in the `\server\data\download` directory. The default path is `C:\Program Files\Hewlett-Packard\PNM`.
2. Navigate to the Software Image Import preferences window:
 - a. Click the Tools menu.
 - b. Select Preferences from the Tools drop-down list.
 - c. Click the + sign at the left of Configuration Management in the Preferences tree.
 - d. Select Software Image Import.

3. Select the device type you want to add from the Select Device Type list, and click **Add**.
4. In the Add Software Image Import window, type the Software Version and Software Image File Name that you downloaded and placed in the \server\data\download directory.
5. Click **OK** to add the device type information to the PRP file. This software information is also added to the Software Image Import preferences window.

To edit an existing entry:

1. Navigate to the Software Image Import preferences window:
 - a. Click the Tools menu.
 - b. Select Preferences from the Tools drop-down list.
 - c. Click the + sign at the left of Configuration Management in the Preferences tree.
 - d. Select Software Image Import.
2. Select the device type you want to edit from the Select Device Type list.
3. Select the software version currently used by the device type, and click **Edit**.
4. Type the desired Software Version and Software Image File Name in the Edit Software Image Import window.
5. Click **OK** to change the device type information in the PRP file. This software information is also updated in the Software Image Import preferences window.

To remove an entry from the PRP file:

1. Navigate to the Software Image Import preferences window:
 - a. Click the Tools menu.
 - b. Select Preferences from the Tools drop-down list.
 - c. Click the + sign at the left of Configuration Management in the Preferences tree.
 - d. Select Software Image Import.
2. From the Select Device Type list, select the device type you want to remove from the PRP file.
3. Select one or more software versions to be removed for the device type, and click **Delete**.

To set the preferred software version for a device type:

1. Navigate to the Software Image Import preferences window:
 - a. Click the Tools menu.
 - b. Select Preferences from the Tools drop-down list.
 - c. Click the + sign at the left of Configuration Management in the Preferences tree.
 - d. Select Software Image Import.
2. From the Select Device Type list, select the desired device type.
3. Select the preferred software version for the device type by checking its Preferred Version check box, which updates the custom.prp file.
4. To save your changes and leave the Preferences window open, click **Apply**.

OR

To save your changes and exit the window, click Ok.

Note:

When updating software for MSM outdoor devices, available software versions are listed under MSM-R if the current software version is 5.3.1 or greater. If the current software version is earlier than 5.3.1, available software versions are listed under MSM.

Using a USB Autorun File

PCM provides a USB Autorun feature that allows you to deploy a configuration in a secure way on multiple devices in remote sites. Using a secure Autorun file on a removable USB drive, you can configure switches, update software, or retrieve diagnostic logs for troubleshooting purposes.

To use a USB Autorun file, follow these steps:

- Identify the devices on which you want to run the command file.
- Configure the necessary security credentials, such as certificates and encryption keys.

Certificates are used by PCM to generate signed Autorun files containing switch CLI commands. Encryption keys are used by PCM to create encrypted Autorun files and decrypt Report files.

- Create an Autorun file that contains the CLI commands to be run on selected devices and copy the file to a removable USB drive.
- Insert the USB drive into a USB port on each target device that you want to configure. The Autorun command file automatically executes.
- To read the Report file generated by a device on which the Autorun file was executed, re-insert the USB drive into the PCM Client on which PCM is running.

Managing USB Certificates

1. Navigate to the USB Management global preferences window by selecting Tools>Preferences>USB Management.
2. To add a certificate, click the **New** button in the USB Certificates pane and, using standard Windows conventions, select the .p12 file (in pkcs12 format) containing the certificate that will be used by PCM to generate signed command files.
3. To delete a certificate, select the certificate to be deleted and click the **Delete** button.
4. To set the default certificate, select the certificate and click the **Default Cert** button.

Managing Encryption Keys

1. Navigate to the USB Management global preferences window by selecting Tools>Preferences>USB Management.
2. To add an encryption key, in the USB Encryption Keys pane, type the key and alias and then click the **Add Key** button. An alias must contain at least 2 alphanumeric characters.

Note:

Use the openssl command `rand 16 -base64` to create an encryption key.

3. To delete a key, select the key to be deleted and click the **Delete** button.
4. To set the default key, select the key and click the **Default Key** button.

Creating the Autorun File



1. Navigate to the USB Autorun Wizard by clicking the USB button on the global toolbar or right-clicking the USB-supported device in the navigation tree and selecting **USB Autorun** from the drop-down list.
2. When the wizard appears, select **Generate Command File**.

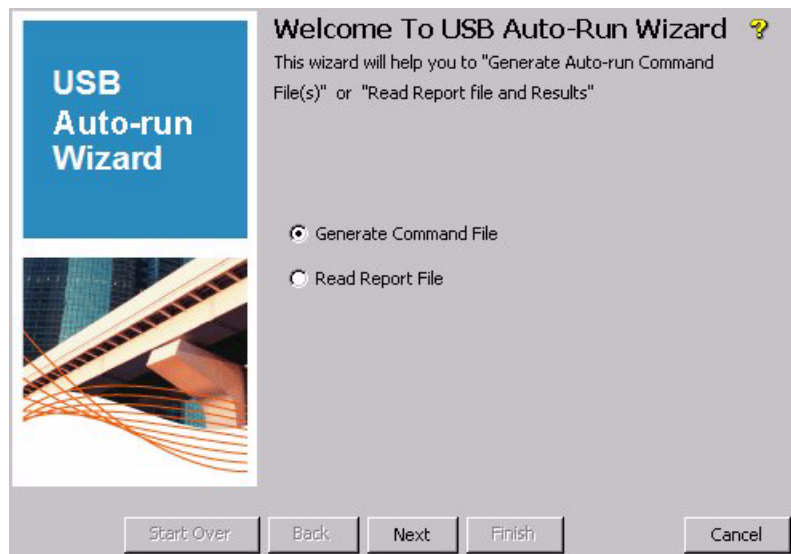


Figure 12-57. USB Autorun Wizard - Generate Command File

3. Click **Next**.
4. To execute the Autorun file on a single device:



Figure 12-58. USB Autorun Wizard - Device

- a. If you opened the USB Autorun Wizard by clicking the USB global toolbar button, click the Create a single xml file for one or more devices radio button.

Note:

If you started the wizard by right-clicking a USB-supported ProCurve device and selecting USB Autorun, the Create multiple xml files for selected device groups option is not displayed and the fields on this window are filled in automatically.

- b. Optionally, in the Mac Address field, identify the device by typing the MAC address of the device where the script will be executed.

All fields are optional. However, PCM validates all entries, and entering the fields reduces the risk of the Autorun file being accepted by an unintended device.
- c. Optionally, in the Serial Number field, type the serial number of the device where the script will be executed.
- d. Optionally, in the Software Version field, type the version of the software used on the device where the script will be executed. This field is optional. However, PCM validates all fields, and entering this field reduces the risk of the Autorun file being rejected by the device.
- e. Optionally, in the ROM Version field, type the ROM version of the device where the script will be executed.

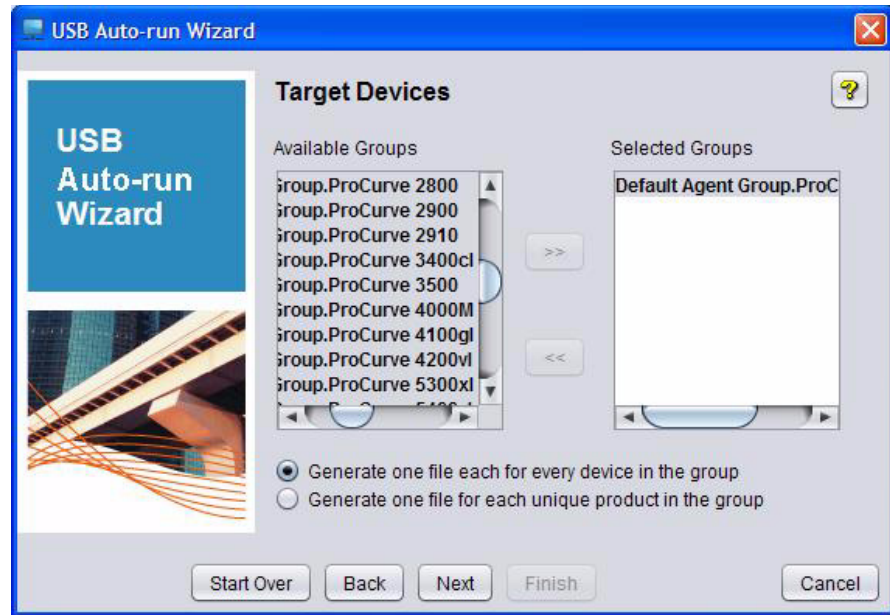


Figure 12-60. USB Autorun Wizard - Select Target Devices

- c. Select the device group(s) where the script will be run and click the >> button.
- d. To generate one command file for all selected device groups, uncheck the Generate one file each for every device in the group check box.

OR

To generate a separate file for each device in the selected groups, check the Generate one file each for every device in the group check box. (Select at least one group that contains more than one USB-supported device.)

Command files will be generated with the IP address as the file name (e.g., 172_16_25_30.cmd.xml).

- e. To generate one command file for each selected product (e.g., ProCurve Switch 5412zl), uncheck the Generate one file for each unique product in the group check box.

OR

To generate a separate file for each USB-supported device in the selected product groups, check the Generate one file for each unique product in the group check box. (Select at least one group that contains more than one USB-supported device.)

- f. Click **Next**, which verifies that the selected groups contain USB-supported devices.
 - g. If you selected a group that does not contain USB-supported devices discovered by PCM, an error message occurs. Click **OK** to close the dialog.
 - h. To select another device group or product group containing USB-supported devices, click the **Back** button and select the desired group(s).
OR
Ignore the warning and continue.
 - i. Click **Next**.
6. Enter the CLI commands:

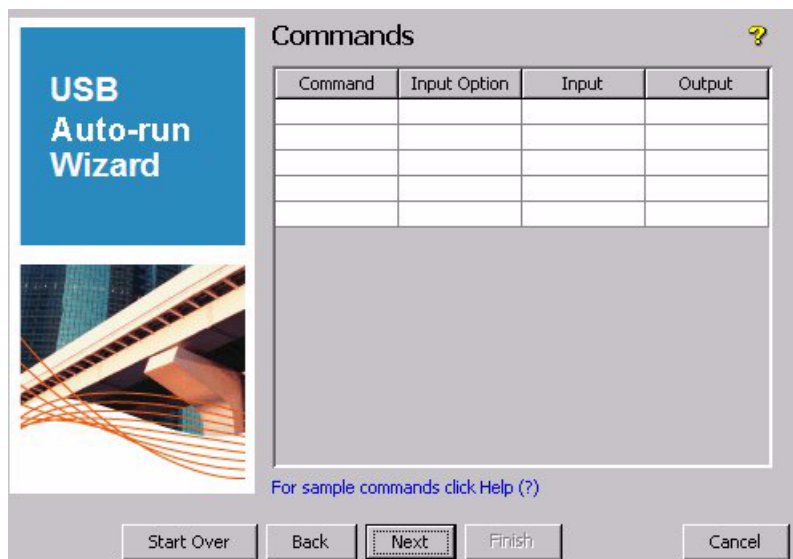


Figure 12-61. USB Autorun Wizard - Commands

- a. In the first blank Command column, type the CLI command to be executed.

If the command is executed from the configuration mode, access the configuration mode first by entering the configure terminal command before entering configuration commands.
- b. In the Input Option field of the same row, select the CLI command's input option.

- Select **Template** to deploy a PCM configuration template to the device. A popup window appears allowing you to select the template. Click the drop-down arrow and select the template you want to deploy.
- Select **External File** to deploy an external configuration file to the device, and use the standard Windows file procedure to select the file.
- Select **Latest Config** to deploy the most recent configuration file from the configuration history in PCM for the selected device. No other input is required.

This option is available only when the wizard is launched from the right-click menu.

The Input field of the same row is populated automatically based on the Input Option chosen (either with the name of the template or the fully qualified path of the external file).

- c. Optionally, use the Output field in the row if the switch should use a specific name for the Result file.
- d. Repeat the above steps for each CLI command.

The following examples illustrate command entries:

To deploy firmware:

<u>Command</u>	<u>Input Option</u>	<u>Input</u>	<u>Output</u>
copy usb flash K_13_02.swi primary	External File	C:\firmwareimages\K_13_02.swi	(blank)

To deploy a configuration file:

<u>Command</u>	<u>Input Option</u>	<u>Input</u>	<u>Output</u>
copy usb startup-config 3500cfg	Template	3500cfg	(blank)

To retrieve log information for troubleshooting:

<u>Command</u>	<u>Input Option</u>	<u>Input</u>	<u>Output</u>
show tech	None	(blank)	techout.txt

7. Enter the Post CLI Commands (executed on the switch after the USB removable drive is removed):

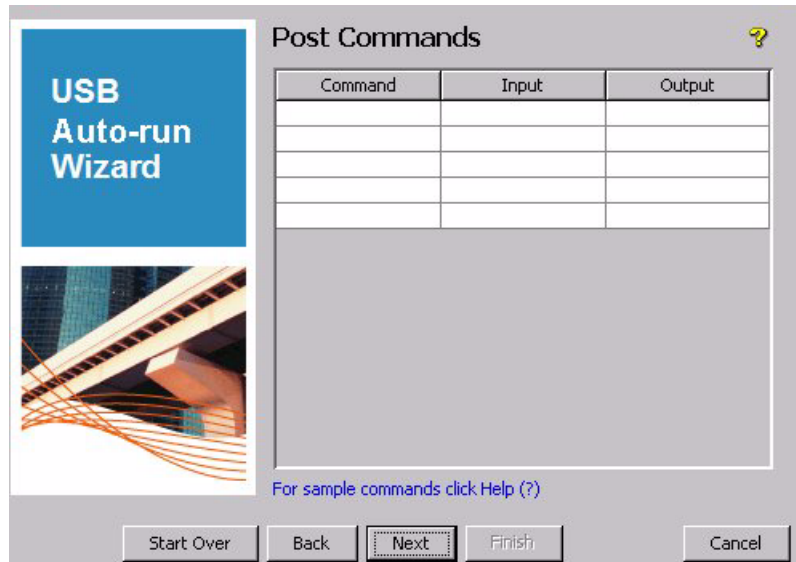


Figure 12-62. USB Autorun Wizard - Post Commands

- a. In the first blank Command column, type the CLI command to be executed.
 - b. In the Input field of the same row, type the configuration file name or the URL where the input file is located. Not all switches support this feature, so check the *Management and Configuration Guide* to ensure this feature is supported by your switch.
 - c. In the Output field of the same row, type the name/path of the output file.
 - d. Repeat the above steps for each CLI command.
8. Select the security options:

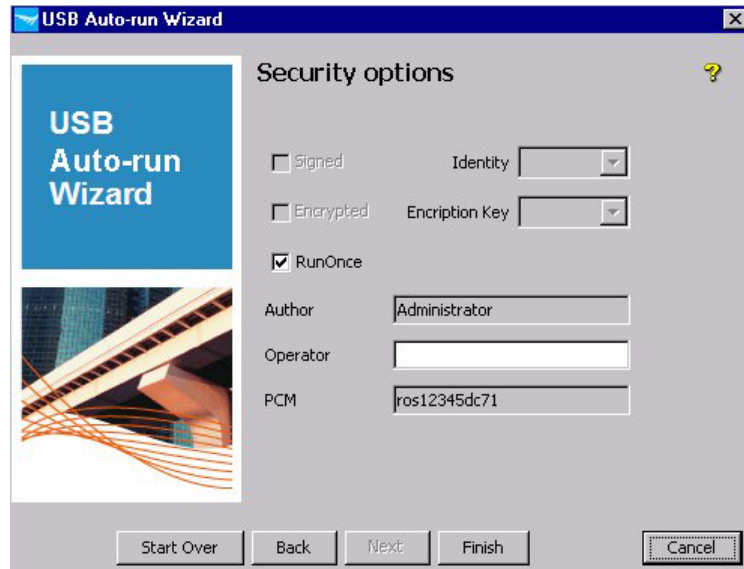


Figure 12-63. USB Autorun Wizard - Security Options

- a. To sign the file, check the Signed check box and select the signature from the Identity drop-down list. Signatures are defined in USB Management global preferences.
 - b. To encrypt the file, ensure the Signed check box is checked (only signed files can be encrypted), check the Encrypted check box, and select the encryption key from the Encryption Key drop-down list. Encryption keys are defined in USB Management global preferences.
 - c. If the file should only be run once by a device, check the RunOnce check box.
 - d. In the Operator field, type your name or another indicator of who will execute the Autorun file on the switch.
 - e. Click **Finish** to select the location where the Autorun file will be created.
9. Select the USB removable drive where the Autorun file will be created (usually drive E:), and type the Autorun file name. If multiple files are generated (because you selected multiple groups and the Generate one file each option), select the drive where the multiple files will be stored.
 10. Insert the USB removable drive into the USB port on the PCM computer.
 11. Click **Finish** and wait for the Autorun file to be copied onto the USB removable drive.

Deploying the Autorun File


1. Once the Autorun file is written to the USB removable drive, remove the USB drive and physically go to a switch that was targeted.
2. Insert the USB drive into the switch auxiliary (USB) port, and wait for the Autorun file to be executed.

Note:

When Autorun is enabled on a switch, inserting the USB removable drive automatically executes the Autorun file and creates a Results file and Report file on the USB removable drive. For additional Autorun information on configuring the switch for Autorun, see the *Management and Configuration Guide* for your switch.

3. Remove the USB drive from the switch, and repeat the previous step on each switch that was targeted.

Reading a Report File

1. Return to PCM and insert the USB drive into the PCM computer's USB port.
2.  Navigate to the USB Autorun Wizard by clicking the USB button on the global toolbar.
3. When the wizard appears, select Read Report File.

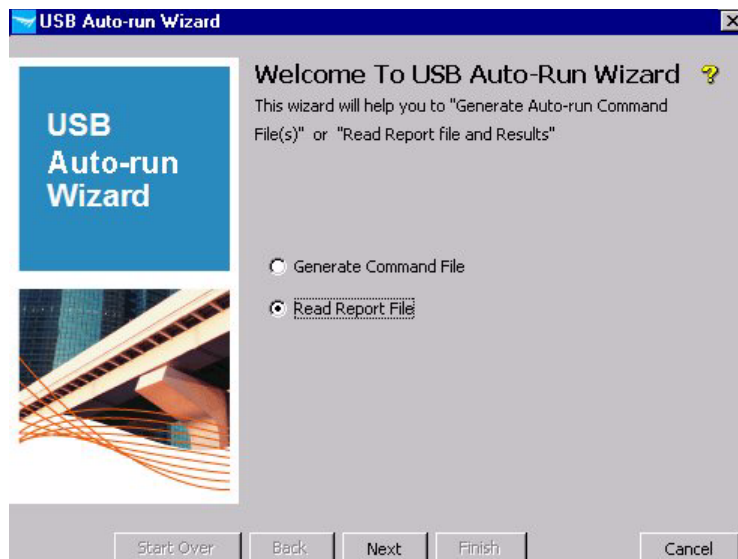


Figure 12-64. USB Autorun Wizard - Read Report File

4. Click **Next**.

Note:

Switches create two files on the USB removable drive: the Report file and the Results file. The Report file is an .xml file identifying the switch and the name of the Results file. The Results file is a .txt file containing the results of each command executed on the switch.

5. Select the report security options:
 - a. If using a file signature, check the Verify Signature check box and use the Certificate drop-down list to select the signature. You must select the certificate that was used to create the Autorun file.
 - b. If using encryption, check the Decrypt Commands check box and use the Decryption Key drop-down list to select the key. You must select the key used to create the Autorun file.
 - c. Click **Finish** to select the report.
6. Click the Open Report button at the top left of the screen and select the files you want to view. This displays the report execution details for the selected files in the top pane.



Figure 12-65. USB Autorun Wizard - Read Report File

7. In the top pane, select the report you want to view, which displays the report (result of the CLI commands executed on the switch) in the bottom pane.
8. Check the report to ensure all commands were completed successfully.

Using a Script to Manage Device Configurations

PCM allows you to create and run custom scripts and applications in a scripting language which you already know, such as perl, python, or Windows PowerShell. In this way, you can extend PCM's functionality for managing and configuring network devices.

Using custom scripts with PCM offers the following benefits:

- PCM ensures security in script execution by performing a secure login using the device credentials stored in the PCM database. There is no need to enter device login credentials in a script.
- By parsing only the actual result of each command in the script, PCM allows you to write simpler scripts and avoid the need to enter code that parses terminal escape sequences.

You can execute a script on a single device or on multiple devices as follows:

- On demand to run against a selected device or group of devices. The script is run on a PCM Client using the Script Wizard.

All scripts that can be executed from a command prompt window on the PCM Client can be invoked from PCM Script Wizard.

- As a policy-based action (see “Configuring Policy Actions” on page 16-30) that is scheduled or triggered by an event. The script is generated using Policy Manager and run on the PCM Server. You enter the command-line parameters when you configure a Group Script action.

On PCM, you can create any script that executes CLI commands on a device (e.g. shell, perl, binary applications) by entering a command-line statement with substitution tags, such as %ip or %write. PCM replaces each tag with a device-specific value, which has been discovered and stored in the PCM database. The data is passed as command-line arguments in the script; for example, a device IP address replaces %ip; a write community replaces %write, and so on.

In this way, you can write a script in general terms and allow PCM to enter device-specific parameters when you run the script. At runtime, PCM logs into each network device, runs the script which executes CLI commands on the device, and then logs out. There is no need for an administrator to enter device credentials.

PCM does not validate a script for correctness or ensure against possible malicious behavior resulting from the execution of commands on a target device. Executing a script outside of PCM has the same result as executing the script in PCM as a policy action or with the Script Wizard.

Prerequisite. The necessary runtime scripting environment (for shell, perl, python, and so on) must exist:

- On the PCM Client before executing a script with the Script Wizard.
- On the PCM Server before executing a script with a Policy Manager action.

For more information, see “Executing a Script” on page 12-88.

Adding a Script to Script Manager

You can add a script (text file or binary executable) and store the command line and other script information in Script Manager for later execution with the wizard.

To add a script to Script Manager for later execution:



1. Open the Script Manager by clicking the Launch Script Manager icon in the global toolbar. The Script Manager window displays a list of existing functions.



2. Click the Add Script icon on the Script Manager toolbar.
3. In the Add Script Wizard window, click **Next**.
4. In the Function Name window, select Create a new function and enter a unique name to identify the function which the script performs (for example, Set SNMPv3 credentials or Turn off Inactive Ports) and a text description. Then click **Next**.

5. In the Script Details window, enter the following information:

Add New Script

Script Details

Script Identifier has to be unique within a function. Please provide the command-line statement to invoke the script, the target of execution and the end of result tag.

Script Identifier:

Command-line: End of Result:

%write	= pass write community name
%manuser	= pass manager username
%manpass	= pass manager password
%opuser	= pass operator username
%oppass	= pass operator password
%v3username	= pass an USM username(if configured)
%auth_pro	= pass the authentication protocol for the USM user
%auth_pwd	= pass the authentication password for the USM user
%priv_pro	= pass the privacy details(aes/des) for the USM user
%priv_pwd	= pass the privacy password for the USM user

Target: Timeout in sec: Default Script

Description:

Figure 12-66. Script Manager - Script Details Window

- a. Enter a unique name in the Script Identifier field. This name identifies the script within the function.

- b. In the command-line field, type the commands to be executed by the script in the format:

`<environment> <directory_path> <command_line_tags>`

Where:

`<environment>` specifies the environment necessary to run the script on the PCM Server or Client; for example, some valid values for the script file are: `sh` (shell), `perl` (shell), and `py` (python).

- **You are responsible for creating the scripting environment on the PCM Server or Client, depending on the location from which you run the script.**
- If the scripting environment is not on the global `PATH` variable, you must enter the full pathname to the scripting environment; for example: `C:/python26/python.exe C:/test.py`

`<directory_path>` specifies the complete directory path and file name of the script. Forward slashes (/) or backslashes (\) are supported.

- If you execute the script from the Script Wizard (see “Using the Script Wizard” on page 12-88), the file must reside at the specified directory path on the PCM Client.
- If you execute the script as a policy action (see “Using Policy Manager” on page 12-93), the file must reside at the specified directory path on the PCM Server.

`<command_line_tags>` specifies the substitution tags that you enter by referring to the Command-line Substitutions list. These tags are the most frequently used script parameters that will be replaced by device parameters when the script is executed. The substituted data is retrieved by PCM from each target device at runtime. For more information on command-line tags, see “Embedded Script Tags” on page 12-95.

- c. In the End of Result field, enter the End of Result flag that the script uses to verify that command execution has completed. This entry is required.

PCM appends the End of Result flag to the output stream being sent to the script to signal the end of output. This flag must also be specified in the script and can be any text string that is unlikely to occur in the output of the command. For example, if you enter `EOR` in this field, be sure to enter `EOR` in the script to signal the end of command output.

- d. In the Target field, select a value from the drop-down list to specify where the script will be run: on the PCM Server, PCM Client, or both.
 - Only scripts with a target of `Client` or `Both` can be run with the Script Wizard.
 - Only scripts with a target of `Server` or `Both` can be run as a policy action from Policy Manager.

Note: If a script has a target of `Both`, it must be stored in the same directory path on both the PCM Server and Client.
 - e. In the Timeout field, select the number of seconds within which the script must execute for a target device. Default: 60 seconds.

Important: This parameter sets the time required for the complete execution of the script. If the execution of the script does not finish within this time, the operation is aborted.
 - f. Select the Default Script check box to use the script as the default script for the function on all device models.

The default script is run if no script has been created for the target device model in a function.
 - g. In the Description field, you can enter an optional text description of the script.
 - h. Click **Next**.
6. In the Device Groups window, select the device groups for which you want to run the script, and click **Add**. Then click **Next**.

The Device Groups window is not displayed if, in the preceding step, you configured the script as the default for the function.

7. In the Summary window, verify the configuration of the script to be added. To store it in Script Manager, click **Close**.

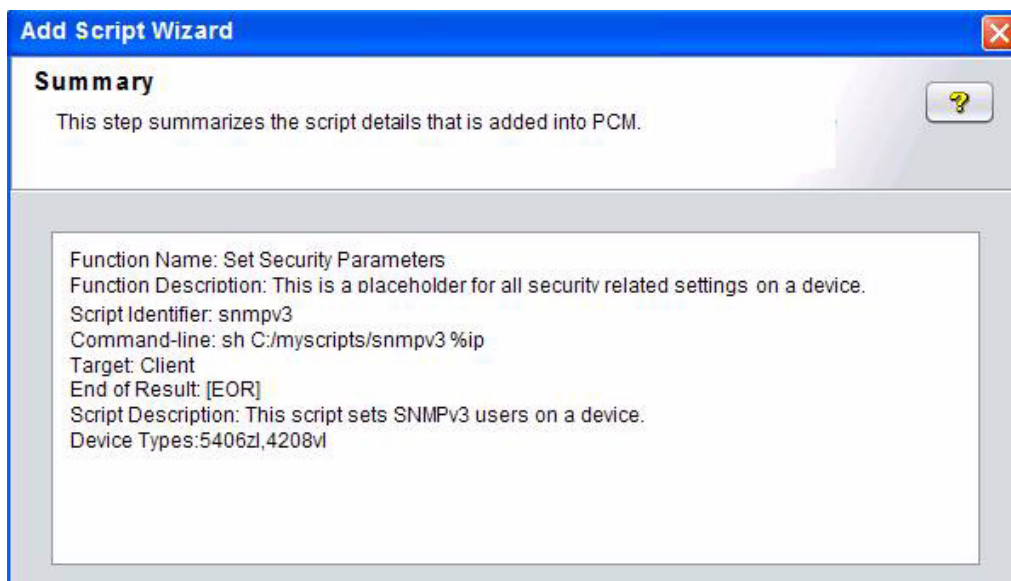


Figure 12-67. Script Manager - Summary Window

Editing a Script

When you start Script Manager, a list of all existing functions and scripts created for each function is displayed. You can edit a function name and description, or the script command line and description.

To edit a function:

1. Open the Script Manager by clicking the Launch Script Manager icon in the global toolbar.
2. Select a function and click the Edit a Script/Function icon on the Script Manager toolbar.
3. In the Edit Function window, type in a new name or text description for the function, and click **OK**.

To edit a script:

1. Open the Script Manager by clicking the Launch Script Manager icon in the global toolbar.



2. Double-click a function name, select a script, and click the Edit a Script/Function icon on the Script Manager toolbar.
3. In the Script Wizard welcome window, click **Next**.
4. In the Edit a Script: Script Details window, change any of the script parameters as described in “Adding a Script to Script Manager” on page 12-82, and click **Next**.
5. In the Edit a Script: Device Groups window, select each device group for which you want to run the script, and click **Add**. Then click **Next**.
6. In the Summary window, verify your changes and click **Close**.

Deleting a Script

You can delete a function or a script from Script Manager. When you delete a function, you delete all scripts configured for the function.

To delete a function:



1. Open the Script Manager by clicking the Launch Script Manager icon in the global toolbar.



2. Select a function and click the Delete a Function icon on the Script Manager toolbar.

3. In the Confirm Delete Function window, click **Yes** to delete the function and all scripts contained in it.

To delete a script:



1. Open the Script Manager by clicking the Launch Script Manager icon in the global toolbar.



2. Double-click a function name, select a script, and click the Delete Script icon on the Script Manager toolbar.

3. In the Confirm Delete Script window, click **Yes**.

Executing a Script

After you create a script, you can execute it by:

- Running the script on demand for a selected device or group of devices using the Script Wizard (see “Using the Script Wizard” on page 12-88).
- Running the script as a policy-based action that is scheduled or triggered by an event (see “Using Policy Manager” on page 12-93).

Using the Script Wizard

The following conditions apply when you use the Script Wizard to run a script:

- All scripts that you can execute from a command prompt window on the PCM Client can be run from the Script Wizard.
- You can execute a script for one or multiple devices.
- The Script Wizard helps you to include command-line arguments in a script.
- You can run any type of script (shell, perl, python, binary applications).
- Interactive CLI commands are supported. See “Embedded Script Tags” on page 12-95 for more information.
- PCM uses the device credentials (such as SNMP Community, CLI user names and passwords) stored in PCM to log in and log out of devices to execute the script.
- When a script is run using the Script Wizard, the output file generated by the script is stored in the `PNM/Client` directory.

Restrictions. The following restrictions apply when you execute a script with the Script Wizard:

- Command buffering is not supported.
- To disable buffering, Perl scripts must include the command: `$| = 1 ;`
- The command line in a Python script must contain the `-u` option.
- When you write a script, take into account that in a script execution, after the script runs a command against a switch, the script waits to receive the full result of the command before executing the next command.

- When you run a script against multiple devices, the script executes serially against each device in turn. Scripts are not run in parallel.
- PCM does not validate the script or the application for any malicious effects.
- The script you run on a PCM Client must reside on the Client PC.

Prerequisite. PCM requires the necessary runtime environment to be created on the PCM Client before executing a script with the Script Wizard.

To run a script that is stored on a PCM Client and executes commands on selected target devices:

1. Verify that the script is stored on the PCM Client on which you open the Script Wizard.
2. Verify that the necessary runtime scripting environment (for example: shell, perl, python, or binary applications) exists on the PCM Client.
3. From the PCM Client, open the Script Wizard:
 - In the navigation pane, under **Devices**, open a device group, select the IP addresses of the device(s) for which you want to run a script, right-click and select **Config Manager > CLI-Script Wizard**.

OR



- In the navigation pane, select **Devices**, click the **Devices List** tab, select the device(s) for which you want to run a script, and do one of the following:
 - Right-click and select **Config Manager Tools > CLI-Script Wizard**.
 - Click the **Config Manager Tools** icon and select **CLI-Script Wizard** from the drop-down list.
- 4. In the **Welcome to CLI Script Wizard** window, click **Next**. The **Script Execution Parameters** window is displayed.

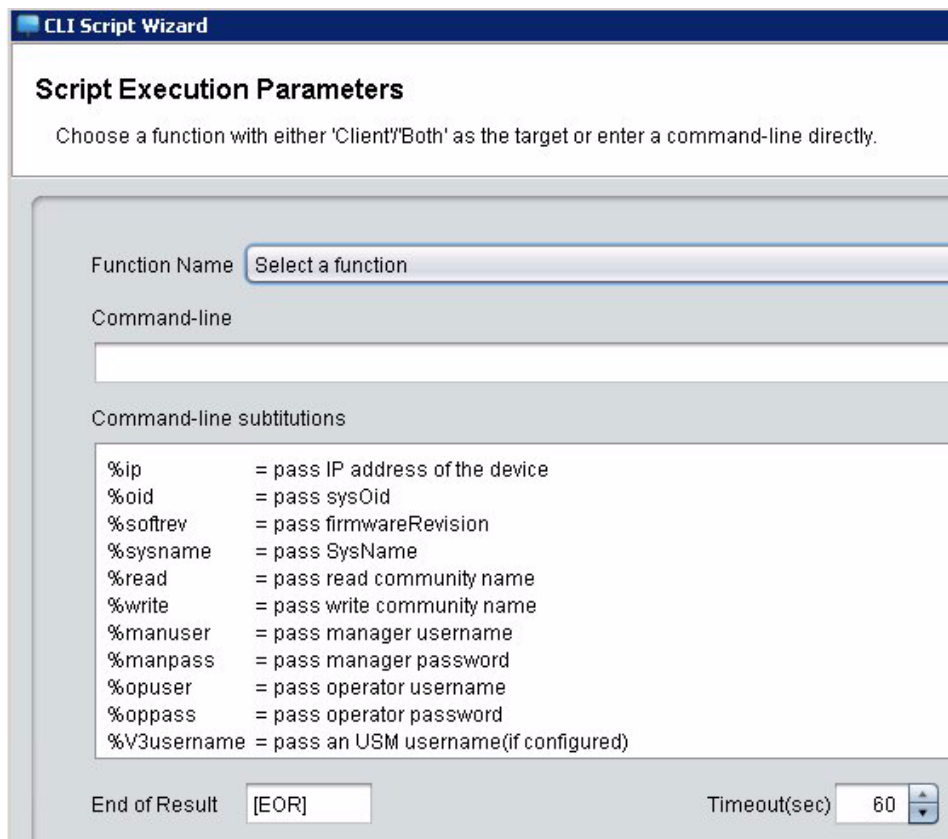


Figure 12-68. CLI Script Wizard - Script Execution Parameters

5. In the Script Execution Parameters window, do one of the following:
 - Select a function from the drop-down list. PCM searches for an existing script that has already been added for the selected device model (see “Adding a Script to Script Manager” on page 12-82).
 - If a predefined script exists, script parameters are automatically entered in the Command Line, End of Result, and Timeout fields. If you selected multiple devices in step 3, which require different command-line parameters to be substituted, the fields may be greyed out.
 - If a predefined script does not exist for the selected function and device model, the fields are greyed out. The default script configured for the function will be used.
 - If you do not select a function, enter a command line and script parameters to define a new script as described in “Adding a Script to Script Manager” on page 12-82.

Then click **Next**.

6. Verify the script execution on all selected devices by following the progress messages displayed in a separate window.

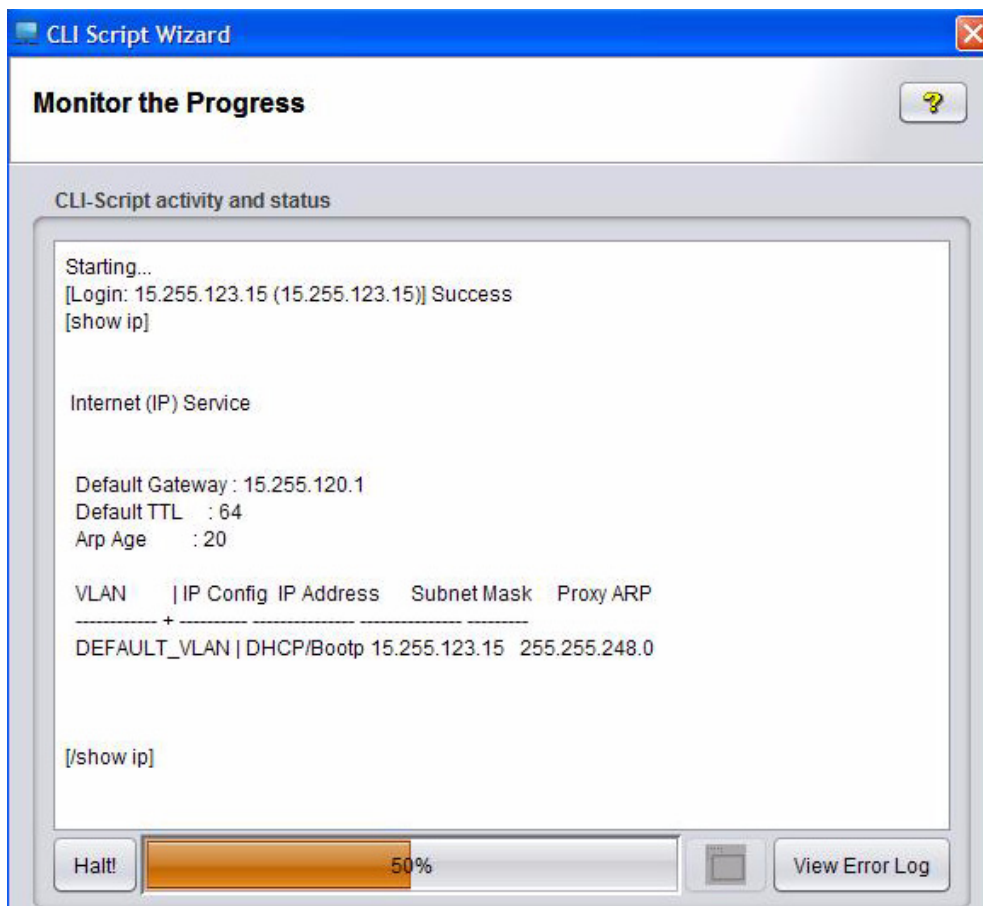


Figure 12-69. CLI Script Wizard - Monitor the Progress Window (Starting)

The Progress window displays each command as it is executed by the script and the command output from the device.

If the script execution encounters an invalid command or incomplete output, it continues to execute the other commands.

If you selected multiple devices, the script command line is executed for one device at a time. Progress messages are displayed device by device. For each device, a new runtime process is started and terminated after a successful execution or unsuccessful completion on the preceding device.

Managing Device Configurations Using a Script to Manage Device Configurations

- To view the standard error stream that results from the script execution, click the **View Error Log** button at the bottom right of the window. You can later save the contents of the detached view to a file.
- To save the progress messages in the script execution to a file, click the **Enlarge to a separate window** button.
- To stop the script execution, click the **Halt!** button.

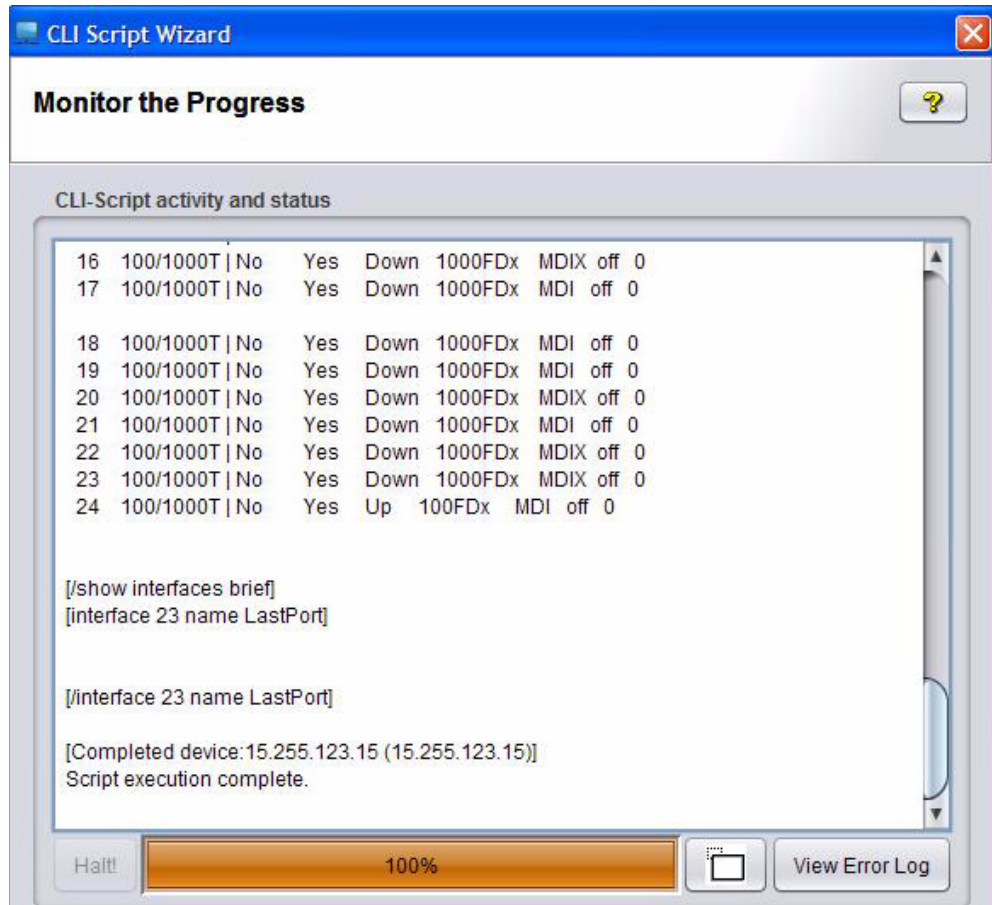


Figure 12-70. CLI Script Wizard - Monitor the Progress Window (Completion)

For information on how to troubleshoot a script execution, see “Troubleshooting a Script Execution” on page 12-96.

Using Policy Manager

In addition to executing a script on demand using the Script Wizard (see “Using the Script Wizard” on page 12-88), you can also execute the script by running it as a policy-based action that is scheduled or triggered by an event with Policy Manager as described in “Configuring Policy Actions” on page 16-30.

When configured as a policy action, a script executes in the same way as on demand using the Script Wizard:

- PCM passes device-specific parameters required by the script (for example, read community, write community, device IP address) using substitution tags in the command line.
- PCM logs into the device using SNMP community names, and CLI user names and passwords defined in PCM. An administrator does not have to know or enter device credentials to execute the script.

A script used as a policy action requires the script to reside on the PCM Server. (A script run from the Script Wizard must reside on the PCM Client.)

To configure a script as an action for a policy:

1. Create the script as described in “Adding a Script to Script Manager” on page 12-82.
2. Verify that the script is stored on the PCM Server.
3. Verify that the necessary runtime scripting environment (for shell, perl, python, or binary applications) exists on the PCM Server.
4. From the PCM Client, open the Policy Manager by clicking the Launch Policy Manager button in the toolbar.
5. In the Policy Manager navigation pane, click **Actions**.
6. In the Manage Actions window, click **New**.
7. In the Create Action window:
 - a. Select **Config Manager: Group Script**.
 - b. Enter a name for the script and click **OK**. The script is added in the navigation pane under Actions and the Group Script window is displayed to enter script parameters.





Figure 12-71. Configuration Manager: Group Script Window

8. In the Group Script window:
 - a. Click the Properties tab and enter a name and text description of the script.
 - b. Click the Script tab and select a function or enter a command line and other parameters as described in “Adding a Script to Script Manager” on page 12-82. Then click **Apply**.
 - c. Click the Options tab and specify whether you want to capture script output to a file. When a script is run as a policy action, the output file is created in the `PNM/Server` directory.
 - d. Click **Close** when you finish.
9. Create a policy as described in “Configuring Policies” on page 16-4 and select the script from the list of available actions.

Embedded Script Tags

You can also include the following tags as embedded meta-language in a script:

- `<PCM_OUTPUT> ... </PCM_OUTPUT>`
- `<PCM_INTERACTIVE> ... </PCM_INTERACTIVE>`

`<PCM_OUTPUT> ... </PCM_OUTPUT>`

All the output statements that you enclose within the `<PCM_OUTPUT>` tags in a script are displayed in the Monitor Progress window without sending them to the switch for which the script is executed. Note that you must enter the end tag `</PCM_OUTPUT>`, otherwise an error message is displayed.

- `PCM_OUTPUT` tags must be separated by newline. The amount of data between the tags cannot exceed 500 bytes.
- You can enter multiple sets of `PCM_OUTPUT` tags. The resulting output from the script is reported back to PCM.

`<PCM_INTERACTIVE> ... </PCM_INTERACTIVE>`

The CLI-Script Wizard supports interactive commands only when the commands are enclosed within the `<PCM_INTERACTIVE>` tags in a script.

- `<PCM_INTERACTIVE>` tags must be separated by newline, and cannot be included in the standard output with CLI instructions to the switch.
- There is no limit to the number of steps supported in an interaction.
- Every line between the tags is sent to the switch as an input to the next step of interaction. The script writer should take into account the content of each input to the interaction.
- If the end tag `</PCM_INTERACTIVE>` is not specified, the entire conversation is treated as interactive and may result in pattern match failures.
- Each response in the interaction is relayed back to the script only if a pattern match is found.

Troubleshooting a Script Execution

The execution of a script may stop due to the following reasons:

- The script file is not present.
- The correct runtime environment is not available on the PCM Server or Client.
- Scripting language errors occur during the execution.
- One of the following timeout values was exceeded:
 - Script idle timeout (Default: 10 seconds)
 - CLI timeout (Default: 15 seconds)
 - Overall script execution timeout (Default: 60 seconds)

To diagnose and troubleshoot the cause of an unsuccessful script execution, follow these steps:

1. Use the execution log in the `cs-out.log`, `cs-err.log`, and `CFG-Manager.log` files in the PCM Client directory to diagnose problems.
2. Check the script output for errors, unexpected actions, or results. By default, script output generated from within the script is written to the `PNM/server` or `PNM/client` folder unless the directory path is explicitly defined in the script.

Note: When redirecting the script execution through a TFTP server, the output is stored in the Root directory of the TFTP server. If the TFTP server associated with the PCM Agent is used, the output is stored in the `PNM\pcm_agent\data\download` directory of the PCM Agent.

3. Execute the script manually (outside of PCM) and ensure that the script is correct and that all variables are defined on the PCM command line for the script.
4. Ensure that the correct SNMP community names, and CLI user name and password are defined in PCM and are currently in use.
5. Ensure that the correct script environment is defined:
 - On the PCM Client that executes a script on demand.
 - On the PCM Server that executes a script as a policy action.
6. Execute the script on other devices of the same model to see if the problem is device specific.
7. If the script uses an End of Result flag, ensure that the End of Result flag is defined in PCM.

8. Ensure that a firewall does not block script communications and switch command output.
 - Scripts initiated with the Script Wizard require communication between the device and Agent, Agent and PCM Server, and PCM Server and PCM Client.
 - Scripts initiated by a policy require communication between the device and Agent, and the Agent and PCM Server.

For more information about how to work around a firewall in your network, see “PCM and Firewalls” on page 2-70 and “Proxy” on page 3-21.

Script Examples

This section contains examples of command lines for:

- A simple shell script
- A more complex, multi-command shell script
- A perl script
- A more complex perl script

In these examples, the script file name (for example, `c:\showtech.sh`) entered in the command line may vary. Depending on where the script file is stored, it is sometimes necessary to specify the complete directory path and file name.

Example: Simple Shell Script

```
#####  
# This program request a show tech output from the switch to  
# be transferred via the supplied tftp server  
#####  
echo 'exit'  
read st  
echo 'copy command-output 'sh tech' tftp 10.1.2.1 $1-shTech.out  
read st
```

Figure 12-72. CLI Script Wizard - Simple Shell Script

This example shows a simple shell script that runs the show tech data command. The script is executed with the command line:

```
c:\showtech.sh %ip
```

In this example:

- The `showtech.sh` shell script is stored on the PCM Client PC at `c:\showtech.sh`.
- The results of the `sh tech` command are sent via TFTP to the output file: `$1-shTech.out`
- The script uses the first argument passed to it as `$1`.
- The IP Address of the PCM Agent is 10.1.2.1.
- PCM passes the IP address of the targeted switch as the first parameter to the script.
- No End of Result flag is required.

For the PC environment from which the script is run, you must preface the shell script with the `sh` command so that Windows understands how to run the script.

In this example, the TFTP server handles the transfer of data from the switch using the TFTP server in the PCM Agent directory. Because the script is executed against a device with the IP address 15.255.121.15, the resulting output file is: `15.255.121.15-shTech.out`, which is stored in the root directory of the PCM Agent's TFTP server.

Example: Multi-Command Shell Script

In this example, a shell script with multiple commands is executed with the command line: `sh c:\temp\sampleScript\countPorts.sh`

- The shell script retrieves switch information about the number of ports on the switch.
- No command-line substitution variables are used.
- The shell script performs some logging and writes information about the execution of the script to the file: `tsout.txt`.
 - If you execute the script using the Script Wizard, output is written to the default `PNM/client` directory.
 - If you execute the script using the Policy Manager, output is written to the default `PNM/server` directory.

Each command that the script executes, such as the `show ip` and `show sys` commands, appears in the Monitor Progress window of the Script Wizard.

The output file, `tsout.txt`, is stored in the `PNM/client` directory, and contains all statements that the shell script redirects to the `tsout.txt` file.

```
#####  
# This subroutine is used to read the response from the switch  
# and it then echoes the output to a file  
#####  
#  
function getDeviceOutput  
{  
    read st  
    while [[ "$st" != "$eor" ]]  
    do  
        print "$st" >> tsout.txt  
        read st  
    done  
}  
#####  
# This subroutine is used to read the response from the switch  
# and parse the output to count the number of interfaces  
# (ports) on the switch. Note that on the 2600 there are  
# 7 lines of header text that comes before the interface table,  
# so we read and discard 7 lines first.  
#####  
#  
function countPorts  
{  
    integer n=1  
    print "Value of n: $n" >> tsout.txt  
    while test n -lt 7  
    do  
        read st  
        print "Header: $st" >> tsout.txt  
        let "n=n+1"  
    done  
  
    read st  
    while [[ "$st" != "$eor" ]]  
    do  
        print "OutputText: $st" >> tsout.txt  
        read st  
        let "numPorts=numPorts+1"  
    done  
  
    let "numPorts=numPorts-1"  
    return numPorts  
}
```

Figure 12-73. CLI Script Wizard - Multi-Command Shell Script


```
#####  
# This is the beginning of the program  
#####  
print "Starting device" > tsout.txt  
#  
#  
eor="[EOR]"  
echo "show ip"  
getDeviceOutput  
  
#  
#  
echo "show sys"  
getDeviceOutput  
  
#  
echo "show interfaces brief"  
integer numPorts=0  
countPorts  
nports=$?  
print "Number of ports=$nports" >> tsout.txt  
  
echo "interface $nports name LastPort"  
read st
```

Figure 12-74. CLI Script Wizard - Multi-Command Shell Script (Continued)

Example: Perl Script

In this example, a Perl script with multiple commands is executed with the command line: `perl c:/temp/sampleScripts/showip.pl`

To run a Perl script, you must include the `perl` executable at the beginning of the command line. This sample Perl script produces the same output data as the previous example (“Example: Multi-Command Shell Script” on page 12-98). The resulting data is stored in an output file in the `PNM/client` directory.

```
#####  
# This subroutine is used to read the response from the switch  
# and it then echoes the output to a file  
#####  
#  
sub getDeviceOutput(outf) {  
    $input=<STDIN>;  
    print TSOUT $input;  
    $pos = -1;  
    while (($pos = index($input, $eor, 0)) < 0) {  
        $input=<STDIN>;  
        print TSOUT $input;  
    }  
}  
  
#####  
# This subroutine is used to read the response from the switch  
# and parse the output to count the number of interfaces  
# (ports)# on the switch.  
# Note that on the 2600 there are 7 lines of # header text that  
# comes before the interface table, so we read and discard  
# 7 lines first.  
#####  
#  
sub countPorts {  
    $n=1;  
    while ($n < 7) {  
        $input=<STDIN>;  
        print TSOUT $input;  
        $n=$n+1;  
    }  
  
    $input=<STDIN>;  
    print TSOUT $input;  
    $pos = -1;  
    while (($pos = index($input, $eor, 0)) < 0) {  
        $input=<STDIN>;  
        print TSOUT $input;  
        $numPorts=$numPorts+1;  
    }  
  
    $numPorts=$numPorts-1;  
}  
}
```

Figure 12-75. CLI Script Wizard - Perl Script

Managing Device Configurations Using a Script to Manage Device Configurations

```
#####  
# This is the beginning of the program  
#####  
  
# It is very important that Perl scripts start with this  
# command!!  
# This enables "command buffering" which automatically flushes  
# the output buffer after each newline  
$| = 1;  
  
# Open the output file where we will write out output "log"  
open(TSOUT, ">tsout.txt");  
print TSOUT "Starting Device\n";  
  
# This is the string we will  
# look for to terminate the  
# output from the switch  
$eor = "[EOR]";  
  
# First command sent to switch  
print "show ip\n";  
&getDeviceOutput;  
  
#  
#  
print "show sys\n";  
&getDeviceOutput;  
  
#  
print "show interfaces brief\n";  
$numPorts=0;  
&countPorts;  
  
print TSOUT ("Number of ports=" . $numPorts . "\n");  
print TSOUT "Done\n";
```

If you run a script using the Script Wizard, the output file is stored on the PCM Client in the PNM/Client directory.

If you run a script as a policy action from Policy Manager, the output file is stored on the PCM Server in the PNM/Server directory.

Figure 12-76. CLI Script Wizard - Perl Script (Continued)

Example: More Complex Perl Script

In this example, a more complex Perl script removes an entry from the trap receiver table in a switch.

```
#####  
# The following Perl script is useful for removing a certain  
# IP address from the snmp-server host table (trap receiver  
# destination) of a switch.  
# If the IP address does not exist, the switch is not modified.  
#  
# Usage:  
# The script requires two parameters be passed in to it:  
#   Parameter1: IP address of the target device  
#   Parameter2: IP address of the host to be removed  
#  
# Ex.:  perl rmsnmp.pl %ip 15.255.123.149  
# (Note that the PCM script wizard will insert the IP address  
# of each device it executes against as the first parameter  
# in place of the %ip)  
#  
# Creates a log file in the current working directory named:  
# 'removedSNMPHost.txt' listing what it did to each device  
#  
#####  
#  
#####  
# This subroutine is used to read the response from the switch  
# up to and including the [EOR]. All output from the switch  
# is discarded.  
#####  
#  
sub getDeviceOutput {  
    $input=<STDIN>;  
    $pos = -1;  
    while (($pos = index($input, $eor, 0)) < 0) {  
        $input=<STDIN>;  
    }  
}
```

Figure 12-77. CLI Script Wizard - More Complex Perl Script

Managing Device Configurations Using a Script to Manage Device Configurations

```
#####  
# This subroutine is used to read the response from the switch  
# and parse the output to look for the target host IP address.  
# If the output contains the target IP address, then  
# $found is set to 1 (true)  
#####  
sub getOutputAndLookforIP {  
    $input=<STDIN>;  
    $pos = -1;  
    while (($pos = index($input, $eor, 0)) < 0) {  
        $input=<STDIN>;  
        if (index($input, $iptarget, 0) < 0) {  
        } else {  
            $found=1;  
        }  
    }  
}  
  
#####  
# This is the beginning of the program  
#####  
  
# It is very important that Perl scripts start with this  
# command!! This enables "command buffering" which automatically  
# flushes the output buffer after each newline  
$| = 1;  
  
# First command line argument will expect the IP address of the  
# device  
$devIp=$ARGV[0];  
  
# Second command line argument will expect the IP host address  
# that is to be removed from the snmp-server host table on the  
# switch  
$iptarget = $ARGV[1];  
  
# Open the output file where we will write out output "log"  
open(TSOUT,">>removedSNMPHost.txt");  
print TSOUT "Device=" . $devIp . " Target IP=" . $iptarget;  
  
# This is the string we will look for to terminate the  
# output from the switch  
$eor = "[EOR]";
```

Figure 12-78. CLI Script Wizard - More Complex Perl Script (Continued)

```
# First command sent to switch
print "show snmp-server\n";
$found=0;
&getOutputAndLookforIP;

if ($found) {
    print "no snmp-server host " . $iptarget . " public\n";
    print TSOUT "    Found and removed " . $iptarget . " from
device\n\n";
    &getDeviceOutput;
    print "write mem\n";
    &getDeviceOutput;
} else {
    print TSOUT "    No target ip found\n\n";
}
}
```

Figure 12-79. CLI Script Wizard - More Complex Perl Script (Continued)

Working with Custom Groups

About Custom Groups	13-2
Rules of Custom Groups	13-2
Creating Custom Groups	13-3
Modifying Groups	13-4
Deleting a Group	13-5
Adding Devices to a Group	13-6
Removing Devices from Groups	13-8
Automatically Adding and Deleting Devices	13-8

About Custom Groups

By default, ProCurve defines device groups for each of the managed ProCurve device types and supported third-party devices. You can define custom groups, which can contain different device types and/or individual ports (or radios on wireless devices) from one or more devices. You can create custom groups for any reason such as to define a specific set of devices or ports for application of Policies, to simplify device management tasks, or for monitoring purposes.

Rules of Custom Groups

- Devices and ports/radios can belong to more than one group tree.
A group tree is a top-level folder under the Custom Groups node, including all groups, subfolders, devices, and ports/radios beneath it.
- Devices and ports/radios can only be assigned to leaf nodes.
A leaf node is an end node (device or port) in a branch of a group tree, which means that a leaf node has no child nodes.
- Devices and ports/radios cannot belong to more than one leaf node in a group tree.
- The devices and ports/radios in a custom group may span one or more PCM Agent Groups.
- If you do not use IDM but do use NIM and NIM alert-driven policies to apply mitigations to offenders' edge ports: Not all (if any) mitigations will be successfully applied in custom groups with devices that span multiple Agent Groups. This is because only the Agent Group where the alert occurred is searched for the offending edge port. Therefore, when creating custom groups, consider how they will be used and, if using them for NIM mitigations, avoid adding devices that span Agent Groups.

Creating Custom Groups

When creating groups, follow the instructions in this section and the rules listed in “Rules of Custom Groups” on page 13-2. But, before creating custom groups, it’s a good idea to identify what tasks would benefit from using custom groups and the hierarchy of these custom groups.

For example, you might want to create policies to stagger software updates on devices. You could create a custom group folder with subordinate folders for each location and custom groups for each group of devices in the location:

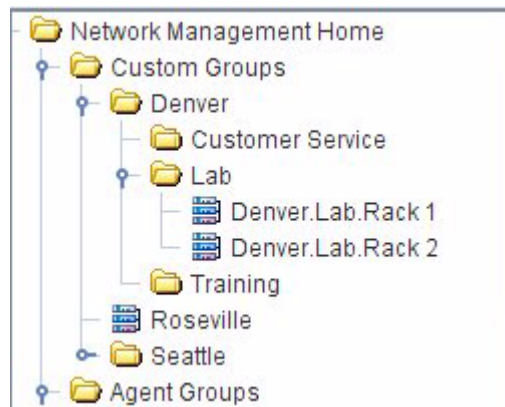


Figure 13-1. Custom Groups Hierarchy

Note:

When a custom group is created, it is added as a custom group folder. When a device is added to this "folder", it becomes a leaf node.

1. To create a custom group, expand the Custom Groups node in the navigation tree and select the node to which you want to add a new group. This displays the Custom Groups window in the right pane.

You can also right-click the custom group folder to which you want to add a new group and select **New...** from the right-click list.



2. Click the Add Group button in the toolbar to launch the Create Group dialog box.



Figure 13-2. Custom Groups, Create Group window

3. Type the Group Name. This is the name that will appear in the tree for the Group folder. The name can contain alphanumeric characters, spaces, and special characters except a period ".".
4. Optionally, type a brief description for the group in the Description field.
5. Click **Ok** to save the new Group and exit the window.

The navigation tree will be updated with the new Group information.

Modifying Groups

1. Expand the Custom Groups node in the navigation tree until the custom group to be modified is displayed and select the group.

You can also select the Custom Groups node in the navigation tree to display the Group Name list in the Custom Groups tab, and then select the group in the Group Name list.



2. On the Custom Groups tab or Folder List tab, click the Modify Group button in the toolbar.

OR

Right-click the custom group to be modified and select **Modify...** from the drop-down list.

The Modify Group dialog is displayed, (similar to Create Group) allowing you to edit the Group Name, Description, and devices/ports assigned to the group.

3. Optionally, change the Group Name and/or the Group Description.
4. Select Only add edge ports to add to the group those ports that are on an end device in a segment.
5. Select Only add inter-switch ports to add to the group those ports on switches that connect to at least two other switches.
6. In the Device Port Selection pane, unselect the device or port that you want to remove from the custom group by unchecking its Add to Group check box.
7. Click **Ok** to save your changes and update the Group information.

Deleting a Group

To delete a Group:

1. Select the folder containing the group(s) to be deleted, and click the Folder List tab.

OR

If you don't use custom group folders, click the Custom Groups node.

2. Select one or more Groups to be deleted.
3. Click the Delete Group button in the toolbar. A confirmation dialog will be displayed.
4. Click **Ok** to remove the Custom Group.



An alternate method for deleting a group is:

1. Expand the Custom Groups node in the navigation tree to display the custom group names.
2. Right-click the group name and select Delete... from the menu.

Adding Devices to a Group

Custom groups can contain any combination of ProCurve managed network devices or third-party devices discovered by PCM. You can create a group that consists of devices, or individual ports on a device (radios on a wireless device) to correspond with location-specific VLANs.

1. Open the Add Devices to Group window in one of the following ways, depending on whether you want to add one device or multiple devices.
 - For a single device only: In the navigation tree or a Devices List, right-click the device to be added to a custom group and select **Add to group**.
 - For a single device or multiple devices: Select the device(s) in the Devices List and click the Add Device to Group button in the toolbar.



You can use Shift + click or Ctrl + click to select multiple devices at once.

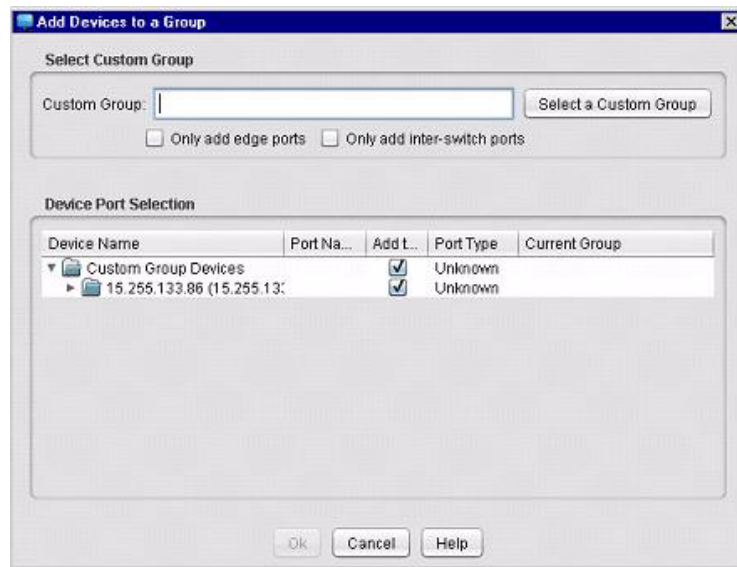


Figure 13-3. Add Device to a Group window

2. In the Add to Group window, click the **Select a Custom Group** button.



Figure 13-4. Select Group window


3. Select the group to which you want to add the device. The Select Group window lists all defined custom groups and leaf node folders, which will be converted to a group if selected.
4. Click **Ok** to return to the Add Device to Group window.

The Custom Group field is populated with the new Group information, and the Device Port Selection list includes the device(s) you added.
5. Optionally, to use a port classification to determine whether a port should be included in the group, select one of the following:
 - Only add edge ports - will include only ports classified as edge ports in the group.
 - Only add inter-switch ports - will include only ports classified as inter-switch (infrastructure) ports.
6. To add all ports in the selected device, check the Add to Group check box for the device.
7. To add specific ports/radios to a custom group:
 - a. Expand the device to show the device ports/radios.
 - b. Uncheck the Add to Group check box for the device to clear the selection for all ports/radios.

- c. Check the Add to Group check box for each port/radio you want to include in the custom group.
8. Click **Ok** to save your entries and close the Add Device to Group window.
The new Group appears in the navigation tree on the left.

Removing Devices from Groups

To remove a device from a single group:

1. Expand the Custom Groups node in the navigation tree to display the group you want to remove the device from.
2. In the Device tab for the group, select the device to be removed from the group.
-  3. Click the Remove from Group button in the toolbar.
4. On the Remove Devices from Group confirmation window, ensure that the correct device was selected for removal and click **Ok**.

To remove a device from one or more groups using the navigation tree:

1. In the navigation tree, right-click the device to be removed.
2. Select Remove from Group from the drop-down list.
3. Select the group(s) from which the device will be removed.
4. Click **Remove**.

To remove a port from a group:

1. Follow the instructions for modifying a group, as explained in “Modifying Groups” on page 13-4.
2. Deselect the ports to be removed.

Automatically Adding and Deleting Devices

Use the Group Member Wizard to add devices to a custom group based on the filters selected. It also allows you to remove devices that do not match the selected filters from a custom group and automatically add any newly discovered devices that match the filters to the group.

However, devices that are already discovered when the group filter is created are not added automatically to the group. In addition, the group assignment is not updated when the group to which a discovered device belongs changes. The Group Member Wizard updates the group assignment for these devices.

To run the Group Member Wizard:

1. In the navigation tree, click the Custom Groups node.
2. In the Custom Groups pane, click the Custom Groups tab, select the name of the group, and click the **Group Member Wizard** button.



The Group Member Wizard is accessible for any leaf node. A leaf node is a custom group (container of device and/or ports) or custom group folder with no subfolders.

3. In the Welcome screen of the Group Member wizard, click **Next**.
4. In the Filters window, select the filters you want to use to display the desired devices for the custom group:

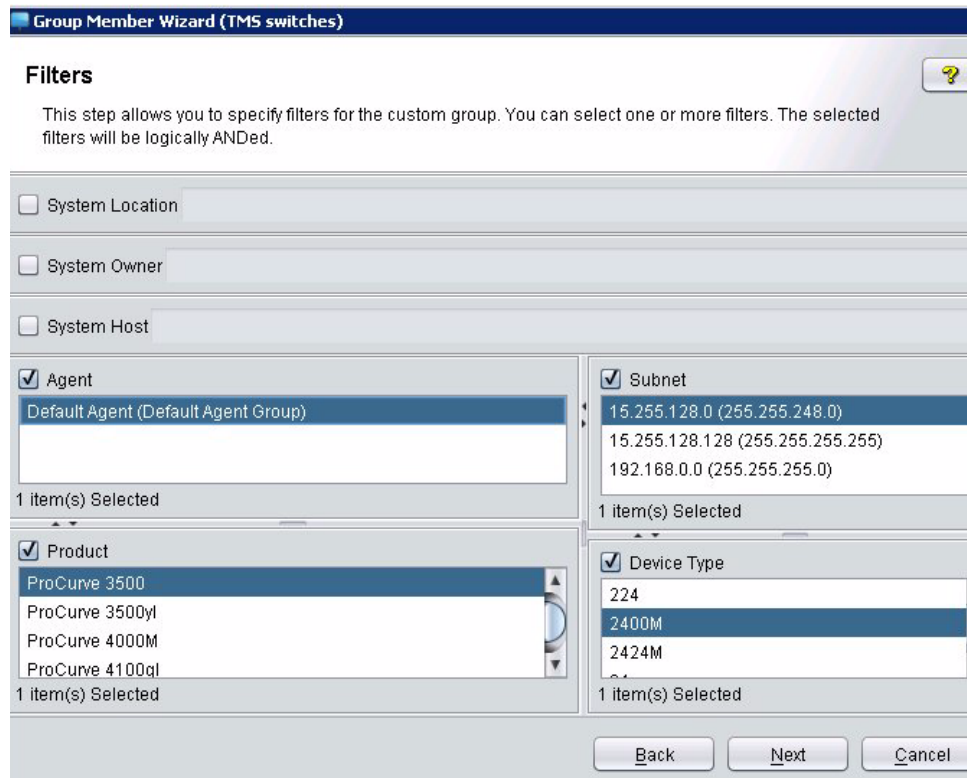


Figure 13-5. Group Member Filters

The following filters are available:

Filter	Description
System Location	System Location (Be sure to type the complete location as it appears on the device.)
System Owner	Contact person for the devices (Be sure to type the complete name as it appears on the device.)
System Host	System name (Be sure to type the complete name as it appears on the device.)
Agent	PCM Agent that manages the devices
Subnet	Subnet containing the devices
Product	Product series (e.g., 5400zl)
Device Type	SysOID of the device (e.g., 5412zl)

Select any combination of filters and multiple Agents, Subnets, Products, and Device Types. Then click **Next**.

5. In the Results window:
 - a. Click **Apply Filters** to display the list of desired devices.
 - b. Do one of the following:
 - To remove all devices from the group that do not match the filter criteria, select the check box for Remove devices not matching filters.
 - To automatically add any newly discovered devices that match the filter criteria to the group, select the check box for Automatically add newly discovered devices matching the filters.
 - c. Click **Next**.

Using VLANs

About VLANs	14-2
Viewing VLAN Groups (Maps)	14-3
Creating a VLAN	14-6
Modifying VLANs	14-9
Configuring Multiple IP Addresses for VLANs	14-9
Adding a Device to a VLAN	14-10
Removing a Device from a VLAN	14-13
Making VLANs Static	14-14
Making a VLAN Primary	14-15
Deleting a VLAN	14-16
Modifying VLAN Support on a Device	14-17
VLAN Support on Wireless Devices	14-18
Port Assignments on a Device	14-22
Modifying Port Assignments	14-23
Modifying GVRP Port Properties	14-24
Using IGMP to Manage Multicast Traffic	14-25
Enabling IGMP on VLANs	14-25
IGMP Settings for Routing Switches	14-29

About VLANs

A VLAN is a group of ports designated by the switch as belonging to the same broadcast domain. That is, all ports carrying traffic for a particular subnet address would belong to the same VLAN.

Using a VLAN, you can group users by logical function instead of physical location. This helps to control bandwidth usage by allowing you to group high-bandwidth users on low-traffic segments and to organize users from different LAN segments according to their need for common resources.

The benefits of VLANs include:

- Grouping users into logical networks for increased performance.
- Providing an easy, flexible, less costly way to modify logical groups in changing environments.
- Preserving current investment in equipment and cabling.
- Allowing administrators to “fine tune” the network.
- Providing independence from the physical topology of the network.
- Improved security for the network.

At default settings, all ports on ProCurve wired switches are members of the default VLAN, with a VLAN ID of 1 and VLAN Name DEFAULT_VLAN. This means that, until you have defined additional VLANs, all of the hosts connected to these switches are in the same VLAN.

The default VLAN is also the primary VLAN. The primary VLAN is the VLAN the switch uses to run and manage DHCP or Bootp, and stacking features. You can designate another VLAN as primary; however it must be a static VLAN, it cannot be a dynamic (GVRP learned) VLAN.

You can use the PCM VLAN Manager to partition switches into multiple virtual broadcast domains by adding one or more additional VLANs and configuring ports for the new VLANs. You can change the name of the default VLAN, but you cannot change the default VLAN's ID (which is always “1”). Although you can remove all ports from the default VLAN, this VLAN is always present; that is, you cannot delete it from the switches that have this default configuration.

For a more detailed description of VLANs and GVRP, please refer to the "Management and Configuration Guide" for your switch.

Viewing VLAN Groups (Maps)

To view a listing of currently configured VLANs in your network, expand the Network Map node in the navigation tree, then click the VLANS node.

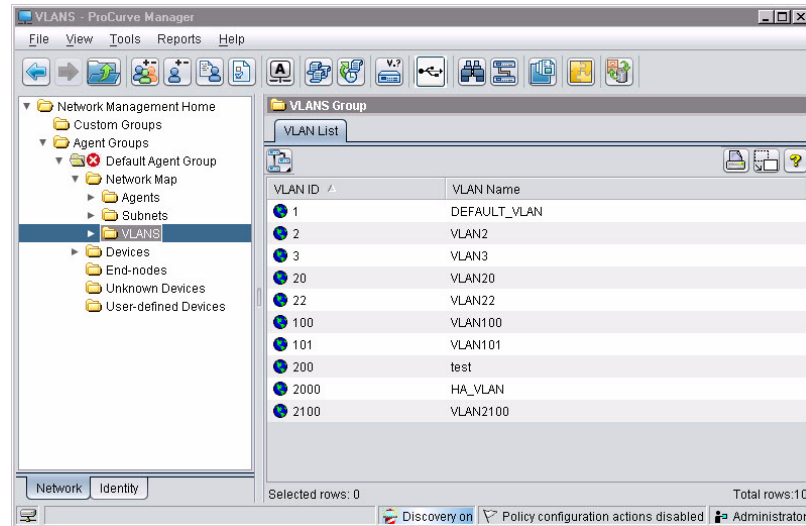


Figure 14-1. VLAN List

You can click the VLAN in either the navigation tree or the VLAN list to view the VLAN Map.

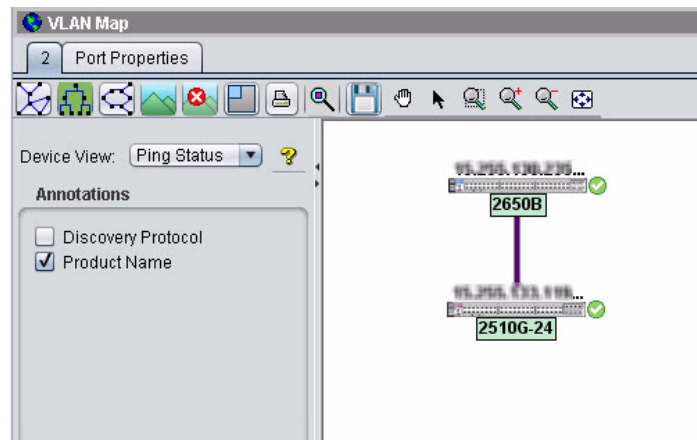


Figure 14-2. VLAN Map display

The VLAN ID (VID) is shown on the tab for the display, and the Port Properties tab is enabled. Otherwise, the map functionality is the same as described in Chapter 5, “Using Maps”.

To review the port properties for the VLAN, click the Port Properties tab. This is a view only display, you cannot alter the port properties in this screen. Refer to the discussion of VLAN Port configuration on page 14-7, or “Modifying Port Assignments” on page 14-23 for more information.

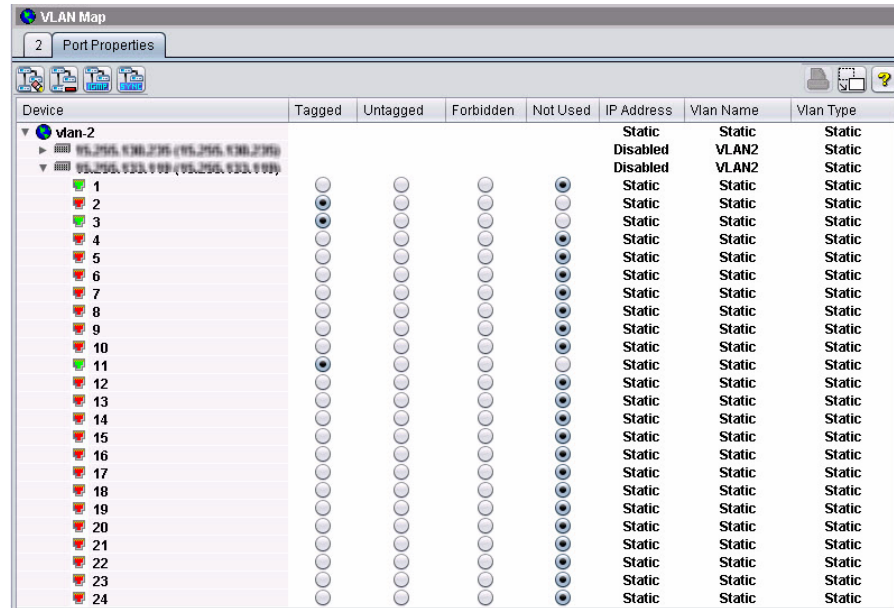


Figure 14-3. VLAN Port Properties display.

The VLAN Port Properties display lists

- The device and ports
- The port properties, one of:
 - Tagged: Port can be included in multiple VLANs.
 - Untagged: Port can be included in only one VLAN.
 - Forbidden: Port cannot be included in this VLAN.
 - Not Used: The port is not included in this VLAN.
- IP Address if applicable
- VLAN Name
- VLAN Type (static or dynamic)

VLAN Configuration Detail

To review the VLANs configurations for the device:



- Select the device in a Devices List, then select the Show VLANs option from the VLAN toolbar menu, or
- Select the device in the Navigation tree and use the right-click menu to select VLAN Manager > Show VLAN.



VLAN Name ^	VLAN Id	VLAN Type	Management V...
DEFAULT_VLAN	1	Static	No
VLAN2	2	Static	No
VLAN3	3	Static	No

Figure 14-4. Show VLAN List for Device window.

The VLAN list includes the VLAN Name, ID, Type, and Management status for all VLANs configured on the device.

Creating a VLAN

You can create a VLAN using the VLAN Wizard as described in this section, or using a VLAN Policy. See Chapter 16 “Using Policy Manager Features” for details.



To launch the Create VLAN Wizard:

1. Select a device in the Devices List tab, then use right-click menu or toolbar menu to select VLAN Manager > Create VLAN.

The following examples of the Create VLAN Wizard dialogs explain the data needed to create a VLAN.

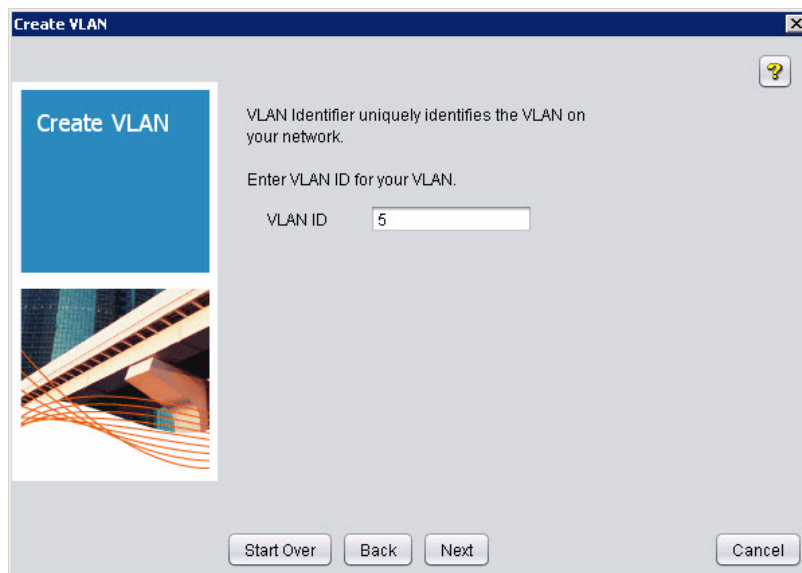


Figure 14-5. Set VLAN ID dialog

2. Enter **VLAN ID**. This is a numeric value between 2 and 4094. The number 1 is reserved for the default VLAN.
3. In the next dialog, configure how the IP Address information for the VLAN will be determined, and configure the ports on the device to be included in the VLAN.

Note that the Port column lists the port number on the device, and whether or not the port is currently active (green), or disabled (red).

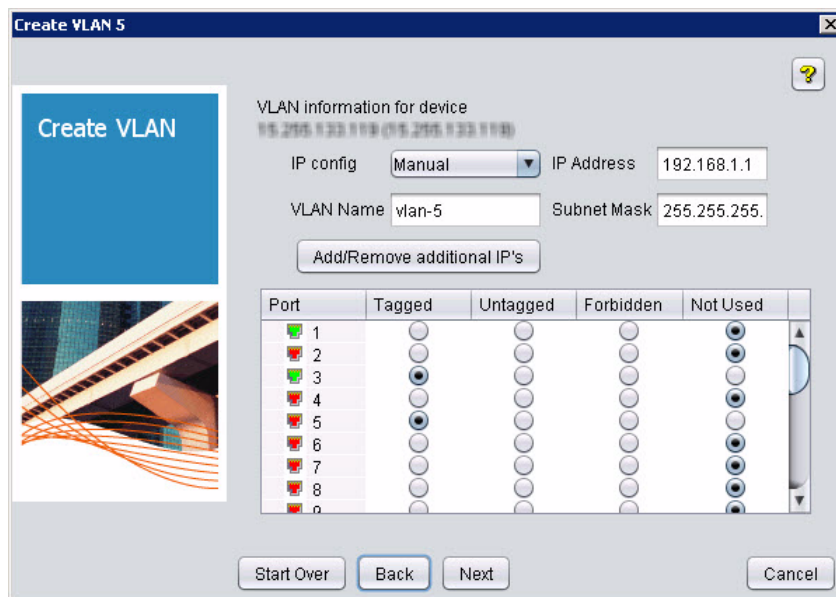


Figure 14-6. VLAN Port configuration dialog

- a. Use the drop down menu to select the **IP Config** method for the IP address used for the VLAN:
 - Manual: Set the IP address at the console. When selected, the IP Address and Subnet Mask fields will be enabled so you can type the IP Configuration information. This also enables the Add/Remove additional IPs option.
 - Disabled: IP is disabled and there is no access to management or telnet. **NOT RECOMMENDED**
 - DHCP/Bootp: The Bootp (or DHCP) protocol automatically sets the IP Address. This is used for dynamic VLANs with devices that support GVRP (IEEE 802.1Q standard)
- b. If the device supports multiple IP addresses (multinetting) and you select **Manual** IP configuration, click the **Add/Remove additional IP's** button and enter the IP address and related subnet mask for each additional IP address used.
- c. Use the radio buttons to select the VLAN option for each port. If you select the option at the top level (A, B, etc.) for a group of ports, it will be applied to all ports in the group.

The VLAN port options are:

- **Tagged:** Port can be included in multiple VLANs.
- **Untagged:** Port can be included in only one VLAN.
- **Forbidden:** Port cannot be included in this VLAN.
- **Not Used:** The port is not included in this VLAN.

If the device does not support 802.1Q (GVRP), or GVRP on the device is Disabled, the Forbidden button will be disabled.

For 9300 series switches, if a port has been classified as tagged in another VLAN, the Untagged option is disabled, and vice versa (once classified as untagged, it cannot be tagged in another VLAN).

4. In the next screen you can review the VLAN port configurations.

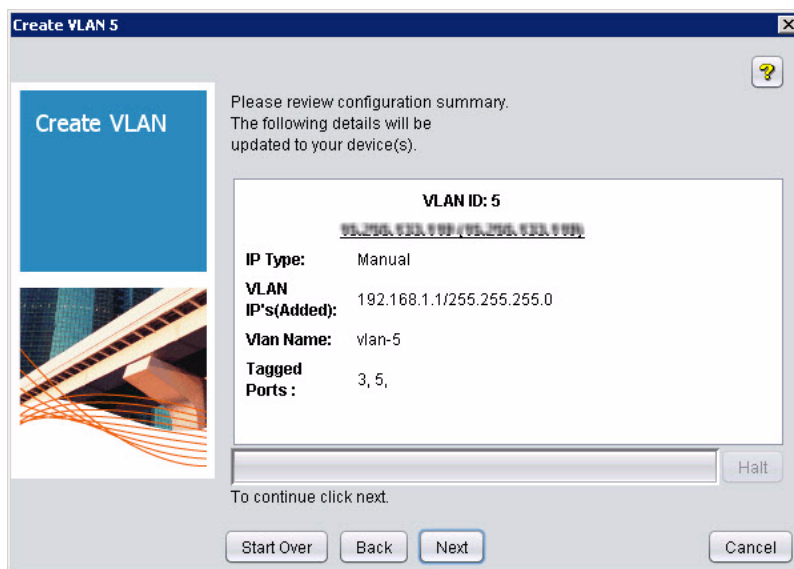


Figure 14-7. VLAN Configuration Review dialog

To complete the Create VLAN process, click **Next**. Devices shown in the list will be rebooted when the VLAN is configured. To halt the process before it completes, click Halt.

If you are not satisfied with the configuration, click Back to return to the configuration screen, or Start Over to return to the Set VLAN ID dialog.

5. Once the VLAN configuration is complete, click **Close** in the final Create VLAN dialog to exit the Create VLAN wizard. The VLAN list should be updated with the new VLAN ID.

Modifying VLANs



To modify a VLAN's configuration:

1. Click the VLAN node in the navigation tree to display the list of VLANs.
2. Select the VLAN ID in the list
3. Use the right-click menu or toolbar menu and select VLAN Manager > Modify VLAN.

This launches the Modify VLAN Wizard, which works similarly to the Create VLAN wizard (see Chapter page 14-6). You can change the IP Address settings and Port settings for devices in the VLAN.

Configuring Multiple IP Addresses for VLANs

You can configure multiple IP Addresses to support "multi-netting" using the VLAN wizard.

To use multiple IP addresses in a VLAN:

1. Use the Create VLAN or Modify VLAN option to launch the VLAN wizard.
2. Select the **Manual** option for IP config to enable the **Add/Remove Additional IPs** button, then click the button to launch the Multinetting window.

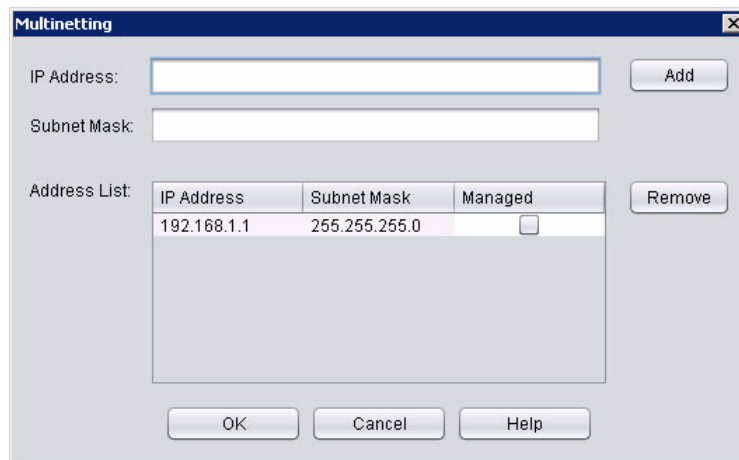


Figure 14-8. Multinetting, for VLAN configuration

3. Enter the additional **IP Address** and **Subnet Mask** that you want to associate with the VLAN. The IP Address must be on a different network.

4. Click **Add**.
The IP address that you just defined is added to the Address List.
5. Repeat the process for any additional IP addresses you want to use.
6. Click **OK** to save your changes and return to the VLAN wizard, then continue through the screens to exit the wizard.

To remove an IP address:

1. Use the Create VLAN or Modify VLAN option to launch the VLAN wizard.
2. In the VLAN/Port properties dialog of the wizard, click **Add/Remove Additional IPs**.
3. In the Address List pane of the Multiple IP Addresses window, select the IP address you want to remove from the VLAN.
4. Click **Remove**.
The IP address is deleted from the Address List.
5. Click **OK** to save your changes and return to the VLAN wizard, then continue through the screens to exit the wizard.

Adding a Device to a VLAN



To add another device to a VLAN that you have already created:

1. Select the device in the Devices List or in the navigation tree, then use right-click menu or toolbar menu to select VLAN Manager > Add to VLAN.

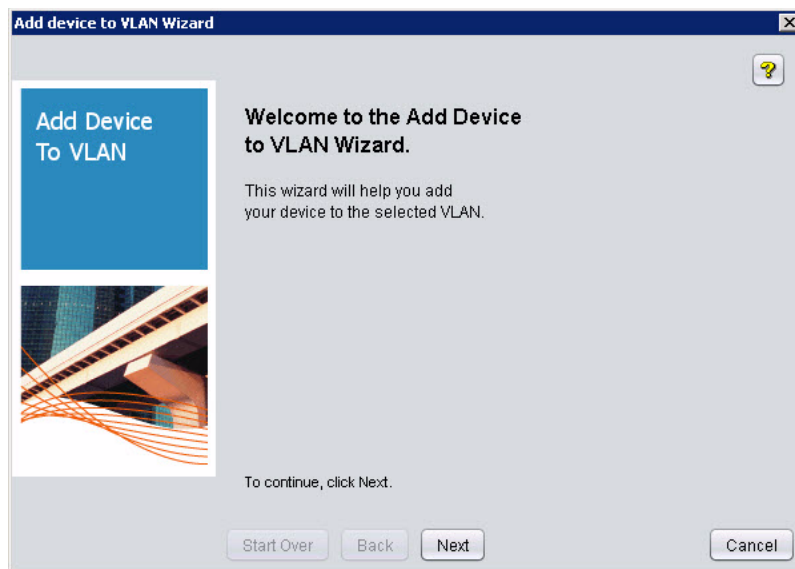


Figure 14-9. Add Devices to VLAN wizard

2. Click **Next** to continue.

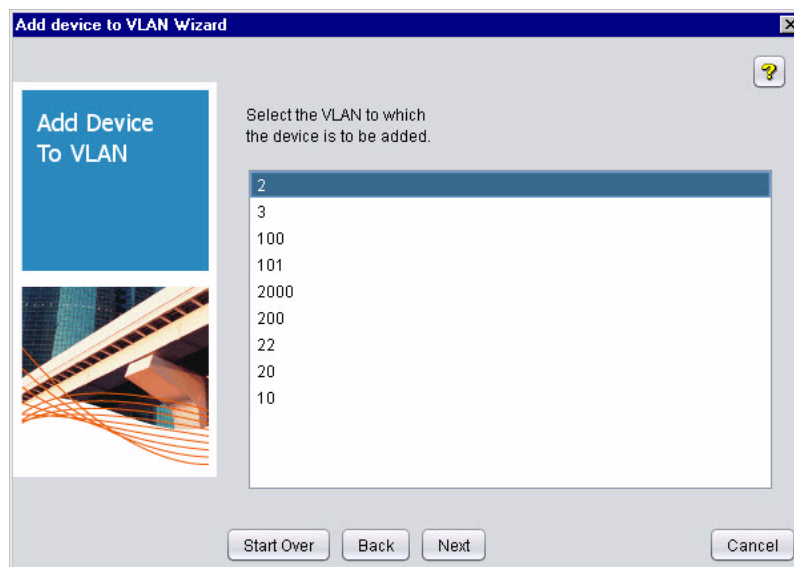


Figure 14-10. Select VLAN

3. Click to select the VLAN where you want to add the device.

If the device is not configured for VLAN support, you will get the following dialog prior to being allowed to add the device to a VLAN.

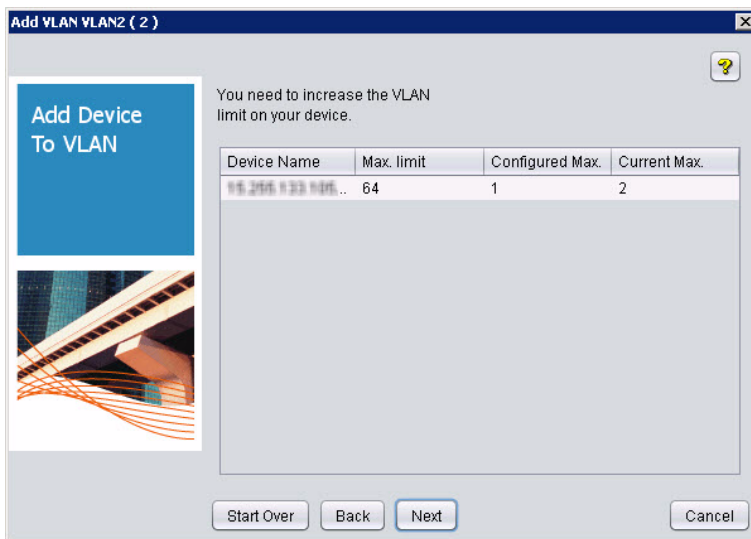


Figure 14-11. VLAN Limit

4. Click **Next** in the VLAN selection dialogue to continue to the Port configuration dialogue.

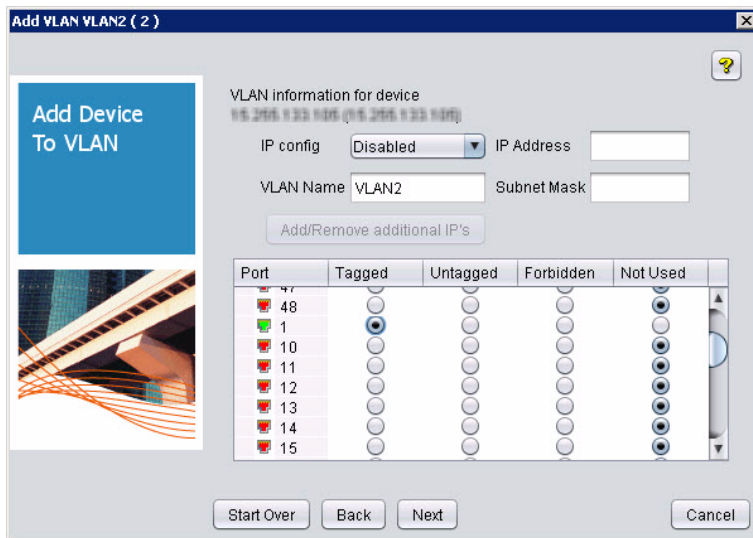


Figure 14-12. VLAN Port Configuration dialog

5. Configure the ports for the VLAN, then proceed through verifying and applying the configuration as described under “Creating a VLAN” on page 14-6.

Synchronizing the VLAN Name

If you add a new device with the wrong VLAN Name, or modify the VLAN name and want to make sure that it appears for all devices (ports) in the VLAN, you can use the "Synchronize" feature to apply the VLAN name to all devices configured in the VLAN.



To synchronize the VLAN name on all devices in a VLAN:

1. Navigate to the VLAN's Port Properties tab (Network Maps > VLANs > VLAN ID), and click the Synchronize button in the toolbar.

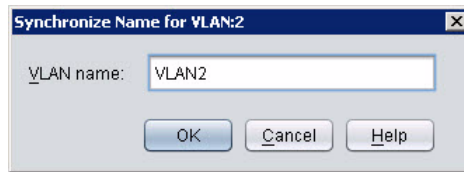


Figure 14-13. Synchronize VLAN Name dialog

2. Enter the **VLAN name** to be used, then click OK.

PCM will check the VLAN name to ensure that it is not a duplicate. If it is already used for another VLAN, you will get an error message. Otherwise, the VLAN name will be updated on all devices in the VLAN and the new name will appear in the Port Properties display.

Removing a Device from a VLAN

To remove a device from a VLAN,

1. Select the device in the Devices List or the VLAN map, then right click and select **Remove from VLAN** on the menu or,
2. Right-click the device in the navigation tree or Devices List, then select the VLAN Manager → Remove from VLAN option in the menu.



The Select VLAN dialog will be displayed.

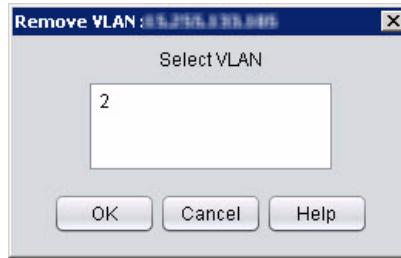


Figure 14-14. Select VLAN, to delete from device

3. Select the VLAN(s) from which the device is to be removed, then click **OK**. You will get a confirmation dialog, click **Yes** to complete the process.

To complete the process and have the changes appear correctly in the VLANs Map display, you may need to do a Manual Discovery, or Re-discover on the device.

Making VLANs Static

You can configure a dynamic VLAN (using DHCP/Bootp), then decide at a later time convert it to a static VLAN.

To convert a VLAN from dynamic to static:

1. Expand the navigation tree to select the VLAN,
2. Click the VLAN node to display the map.
3. Right click a device in the VLAN map,
4. Select the Make VLAN Static option from the VLAN Manager menu.

A dynamic VLAN does not have an IP address, it moves traffic on the basis of port membership in VLANs. However, after you convert a dynamic VLAN to a static VLAN, it is then necessary to assign ports to the VLAN in the same way you would for a manually configured VLAN.

Making a VLAN Primary

Because certain features and management functions run on only one VLAN in the switch, and because DHCP and Bootp can run per-VLAN, there is a need for a dedicated VLAN to manage these features and ensure that multiple instances of DHCP or Bootp on different VLANs do not result in conflicting configuration values for the switch. The *primary* VLAN is the VLAN the switch uses to run and manage these features and data. In the factory-default configuration, the switch uses the default VLAN (VID 1) as the primary VLAN. However, to provide more control in your network, you can designate another VLAN as primary.

Designating a non-default VLAN as primary means that:

- The stacking feature runs on the switch's designated primary VLAN instead of the default VLAN
- The switch reads DHCP responses on the primary VLAN instead of on the default VLAN.
- The default VLAN continues to operate as a standard VLAN (except, as noted previously, you cannot delete it or change its VID).
- Any ports not specifically assigned to another VLAN will remain assigned to the Default VLAN, regardless of whether it is the primary VLAN.

Candidates for primary VLAN include any static VLAN currently configured on the switch. (A dynamic—GVRP-learned—VLAN that has not been converted to a static VLAN cannot be the primary VLAN.)

To designate a VLAN as Primary:

1. Expand the navigation tree to select the VLAN,
2. Click the VLAN node to display the map.
3. Right-click a device in the VLAN map,
4. Select the Make VLAN Primary option from the VLAN Manager menu.

Note that the Make VLAN Primary option is disabled if the VLAN is dynamic.

If you configure a non-default VLAN as the primary VLAN, you cannot delete that VLAN unless you first select a different VLAN to act as primary.

Deleting a VLAN

To delete a VLAN:



1. Select the VLAN in the navigation tree or VLANs list, then select the VLAN Manager →Delete VLAN option from the right-click menu, or toolbar.

Prior to deleting the VLAN, make sure that all ports are assigned to a different VLAN. If the ports in the VLAN are all "Tagged" this should not be a problem as they should still be included in the Default VLAN (VID 1). If the Ports are "Untagged" the VLAN manager will re-assign the ports to the Default VLAN.

You cannot delete the Primary VLAN, and you cannot delete the Default VLAN (VID 1).

Modifying VLAN Support on a Device



To modify the VLAN support on a device:

1. Click the device node in the Navigation tree (or in the Devices List) to display the Dashboard tab,
2. Use the right-click menu or toolbar to select the VLAN Manager → Modify VLAN Support option.

Note that you must use the toolbar to access wireless devices. This launches the VLAN Properties Info dialogue.

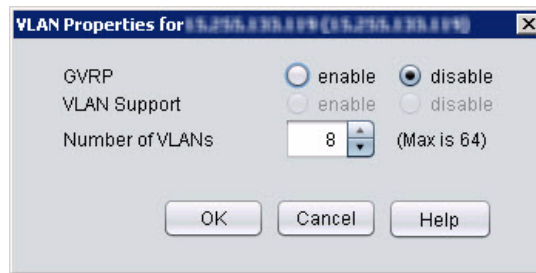


Figure 14-15. VLAN Properties (Support for VLAN on device)

3. If the device is **GVRP** capable, you can select to **Enable** or **Disable** support for GVRP.

For devices that are not GVRP capable (such as 1600 and 4000m series) you can Enable or Disable **VLAN Support**.

4. The **VLAN Value** indicates the **Maximum** number of VLANs to which ports on the switch can be assigned. The **Current** field indicates the number of VLANs currently configured per port. You can increase or decrease the current number of allowed VLANs.
5. Click **OK** to apply the changes and close the dialogue

NOTE

Enabling VLAN support can cause the selected device to reboot.

VLAN Support on Wireless Devices

Options specific to configuring VLAN support on ProCurve Wireless devices are described below.

VLAN Support on AP420 Devices:

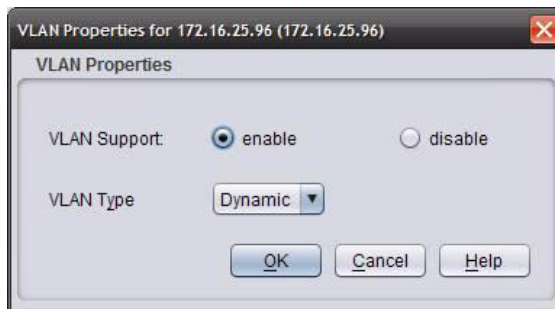


Figure 14-16. VLAN Properties for AP420

1. Click the **Enable** button to enable VLAN support.
2. Use the **VLAN Type** drop-down list to select the type of VLAN.

OR

If using an older software version, in the **Native VLAN ID** field, type the VLAN ID of the native VLAN for the device.

3. Press **OK** to apply these changes to the device.
Click **Cancel** to close the window without saving your changes.

Note:

For AP420 devices, the Telnet password must be set, or the Modify VLAN Support feature will not work.

VLAN Support on 520wl Devices:

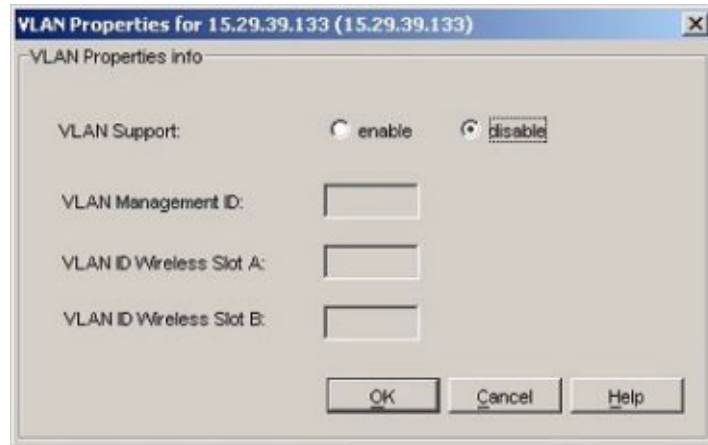


Figure 14-17. VLAN Properties for 520wl

1. To enable **VLAN support**, click the **Enable** button.
2. In the **VLAN Management ID** field, type the ID of the VLAN you want to set as the management VLAN. The management VLAN is used by PCM to manage the network.
3. In the **VLAN ID Wireless Slot A** and **Slot B** fields, type the VLAN ID of the VLAN you want to associate with each slot on the device.
4. Press **OK** to apply these changes to the device.
Click **Cancel** to close the window without saving your changes.

Note:

Enabling VLAN support can cause the selected device to reboot.

VLAN Support for 520wl With Version 2.4.5 or Newer Software

If you have installed version 2.4.5 of the 520wl switch software, the VLAN properties dialog will appear as follows:

Using VLANs
Modifying VLAN Support on a Device

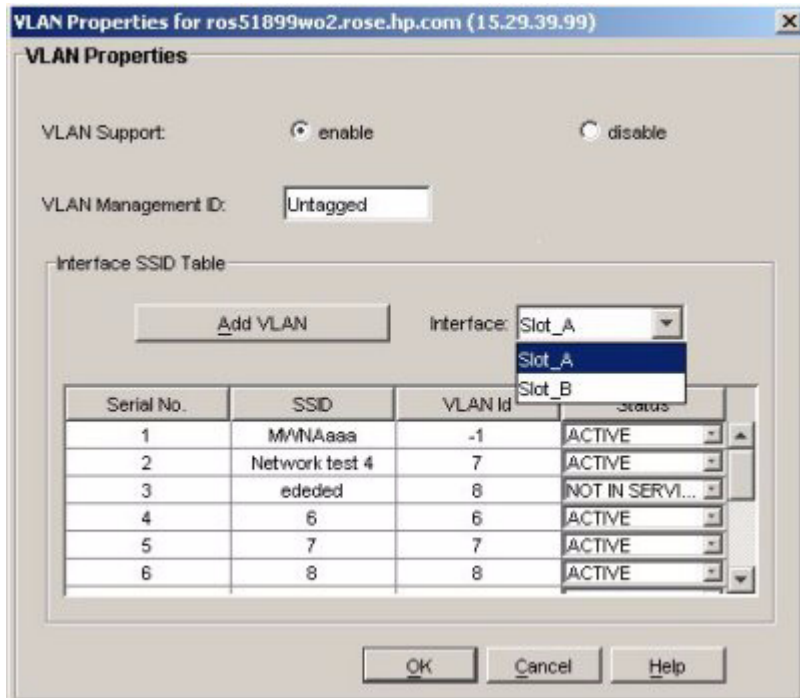


Figure 14-18. VLAN Properties for 520wl, running version 2.4.5 software

1. In the **VLAN Management ID** field, type the ID of the VLAN you want to set as the management VLAN. You can enter a number from -1 to 4094, or type "Untagged" (-1 is equivalent to Untagged).
2. You can edit the SSID (network) name. Just click in the **SSID** field of the table for the interface you want to edit.
3. To edit the VLAN ID, click in the VLAN Id field to select it then enter the number you want to assign.
4. Click in the **Status** field, then select the Status from the pull-down menu. The options are Active, Delete or Not in Service.
If you select the Delete option, the VLAN will be removed.
5. Click the **Add VLAN** button to add a SSID/VLAN pair to an interface.



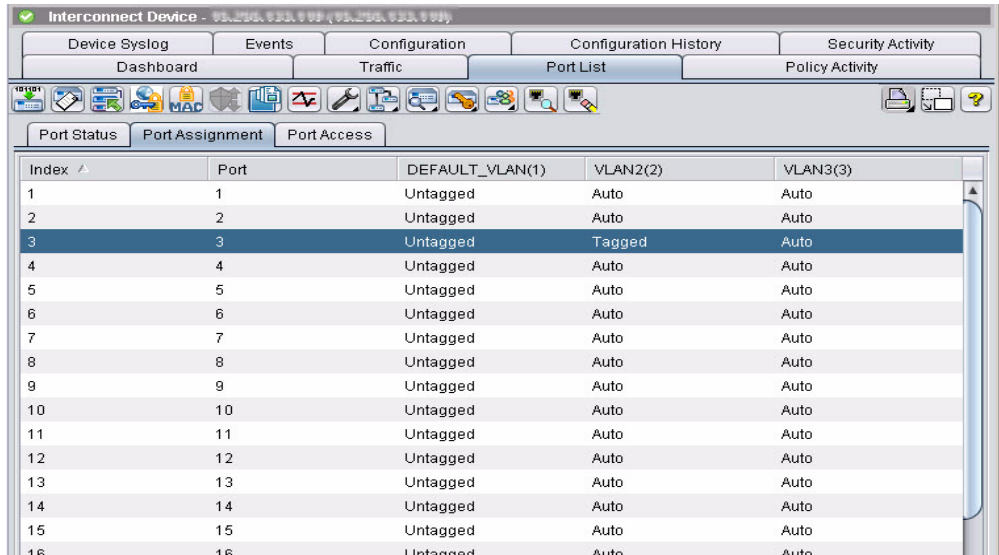
Figure 14-19. Add VLAN for 520wl

- a. Enter the **VLAN ID**, either Untagged, or a number from 1-4094.
- b. Enter the **SSID** (network name) for the VLAN.
- c. Select the **Status** from the pull-down menu. "Active" or "Not In Service."
- d. Click **OK** to save the new VLAN configuration and close the dialog.

If the interface (network card) does not support multiple SSIDs, only the SSID and VLAN Id fields are editable, the Status will always be Active, and the Add VLAN button will be disabled.

Port Assignments on a Device

To review the current port assignments for the Device, click the Port Assignment tab in the Port List.



Index	Port	DEFAULT_VLAN(1)	VLAN2(2)	VLAN3(3)
1	1	Untagged	Auto	Auto
2	2	Untagged	Auto	Auto
3	3	Untagged	Tagged	Auto
4	4	Untagged	Auto	Auto
5	5	Untagged	Auto	Auto
6	6	Untagged	Auto	Auto
7	7	Untagged	Auto	Auto
8	8	Untagged	Auto	Auto
9	9	Untagged	Auto	Auto
10	10	Untagged	Auto	Auto
11	11	Untagged	Auto	Auto
12	12	Untagged	Auto	Auto
13	13	Untagged	Auto	Auto
14	14	Untagged	Auto	Auto
15	15	Untagged	Auto	Auto
16	16	Untagged	Auto	Auto

Figure 14-20. Port List: Port Assignment table

The table lists each of the VLANs to which a port is assigned and current configuration of the port VLAN support (tagged, untagged, etc.)

Modifying Port Assignments



Select a port and click the Modify Port Assignment button in the toolbar to change the VLAN port assignments. This will launch the Port Assignment Table window.

Index	Port	DEFAULT_VLAN(1)	VLAN2(2)	VLAN3(3)
1	1	Untagged	Auto	Auto
2	2	Untagged	Auto	Auto
3	3	Untagged	Tagged	Auto
4	4	Untagged	Auto	Auto
5	5	Untagged	Auto	Auto
6	6	Untagged	Auto	Auto
7	7	Untagged	Auto	Auto
8	8	Untagged	Auto	Auto
9	9	Untagged	Auto	Auto
10	10	Untagged	Auto	Auto
11	11	Untagged	Auto	Auto
12	12	Untagged	Auto	Auto
13	13	Untagged	Auto	Auto
14	14	Untagged	Auto	Auto
15	15	Untagged	Auto	Auto
16	16	Untagged	Auto	Auto
17	17	Untagged	Auto	Auto
18	18	Untagged	Auto	Auto
19	19	Untagged	Auto	Auto
20	20	Untagged	Auto	Auto
21	21	Untagged	Auto	Auto

Figure 14-21. Port Assignment Table window

To modify port assignments:

1. Click the VLAN properties cell in the table. This will enable a pull-down menu you can use to select the option you want to have for the port in that VLAN. The VLAN port options are:
 - Tagged: Port can be included in multiple VLANs.
 - Untagged: Port can be included in only one VLAN.
 - Forbidden: Port cannot be included in this VLAN.
 - Auto: The port is not included in this VLAN.

Change the port properties as needed, then click **Apply** to save the changes and close the Port Assignment Table.

Modifying GVRP Port Properties

To modify VLAN support by individual port on a device that supports GVRP:



1. Click the Modify GVRP Port Properties button in the Port Assignment Table toolbar.

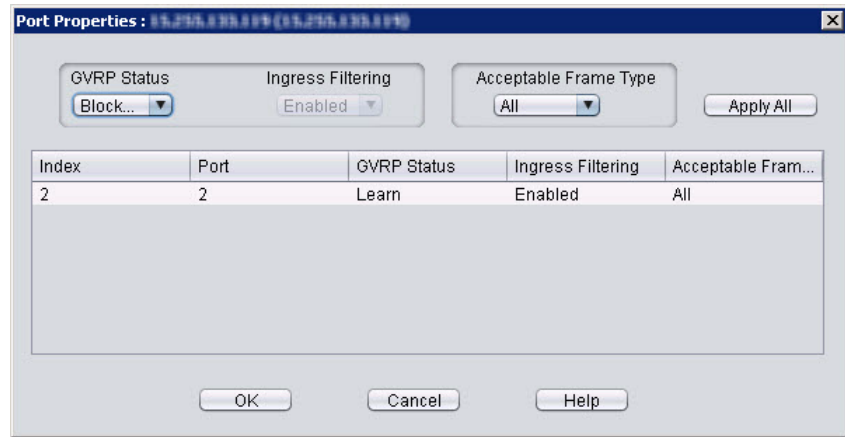


Figure 14-22. Device Properties: Port Properties dialog.

2. Select the **GVRP status** for the port: Blocked, Learn, or Disabled.
3. Select the **Acceptable Frame Type**: All or Tagged.
4. Click **Apply** to update the Port Properties display, then click **OK** to close the dialog.

Using IGMP to Manage Multicast Traffic

This section describes how to configure IGMP controls to reduce unnecessary bandwidth usage on a per-port basis in your VLANs.

In a network where IP multicast traffic is transmitted for various multimedia applications, you can reduce unnecessary bandwidth usage on a per-port basis by configuring IGMP (Internet Group Management Protocol) controls. In the factory default state (IGMP disabled), the switch simply floods all IP multicast traffic it receives on a given VLAN through all ports on that VLAN (except the port on which it received the traffic). This can result in significant and unnecessary bandwidth usage in networks where IP multicast traffic is a factor.

Enabling IGMP (on switches that support it) allows the ports to detect IGMP queries and report packets, and manage IP multicast traffic through the switch. Using IGMP, switches can be configured to direct the multicast traffic to only the ports where needed. If multiple VLANs are configured, you can configure IGMP on a per-VLAN basis.

For a more detailed description of using IGMP on ProCurve devices, refer to the "Management and Configuration Guide" for your switch.

Enabling IGMP on VLANs

IGMP configuration on the switch operates at the VLAN context level. If you are not using VLANs, then configure IGMP in VLAN 1 (the default VLAN) context.

To enable IGMP settings on a VLAN, select the VLAN node in the navigation tree and display the Port Properties tab.



1. Select the IGMP option from the toolbar to launch the IGMP Settings Wizard. (You can also select the IGMP Settings option from the right-click menu.)
2. Click **Next** in the "Welcome" dialog to continue.

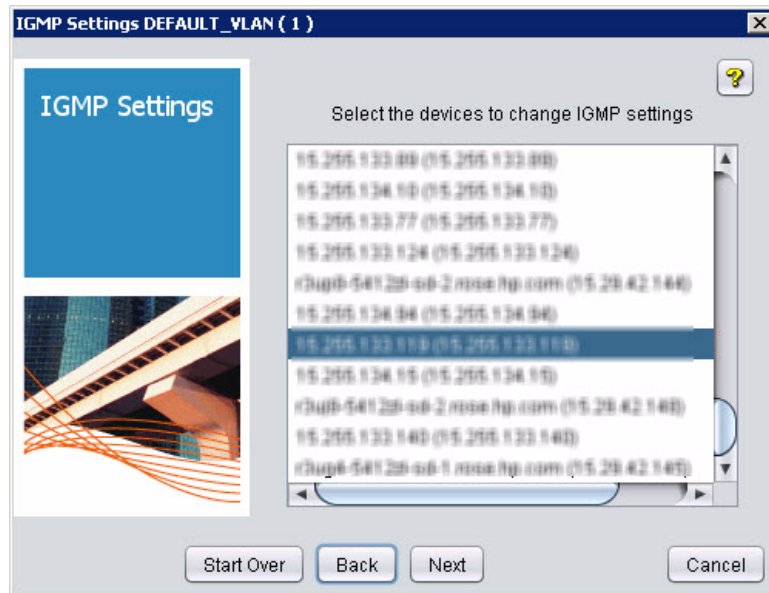


Figure 14-23. IGMP Device Selection dialog.

3. Click to select the device(s) on which you want to change the IGMP settings, then click **Next**.

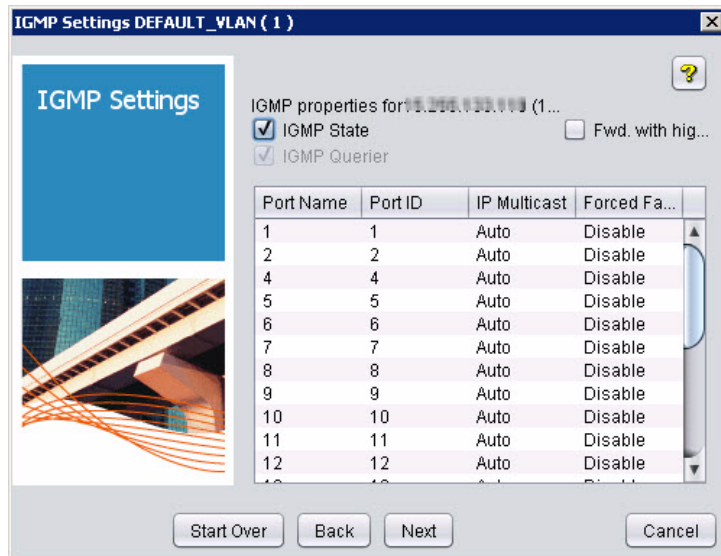


Figure 14-24. IGMP Properties dialog

4. Use IGMP Settings dialog to enable or disable multicast operations. The wizard lists the following information about ports on the selected device:

Port Name	The name used to identify the port
Port ID	The port number
IP Multicast	Indicates the individual ports are configured to one of the following states: Auto (the default): Causes the switch to interpret IGMP packets and to filter IP multicast traffic based on the IGMP packet information for ports belonging to a multicast group. This means that IGMP traffic will be forwarded on a specific port only if an IGMP host or multicast router is connected to the port. Blocked: Causes the switch to drop all IGMP transmissions received from a specific port and to block all outgoing IP Multicast packets for that port. This has the effect of preventing IGMP traffic from moving through specific ports. Forward: Causes the switch to forward all IGMP and IP multicast transmissions through the port.
Forced Fast Leave	indicates whether "Forced Fast Leave" is enabled or disabled. Where a port is connected to multiple end nodes, this feature improves blocking of unnecessary IGMP traffic to the port. (Refer to the discussion of "Automatic Fast-Leave IGMP" in the "Management and Configuration Guide" for your switch for details on using this option).

5. To configure IGMP settings for the device:
- To enable IGMP on the device, click the **IGMP State** check box.
 - To disable the IGMP Querier on the selected device, click the **IGMP Querier Mode** check box. (The default is "enabled")

The IGMP Querier eliminates the need for a multicast router. HP recommends that you leave the IGMP Querier enabled even if a multicast router is performing the querier function in your multicast group.

Note that the IGMP Querier can only be enabled if an IP address is configured for the VLAN.

- To give IGMP traffic a higher priority than other traffic, check the **IGMP Forward with High Priority** check box. When this feature is disabled, the switch or VLAN processes IP multicast traffic and all other traffic in the order received.

Note that the Forward with high priority setting is not available when configuring IGMP settings for 9315, 9308, 9304, 6208, and 6308 switches.

- d. Click **Next**.
- e. Click in the IP Multicast column to change the setting on an individual port. When you click in the field a drop-down menu is enabled from which you can select Auto, Forward, or Blocked
- f. Click in the **Forced Fast Leave** column to select Enabled or Disabled for individual ports.

Repeat the IGMP configuration described above for each of the VLAN devices you selected.

After the final device is configured, the IGMP Settings Summary dialog is displayed.

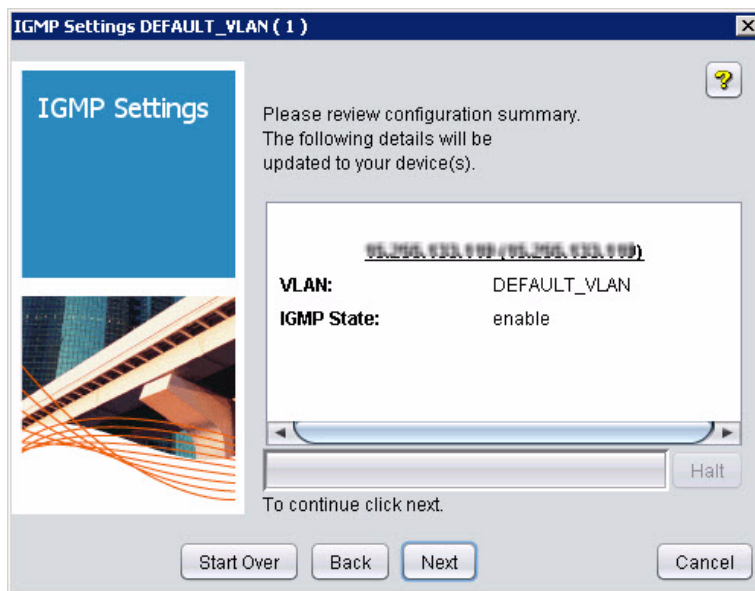


Figure 14-25. IGMP Settings Summary dialog

- 6. Review the IGMP configurations.
To change the settings, click Back or Start Over, and modify the settings as needed.
- 7. If the settings are correct, click **Next** to download the new settings.
Click Halt to stop the download if needed.

8. Check the results to ensure that the settings were downloaded successfully, then click **Close** to exit the IGMP Wizard.

IGMP Settings for Routing Switches

For the ProCurve Routing Switches, series 93xx, 62xx, and 63xx, the IGMP settings are configured somewhat differently than for other supported Switches.

To configure IGMP on routing switches:

1. Select the switch in the Devices list or navigation tree
2. Use the right-click menu or toolbar menu to select VLAN Manager > IGMP Settings.

This launches the IGMP Configuration window.



Figure 14-26. IGMP Setting for Routing Switches

3. Click the **Enable** radio button.
4. Set the **IGMP Querier Interval** (the frequency the device will query for group membership). The value can be from 1 to 3600 seconds.
5. Set the **IGMP Group Membership Time** (the value after which the group membership becomes inactive). The value can range from 1 to 7200 seconds.
6. Click **OK** to save the settings and close the window.

To Modify IGMP Settings:

To modify the IGMP Settings on a VLAN, use the IGMP Settings wizard as described for “Enabling IGMP on VLANs” beginning on page 14-25.

You can also modify IGMP setting for an individual device in a VLAN.

1. Select the device node in the navigation tree to display the device “Properties” tab.

Using VLANs

Using IGMP to Manage Multicast Traffic

2. Click the IGMP button in the toolbar to launch the IGMP Settings Wizard.
3. Edit the IGMP settings as described for enabling IGMP, starting on page 14-25.

Using Virus Throttle

Introduction	15-2
General Operation of Virus Throttle	15-3
Filtering Options	15-3
Sensitivity to Connection Rate Detection	15-4
Operating Notes	15-5
Terminology	15-6
General Configuration Guidelines	15-7
For a network operating normally:	15-7
When the network appears to be under attack	15-8
VT Configuration in PCM	15-9
VT Configuration for Blocked Hosts	15-12
Virus Throttle Log and Trap Messages	15-13

Introduction

The PCM Virus Throttle feature can improve network security on the edge of a network. It works to reduce attacks from malicious code that tries to replicate itself using weaknesses in network applications behind unsecured ports.

Virus Throttle (also called Virus filtering or connection-rate filtering) exploits the network behavior of malicious code that tries to create a large number of outbound IP connections on a routed interface in a short time. When a host exhibits this behavior, warnings are sent, and connection requests can be blocked or dropped to minimize the barrage of subsequent traffic from the host. When enabled on a 5300xl switch with software version E.09.02 or greater, virus throttling reduces the impact of malicious code attacks and gives system administrators more time to isolate and eradicate the threat. You still need to deploy traditional worm- and virus-signature updates to hosts, but the network remains functional and distribution of the malicious code is limited.

Major benefits of Virus Throttle include:

- Behavior-based operation that does not require identifying details unique to the malicious code operation.
- Handles unknown worms.
- Needs no signature updates.
- Protects network infrastructure by slowing or stopping routed traffic from hosts exhibiting high connection-rate behavior.
- Allows network and individual switches to continue to operate, even when under attack.
- Provides Event Log and SNMP trap warnings when malicious code behavior is detected

Note

When configured on a port, virus throttling is triggered by routed IPv4 traffic received inbound with a relatively high rate of IP connection attempts. Virus throttling is not triggered by such traffic when both the SA (source address) and DA (destination address) are in the same VLAN—that is, switched traffic. virus throttling applies only to routed traffic. Switched traffic from a blocked or throttled host is not blocked or throttled.

For 5400zl, 3500yl, and 6200yl running switch software version K.12.02 or later, PCM supports VT for switched traffic on the same VLAN (routing off).

General Operation of Virus Throttle

The Virus Throttle feature enables notification of malicious code behavior detected in inbound routed traffic and, depending on how you configure the feature, also throttles or blocks such traffic. This feature also provides a method for allowing legitimate, high connection-rate traffic from a given host while still protecting your network from suspected malicious traffic.

Filtering Options

In the default configuration, Virus Throttle is disabled. When enabled on a port, Virus Throttle monitors inbound routed traffic for a high rate of connection requests from any given host on the port. If a host is attempting to establish a large number of outbound IP connections (or destination addresses) in a short period of time, the switch responds in one of the following ways, depending on how Virus Throttle is configured:

- **Notify-only:** The switch generates an Event Log notice identifying the source address of the offending host and (if a trap receiver is configured on the switch) a similar SNMP trap notice).
- **Throttle:** In this case, the switch temporarily blocks inbound routed traffic from the offending host SA for a “penalty” period and generates an Event Log notice of this action and (if a trap receiver is configured on the switch) a similar SNMP trap notice. When the “penalty” period expires the switch re-evaluates the routed traffic from the host and continues to block this traffic if the apparent attack continues. (During the re-evaluation period, routed traffic from the host is allowed.)
- **Block:** This option blocks routing of the host’s traffic on the switch. When a block occurs, the switch generates an Event Log notice and (if a trap receiver is configured on the switch) a similar SNMP trap notice. Note that you must explicitly re-enable a host that has been previously blocked.

Sensitivity to Connection Rate Detection

The switch includes a global sensitivity setting that enables adjusting the ability of Virus Throttling to detect relatively high instances of connection-rate attempts from a given source.

low: Sets the virus throttle sensitivity to the lowest possible sensitivity, which allows a mean of 54 routed destinations in less than 0.1 seconds, and a corresponding penalty time for Throttle mode (if configured) of less than 30 seconds.

medium: Sets the virus throttle sensitivity to allow a mean of 37 routed destinations in less than 1 second, and a corresponding penalty time for Throttle mode (if configured) between 30 and 60 seconds.

high: Sets the virus throttle sensitivity to allow a mean of 22 routed destinations in less than 1 second, and a corresponding penalty time for Throttle mode (if configured) between 60 and 90 seconds.

aggressive: Sets the virus throttle sensitivity to the highest possible level, which allows a mean of 15 routed destinations in less than 1 second, and a corresponding penalty time for Throttle mode (if configured) between 90 and 120 seconds.

Operating Notes

- When changing the configuration of virus filters in the switch, execute the **clear arp** command to reset the routing table.
- Virus Throttling is triggered by inbound IP *routed* traffic exhibiting high rates of IP connections to new hosts. Inbound *switched* traffic with high IP connection rates does not trigger Virus Throttling. However, after Virus Throttling has been triggered on a port, all traffic (switched or routed) from the suspect host is subject to the configured virus policy (**notify-only**, **throttle**, or **block**).
- Where the switch is throttling or blocking inbound routed traffic from a host, any outbound routed or switched traffic for that host is still permitted.
- A host blocked by Virus Throttling remains blocked until explicitly unblocked by one of the following:
 - Using the **unblock** option in the VT configuration dialog.
 - Rebooting the switch
 - Deleting a VLAN removes blocks on any hosts on that VLAN.

Note that changing a port setting from Block to either Throttle or Notify-Only, does not unblock a blocked host on any port previously set to Block.

Terminology

DA: The acronym for *Destination Address*. In an IP packet, this is the destination IP address carried in the header, and identifies the destination intended by the packet's originator.

Routed Traffic: Traffic moving from an SA in one VLAN to a DA in a different VLAN.

SA: The acronym for *Source Address*. In an IP packet, this is the source IP address carried in the header, and identifies the packet's originator.

Switched Traffic: Traffic moving from an SA in a given VLAN to a DA in the same VLAN. (Sometimes referred to as "bridged traffic".)

Throttle: Means to temporarily block traffic from a host exhibiting a relatively high incidence of attempts to connect with other devices. Traffic is blocked from the host for a calculated period of time, and then allowed to resume. If the undesired behavior persists, the cycle is repeated.

General Configuration Guidelines

As stated earlier, Virus Throttle is triggered only by routed, inbound traffic generating a relatively high number of new IP connection requests from the same host. Thus, for the switch to apply virus throttle, IP routing and multiple VLANs with member ports must first be configured.

For a network operating normally:

1. Enable **notify-only** mode on the ports you want to monitor.
2. Set global sensitivity to **low**.
3. Use **clear arp** to clear the arp cache.
4. If SNMP trap receivers are available in your network, use the **Alerts dialog** to configure the switch to send SNMP traps.
5. Monitor the SNMP Traps (Events) to identify hosts exhibiting high connection rates, or configure e-mail alerts that will notify you of same.
6. Check any hosts that exhibit relatively high connection rate behavior to determine whether malicious code or legitimate use is the cause of the behavior.
7. Increase the sensitivity to **Medium** and repeat steps 6 and 7.

Note

On networks that are relatively infection-free, sensitivity levels above **Medium** are not recommended.)

8. Continue to monitor the Event Log or configured trap receivers for any sign of high connectivity-rate activity that could indicate an attack by malicious code, and if needed, apply throttle or blocking options to the affected ports. (Refer to “Virus Throttle Log and Trap Messages” on page 15-13.

When the network appears to be under attack

The major difference is in policies suggested for managing hosts exhibiting high connection rates. This allows better network performance for unaffected hosts and helps to identify hosts that may require updates or patches to eliminate malicious code.

1. Configure Virus Throttle to **throttle** on all ports.
2. Set global sensitivity to **medium**.
3. Use **clear arp** to clear the arp cache.
4. If SNMP trap receivers are available in your network, use the **snmp-server** command to configure the switch to send SNMP traps.
5. Monitor the Event Log or the available SNMP trap receivers (if configured on the switch) to identify hosts exhibiting high connection rates.
6. Check any hosts that exhibit relatively high connection rate behavior to determine whether malicious code or legitimate use is the cause of the behavior.
7. To immediately halt an attack from a specific host, group of hosts, or a subnet, use the per-port block mode on the appropriate port(s).

VT Configuration in PCM

Note:

Connection Rate Filtering is also referred to as Virus Throttling, or VT for short. The VT acronym is used in the PCM GUI, as reflected in this text.

To view the existing Virus Throttle configuration for a switch:

1. Select the switch in the Navigation tree, or in the Devices List.



2. Click the VT Configuration button in the toolbar.

If you selected in the Devices List, you can also use the VT Configuration option from the right-click menu.

3. The VT Configuration dialog displays.

Review and change the VT Configuration as needed by selecting the desired option from the drop-down menus.

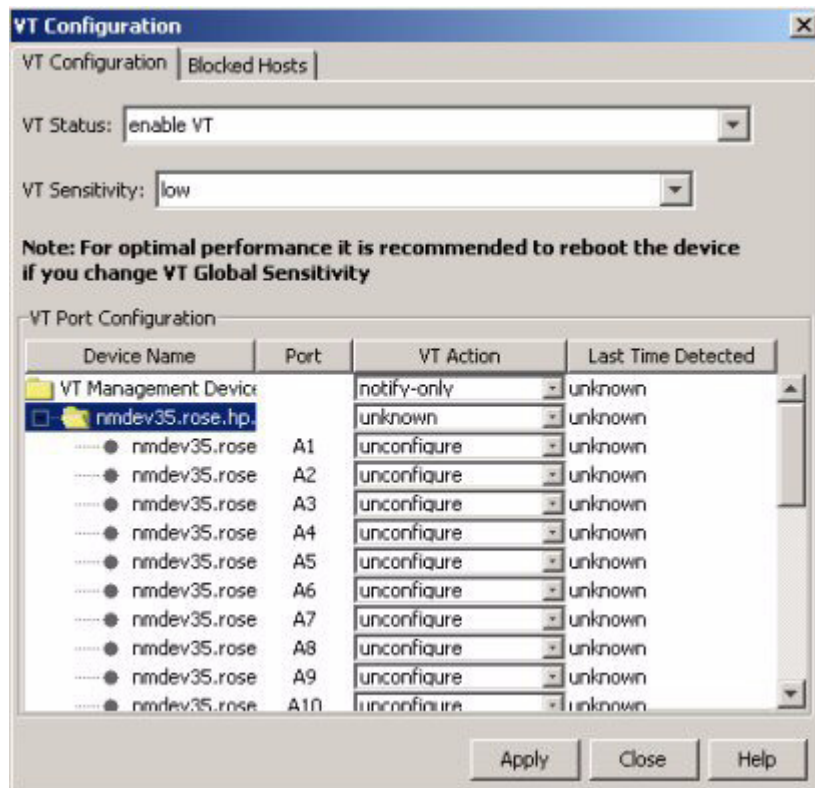


Figure 15-1. Virus Throttle Configuration display

VT Status: When virus throttle is used on the switch, the VT Status field shows the enable VT option. Use the drop-down menu to select the enable or disable option.

VT Sensitivity: The default setting for virus throttle sensitivity is low. The entry shown in the field indicates the current sensitivity setting in use. Use the drop-down menu to select the sensitivity option to use:

- **low:** Sets the virus throttle sensitivity to the lowest possible sensitivity, which allows a mean of 54 routed destinations in less than 0.1 seconds, and a corresponding penalty time for Throttle mode (if configured) of less than 30 seconds.
- **medium:** Sets the virus throttle sensitivity to allow a mean of 37 routed destinations in less than 1 second, and a corresponding penalty time for Throttle mode (if configured) between 30 and 60 seconds.
- **high:** Sets the virus throttle sensitivity to allow a mean of 22 routed destinations in less than 1 second, and a corresponding penalty time for Throttle mode (if configured) between 60 and 90 seconds.
- **aggressive:** Sets the virus throttle sensitivity to the highest possible level, which allows a mean of 15 routed destinations in less than 1 second, and a corresponding penalty time for Throttle mode (if configured) between 90 and 120 seconds.

VT Port Configuration: Click the device node to expand the display and show VT configuration information for all ports on the switch. The VT Action field indicates the current configuration applied on the switch and ports. Use the drop-down menu to change the VT configuration option:

- **Notify-only:** An Event Log notice identifying the offending host SA is generated, and if a trap receiver is configured on the switch a similar SNMP trap notice is sent.
- **Throttle:** In this case, the inbound routed traffic from the offending host SA is blocked for a “penalty” period and generates an Event Log notice of this action and (if a trap receiver is configured on the switch) a similar SNMP trap notice. When the “penalty” period expires the routed traffic from the host is re-evaluated, and if the apparent attack continues, the traffic block is continued. (During the re-evaluation period, routed traffic from the host is allowed.)
- **Block:** This option blocks routing of the host’s traffic on the switch or port. When a block occurs, an Event Log notice is generated, and (if a trap receiver is configured on the switch) a similar SNMP trap notice.

Note that you must explicitly re-enable a host that has been previously blocked. (See “VT Configuration for Blocked Hosts” on page 15-12)

- **No:** This option lets you remove the virus throttle configuration on the switch and/or port.
 - **Unknown:** This state is shown only if the VT secondary discovery fails on the device, indicating the state of VT port configuration is not known.
4. Click **Apply** to save the configuration information.
Click **Close** to exit the dialog without saving or applying the configuration changes.
 5. When you click **Apply** at the bottom of the window the VT Configuration Status dialog will display, indicating the device and configuration change status.

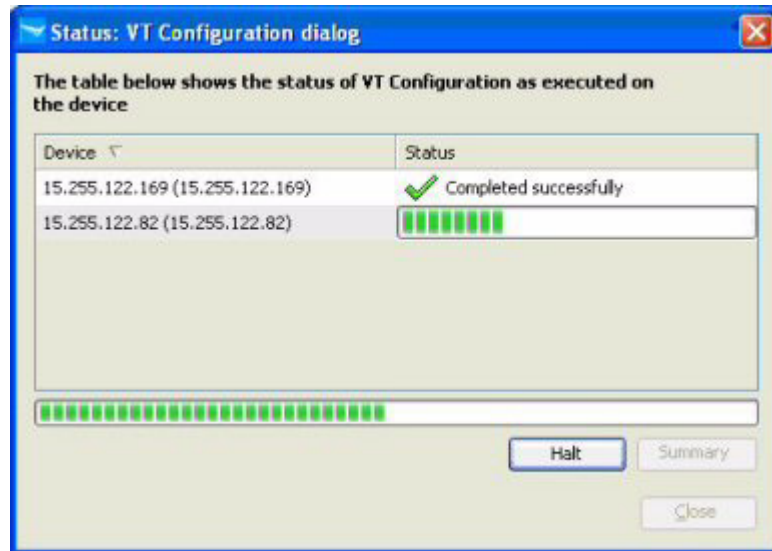


Figure 15-2. VT Configuration, status display

If the configuration change process appears to hang, click the **Halt** button to stop the process, then click **Summary** button to display the Status Summary dialog and check for error messages or reason for failure of the configuration change.

6. Click **Close** to exit the dialog.

VT Configuration for Blocked Hosts

The Blocked Hosts tab in the VT Configuration dialog lists the devices (SAs) that are blocked as a result of virus throttling configured on the switch.

To review blocked hosts and, or restore (unblock) a blocked host:

1. Select the switch in the Navigation tree, or in the Devices List.

2. Click the VT Configuration button in the toolbar.



If you selected in the Devices List, you can also use the VT Configuration option from the right-click menu.

3. Click the Blocked Hosts tab in the VT Configuration dialog.

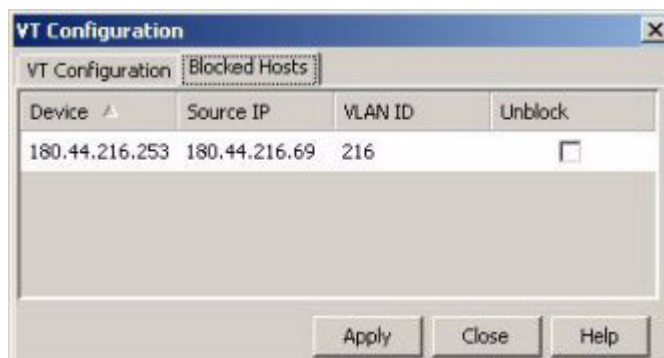


Figure 15-3. VT Configuration, blocked hosts

The Blocked Hosts tab displays the list of devices/sources blocked due to enabling of VT on a device or a Port, including:

- **Device:** The device IP on which the source is blocked
- **Source IP:** The blocked source IP.
- **VLAN ID:** The VLAN ID on which the Source IP is blocked
- **Unblock:** Select the check-box to unblock the selected Source IP.

4. When you complete a VT configuration change to unblock hosts, click **Apply** at the bottom of the window.

The VT Configuration Status dialog will display, indicating the device and configuration change status.

If the Unblock Host process appears to hang, click the **Halt** button to stop the process, then click **Summary** button to display the Status Summary dialog and check for error messages or reason for failure of the configuration change.

5. Click **Close** to exit the dialog.

Virus Throttle Log and Trap Messages

These messages will appear in the switch's Event Log. If SNMP trap receivers are configured on the switch, it also sends the messages to the designated receiver(s).

Message	Meaning
W < mm/dd/yy hh:mm:ss > virusfilt: Source IP address <xxx.xxx.xxx.xxx> is exhibiting virus-like behavior	A warning that results when a port configured for notify-only detects a relatively high number of connection-rate attempts from a host.
W < mm/dd/yy hh:mm:ss > virusfilt: Source IP address <xxx.xxx.xxx.xxx> has been throttled	A warning and indication of the switch's response when a port configured for throttle detects a relatively high number of connection-rate attempts from a host.
W < mm/dd/yy hh:mm:ss > virusfilt: Src IP <xxx.xxx.xxx.xxx> blocked	A warning and indication of the switch's response when a port configured for block detects a relatively high number of connection-rate attempts from a host.

Using Policy Manager Features

How the Policy Manager Works	16-2
Policy Configuration Overview	16-3
Configuring Policies	16-4
Editing Policies	16-12
Deleting Policies	16-12
Enabling/Disabling Policies	16-13
Manually Enforcing Policies	16-13
Policy History	16-14
Creating Times for Policies	16-17
Custom Groups for Policies	16-20
Defining Alerts for Policies	16-21
Creating Event-based Alerts	16-21
Creating Schedule Driven Alerts	16-26
Configuring Policy Actions	16-30
Creating an Action	16-30
Editing Policy Actions	16-38
Deleting Policy Actions	16-39
Action Type Definitions	16-40
Viewing Configuration Manager Policy Status	16-49
To Enable/Disable a Policy	16-49
To Edit a Policy	16-49
To Delete a Policy	16-50
Setting Policy Management Preferences	16-51

How the Policy Manager Works

As the term suggests, *policy* refers to settings or actions you can apply across a range of devices or ports on the network. Using the PCM Policy Manager, you can perform a wide range of actions, including:

- Define and enforce community names, trap receivers, authorized managers, and Spanning Tree settings consistently on any group of selected devices.
- Test est communication parameters.
- Manage VLANs and VLAN port settings.
- Automatically apply a configuration template on newly discovered network devices.

The Policy Manager provides a unified toolset you can use to:

- Configure an alert (trigger) to notify the Administrator about specific network issues (e.g., CRF events)
- Configure an event driven action—an action taken in response to the alert notification (event occurrence). For example, set MAC Lockout on a port in response to a CRF alert.
- Schedule some action to occur at set intervals in the future. For example, schedule configuration scans to occur on a weekly basis.
- Define an action that can be re-used on demand. Such as: set rate limit to DEFCON1, NORMAL.

Policy Configuration Overview

Policies are configured with a combined set of parameters that you define:

- **Times** - Time periods when the policy can be executed. If no time is specified, the policy can execute at any time.
- **Sources** - Devices or ports from which events are received. If no source (Device or Custom group) is selected, the policy will match events from any source.
- **Targets** - Devices or ports on which a defined action will be performed in response to an alert, if applicable. If no Target is selected, the Alert will log a Policy Manager event in the event browser.
- **Alerts** - A defined trigger used to launch a Policy. Alerts can be event-driven, or scheduled to occur at a specified time.
- **Action** - The action taken on Targets in response to the Alert. If no action is specified, the alert will generate a Policy Manager event in the Event browser.

Multiple parameters of each type can be applied to a Policy. When the Policy is activated, it reads through each set of parameters until a match is found. For the policy to execute, it must find a match for each defined parameter. If there is no match the policy does not execute. For example, if you configure a policy with Times limited to “weekdays”, defined as 9:00 am to 5:00 pm and an alert trigger is received at 10:00 pm, the policy will not execute.

You can separately define specific Times, Alerts, Actions, and use Custom Groups to define event sources or targets for the policy action. The "new definitions" will be available in the selection lists in the Policy Configuration Manager when you create your Policy. Or you can create Times, Alerts, Actions, and Custom Groups as needed within the Policy Configuration Manager tabs.

Configuring Policies

To configure a Policy:



1. Click the Launch Policy Manager button in the toolbar to launch the Policy Manager configuration window.

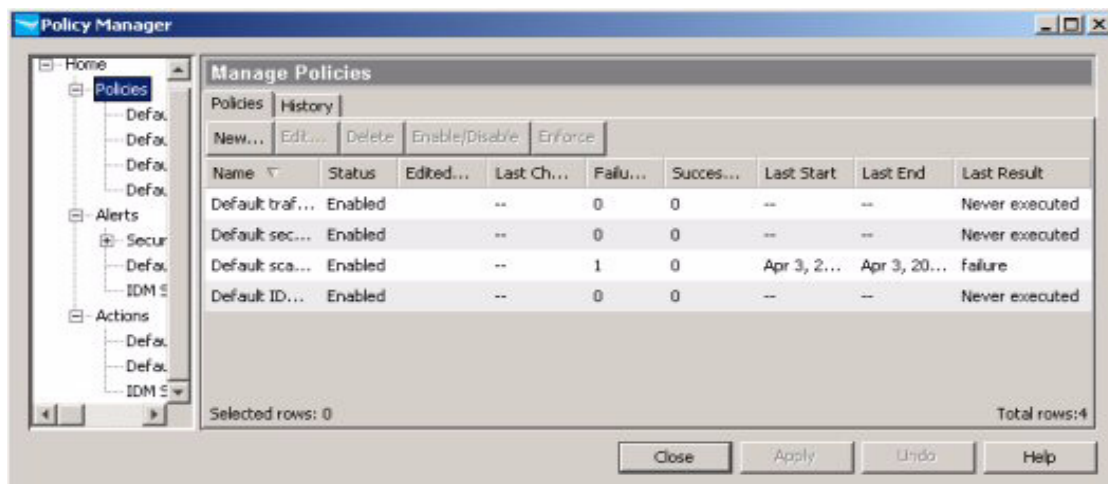


Figure 16-1. Policy Manager: Manage Policies pane

2. Select the Policies node in the navigation tree to display the Manage Policies pane, then click New... to launch the Create Policy dialog.

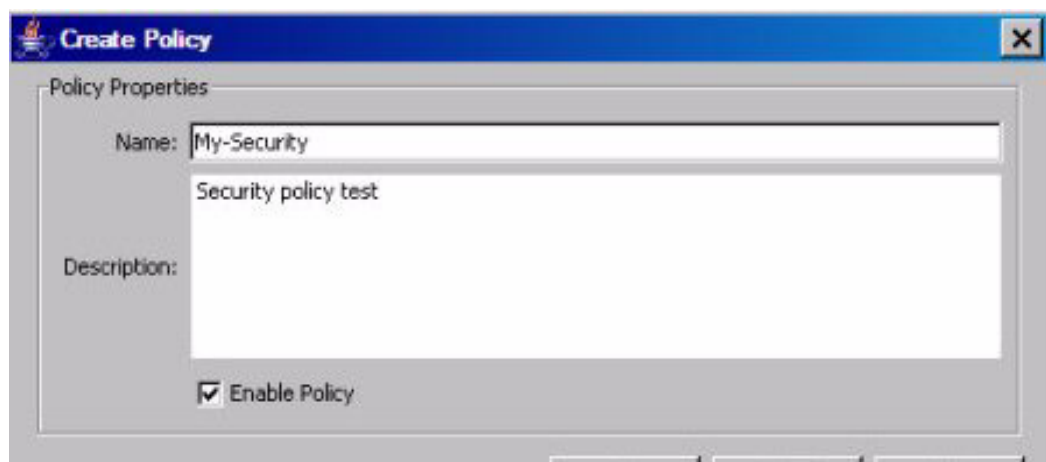


Figure 16-2. Policy Configuration: Properties

3. Fill in the Policy information:
 - a. In the Name field, type a name to identify the policy.
This name will appear as a node in the Policies navigation tree, and in the list in the Manage Policies pane.
 - b. In the Description field, type a brief description to help you identify the policy and what it will do.
 - c. Select the Enable Policy check box to enable the policy.
A check in the box indicates that the policy will be ready to execute immediately after the configuration is completed.
If the check box is empty, the policy is disabled. It will not take effect until you enable it.
 - d. Click OK to save the Policy Properties and display the Policy Configuration pane for your new policy.

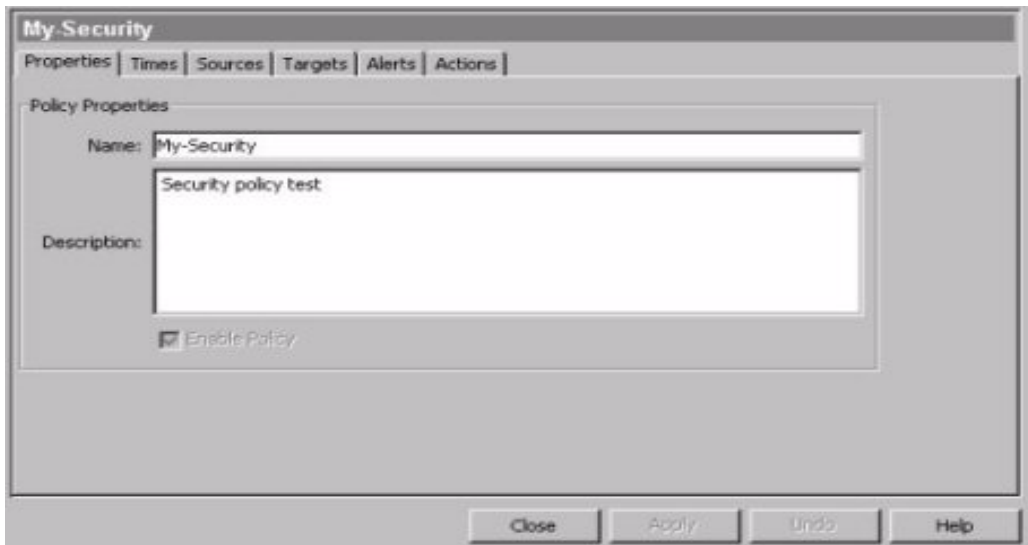


Figure 16-3. Policy Configuration: Properties tab

4. Click the Times tab to configure the time periods that will be applied for your policy.

Applying “Times” to a policy restricts the application of the policy to the defined time. If no times are selected, the policy will always be active and can be executed at any time.

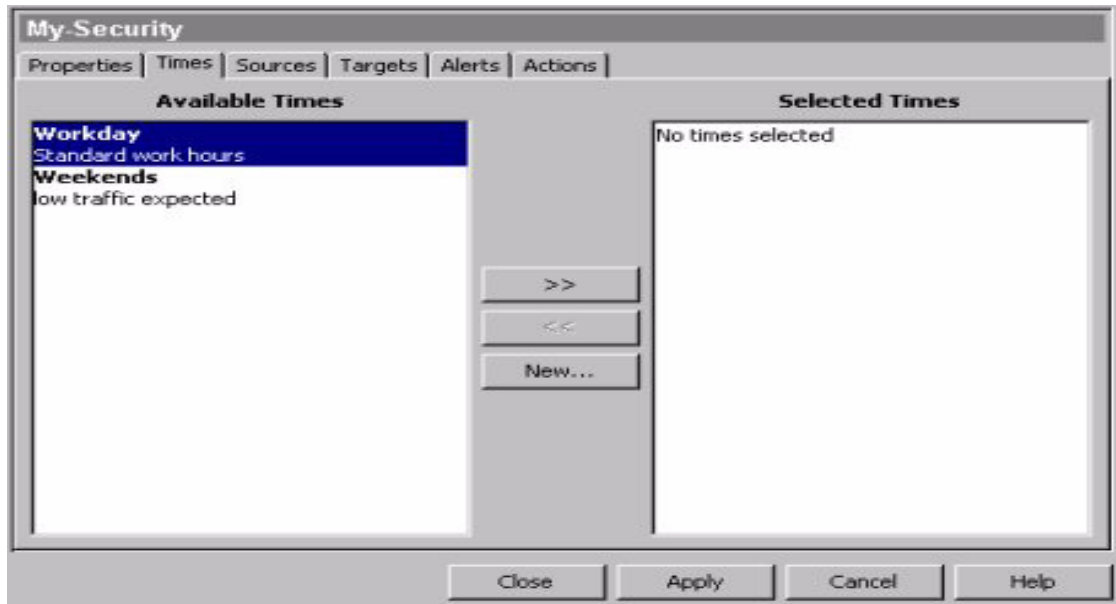


Figure 16-4. Policy Configuration: Times tab

5. To apply a time, select it in the Available Times list on the left, then click >> to move it to the list of Selected Times.

You can apply more than one Time. When the policy is activated, it will read each time entry until a match is found.

Click **New...** to launch the Configure Times dialog.

See “Creating Times for Policies” on page 16-17 for details.

6. Click the Sources Tab to configure the device groups from which an event trigger will be applied.

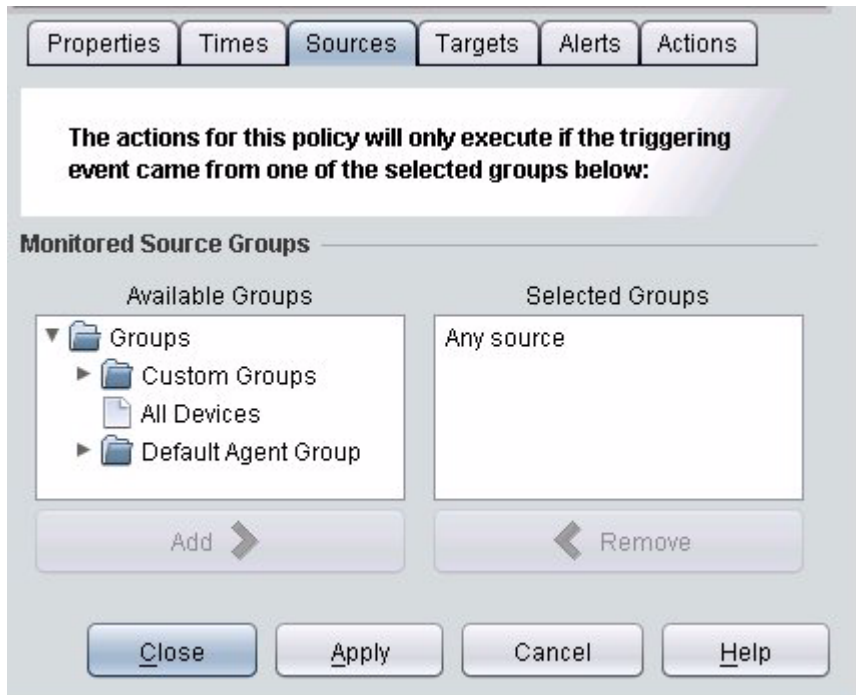


Figure 16-5. Policy Configurations: Sources tab

7. To apply a Group, double-click folders in the Available Groups list on the left to display custom groups and device groups, select the custom group or device group, and then click **Add >** to move it to the list of Selected Groups on the right.

If no group is selected, the Policy will accept events from any source.

If you select one or more groups, the policy will only execute if an event is received from a device in the Selected Groups list.

If you configured Custom Groups, they will appear in the Available Groups list. You can use a Custom Group to define a group of ports on various devices, rather than all ports on a single device type. “Working with Custom Groups” on page 13-1 for details.

8. Click the Targets Tab to configure the device groups to which the policy action will be applied.

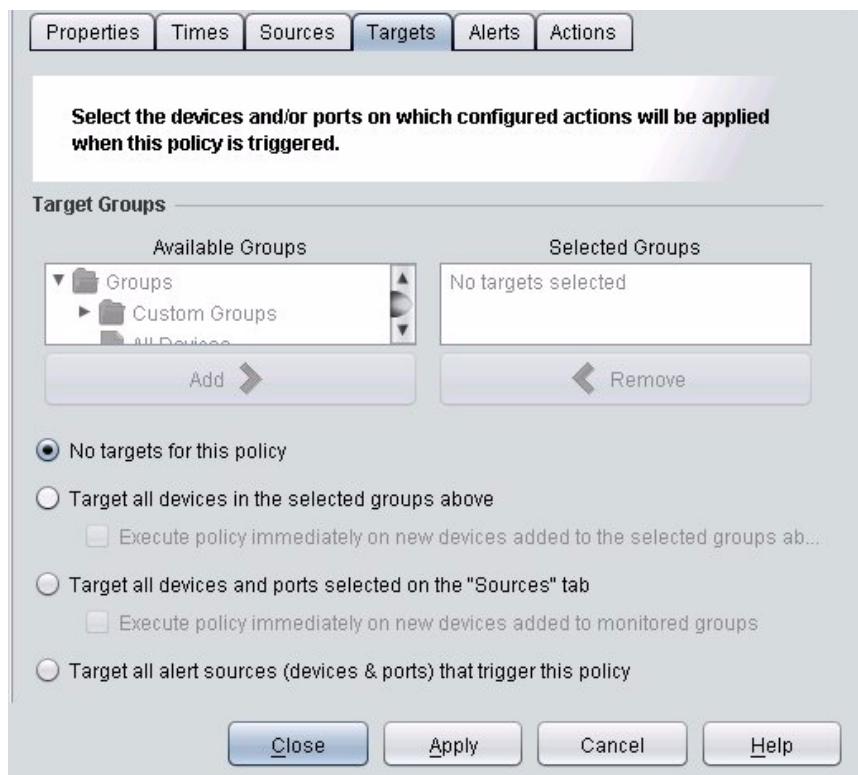


Figure 16-6. Policy Manager: Targets tab

9. To target specific groups:
 - a. Select Target all devices in the select groups above.
 - b. To enforce the policy on newly discovered devices in the selected group, check the Execute policy immediately on new devices added to the selected groups above check box. This is useful for applying standardized configurations.
 - c. In the Available Groups list on the left, select the group where the policy is to be enforced, then click >> to move it to the list of Selected Groups on the right.

The policy will be applied to all discovered devices of that type, unless you select one of the target qualifiers in the bottom portion of the window.

If no group is selected, the policy action will not be executed on any device and the No targets for this policy option must be selected. If the All Devices is selected, the policy action will be executed on all devices

- in predefined ProCurve device groups. If the Devices group is selected, the policy action will be executed on all devices in ProCurve devices managed by the Agent group.
- d. Repeat the previous step for each group that you want to include in the policy. You can select any combination of custom groups and implicit groups (groups automatically created during Discovery).
10. To target source devices:
 - a. Select Target all devices and ports selected on the Sources tab. At least one Source group must be selected before you can use this option.
 - b. To enforce the policy on newly discovered devices in monitored Source groups, check the Target any new devices added to monitored groups check box.
 11. Click the Alerts tab to configure the alerts that will trigger the policy execution.

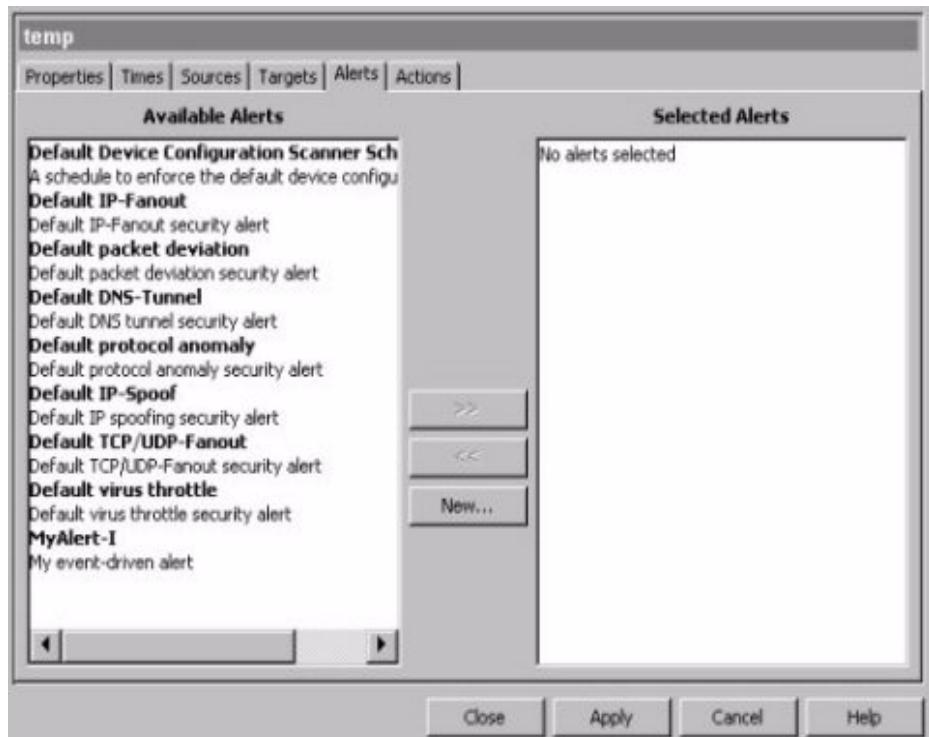


Figure 16-7. Policy Configuration: Alerts tab

12. The Alerts tab lists the pre-configured alerts in the Available Alerts list. To apply an Alert, select it in the Available Alerts list on the left, then click >> to move it to the list of Selected Alerts on the right.

You can select multiple alerts, and when an event is received each of the alerts will be evaluated until a match is found. The policy will execute on the first matching Alert.

If you configured any custom Alerts they will appear in the Available Alerts list.

Click New... to launch the Create Alert dialog to define an Alert and add it to the list of available Alerts. See “Defining Alerts for Policies” on page 16-21 for details.

13. Click the Actions tab to configure the actions the policy will take when it is executed.

If you do not specify an Action for the policy, when the policy executes it will log a Policy Manager event in the Event browser.

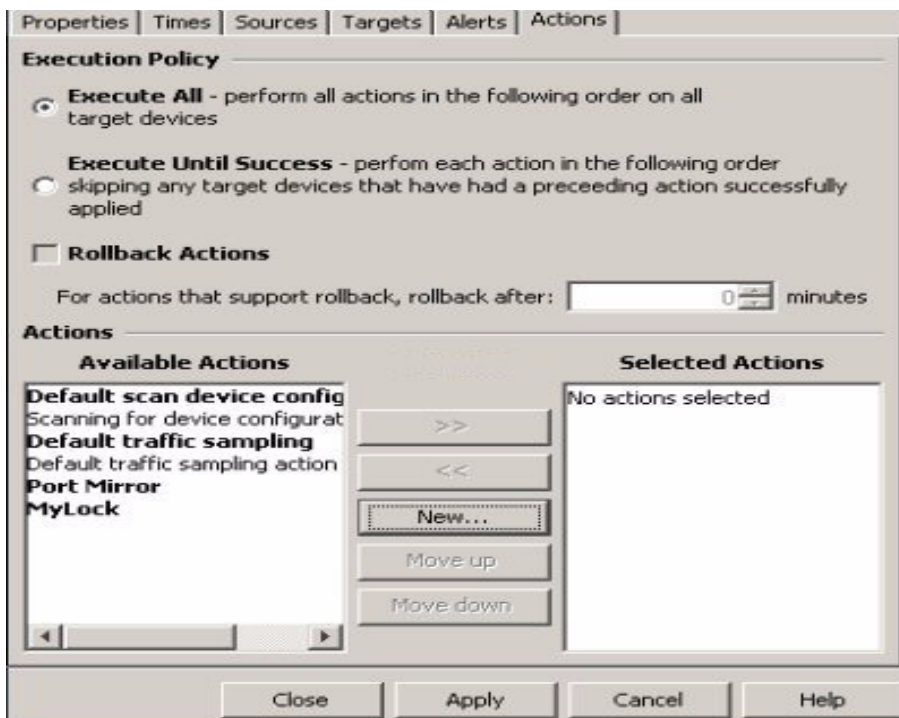


Figure 16-8. Policy Configuration: Actions tab display

14. Select the Execution Policy options you want to apply by clicking the radio buttons or check box.

- Execute All - this is the default setting. Indicates all selected actions will be attempted when the Policy runs.
- Execute Until Success - this will attempt to execute each selected action on each target device or port in the order listed. As soon as an action completes successfully, the policy moves to the next target device/port and attempts to execute the selected actions.

This can be used to create a single policy to that is applied across multiple device types on the network. For example:

- Click **New** and create one action for Security:VT Configuration that uses the port supplied in the event source. Then create an action to Disable the port (Port Settings:Enable/Disable Port(s) action option).
- Create a Policy that targets all source devices/ports when an alert is generated.
- In the Actions tab, select the Security:VT Configuration action and the Port Settings:Enable/Disable Port(s) action, in that order.

When the Policy executes, it will first attempt to use the Virus Throttle (VT) action on the target device or port. If the target device does not support the Virus Throttle feature, the Policy will attempt the Disable Port action.

- Act on Edge Ports Only - execute the action on edge ports (end nodes with no downstream devices) only. This option is enabled by default to help avoid inter-switch port configuration changes caused by security alerts. However, this setting may result in a policy not targeting all ports in a targeted custom group.
 - Roll Back after Expiration Period - for Action types that support a rollback operation, it will stop the action, returning the target of the action to its original state after the time specified (in the next line). This option is not enabled until an action that supports rollback is selected. The rollback feature is supported by the following actions:
 - Port Mirroring
 - MAC Lockout
 - Port Status (enable/disable)
 - Rate Limit
 - Traffic Sampling
15. The Actions tab lists the pre-configured actions in the Available Actions list, and any new actions created. To apply an Action, select it in the Available Actions list on the left, then click >> to move it to the list of Selected Actions on the right.

You can select multiple actions to apply when the Policy executes. The actions will be applied according to the Execution Policy options you select.

16. Click **Apply** to save the changes, then click **Close** to exit the Policy Manager window.

If you click Close before Apply, you will be prompted to save or cancel the changes.

The new policy appears in the Policies list in the Manage Policies window.

Editing Policies

To edit a policy:



1. Click the Launch Policy Manager button in the toolbar to launch the Policy Manager window.
2. To display the Manage Policies (modify) pane, click the Policies node in the Policy Manager window, and either:
 - Right-click a policy in the table and select Modify policy in the menu, or
 - Double-click an entry in the table, or
 - Select an entry in the table and click Edit in the tool bar.
3. If you select a policy in the list, the Edit... and Delete buttons are enabled.
4. Click Edit... to launch the policy properties window and edit the policy parameters as needed.
5. Click Apply to save your changes, then click Close to exit the Policy Manager window.

Deleting Policies

To delete a policy action:



1. Click the Launch Policy Manager button in the toolbar to launch the Policy Manager window.
2. Click the Policies node in the Policy Manager window to display the Manage Policies pane.
3. Right-click a policy in the table and select Delete policy in the menu, or
Select the policy in the list, which enables the Edit... and Delete buttons, and then click the Delete button.
4. Click Yes in the confirmation dialog to delete the policy.

The policy is removed from the Policies list.

5. Click Close to exit the Policy Manager window.

Enabling/Disabling Policies

When you create a policy, the default configuration automatically enables the policy so it is set to run whenever a triggering alert is received. When running tests or reconfiguring parts of the network, you may want to temporarily disable or stop the policy from taking any action.

To disable or enable the enforcement of a policy:



1. Click the Launch Policy Manager button in the toolbar to launch the Policy Manager window.
2. Click the Policies node in the Policy Manager window to display the Manage Policies pane.
3. Select the policy in the list, which enables the Enable/Disable button.
4. Click Enable/Disable to enable or disable the policy.

This button works as a toggle. The Status shown in the Policies list will change from Enabled to Disabled and back, each time you click the button.

Manually Enforcing Policies

Policies use the Alert parameters to trigger actions, that is enforcement of the policy. If the policy was disabled at the time it would normally have been enforced, you can re-enable the policy, then manually enforce the policy, rather than wait for the next Alert to trigger the policy action.

To enforce a policy manually at any time:



1. Click the Launch Policy Manager button in the toolbar to launch the Policy Manager window.
2. Click the Policies node in the Policy Manager window to display the Manage Policies pane.
3. Select the policy in the list, which enables the Enforce button.
4. Click Enforce to run the policy immediately, that is execute the policy action without waiting for the alert trigger.

The status columns for the policy will be updated with the results of the policy enforcement, and the Progress column in the Policy History will show the percentage (%) completion of the policy. The history will indicate a "Manual" alert name and type to indicate manual enforcement of the policy. You can click the Cancel Action button in the History tab to halt the policy action.

Policy History

Use the History tab in the Policy Manager window to check the policies that have executed and the current status of a policy's action.

To stop the current execution of a policy or a pending rollback action, select the row with the policy name and action, and click the **Cancel Action** button

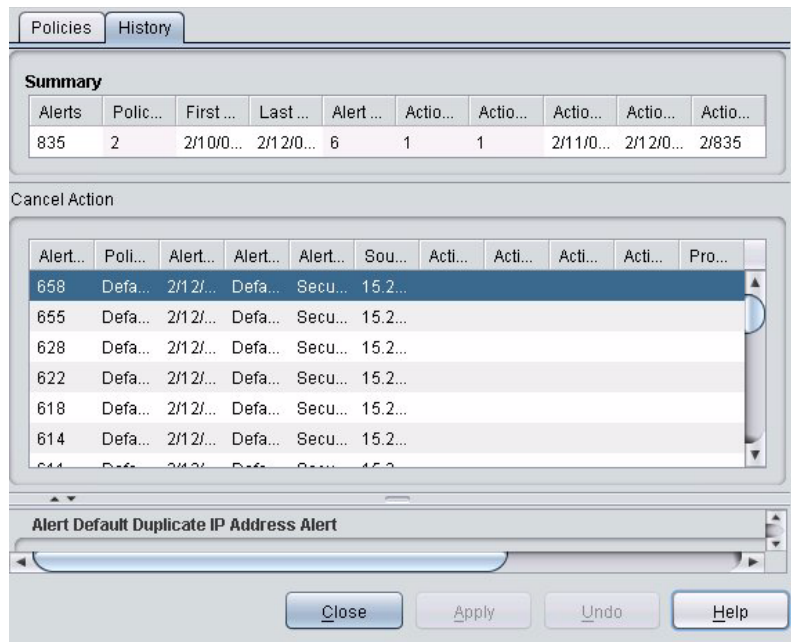


Figure 16-9. Manage Policies: History tab

The top pane, Summary, provides an overview of all alerts.

The middle pane lists the following information on the policies that have executed or are currently executing:

Alert #	Unique ID number assigned to the alert. An alert is provided a unique ID, and each action that results from that alert will have its own history table row, thus the alert ID shows which actions resulted from which alert. You can sort by alert ID to group together all the actions from a single alert.
Policy Name	Name assigned when the policy was configured
Alert Date	Timestamp for when the alert trigger was generated
Alert Name	Name assigned when the alert was configured
Alert Type	Type of alert that triggered the policy (e.g., Event-driven, Schedule-driven, or Manual if policy was manually enforced)
Source	IP address of the switch, server, or UTM that generated the alert or the device identified by the alert as the source (for example, an edge switch connected to a host identified by a VT alert), or N/A for manually enforced policies.
Action Taken	The name of the action executed by the policy.
Action Type	The action type of the action executed by the policy.
Action Start	Timestamp for when the action was started by the policy.
Action End	Timestamp for when the action was completed
Progress	Indicates percentage of action completed. If less than 100% then the action did not successfully complete. For example, in cases such as Configuration Scan policy, if the action is unable to complete on all device targets, the percentage of devices successfully scanned displays.

The details pane at the bottom displays information about the Alerts associated with the selected Policy, and the Actions taken by the policy.



Figure 16-10. Policy History: Bottom pane display

You can scroll to review all of the alert properties and action properties associated with the selected policy.

Creating Times for Policies

You can define times at the point when you create the policy, or use the Times configuration option to define a set of times separate from the policies, that can be applied as needed when creating automated Policies.

To create a pre-defined Time:



1. Click the Times Configuration button in the PCM toolbar to display the Configure Times pane.



Figure 16-11. Configure Times window



2. Click the Create a new Time button in the Times toolbar to display the Create a new Time dialog.

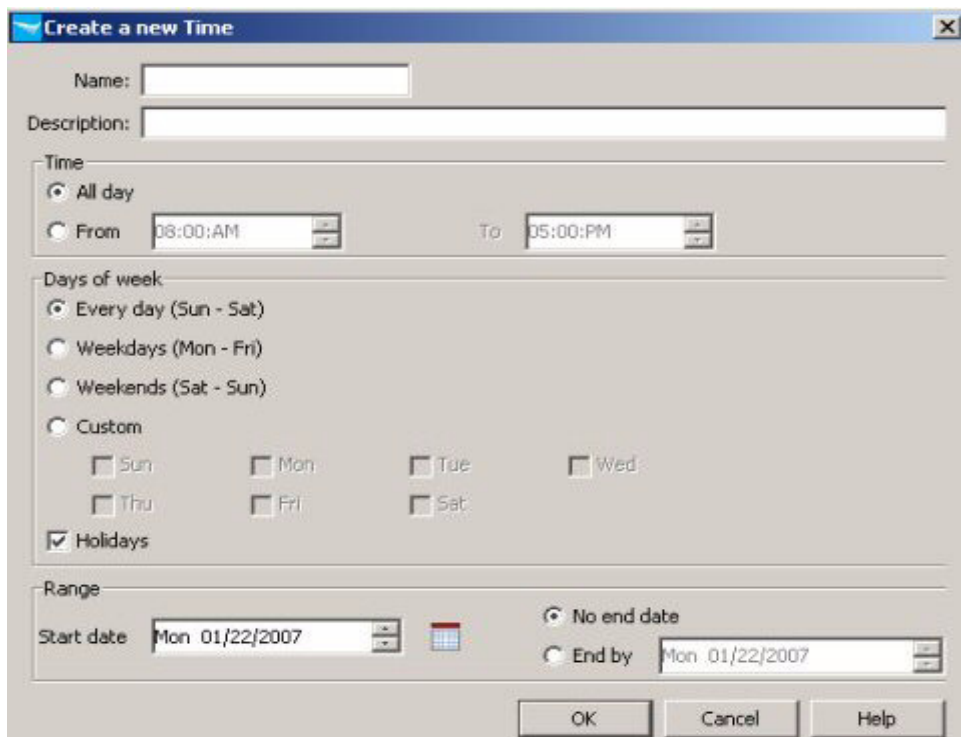


Figure 16-12. Configure Times: Create New Time window

3. Define the properties for the new time.

Name Name used to identify the time

Description Brief description of the time

Time Time of day being defined. The default is **All day** (24 hours). To restrict the time to specific hours of the day, click the From radio button and type the start (from) time, and the (end) To times. The To time must be later than the From time. AM or PM must be specified.

Days of week Days of the week that the Time applies. **Every day** is the default. Click the radio button next to the desired days. Click the Custom radio button to enable the day(s) of the week check boxes.

Range Dates during which the time will be in effect. Select the **Start Date** and then click the No End Date radio button, or select the **End Date**.

4. Click **Ok** to save the new "Time" and close the pane.
The new time appears in the Times pane.

When you create a new Time in PCM, it is automatically added to the list of Available Times in the Times tab of the Policy Manager.

Modifying a Time

1. Click the Times Configuration button in the PCM toolbar to display the Configure Times pane.
2. Double-click a Time in the list to display the Time details in edit mode, similar to the Create a new Time pane.



You can also select the Time in the list then click the Edit Time button in the toolbar to display the modify pane.

3. Modify the time parameters as described in step 3, on the previous page.
4. Click **Close** to save your changes and close the window

Note:

Before you modify or delete a Time, check to make sure that the changes do not adversely affect an automated Policy already in use.

Deleting a Time

To remove an existing Time:

1. Click the Times Configuration button in the PCM toolbar to display the Configure Times pane.
2. Click a Time in the list to select it.
3. Click the Delete Time button in the toolbar to remove the time.



The first time you use the Delete Time option, a warning pop-up is displayed. Click **Yes** to continue, or **No** or **Cancel** to stop the delete process.

4. The Time is removed from the Times list.

Custom Groups for Policies

ProCurve comes with defined device groups for each of the managed ProCurve device types. You can also create custom groups to define a specific network segment or set of devices for application of Policies.

All of the device groups and custom group names are listed in the Available Groups lists for setting Sources and Targets for Policies. For additional details on creating Custom Groups, see Chapter 13, “Working with Custom Groups” for details.

Defining Alerts for Policies

There are two types of Alerts you can configure to serve as policy action triggers.

- Use Event-driven alerts to create policies that will take an action in response to a specific event. These can be especially useful in detecting and mitigating possible security or process problems.

Note: Events are SNMP traps or application messages generated by PCM and/or its plug-in modules.

- Use Schedule-driven alerts to enforce (apply) the policy immediately, and/or schedule the Policy for automatic enforcement at specific, recurring times. You can use this for running intensive scans or discovery functions at times when it will have the least impact on network operations.

If you are using the Network Immunity Manager, you will also see Security Alert types in the Policy Configuration Manager tree. Refer to the *Network Immunity Manager User's Guide* for details on using Security alerts.

Creating Event-based Alerts

To configure an event-based alert type:



1. Click the Launch Policy Manager button in the toolbar to launch the Policy Manager window.
2. Click the Alerts node in the Policy Manager window to display the Manage Alerts pane.

Using Policy Manager Features Defining Alerts for Policies

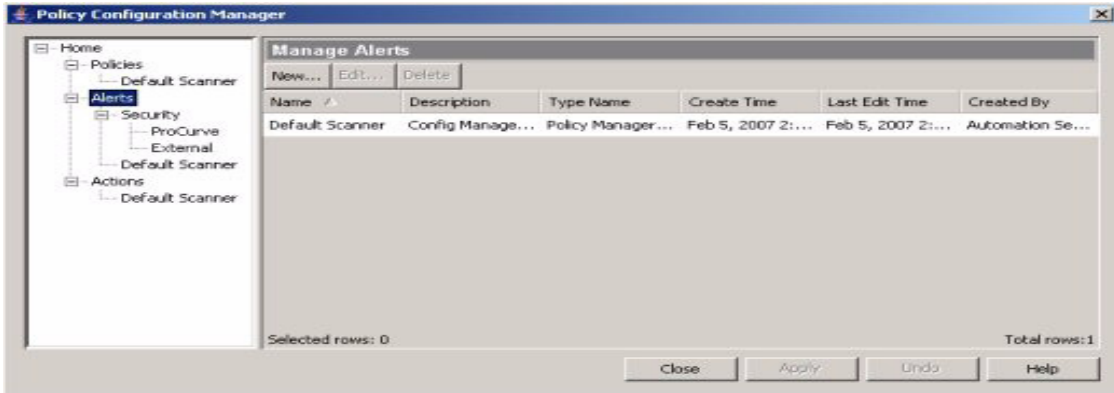


Figure 16-13. Policy Configuration, Manage Alerts

The Manage Alerts window displays the list of defined Alerts.

3. Click New... to launch the Create Alert dialog:

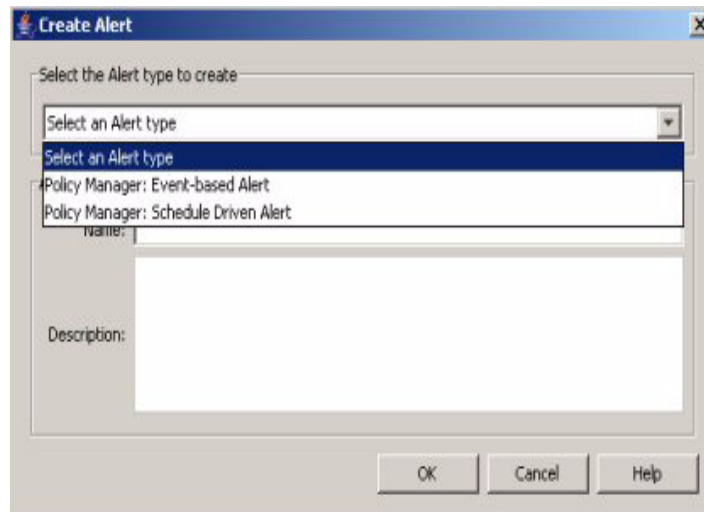


Figure 16-14. Create Alert dialog, with alert type options

4. Select the Policy Manager: Event-based Alert option in the Alert type pull-down menu.
5. Type a Name for the Alert (required) and a brief Description (optional).
6. Click OK to save the Alert and display the Alert Properties tab. The properties you set in the previous step should appear.

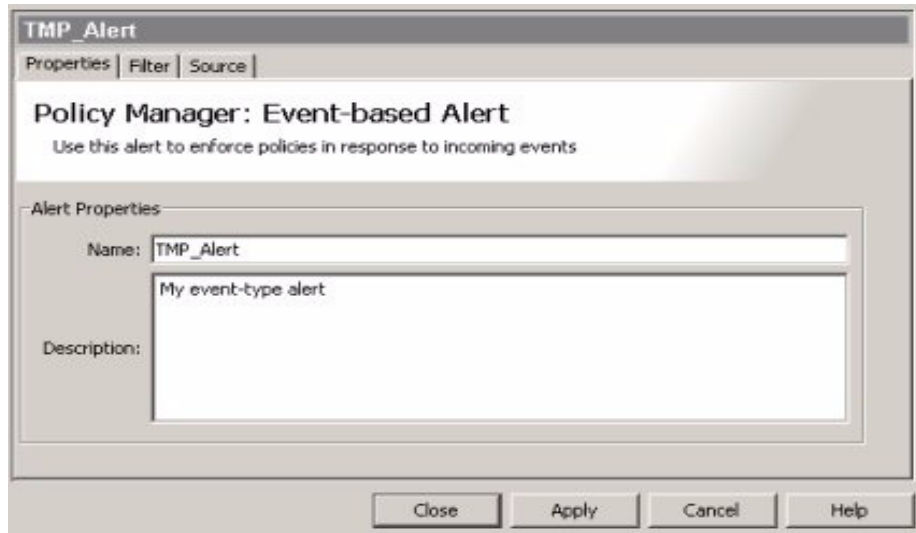


Figure 16-15. Policy Manager: Alert Properties example

7. Click the Filter tab to enter the event filter criteria.

The Filter defines one or more conditions required to issue an alert. At least one condition must be defined. You can also combine two or more filter types, for example severity, source IP, and group. Just enter the data for each filter to be applied for the event condition.

To configure the filter:

- a. For the **Alert me when I receive** field, click the up and down arrows in the events field to set the minimum number of events (meeting all other filter criteria) that must occur before issuing an alert.

The number of events works in conjunction with the time period condition in the lower section of the dialog. For example, you can issue an alert when more than five events are issued within ten minutes. The default setting is one event within one second.

- b. Click the **has OID starting with** check box to filter events by the OID of the trap that was received, and then type the OID for traps you want included in the alert.

Note: OID values always start with a leading period ".".

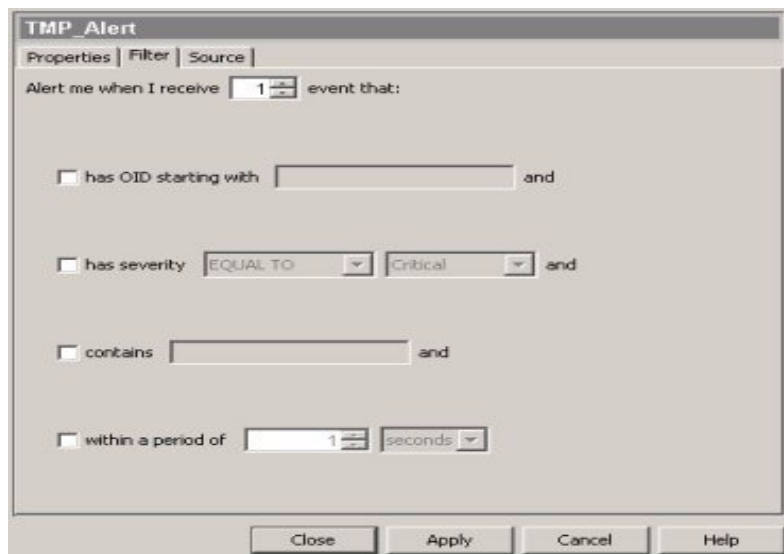


Figure 16-16. Policy Manager, Event-driven Alerts filter

- c. Click the **has severity** check box to filter events by severity, then use the pull down menus to select the operator (equal, not equal, greater than, or less than), and the severity level (Any, Informational, Warning, Minor, Major, and Critical). For example, to issue an alert when a Major or Critical event occurs, select "Greater Than" and "Minor."
- d. Click the **contains** check box to filter events by their content (text), and type the text (1-35 characters) that you want to use as a filter. For example, you can issue an alert when an event contains the phrase "Error occurred when" or "port number 12."
- e. Use the **within a period of** field to set the time interval used to count the minimum number of events that must occur before an alert is issued. Click the up and down arrows in the field to select the desired time period, then select the interval type: second, minute, hours, or days.

If you configure a time window and the alert fires, it will not fire again until the time since the first event that was used to trigger the alert is greater than the time window. In other words, the alert will only fire once per given time period, then it will go silent.

8. Click the Source tab to set Alert Source criteria.

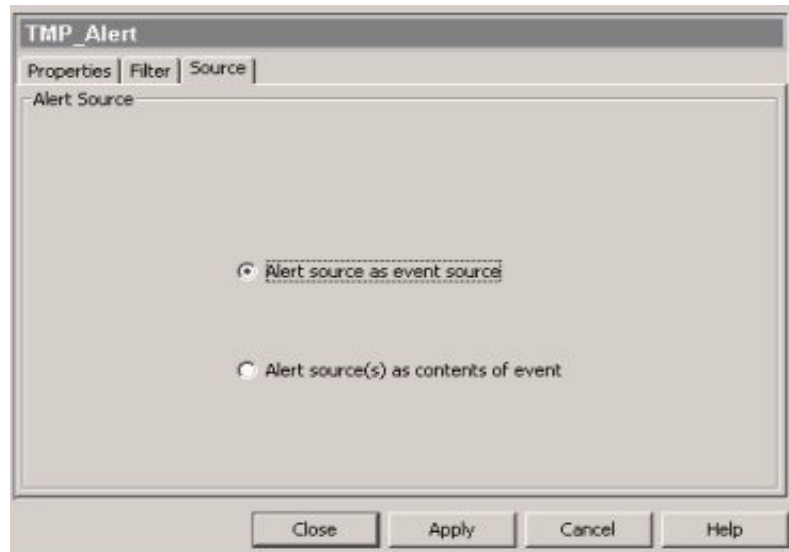


Figure 16-17. Policy Manager, Event-driven Alerts Source selection

9. Click the radio button to select one of the Alert Source options:
 - Alert source as event source will include the IP address of the device that generates the Alert as the alert source.
 - Alert source(s) as contents of event will include the IP addresses of devices generating alerts in the description text of the event message. That is, the source device IP addresses and/or ports will be taken from the payload of the trap.
10. Click **Apply** to save the Filter criteria.
11. Click **Close** to exit the Policy manager.

If you click **Close** before **Apply**, you will be prompted to save or cancel the changes.

Creating Schedule Driven Alerts

To configure a Schedule Driven alert type:



1. Click the Policy Manager button in the toolbar to launch the Policy Configuration Manager window.
2. Click the Alerts node in the Policy Manager window to display the Manage Alerts pane.

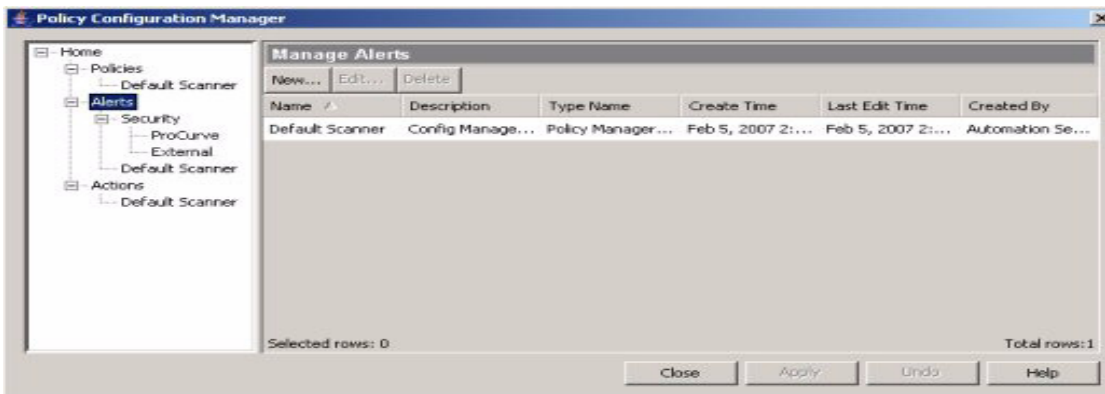


Figure 16-18. Policy Configuration, Manage Alerts

The Manage Alerts window displays the list of defined Alerts.

3. Click New... to launch the Create Alert dialog (see figure 16-14 on page 16-22)
4. Select the Policy Manager: Schedule Driven Alert option in the Alert type pull-down menu.
Type a Name for the Alert (required) and a brief Description (optional)
5. Click OK to save the Alert and display the Alert Properties tab.
The properties you set in the previous step should appear.
6. Click the Schedule tab to set the schedule parameters.

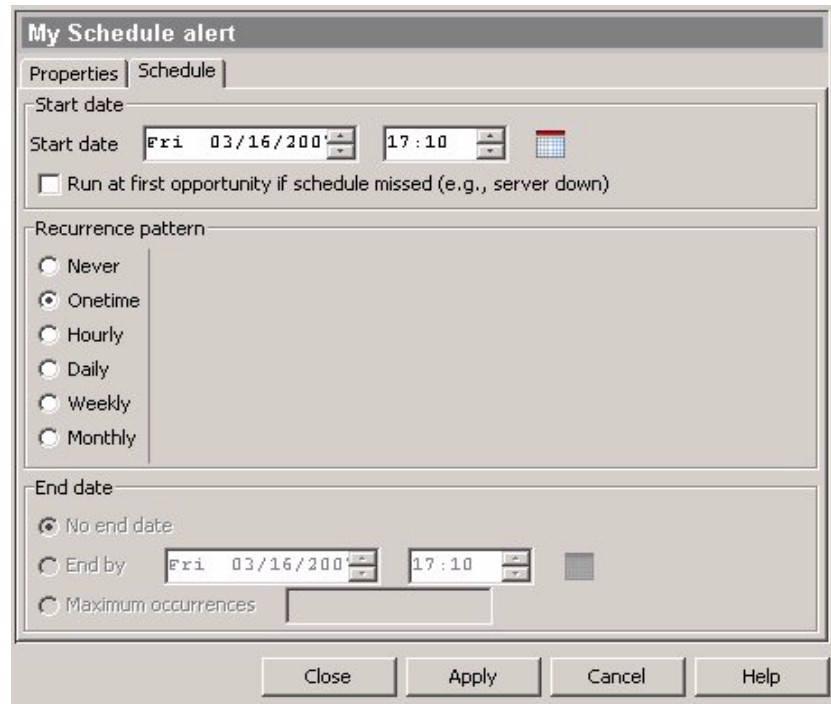


Figure 16-19. Policy Manager, Schedule-driven Alerts filter

7. Set the **Start Date** for enforcement of the policy. The default is the date and time the policy is created.

You can type a new date and time, or use the arrows to increase or decrease the date and time entries. Note that the time clock uses 24 hour format; thus a time of 22:00 is used to indicate a start time of 10:00 pm.

Check (click) the **Run at first opportunity if schedule missed** check box to enforce a policy as soon as possible after the start date. This is especially useful when a policy is re-enabled (after being disabled). The policy will be enforced immediately if it missed a scheduled enforcement time while disabled.

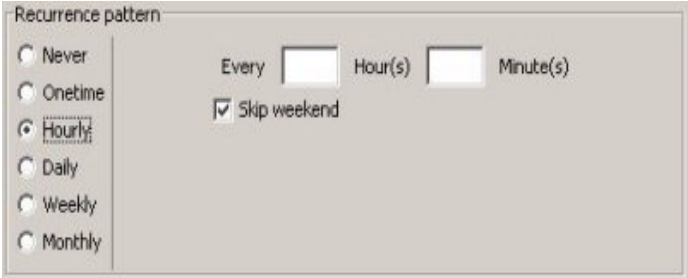
8. Define the alert schedule using the **Recurrence pattern** options:

Never	No further action is required (Use this option with event-driven policies, to disable the recurring enforcement schedule).
One time	No further action is required (the currently scheduled time is used with no recurrences).

Using Policy Manager Features Defining Alerts for Policies

Hourly	Type the number of hours and minutes to wait between enforcements. If you do not want the policy enforced on Saturdays and Sundays, select the Skip weekend check box.
Daily	Type the number of days to wait between enforcements. If you do not want the policy enforced on Saturdays and Sundays, select the Skip weekend check box.
Weekly	Select the days of the week you want to enforce the policy.
Monthly	This will enforce the schedule on the last day of the month, OR Select the Day option and set the day of the month for enforcement.

The screen display will vary based on the Recurrence pattern you select. For example, the figure below shows the recurrence options for hourly.



The screenshot shows a dialog box titled "Recurrence pattern". On the left, there is a vertical list of radio buttons for "Never", "Onetime", "Hourly", "Daily", "Weekly", and "Monthly". The "Hourly" option is selected. To the right of the radio buttons, there are input fields for "Every" (with a value of 1), "Hour(s)" (with a value of 1), and "Minute(s)" (with a value of 0). Below these fields is a checked checkbox labeled "Skip weekend".

Figure 16-20. Hourly Recurrence pattern options

- To set the End date options, click the radio button to identify when the schedule should end.

No end date	Policy will run as scheduled until it is changed or deleted.
End by	Set the date and time that the policy enforcement will "end by."
Maximum occurrences	Set the number of times the policy should be enforced before it is disabled automatically.

- Click **Apply** to save the Filter criteria.
- Click Close to exit the Policy manager.
If you click Close before Apply, you will be prompted to save or cancel the changes.

Editing Policy Alerts

To edit a policy alert:



1. Click the Launch Policy Manager button in the toolbar to launch the Policy Manager window.
2. To display the Manage Alerts (modify) pane
 - Click the Alerts' node in the Policy Manager navigation pane, or
 - Right-click an Alert in the list and select Modify in the menu, or
 - Double-click an entry in the list.
3. Click the Alerts node in the Policy Manager window to display the Manage Alerts pane.
4. Select the alert in the list, which enables the Edit... and Delete buttons.
5. Click Edit... to launch the action properties window and edit the Alert parameters as needed.

The alert property tabs displayed will vary based on the Alert type.

6. Click Apply to save your changes, then click Close to exit the Policy Manager window.

Note:

When an alert is used by Policies, those policies will be temporarily disabled while changes are saved, or the alert is deleted.

Deleting Policy Alerts

To delete a policy action:



1. Click the Launch Policy Manager button in the toolbar to launch the Policy Manager window.
2. Click the Alerts node in the Policy Manager window to display the Manage Alerts pane.
3. Select the alert(s) in the list, which enables the Edit... and Delete buttons.
4. Click the Delete button, then click Yes in the confirmation dialog to delete the alert.

The alert is removed from the Alerts list in Policy Manager.

5. Click Close to exit the Policy Manager window.

Configuring Policy Actions

ProCurve Manager Plus comes with a set of pre-defined actions, that you can customize for use in your Policies. You can also create user-defined actions using the Configurable Integration Platform (CIP) feature. See “Adding Plug-in Applications” on page 19-12 for detail on using User-defined Actions. The basic process for configuring Actions is described below, using one of the Policy Manager action types.

The configuration parameters for each Action type are described in the tables under “Action Type Definitions” on page 16-40. The tables correspond to the Action type groups (Config Manager, Device Management, Policy Manager, etc.).

Creating an Action

The following process describes a fairly simple Action type configuration, that includes a single tab of action parameters:



1. Click the Launch Policy Manager button in the toolbar to launch the Policy Manager window.
2. Click the Actions node in the Policy Manager window to display the Manage Actions pane.

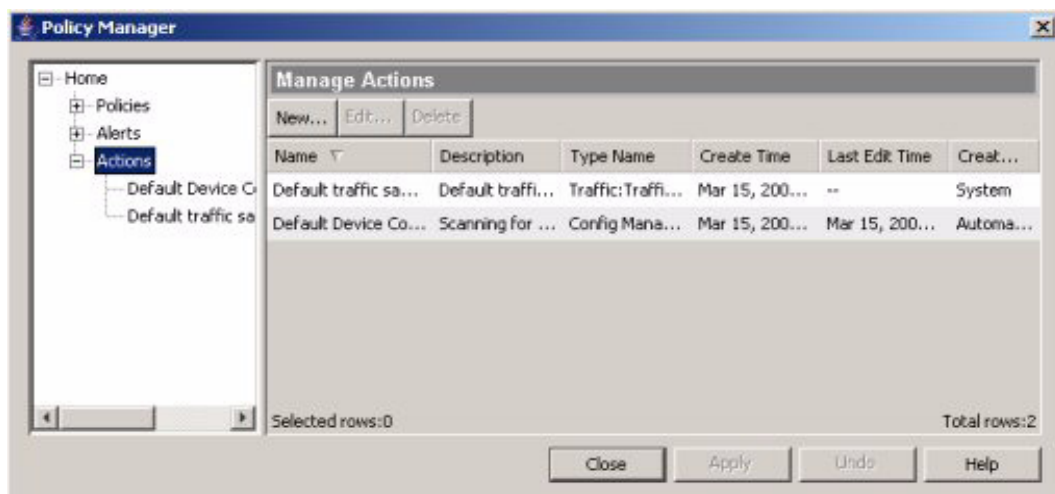


Figure 16-21. Policy Manager: Manage Actions

The Manage Actions window displays the list of defined Actions.

3. Click New... to launch the Create Action dialog:

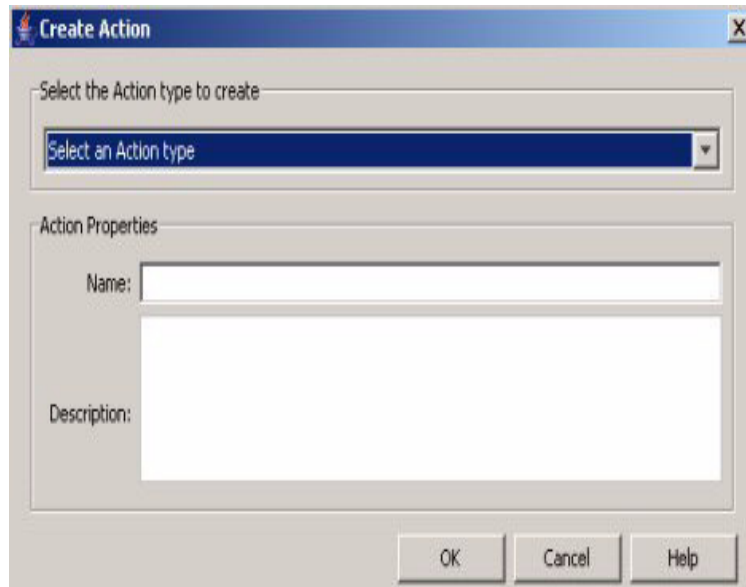
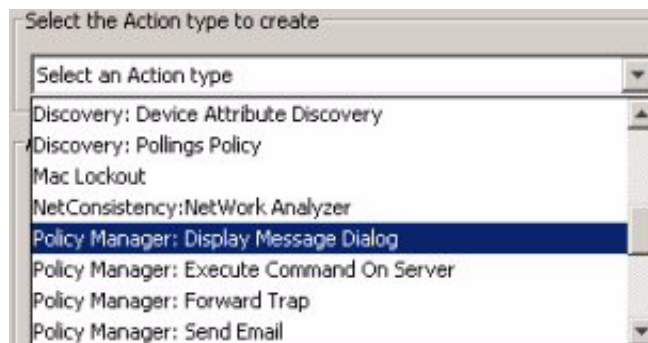


Figure 16-22. Create Action dialog

4. Select the Action type from the pull-down menu.



For this example, you would need to scroll the menu to select the Policy Manager: Display Message Dialog option.

5. Type a Name for the Action (required) and a brief Description (optional)
6. Click OK to save the Action and display the Action Properties tab. The properties you set in the previous step should appear.

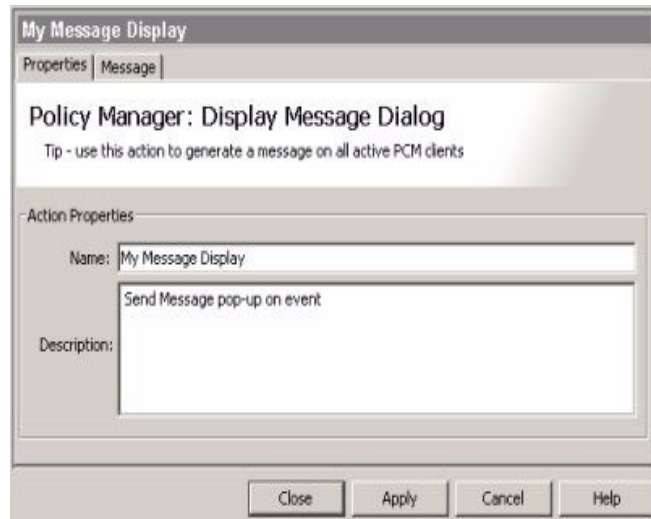


Figure 16-23. Action Properties window

7. Click the Message tab to configure parameters for the Display Message.

Tip:

For users of PCM 2.1 or earlier, this is what you would do to create a Pop-up Message Dialog for an alert.

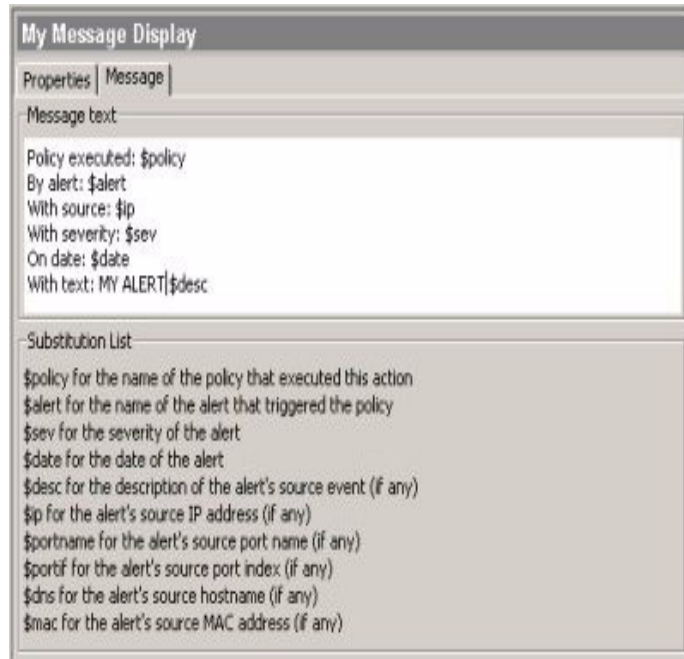


Figure 16-24. Display Message Action: Message tab

Type the message text (a string from 1-75 characters) you want to appear in a pop-up dialog when an alert is issued. The default is to include the variables described in the Substitution List. You can enter additional text, and/or delete any of the default message variables.

The Substitution List describes the default variables included with the message, which will be replaced (before the message is displayed) by data from fields in the alert that triggers the action.

8. Click Apply to save the Action configuration.
9. Click Close to exit the Policy Manager

If you click Close before Apply, you will be prompted to save or cancel the changes.

Creating an Action: Multi-tab Configuration Process

The following example steps you through a more complex Action type, that includes multiple tabs for setting the action parameters.

The first few steps are the same as before.

1. Open the Policy Manager and select the Actions node to display the Action Manager window.
2. Click New... to launch the Create Action window.
3. Select the Action type from the pull-down menu, then type a Name and description for the Action.

For this example, we selected the NetConsistency:Network Analyzer action.

4. Type a Name for the Action (required) and a brief Description (optional)
5. Click OK to save the Action and display the Action Properties tab. The properties you set in the previous step will appear.

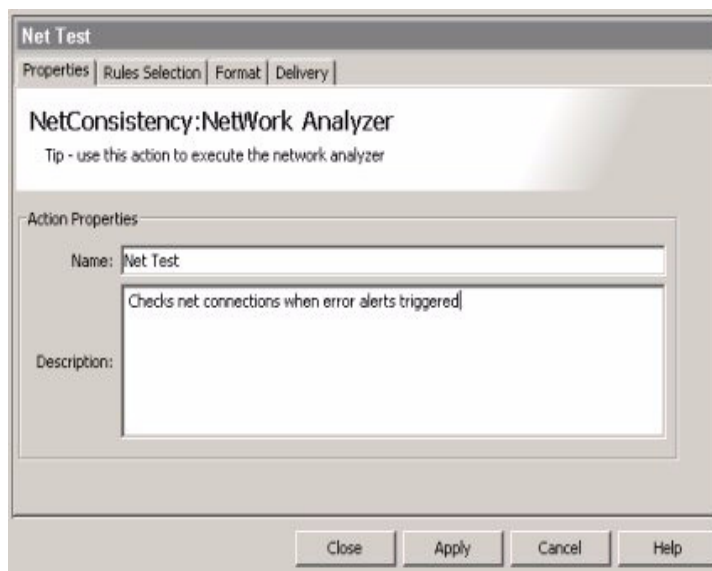


Figure 16-25. Network Analyzer Action:Properties tab

As you can see there are three additional tabs included for this Action type. You need to set the parameters in each tab to complete the Action configuration.

6. Click the Rules Selection tab and select the rules to include in the action.

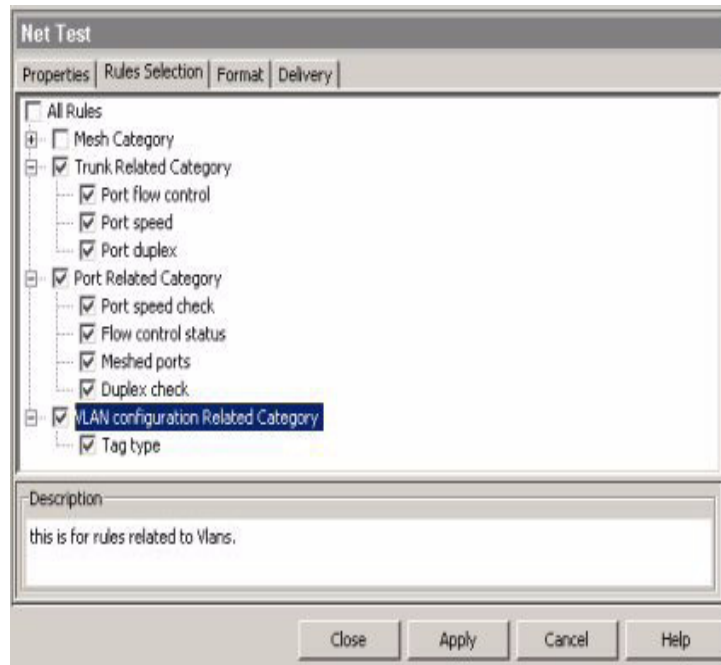


Figure 16-26. Network Analyzer Action:Rules Selection tab

In this screen, you click the check boxes to select or deselect the rules options. You can select All Rules, or any Category of rules (Mesh, Trunk, Port), or individual test options within a category. When you select a rule Category or individual rule, the description of the rule that will be tested displays.

7. Click the Format tab to select the Report format that will be used to output the Network Analyzer test results.

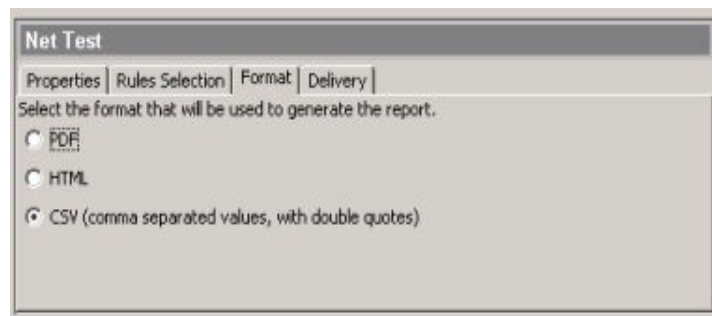


Figure 16-27. Network Analyzer Action:Format tab

Using Policy Manager Features Configuring Policy Actions

8. Click the Radio button to select the format. Only one option can be selected at a time.
9. Click the Delivery tab to set the method used to send the report to the appropriate person.

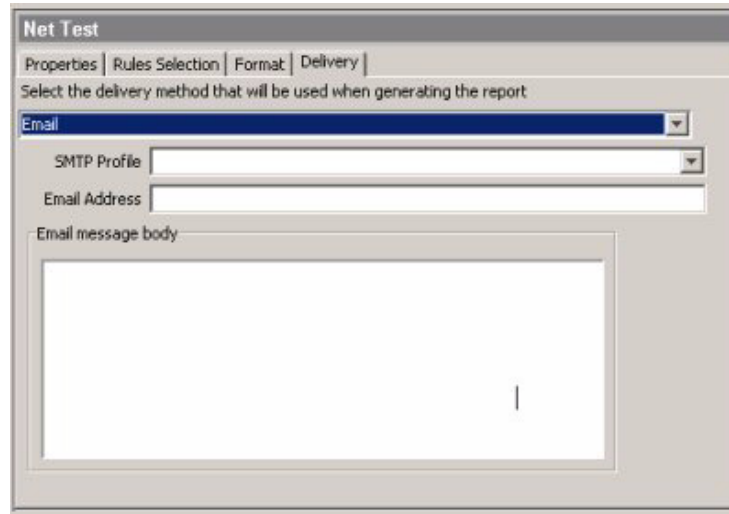


Figure 16-28. Network Analyzer Action:Delivery tab

E-mail is the default method. It will e-mail the report to the address specified. It also requires that you have an SMTP profile for the E-mail address. See “Creating SMTP Profiles” on page 2-51 for details.

If you select FTP, the fields in the Delivery tab will change to allow input of the required information for FTP.

The screenshot shows the 'Delivery' tab of the Network Analyzer Action configuration window. At the top, there are tabs for 'Properties', 'Rules Selection', 'Format', and 'Delivery'. Below the tabs, the text reads 'Select the delivery method that will be used when generating the report'. A dropdown menu is set to 'FTP'. Below this, there are five text input fields: 'FTP Server', 'Path (on server)', 'Filename', 'Username', and 'Password'. At the bottom, there is a section titled 'Filename conventions' with three radio button options: 'No timestamp in file name (overwrite file)' (which is selected), 'Prepend timestamp to file name', and 'Append timestamp to file name'.

Figure 16-29. Network Analyzer Action: Delivery tab, FTP options

Similarly, if you select the "File" option, the displayed fields reflect requirements for delivery of the report output to a file.

The screenshot shows the 'Delivery' tab of the Network Analyzer Action configuration window. At the top, there are tabs for 'Properties', 'Rules Selection', 'Format', and 'Delivery'. Below the tabs, the text reads 'Select the delivery method that will be used when generating the report'. A dropdown menu is set to 'File'. Below this, there are two text input fields: 'Path (on server)' and 'Filename'. At the bottom, there is a section titled 'Filename conventions' with three radio button options: 'No timestamp in file name (overwrite file)' (which is selected), 'Prepend timestamp to file name', and 'Append timestamp to file name'.

Figure 16-30. Network Analyzer Action: Delivery tab, File options

In each case, enter the required data.

10. When you have defined the parameters in each tab, click Apply to save the Action configuration, then click Close to exit the Policy Manager window.

Each of the Actions you create under the Actions node in the Policy Manager, and in the Manage Actions list.

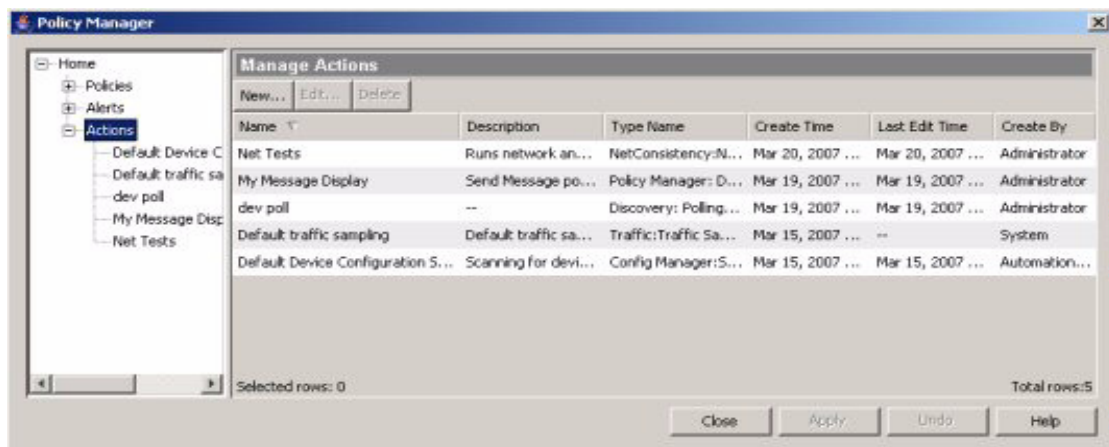


Figure 16-31. Policy Manager: Actions list display

Editing Policy Actions

To edit a policy action:



1. Click the Launch Policy Manager button in the toolbar to launch the Policy Manager window.
2. Click the Actions node in the Policy Manager window to display the Manage Actions pane.
3. Select the action in the list, which enables the Edit... and Delete buttons.
4. Click Edit... to launch the action properties window and edit the Action parameters as needed.

The action property tabs display will vary based on the Action type.

5. Click Apply to save your changes, then click Close to exit the Policy Manager window.

Note:

When an action is used by Policies, those policies will be temporarily disabled while changes are saved, or the action is deleted.

Deleting Policy Actions

To delete a policy action:



1. Click the Policy Manager button in the toolbar to launch the Policy Configuration Manager window.
2. Click the Actions node in the Policy Manager window to display the Manage Actions pane.
3. Select the action in the list, which enables the Edit... and Delete buttons.
4. Click the Delete button, then click Yes in the confirmation dialog to delete the action.

The action is removed from the Actions list in Policy Manager.

5. Click Close to exit the Policy Manager window.

Action Type Definitions

The following tables provide a description of the Action types, along with the tabs and configurable parameters for that action.

Note that the "Properties Tab" is not listed as it is the same for all Action types; that is, you use it to select the action type, and enter a name and description for the configured action.

Table 16-1. Action Types

Action Type	Description	Tabs	Parameters
Config Manager: The Config Manager action types can be used in policies to automate various device configuration tasks. The functionality provided is similar to the configuration manager functions described in Chapter 12, "Managing Device Configurations".			
Deploy Device Group	Used to deploy a configuration to a device group (all same model)	Rollback: Used to select a labeled (known good) configuration to apply to target devices.	<ul style="list-style-type: none"> Select Label Prerequisite: a labelled configuration for the device group.
		File Copy: Used to set Secure Copy options for transfer of configuration files.	<ul style="list-style-type: none"> Use TFTP Use Secure Copy* Allow TFTP failover options *Must have SSH enabled on device
Deploy Template to Group	Deploy configuration template to device group	Template File Copy: (see above)	<ul style="list-style-type: none"> Select Template Prerequisite: Configuration template already created for device type.
Export Device Configuration	Export archived device config file	Properties only	Refer to "Exporting Device Configurations" on page 12-43.
Group CLI	Use to execute CLI commands on target devices	Script	<ul style="list-style-type: none"> Enter commands Commit to Flash Capture Config
		Options	<ul style="list-style-type: none"> Capture output to a file (enter Filename, select Append option)
Group Script	Use to execute a script against selected devices	Properties	<ul style="list-style-type: none"> Name and text description
		Script	<ul style="list-style-type: none"> Function name Command line End of Result and Timeout
		Options	<ul style="list-style-type: none"> Capture output to a file (enter Filename, select Append option)

Table 16-1. Action Types

Action Type	Description	Tabs	Parameters
Scan Device	Scan Device Configurations	File Copy: (see above)	
<p>Device Management: Device Manager action types are similar to the device manager functions described in Chapter 7, “Managing Network Devices”. Use these actions in a Policy to automate device management. Note that the “Properties Tab” is not listed as it is the same for all Action types; that is, you use it to select the action type, and enter a name and description for the configured action.</p>			
Authorized Managers	Add/edit Authorized Manager on target device	<p>Authorized managers (Add, edit, delete) See “Adding Authorized Managers” on page 7-8 for additional information.</p>	<ul style="list-style-type: none"> • IP Address Mask • Access level • Previous Device Settings: Leave/Clear
Communication Parameters	Set Communication Parameters in device for SNMP, CLI	General	<ul style="list-style-type: none"> • Select settings to configure: SNMP and/or CLI
		SNMP version	<ul style="list-style-type: none"> • select SNMP versions (V1/2, V3)
		<p>SNMP Credentials</p> <p>See “Setting Communication Parameters in Devices” on page 7-15 for additional information.</p>	<ul style="list-style-type: none"> • Community Names (add, edit, delete) <ul style="list-style-type: none"> – Community Name – Read Access – Write Access – Set Management community • SNMPV3 users- <ul style="list-style-type: none"> – Username – Auth Protocol, Auth password – Group – Priv Protocol, Priv Password – assign Management User
		CLI Mode	<ul style="list-style-type: none"> • Select Telnet and/or SSH
		SSH Credentials	<ul style="list-style-type: none"> • Select SSH1 or SSH2, and • Password, or Key Authentication
		User Credentials	<ul style="list-style-type: none"> • Leave Existing settings, or Enable Password Protection: <ul style="list-style-type: none"> – Set Mgr Username, Password – Set Opr Username, Password

Table 16-1. Action Types

Action Type	Description	Tabs	Parameters
Spanning Tree Protocol (See below)	Use to enable or disable STP on target devices	STP State	Enable or Disable
	<p>Using Spanning Tree Protocol</p> <p>The Spanning Tree Protocol (IEEE 802.1d) maintains a loop-free topology in networks with redundant bridges or switches. The spanning tree devices determine which devices will be active and which will be backups so that no two nodes in a network have more than one active path between them at any time. The Spanning Tree Protocol uses the most efficient path between segments. If a bridge or switch fails, the other bridges and switches reconfigure the network automatically. When the problem is repaired, the bridges and switches automatically return to the original network configuration</p>		
Test Communication Parameters	Runs communication parameters test	Properties only	See "Using Test Communication Parameters in PCM" on page 7-36 for additional information on this feature.
Trap Receivers	Add trap receiver for target device	Trap Receivers	<ul style="list-style-type: none"> • Add, edit, delete trap receivers: <ul style="list-style-type: none"> – IP Address – Event log filter
Discovery action type.			
Device Uptime and Status Polling	Polls target devices for their current status.	Properties only	<ul style="list-style-type: none"> • Name and text description
MAC action types			
MAC Mirroring	Monitor the source MAC address and/or destination MAC address contained in events	MAC Monitoring: Used to configure monitored MAC addresses.	<ul style="list-style-type: none"> • Monitor MACs in the event • Event field <ul style="list-style-type: none"> – Source – Destination – Both • MACs to be monitored
MAC Lockout	Configure MAC lockout parameters on the target devices.	MACs	<ul style="list-style-type: none"> • MACs in the event • MACs to be locked out

Table 16-1. Action Types

Action Type	Description	Tabs	Parameters
NetConsistency action type			
Network Analyzer		Rules Selection	<ul style="list-style-type: none"> Use check boxes to select network rules to be tested. See Chapter 17, "Using the Network Consistency Analyzer" for rule details.
		Format	<ul style="list-style-type: none"> Select report format: PDF, HTM, CSV, ODT, XLS, RTF
		Delivery	<ul style="list-style-type: none"> Select Delivery Method and enter details <ul style="list-style-type: none"> Email (requires SMTP profile) FTP - set FTP server and filename, username and password File - set server path and filename
<p>Policy Manager: The Policy Manager action types can be used to generate alerts in response to the triggering event. For users familiar with PCM 2.0 and 2.1 versions, these action types replace the Alert Configuration Wizard features. (Note that the "Properties Tab" is not listed as it is the same for all Action types; that is, you use it to select the action type, and enter a name and description for the configured action.)</p> <p>Content Variables for use in Policy Manager Actions</p> <p>The Substitution List in the tabs for configuring Policy Manager actions describes the variables you can use in the Content and text fields. The variables will be replaced (before the trap or message is forwarded) by data from fields in the event that invokes the alert.</p>			
Display Message Dialog	<p>Use to display text pop-up message for the alert</p> <p>Note: When sFlow data comes from a source device that PCM has not discovered (typically when sFlow is configured directly on a device's CLI and sent to PCM), the source-related contents of the message dialog are not populated.</p>	Message	<ul style="list-style-type: none"> Message text Can use substitution list for variables provided on tab.

Table 16-1. Action Types

Action Type	Description	Tabs	Parameters
Execute Command on Server	Execute system command on management server	Command	<ul style="list-style-type: none"> Command text can use substitution list for variables provided on tab.
Forward Trap		Trap	<ul style="list-style-type: none"> Trap Receiver (IP address) Port (default is 162) Content - enter contents to be included in trap message, can use substitution list for variables, provided on tab.
Send Email	<p>Fwd e-mail with alert details</p> <p>Note: When sFlow data comes from a source device that PCM has not discovered (typically when sFlow is configured directly on a device's CLI and sent to PCM), the source-related contents of the message dialog are not populated.</p>	Email	<ul style="list-style-type: none"> SMTP Profile* To: email address From: email address Subject: text input, can use variable substitutions. Message Body: text input, can use variable substitutions shown in tab. <p>* Prerequisite: Must set up SMTP profile first. See "Creating SMTP Profiles" on page 2-51 for details.</p>
Stop and backup PCM server	Stop PCM Server and execute an automatic backup	Properties	<ul style="list-style-type: none"> Name and text description
		Path Selection	<ul style="list-style-type: none"> Pathname (on PCM Server) where backup file is stored
Port Mirroring action type			
Port Mirroring	Configures mirror destination ports for source ports to be monitored.	Port Mirroring	<ul style="list-style-type: none"> Any available mirror destination Any of below selected mirror destinations <ul style="list-style-type: none"> - Add -Delete
Port Settings: The Port Settings action types can be used to limit access, or service available at the target port			
Enable/Disable Port(s)	Use to temporarily shut down a port	Port Status	<ul style="list-style-type: none"> Enabled Disabled

Table 16-1. Action Types

Action Type	Description	Tabs	Parameters
Guaranteed Minimum Bandwidth (GMB)	Use to set the percentage of bandwidth allocated to the various priority levels of each outbound traffic priority queue of the targeted ports on devices that support GMB.	Guaranteed Minimum Bandwidth	<ul style="list-style-type: none"> • Configure GMB on target port <ul style="list-style-type: none"> - Disable GMB - Enable GMB • If enable GMB, set <ul style="list-style-type: none"> Low Priority Queue % Normal Priority Queue % Medium Priority Queue % High Priority Queue %
Quality of Service	Used to set the priority of packets handled by the targeted ports on devices that support Quality of Service (QoS).	Quality of Service	<ul style="list-style-type: none"> • Configure source port QoS settings on targeted port • No override • 802.1p Priority, priority (0 - 7) • DSCP Priority, priority (0 - 7) and codepoint (0 - 63). See Operating Notes for QoS below.
Rate-limit	Limits the inbound bandwidth on a switch port that a user or device can utilize. Effectively enforces maximum service level commitments granted to network users.	Rate Limit	Configure Rate Limiting on target ports <ul style="list-style-type: none"> • Disable Rate Limiting • Enable Rate Limiting • Rate Limit % : set the maximum percentage of bandwidth to be allocated to the targeted ports.
<p>Operating Notes for QoS:</p> <p>With No override, QoS does not affect the packet queuing priority or VLAN tagging, and packets are handled as follows:</p> <ul style="list-style-type: none"> • If received and forwarded on a tagged VLAN, the 802.1 priority is not changed. • If received on an untagged VLAN and forwarded on a tagged VLAN, the 802.1 priority is 0 (normal). • If forwarded on an untagged VLAN, no 802.1 priority is used. <p>For 802.1p Priority: Assigns an 802.1p traffic priority setting (0-7) carried by packets moving from one device to another in an 802.1Q tagged VLAN environment. The switch uses the 802.1p priority to determine the queue in the outbound port to use for the packet. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority to the next downstream device. If the packet leaves the switch through an untagged VLAN, this priority is dropped, and the packet arrives at the next downstream device without an 802.1p priority assignment. 802.1p priorities range from 0-7 with 7 being the highest priority.</p> <p>For DSCP Priority: Associate a handling priority with a codepoint in an incoming IPv4 packet. DSCP priority is not dependent on tagged VLANs to carry priority policy to downstream devices. DSCP priorities range from 0-7 with 7 being the highest priority. Codepoints range from 0-63. The priority selected will be assigned to this codepoint regardless of its current setting.</p>			

Table 16-1. Action Types

Action Type	Description	Tabs	Parameters
Report Manager action type.			
Generate Report	Creates a report in selectable formats.	<p>Type</p> <p>Format</p> <p>Delivery</p> <p>Additional tabs to set report filters.</p>	<ul style="list-style-type: none"> • Select report format: PDF, HTM, CSV, ODT, XLS, RTF • Select Delivery Method and enter details <ul style="list-style-type: none"> – Email (requires SMTP profile) – FTP - set FTP server and filename, username and password – File - set server path and filename • Refer to Chapter 18, "Using Reports" for details on specific report parameters and settings.
Security action type			
VT Configuration	Configure Virus Throttle on target device. See Chapter 15, "Using Virus Throttle" for details on configuration.	VT Configuration	<ul style="list-style-type: none"> • Disable/Enable, • Set Global sensitivity (low, medium, high, aggressive) • Set VT Action to take. (notify only, throttle, block, no)
Software Update action types.			
DownLoad Software for Devices	Download switch software	Software Version(s)	Select switches Select software versions
Download Software Index	See "Downloading the Software Version List" on page 12-60 for details.	Properties only	
Reboot Device(s)	Schedule a reboot time for device(s).	Reboot Time	<ul style="list-style-type: none"> • Set a reboot time. If a reboot time is not specified, the device(s) will reboot at the time of execution of the action.

Table 16-1. Action Types

Action Type	Description	Tabs	Parameters
TMS-Manager action type.			
Firewall Policies		Configure Firewall Policies	<ul style="list-style-type: none"> • Select Zones and Action • Select Access • Enable this Policy • Enable IPS for this Policy • Enable logging on this Policy
		Action Settings	<ul style="list-style-type: none"> • Traffic Devices Selection <ul style="list-style-type: none"> – Use preconfigured targets – Auto Determine targets • Action Configuration <ul style="list-style-type: none"> – Display summary of changes in alert without making configuration changes to targets – Apply policies to target devices
Traffic action type.			
Traffic Sampling - SFLOW	Use to automatically enable or disable traffic sampling (sFlow) in response to an event.	Traffic Sampling State	<ul style="list-style-type: none"> • Click to select the sampling option <ul style="list-style-type: none"> – Enable traffic sampling – Disable traffic sampling
VLAN Manager action types			
Configure VLAN		VLAN Settings	<ul style="list-style-type: none"> • Click check box to select the Ignore and reboot options: <ul style="list-style-type: none"> – Ignore if VLAN not enabled on device – Ignore if max. VLANs reached on device – Ignore VLAN IDs that already exist on device. – Allow device reboot if required
		VLAN Information	<ul style="list-style-type: none"> • VLAN name, • IP Config (DHCP or disabled), • Subnet Mask (for DHCP), • VLAN IDs for <ul style="list-style-type: none"> – Tagged – Untagged – Forbidden VLAN IDs

Using Policy Manager Features
Action Type Definitions

Table 16-1. Action Types

Action Type	Description	Tabs	Parameters
Quarantine VLAN		Quarantine VLAN Policy	<ul style="list-style-type: none">• Quarantine VLAN ID• Port Tag Status<ul style="list-style-type: none">– Tagged– Untagged• Create VLAN (if it does not exist)<ul style="list-style-type: none">– IP Config (DHCP or disabled),– Subnet Mask (for DHCP) <p>Use Create VLAN if it does not exist already to create VLAN if it does not already exist. Otherwise, the policy action will fail.</p>

Viewing Configuration Manager Policy Status

Use the ConfigManager Policy Status tab of Configuration Management Status to view, enable/disable, edit, and delete scheduled policies created with Configuration Manager wizards (e.g., CLI, Deploy Configuration, Deploy Template wizards). This will NOT display any automation policies.



Clicking the Configuration Management Status button on the global toolbar and then clicking the ConfigManager Policy Status tab displays the following information for all scheduled Configuration Manager policies.

Policy Name	Name of policy
Policy Type	Type of policy
Policy Status	Whether the policy is enabled or disabled
Last Enforcement	Date and time the policy was last executed
Last Execution Status	Whether the policy successfully completed the last time it was executed

To Enable/Disable a Policy

1. Select the policy to be enabled or disabled.
2. Click **Enable/Disable**.

To Edit a Policy

1. Select the policy to be edited.
2. Click **Edit**, which opens the wizard used to create the scheduled configuration manager policy.
3. Edit the policy as explained in the related configuration manager wizard.

Remember the following when editing Configuration Manager policies:

- Recurring policies are triggered once they are re-enabled.
- Deploy Template policy names cannot be edited.
- Deploy Configuration policy names are in the format:

DeployConfig:<IP Address>:<timestamp of policy add/edit>

To Delete a Policy

1. Select the policy to be deleted.
2. Click **Delete** to delete the policy and its corresponding custom group, if applicable. (For scheduled CLI and Deploy Template policies, a custom group with the same name as the policy is created and contains all selected devices.)

Setting Policy Management Preferences

Use the Preferences for Global Policy Management to set the parameters that define the number of entries to include in the Policy History, the global setting for execution of device configuration changes by policies, and logging options for policies in the Events browser.

To set Policy Management Preferences:

1. Navigate to the Policy Management Preferences window.
 - a. Click the Preferences button in the toolbar (or use the Tools Menu).
 - b. In the Preferences navigation Pane, select Policy Management.

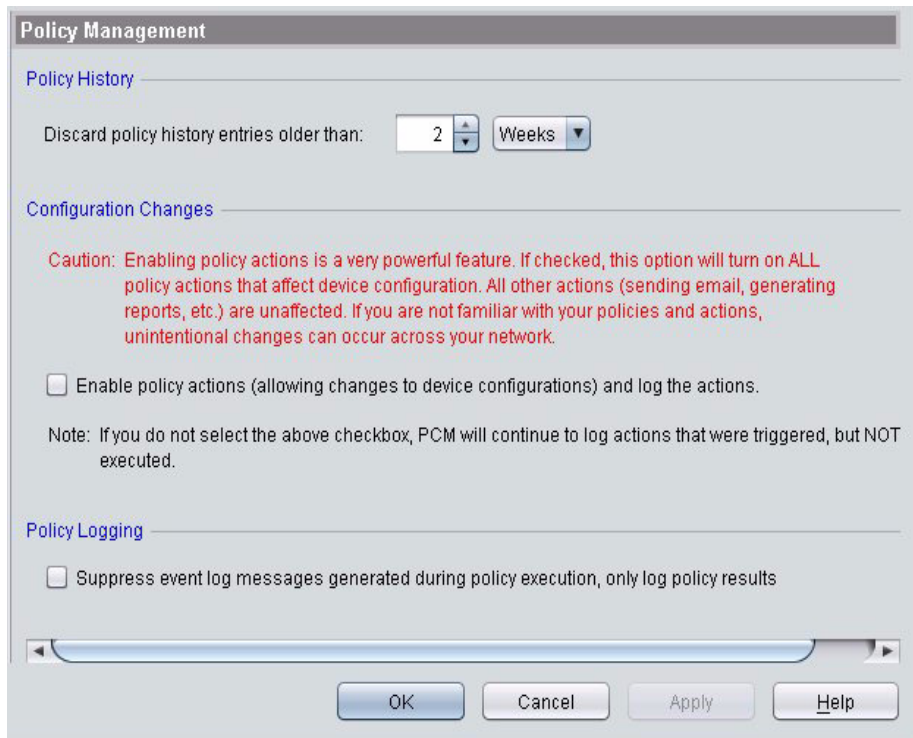


Figure 16-32. Policy Management Preferences

2. Set the discard policy in the **Policy History** section. Select the Discard policy history entries older than: value, and specify Weeks or Days for that value. The default is 2 weeks. You can type a number, or use the buttons to increase or decrease the value.

3. In the **Configuration Changes** section, use the check box to enable policy actions and log the actions.
 - If policy actions are disabled (check box is clear), you can monitor or test policies prior to full implementation. Policy activity will be logged as if all actions were executed, but it will not actually allow any policy action to change a device configuration.
 - If policy actions are enabled (check box contains a check mark) policies are implemented, including device configuration changes. Enable policies after testing and when you are confident the result of a device configuration is what you intended.
4. In the **Policy Logging** section, choose whether to suppress event log messages during policy execution.

Enable (check) the Suppress event log messages during policy execution, only log policy results check box to trim the reporting of intermediate steps taken during the execution of a policy, and log only the result of the final policy action. ProCurve recommends that you do not suppress Policy Logging until you have tested the policy and fully understand how your policy is operating. Once you are confident the policy is operating as intended you can suppress policy logging to reduce the number of policy activity events in the Events browser.
5. Click Apply to save your changes and OK to save and exit the window.

Notes:

- The number of Policy History entries retained is global and effects all policy history tables (Policy Activity tab, Security Activity tab and Policy Manager dialog). The selection chosen will impact the length of history available. If necessary, older records will be deleted to make room for new records.
- Policy History entries are not archived, except in the sense that the policy activity events shown in the event browser will be archived.
- When you enable the Policy Logging suppression, you will not be able to recover the suppressed policy events, they are lost forever.

Using the Network Consistency Analyzer

Introduction	17-2
Creating a Network Analyzer Policy	17-3
The Network Consistency Analysis Report	17-10
Network Consistency Rule by Device Type	17-11
Misconfiguration Messages	17-12

Introduction

The Network Consistency Analyzer feature helps you to find and correct problems in the network that may be affecting network performance and security. The Analyzer lets you check the ProCurve managed devices on the network to ensure that the device configuration is correct for the individual device, and according to network topology configurations. If incorrect configurations are found, the data for the specific device along with the configuration error is captured in a Network Analysis report.

PCM uses a "Network Consistency: Network Analyzer" Policy, that includes a series of pre-defined rules for various network and device configuration categories, including Port, Trunk, Mesh, STP, VLAN, ACLs, and Security. When the Policy is run, it compares each device in the specified group against the selected rules. It then creates a report in your choice of PDF or HTML format that can be saved as a file, sent by FTP to a specified address, or sent via e-mail. The Network Consistency Analysis Report:

- Lists the configuration category,
- Identifies the Ports, Devices, or VLANs where the problem was found,
- Defines the required action to correct the problem

Creating a Network Analyzer Policy

You can use the Network Consistency:Network Analyzer action with Policy Manager to specify the Report type and output method, specify the network consistency checking schedule, select device groups, and rules that will be used. Refer to “Configuring Policies” on page 16-4 for more detailed information on creating policies.

The basic steps to create a Network Analyzer Policy are:



1. Click the Policy Manager button in the toolbar to launch the Policy Configuration Manager window.

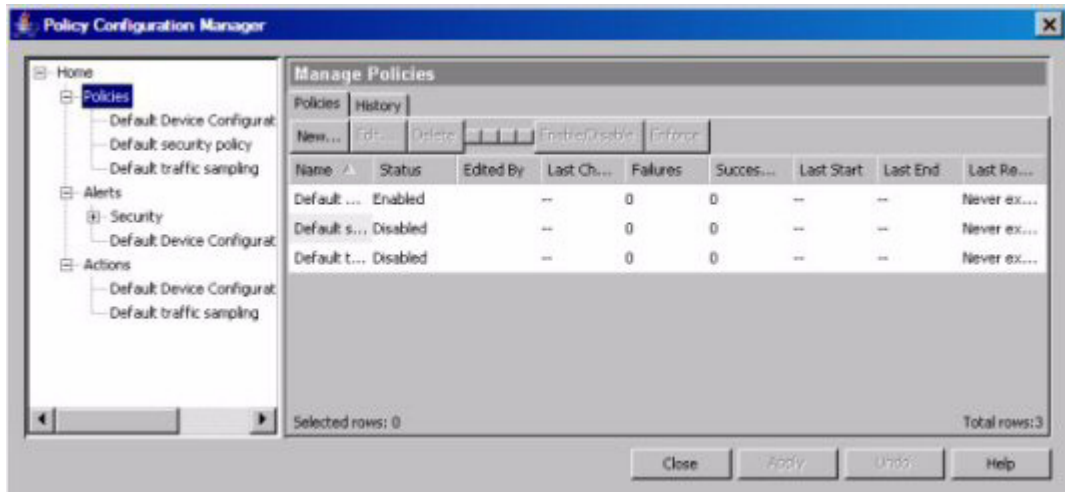


Figure 17-1. Policy Manager, Policies

2. Select the Policies node in the navigation tree to display the Manage Policies pane, then click New... to launch the Create Policy dialog.
3. Fill in the Policy information:
 - a. In the Name field, type a name to identify the policy, for example: Network Analyzer.
This name will appear as a node in the Policies navigation tree, and in the list in the Manage Policies pane.
 - b. In the Description field, type a brief description to help you identify the policy and what it will do.

- c. Click the Enable Policy check box to enable the policy.
A check in the box indicates the policy will take effect immediately when its configuration is completed.
If the check box is empty, the Policy is disabled. It will not take effect until you Enable it.
 - d. Click OK to save the Policy Properties and display the Policy Configuration pane for your new policy.
4. Click the tabs to fill in the required information:
- **Times** - Time periods when the policy can be executed. If no time is specified, the policy can execute at any time.
 - **Sources** - Devices or ports from which events are received. If no source (Device or Custom group) is selected, the policy will match events from any source.
 - **Targets** - Devices or ports on which a defined action will be performed in response to an alert, if applicable. If no Target is selected, the Alert will log a Policy Manager event in the event browser.
 - **Alerts** - A defined trigger used to launch an Action. Alerts can be event-driven, or scheduled to occur at a specified time.
 - **Action** - Select the NetConsistency:Network Analyzer action. You can customize the Network Analyzer action as described below.

To customize the Network Analyzer Action:

1. Open the Policy Manager and select the Actions node to display the Action Manager window.
2. Click New... to launch the Create Action window.
3. Select the NetConsistency:Network Analyzer Action type from the pull-down menu.
4. Type a Name for the Action (required) and a brief Description (optional)
5. Click OK to save the Action and display the Action Properties tab.
The properties you set in the previous step will appear.

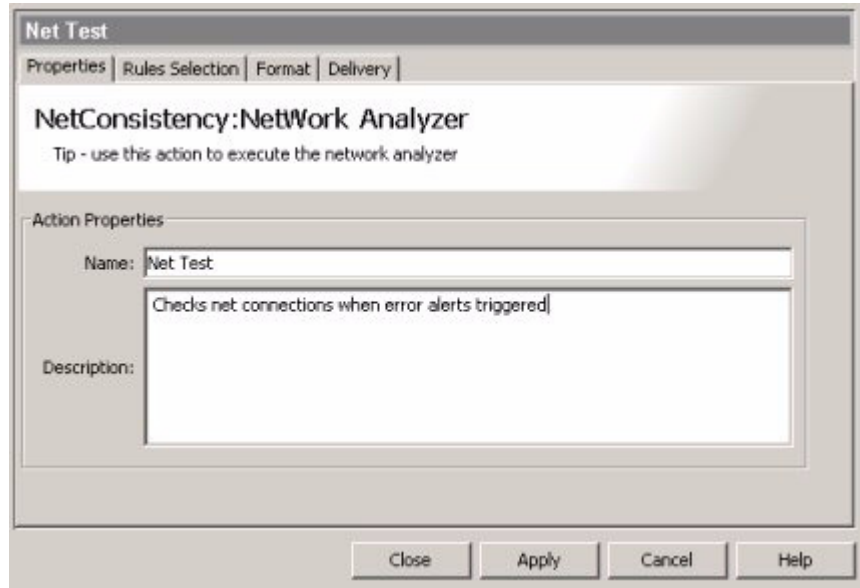


Figure 17-2. Network Analyzer Action:Properties tab

Set the parameters in each tab to complete the Action configuration.

6. Click the Rules Selection tab and select the rules to include in the action.

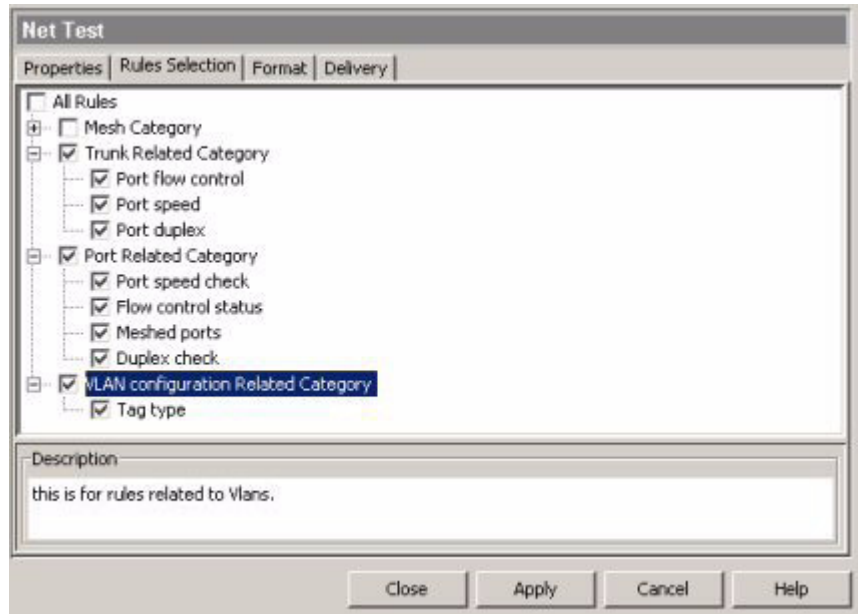


Figure 17-3. Network Analyzer Action:Rules Selection tab

In this screen, you click the check boxes to select or deselect the rules options. You can select All Rules, or any Category of rules (Mesh, Trunk, Port), or individual test options within a category. When you select a rule Category or individual rule, the description of the rule that will be tested displays.

7. Click the Format tab to select the Report format that will be used to output the Network Analyzer test results.

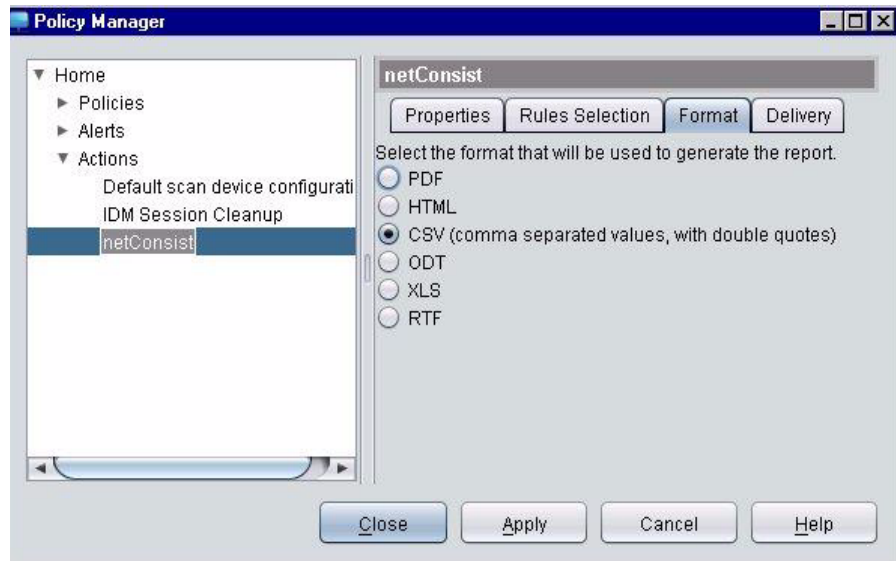


Figure 17-4. Network Analyzer Action:Format tab

Click the Radio button to select the format. Only one option can be selected at a time.

8. Click the Delivery tab to set the method used to send the report to the appropriate person.

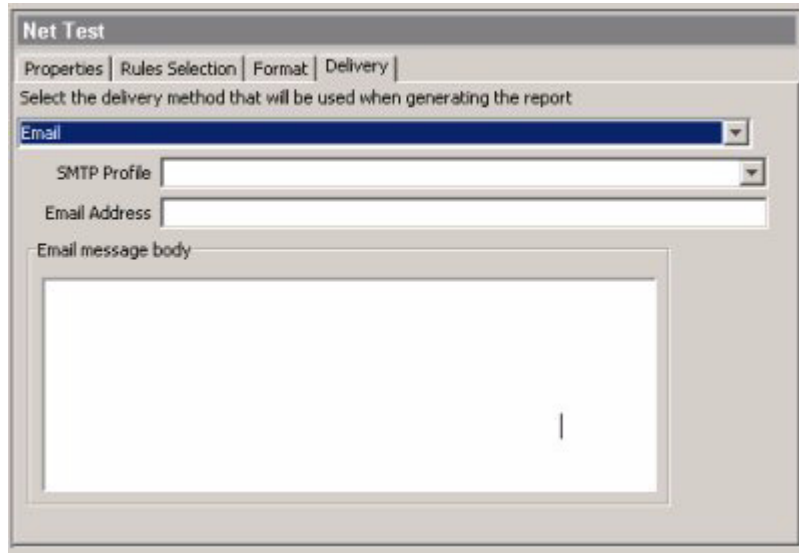
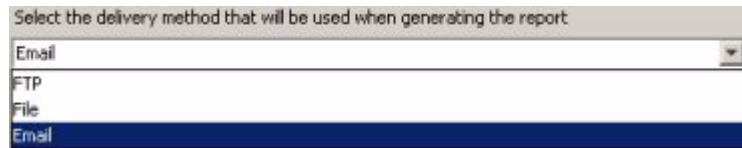


Figure 17-5. Network Analyzer Action:Delivery tab

Email is the default method. It will e-mail the report to the address specified. It also requires that you have an SMTP profile for the email address. See “Creating SMTP Profiles” on page 2-51 for details.

- a. Use the pull-down menu to select a different delivery method.



If you select FTP, the fields in the Delivery tab will change to allow input of the required information for FTP.

The screenshot shows a software window with four tabs: Properties, Rules Selection, Format, and Delivery. The Delivery tab is active. Below the tabs, there is a label: "Select the delivery method that will be used when generating the report". A dropdown menu is set to "FTP". Below the dropdown are five text input fields: "FTP Server", "Path (on server)", "Filename", "Username", and "Password". At the bottom, there is a section titled "Filename conventions" with three radio button options: "No timestamp in file name (overwrite file)", "Prepend timestamp to file name", and "Append timestamp to file name".

Figure 17-6. Network Analyzer Action: Delivery tab, FTP options

Similarly, if you select the "File" option, the displayed fields reflect requirements for delivery of the report output to a file.

The screenshot shows the same software window as Figure 17-6, but the Delivery tab is set to "File". The dropdown menu is set to "File". Below the dropdown are two text input fields: "Path (on server)" and "Filename". The "Filename conventions" section at the bottom remains the same, with three radio button options: "No timestamp in file name (overwrite file)", "Prepend timestamp to file name", and "Append timestamp to file name".

Figure 17-7. Network Analyzer Action: Delivery tab, File options

- b. In each case, enter the required data.
- c. When you have defined the parameters in each tab, click **Apply** to save the Action configuration, then click Close to exit the Policy Manager window.

The Network Consistency Analysis Report

After running the Network Analyzer Policy, you can review the report you specified in the Policy for any network consistency problems that may exist, and the action needed to correct the problem.

An HTML format report, saved to a file will appear similar to the following figure.

HP ProCurve Manager		Misconfiguration Report		Your Company Name	
				Street Address	
				City, State Zip	
Suite	Items	Misconfiguration	Required Action		
Port	Ports:XXX(p4),YYY(p5)	The link ports XXX(P4) speed 100 and	The port speed should be configured		
Port	Ports:XXX(p4),ZZZ(p5)	The link ports XXX (p4) is half duplex:	Ports duplex should be configured		
Port	Ports:XXX(p4),ZZZ(p5)	The link ports XXX (p4) is half duplex:	Ports duplex should be configured		
Trunk	Ports:XXX (P4),YYY(P5) Trunks:	Some of the links in trunk group XXX:	All ports on both ends of trunk group		
Trunk	Ports:XXX(P4),YYY(P5) Trunks:	Some of the links in trunk XXX (TRK1):	All ports in the trunk must have same		
Trunk	Ports:XXX(P4),YYY(P5)	Some of the links in trunk XXX (TRK1):	In Omega devices the primary port in		
Mesh	Ports:XXX (P4),XXX (P5),YYY (P4)	Meshed ports XXX (P4),XXX (P5) are	Meshed ports should be connected to		
Mesh	XXX,YYY	The device(s) XXX,YYY is not	Switches from same product family in		
Mesh	XXX,YYY	In the meshed devices XXX,YYY	In a mesh all devices must enable or		
Mesh	XXX,YYY	In the meshed devices XXX,YYY	In a mesh all devices must enable or		
Mesh	XXX,YYY,ZZZ,JJJ	In the meshed devices XXX,YYY	The devices in the mesh must have		
Mesh	XXX,YYY,ZZZ,JJJ	In the meshed devices XXX,YYY	In a mesh all devices must enable or		
Mesh	XXX,YYY	In the meshed devices XXX,YYY	In a mesh all devices must enable or		
Mesh	XXX	The device XXX of type 5300	The device of type 5300 must execute		
Mesh	XXX,YYY	The device(s) XXX,YYY in the mesh	Configuring them on meshed ports		
STP	XXX	In the device XXX have STP enabled	If spanning tree enabled multiboot		
STP	XXX,YYY,ZZZ	In the device XXX and its peers YYY,	If STP enabled and has links between		
STP	XXX,YYY,ZZZ	The 802.1Q compliant device(s)	A VLAN assigned to a port		
STP	VLANs:XXX (VLAN1,VLAN2)	In the device XXX these IPv4	If you create an IPv4 protocol VLAN,		
STP	XXX,YYY	In the device(s)XXX,YYY ACLs is	Source routing is enabled by default		
17 Jan 2005		Administrator		Page 1 of 2	

Figure 17-8. Network Consistency Analysis Report example

Network Consistency Rule by Device Type

Suite	Rule	Supported ProCurve Devices
Port	Port Speed should be same on both sides of a link or one side should be set to "Auto".	All managed ProCurve switches.
	Ports in a link should be configured the same on both sides, either Half duplex or Full duplex.	All managed ProCurve switches.
	Flow control status should be the same on ports forming a link	All managed ProCurve switches.
Trunk	All ports in the trunk must have the same flow control, duplex and speed.	All managed ProCurve switches
Mesh	Meshed ports in a switch should be connected to a meshed port in the other switch	8000M/4000M/2424M/2400M/1600M, 5300xl series, 3400cl series, and 6400cl series.
	Switches from the same product families in a mesh must run the same version of the OS.	8000M/4000M/2424M/2400M/1600M, 5300xl series, 3400cl series, and 6400cl series.
	Spanning tree must be same for all switches in the mesh (enabled or disabled). If spanning tree is enabled in the mesh, it must be the same enabled/disabled on all switches in the Mesh (STP or RSTP).	8000M/4000M/2424M/2400M/1600M, 5300xl series, 3400cl series, and 6400cl series.
	If a switch in the mesh has GVRP enabled, then all switches in the mesh must have GVRP enabled.	8000M/4000M/2424M/2400M/1600M, 5300xl series, 3400cl series, and 6400cl series.
	If a switch in the mesh has a particular static VLAN configured, then all switches in the mesh must have that static VLAN configured.	8000M/4000M/2424M/2400M/1600M, 5300xl series, 3400cl series, and 6400cl series.
	If a switch in the mesh has per VLAN's IGMP enabled/disabled, then all switches in the mesh must have IGMP enabled/disabled for their respective particular VLAN.	8000M/4000M/2424M/2400M/1600M, 5300xl series, 3400cl series, and 6400cl series.
	If a switch in the mesh has CDP enabled, then all switches in the mesh must have CDP enabled.	8000M/4000M/2424M/2400M/1600M, 5300xl series, 3400cl series, and 6400cl series.
	If a 5300 switch is connected to older devices in a mesh the "mesh backward compat" command should be executed in that switch.	5300xl series, 3400cl series, and 6400cl series.

**Using the Network Consistency Analyzer
The Network Consistency Analysis Report**

Suite	Rule	Supported ProCurve Devices
Mesh	Automatic Broadcast Control (ABC) on HP Procurve 8000M/4000M/ 2424M/2400M/1600M switches is not supported when these switches are used in the same mesh domain with Series 5300XL switches. Thus, in a mesh domain populated with both types of switches, ABC must be disabled	ABC available only on 8000M/4000M/2424M/2400M/1600M,
	Because paths through the mesh can vary with network conditions, configuring filters on meshed ports can create traffic problems that are difficult to predict, and is not recommended.	8000M/4000M/2424M/2400M/1600M, 5300xl series, 3400cl series, and 6400cl series.
VLAN	A VLAN assigned to a port connecting two 802.1Q-compliant devices must be configured with the same tag-type on both sides.	All managed ProCurve switches
	If you create an IPv4 protocol VLAN, you must also assign the ARP protocol option to the VLAN to provide IP address resolution. Otherwise, IP packets are not deliverable.	5300xl series, 3400cl series, 6400cl series, and 9300 series.

Misconfiguration Messages

SUITE	Items	Misconfiguration	Required Action
Port	Ports: X.X.X.X[A4], Y.Y.Y.Y[A1]	The link ports X.X.X.X[A4] speed is 100 and Y.Y.Y.Y[A1] speed is 200	The port speed should be configured the same on both ends of link, or it should be configured "Auto," otherwise this may lead to network breakdown.
	Ports: X.X.X.X [A4], Z.Z.Z.Z[A5]	The link ports X.X.X.X[A4] is half duplex and Z.Z.Z.Z[A5] is full duplex.	Ports duplex should be configured the same on both ends of link.
	Ports: X.X.X.X[C4], T.T.T.T[B5]	In X.X.X.X[C4] flow control status is disabled and T.T.T.T[B5] flow control status is enabled.	Both ends of the link must have their flow control set the same.
Trunk	Ports: X.X.X.X[A3], Y.Y.Y.Y[C3]	The Ports X.X.X.X[A3], Y.Y.Y.Y[C3] in trunk (TRK1) have different flow control settings.	All ports in the trunk must have same flow control, duplex and speed configured.

SUITE	Items	Misconfiguration	Required Action
Mesh	Devices: X.X.X.X, Y.Y.Y.Y, Z.Z.Z.Z	The device(s) X.X.X.X, Y.Y.Y.Y are running OS version 1 and Z.Z.Z.Z is running OS version 2 in the MESH	Switches from same product family in a mesh must run the same version of OS
	X.X.X.X, Y.Y.Y.Y Z.Z.Z.Z, J.J.J.J	In the meshed devices X.X.X.X, Y.Y.Y.Y STP is enabled, and Z.Z.Z.Z, J.J.J.J STP is disabled	In a mesh all devices must enable or disable STP.
	X.X.X.X, Y.Y.Y.Y Z.Z.Z.Z, J.J.J.J	In the meshed devices X.X.X.X, Y.Y.Y.Y GVRP is enabled, and Z.Z.Z.Z, J.J.J.J GVRP is disabled	In a mesh all devices having VLANs must enable or disable GVRP.
	X.X.X.X, Y.Y.Y.Y, Z.Z.Z.Z, J.J.J.J	In the meshed devices X.X.X.X, Y.Y.Y.Y static VLAN200 is configured and not configured in Z.Z.Z.Z, J.J.J.J	The devices in the mesh must have same static VLAN configured, if at all it's configured in one.
	X.X.X.X, Y.Y.Y.Y, Z.Z.Z.Z, J.J.J.J	In the meshed devices X.X.X.X, Y.Y.Y.Y IGMP enabled and Z.Z.Z.Z, J.J.J.J IGMP disabled	In a mesh all VLANs must have the same IGMP status (enable or disable) on all the meshed devices.
	X.X.X.X, Y.Y.Y.Y, Z.Z.Z.Z, J.J.J.J	In the meshed devices X.X.X.X, Y.Y.Y.Y CDP enabled and Z.Z.Z.Z, J.J.J.J CDP disabled	In a mesh all devices must enable or disable CDP.
	X.X.X.X	The "mesh backward compat" command is not configured on device X.X.X.X. This is required if the device is connected to older devices in a MESH.	The newer device types 5300/3400, etc., must execute "mesh backward compat" when connected to older devices in a mesh.
	X.X.X.X, Y.Y.Y.Y	The device(s) X.X.X.X, Y.Y.Y.Y in the mesh MESH have filter FL1, FL2	Configuring filters on meshed ports can create traffic problems and it's not recommended.
VLAN	X.X.X.X, Y.Y.Y.Y, Z.Z.Z.Z	The 802.1 Q compliant device(s) X.X.X.X, Y.Y.Y.Y, Z.Z.Z.Z have VLANS1, VLAN2 configured and connected but their port tagging is not same.	A VLAN assigned to a port connecting two 802.1Q-compliant devices must be configured with the same tag-type on both sides.
	VLANs: X.X.X.X (VLAN1, VLAN2)	In the device X.X.X.X these IPV4 protocol VLANs VLAN1, VLAN2 ARP protocol options is not assigned.	f you create an IPv4 protocol VLAN, you must also assign the ARP protocol option to the VLAN to provide IP address resolution.

Using Reports

Introduction	18-2
Setting Report Preferences	18-2
Using the Report Wizard	18-4
Creating a Report Policy	18-7
Types of Reports	18-13
Asset Management Reports	18-13
Device Access Control Reports	18-14
Diagnostics Reports	18-18
Network Activity Reports	18-22

Introduction

You can generate reports for auditing and regulatory compliance purposes using the Reports menu that provides pre-defined report formats for PCM and its plug-in modules.

- PMM reports are described in the *HP ProCurve Mobility Manager Network Administrator's Guide*.
- IDM reports are described in the *HP ProCurve Identity Driven Manager User's Guide*.
- NIM reports are described in the *HP ProCurve Network Immunity Manager Security Administrator's Guide*.

Note:

Unlicensed versions of PCM include only the Inventory Report.

Setting Report Preferences

To set the format and company information that appears in your PCM reports:

1. Open the Reports window in one of the following ways:



- Click the Preferences button in the PCM toolbar and select the Reports option.
- Select Tools > Preferences > Reports.

Reports

Orientation

Portrait Landscape

Footer Information

Company: Your Company Name

Address: Street Address

City/State/Zip: City, State Zip

Footer Logo Image

Image Preview Your Image Here

Figure 18-1. Reports Preferences

2. In the Reports window:
 - a. Select Portrait or Landscape. (The recommended orientation of reports with multiple columns and larger page widths is Landscape.)
 - b. Type your company name and full address. (Unusually long company names are truncated from the right.)
 - c. To add a logo in the footer of reports, click **Image** and select the graphic file (jpg, gif, or png) to be used. It is recommended that you use a high resolution graphic that is no larger than 135 x 65 pixels.
3. Save your new report settings:
 - Click **OK** to save and exit the Reports window.
 - Click **Apply** to save and leave the Reports window open.

Using the Report Wizard

This section describes how to use the Report Wizard to generate a report for any of the report types in the Reports menu.

To generate a report using the Report Wizard:

1. Select an option from the Reports menu, such as Device Access Control > Credential Change History, to start the Report Wizard for the selected report.
2. In the Credential Change History window:

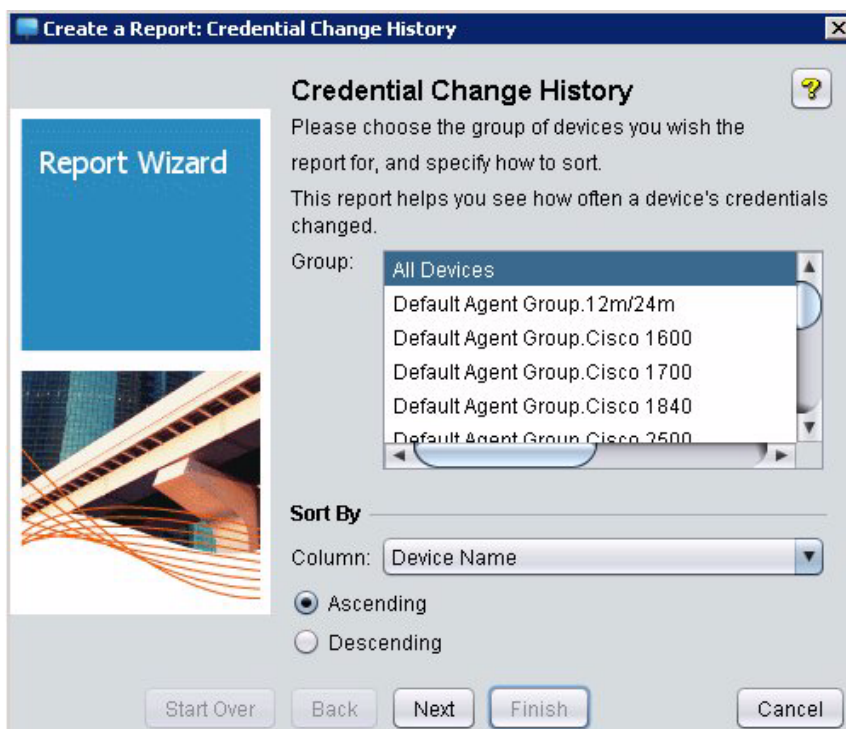


Figure 18-2. Report Wizard: Credential Change History

- a. Use the Group scroll list to select the Agent and Group (device or custom group) from which the report data will be generated. Select All Devices to include information on all devices.
- b. Use the Sort By: Column drop-down list to select the column to use to sort the report output. The default is Device Name. Entries in the drop-down list vary according to report type.

- c. Click the Ascending or Descending radio button to select the order in which items will be sorted.
 - d. Click **Next** to continue to configure additional report filters. (In this example, the Change Selection Criteria screen is displayed.)
3. In the Change Selection Criteria window:

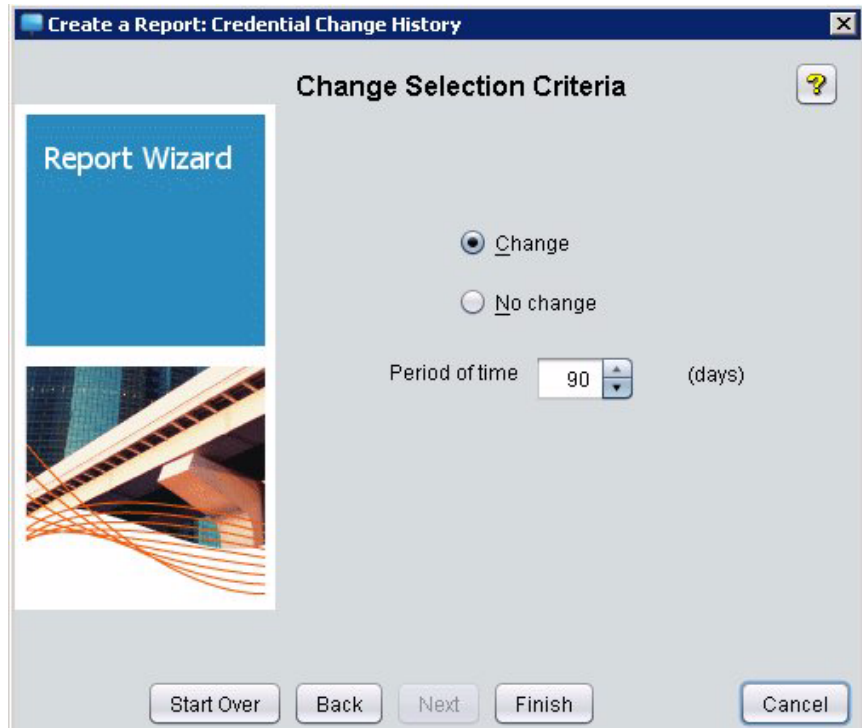


Figure 18-3. Report Wizard: Change Selection Criteria

- a. Click the radio button to select the report criteria:
 - Select Change to report on all devices in the selected group(s) where the access credentials have changed.
 - Select No Change to report on all devices in the selected group(s) where the access credentials have not changed.
- b. Set the Period of time to be included in the report. The default is 90 days. You can type a number or use the buttons to increase or decrease the number of days to be included.
- c. Click Finish to create and display the report.

Note: If you run a report on more than 1000 items, the output is limited to 40 pages. You may need to run several separate reports to generate the desired data.

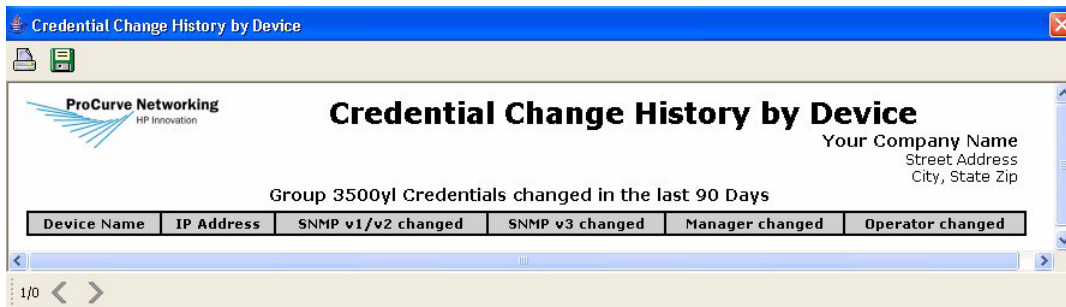




Figure 18-4. Report Wizard output: Credential Change History Report

-  Click the Print button to send the displayed report to a printer, using standard Windows print functionality.
-  Click the Save button to save the report using the Windows "Save" functionality in a standard file format, such as .xls, .html, .rtf, .csv, or .pdf.
- Scroll through multiple page reports using the forward and back buttons (> or <) at the bottom of the window.

For information on how to generate other report types, see “Types of Reports” on page 18-13.

Creating a Report Policy

You can also use the Policy Manager feature to schedule reports to be generated at regular intervals or in response to an event. For more information, refer to “Configuring Policies” on page 16-4. A Report policy consists of the following parameters:

- **Time** - Configure the Time periods when the report policy can be executed. If no time is specified, the policy can execute at any time.
- **Alerts** - Alerts can be event-driven or scheduled to occur at a specified time. Alerts serve as the trigger used to launch an event-driven Action. Use the Scheduled Alert option to set a recurring schedule for a report to be generated.
- **Action** - Configure the Report Manager:GenerateReport action for the policy. The following section describes the Report action types and configurable parameters and filters for each report type.

You will select the device groups the policy applies to in the Generate Report action.

To configure a Policy Action to run a report, such as Credential Change History:



1. Click the Policy Manager button in the toolbar to launch Policy Manager.
2. In the navigation pane of the Welcome window, click **Actions**.
3. In the Manage Actions pane, click **New**.

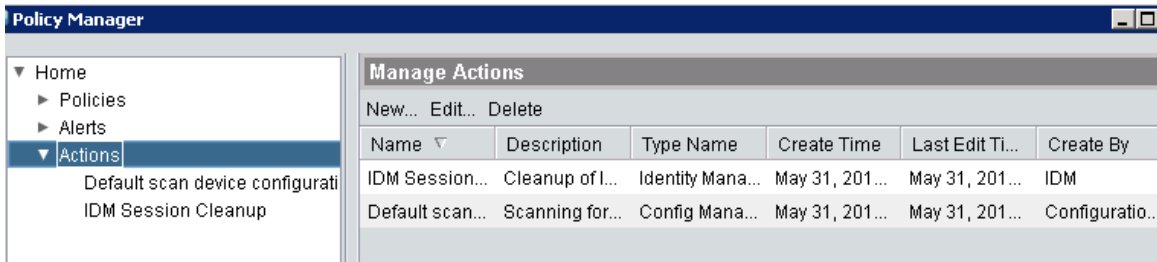


Figure 18-5. Policy Manager: Manage Actions

4. In the Create Action window:

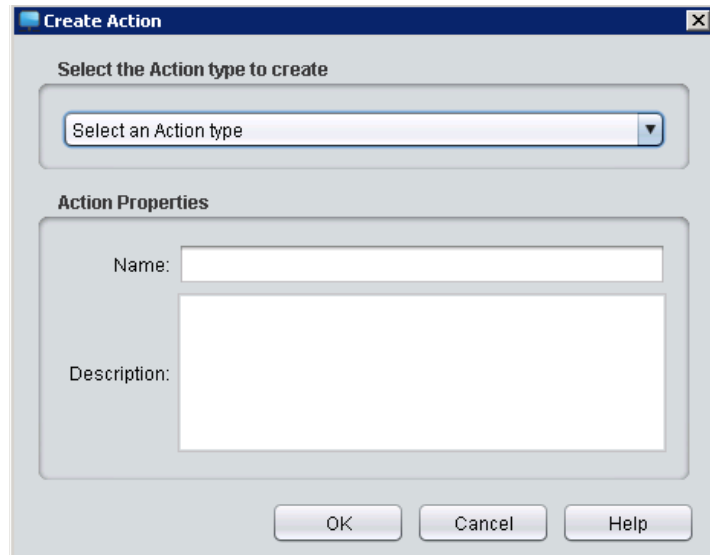


Figure 18-6. Policy Manager: Create Action

- a. Select Report Manager:Generate Report from the drop-down Action list.
- b. Enter a name for the report and an optional, text description.
- c. Click **OK**.

The name of the Report action is displayed under Actions in the PCM navigation pane. A Report Action window opens with the Type tab displayed. (The Action name and description are automatically entered in the Properties tab.)

5. In the Type tab, click on the report type you want to generate (in this example, Device Access Control: Credential Change History).

Additional tabs are displayed to the right of the Type tab according to the report type you select.

6. Click the next tab to the right of the Type tab (in this example, Credential Change History) and do the following:

The screenshot shows a software interface with several tabs at the top: Properties, Type, Credential Change History (selected), Change Selection Criteria, Format, and Delivery. Below the tabs, there is instructional text: "Please choose the group of devices you wish the report for, and specify how to sort. This report helps you see how often a device's credentials changed." A "Group:" label is followed by a scrollable list box containing the following items: "All Devices", "Default Agent Group.12m/24m", "Default Agent Group.Cisco 1600", "Default Agent Group.Cisco 1700", "Default Agent Group.Cisco 1840", "Default Agent Group.Cisco 2500", "Default Agent Group.Cisco 2950", "Default Agent Group.Cisco 2960", "Default Agent Group.Cisco 2970", "Default Agent Group.Cisco 3500", "Default Agent Group.Cisco 3560", "Default Agent Group.Cisco 3660", "Default Agent Group.Cisco 3750", "Default Agent Group.Cisco 4500", "Default Agent Group.Cisco 6500", and "Default Agent Group.Cisco 806". Below the list box, there is a "Sort By" section with a "Column:" label and a dropdown menu currently showing "Device Name". Underneath the dropdown are two radio buttons: "Ascending" (which is selected) and "Descending".

Figure 18-7. Policy Manager: Credential Change History

- a. Select the Agent and device group (including custom groups) for the devices on which you want to report. Select All Devices to generate a report on all discovered devices.
- b. In the Column drop-down list, select the column to use to sort the data in the report. The default is Device Name. Entries in the Column list vary according to report type.
- c. Click the Ascending or Descending radio button to specify the order in which information is displayed.
- d. Click the Change Selection Criteria tab.

7. In the Change Selection Criteria tab:

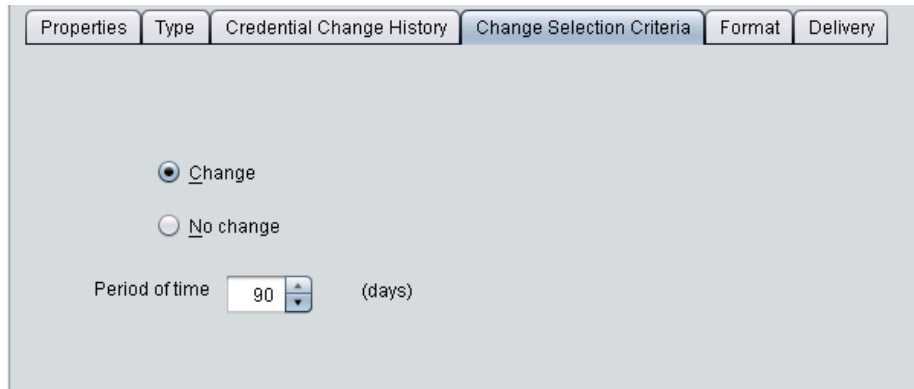


Figure 18-8. Policy Manager: Change Selection Criteria

- a. Specify the criteria to be used to select devices for the report:
 - Select Change to report on the devices in the selected group(s) for which access credentials have changed.
 - Select No Change to report on the devices in the selected group(s) for which access credentials have not changed.
 - b. Enter the Period of time (number of days) to use to gather device data. The default is 90 days.
 - c. Click the Format tab.
8. In the Format tab, select the output format to use for the report:

PDF	Generates the report in .pdf format. To view this file format, you will need Adobe Acrobat Reader, which can be downloaded free from http://get.adobe.com/read .
HTML	Generates the report in .html format, which can be viewed with any Web browser.
CSV	Generates the report using comma separated values with double quotes. This report can be viewed using WordPad, NotePad, or imported into other spreadsheet programs, such as Excel.
ODT	Generates the report in .odt format, which is a zipped .xml file.
XLS	Generates the report in .xls format, which can be viewed in MS Excel spreadsheets.
RTF	Generates the report in .rtf format, which can be viewed in most word processing applications.

9. Click the **Delivery** tab and configure the method to use to deliver the report.

The screenshot shows a configuration window for the 'Delivery' tab. At the top, there are several tabs: 'Properties', 'Type', 'Credential Change History', 'Change Selection Criteria', 'Format', and 'Delivery'. Below the tabs, the text reads 'Select the delivery method that will be used when generating the report'. There is a dropdown menu currently set to 'Email'. Below this, there is another dropdown menu labeled 'SMTP Profile'. Underneath that is a text input field labeled 'Email Address'. At the bottom, there is a section titled 'Email message body' with a large empty text area for entering content.

Figure 18-9. Report Manager Action: Delivery

From the top drop-down list, select a delivery method. Valid values are: FTP, File, and Email. The default is Email.

Select Email to send the report by e-mail to a specified address when the policy action is executed:

- a. Enter an SMTP profile for the e-mail address. See “Creating SMTP Profiles” on page 2-51 for more information.
- b. Enter the e-mail address.
- c. Enter an optional text to be included in the e-mail.

Select FTP to save the report on an FTP site. Proxy support is not provided.

- a. In the FTP Server field, type the IP address of the FTP site where you want to save the report.
- b. In the Path field, type the complete path to the server location where you want to save the report.
- c. In the Filename field, type the filename you want to assign to the report. You can automatically add a timestamp to the filename in the Filename conventions pane.
- d. In the Username field, type the username used to access the FTP site.
- e. In the Password field, type the password used to access the FTP site.
- f. Select the Filename conventions to use:

- No timestamp in file name: Name the file exactly as entered in the Filename field. A timestamp is recommended if you want to retain all versions of the report.
- Prepend timestamp to file name: Add the timestamp at the beginning of the filename entered in the Filename field
- Append timestamp to file name: Add the timestamp at the end of the filename entered in the Filename field.

Select File to save the report in a file on the PCM Server:

- a. In the Path field, type the complete path to the server location where you want to save the report.

The path is relative to the server (not to the Client). To save the report on the Client, there must be a path from the server to the Client. For example, use UNC paths, since the server runs as a service and cannot be set up easily to use mapped drives.
 - b. In the Filename field, type the filename you want to assign to the report. You can automatically add a timestamp to the filename in the File-name conventions pane.
 - c. Select the Filename conventions to use, as described above for FTP files.
10. Save the configuration of the Report action:
- Click **Apply** to save and leave the Policy Manager window open.
 - Click **Close** to save and close the window.

Types of Reports

This section describes the different types of reports that you can create in PCM by:

- Selecting a report type from the Reports menu and using the wizard to generate a report, as described in “Using the Report Wizard” on page 18-4.
- Using Policy Manager to generate a report as a policy action in response to an alert or at predefined times, as described in “Creating a Report Policy” on page 18-7.

When you generate a report as a policy action, the information to enter for the Properties, Type, Format, and Delivery tab options is described in the “Creating a Report Policy” section.

Asset Management Reports

From the Reports > Asset Management menu, you can generate the following reports:



Figure 18-10. Reports Menu: Asset Management

- **Inventory Report:** Lists each device in the selected group and provides pertinent information about each device. This report is especially useful when determining the operational status of devices. It provides information similar to that displayed on a Devices List, along with scheduling and report delivery capabilities.

Set the following criteria in the Inventory tab or window:

- Use the Group drop-down list to select the Agent and device group for which you want to print a report. Select All Devices to include all devices managed by all Agents.
- Use the Column drop-down list to select the report column that will be used to sort rows of data.

- **MED Device Inventory Report:** Lists each MED device in the selected device group with device-specific information, such as IP address, power requirements, VLAN ID, and QoS configuration for network traffic. For more information, see “Creating a MED Device Report” on page 9-11.

You can merge a MED Device Inventory report with MED data from a private branch exchange (PBX) to locate an IP phone by phone number. See “Importing MED Information” on page 9-8 for more information.

Device Access Control Reports

From the Reports > Device Access Control menu, you can generate the following reports using the Report Wizard:

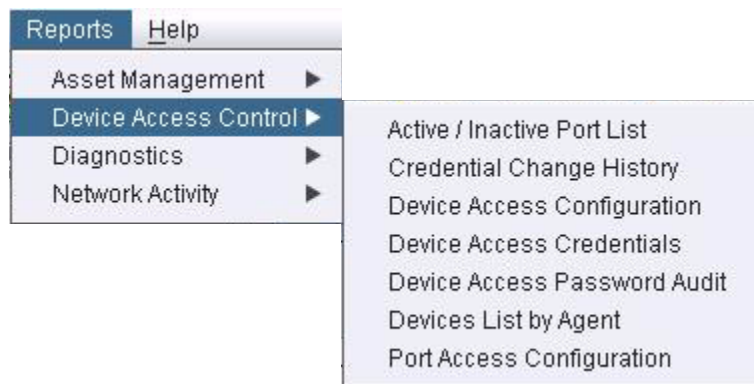


Figure 18-11. Reports Menu: Device Access Control

- **Active/Inactive Port List:** Provides port utilization statistics. This report consists of a color-coded bar graph showing the number of ports on each selected device that are currently active or inactive. Active ports are shown in blue, and inactive ports are shown in red.

Set the following criteria in the Active/Inactive Port List window:

- Use the Group drop-down list to select the Agent and device group for which you want to create the report. Select All Devices to include all devices managed by all Agents.
- Select the IP addresses of devices to include in the report, or select ALL to include all devices in the selected group. You can select multiple devices by using standard Windows conventions.
- To include inactive ports in the report, select Inactive Ports.
- To include active ports in the report, select Active Ports. You can display both Inactive Ports and Active Ports in the same report.

- **Credential Change History Report:** Identifies devices on which the access credentials have changed. This allows users to identify how recently credentials have changed and which devices have not had credential changes in a specified period of time. The access credentials include SNMP community names (read and write and SNMPv3 credentials if specified), and Telnet Manager and Operator usernames and passwords.

Set the following criteria in the Credential Change History tab or window:

- Use the Group drop-down list to select the Agent and device group for which you want to create the report. Select All Devices to include all devices managed by all Agents.
- Use the Column drop-down list to select the column used to sort entries in the report.
- To sort report data in ascending order based on the column you selected, select Ascending.
- To sort report data in descending order based on the column you selected, select Descending.

Set the following criteria in the Change Selection Criteria tab or window:

- Select Change to display devices with access credentials that have changed within the selected reporting period.
- Select No Change to display devices with access credentials that have NOT changed within the selected reporting period.
- Use the Period of time up or down arrows to select the number of days to include in the report (counting backwards from the current day).

- **Device Access Configuration Report:** Lists the security (authentication) configuration for device access on the selected devices. This report can be filtered by access type and authentication type.

Set the following criteria in the Device Access Configuration tab or window:

- Use the Group drop-down list to select the Agent and device group for which you want to create the report. Select All Devices to include all devices managed by all Agents.
- Use the Sort by drop-down list to select the column used to sort entries in the report.
- Check the access types (SSH, Console, Telnet) you want to report.
- Check the authentication types (Radius, TACACS, Local, None) you want to report.

For example, to report only device access configurations initiated from 3500 switches that are managed by the Western Agent and use RADIUS for authentication:

Group = Western:ProCurve 3500yl

Type of access = Console

Type of authentication = Radius

- **Device Access Credentials Report:** Lists the device access credentials for the selected devices. This includes SNMPv2 community names, SNMPv3 credentials, and Telnet Manager and Operator user names and passwords.

Set the following criteria in the Device Access Credentials tab or window:

- Use the Group drop-down list to select the Agent and device group for which you want to print a report. Select All Devices to include all devices managed by all Agents.
- Use the Column drop-down list to select the report column that will be used to sort rows of data.
- To sort credential changes in ascending order based on the column you chose, select Ascending.
- To sort credential changes in descending order based on the column you chose, select Descending.

- **Device Access Password Audit Report:** Identifies all devices in the selected group whose passwords do or do not comply with a specified set of rules governing the passwords.

Set the following criteria in the Device Access Password Audit tab or window:

- Use the Group drop-down list to select the Agent and device group for which you want to print a report. Select All Devices to include all devices managed by all Agents.
- Use the Column drop-down list to select the report column that will be used to sort rows of data.
- To sort report data in ascending order based on the column you selected, select Ascending.
- To sort report data in descending order based on the column you selected, select Descending.

Set the following criteria in the Password Policy tab or window:

- In the Minimum Length field, type the minimum length required for passwords (used to login to the network) to be included in the report. For example, selecting 6 means the report will include only passwords that contain at least 6 characters.

- In the Maximum Length field, type the maximum length required for passwords to be included in the report.
- To report passwords that contain a minimum number of special characters (lowercase, uppercase, numbers, spaces, or punctuation symbols), check the desired check box and type the minimum number to be reported. For example, to report all passwords that contain at least one space, check the Spaces check box and type 1 next to it.

Set the following criteria in the Fields to Verify tab or window:

- Check each password/credential check box that you want to verify.

■ **Devices List by Agent Report:** Identifies all devices in the selected group.

Set the following criteria in the Devices List by Agent tab or window:

- Use the Group drop-down list to select the Agent and device group for which you want to create the report. Select All Devices to include all devices managed by all Agents.

■ **Port Access Configuration Report:** Lists the security settings for all ports in all devices in the selected group and includes security configuration information for each port, similar to data available in the Port Access tab.

Set the following criteria in the Port Access Configuration tab or window:

- Use the Group drop-down list to select the device group for which you want to create the report. Select All Devices to include all devices managed by all Agents.
- Use the Column drop-down list to select the column used to sort entries in the report.
- To sort report data in ascending order based on the column you selected, select Ascending.
- To sort report data in descending order based on the column you selected, select Descending.

Diagnostics Reports

From the Reports > Diagnostics menu, you can generate the following reports using the Report Wizard:



Figure 18-12. Reports Menu: Diagnostics

- **Device Config Change History Report:** Identifies devices in the group with software, hardware, or ROM configurations that have changed during the specified period.

Set the following criteria in the Device Config Change tab or window:

- Use the Group drop-down list to select the Agent and device group for which you want to print a report. Select All Devices to include all devices managed by all Agents.
 - Select Changed to display devices with configurations that have changed within the selected reporting period.
 - Use the Period of time up or down arrows to select the number of days to include in the report (counting backwards from the current day) to display devices with software, hardware, or ROM configurations that have changed within the selected reporting period.
 - Use the Column drop-down list to select the report column that will be used to sort rows of data.
 - To sort credential changes in ascending order based on the column you chose, select Ascending.
 - To sort credential changes in descending order based on the column you chose, select Descending.
- **Device Config Change Totals Report:** Displays the number of devices in the selected device group whose software, hardware, or ROM configuration has changed during specified time periods.

In the Device Config Change Totals window, select the Agent and device group for which you want to print a report from the Group list. Select All Devices to include all devices managed by all Agents.

- **Device Uptime and Status Report:** Generates a summary view of device status and uptime for a group of devices over a specified time period. Uptime and status data is provided by periodic polling scheduled:
 - For a device group with the Discovery: Device Uptime and Status Polling action in Policy Manager (see “Configuring Policies” on page 16-4)
 - By the default Device Status Polling Interval set for an Agent in the Discovery > General tab in Agent Manager (see “Discovery” on page 3-23)

Page 1 of the Device Uptime and Status Report is a pie chart that shows the number of devices in Critical, Warning, and Good states based on the percentage of device uptime. You configure the time range used to gather uptime data and the color code for percentage thresholds with the Report Wizard.

Page 2 and later pages of the report fulfill SLA reporting requirements by displaying the time at which each device was discovered and the percentage of time that the device was operational (in-service since time). You configure the time range used to gather uptime data and the sorting criteria for the device listing with the Report Wizard.

Note: Statistics in the report are more accurate if you schedule device polling more often. You set the status polling interval when you configure the:

- Discovery: Device Uptime and Status Polling action for a policy in Policy Manager (see “Discovery” on page 3-23)
- Discovery preferences in Agent Manager (see “Discovery” on page 3-23)

By carefully scheduling status polling, you can generate a Device Uptime and Status report that contains data:

- Polled only from the devices, groups, or custom groups from which you want uptime data.
- Polled during operational hours, not during known off hours.
- Retained for up to one year or until the database reaches 500k. The database is trimmed periodically by removing state-change records (changing between UP and DOWN) that exceed the maximum number of records.

When you generate a Device Uptime and Status report:

- a. In the Device Uptime and Status window, select a device group and a reporting time period by specifying a:
 - From and To value in the Range tab
 - Number of minutes, hours, or days in the Since tab

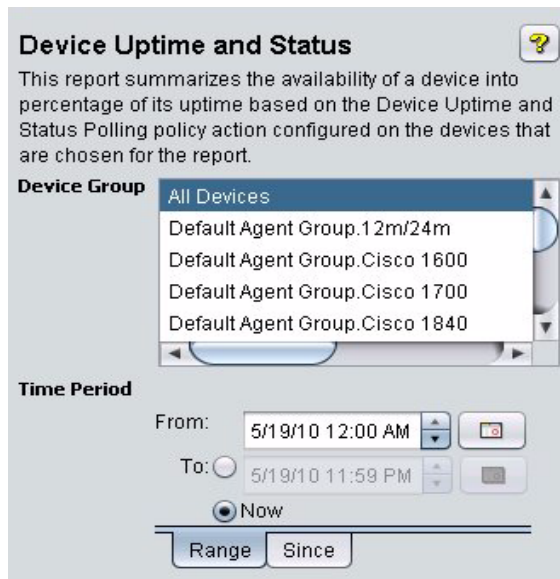


Figure 18-13. Device Uptime and Status Window

- b. In the Sorting and Color Code Settings window:
 - Specify how you want to sort the device uptime data on page 2 in the report; for example, by managing agent, percentage of device uptime, IP address, or the date from which a device is operational (in service).
 - Select the percentage of uptime that corresponds with the green and blue sections of the pie chart on page 1 of the report. The red section always represents a critical status for device uptime.

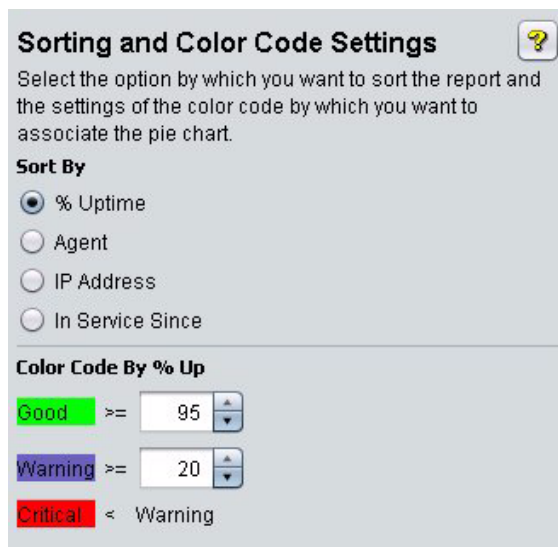


Figure 18-14. Sorting and Color Code Settings Window



Note

You can also generate a Device Uptime and Status report for a specified device by clicking the Reports button in the Device toolbar of an Interconnect Device window and selecting Uptime Report.

Network Activity Reports

From the Reports > Network Activity menu, you can generate the following reports using the Report Wizard. Network Activity reports are grouped into Policy Activity and Wireless reports.



Figure 18-15. Reports Menu: Network Activity

- **Configured Policies Report:** Identifies all policies configured in PCM, along with the devices where the policy action will be executed when triggered and policy parameters.

The Configured Policies Report has no selection criteria.

- **Event Activity Report:** Lists event occurrences on a group of devices over a specified time, based on events in the Event Manager. Events in this report can be filtered by event severity or content.

Set the following criteria in the Event Activity tab or window:

- Use the Group drop-down list to select the Agent and device group for which you want to print a report.
- Use the Time up or down arrows to select the number of minutes, hours, or days to include in the report (counting backwards).
- Use the Events that are up or down arrows to select the types of events to include in the report.
- Use the Column drop-down list to select the report column that will be used to sort rows of data.
- To sort events in ascending order based on the column you chose, select Ascending.
- To sort events in descending order based on the column you chose, select Descending.

- **Event Totals by Severity Report:** Displays the number of events at each severity level (critical, major, minor, and warning) that occurred on a device group or all network devices during a specified time period.

Only events from network devices are reported. Events from PCM core functions and plug-in modules (such as Mobility Manager and Network Immunity Manager) are not included in the totals.

You can group data in the report by source IP address or by specified time intervals.

- When displaying event totals by source IP address, the MAC address and agent managing each device is displayed for groupings of IP addresses.
- When displaying event totals by time intervals, a graphical chart and a list of event totals for each time interval is generated. You can optionally display informational events.

Note: The graphical chart is displayed only if there are event totals for more than one time interval.



Note

You can also generate an Event Totals by Severity report for a specified device by clicking the Reports button in the Device toolbar of an Interconnect Device window and selecting Event Totals by Severity.

- **Historical Event Aggregation Report:** Displays the number of events at each severity level that occurred on a device group or all network devices during a specified time (day, week, month, year).

Only events from network devices are reported. Events from PCM core functions and plug-in modules (such as Mobility Manager and Network Immunity Manager) are not included in the report.

The total number of critical, major, minor, warning, and information events are displayed in a graphical and tabular view for several time periods.

Note:

If PCM plug-in modules, such as PMM, IDM, and NIM, are installed, you can generate additional reports. For more information, go to <http://www.procurve.com/customercare/support/manuals/index.htm> and scroll down to Network Management to find links to documentation for:

HP ProCurve Identity Driven Manager

HP ProCurve Mobility Manager

HP ProCurve Network Immunity Manager

Using the Configurable Integration Platform

Introduction	19-2
Supporting Undiscovered Network Devices	19-3
Managing 3rd-Party Network Devices	19-8
Adding User-defined Devices	19-9
Discovering User-defined Devices	19-11
Adding Plug-in Applications	19-12
Adding User-defined Web Tabs	19-15
Decoding Third-Party Traps	19-17
Editing and Deleting CIP Definitions	19-21
Editing CIP Definitions	19-21
Deleting CIP Definitions	19-21
Troubleshooting CIP	19-22
Manually Creating CIP Files	19-23
Coding Conventions and Syntax	19-23
Supporting 3rd-Party Network Devices	19-24
Adding User-defined Devices	19-32
Adding User-defined Actions	19-36
Adding User-defined Triggers	19-38
Decoding Third-Party Traps	19-45
Troubleshooting Manual CIP Files	19-49

Introduction

You can customize PCM by using the Configurable Integration Platform (CIP) to:

- Define additional network devices and third-party devices not automatically discovered by PCM, so you can display and monitor the device in PCM,
- Receive SNMP traps from the user-defined devices and display related events in PCM,
- Launch the user interface for other Web-based applications from PCM.
- Customize PCM toolbars and menus to add links to additional management tools with a single click.

CIP consists of a multi-purpose wizard used to perform all CIP tasks and CIP application utilities used to add and edit applications. If you prefer to manually create CIP files instead of using the wizards, instructions are provided in “Manually Creating CIP Files” on page 19-23.

Supporting Undiscovered Network Devices

PCM's discovery engine will discover any device that supports MIB 2 and SNMP. The CIP Wizard can then be used to customize the appearance and basic behavior of these third-party switches.

Do not select Network Devices to add non-switch devices that wouldn't be discovered by the PCM discovery engine. Instead, use the User-defined device option to configure devices that are not switches (things like DNS, DHCP and RADIUS servers), as explained on page 19-9.

To add support for a non-ProCurve network (switch) device:



1. Open the CIP Wizard by clicking the CIP Wizard button in the Global toolbar.



Figure 19-1. CIP Wizard Welcome window

1. Click **Next** to select an option:

Using the Configurable Integration Platform Supporting Undiscovered Network Devices

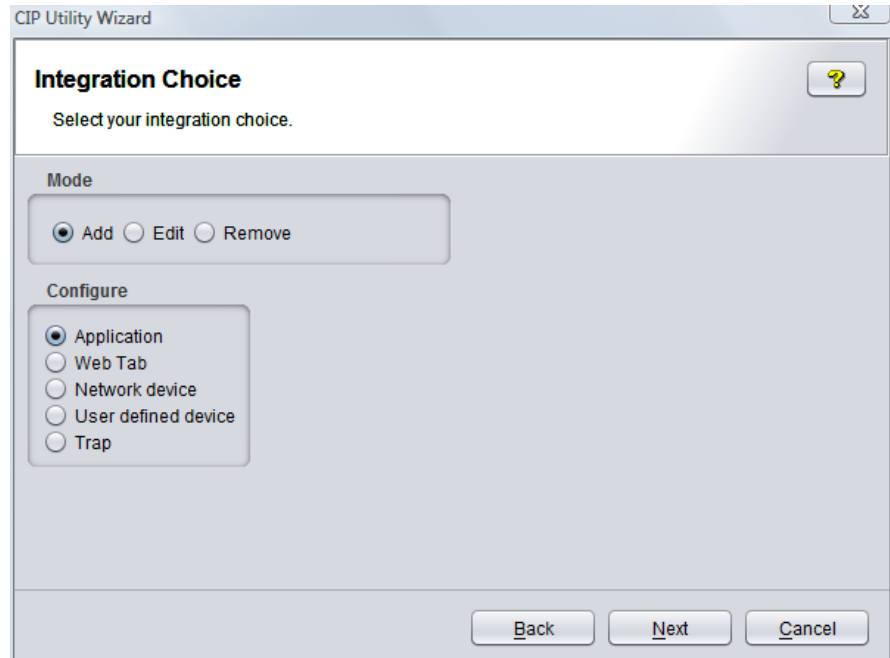


Figure 19-2. CIP Wizard, Integration Choice window

2. Select the Add, and then select Network Device.
3. Click **Next** to display the Device Information window.

The screenshot shows a window titled "CIP Utility Wizard" with a close button in the top right corner. The main heading is "Enter Device Information" with a help icon (question mark) to its right. Below the heading is a subtitle: "Provide the OID number and other properties of the device you want to integrate to PCM." The form contains five input fields: "SYSOID", "Model", "Vendor", "Product", and "Node". The "Node" field has a small text label to its right: "Create a node in PCM tree with this name." At the bottom of the window are three buttons: "Back", "Next", and "Cancel".

Figure 19-3. CIP Wizard, Enter Network Device Information

4. Enter the device properties:
 - a. In the SYSOID field, type the SNMP system object ID for the type of device you want PCM to discover. This can be found using the MIB browser to query for sysObjectID.
 - b. In the Model field, type the vendor's model number. The Model name cannot contain spaces, so replace any spaces with a hyphen or underscore.
 - c. In the Vendor field, type the name of the vendor who manufactures the device.
 - d. In the Product field, type a descriptive name to identify the device type.
 - e. In the Node field, type the name that will be used for the node (device class/group) that will be created in the navigation tree (e.g., Cisco). All devices with the specified class will be grouped under this node.
5. Click **Next** to display the Device Capabilities window:

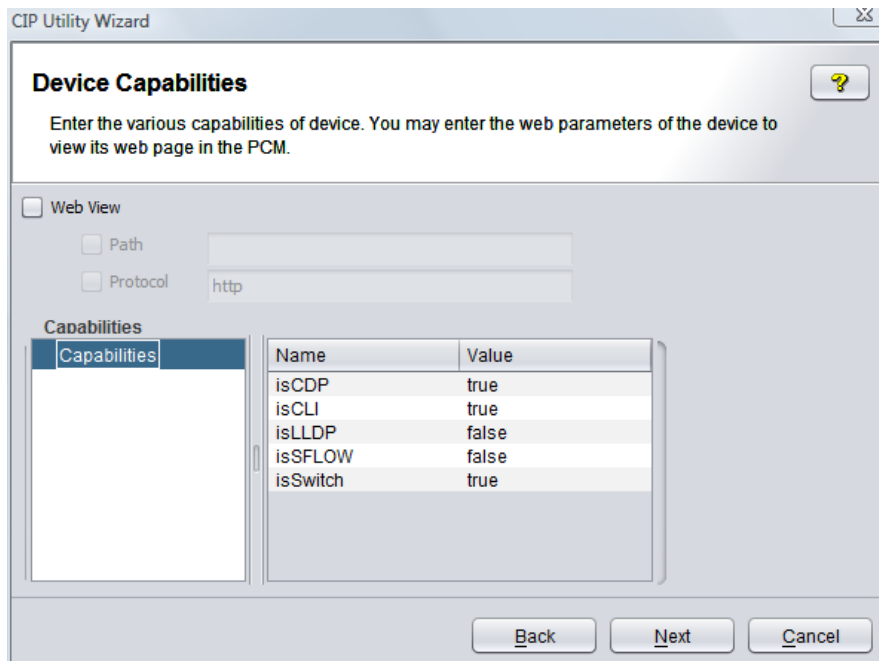


Figure 19-4. CIP Wizard, Network Device Capabilities window

6. If the Web view will be enabled for the device, check the Web View check box. This specifies whether the device supports a Web-based view that can be presented in PCM's Live View tab.
7. If Web View is selected and the Live View image of the device is not located in the default location `http://<device_IP_address>`, check the Path check box and enter the correct URL.

Some devices have the Live View buried deeper in the device's UI hierarchy. For example, the Live View for ProCurve devices can be found at: `http://<device_IP_address>/configuration/device_viewf.html`.

If your device requires a special path, set the path to the part of the URL following the IP address. For example:

```
/configuration/device_viewf.html
```

8. If Web View is selected and a protocol other than the default http protocol is needed to get the Live View image, check the Protocol check box and enter the correct protocol. For example, if the device supports only https, type https.

9. The Capabilities panel is used to change how device capabilities are configured in PCM. To enable a device capability, in the Capabilities panel double-click its value and type true. Or, to disable a device capability, double-click its value and type false. You can also add capabilities by right-clicking the capabilities (if the capability is a key with name value pairs) on the left, selecting Add Name, and adding the name value pair for the capability. In addition, the right-click menu provides capabilities to delete and edit keys and name value pairs.

Possible capabilities are:

- **isCLI**: Indicates if the device allows Telnet access. If set to true, PCM will enable a right-click action to launch a telnet session to the device.
- **isSwitch**: The device will not appear in the PCM device tree unless this is set to true. Any device that routes, forwards or bridges network traffic should have it set to true.
- **isLLDP**: Indicates if the device supports the Link Layer Discovery Protocol. If set to true, PCM will attempt to read LLDP information from the device, which allows PCM to discover the network topology of non-ProCurve devices much more quickly, and construct more accurate network maps.
- **isCDP**: Indicates if the device supports the Cisco Discovery Protocol. Works similarly to LLDP.
- **isSFLOW**: Indicates if the device supports sFlow, which is used by Traffic Monitor.

10. Click **Next** to display the Image Properties window:

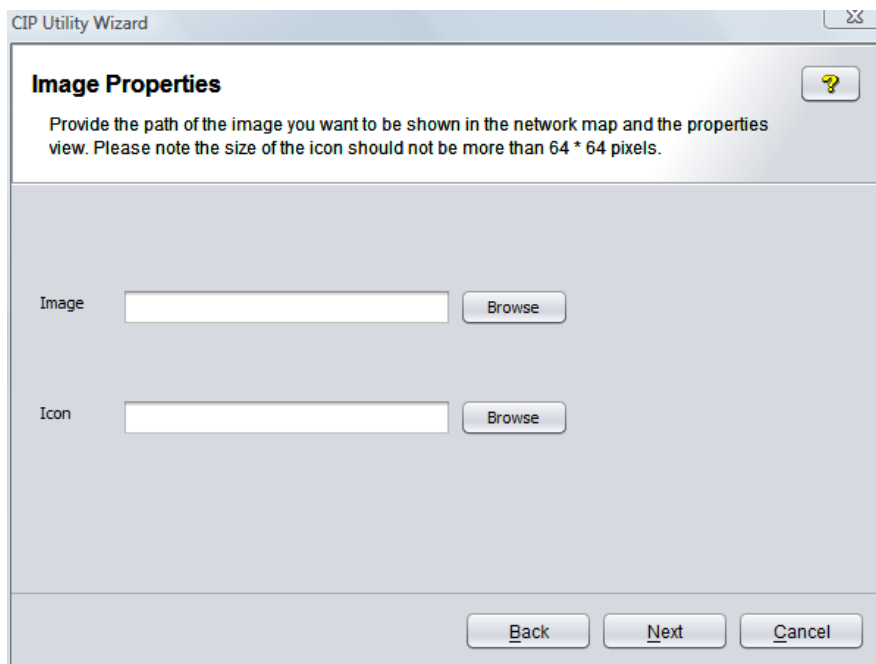


Figure 19-5. CIP Wizard, Image Properties window

11. Optionally, click the Image **Browse** button and select the graphic file you want to display as the larger image on the device properties tab when the device is selected in the PCM tree. The file must be a .jpg or .gif file.
12. Optionally, click the Icon **Browse** button and select the .jpg or .gif graphic file you want to use as the small image representing the device on the network map. It should be a small image, no larger than 64x64 pixels.
13. Click **Finish** to add the network device or device group.

Managing 3rd-Party Network Devices

PCM's discovery engine discovers any device that supports MIB 2 and SNMP. The CIP Wizard can then be used to customize the appearance and basic behavior of these third-party switches by allowing device configurations (including templates) to be collected (scanned) and deployed to third-party network devices.

If PCM discovers a third-party device but cannot obtain the subnet, subnet 255.255.255.255 is automatically assigned.

Adding User-defined Devices

User-defined devices are devices other than switches, such as printers or DNS, DHCP and RADIUS servers. Adding user-defined devices allows you to display the device information in the PCM display, and to receive traps from the specified devices and display them as events in the PCM event browser. These devices will always appear in the “User-defined devices” folder in PCM.

To add a user-defined device:



1. Open the CIP Wizard by clicking the CIP Wizard button in the Global toolbar. Click **Next** to select an option.
2. Select the Add radio button, and then select User defined device.
3. Click **Next** to display the Device Information window.

CIP Utility Wizard

User Defined Device Information

Provide the details of the user defined device like printer and radius server.

SYSOID

IP

Agent Address

Model

Vendor

Product

Class

Add more device properties

Figure 19-6. CIP Wizard, User-defined Device Information window

4. Enter the device properties:

Using the Configurable Integration Platform

Adding User-defined Devices

- a. In the SYSOID field, type the SNMP system object ID for the type of device you want PCM to discover. For user-defined devices, the SYSOID is the user friendly name.
 - b. In the IP field, type the IP address of the device.
 - c. Select the Agent to which the user-defined device must be contributed.
 - d. Optionally, in the Model field, type the vendor's model name or number. The Model cannot contain spaces, so replace any spaces with a hyphen or underscore.
 - e. Optionally, in the Vendor field, type the name of the vendor who manufactures the device.
 - f. In the Product field, type a descriptive name to identify the device type.
 - g. To define additional properties that will be shown on the device Properties tab, check the Add more device properties check box, which displays the Device Properties window.
5. Click **Next** to display the next window. If you checked the Add more properties check box, the Properties window is displayed.

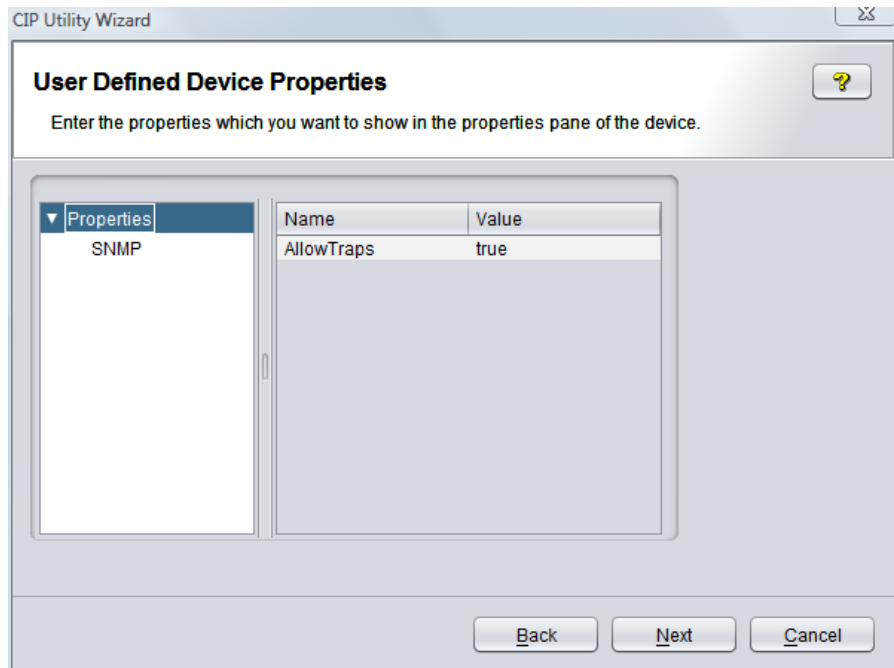


Figure 19-7. CIP Wizard, User-defined Device Properties window

6. The Properties window describes to PCM the device properties. Identify any other device information you want to display in the device Properties tab in PCM. You may include as many optional properties as you like. These will be displayed in the order listed. Note that this window is shown only when the Add more properties check box on the User-Defined Device Information window is checked.
 - a. In the left pane, click the Properties category to be changed.
 - b. To change the name of the property, in the Name column of the right pane, double-click the name to be changed (e.g., SysName, SysDescription, Contact, Location, etc.).
 - c. In the *Value* column, type the value to be displayed for the named property.
 - d. To add more properties, right-click the properties on the left, select Add Name, and enter the name value pair for the property. If the property is a key with name value pairs, select Add Key from the right-click menu. You can also delete and edit keys and name value pairs from the right-click menu.
 - e. Click **Next** to display the Image Properties window (shown in Figure 19-5).
7. Optionally, click the Image **Browse** button and select the graphic file you want to display as the larger image on the device Properties tab when the device is selected in the PCM tree. The file must be a .jpg or .gif file.
8. Optionally, click the Icon **Browse** button and select the .jpg or .gif graphic file you want to use as the small image representing the device on the network map. It should be a small image, no larger than 64x64 pixels.
9. Click **Next** to add the user-defined device.
10. When the final window appears, confirm the integration completed successfully and click **Finish**.

Discovering User-defined Devices



If you added user-defined devices, display the General subtab on the Agent Manager Discovery tab, and click the **Rescan for user defined devices!** button.

This launches a scan of the <PCM>/server/config/devconfig/extern directory for the files for user defined devices. If any new file is found, the related device is created in PCM, and the device will show up in the user-defined devices folder in the navigation tree.

Adding Plug-in Applications

Plug-in applications can be launched from PCM through a custom icon on the toolbar or a custom right-click menu action. These applications can be designated for specific devices or device groups.

To add a plug-in application using the CIP Wizard:



1. Open the CIP Wizard by clicking the CIP Wizard button in the Global toolbar.

Note:

Plug-in applications can also be added by right-clicking the device or group where you want to add the application, selecting CIP Applications Utility from the right-click menu, and then select **Add an application**. Once the Add an Application Wizard appears, click Next to display the Add an Application window.

2. In the Integration Choice window of the CIP Wizard, select Add, select Application, and then click **Next**.

The screenshot shows a window titled "CIP Utility Wizard" with a close button in the top right corner. The main title is "Add an Application" with a help icon (question mark) to its right. Below the title is a text box containing the instruction: "Select 'Add a new Application'. The list shows the applications added to PCM using Configurable Integration Platform Utility." There is a large empty rectangular box below this text. The form contains several fields: "Name of Application" with the text "Mib Browser"; "Type" with a dropdown menu set to "CLI"; "Command" with the text "am Files\Mib browser\mibbrowser.exe"; "Command Parameters" with a dropdown menu set to "NONE"; and "Target" with a dropdown menu set to "Client". At the bottom right, there are three buttons: "Back", "Next", and "Cancel".

Figure 19-8. CIP Wizard, Add an application window

3. Define the application:

- a. In the Name of Application field, type a unique name to identify the application in PCM.
- b. Use the Type drop-down list to select whether the application will be accessed using a **CLI** command, **Web** URL, or **PCM Policy**.
- c. Depending on the Type you selected, enter the following in the Command field.

CLI	CLI command, including its absolute path
Web	URL or IP address of the browser-based application. The application must support Internet Explorer
Policy	Name of PCM policy. The Policy must be defined in PCM before this option will work. Refer to "Configuring Policies" on page 16-4 for more information.

- d. Use the Command Parameters drop-down list to select variables for the command entry.

Note: If you entered **Policy** in the Command field, you must select **None** in the Command Parameters field because policies do not support parameters.

NONE	Execute the command without any parameters.
IP	Append the IP address of the device selected for operation to the command.
IP List	Append the IP addresses of all devices selected for operation to the command.
Group Name	Append the name of the group to the command.
OID	Append the OID of the selected device to the command.

4. In the Target field, select **Client** to add the application to the PCM Server and all its Clients, or select **Server** to add the application to the PCM Server only.
5. Click **Next** to display the Global Parameters window.

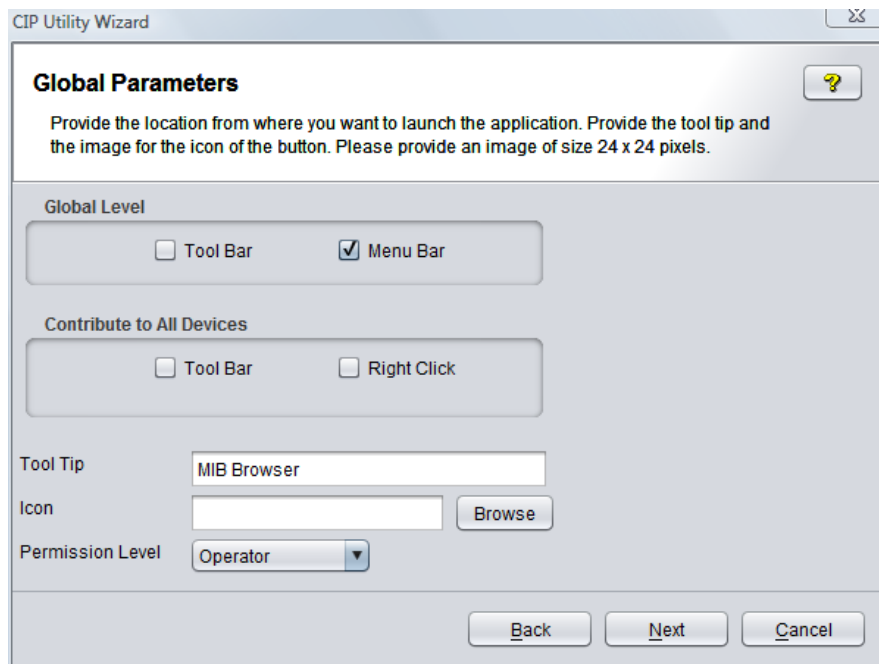


Figure 19-9. CIP Wizard, Global Parameters window

6. Define the parameters for the method used to trigger the application. Select any number and combination of methods:
 - a. To access the application by clicking a button on the global toolbar, check the Tool Bar check box in the Global Level pane.
 - b. To access the application by selecting it from the PCM menu bar, check the Menu Bar check box in the Global Level pane.
 - c. To access the application from a device or device group toolbar, check the Tool Bar check box in the Contribute to All Devices pane.
 - d. To access the application from the right-click menu for a device or device group, check the Right Click check box in the Contribute to All Devices pane.
 - e. If you checked Tool Bar and want to include a tool tip that appears when users hover the pointer over the button, type the text to be displayed.
 - f. If you checked Tool Bar, click the Icon **Browse** button and select the icon used for the toolbar button. The image must be in a .jpg or .gif file.
 - g. Click **Next** to add the application.
7. When the final window appears, confirm the integration completed successfully and click **Finish**.

Adding User-defined Web Tabs

User-defined tabs that link to a Web site can be added to any PCM group or device bank of tabs.

To add a tab:



1. Open the CIP Wizard by clicking the CIP Wizard button in the Global toolbar.
2. Click Next to display the Integration Choice window, as shown in figure 19-2.
3. Select Add, select Web Tab, and click **Next**.

CIP Utility Wizard

Web Parameters

Provide the name and the location of the tab along with the url of the web page you wish to monitor. Please ensure that the name of the node should match exactly the name on the tree.

Name of tab: ProCurve

Name of Node: Network Management Home

URL: http://www.procurve.com

Back Next Cancel

Figure 19-10. Web Tab Parameters window

4. In the Name of tab field, type the text you want to display on the tab. Remember to keep the text as brief as possible.
5. In the Name of Node field, type the name of the node where the Web tab will be added. Your entry must be typed exactly as shown in the navigation tree. For example, type Network Management Home to display the tab

Using the Configurable Integration Platform Adding User-defined Web Tabs

when the Network Management Home node is selected, or type ProCurve 2600 to include the tab on all device-related windows for ProCurve 2600 switches.

6. Type the URL of the Web site you want to display in the tab.
7. Click **Next** to create the tab.
8. Click **Finish** to close the wizard. You must restart PCM to display the tab. The following figure is an example of a tab added to PCM for the ProCurve Web site:

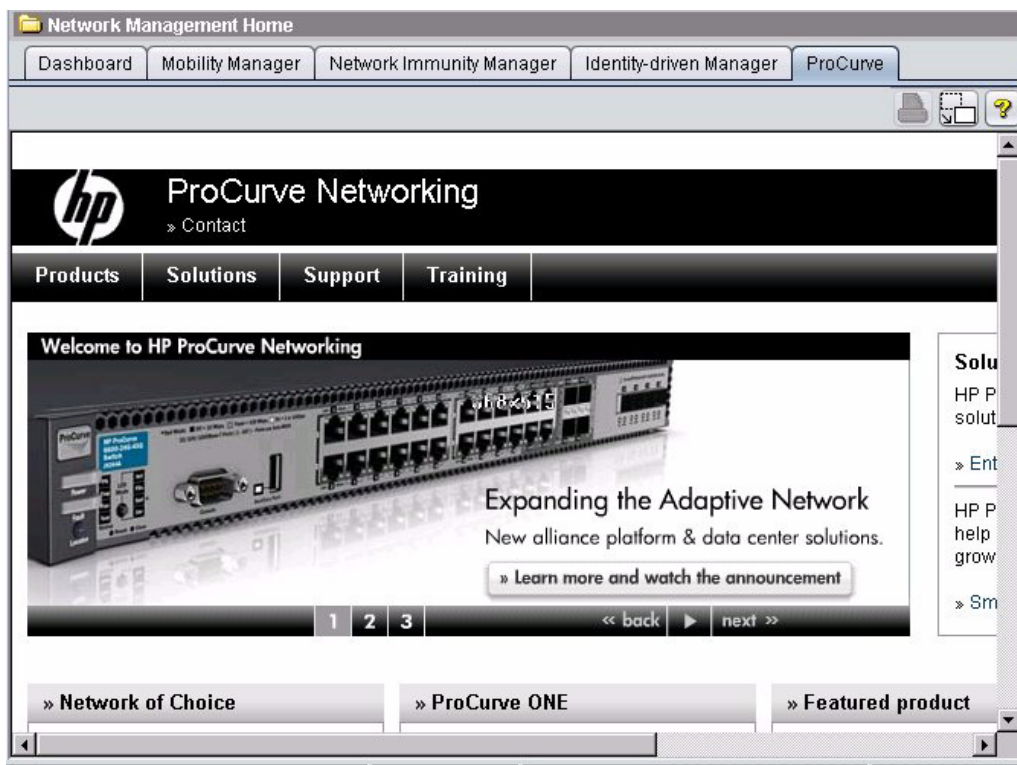


Figure 19-11. ProCurve Web tab added to Network Management Home

Decoding Third-Party Traps

The CIP feature in PCM also allows you to specify information on how to decode and display SNMP traps for non-ProCurve devices not otherwise supported by PCM. Once you have defined a trap, the PCM Event Manager server will process it in the same manner as traps sent from ProCurve managed devices.

To receive traps and log events to the PCM Event Browser for "User-defined" or non-ProCurve network devices, define the attributes needed by PCM to decode the trap:



1. Open the CIP Wizard by clicking the CIP Wizard button in the Global toolbar or selecting CIP Wizard from the Tools menu. Click **Next** to select an option.
2. Select the Add radio button, and then select Trap.
3. Click **Next** to display the Trap Details window.

CIP Utility Wizard

Trap Details

Provide the details of the trap you want to define. Select the severity level and the information you want to see in the event browser.

OID

Severity

Name

Text

Define Variables for the text to be displayed on the Event Browser

Figure 19-12. CIP Wizard, Trap Details window

Using the Configurable Integration Platform

Decoding Third-Party Traps

4. In the OID field, type the OID of the trap, with the "." delimiter replaced by the "_" delimiter. For example, a trap OID of 1.3.4.1.6.11 is entered as 1_3_4_1_6_11. Trap OIDs can be found in the device MIB.
5. Use the Severity drop-down list to select the severity of the event. Possible values are (shown in order of severity with Critical being most severe):
 - Informational
 - Warning
 - Minor
 - Major
 - Critical
6. In the Name field, type a descriptive name (string) used to identify the event in the PCM Events tab.
7. In the Text field, type the text that will be visible to the user from the Event Browser. This text can have place holders in it such as %VARIABLE_NAME_1, %VARIABLE_NAME_2, etc.
8. To include variables in the text shown in the Event Browser, check the Define variables for the text check box, click **Next**, and define the variables on the next window. The Variables window is shown only when Define Variables for the text to be displayed in event browser is selected on the Trap Details step.

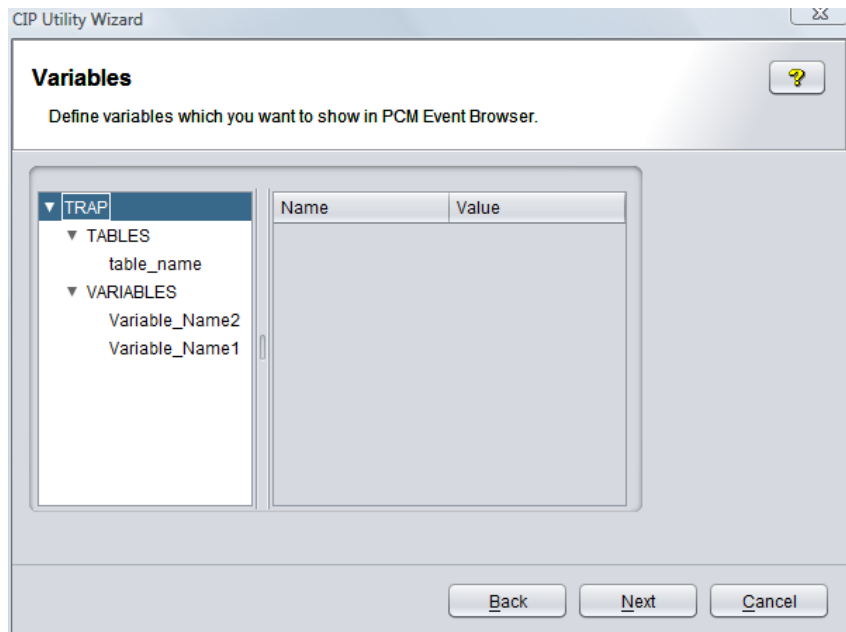


Figure 19-13. CIP Wizard, Trap Variables window

9. Select a variable name in the left pane of the Variables window and define the value for it in the Value column in the right pane.

The left pane lists "well known" variable names that PCM uses to extract data from traps after they have been processed and stored in the database. It is not mandatory that you define these names for processing third-party traps, but it is strongly recommended that you do to avoid problems and simplify troubleshooting if needed.

- **VARIABLE_NAME_X** - where X is the variable number, so for example if you have 3 variables they would be named VARIABLE_NAME_1, VARIABLE_NAME_2, VARIABLE_NAME_3. The VARIABLE_NAME key can specify where to find the value in two ways:
 - The first is just by simply defining the **INDEX** tag. The INDEX tag defines the index into the array of values encoded in the SNMP trap.
 - The second is by defining the INDEX tag and also defining the **TABLE_NAME** tag. The TABLE_NAME tag should be used when the value at the specified index needs to be translated to another value. PCM will retrieve the value at the specified index of the SNMP trap, and use it to find a matching property in the specified table. If such a matching property is found, then the value associated with that property is returned and substituted in the proper place in the BASE_TEXT string.
- **XXX_TABLE** - This is a list of name/value pairs used to translate values located at an index of the SNMP trap to another value. Well known variable names include:
 - END_NODE_IP_LIST – A list of one or more IP addresses that belong to one or more end-nodes. End-nodes are defined as a Server, Client machine, printer, etc.
 - END_NODE_MAC_LIST – A list of one or more MAC addresses that belong to one or more end-nodes. End-nodes are defined as a Server, Client machine, printer, etc.
 - PORT_LIST – A list of one or more ports
 - DEVICE_IP_LIST
 - DEVICE_MAC_LIST
 - RISING_THRESHOLD – The rising threshold that was exceeded
 - FALLING_THRESHOLD – The falling threshold that was violated
 - THRESHOLD_DELTA – The delta between the threshold and the value that was violated

Using the Configurable Integration Platform

Decoding Third-Party Traps

10. To add more variables, right-click the variables on the left, select **Add Name**, and enter the name value pair for the variable. If the variable is a key with name value pairs, select **Add Key** from the right-click menu. You can also delete or edit keys and name value pairs from the right-click menu.
11. Click **Next** to add the trap.
12. Click **Finish** to close the wizard. You must restart PCM to integrate the trap.

Editing and Deleting CIP Definitions

Once a CIP definition is added, it can be edited or deleted using the CIP Wizard.

Editing CIP Definitions

Use the CIP Wizard to edit all CIP definitions. You can also use the Edit an Application Wizard to edit a CIP application.

To edit a definition using the CIP Wizard:



1. Open the CIP Wizard by clicking the CIP Wizard button in the Global toolbar or selecting CIP Wizard from the Tools menu. Click **Next** to select an option.
2. Select the Edit radio button, and then select the type of configuration you want to change.
3. Click **Next** and select the definition you want to change.
4. Make the desired changes and click **Finish**.

To edit an application using the Edit an Application Wizard:

1. Right-click the device or group for which you want to edit an application.
2. Select CIP Applications Utility from the right-click menu, and then select **Edit an application**.
3. Once the Edit an Application Wizard appears, click Next to display the Edit an Application window.
4. Make the desired changes and click **Finish**.

Deleting CIP Definitions

1. Open the CIP Wizard by clicking the CIP Wizard button in the Global toolbar or selecting CIP Wizard from the Tools menu. Click **Next** to select an option.
2. Select the Remove radio button, and then select the type of configuration you want to delete.
3. Click **Next** and select the definition you want to delete.
4. Click **Finish**.

Troubleshooting CIP

If you are not getting the expected results, here are some things to check.

- Are you running the latest version of PCM? Some of the CIP features described here are not enabled unless you have the latest release of PCM with all the auto-update patches applied.
- Check the Events tab in PCM. If PCM encounters a CIP property file with bad syntax, it will create an event indicating the file that caused the problem. The severity level of the error will be "Warning". The source of the event will be `CoreServer (Config.Integration)`, and the detail message will read:
 - Syntax error parsing user-defined Trigger file (<filename>).
- Did you restart the PCM Client? Note that for adding support to decode new SNMP traps (events) and new network devices, the PCM Server must be restarted as well.

Manually Creating CIP Files

If you prefer, you can manually create CIP files instead of using the CIP Wizard. The CIP files are simple text files that follow a hierarchical key/subkey format with name/value pairs (known internally to PCM as "PropertyDB" files). The files (except the .oid files) must be placed in the <PCM>/server/config/devconfig/extern directory.

Coding Conventions and Syntax

The file definitions described in the following sections use the following conventions:

- Items inside angle brackets (< >) are required elements. Replace the item, including the angle brackets, with a string of your own.
- Values in angle brackets separated by a vertical bar, "|" means you must choose one of the specified options. For example "Enabled=<true | false>" means you must include either "true" or "false". If "true" the line of code will read: Enabled=true.
- Entries shown in square brackets ([]) are optional. If the item contains an ellipses (...) you may repeat the item.
- Angle brackets inside square brackets [blah = <>] indicate a required item within an optional element.
- Text between a slash and asterisk (/ * foo blah * /) are comment text offering further instructions on the items next to or below the comment.

Note:

Always create or edit CIP files using a simple text editor, such as Notepad. Do not edit these files with MS Word or another high-end word processor, because the file format created by such applications is not usable by PCM.

Supporting 3rd-Party Network Devices

Here are the steps you should follow to add support for a non-ProCurve network (switch) device:

1. Create a property file describing the device. A sample file is shown and described below these instructions.
2. Save the device property file (with a unique name ending in .oid) in the <installdir>\PNM\pcm-agent<server id>\config\devConfig directory on the Agent.
3. For third-party devices, save the device property file (with a unique name ending in .oid) in the <installdir>\PNM\pcm-agent<server id>\config\devConfig directory on the Agent AND in the <installdir>\PNM\server\config\devConfig directory on the PCM Server.
4. If you want an image associated with the device, create a .zip file containing the images (described below) for the device. If used, you must also copy this .zip file into the <installdir>\PNM\server\config\devConfig directory.
5. Restart the PCM services, and then use Manual Discovery to test that the new device type can be discovered by PCM.

The following device property file (Cis3500xl.oid) example could be used to add support for Cisco C3500xl devices.

```
Cisco3500xl {
  WebViewEnabled=true
  model=C3500xl
  class=Cisco
  product=C3500xl
  SYSOID=.1.3.6.1.4.1.9.1.248
  isCIP=true
  vendor=Cisco
  Capabilities {
    isCLI=true
    isSwitch=true
    isCDP=true
    isSFLOW=false
  }
  ImageInfo {
    jarname=ciscoimages.zip
    mapIcon=ciscoicon.jpg
    image=cisco3500.jpg
  }
}
```

Description of properties

- **WebViewEnabled:** Specifies whether the device supports a Web-based view that can be presented in PCM's "Live View" tab.

The default URL that PCM uses to get the "Live View" is: `http://<device_IP_address>`. Some devices have the "Live View" buried deeper in the device's UI hierarchy. For example the "Live View" for ProCurve devices can be found at: `http://<device_IP_address>/configuration/device_viewf.html`. If your device requires a special path, you can specify that path with the property "WebViewPath" (not shown in the file above). Set the WebViewPath to the part of the URL following the IP address. For example, the .oid file for ProCurve devices includes the property:

```
WebViewPath=/configuration/device_viewf.html
```

If a different protocol (other than http) is needed to get the live Web view, that can be specified with a property called "WebProtocol". For example, if the device in question only supports https, you would specify the following additional property: `WebProtocol=https`

- **model, vendor, and product:** These properties display in the "Device Properties" tab in PCM. Note that the Model name cannot contain spaces, use a hyphen or underscore if needed.
- **class:** This value is used to create a folder within the PCM tree by that name. All devices with the specified class will be grouped in that folder. In this example, all these devices will appear in a folder named "Cisco".
- **SYSOID:** You must specify the SNMP system object ID here. This can be found using the MIB browser to query for sysObjectID.
- **isCIP:** Indicates if the device has been added through CIP.
- **Capabilities:** The capabilities section of the file describes to PCM the properties that are necessary in order to enable some functionality. These properties are described below:
 - **isCLI:** Indicates if the device allows Telnet access. If set to true, PCM will enable a right-click action to launch a telnet session to the device.
 - **isSwitch:** The device will not appear in the PCM device tree unless this is set to true. Any device that routes, forwards or bridges network traffic should have it set to true.

- **isLLDP:** Indicates if the device supports the Link Layer Discovery Protocol. If set to true, PCM will attempt to read LLDP information from the device, which allows PCM to discover the network topology of non-ProCurve devices much more quickly, and construct more accurate network maps.
 - **isCDP:** Indicates if the device supports the Cisco Discovery Protocol. Works similarly to LLDP.
 - **isSFLOW:** Indicates if the device supports sFlow, which is used by Traffic Monitor.
- **ImageInfo:** This (optional) section specifies where PCM can find images it should display when the device is selected. The images for the device should be in a .zip or .jar file, and the "**jarname**" property must be set to the name of the .zip or .jar file containing the images.
- There are two images which you can specify for each device, the "**maplcon**" and the "**image**".

The "**maplcon**" specifies the name of the small image used to represent the device on the network map (it should be a small image, no larger than 64x64 pixels).

The "**image**" property specifies the name of the larger image that is displayed on the device properties tab when the device is selected in the PCM tree.

PCM supports only jpg and gif image formats.

The .zip file should be copied into the same directory as the .oid file, that is:

```
<installdir>\PNM\server\config\devConfig
```

If you are creating several .oid files in order to support several different types of devices, you may put all the images in the same .zip file and reference the same .zip file in each .oid file.

Operating Notes

The .oid files should be used to customize the appearance and properties of third-party "interconnect devices" (basically switches). PCM's discovery engine will discover any device that supports MIB 2 and SNMP. The .oid file can then be used to customize the appearance and basic behavior of these third-party switches.

The .oid files should not be used to add non-switch devices that wouldn't be discovered by the PCM discovery engine. The .udt and .udd files should be used for adding user-defined devices that are not switches (things like DNS, DHCP and RADIUS servers). These devices will always appear in the "User-defined devices" folder in PCM.

Managing 3rd-Party Network Devices

You can also use the PCM CIP to allow device configurations (including templates) to be collected (scanned) and deployed to 3rd-party network devices. This section describes how to configure PCM and the program/script that will allow PCM to capture and manage the device configuration of 3rd-party network devices like any other supported ProCurve device.

First, you must create a program or shell script to perform one or more of the several operations that the PCM configuration manager uses to perform its functions on devices, for instance, scanning a device.

When scanning a device, PCM configuration manager will perform the following operations:

- Get the device's software configuration,
- Get the device's hardware configuration,
- Get the device's software (OS) version number, and
- Get the device's ROM version number.

You may choose to implement one or all of these operations. The data for operations that are not implemented will simply be unavailable in PCM.

When you deploy a configuration or template to a device, you must perform two additional operations: install the configuration on the device and wait for the device to reboot. Note that a deployment action also uses the four scan operations (following the configuration deployment).

This custom written process in combination with the device property (.oid) file, allows you to associate configuration management actions with a set of non-ProCurve devices and the process/shell script that will perform those actions.

Two files are necessary:

- The .dvc file selects which devices the user-supplied executable will act on.
- The .pdt file configures the process to execute and the run string parameters to pass to it.

Using the Configurable Integration Platform Manually Creating CIP Files

You must store the .dvc and .pdt files in the following directories:

- <PCM_Install_Location>\pcm-agent\- <PCM_Install_Location>\server\config\devConfig\extern

Then you must restart the PCM Server in order for PCM to associate the configuration management operations with the set of devices indicated in the files.

When you initiate a configuration management action on a device, such as scanning for the device's configuration data that has a user supplied ".dvc" file associated with it, PCM schedules the user specified process and passes it information on what data to collect. The process is expected to collect the appropriate information (e.g. ROM version, OS version number, hardware configuration or software configuration) and return it on standard out. If an error occurs, the process may return any textual error message it wants logged to PCM's event log on standard error. In addition, the process must return a non-zero error code on exit for failure and a zero (0) return code on success. If the user is not interested in some parts of the data collected by the configuration manager, the ROM version number for instance, the process may return 0 on exit (success) and simply close standard out without returning any data.

The configuration manager ".dvc" template file appears as follows:

```
CfgMgr3rdPartyDevs {
  // OID of the device(s) - can use wild cards.
  ProductClass=1.3.6.1.4.1.11.2.3.7.11.8
  AppName=ConfigManagerServerComponent
  CacheTimeout=60000
  Image1{
    Version=1
    JarName=lib/devLib/Cm3rdPartyDevs.jar
    Classname=com.hp.nis.drivers.cfgmgr.3rdPartyDevs.Cm3rdPartyDevs
    // File specifying how to execute the process to perform the
    // configuration management actions.
    PrivDataName=config/devConfig/Cm3rdPartyDevs.pdt
    AlwaysReturnNewInstance=true
  }
}
```

Operating Notes:

PCM provides a template file named "CfgMgr3rdPartyDevs.dvc" in the <PCM_Install_Location>\server\config\devConfig\extern\templates\ directory. When customizing it for your devices, you may name the file anything you wish, but the file extension MUST be ".dvc". The "CfgMgr3rdPartyDevs" string at the beginning of the file should be modified to match the name chosen for the file. This file has two parameters you must customize.

- The ProductClass parameter specifies the OID values of the device(s) to which the user supplied program applies. The OID value may contain wild cards to select multiple devices.
- The PrivDataName parameter specifies the name of the file containing the parameters used to execute the user supplied process that performs the configuration management actions for the specified devices. The file name can be named anything you wish, but should have an extension of ".pdt". All other data in this file (.dvc) must not be changed in any way.

The other required file is the one specified in the PrivDataName parameter of the ".dvc" file. PCM provides a ".pdt" template file, Cm3rdPartyDevs.pdt, in the <PCM_Install_Location>\server\config\devConfig\extern\templates directory. The template file appears as follows:

```
Cm3rdPartyDevs {
  Version=1.0
  // The full file path to the shell script or process to execute that will
  // perform the required configuration management actions.
  TargetProcess=
  // Maximum time to allow the target process to complete tasks, in seconds.
  // The default value is 5 minutes. If the process does not return within
  // this time period, PCM will terminate it and display a timeout failure.
  MaximumTime=300
  // If the target process is a shell script, then this must contain the
  // full file path to the process used to execute the shell script file.
  ShellInterpreter=
  // The parameters to pass to the process or shell script being executed.
  // The first parameter is the operation being requested by the PCM
  //configuration management module. It will be one of the following values:
  //
  // 1 = Capture device software configuration data.
  // 2 = Capture device hardware configuration data.
  // 3 = Capture the device's OS (software) version number.
  // 4 = Capture the device's ROM version number.
  // 5 = Deploy configuration to device.
  // 6 = Wait for the device to reboot (if device requires a reboot after
```


Using the Configurable Integration Platform Manually Creating CIP Files

```
//      a configuration deployment).  
//  
// All text data in the RunString parameter immediately follows the  
// operation parameter exactly as entered with the exception of any  
// tokens that have the appropriate value substituted for the token.  
// The following tokens are supported:  
//  
// %optype- Will substitute the configuration manager operation type.  
// %ip    - Will substitute the IP address of the target device.  
// %oid   - Will substitute the OID value for the target device.  
// %wc    - Will substitute the write community name of the target device.  
// %rc    - Will substitute the read community name of the target device.  
// %mgmtuser- Will substitute the telnet management user name.  
// %mgmtpw- Will substitute the telnet management user password.  
// %opuser- Will substitute the telnet operator user name.  
// %oppw- Will substitute the telnet operator user password.  
// %cfgfile - Will substitute the base file name containing the device's  
// configuration data for a "deploy configuration to device"  
// operation (5). That file is always in the <PCM Install Dir>\pcm-  
// agent\data\download\ directory. All other operations return  
// an empty string for this token.  
//  
//An example runstring might be "RunString= <target process string as  
//specified above> %optype,%ip,%wc,%mgtpw". Note that the string to be  
//replaced begins with a space. If the user then issued a PCM  
//configuration management device scan for a device with IP address  
//192.168.0.5 and a write community name of "private" with a  
//telnet management password of "myCLIpw", the user process would  
//be launched via the ShellInterpreter using the following string to  
//capture the device's software configuration data:  
// " C:/configscan.sh 1,0,192.168.0.5,private,myCLIpw"  
//  
//The assumption is that the target process is C:/configscan.sh.  
//After %optype 1 for 'Capture device software configuration data',  
//the '0' indicates the execution status of the script.  
//  
RunString=  
}
```

In the Cm3rdPartyDevs.pdt template file, there are four parameters that must be customized by the user.

- The TargetProcess parameter must contain the full file path name of the process or shell script used to perform the configuration manager operations requested by PCM. PCM will schedule this process when it needs information about a device targeted by the associated ".dvc"

file. The process is expected to exit with a return code of 0 on success. If the process supports the requested operation, it must return the data on standard out.

- The `MaximumTime` parameter specifies the maximum time, in seconds, that PCM will allow for the user process or shell to carry out the requested configuration manager operations. The default is 300 seconds (5 minutes). If the process does not return an exit value to PCM within this time period, PCM terminates the process and logs a time-out failure.
- The `ShellInterpreter` parameter must only be customized when the `TargetProcess` parameter specifies a shell script to execute. It will be specific to the type of shell script (e.g. korn shell, C-shell, Windows XP shell, etc.). Enter the full path of the shell interpreter to use for the specified shell script. PCM always reads the shell script and passes it the shell interpreter on std in.

Note: PCM first checks if the file specified by "target process" is present or not. It then executes the process by invoking a runtime command execution of the string formed by appending "ShellInterpreter" and "RunString".

- The final parameter is the `RunString` to pass to the target process. The runstring contents may contain PCM tokens that will be replaced with values when the run string is passed to the process. For example, the `%ip` token is replaced by the target device's IP address. If the `"%optype"` token is not supplied, the first character of the run string after the target process is mentioned will contain a numeric value indicating the configuration management operation that is being requested. (See the comments in the `.pdt` template file for the operation types.)

The process is not required to support all of the possible operation types. The process may immediately close standard out and return an exit code of 0 for unsupported operation types. Alternatively, if you would like PCM to notify the user that this operation is not supported, an appropriate error message should be returned on standard error and the process exits with a non-zero return code.

When you finish editing the `Cm3rdPartyDevs.pdt` file, you must store it in the following directories, and then restart the PCM Server:

- `<PCM_Install_Location>\pcm-agent\<server id>\config\devconfig\extern`
- `<PCM_Install_Location>\server\config\devConfig\extern`

Adding User-defined Devices

To support discovery and monitoring of connection status for devices not natively supported in PCM, you need to provide:

- An entity or type definition (.udt file) that provides general information about the device or model type. The .udt file should be saved in the <install directory>\PNM\server\config\devConfig directory.
- A device definition (.udd file) that provides specific details for a given device. There can be multiple device definition files for a single entity definition.
- Display images associated that will be associated with the entity type, in .gif or .jpg format. All images for a device type must be placed in a .jar or .zip file in the "devConfig" directory (<install directory>\PNM\server\config\devConfig).

The .udt and .udd files are intended for adding user-defined devices that are not switches (things like printers, or DNS, DHCP and RADIUS servers). This will allow you to display the device information in the PCM display, and to receive traps from the specified devices and display them as events in PCM event browser. These devices will always appear in the "User-defined devices" folder in PCM.

Creating a User-Defined Type

You need to create a user-defined type file to provide PCM with a definition for the device type you want to support in PCM. This file provides the general characteristics associated with an entire group of devices. It is similar to the entity files used in PCM to define the Device Groups in the navigation tree.

Each user-defined entity file must have a file extension of .udt. The basic file definition is shown below:

```
<typename> {
  product=<model number>
  model=<model name>
  class=<family name>
  SYSOID=<sys object id>
  vendor=<vendor name>
  isCIP=true
  ImageInfo {
    jarname=<jar name> //or zip name
    image=<large image name>
    mapIcon=<map icon>
  }
}
```

Notes:

<typename> must be a unique string identifying the type of device. We suggest a naming convention that will minimize the likelihood of collisions with other user-defined entity types.

SYSOID need not be a real sys object ID, but it must be a string that uniquely identifies this type of device. This ID will be referenced in the device definition (.udd) file.

ImageInfo defines the images associated with the entity type in the PCM display.

- image (large image) is the device image that will be displayed in the lower portion of the Device Properties tab in PCM.
- mapIcon is the image that will be displayed for devices of this type in the PCM network maps.

If images are not supplied, a default map icon will be provided on the network map (if mapped), however there will be no device image in the properties tab view.

An example of the User-defined entity follows. The filename is **MySwitch.udt**

```
RADIUS-Server {
  product=rxServer
  model=rx6600
  class=Server
  SYSOID=RADIUS-1
  vendor=HP
  isCIP=true
  ImageInfo {
    jarname=baseImages.jar
    image=R-Server.jpg
    mapIcon=RADIUS-1.gif
  }
}
```

Creating a User-defined Device Definition

Once you have defined the type of device(s) you want to add to PCM, you need to provide a definition for the individual device that you want to add to PCM. This is where the characteristics of the specific device are defined. When the file is first scanned, a "user Defined Device" model object is created and stored in the PCM database. Properties of the device are obtained from this file.

Each user-defined device file must have an extension of .udd. The basic file definition is shown below:

```
<deviceUniqueID> {  
//SYSOID is same as in the entity definition(.udt)file  
  SYSOID=<sys object id or other device type identifier>  
  IP=<ip address>  
  Asset=<asset tag>  
  Location=<location tag>  
  Contact=<contact or owner>  
  SerialNo=<serial number>  
  SysDesc=<sysdescriptor>  
  SysName=<sysname>  
  Mac=<MAC address>  
  Agent=<Agent Number>  
  ProfileMask=<profile mask>  
  AllowTraps=<true|false>  
  SNMP {  
    Read=<SNMP read community name>  
  }  
  <OptionalProperty>=<property value>  
}
```

Notes:

`OptionalProperty` is a string for any other device information you want to display in the device Properties tab in PCM. You may include as many optional properties as you like. These will be displayed in the properties tab view in the order given in the .udd file.

User-Defined Device Example

An example of the User-defined device follows. This would work in conjunction with the .udt file example given on page 12-5.

```
RADIUS-01 {  
    IP=180.44.184.32  
    Agent=1  
    ProfileMast=7L  
    isCIP=true  
    Asset=A121  
    DBID=14595707  
    Model=3550  
    Contact=Ben  
    Manufacturer=HP  
    Location=NTC Lab  
    AllowTraps=true  
    SerialNo=J437208  
    SysDesc=rxServer  
    SYSOID=RADIUS-1  
    SNMP {  
        Read=public  
    }  
}
```

Discovering User Defined Devices

If you have added user-defined devices, use the Discovery tab in the Agent Manager [Preferences->Discovery] and click the **Rescan for user defined devices!** button.

This launches a scan of the <PCM>/server/config/devconfig/extern directory for the files for user defined devices. If any new file is found, the related device is created in PCM, and the device will show up in the user-defined devices folder in the navigation tree.

Adding User-defined Actions

To launch other applications from within PCM, or to create a custom Policy in PCM, create an action (.uda) file and place it in the "extern" directory.

Actions can be used to:

- Run the specified command or custom script on the target.
- Launch a WEB browser and go to the specified URL, or open the WEB Agent for the selected device(s) on the PCM Client.
- Run the specified policy from the PCM Server.

User-defined actions linked to a user-defined trigger allow you to create custom toolbar and menu actions in PCM. The policy option can also be used along with alerts to automatically run the policy when the event that causes the alert occurs.

The basic .uda (action) file definition is shown below:

```
<actionID> {  
    Name=<name>  
    Type=<CLI | WEB | POLICY>  
    Command=<commandline | url | policyname>  
    Target=<Server | Client>  
}
```

Notes:

For Type=CLI, enter the full pathname of the .exe file you want to run.

For Type=WEB, the ExecTarget must be Client. Do not use the Server as the target.

For Type=Policy, enter the name of the Policy. The Policy must be defined in PCM before this option will work. Refer to "Configuring Policies" on page 16-4 for more information. The Target must be Server when using the Policy action type. Do not use Client as the target.

The <commandline> and <url> values may contain the following tokens which will be substituted for the appropriate values when the action is run:

- %ip
This will be substituted with an IP address of the device the action was triggered from.
- %ipl
This will be substituted with a list of IP addresses representing the set of devices the action was triggered from (via multiple selection).

- %gn
This will be substituted with the name of the group the action was triggered from.
- %oid
This will be substituted with the OID of the device the action was triggered from.

A User-defined trigger for the action must be created to use any of these options. This allows you to select a device, devices, or group in PCM, and then use the trigger to run the action.

User-Defined Action Examples

The following .uda file example, for Type=WEB, would launch a browser to Google from the PCM Client.

```
Google {  
    Name=Launch Google  
    Type=WEB  
    Command=www.google.com  
    Target=Client  
}
```

The following .uda file example, for Type=POLICY, will run "MyPolicy" on the PCM Server when triggered.

```
Policy01 {  
    Name=MyPolicy  
    Type=POLICY  
    Command=MyPolicy  
    Target=Server  
}
```

For the example above, you must also create a Policy (MyPolicy) in PCM. Refer to Chapter 16, "Using Policy Manager Features" for details on creating policies.

The following .uda file example, for Type=CLI, will run the mibrowser.exe script to launch a MIB Browser window on the PCM Client (PC).

```
MibBrowser {  
    Name=MIB Browser  
    Type=CLI  
    Command=C:\Program Files\HP\ProCurve MIB Browser\  
    bin\mibrowser.exe %ip  
    Target=Client  
}
```


Note the %ip at the end of the command line. When the command is activated, the IP address for the currently selected device will be substituted here.

Adding User-defined Triggers

To launch user-defined actions or to customize the PCM menus and toolbars, you need to create a User-defined trigger file. A "trigger" is simply a menu item or toolbar button that launches an action. The user-defined trigger (.trg) file specifies:

- whether the trigger item will appear in the PCM global toolbar or Tools menu, or in the device (tab) specific toolbars and right-click menu,
- the Action it will deploy, and
- the Permissions required to use the trigger.

Creating a User-Defined Trigger

There are three types of triggers possible in the PCM display, specified by the `Scope=` parameter in your ".trg" file:

Global - Triggers that appear in the global Tools menu in PCM, or on the global toolbar.

Context - Triggers that appear in contextual (device specific or tab views) toolbars or in the right-click menu.

The trigger definition will vary based on the Scope. The parameters you need to specify are governed by the level and type of trigger. The Notes following the file format describe the rules and parameters for the various trigger definitions.

Each user-defined trigger file must have an extension of .trg. The .trg file must be stored in the "extern" directory on the PCM Server. The basic user-defined trigger (.trg) file definition is shown below:

```
<uitriggerID> {
Scope=<Global | Context>
Type=<MENU | RIGHTCLICK | TOOLBAR>
Name=<name>
ImageInfo {
    jarname=<jar name> //or zip name
    Icon=<image name>
Global { //Define If Scope==GLOBAL
    MenuPath=<menupath>
    ToolGroup=<groupname>
}
Context { //Define If Scope==Context
```

```
Device { // Trigger used for individual device tabs or nav
        objects)
    Type=<OID|IP>
    Value=<sysoid|ip>
}
GroupTab {
    Selection=<n>
    //0=Always on, 1..9=Exact selection count,
    1000=Allow arbitrary multiple selection
    GroupName=<name>
}
}
ActionID=<actionID>
Permission=<PER_ADMIN_x |PER_OPERATOR_x |PER_VIEWER_x>
}
```

Operating Notes:

For all triggers you must specify the following parameters:

Type=MENU | RIGHTCLICK | TOOLBAR

- If Scope=Global, use the MENU option to add an entry in the PCM global Tools menu. Use the TOOLBAR option to create a Global toolbar button. The RIGHTCLICK option is not valid for the Global scope.
- If Scope=Context, use the RIGHTCLICK option to add an entry in the PCM right-click menu. Use the TOOLBAR option to create a toolbar button in the tab views. The MENU option is not valid for the Context scope.

Name=<name>

Enter a string for the name that will appear in the Menu (either Tools or right-click), or on the default Toolbar icon if no icon image is supplied.

jarname=<file.jar | file.zip>

icon=<imagename>

For Type=TOOLBAR triggers you can provide an .jpg or .gif image for the toolbar icon. The image file must be placed in a .jar or .zip file, and you must supply the filename (.zip or .jar) and the icon image name must be specified. If an image is not supplied, a default image will be used.

Tooltip=<tooltip text>

This is an optional parameter. Use it to provide explanatory text that will be displayed when the user hovers over the toolbar icon.

ActionID=<actionID>

This parameter specifies the action the trigger will deploy. Use the same actionID as specified in the .uda file.

Permissions=<PER_ADMIN|PER_OPERATOR|PER_VIEWER>

This parameter specifies the permissions required to use the trigger. The parameter must be one of the following:

- PER_ADMIN_1 or PER_ADMIN_2
use one of these options to make the trigger available to users with an Administrator profile.
- PER_OPERATOR_1 or PER_OPERATOR_2
use one of these options to make the trigger available to users with Operator or Administrator profiles.
- PER_VIEWER_1 or PER_VIEWER_2
use one of these options to make the trigger available to users with Viewer, Operator, or Administrator profiles.

If you set the Scope=Global, then you must define the Global parameters, and the Action and Permission parameters. Do not use the parameters in the Context section of the file.

SubMenu=<subname>

This parameter is optional. Use it if you want a Global-Menu trigger to appear in a sub-menu, off of the global Tools menu.

For example, if you set Name=Custom, and SubMenu=myAction1 the Tools menu will show Custom, and a submenu item of MyAction1. You could then create a second Global-Menu trigger, with Name=Custom and SubMenu=MyAction2.

ToolGroup=<groupname>

This parameter is optional. Use it if you are creating multiple toolbar triggers and want to group them together. The default placement of user-defined triggers is to the right of the existing global toolbar buttons.

If you set the Scope=Context, then you must define the Context parameters. Do not use the parameters in the Global section of the file.

When you set Scope=Context and Type=TOOLBAR, you must specify either:

Device parameters—used for triggers added to the Interconnect Device view tabs, or

GroupTab parameters—used for triggers added to the Device Group view tabs.

When you set Scope=Context and Type=RIGHTCLICK, you must specify the Device parameters. The GroupTab parameters will not work with right-click menu triggers.

For Device parameters, specify the Type and Value, where:

```
Type=<OID|IP>  
Value=<sysoidlip>
```

Use `OID` to define a trigger that works with devices of that type. When you set the `Type=OID`, then you must supply the System OID (`sysoid`) in the `Value` parameter. For example, `Value=1.3.6.4.11.2.37.11.35`. To create a trigger for User-defined devices, use the `Sysoid` you specified in the `.udt` file.

Use `IP` to define a trigger that works for a specific device. When you set the `Type=IP`, then you must supply the device IP address in the `Value` parameter. For example, `Value= 16.29.12.110`

For `GroupTab` parameters, specify the `Selection` and `GroupName`, where:

`Selection=<n>` configures when the trigger is activated, it can be one of the following

- `Selection=0` will configure the trigger as on at all times.
- `Selection=<1..9>` will configure the trigger to be active only when the specified number of devices are selected in the device list of the group tab. Only one digit can be specified, this is not given as a range, i.e., `Selection=1`, or `Selection=2`, etc.
- `Selection=1000` will configure the trigger to be activated when any number of devices are selected in the device list of the group tab.

`GroupName=<name>` where the name is the same as the device group labels found in the PCM navigation tree, e.g., `GroupName=2800`

For `Web Tab` parameters, specify the `TabName` and `NodeName`

User-Defined Trigger Examples

The following example creates an entry (`Notepad`) in the `Tools` menu, with a sub-menu trigger (`Dans Custom`) that launches the "`MibBrowser`" action.

```
GlobalMenu01 {  
    Scope=Global  
    Type=MENU  
    Name=Notepad  
    Global {  
        SubMenu=Dans Custom  
        ToolGroup=UserTools  
    }  
    ActionID=MibBrowser  
    Permission=PER_OPERATOR_1  
}
```

The following .trg file creates a Global toolbar icon to launch the MibBrowser.

```
GlobalNp01 {
  Scope=Global
  Type=TOOLBAR
  Name=Notepad
  Global {
    ToolGroup=UserTools
  }
  Tooltip=Launch MIB Browser
  Icon=trigger.gif
  Jarname=triggers.jar
  ActionID=MibBrowser
  Permission=PER_ADMIN_1
}
```

The following two examples create triggers to launch the WEB Agent for a device, in the right-click menu and device Toolbar, respectively.

```
//rightclick webagent trigger
RgtNp02 {
  Scope=Context
  Type=RIGHTCLICK
  Name=Custom WebAgent
  Context {
    Device {
      DevType=IP
      Value=15.255.120.253
    }
  }
  ActionID=Web02
  Permission=PER_OPERATOR_1
  Tooltip=Operator
  Icon=trigger.gif
  Jarname=triggers.jar
}

-----
//device toolbar webagent trigger
TbNp04 {
  Scope=Context
  Type=TOOLBAR
  Name=Custom WebAgent
  Context {
    Device {
      DevType=OID
      Value=.1.3.6.1.4.1.11.2.3.7.11.34
    }
  }
}
```

```
ActionID=Web02  
Permission=PER_OPERATOR_1  
Tooltip=Operator  
Icon=trigger.gif  
Jarname=triggers.jar  
}
```

Using CIP to Plug-in Other WEB-based Applications to PCM

You can plug in the user interface for other Web-based applications into the PCM user interface to give you a single integrated pane of management. Simply create a trigger file with the Scope set the "Web Tab" whose contents will be the application of your choice (as long as that user interface is a Web-based user interface supported by Internet Explorer).

Creating the interface for other Web-based applications is done in three steps, as described in the details and examples given below:

1. Create a property file (.trg) that specifies the attributes of the application. The format of the file is shown in the example below:

```
AirWaveTab {  
    Scope=WebTab  
    TabName=AirWave  
    NodeName=Network Management Home  
    URL=https://10.3.4.147  
}
```

Operating Notes:

- The file can be named anything you want, but it must have the ".trg" extension. For the above example it might be `airwave.trg`.
- The **Scope** property must be set to "WebTab". That specifies that a custom tab should be created for the new application.
- The **TabName** property can be set to any value you like. Whatever you put there will appear as the name of the tab in PCM. In this case we chose to call it "AirWave".
- The **NodeName** property specifies the name of the node in the PCM navigation tree that will be associated with the tab. In the example above, you will see that the "Network Management Home" node in the tree is specified. The tab created for the AirWave application will only appear when that node is selected. You may specify the name of any node in the PCM tree, including the names of Custom Groups, which can be quite useful for plugging in applications for specific groups of devices.

Using the Configurable Integration Platform Manually Creating CIP Files

- Finally, the **URL** property must specify a Web address/path to the Server of the application. In this case the URL needed to launch the AirWave Management Platform is `https://10.3.4.147`.
2. Save the text property (.trg) file on the PCM Server, in the `<installdirectory>\PNM\server\config\devconfig\extern` directory
 3. Restart your PCM Client (no need to restart the Server).

Be sure to create and save the file with a text editor such as Notepad. Do not create the file with MS Word or another high-end word processor.

If the tab doesn't appear check the syntax of the file carefully to ensure it matches the format shown in the example, and check that it was copied into the correct location on the PCM Server.

For example, to call the ProCurve Web site directly into PCM as a tab associated with the root node of the tree, you would create the following ".trg" file in the `<installdir>\PNM\server\config\devconfig` directory:

```
ProCurveTab {  
    Scope=WebTab  
    TabName=ProCurve  
    NodeName=Network Management Home  
    URL=http://www.procurve.com  
}
```

The following figure is an example of a Web Tab for ProCurve Web site added to PCM:

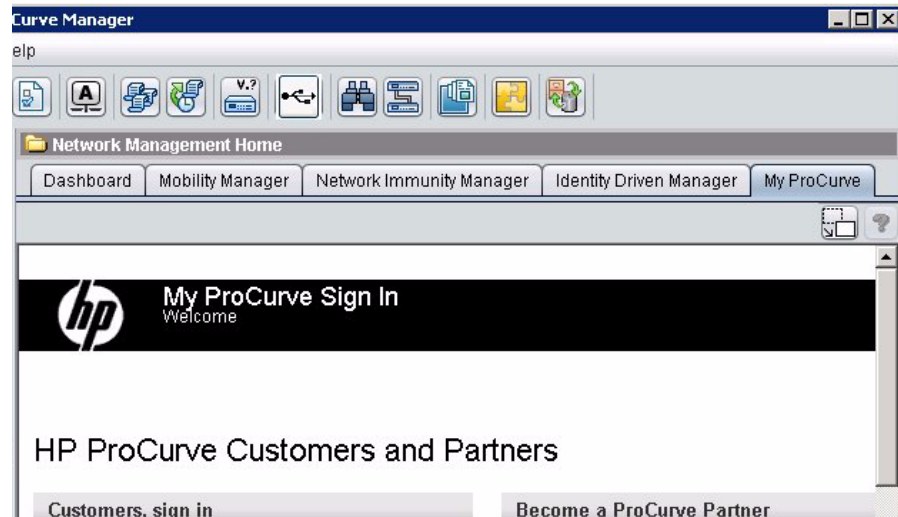


Figure 19-14. CIP Web Tab Example

Decoding Third-Party Traps

The CIP feature in PCM also allows you to specify information on how to decode and display SNMP traps for non-ProCurve devices not otherwise supported by PCM. Once you have defined a trap, the PCM Event Manager server will process it in the same manner as traps sent from ProCurve managed devices.

In order to receive traps and log events to the PCM Event Browser for "User-defined" or non-ProCurve network devices, you create a trap configuration file (.trp) file that defines the attributes needed by PCM to decode the trap. The .trp file must be placed in the <PCM>/server/config/TrapEventConfig directory and on the Agent in the <install directory>\PNM\pcm-agent\<<Server ID>\config\TrapEventConfig directory.

The .trp property file should contain the following attributes:

- Root node of the trap. This is the OID of the trap, with the "." delimiter replaced by the "_" delimiter. For example, a trap OID of 1.3.4.1.6.11 is defined in the .trp file as 1_3_4_1_6_11. Trap OIDs can be found in the device MIB.
- **SEVERITY** - The severity of the event. Possible values are:
 - Informational
 - Warning
 - Minor
 - Major
 - Critical
- **FRIENDLY_NAME** - This is a descriptive name (string) used to identify the event in the PCM Event Browser.
- **BASE_TEXT** - This is the text that will be visible to the user from the Event Browser. This text can have place holders in it such as %VARIABLE_NAME_1, %VARIABLE_NAME_2, etc. If the BASE_TEXT key entry is not included in the definition file, a "toString" will be done on the trap PDU (Protocol Data Unit, or packet). There are "well known" variable names that PCM uses to extract data from traps after they have been processed and stored in the database. See below for more information on "well known" variable names.
- **VARIABLE_NAME_X** - where X is the variable number, so for example if you have 3 variables they would be named VARIABLE_NAME_1, VARIABLE_NAME_2, VARIABLE_NAME_3. The VARIABLE_NAME key can specify where to find the value in two ways...
 - The first is just by simply defining the **INDEX** tag. The INDEX tag defines the index into the array of values encoded in the SNMP trap.

- The second is by defining the INDEX tag and also defining the **TABLE_NAME** tag. The TABLE_NAME tag should be used when the value at the specified index needs to be translated to another value. PCM will retrieve the value at the specified index of the SNMP trap, and use it to find a matching property in the specified table. If such a matching property is found, then the value associated with that property is returned and substituted in the proper place in the BASE_TEXT string.
- **XXX_TABLE** - This is a list of name/value pairs used to translate values located at an index of the SNMP trap to another value.

The basic user-defined trap (.trp) file definition is shown below.

```
1_3_1_4_6_1_11 {
    SEVERITY=<Critical|Major|Minor|Warning|Informational>
    FRIENDLY_NAME=<name>
    BASE_TEXT=<event string> //may include VARIABLES

    VARIABLES{ //optional, defines variables in base_text.
        Variable_name {
            INDEX=0
        }
        Variable_name {
            INDEX=1
        }
        Variable_name {
            INDEX=2
            TABLE_NAME=<table_name>
        }
    }
    TABLES { //optional, defines tables for variable index.
        table_name {
            1=value_a //a string for the translation value.
            2=value_b
            3=value_c
        }
    }
}
```

Well Known Variables

PCM uses several "well known" or common variables to extract information from traps. It is not mandatory to define these names for processing third-party traps, but it is strongly recommended that you do to avoid problems and simplify troubleshooting if needed. These well known variable names include:

- END_NODE_IP_LIST – A list of one or more IP addresses that belong to one or more end-nodes. End-nodes are defined as a Server, Client machine, printer, etc.
- END_NODE_MAC_LIST – A list of one or more MAC addresses that belong to one or more end-nodes. End-nodes are defined as a Server, Client machine, printer, etc.
- PORT_LIST – A list of one or more ports
- DEVICE_IP_LIST
- DEVICE_MAC_LIST
- RISING_THRESHOLD – The rising threshold that was exceeded
- FALLING_THRESHOLD – The falling threshold that was violated
- THRESHOLD_DELTA – The delta between the threshold and the value that was violated

Trap Decoder Examples

The following .trp file example is for a simple trap file with no variables.

```
1_3_1_4_6_1_11{  
    SEVERITY=Informational  
    FRIENDLY_NAME=IDS initialization trap  
    BASE_TEXT=IDS started and running  
}
```

Below is an example .trp file that can be used to decode an Airwave Management Platform event indicating that an AP has gone down.

```
1_3_6_1_4_1_12028_4_15_13 {  
    SEVERITY=Major  
    FRIENDLY_NAME=AP Down  
    BASE_TEXT=AP Down: IP=%DEVICE_IP_LIST : Description=%DESC  
    VARIABLES {  
        DEVICE_IP_LIST {  
            INDEX=3  
        }  
        DESC {  
            INDEX=2  
        }  
    }  
}
```

Using the Configurable Integration Platform Manually Creating CIP Files

The following .trp file example is for a trap file with defined variables and tables.

```
1_3_1_4_6_1_13{
  SEVERITY=Critical
  FRIENDLY_NAME=Rogue AP detected
  BASE_TEXT= Rogue AP %IP_ADDRESS detected on radio %RADIO_NUM.
  Detected by %DETECTION_METHOD
  VARIABLES{
    IP_ADDRESS {
      INDEX=0
    }
    RADIO_NUM {
      INDEX=1
    }
    DETECTION_METHOD {
      INDEX=2
      TABLE_NAME=DETECTION_TABLE
    }
  }
  TABLES {
    DETECTION_TABLE {
      1=Scanning
      2=Association
      3=Attempted Authentication
      DEFAULT=unknown
    }
  }
}
```

Notes:

If names in the TABLE keys contain a "." they will be substituted with a "_". So if the value in a PDU is an OID, all "." delimiters will be replaced with a "_".

All Names you specify in the .trp file must consist of an alpha-numeric string. Special characters (except for the underscore "_") are not allowed.

Troubleshooting Manual CIP Files

If you are not getting the expected results, here are some things to check.

- Are you running the latest version of PCM? Some of the CIP features described here are not enabled unless you have the latest release of PCM with all the auto-update patches applied. At a minimum you should have PCM 2.2 installed.
- Did you save the property file with a plain text editor rather than a word processor? Try opening the property files you created with Notepad to verify that the file is readable.
- Double check the syntax of the property files. Are all opening braces ("{") matched by a closing brace?
 - Check the Events tab in PCM. If PCM encounters a CIP property file with bad syntax, it will create an event indicating the file that caused the problem. The severity level of the error will be "Warning". The source of the event will be: CoreServer (Config.Integration), and the detail message will read:
Syntax error parsing user-defined Trigger file (<filename>).
- Is the file stored in the correct directory?
 - Most CIP files should be copied to <installdir>\PNM\server\config\devConfig\extern. The default install directory is: C:\Program Files\Hewlett-Packard.
 - The .oid files needed to add support for non-ProCurve devices are the exception to the above rule. These files should be copied to <installdir>\PNM\server\config\devConfig. The image .zip files containing the images and icons for the non-ProCurve devices must also be in the same directory as the .oid files.
- Did you restart the PCM Client? Note that for adding support to decode new SNMP traps (events), the PCM server must be restarted as well.
- Is the name of the main property unique? In the property files, note that they all start with a name followed by a curly brace, for example:

```
MibLaunchTrigger {  
    ...  
}
```

In this case, the "MibLaunchTrigger" must be a unique name. If some other property file also uses the name "MibLaunchTrigger" as the main property, then only one of them will be acknowledged and used.

Integrating PCM with NNM or NNMi

Overview	A-2
Additional References	A-2
Using PCM with NNM	A-3
Starting the PCM Client from NNM	A-4
Database User Management	A-6
Differences in PCM for NNM	A-7
Integrating PCM with NNMi	A-10
Prerequisites	A-10
Integration Procedure	A-10
Additional References	A-11
Configuring NNMi Communication Settings	A-11
Adding NNMi Subnets	A-14
Differences in PCM for NNMi	A-15
PCM-NNM/NNMi Synchronization	A-19
Setting Synchronization Intervals	A-19
SNMP Data Synchronization	A-20
Device Database Synchronization	A-20

Overview

ProCurve Manager for HP Network Node Manager (NNM) is PCM operating in plug-in mode with NNM:

- PCM integrates with NNM version 7.5 on Windows 2000, XP, and Windows Server 2003.
- PCM integrates with HP Network Node Manager i (NNMi) software versions 8.1x and 9.0 running on:
 - 32-bit Windows XP, Windows Server 2003, or Windows Server 2008
 - 64-bit Windows Server 2008

PCM and NNMi must run on different PCs.

Integrating PCM and NNM/NNMi provides a robust solution for managing ProCurve network products in a multi-vendor network environment. PCM with NNM offers the following benefits:

- ProCurve device management
- Schedulable software updates
- Group management
- Traffic monitoring

Important:

NNM version 7.5 is a different product than NNMi version 8.x. NNMi can be integrated with PCM by using PCM Preferences, as explained in “Configuring NNMi Communication Settings” on page A-11.

When you use PCM with NNM, NNM is registered as a trap receiver for PCM on each ProCurve device. Device events and PCM application events are displayed in the NNM events browser and PCM Events tabs.

Additional References

This document provides information on managing ProCurve devices using PCM. For more information related to using HP Network Node Manager (NNM), refer to *Managing Your Network with HP Network Node Manager* available on the HP Web at:

<http://h20230.www2.hp.com/selfsolve/manuals>

Using PCM with NNM

When you install the PCM for NNM module, the PCM Client and Server software are installed on the same system by default. You can then install a copy of the PCM Client on another computer running an NNM client.

The following directories and files are created at installation:

- PCM Server (Program Files\Hewlett-Packard\PNM\server), contains all the files needed for the PCM Server.
- PCM Agent (Program Files\Hewlett-Packard\PNM\pcm-agent), contains all the files needed for the PCM Agent.
- PCM NNM (Program Files\Hewlett-Packard\PNM\nnm), contains configuration files.
- PCM Client (Program Files\Hewlett-Packard\PNM\client), contains all the files, images, and configuration files needed for the PCM Client application.
- Java Runtime Environment (Program Files\Hewlett-Packard\PNM\hp_pcm_jre)

When using PCM with NNM you start PCM from the NNM display. PCM will read the NNM database to get the IP Address and SNMP community name of all ProCurve devices supported by PCM, then use it to build the device list and nodes within the PCM navigation tree. PCM will then run device scans to determine device configuration, VLAN, and network topology. You can access all other PCM device configuration and management features from the PCM display launched by NNM.

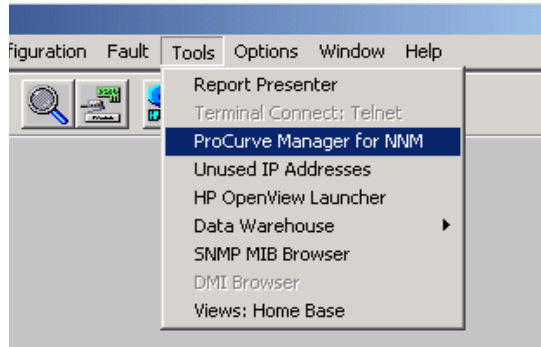
Note:

To synchronize the PCM and NNM database and SNMP community names, use the PCM synchronization functions, as explained in “PCM-NNM/NNMi Synchronization” on page A-19.

Starting the PCM Client from NNM

Use one of the following methods to launch the PCM Client display from the NNM window:

- Open the Tools menu and select the ProCurve Manager for NNM option.



- Click the ProCurve button in the toolbar.

The PCM Client starts in a separate window, as shown in Figure A-1 on the next page.

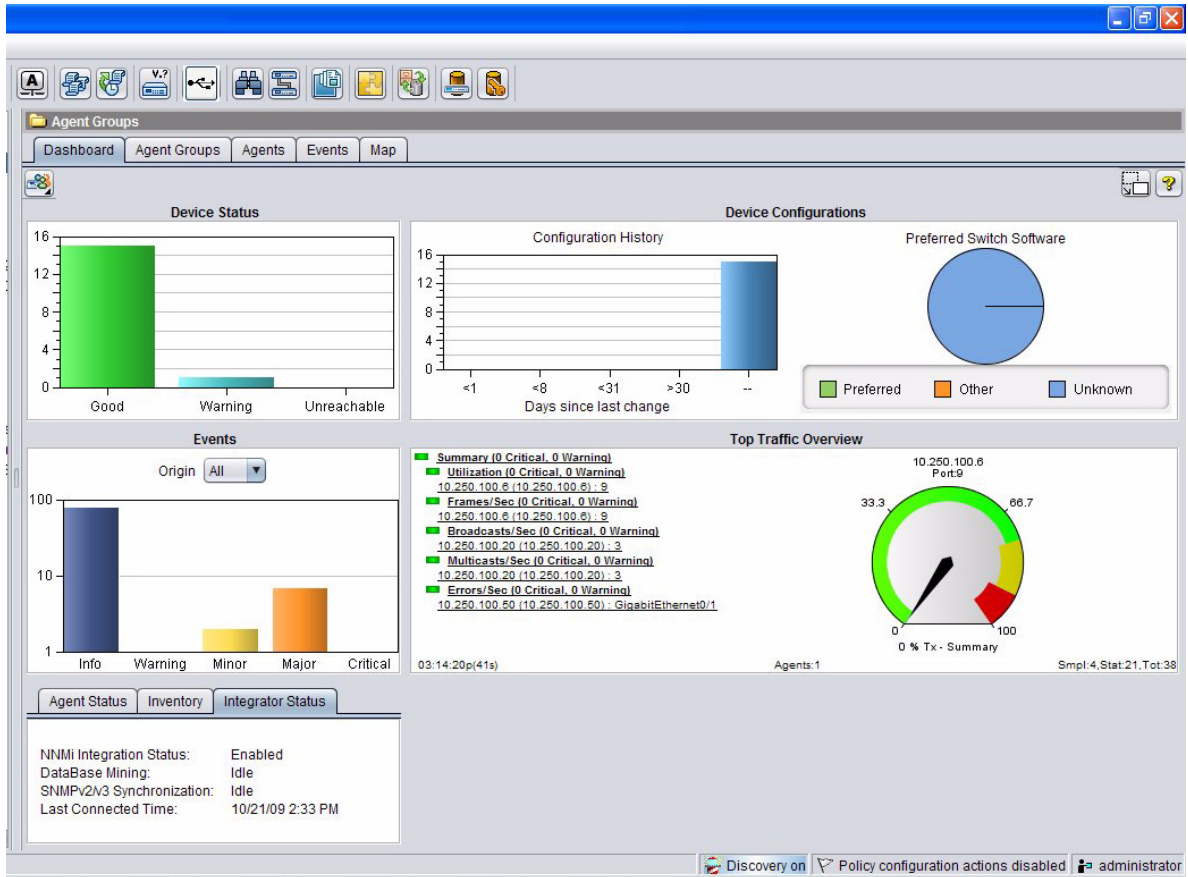


Figure A-1. PCM-NNM dashboard display

Please refer to “Network Management Home” on page 2-17 for more information on using the dashboard display.

- A third option for launching PCM is to right-click a ProCurve switch in the NNM map, then select the ProCurve Manager option.

PCM starts and displays the PCM Device Properties window with information for the device that was targeted on the NNM map. For more information on the Device Properties window, refer to “Viewing Device Information” on page 2-32.

Database User Management

The PCM database stores the network and device information retrieved by the PCM Discovery function. This PCM database can be accessed directly through supported protocols. (JDBC, ODBC, solsql, etc.).

When using PCM in standalone mode, the User Management feature allows you to configure access to external applications. In the PCM-NNM application this feature is unavailable. To provide read-only access to the PCM model database in PCM-NNM, use the User Management feature.

Note:

This feature is available in NNM only and not available in NNMi.

Adding Database User Accounts

To create a database user account in PCM-NNM, create a user as explained in “Managing User Accounts” on page 2-40. However, you must Grant external DB access.

Editing and Deleting Database User Accounts

To edit a PCM Database user account,

1. Select the account in the Manage Users window to enable the Edit and Delete option.
2. Select the Edit option to open the Edit Users window. It contains the same parameters as defined in the Add Users window.
3. Edit the user account parameters as desired, then click **Ok**.

To delete a user account,

1. Select the account in the Manage Users window to enable the Edit and Delete options.
2. Click Delete.

A confirmation pop-up will be displayed indicating the edit or deletion was successful.

Differences in PCM for NNM

PCM for NNM provides the network device management, configuration, and traffic monitoring functions of the PCM application for ProCurve devices on your network. The following section details differences in operation when using PCM for NNM, with references to additional information provided in earlier chapters of this book.

Device Discovery

The integration of PCM into the NNM application results in the following changes in the Device Discovery in PCM. For additional details on using the PCM Discovery feature, refer to Chapter 4, “Discovering Devices”.

- Because NNM includes ARP and Ping discovery, the ARP and Ping Sweep features of PCM discovery are not used. Instead, PCM will read the data collected in the NNM database periodically.
- Buttons on the PCM global toolbar allow you to force database mining of devices discovered by NNM and synchronize SNMPv2/v3 community names in PCM with those in NNM.
- By default NNMi does not discover end nodes. Because PCM only gets information for ProCurve devices discovered by NNM, the end-nodes and unknown devices will not appear in the PCM displays (navigation, devices list, maps).
- You can use the Manual Discovery Wizard in PCM to discover new network devices. If a device is not found in NNM (or PCM), you will need to troubleshoot in the NNM discovery process. (Refer to *Managing Your Network with HP Network Node Manager* for details).
- Because PCM does not get information on unknown devices from NNM, the PCM Device Reclassification Wizard will not work.
- Because the initial device data must come from NNM, you will not be able to change the Starting Device for PCM Discovery.
- You can change the PCM topology Discovery settings and VLAN Discovery settings on the PCM Discovery tab of the Agent Manager. Because NNM is already performing ARP and Ping Sweep discovery, the intervals for these functions are set in NNM.
- PCM device Discovery is stopped, but you can stop and start the PCM device attribute Discovery processes at any time without affecting NNM device discovery.

- The NNM database mining interval is user configurable. You can change this interval by clicking the Database Mining icon on the global toolbar.

For information on NNM Discovery, refer to Chapter 5 in *Managing Your Network with HP Network Node Manager*.

Network Maps

The integration of PCM into the NNM application has little affect on the PCM Network Maps feature. The only real difference is related to the fact that PCM does not get any data on end-nodes or unknown devices, thus all devices that appear in the maps will be properly identified.

Please refer to Chapter 5, “Using Maps” for more information on using the PCM Map feature. For information on using NNM maps, refer to *Managing Your Network with HP Network Node Manager*.

Network Events and Alerts

The integration of PCM into the NNM application results in the centralization of all network device and PCM application event processing within the NNM Events database. As noted in the discussion of PCM Discovery, the NNM management station is registered as a trap receiver for all discovered Pro-Curve devices, and all device and application events are sent to NNM (unless they are blocked). Thus the PCM Event Browser and Alerts features will not appear when using PCM for NNM.

Please refer to Chapter 6, “Using the Event Manager” for more information on the PCM Events browser feature. For information on working with NNM Events, refer to *Managing Your Network with HP Network Node Manager*.

Network Device Management

The integration of PCM into the NNM application results in the following changes in the Device Discovery feature in PCM.

- The default SNMP Community Name comes from NNM, but PCM will not prevent you from changing the default SNMP community names. After you change the SNMP community names in PCM, the SNMP names will be updated in the NNM database.
- SNMP settings, SNMP timeout and SNMP retry, are set by NNM during initial setup.

- To enable SNMP V3 support on NNM, the SNMP Security Pack product (BRASS plug-in) from SNMP Research has to be installed. Please refer to SNMP Research SNMP Security Pack User's Manual for more information.

Please refer to Chapter 7, “Managing Network Devices” for more information on using the PCM Device Management features.

Network Traffic Monitor

The integration of PCM into the NNM application has virtually no effect on the PCM Traffic Monitor feature. You can still monitor the network traffic and configure ports on PCM devices as described in Chapter 11, “Monitoring Network Traffic”.

Note that the SNMP write community name in NNM must be set the same as in PCM for traffic monitoring to work. SNMP read/write community names are automatically synchronized at intervals set in the PCM Integrations preferences window, as explained in “Setting Synchronization Intervals” on page A-19.

Device Configuration Management

The integration of PCM into the NNM application has virtually no effect on the PCM Configuration Manager feature. You can still review and update ProCurve device configurations as described in Chapter 12, “Managing Device Configurations”.

VLAN Management

The integration of PCM into the NNM application has virtually no effect on the PCM VLAN Manager feature. You can create VLANs, view VLAN Maps, and update VLAN configuration on ProCurve devices as described in Chapter 14, “Using VLANs”.

Configuration Policy Management

The integration of PCM into the NNM application results in a change to the Policy Manager feature in PCM — application events resulting from enforcement of policies will be sent to the NNM events log.

All other features of PCM policy management operate in the same manner as described in Chapter 16, “Using Policy Manager Features”. You will be able to create ProCurve device groups, and create and enforce configuration policies.

Integrating PCM with NNMi

PCM with NNM integration allows PCM to use data from the HP Network Node Manager i (NNMi) software versions 8.1x and 9.0. Similar to NNM, integration can provide the following features:

- Receive (mine) device and subnet data
- Synchronize SNMP v2/v3 community names (SNMP v1 is not supported in PCM)
- Listen for integrator notifications, such as device additions and deletion
- Forward PCM application events to the integrator (e.g., NNMi incident views)

Prerequisites

- PCM and NNMi must be installed on different PCs.

PCM and NNMi communication uses a HTTP or HTTPS connection, depending on the connection type configured in the NNMi Communication Settings window. (The default is HTTP.) This connection is opened only when data is transferred.

- The PCM+ Server and NNMi 9.0 server must run the same date, time, and time zone.

This means that the PCM+ Server and NNMi Server must refer to the same Time Server. Otherwise PCM+ fails to subscribe events from the NNMi server. As a result, PCM+ will stop receiving device addition and device deletion events from the NNMi Server.

For example, if the time running on the PCM+ Server is:
3 May 2010 Monday 14:24 PM Pacific Time,
Then the time running on the NNMi Server must also be:
3 May 2010 Monday 14:24 PM Pacific Time.

Integration Procedure

To integrate PCM and NNMi:

1. Configure the NNMi Communication Settings, as explained in “Configuring NNMi Communication Settings” on page A-11.

Integrating NNMi with PCM does not require a NNMi Integration Enablement license.

2. Configure Integration preferences, as explained in “Setting Synchronization Intervals” on page A-19.
3. Assign NNMi subnets to a PCM Agent, as explained in “Adding NNMi Subnets” on page A-14.
4. Synchronize the PCM SNMP settings with NNMi, as explained in “SNMP Data Synchronization” on page A-20.
5. Mine the NNMi database, as explained in “Device Database Synchronization” on page A-20.

Additional References

This document provides information on managing ProCurve devices using PCM. For more information related to using NNMi, refer to *NNMi Help for Administrators* available at:

<http://h20230.www2.hp.com/selfsolve/manuals>.

Configuring NNMi Communication Settings

Use NNMi Communication Settings Preferences to enable and configure NNMi integration. Communication Settings are set initially during installation.

To configure NNMi communication parameters:



1. Navigate to the NNMi Communication Settings window:
 - a. Click the Tools button on the global toolbar.
 - b. Select Integrations from the Preferences navigation tree.
 - c. Select NNMi Communication Settings from under Integrations.

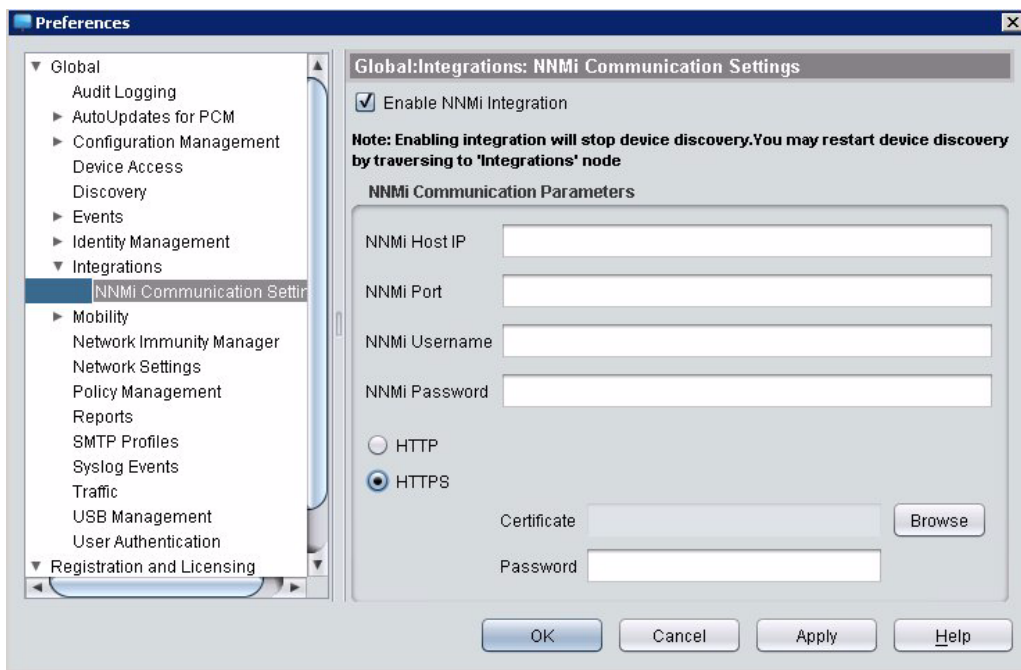


Figure A-2. NNMi Communication Settings

2. Ensure the Enable NNMi Integration check box is not checked. (NNMi communication parameters can be edited only when NNMi integration is disabled.)
3. Type the NNMi management server IP address in the NNMi Host IP field.
4. Type the NNMi jboss Web server port in the NNMi Port field.
5. Type the Administrator user name used to access the NNMi console in the NNMi Username field.
6. Type the Administrator password used to access the NNMi console in the NNMi Password field.
7. Select the protocol used to communicate with the NNMi WSDL URLs by selecting either the HTTP or HTTPS. The protocol selected must be the same as the protocol used to access the NNMi console. (You can change the protocol only if you have user permission and the PCM Plus license is in compliance.)

8. To use HTTPS as the protocol, ensure that NNMi uses the HTTPS protocol (HTTPS is not enabled by default in NNMi) and that the `nnm.keystore` certificate is copied from the NNMi location to the PCM Server. By default, the `nnm.keystore` certificate is located on the NNM management station in the following directory:

Documents and Settings\All Users\Application Data\HP\HP BTO Software\shared\nnm\certificates

Next, click the Certificate **Browse** button on PCM's NNMi Communication Settings window to browse to and select the `nnm.keystore` certificate. You can also create a keystore to configure HTTPS on NNMi, but need to use the same keystore in PCM.

9. If you selected HTTPS as the protocol, type the password of the selected certificate in the Password field.
10. Check the Enable NNMi Integration check box to enable integration.
11. To save your changes, enable integration and leave the Preferences window open, click **Apply**.

OR

To save your changes and exit the window, click **Ok**.

12. Assign each integrator subnet to the corresponding Agent using the Managed Subnet subtab in the Agent Manager Discovery tab to complete device and SNMP data mining. Devices discovered by the integrated application will not appear in the PCM navigation tree until their subnet is assigned to an Agent, as explained in “Adding NNMi Subnets” on page A-14.

To enable or disable NNMi integration:


1. To enable NNMi integration, check the Enable NNMi Integration check box.
2. To disable NNMi integration, uncheck the Enable NNMi Integration check box.

When NNMi integration is enabled, the Integration preferences and Agent Manager Discovery Integrator Subnet Management windows are activated. You can then configure the NNMi integration.

If PCM has already discovered devices before NNMi integration is enabled, the PCM-NNMi component will continue to mine devices and post it as manual discovery events. PCM will ignore those devices if they are already available in PCM. In this case, Agents will have subnets and the PCM windows showing the discovered devices are refreshed.

Adding NNMi Subnets

NNMi subnets must be assigned to an Agent before devices discovered by NNMi will appear in the PCM navigation tree, databases will be synchronized, and SNMP data will be transferred from the integrator. To assign each NNMi subnet to the corresponding Agent:

1. Ensure the integrator is enabled, as explained in “Configuring NNMi Communication Settings” on page A-11.
2. Ensure PCM is registered to receive traps from discovered devices in the imported subnet (on the Agent Manager Discovery tab for the Agent that will manage the subnet).
3.  Navigate to the Add Integrator Subnets window.
 - a. Click the Agent Manager button on the global toolbar to open the Agent Manager.
 - b. Select the Agent from the left pane of the Agent Manager.
 - c. Click the Discovery tab in the right pane.
 - d. Click the Managed Subnet subtab.

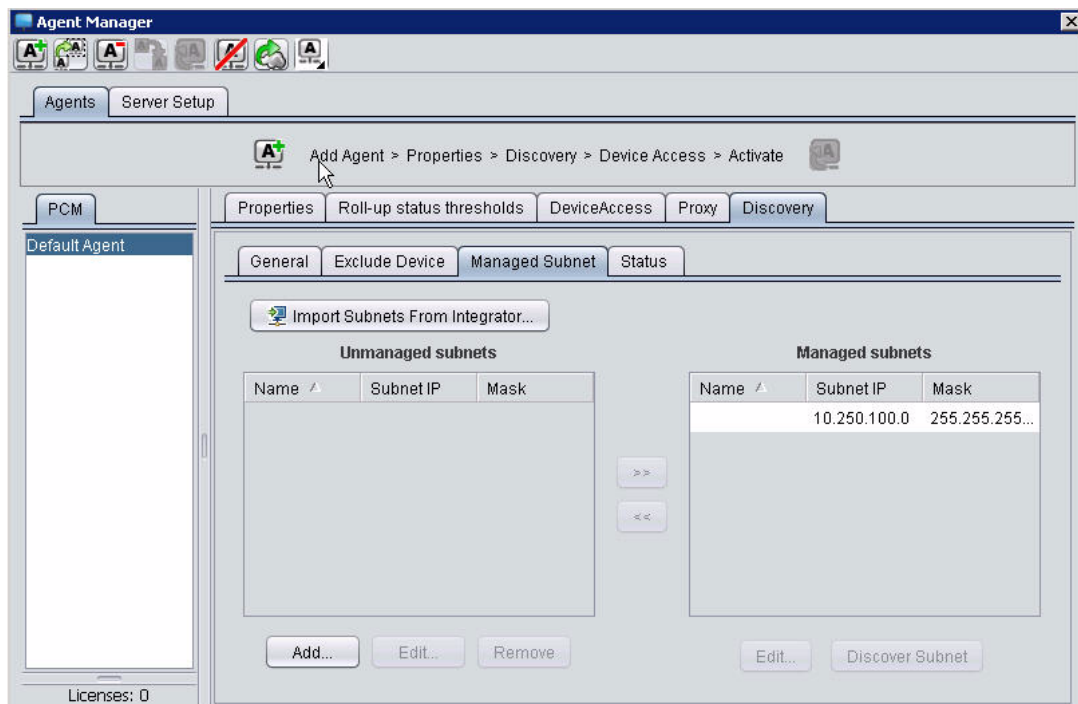


Figure A-3. NNMi Communication Settings

- e. Click the **Import Subnets From Integrator** button.



Figure A-4. Add Integrator Subnets

4. Select the NNMi subnet(s) to be added to the selected Agent. Use standard Windows selection conventions to select multiple subnets.
5. Click **Ok** to save your changes.

Differences in PCM for NNMi

PCM for NNMi provides the network device management, configuration, and traffic monitoring functions of the PCM application for ProCurve devices on your network. The following section details differences in operation when using PCM for NNMi, with references to additional information provided in earlier chapters of this book.

Device Discovery

The integration of PCM into the NNMi application results in the following changes in the Device Discovery in PCM. For additional details on using the PCM Discovery feature, refer to Chapter 4, “Discovering Devices”.

- When integration is enabled, PCM device Discovery is stopped on all Agents, but you can start or stop device Discovery by selecting the Enable Device Discovery check box on the Integrations preferences window or by enabling Discovery for an Agent.

- Because NNMi has ARP and Ping discovery the ARP and Ping Sweep features of PCM discovery are not used. Instead, PCM will read the data collected in the NNMi database periodically.
- Because PCM only gets information on ProCurve devices from NNMi, the end-nodes and unknown devices will not appear in the PCM displays (navigation, devices list, maps). You can get information on unknown or end-node devices in the NNMi displays.
- You can use the Manual Discovery Wizard in PCM to discover new network devices. If a device is not found in NNMi (or PCM), you will need to troubleshoot in the NNMi discovery process. (Refer to *NNMi Help for Administrators* at <http://h20230.www2.hp.com/selfsolve/manuals> for details).
- Because PCM does not get information on unknown devices from NNMi, the PCM Device Reclassification Wizard will not work.
- Because the initial device data must come from NNMi, you will not be able to change the Starting Device for PCM Discovery.
- You can change the Topology Discovery Settings and VLAN Discovery settings in the Global Discovery Settings. Because NNMi is already performing ARP and Ping Sweep discovery, the intervals for these functions are set in NNMi.

Note:

The default configuration for the IP Discovery interval in NNMi is 4 hours. Change (reduce) this interval to improve the PCM discovery performance.

For information on NNMi Discovery, refer to *NNMi Help for Administrators* at <http://h20230.www2.hp.com/selfsolve/manuals>.

Network Maps

The integration of PCM into the NNMi application has little affect on the PCM Network Maps feature. The only real difference is related to the fact that PCM does not get any data on end-nodes or unknown devices, thus all devices that appear in the maps will be properly identified.

Please refer to Chapter 5, “Using Maps” for more information on using the PCM Map feature. For information on using NNMi maps, refer to *NNMi Help for Administrators* at <http://h20230.www2.hp.com/selfsolve/manuals>.

Network Events and Alerts

The integration of PCM into the NNMi application results in the centralization of all network device and PCM application event processing within the NNMi Events database. As noted in the discussion of PCM Discovery, by default the NNMi management server is NOT registered as a trap receiver and blocks all traps unless you configure NIM to receive traps.

Please refer to Chapter 6, “Using the Event Manager” for more information on the PCM Events browser feature. For information on working with NNM Events, refer to *NNMi Help for Administrators* at <http://h20230.www2.hp.com/selfsolve/manuals>.

Network Device Management

The integration of PCM into the NNMi application results in the following changes in the Device Discovery feature in PCM.

- The default SNMP Community Name comes from NNMi, but PCM will not prevent you from changing the default SNMP community names. After you change the SNMP community names in PCM, the SNMP names will be updated in the NNMi database.
- To enable SNMP V3 support on NNMi, the SNMP Security Pack product (BRASS plug-in) from SNMP Research has to be installed. Please refer to *NNMi Help for Administrators* at <http://h20230.www2.hp.com/selfsolve/manuals> for more information.

Please refer to Chapter 7, “Managing Network Devices” for more information on using the PCM Device Management features.

Network Traffic Monitor

The integration of PCM into the NNMi application has virtually no effect on the PCM Traffic Monitor feature. You can still monitor the network traffic and configure ports on PCM devices as described in Chapter 11, “Monitoring Network Traffic”.

Note that the SNMP write community name in NNMi must be set the same as in PCM for traffic monitoring to work.

Device Configuration Management

The integration of PCM into the NNMi application has virtually no effect on the PCM Configuration Manager feature. You can still review and update ProCurve device configurations as described in Chapter 12, “Managing Device Configurations”.

VLAN Management

The integration of PCM into the NNMi application has virtually no effect on the PCM VLAN Manager feature. You can create VLANs, view VLAN Maps, and update VLAN configuration on ProCurve devices as described in Chapter 14, “Using VLANs”.

Policy Management

The integration of PCM into the NNMi application results in a change in the Policy Manager feature in PCM — application events resulting from enforcement of policies will be sent to the NNMi events log.

All other features of PCM policy management operate in the same manner as described in Chapter 16, “Using Policy Manager Features”. You will be able to create ProCurve device groups, and create and enforce configuration policies.

PCM-NNM/NNMi Synchronization

To avoid data conflicts between PCM and NNM/NNMi, several synchronizations must occur periodically. Set the intervals between automatic synchronizations and define the NNMi Communication settings using the PCM Integrations Preferences windows. Manually synchronize SNMP data and devices using the SNMP Synchronization and Database Mining buttons on the PCM global toolbar.

Setting Synchronization Intervals

You can enable device discovery and configure the intervals at which the PCM and NNM/NNMi synchronization functions occur using the PCM Integrations Preferences option.

1. Select Tools > Preferences > Integrations.

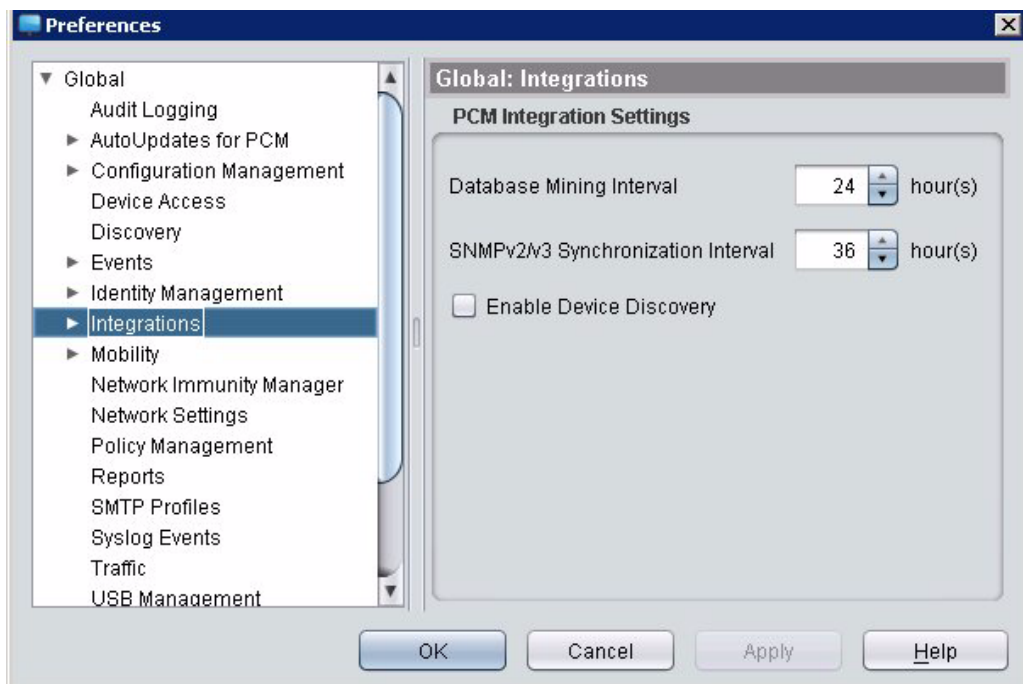


Figure A-5. Integrations Preferences

2. Type the Database Mining interval and the SNMPv2/v3 Synchronization interval to set the intervals at which PCM data is synchronized with NNM/NNMi data. You can also use the arrows to increase or decrease the intervals.

Set the interval to 0 if you do not want to use the automatic synchronization feature.

3. To enable PCM device discovery, check the Enable Device Discovery check box. (When you enable integration, PCM device discovery is stopped.)
4. Click **Apply** to save the changes, and then click **OK** close the window.

SNMP Data Synchronization

The SNMP settings (SNMP time-out, SNMP retry, Community names, and Discovery Status polling interval) in the NNM/NNMi database and PCM device database are synchronized as follows:

- During start-up or when integration is enabled, PCM gets the NNM/NNMi SNMP and Polling settings and updates the SNMP information in the PCM device database.
- Whenever you change the SNMP settings using PCM, the changes are passed to NNM/NNMi, and the NNM/NNMi SNMP data is automatically updated.
- Periodically, PCM will poll NNM for changes in SNMP settings and update the PCM device database to match information found in NNM. If the SNMP configuration is changed in the device using PCM, PCM will update NNM.



You can also click the SNMPv2/v3 Synchronization button in the PCM global toolbar to manually run the synchronization process at any time. PCM will read the NNM/NNMi database to get SNMP and polling information, and then update the correlating data within the PCM database.

Device Database Synchronization

When PCM is first started, it reads the NNM/NNMi database to get a list of managed ProCurve devices. This list is used to create the initial device list in PCM. At periodic intervals after start-up, PCM will read the NNM/NNMi database to check for new devices. The data is then used to update the PCM device lists to match the data found in NNM/NNMi.



Click the Device Database Mining button in the PCM global toolbar to read the NNM/NNMi device database at any time and automatically update the PCM device list.

If an unmanaged subnet is changed to a managed subnet in NNM/NNMi, PCM will automatically run Device Database Mining to get the information on devices in the new managed subnet. If a subnet is changed from managed to unmanaged in NNM/NNMi, the change will be passed to PCM, and the unmanaged subnet will no longer appear in the managed subnets list in PCM. However, moving a subnet from managed to unmanaged in PCM will have no affect on the subnet status in NNM/NNMi.

Glossary

The following terms and definitions are used in this book, and in other ProCurve Management Software documentation.

- Access Control:** Access Control is the ability to determine which endpoints can access the network and the level of access they receive. Access can be controlled based on an endpoint's compliance with network standards, for example, or on other configurable settings.
- Access Point:** A device that has station functionality and provides access to the distribution services, via the wireless medium (WM) for associated stations.
- Access Policy Group:** An IDM access policy group consists of one or more rules that govern the login times, devices, quality of service, bandwidth, and VLANs for users assigned to the access policy group.
- Access Profile:** An IDM access profile sets the VLAN, quality of service, and bandwidth (rate-limits) applied when a user logs in and is authenticated on the network.
- ACL:** An Access Control List (ACL), is a mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resource.
- ACS:** Access Control Service (ACS) protects against a system entity using a system resource in a way not authorized by the system's security policy; in short, protection of system resources against unauthorized access.
- Action:** An operation to be performed by ProCurve Manager when called upon by a policy.
- Ad Hoc:** In ad-hoc wireless networks, a series of stations operate in slave mode with no base station running in master mode. Also referred to as Independent Basic Service Set (IBSS), these stations can communicate directly with each other.
- AES:** Advanced Encryption Standard (AES) is a block cipher that has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits.
- Alert:** An alert notifies you when certain types of events occur that meet the alert's filter criteria.

ALG: Application-Layer Gateway (ALG) is an application-level gateway that acts as a proxy server between a trusted client and an untrusted host and accepts only packets generated by services it is designed to copy, forward, and filter.

ARP: Address Resolution Protocol (ARP) is a procedure by which TCP/IP devices obtain MAC addresses corresponding to a desired IP address. The originator emits a broadcast requesting the MAC address of a specific IP address, and the responder returns a packet containing its MAC address. RARP - Reverse Address Resolution Protocol performs the converse - obtains IP addresses from provided MAC addresses.

Attenuation: Reduction of signal strength during transmission. Attenuation is normal when a signal is sent from one point to another. If the signal attenuates too much, it becomes unintelligible, which is why most networks require repeaters at regular intervals. Attenuation is measured in decibels.

Authentication: Authentication is the process of verifying an identity claimed by or for a system entity.

Average Packet Size Deviation: Attack detected by a statistically unusual change in the average size of sent and/or received packets.

Bandwidth: Bandwidth is the capacity of a communication channel to pass data through the channel in a given amount of time. Usually expressed in bits per second.

BOOTP: Bootstrap Protocol (BOOTP) is a protocol used primarily on TCP/IP networks to configure workstations. DHCP is a later boot configuration protocol that uses this protocol.

BSS: Basic Service Set (BSS) in the IEEE 802.11-1999 Standard is the basic building block of an IEEE 802.11 wireless LAN. The most basic BSS is two stations in IBSS mode. In infrastructure mode, a basic BSS consists of at least one station and one access point. However, in infrastructure mode, groups of BSSs can be abstracted as an ESS when the BSSs share a common Network Name or SSID.

BSSID: Basic Service Set Identifier (BSSID) is the wireless MAC address of a detected access point.

CA: Certification Authority (CA) is an entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

CHAP: Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol used by a remote access client to send its authentication credentials to a remote access server in a secure form.

- CIP:** Configurable Integration Platform
- Client:** A client is a computer running an application that interacts with another program running on a server.
- Community Name:** A community name defines authentication and access control between an SNMP agent and a management station. This name is placed in SNMP messages sent between SNMP-managed devices.
- Country Code:** An identifier that is defined for a nation by ISO. For each nation, ISO Standard 3166 defines a unique two-character alphabetic code, a unique three-character alphabetic code, and a three-digit code. Among many uses of these codes, the two-character codes are used as top-level domain names.
- Credentials:** Credentials are a set of information that includes identification and proof of identification used to access local and network resources (e.g., user names and passwords).
- Custom Group:** A customized group of devices to indicate typically a network location. A group can have devices or subfolders. In addition, a single device may span multiple custom groups. Custom Groups become nodes in the tree of ProCurve Manager, where other components can contribute functionality that applies to any ProCurve Manager device group.
- DA:** Destination Address. In an IP packet, this is the destination IP address carried in the header, and identifies the destination intended by the packet's originator.
- Database:** The database, a storage location for events, is allocated a specific size. When the database is full, the oldest events are replaced by new events.
- Default Gateway:** A default gateway for the TCP/IP protocol is the IP address of a directly reachable IP router.
- DES:** Data Encryption Standard (DES) is a U.S. Government standard [FP046] that specifies the Data Encryption Algorithm and states policy for using the algorithm to protect unclassified, sensitive data. (See: AES.)
- Device:** A device is a networking computer that includes the hubs, bridges, switches, routers, protocol analyzers, or other LAN devices in a network.
- DHCP:** Dynamic Host Configuration Protocol (DHCP) is software that assigns IP addresses to devices without a permanent IP address. DHCP allows a finite number of IP addresses to be reused quickly and efficiently by many clients.

- Distinguished Name:** Distinguished Name (DN) is an identifier that uniquely represents an object in the X.500 Directory Information Tree (DIT) [X501]. (See: domain name.) A DN is a set of attribute values that identify the path leading from the base of the DIT to the object that is named. An X.509 public-key certificate or CRL contains a DN that identifies its issuer, and an X.509 attribute certificate contains a DN or other form of name that identifies its subject.
- DNS:** Domain Name System (DNS) is a process and model by which IP addresses are correlated to a naming convention or "friendly name". DNS servers typically provide a resolution service providing an IP address when a requester supplies a host name.
- Domain:** A domain is a group of computers and devices on a network that are administered as a unit with common rules and procedures. Within the internet, domains are defined by the IP Address. All devices sharing a common part of the IP address are said to be in the same domain.
- EAP:** Extensible Authentication Protocol (EAP) is built on a public-key encryption system to ensure that only authorized network users can access the network. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication.
- Edge Port:** An edge port connects two networks such as connecting your network to the internet.
- Egress:** Network traffic from an internal source to an external destination.
- End Node:** An end node is a device such as a computer that is directly attached to a hub or switch. End nodes, in Hewlett-Packard's terminology, are known by their station addresses only, not by an IP or IPX address.
- Enforcement:** Enforcement of a policy performs the actions defined in the policy, usually in specific devices or device groups.
- ESS:** A set of one or more interconnected basic service sets (BSSs) and integrated local area networks (LANs) that appears as a single BSS to the logical link control layer at any station associated with one of those BSSs.
- ESSID:** Extended Service Set identification.

- Event:** A message that indicates something has happened and helps you to quickly identify the number and severity of the problem in the network. It is indicated by SNMP traps and application messages received by PCM. PCM organizes and displays the events based on Source, Severity, Status, Date and Description.
- Filter:** A filter defines one or more conditions required to issue an alert, or display an event. Filtering is a process that screens incoming information for certain characteristics, allowing only a subset of that information to pass through.
- Firewall:** A firewall is a dedicated appliance or software running on another computer that inspects network traffic and denies or permits passage based on a set of rules.
- FQDN:** Fully Qualified Domain Name (FQDN) specifies the exact location of a node in the DNS tree hierarchy (e.g., eng.procurve.edu).
- Fragmentation Threshold:** Fragmentation threshold sets the minimum packet size that can be fragmented. Fragmentation of the PDUs (Package Data Unit) can increase the reliability of transmissions because it increases the probability of a successful transmission due to smaller frame size.
- FTP:** File Transfer Protocol (FTP) is a part of the TCP/IP suite of Internet protocols. It is software that lets users download files from a remote computer to their computer's hard drive.
- Gateway:** A gateway device allows equipment with different protocols to communicate with each other. It is a conceptual or logical network station that interconnects two otherwise incompatible networks, network nodes, subnetworks, or devices. Gateways perform a protocol-conversion operation across a wide spectrum of communications functions or layers.
- Global Toolbar:** The Global Toolbar, which is located across the top of the PCM window, contains buttons that act as shortcuts to PCM functions.
- GVRP:** GARP VLAN Registration Protocol (GVRP) is a protocol designed to propagate VLAN information from device to device. A single switch is configured with all VLANs in the network, and other switches learn those VLANs dynamically.
- HP:** Hewlett-Packard
- IBSS:** Independent Basic Service Set (IBSS), the most basic type of IEEE 802.11 wireless LAN, is commonly referred to as an ad-hoc network. An IBSS can consist of as few as two stations. Unlike infrastructure mode, all stations are capable of communicating directly with each other.

- IGMP:** Internet Group Management Protocol (IGMP) is a protocol used by Internet hosts to report their multicast group memberships to any immediately-neighboring multicast routers. It is required to be implemented by all hosts wishing to receive IP multicasts. Multicast protocols are important for VLANs, or when you are trying to reduce or limit broadcast traffic on a network.
- Infrastructure network:** In infrastructure wireless networks, a basic BSS consists of at least one station and one AP.
- Ingress:** Network traffic from an external source to an internal destination.
- Ingress Filtering:** Ingress filtering manages traffic flow entering your network to prohibit externally initiated inbound traffic to unauthorized services.
- IP Address:** An IP address consists of the network ID and a unique host ID, typically represented with the decimal value of each octet separated by a period (for example, 15.241.125.60)
- IV:** In cryptography, an initialization vector (IV) is a block of bits that is required to allow a stream cipher or a block cipher executed in any of several streaming modes of operation to produce a unique stream independent from other streams produced by the same encryption key, without having to go through a (usually lengthy) re-keying process.
- Kerberos:** Kerberos is a computer network authentication protocol that allows individuals communicating over an insecure network to prove their identity to one another via a trusted third party. Kerberos prevents eavesdropping or replay attacks, and ensures the integrity of the data. It provides mutual authentication (both the user and the service verify each other's identity).
- LDAP:** Lightweight Directory Access Protocol, an Internet protocol used to look up contact information from a server.
- Leaf Node:** Node in a tree data structure that has no child nodes (end node in a tree branch).
- LLDP:** Link Layer Discovery Protocol. LLDP provides a standard method for Ethernet network devices (such as switches, routers, and wireless LAN access points) to advertise information about themselves to other nodes on the network and to store the information they discover from other nodes.
- Local Subnet:** A Local Subnet is a LAN that interconnects a variety of devices within a small area. The local subnet might connect computers on adjacent desks or within a department. A local subnet ends at a router or a gateway.

- MAC:** Media Access Control (MAC) address is a data link-layer address that is unique for each node on a LAN. MAC addresses consist of a 12-digit hexadecimal number and are designed to be unique and contain a code identifying the manufacturer of the network adapter or interface within the beginning of the address.
- MD5:** Message-Digest algorithm 5 is a cryptographic hash function with a 128-bit hash value. MD5 is used in a wide variety of security applications and is also can used to check the integrity of files.
- MIB:** Management Information Base (MIB) is a coded, hierarchical description of the SNMP objects that a device supports. A MIB is used by the SNMP agent and SNMP manager to communicate. In common usage, SNMP agents and managers support standardized MIBS that contain information offered by most managed devices.
- Navigation Tree:** A tree structure that contains selectable links (e.g., devices and PCM functions) and nodes (groups) containing related links. These links are used to access PCM functions. The link provides access to the primary screen/function, and right-click to the link provides access to related functions.
- Network Resource:** A network resource is a server or a protocol to which you want to grant or deny access (for example, a server running financial data that can be accessed by financial personnel only). Also referred to as ACLs in other ProCurve documentation.
- NNM:** HP Network Node Manager (NNM) is a network management platform created and distributed by Hewlett-Packard.
- Node:** A Node is a device with a network address that is the source or destination of traffic on a network.
- PCM:** ProCurve Manager (PCM) is an advanced Windows-based network management tool that provides administrators with easy-to-use screens for configuring, updating, monitoring, and troubleshooting ProCurve devices.
- Ping Sweep:** During discovery every device in the subnet is sent a ping, and the devices respond to the ping. This response is used to "discover" the device and identify its status.
- Policy:** A policy is a set of actions performed (enforced) at a scheduled time, usually on specific devices or device groups.
- Pre-shared Key:** A shared secret authentication key sent before other credentials such as a username and password. Pre-shared (PSK) key mode requires each user to enter a passphrase to access the network. The passphrase may be from 8-63 ASCII characters or 64 hexadecimal digits (256 bits).

- PSK:** Pre-shared Key (PSK) or shared secret authentication key sent before other credentials such as a username and password.
- RADIUS:** Remote Authentication Dial-In User Service (security).
- Rate Limiting:** An option for firewall policies that permits limits to be put on the amount of bandwidth a connection type can use.
- Read Access:** Permissions that govern the community name's ability to read data on a device
- RMON:** Remote Monitoring (RMON) is an extension of the SNMP standard. RMON provides for use of SNMP in monitoring detailed network traffic information. A network traffic capture utility or network probe typically uses RMON to collect statistics and packets for later analysis by a central monitoring console.
- Roaming:** Roaming refers to the movement of a wireless node between two microcells. Roaming usually occurs in infrastructure networks built around multiple access points.
- Rollback:** The process of “undoing” any configuration changes made by certain actions that support rollback after a user-defined time period has elapsed since the action first went into effect.
- Routed Traffic:** Traffic moving from an SA in one VLAN to a DA in a different VLAN.
- Router:** A computer that is a gateway between two networks at OSI layer 3 and that relays and directs data packets through that internetwork. The most common form of router operates on IP packets. In the context of the Internet protocol suite, a router is a networked computer that forwards Internet Protocol packets that are not addressed to the computer itself.
- RSSI:** Received Signal Strength Indication (RSSI) is a measurement of the strength of a received signal in a wireless environment, A value of 1 indicates the minimum signal strength detectable by the wireless card, while 0 indicates no signal.
- SA:** Source Address. In an IP packet, this is the source IP address carried in the header, and identifies the packet's originator.
- Self-signed Certificate:** A self-signed certificate is a public-key certificate for which the public key bound by the certificate and the private key used to sign the certificate are components of the same key pair, which belongs to the signer. In a self-signed X.509 public-key certificate, the issuer's DN is the same as the subject's DN.
- Severity:** Severity indicates the level of seriousness based on implications of the condition (e.g., Critical, Warning, Informational, etc.).

- SNMP:** Simple Network Management Protocol (SNMP) is an industry standard protocol for managing network devices, such as hubs, bridges, and switches. SNMP is a collection of specifications for network management that includes the protocol itself, the definition of a database, and associated concepts. SNMP minimizes network traffic and firmware code size and allows control of retry rates and reporting of detected events, using SNMP traps.
- SSID:** A Service Set Identifier (SSID) is a code (32 alphanumeric characters maximum) attached to all packets on a wireless network to identify each packet as part of that network. All wireless devices attempting to communicate with each other must share the same SSID. SSID also serves to uniquely identify a group of wireless network devices used in a given service set.
- Station:** A device containing an IEEE 802.11-conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (e.g., laptop, wireless printer, etc.).
- STP:** Spanning Tree Protocol (STP) is the IEEE bridging standard that includes spanning tree. In a switched/bridged environment, you cannot have loops in the topology. If you have designed loops for the sake of redundancy, then the switches/bridges must all adhere to the same spanning tree standard (e.g., IEEE 802.1d) to properly break the link forming the loop, until such time that link is needed.
- Subnet Address:** A Subnet Address is an extension of the IP addressing scheme that allows a site to use a single IP network address for multiple physical networks.
- Subnet Mask:** A Subnet Mask is a value that tells a device the total length of the IP address chosen for the IP network (and subnetwork) fields and the total length of the IP address chosen for the host field. The subnet mask does this by designating network and subnetwork fields within the IP address as 1's and the host field as 0's.
- Tagged Frame:** A VLAN-tagged frame is a basic MAC data frame with a four-byte VLAN header inserted between the SA and Length/Type fields.
- TCP/IP:** Transmission Control Protocol/Internet Protocol (TCP/IP) is the Routable Network and Transport layer protocols that have become the defacto standard for the Internet and most heterogeneous networks.
- Telnet:** Telnet provides DEC VT100, DEC VT52, or ANSI emulation interface to many hardware devices such as network hubs, switches, and routers. The interface uses a connection-based service of TCP and usually connects via port 23.

- TKIP:** Temporal Key Integrity Protocol (TKIP) is a security protocol used in Wi-Fi Protected Access (WPA) to replace WEP without replacing legacy hardware. TKIP, like WEP, uses a key scheme based on RC4, but unlike WEP, TKIP provides a message integrity check, a re-keying mechanism, and ensures that every data packet is sent with its own unique encryption key. TKIP also hashes the initialization vector values with the WPA key to form the RC4 traffic key.
- TLS:** Transport Layer Security, a successor of Secure Sockets Layer (SSL), is a cryptographic protocol that provides secure communications on the Internet. TLS provides endpoint authentication using cryptography. Typically, only the server is authenticated. However, mutual authentication is available with PKI deployment to clients. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery.
- Toolbar:** A Toolbar contains buttons that act as shortcuts to PCM functions. PCM contains a global toolbar located at the top of the PCM window and related-functions toolbars located at the top of the right pane.
- Trap:** SNMP traps are received by PCM using the SNMP communication mechanism.
- Tree:** A Navigation Tree contains selectable links (e.g., devices and PCM functions) and nodes (folders) containing related links. These links are used to access PCM functions. Click the link to access its primary screen/function, or right-click the link to access related functions.
- Unassociated Event:** An unassociated event is not associated with a managed device and typically originates in the PCM application, PCM plug-in modules, or undiscovered devices.
- USM** User Security Model (USM) is an SNMPv3 core module is in charge of authenticating/encrypting/decrypting SNMP packets.
- VLAN:** A Virtual Local Area Network (VLAN) is a location independent broadcast domain. A VLAN is like the standard definition of a LAN without the physical constraints. These VLAN domains are a collection of workstations that are part of the same logical, working community but not likely part of the same physical community. The goal of VLANs is to allow for complete mobility and flexibility of workstation placement, yet keeping cross domain broadcast traffic to a minimum.
- VPN:** Virtual Private Network (VPN) is a restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network. For example, if a corpo-

ration has LANs at several different sites, each connected to the Internet by a firewall, the corporation could create a VPN by (a) using encrypted tunnels to connect from firewall to firewall across the Internet and (b) not allowing any other traffic through the firewalls. A VPN is generally less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the real network.

WebAgent: The WebAgent is the Web server application that provides device management information to remote requesting Web browsers. WebAgents may reside with a device's firmware, or as a program running within the operating system of a computer.

WEP: Wired Equivalent Privacy (WEP) is a security protocol for wireless local area networks (WLANs) that uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity. Standard WEP uses a 40 bit key, to which a 24-bit initialization vector (IV) is concatenated to form the RC4 traffic key. WEP is used at the two lowest layers of the OSI model - the data link and physical layers. Therefore, it does not offer end-to-end security.

Wizard: A Wizard is a Windows application that automates a multi-step procedure.

WLAN: Wireless Local Area Network (WLAN) or wireless LAN is a local area network (LAN) that users access through a wireless connection. 802.11 standards specify WLAN technologies. WLANs are frequently some portion of a wired LAN.

WPA: Wi-Fi Protected Access (WPA) is a Wi-Fi standard that authenticates users and uses the temporal key integrity protocol (TKIP). User authentication uses the extensible authentication protocol (EAP). EAP is built on a public-key encryption system to ensure that only authorized network users can access the network. TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

Write Access: Permissions that govern the community name's ability to write data on a device

Index

A

Acknowledge events 6-8
ACL Details 10-13
Action types 16-40
Activate Agent 3-15
Active Users 2-48
Active/Inactive Port List 18-14
Add Agent 3-13
Add an application 19-12
Add subnet 3-28
Add Subnets 4-41
Adding Devices to Profile 2-43
Adding User Accounts 2-45
Administrator 2-41
Agent File Manager 3-55
Agent Information 3-10
Agent Manager 3-19
Agent Map 5-7
Agent password 3-21
Agent Status tab 2-25
Agent UI 3-6
Agent-initiated Connection 3-5
Agents 2-8, 3-2
Agents Map 5-6
Agents Tab 3-53
Agents tab 2-9, 3-3
Aggregated Events 6-15
Alert Configuration 16-43
Alerts 7-43
application menus 2-27
Architecture 1-8
Auth Type 10-9
authorized IP managers
 precedence over other security 7-7
Authorized Managers 7-7
auto port setting 14-27
automatic device registration 2-59
Automatic Updates 2-54

B

background 5-22
Backing Up PCM

 Automatically 2-65
 Manually 2-61
blocked port
 from IGMP operation 14-27
broadcasts 11-12

C

CDP discovery 4-3
CIP Wizard 19-3
CLI Credentials 7-30
CLI Settings for PCM 7-28
CLI Wizard 12-20
Client permissions 2-70
client-server authentication 2-70
Clone Agent 3-14
clone profile 2-42
Communication Parameters in Devices 7-15
Communication Parameters in PCM 7-14, 7-24
Config Manager action 16-40
Configuration
 detail 12-11
 history 12-12
 label 12-13
Configuration export 12-43
Configuration Manager 12-3
 Scan Preferences 12-56
Configuration Manager preferences 12-55
configuration policy 16-2
Configuration, import 12-45
Configurations
 compare 12-14
 manual scan 12-4
Configurations tab 12-10
Configured Policies Report 18-22
connect to remote Agents 2-9, 3-2
connection-rate filter 15-2
connection-rate filtering
 activation 15-2, 15-5
 benefits 15-2
 blocked host 15-3, 15-5, 15-10
 blocked host, re-enable 15-3
 event log notice 15-3, 15-10
 guidelines 15-7, 15-8

- notify and reduce 15-3, 15-10
- notify only 15-3, 15-10
- operation 15-3
- options 15-3
- port setting change, effect 15-5
- reboot, effect 15-5
- re-enable blocked host 15-5
- routed traffic 15-2
- sensitivity level 15-4, 15-7
- signature recognition 15-2
- SNMP trap 15-3, 15-10
- switched traffic 15-2
- throttle 15-6
- trigger 15-2, 15-5
- VLAN delete, effect 15-5
- Consistency 1-5, 1-6, 17-10
- Console Access 10-4
- Console Authentication 10-4
- Content Variables 16-43
- Credential Change History Report 18-15
- CSV file 9-8

D

- Dashboard 2-18
- Data Synchronization
 - SNMP A-20
- Database User Management A-6
- dedicated management VLAN 14-15
- default gateway 4-28
- default VLAN 14-2
- definition 4-2
- Delete Agent 3-63
- Delete device 4-36
- delete device 4-39
- Deploy Wizard 12-16
- Device Access 10-2
- Device access 7-40
- device access 7-14
- Device Access Configuration Report 18-15
- Device Access Credentials Report 18-16
- Device Access Password Audit Report 18-16
- Device Access tools 7-2
- Device Config Change History Report 18-18
- Device Configuration Change Totals Report 18-18
- Device Configurations 12-10
- Device Discovery, with NNM A-7
- Device Discovery, with NNMi A-15

- Device Help 2-72
- Device List Synchronization A-20
- Device Log Viewer 7-46
- Device Manager 7-2
- Device Manager action 16-41
- Device Properties
 - Live view 2-35
 - static view 2-34
- Device properties 2-33
- device properties 2-34
- Device re-classification 4-43
- Device Status 2-18
- Device Uptime and Status Report 18-19
- Devices List 2-33
- Devices List by Agent Report 18-17
- disable discovery 3-23
- Discover Subnet button 3-29, 4-3
- Discovery
 - CDP and FDP 4-3
 - default gateway, Starting device 4-28
 - delete 4-36
 - devices found 4-2
 - exclude 4-36
 - loopback interfaces 4-17
 - Manual process 4-7
 - starting device 4-33
 - status 2-26, 4-5
 - subnets 4-40
- Discovery Preferences 3-23
- Discovery Troubleshooting 4-57
- display a log 3-59
- Displaying 2-48
- Download Agent software 3-5

E

- enable discovery 3-23
- encryption 3-21
- End Nodes 2-30, 2-31
- Event Activity Report 18-22
- Event Browser Configuration 6-18
- Event details 6-10
- Event Preferences
 - ignore list 6-21
- Event Totals by Severity Report 18-23
- event-based alert 16-21
- Events archive preferences 6-19
- Events summary 2-19

- Events tab 2-19
- Events, with NNM A-8
- Events, with NNMi A-17
- Exclude Device 3-25
- Exclude device 4-36
- Export Configurations 12-43

F

- FDP discovery 4-3
- Filtering syslog events 7-48
- Find Node 4-22
- Find node 5-18, 5-19
- firewalls 2-70
- Firmware 12-60
- Firmware Updates
 - delete 12-66
- firmware updates 12-61
- Firmware versions 12-60
- forwarding port, IGMP 14-27
- frames 11-12

G

- Generate Report 16-46
- Groups
 - add devices 13-6
 - delete 13-5
- GVRP Port 10-15

H

- Hardware replacement 7-54
- Hierarchical map 5-10

I

- IGMP
 - benefits 14-25
 - port states 14-27
- Ignore events 6-21
- Import Configuration 12-45
- Integrator Status tab 2-26
- Inventory pane 4-6
- Inventory Report 18-13
- Inventory tab 2-25
- IP Discovery, NNMi A-16
- IP Managers 7-7

L

- Labels 12-13
- LACP
 - monitoring static trunk 10-16
- Last 24 Hours tab 2-21
- Learn-Mode 10-10
- License 2-15
- License Software 12-49
- Link Status 5-12
- Live view 2-35
- local Agent 1-9, 2-8, 3-2
- Logging scan results 12-56
- Loopback interfaces 4-17

M

- MAC Lockout 10-25
- MAC Monitor 10-19
- Managed Subnets 3-27
- Management community name 7-34
- Manual discovery 4-7
- Manual scans 12-4
- map annotations 5-15
- Maps
 - agents 5-6
 - agent-specific 5-7
 - find node 5-18, 5-19
 - hierarchical 5-10
 - layout options 5-10
 - Legend 5-16
 - network 5-5
 - radial tree 5-10
 - Refresh button 5-4
 - subnets 5-9
 - Toolbar buttons 5-18
 - tools 5-18
 - tree layout 5-10
 - VLANs 5-9
- Mark as Inactive 3-15
- MED Device Inventory Report 18-14
- MED devices
 - configuration 9-7
 - displaying 9-2
 - end host map 9-5
 - importing MED information 9-8
 - location 9-7
 - Power over Ethernet 9-7
 - supported 9-2

- switch view 9-4
- Media endpoint devices
 - See also* MED devices.
- meshed ports, monitoring 10-16
- Mirror Port 10-17
- Modify Subnets 4-42
- Modifying Profiles 2-43
- Modifying User Accounts 2-47, A-6
- monitoring meshed ports 10-16
- monitoring port 10-16, 10-17
- monitoring, port 10-16
- Move subnet 3-30
- multicast 11-12
- MyProCurve device registration 2-59

N

- Navigation 2-30
- Network Analyzer 17-2, 17-10
- Network Consistency 1-5, 1-6
- Network Consistency Analyzer 17-2, 17-10
- Network Management Home 2-17
- Network Map 5-5
- network monitoring
 - traffic overload 10-16
- NIM Security Monitoring 3-50
- NIM Top Offenders 2-27
- NNM Events A-8
- NNMi Events A-17
- no contexts defined 2-70
- Node search 4-22
- node-to-node path 4-26

O

- ONE zl Modules
 - activating license 8-13
 - displaying 8-2
 - installing application 8-9
 - PCM+ Agent application 3-2
 - troubleshooting 8-3, 8-18
 - uninstalling application 8-16
- Operator 2-41

P

- password
 - authorized IP managers, precedence 7-7

- Passwords 2-40
- Path trace 4-26
- PCM Client 1-8
- PCM Client, installing 2-4
- PCM database A-6
- PCM device access 7-14
- PCM Server 1-8
- PCM Services 2-69
- PCM toolbar 2-28
- PCM-NNM/NNMi Synchronization A-19
 - Setting Intervals A-19
- Perl script, example 12-100
- Ping Status 5-11
- Ping Sweep discovery 3-29, 4-3
- Ping Sweep settings 4-33, 4-34
- plug-in application 19-12
- Policy
 - Action 16-3
 - Alerts 16-3
 - Sources 16-3
 - Targets 16-3
 - Times 16-3
- Policy Actions 16-30
- Policy configuration 16-4
- Policy History 16-14
- Policy Manager
 - executing a script 12-80, 12-93
- Policy Manager action 16-43
- Polling, Discovery action type 16-42
- port
 - auto, IGMP 14-27
 - blocked, IGMP 14-27
 - forwarding, IGMP 14-27
 - monitoring, static LACP trunk 10-16
 - state, IGMP control 14-27
- Port Access 10-2
- Port Access Configuration Report 18-17
- Port Access tab 10-9
- port assignments 10-8, 14-22
- port classification 4-19
- port mirror 10-16
- Port security 10-2
- port security
 - authorized IP managers, precedence 7-7
- Port Settings actions 16-44
- Port Traffic 11-14
- Port-access 10-4

- port-based access control
 - authorized IP managers, precedence 7-7
- Power over Ethernet (PoE) 9-7
- Preferences
 - device access 7-40
- Preferences, configuration 12-55
- Preferences, Switch software 12-57
- Primary image 12-63
- primary server 2-11
- Profiles
 - removing device 2-45
- Proxy 3-21
- Proxy settings 12-58

R

- Radial Tree map 5-10
- RADIUS
 - authorized IP managers, precedence 7-7
- RADIUS Authentication 2-49
- reboot Agent 3-59
- Re-classify device 4-43
- Re-Discover Device 4-14
- Re-discover device 4-6
- Refresh map 5-4
- Registration, for devices 2-59
- Regulatory Compliance Reports 18-13, 18-14, 18-18, 18-22
- remote Agent 1-9, 3-2
- Remove Subnets 4-42
- Removing Devices from Profile 2-43
- Replace Agent 3-62
- replace Agent 3-62
- Replace hardware 7-54
- Report Delivery 18-11
- Report file 12-78
- Report format 18-10
- Report Heading 18-2
- Report Policy 16-46, 18-7
- Reports 2-28, 2-38
- Reports menu 18-2
- Reports Wizard 18-4
- Rescan for user-defined devices 3-25
- restore 2-64
- Restoring PCM 2-64
- RMON
 - alerts 7-43
- RMON Manager 7-42

- Rollback Actions 16-11

S

- Schedule-driven alert 16-26
- Script Wizard 12-80
- Scripts
 - adding to Script Manager 12-82
 - deleting 12-87
 - editing 12-86
 - embedded tags 12-95
 - executing as a policy action 12-93
 - executing with Script Wizard 12-88
 - managing devices 12-80
 - perl example 12-100
 - runtime environment 12-82
 - shell example 12-97, 12-98
 - troubleshooting 12-96
- Secondary image 12-63
- Secure Copy 12-56
- Security Report Types 18-13
- Security State 5-11
- seed device 3-24, 4-33
- Select PCM Server 2-11
- Server discovery 2-12
- Server Information 3-11
- Server-initiated Connections 3-9
- sFlow sampling 11-2
- Shell script, example 12-97, 12-98
- SNMP Community Name, NNM A-8
- SNMP Community Name, NNMi A-17
- SNMP Data Synchronization A-20
- SNMP settings for PCM, 7-25
- SNMP Synchronization, NNM/NNMi A-20
- SNMP V2 Credentials 7-26
- SNMP V3 7-14
- SNMP V3 Credentials 7-27
- Software Unlicensing 12-52
- Software update 12-60
- Software Update Wizard 12-61
- software updates 12-60
- software, auto-updates 12-61
- Sorting device lists 2-32
- Spanning Tree Protocol (STP) 16-42
- SSH Access 10-4
- SSH Authentication 10-4
- SSH Credentials 7-31
- SSL

- behind firewall 3-7
- in Client/Server connections 2-7
- Unique certificates 3-16
- start device for discovery 3-24
- Starting device 4-28, 4-33
- Static view 2-34
- statistics polling 11-2
- Status bar 2-27
- status polling interval 3-24
- subnet discovery 4-40
- Subnet maps 5-9
- Substitution List 16-43
- Switch software versions 12-57
- synchronize VLAN name 14-13
- Syslog
 - Acknowledge events 7-48
 - Delete event 7-49
- Syslog events filter 7-48

T

- TACACS
 - authorized IP managers, precedence 7-7
- Telnet Access 10-4
- Telnet Authentication 10-4
- Telnet credentials 7-30
- Test Credentials 3-58
- test credentials 3-58
- test link 3-58
- Third-Party Trap 19-17
- Threshold button 2-22
- thresholds 7-43
 - default values 11-22
- Times
 - changing 16-19
 - delete 16-19
 - properties 16-18
- Toolbars
 - map 5-18
- Top Connections 11-12
- Top Destinations 11-12
- Top Protocols 11-12
- Top Sources 11-12
- Top Talkers 11-11
- Top Traffic Overview 2-23
- Trace Path 4-26
- Traffic Gauge 11-7
- Traffic Link View 5-14

- traffic monitor
 - description 11-2
 - troubleshooting 11-28
- Traffic Overview 11-7
- traffic sampling 11-2
- Traffic Status 2-19
- traffic thresholds 11-20
- Traffic, automatic sampling 11-19
- Traffic, configure thresholds 11-20
- Traffic, data logging 11-24
- Traffic, events 11-18
- Traffic, Line Speeds 11-22
- Traffic, manual mode 11-22
- Traffic, Port Summary 11-14
- Traffic, Preferences 11-25
- Traffic, Rx-Tx 11-10
- Traffic, Statistics Tab 11-14
- transfer license 2-15
- Trap Receiver 3-25
- Tree map 5-10
- Troubleshooting
 - Agent Communication 3-58
 - CIP 19-22, 19-49
 - Client Permissions 2-70
 - Device Communication 7-38, 7-46
 - Discovery 4-57
 - Multi-homes Systems 2-70
 - PCM Services 2-69
 - Traffic Monitor 11-28
- Tune PCM memory
 - local Agent 3-49
 - Server 4-44

U

- UniformLengthEdges 5-10
- Uninstall ID 8-17
- Unknown Devices 2-31
- unlicense software 12-52
- USB Autorun 12-69
- USB Solution 12-69
- user sessions 10-11
- user-defined device 19-9
- User-defined tab 19-15
- Users
 - adding 2-41, 2-45
 - deleting 2-43, 2-48, A-6
 - editing 2-43, 2-47, A-6

show 2-48
utilization 11-12

V

Viewing Events 6-2
Virus Throttle 15-2
VLAN
 dedicated management 14-15
 port options 10-14, 14-4, 14-8, 14-23
 primary 14-15
VLAN link view 5-13
VLAN map 5-9
VLAN Name
 synchronize 14-13
VLAN Properties 14-17, 14-18, 14-19
VLANS
 deleting 14-16
 static, dynamic 14-14
VLANs
 add device 14-10
 create 14-6
 definition 14-2
 listing 14-3
 modify 14-9
 modify ports 10-14, 14-23
 modify support 14-17
 port assignments 10-8, 14-22
 primary 14-15
 remove device 14-13
VT 15-3
VT, Configuration 15-7
VT, filter 15-3
VT, rules 15-5
VT, sensitivity 15-4

W

warranty 1-2
Web Help 2-72
WebAgent Credentials for PCM 7-33

Technology for better business outcomes

To learn more, visit www.hp.com/go/procurve/

© Copyright 2004, 2005, 2007, 2009, 2010 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice. The only warranties
for HP products and services are set forth in the express warranty statements accompanying
such products and services. Nothing herein should be construed as constituting an addi-
tional warranty.



October 2010

Manual Part Number
5998-0573

