System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

Private Network Management Client

OCTOBER 2019

MN003341A01-B

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

Contact Us

The Solutions Support Center (SSC) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions.

Service agreement customers should be sure to call the SSC in all situations listed under Customer Responsibilities in their agreement, such as:

- Before reloading software
- To confirm troubleshooting results and analysis before taking action

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

1. Enter motorolasolutions.com in your browser.
2. Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
3. Select "Support" on the motorolasolutions.com page.

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number or title of the section with the error
- A description of the error

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to https://learning.motorolasolutions.com to view the current course offerings and technology paths.

Document History

Version	Description	Date
MN003341A01-A	Original release of the *Private Network Management Client* manual.	November 2016
MN003341A01-B	Sections updated: • Installing Windows on page 25	October 2019

Contents

List of Figures

List of Tables

List of Procedures

List of Processes

About Private Network Management Client

This manual provides an introduction to the hardware and software components associated with the Private Network Management (PNM) client. Included are the detailed procedures for installation, configuration, and replacing Field Replaceable Units (FRUs).

This manual is intended to be used by field service managers and field service technicians after they have attended the Motorola Solutions formal training for the PNM Client.

What Is Covered In This Manual

This manual contains the following chapters:

- PNM Client Description on page 15 contains an overview of the PC client hardware, PNM Client, and the software applications for McAfee Anti-Malware, as well as specifications and requirements.
- PNM Client Theory of Operations on page 17 provides a list of software installed on the PNM Client.
- PNM Client Installation on page 18 describes the software installation instructions for the PC client.
- PNM Client Configuration on page 29 provides the configuration instructions for setting up the PC client hardware and PNM Client after the software is installed.
- PNM Client Operations on page 33 provides information on how to start, create, display, and exit applications.
- PNM Client Maintenance on page 36 provides instructions for uninstalling the Private Radio Network Manager (PRNM) suite of applications from the PNM Client.
- PNM Client Troubleshooting on page 38 is a reference for where to find operating system or application-specific troubleshooting information.
- PNM Client FRU Information on page 39 lists the Field Replaceable Units (FRUs).
- PNM Client Disaster Recovery on page 40 provides disaster recovery procedures pertaining to PNM Client.
- Local Backup/Restore of PNM Client SSH Data on page 42 contains information on Windows Vista PNM Client SSH Data local backup and restore.
- PNM Printer Security Configuration on page 44 describes configuration of the PNM printer.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known

Related Information	Purpose
	as R56 manual. This may be purchased on CD 9880384V83, by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
System Overview and Documentation	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.
Virtual Management Server Software	Provides procedures for implementing and managing VMware ESXi-based virtual server hosts on the common Hewlett-Packard® hardware platform in an ASTRO® 25 system. Includes common procedures for virtual machines/virtual appliances on the virtual server host.
Virtual Management Server Hardware	Provides information for implementing, maintaining, and replacing common Hewlett-Packard® hardware for servers in an ASTRO® 25 system.
Historical Reports	Covers the use of the Historical Reports software application to generate reports that show system-wide and zone-level historical data for an ASTRO® 25 IV&D system.
Windows Supplemental Configuration	Provides additional procedures that must be performed on all Windows®-based devices in an ASTRO® 25 system, and additional procedures that are performed only for specific Windows®-based devices.
Core Security Management Server	Provides information relating to implementation and management of basic network security software components in an ASTRO® 25 IV&D system. This includes server functions and client functions that support multi-factor RADIUS authentication for remote users accessing the system through a modem and terminal server. Information is also included about the server and client functions for managing system-wide anti-malware protection (including anti-virus and anti-spyware).
Securing Protocols with SSH	Provides information relating to the implementation and management of the Secure Shell (SSH) protocol for secure transmission of data between devices in an ASTRO® 25 system. Includes configuration sequences that minimize downtime when adding this feature to a system that is already in operation.
Unified Event Manager	Covers the use of Unified Event Manager (UEM), the application that provides reliable fault management services for devices in the ASTRO® 25 IV&D radio system.
Backup and Restore Services	Provides information relating to the implementation and management of a backup service for supported devices in an ASTRO® 25 system. This manual addresses server and client functions required for these services, and provides information relating to the implementation and replacement of the Network Attached Storage (NAS) hardware/software component.
Authentication Services	Provides information relating to the implementation and management of the Active Directory (AD) service, Remote Authentication Dial-In User Service (RADIUS), and Domain Name Service (DNS) in ASTRO® 25 systems.

Related Information	Purpose
MAC Port Lockdown	Provides information relating to the implementation and management of MAC Port Lockdown for standard Ethernet ports on Hewlett-Packard®switches and on the internal switch of GCP 8000 site controllers and GPB 8000 Reference Distribution Modules (RDMs), in an ASTRO® 25 system. Also provides information required for supplemental Ethernet port security, including the implementation of fiber optic ports on Hewlett-Packard® switches.

Chapter 1

PNM Client Description

The Private Network Manager (PNM or NM) client workstations are commercial personal computers that run the Microsoft® Windows® operating system for network computers. Authorized system managers or network administrator personnel use the client PC workstations to start and run the software applications for configuring, viewing equipment operational status, and monitoring network utilization and performance.

1.1 PNM Client Hardware

The Hewlett-Packard Z420 and Z440 workstations are the specified hardware platforms for the PNM Client.

1.2 PNM Client Applications Overview

For the list of the PNM Client applications, see the following sections:

- For applications launched from the Motorola Private Radio Network Management (PRNM) Suite, see Motorola PRNM Suite Applications on page 15.
- For applications launched using the web browser, see Applications Launched with the Web Browser on page 16.

1.2.1 Motorola PRNM Suite Applications

FCAPS is a Network Management model intended to maximize the available resources and minimize system downtime and maintenance costs. It consists of five functional areas: Fault Management, Configuration Management, Accounting, Performance Management, and Security Management.

Table 1: Motorola PRNM Suite Applications

Application	FCAPS	Purpose
System-Level Applications:		
System Historical Reports	Accounting, Performance	Application that allows to generate reports for system-wide activity. **NOTICE:** For details on the Custom Historical Reports application, see the *Historical Reports* manual.
Zone-Level Applications:		
Affiliation Display	Performance	Application that displays the association of a radio with a talkgroup and a site,and information about conventional channels, console sites, and consoles.
Air Traffic Information Access (ATIA) Log Viewer	Performance	Application that displays log files generated by the Air Traffic Router server application (ATR) andZoneWatch. These log

Application	FCAPS	Purpose
		files contain records of all recent zone activity, such as site registrations andcalls processed.
Dynamic Reports	Accounting, Performance	Application that provides predefined report templates you can use to display statistics for a zone, site, or a console site in near real time.
Zone Historical Reports	Accounting, Performance	Application that allows to generate reports for individual zones. **NOTICE:** For details on the Custom Historical Reports application, see the *Historical Reports* manual.
ZoneWatch	Fault, Performance	Application that allows monitor radio call traffic for an individual zone in real time. This application uses different Watch Windows that allow to display only the required information.

1.2.2

Applications Launched with the Web Browser

The License Manager, Unified Network Configurator (UNC), Unified Event Manager (UEM), and the Provisioning Manager applications are launched using browser shortcuts. For more information, see Creating a PRNM Suite Application Shortcut on page 33.

Table 2: Applications Launched with the Web Browser

Application	FCAPS	Purpose
License Manager	Accounting	An application for loading licenses, checking license status, and managing licensed application session.
UEM	Fault	A tool that provides reliable fault management services, such as service discovery, fault management, supervision, and synchronization.
UNC	Configuration	An advanced network configuration tool that provides controlled and validated configuration management of system devices. It includes VoyenceControl and Unified Network Configurator Wizards (UNCW). **NOTICE:** The names EMC Smarts™ and VoyenceControl are used interchangeably for this product.
Provisioning Manager	Configuration	A management application used to enter and maintain configuration information for the User Configuration Server (UCS). The Provisioning Manager configures Consoles, CCGWs, AuC, System, Subscribers, Security, and applications (such as ZoneWatch).
Radio Control Manager	Configuration, Security	The Radio Control Manager (RCM) is an application used primarily by dispatchers to monitor and manage radio events, issues; to monitor commands, and make informational queries of the system database. It also enables to present and analyze data showing RCM activity in the system.

Chapter 2

PNM Client Theory of Operations

This chapter provides a list of the Motorola Private Radio Network Manager (PRNM) Suite software installed on the PNM Client.

2.1 Windows Remote Desktop Connection

PNM Client is a remote control software application. You can use it to remotely manage Windows systems.

In the ASTRO® 25 system, the default version of Microsoft Windows Remote Desktop including Remote Desktop for Administration and Remote Desktop Connection that are included with Microsoft Windows OS by default are supported.

For supplemental remote desktop procedures that may be required depending on policies in your organization, see the *Windows Supplemental Configuration* manual.

2.2 McAfee Anti-Malware

The McAfee anti-malware server is located on the Core Security Management Server (CSMS). It performs the following functions:

- Manages and deploys agents on Windows and Red Hat Linux devices
- Manages, deploys, and enforces McAfee ePO* product policies
- Distributes updates to McAfee clients for new McAfee products, upgrades, and patches
- Provides status for the McAfee implementation and manages clients through predefined or customized reports

* McAfee® ePolicy Orchestrator (ePO) is the McAfee anti-malware server software. For more information, see the *Core Security Management Server* manual.

Chapter 3

PNM Client Installation

This chapter details installation procedures relating to the PNM Client.

NOTICE: After the initial installation, all procedures assume that you are already accessing PNM Client.

For procedures and related information in the virtual environment, see the *Virtual Management Server Software* manual.

3.1

PNM Client Installation Prerequisites

Table 3: PNM Client Software Installation Media

Software/Optical Media	Description/Version	Provided with:	
		Z420/Z440	Virtual Machine (VM)
Microsoft Windows Operating System Installation DVD	Windows 10	✓	✓
Motorola Windows CommonOS Box Profile	Current certified version	✓	✓
Motorola Windows 10 OS image (for z420/z440)	Current certified version	✓	✗
Motorola Windows 10 OS image	Current certified version	✗	✓
Private Network Management (PRNM) Suite Client Application CD	Current certified version	✓	✓
Windows Supplemental Media	Current certified version	✓	✓
MOTOPATCH for Windows DVD	Current certified version	✓	✓

For additional prerequisites specific to the virtual environment, see the *Virtual Management Server Software* manual.

3.2

IP Addresses and Login Information

Before performing procedures from this manual, locate the following information pertaining to the PNM Client (see your system documentation or contact your system administrator):

- IP address
- Subnet mask
- Gateway
- Primary DNS

- Alternate DNS
- Administrative login and password

3.3 Installing the PNM Client

Process:

1. Perform one of the following actions, depending on your installation hardware/environment:
    - If you are installing the PNM Client on the HP Z420 or Z440 workstation, perform the following actions:
        1. Turn on the workstation.
        2. Install Windows. See Installing Windows on page 25
    - If you are installing the PNM Client as a Virtual Machine on an ESXi-based Virtual Server, perform the following actions:
        1. Make sure that the installation/configuration process for virtual server host has been completed. See the *Virtual Management Server Hardware* and *Virtual Management Server Software* manuals.
        2. Import the PNM Client Virtual Machine. See Importing the Virtual Machine on page 20.
        3. Set the correct startup and shutdown order. See Setting the Virtual Machine Startup and Shutdown Order on page 22.
        4. Configure the PNM Client Virtual Machine. See Configuring Virtual Machine Resources on page 24.
        5. Turn on the PNM Client Virtual Machine you imported. See the “Turning On an Individual Virtual Machine” section in the *Virtual Management Server Software* manual.
2. Apply OS-Level Identity on the PNM Client. See Applying OS-Level Identity on the PNM Client on page 26
3. Perform one of the following actions:
    - If you are installing the PNM Client as a Virtual Machine on an ESXi-based Virtual Server, perform the “Upgrading VMware Tools on Windows-Based Virtual Machine” procedure from the *Virtual Management Server Software* manual.
    - If you are installing the PNM Client on the HP Z420 or Z440 workstation, go to step 4.
4. Change the Windows login warning banner and title. See the “Changing Logon Banners Locally” section in the *Windows Supplemental Configuration* manual.
5. Optional: If a printer (local or network) is present in your system, install it.

    See the printer's vendor documentation.
6. Into the optical drive, insert the latest *Windows Supplemental* media and install the needed common software.

    See the“Windows Supplemental Media Contents” section in the *Windows Supplemental Configuration* manual.

    Common software:

    - Network Management Client (`NETWORK_MANAGEMENT_CLIENT.xml`)
    - Backup and Restore Client * (`Motorola Windows Bar Client.xml`)
    - Centralized Event Logging Client * (`Motorola Windows Logging Client.xml`)

* Optional features. For additional information, see Centralized Event Logging Client and Backup and Restore Client Installation on page 27.

  a. Open the **Command Prompt**. On the *Windows Supplemental Media*, navigate to the `wif` folder.

  b. To install the components, enter: `WindowsInstallFramework.exe /e /i` ***<feature name>***`.xml`

     You can include one, two, or three ***<feature name>***`.xml` parameters separated with a space.

     Insert quotation marks around filenames that contain spaces.

  During the installation, the machine may reboot several times. When this occurs, you have to confirm user access to continue.

7. At the installation finished message, click **OK**.
8. Optional: If you are installing the PNM Client on the HP Z420 or Z440 workstation, and if it is going to be used to access an ESXi Server and other virtual elements of the system, perform the following actions:

   a. Install a vSphere Client application. See “Installing the VMware vSphere Client on Windows-Based Devices” in the *Virtual Management Server Software* manual.

   b. Install VMware PowerCLI. See “Installing VMware PowerCLI” in the *Virtual Management Server Software* manual.
9. Ensure that the date, time, and time zone are set correctly.
10. Install the **Motorola PRNM Suite** of applications. See Installing the Motorola PRNM Suite of Applications on page 26.
11. Install the ASTRO® 25 system documentation set. See ASTRO 25 System Release Documentation Set Installation on page 28.
12. For local user secmoto perform Changing Password for Windows User Account on page 30.
13. Install patches for the operating system. See MOTOPATCH for Windows on page 30.
14. Perform “Joining and Rejoining a Windows-Based Device to an Active Directory Domain with a Script” from the *Windows Supplemental Configuration* manual.
15. Complete all procedures from the “Common Windows Procedures” chapter in the *Windows Supplemental Configuration* manual, including:
    - “Boot Order for Windows Devices (Not for Virtual Machines)”
    - “Configuration Using the ASTRO 25 System Windows Supplemental Media User Interface”
    - “Deploying McAfee Anti-Malware From the CSMS”
    - “Changing Logon Banners Through a Domain Controller”
16. If your organization can generate Point-to-Point (PTP) certificates (such as a valid certificate authority), install them now. See Installing PTP Certificates on PNM Client for Each PTP Radio on page 31.

3.4 Importing the Virtual Machine

Importing a virtual machine may take approximately an hour, depending on network traffic and disk usage.
For information about the Direct Attached Storage (DAS) device, see the *Virtual Management Server Software* manual.

Prerequisites: Obtain the following media and information:

- *Motorola Windows 10 OS image*
- IP address of the ESXi-based server (Virtual Management Server host)
- ESXi-based server root account password
- Hostname for the device that you are importing
- Zone network for the virtual machine

Procedure:

1 From a Windows-based device, launch the VMware vSphere Client.

A desktop shortcut was created during installation.

A dialog box appears prompting for an IP address, user name, and password.

2 Log on to the server by entering the IP address of the ESXi server, `root` in the user name field, and the appropriate password in the password field.

3 In the **vSphere Client Inventory** window, perform one of the following actions:

- If you are installing from the DVD, insert the media listed in the prerequisites in the DVD drive of the device where the vSphere Client resides.
- If you are not installing from the DVD, determine the location of the following file: `Win10-OVF-aa.bb.cc.dd`

4 Select **File → Deploy OVF Template**.

5 In the **Deploy OVF Template – Source** window, click **Browse**.

A window displays file directories.

6 Perform the following actions:

a Navigate to the file location.

b Select the file:

`Win10-OVF-aa.bb.cc.dd`

c Open the file.

d Click **Next**.

7 In the **Deploy OVF Template – OVF Template Details** window, click **Next**.

8 In the **Deploy OVF Template – Name and Location** window, perform the following actions:

a In the **Name** field, enter the appropriate host name.

Step example: Enter: `z001nmc01`

b Click **Next**.

9 Optional: If the **Resource Pool** window appears, click on the IP address of the server. Click **Next**.

10 If the **Datastore** window appears, perform the following actions:

a Select a datastore to install the virtual machine upon.

Always select: `z00`***<X>***`das`***<YY>***`_datastore1`

where:

<X> is the zone number. The possible values are: 1-7.
<YY> is the instance of the Direct Attached Storage (DAS).

b Click **Next**.

11 In the **Deploy OVF Template – Disk Format** window, perform one of the following actions:

- If the **Thick Provision Eager Zeroed** format is an available option, select it.
- If that option is not available, select **Thick Provision**.

12 Click **Next**.

13 In the **Deploy OVF Template – Network Mapping** window, select the appropriate **Destination Network** for each **Network Source**.

For a zone-level PNM Client, select **znm0**.

14 Click **Next**.

15 In the **Deploy OVF Template – Ready to Complete** window, verify the deployment settings. Click **Finish**.

The import starts.

16 When the process is completed successfully, verify that the left pane of the **vSphere Client** main window displays the application virtual machine name. You may need to expand the list in the left pane to locate the virtual machine name.

17 In the **Deployment Completed Successful** window, click **Close**.

18 Optional: If you used the DVD, remove it from the DVD drive.

3.5 Setting the Virtual Machine Startup and Shutdown Order

In an ASTRO® 25 system, virtual machines hosted on a Virtual Management Server (VMS) are configured to boot automatically with the system in a prescribed order. When you install a virtual machine on a VMS, change the VMS settings to ensure that the new virtual machine boots in the correct order with respect to the other virtual machines hosted on the VMS.

Procedure:

1 From a Windows-based device, launch the VMware vSphere Client.

A desktop shortcut was created during installation.

2 Log on to the server as a user with root privileges.

3 On the upper left side of the **vSphere Client Inventory** window, select the ESXi server.

4 On the right side of the window, select the **Configuration** tab.

The window displays information about the configuration of the ESXi server.

5 In the **Software** section, select **Virtual Machine Startup/Shutdown**.

6 On the right side of the main window, select **Properties**.

7 In the **System Settings** area, select **Allow virtual machines to start and stop automatically with the system**.

8 In the **Default Startup Delay** area, select **Continue immediately if the VMware Tools start**.

9 In the **Default Shutdown Delay** area, from the **Shutdown Action** drop-down list, select **Guest Shutdown**.

10 Put the virtual machines hosted on the ESXi server in the correct boot order:

a In the **Startup Order** area, from the **Automatic Startup** list, select a virtual machine.

b By using the **Move Up** and **Move Down** buttons, move the virtual machine to the correct ordered slot.

NOTICE:
Zone Core Virtual Machine Boot Order on page 23 outlines the boot order for the virtual machines that can reside on an ESXi-based Zone Core Virtual Management Server (VMS).

To determine the correct ordered slot for each virtual machine hosted on the ESXi server that you are configuring, see the boot order table.

c Repeat step 10 a and step 10 b until the boot order for the virtual machines is correct.

11 Click **OK**.

The **Properties** window closes.

3.5.1 Zone Core Virtual Machine Boot Order

NOTICE:
Up to two instances of the GMC can be on the server.

If UNCDS is present, three instances of the UNCDS are on the server.

Table 4: Zone Core Virtual Machine Boot Order

Order		Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Automatic Startup						
	1	ZC	Enabled	Use Default	Use Default	Use Default
	2	Transcoder	Enabled	Use Default	Use Default	Use Default
	3	ISGW	Enabled	Use Default	Use Default	Use Default
	4	PDG-Conv	Enabled	Use Default	Use Default	Use Default
	5	PDG-HPD	Enabled	Use Default	Use Default	Use Default
	6	PDG-IV&D	Enabled	Use Default	Use Default	Use Default
	7	License Manager	Enabled	Use Default	Use Default	Use Default
	8	ATR	Enabled	Use Default	Use Default	Use Default
	9	DC-System	Enabled	Use Default	Use Default	Use Default
	10	DC-Zone	Enabled	Use Default	Use Default	Use Default
	11	IPCAP	Enabled	Use Default	Use Default	Use Default
Any Order		AuC	Enabled	Use Default	Use Default	Use Default
		BAR	Enabled	Use Default	Use Default	Use Default
		CSMS	Enabled	Use Default	Use Default	Use Default
		InfoVista	Enabled	Use Default	Use Default	Use Default
		FMS – Fortinet	Enabled	Use Default	Use Default	Use Default
		GDG	Enabled	Use Default	Use Default	Use Default
		GMC	Enabled	Use Default	Use Default	Use Default
		NM Client	Enabled	Use Default	Use Default	Use Default
		UCS	Enabled	Use Default	Use Default	Use Default

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
	SSS	Enabled	Use Default	Use Default	Use Default
	Syslog	Enabled	Use Default	Use Default	Use Default
	UEM	Enabled	Use Default	Use Default	Use Default
	UNC	Enabled	Use Default	Use Default	Use Default
	UNCDS	Enabled	Use Default	Use Default	Use Default
	vCenter App	Enabled	Use Default	Use Default	Use Default
	ZDS	Enabled	Use Default	Use Default	Use Default
	ZSS	Enabled	Use Default	Use Default	Use Default
Manual Startup	DESU Waypoint	Disabled	Use Default	Use Default	Use Default

3.6 Configuring Virtual Machine Resources

Common OS-based Virtual Machines (VMs) require a device-specific resource profile to be applied to improve their performance and resource utilization of the ESXi Server.

You can change VM resource configuration by running the script that is part of the **Motorola VM Automation Tools** package on the *Windows Supplemental* media. To perform this procedure, use a Windows-based device, such as the Network Management (NM) Client, or a service computer/laptop.

Prerequisites:
Obtain the *Motorola Windows Box Profile* media (provided by Motorola Solutions; contains initial setup for individual devices and initial configuration scripts; drivers for Windows client and server).

Install VMware PowerCLI on the Windows-based device. See "Installing VMware PowerCLI" in the *Virtual Management Server Software* manual.

Install **Motorola VM Automation Tools** on the Windows-based device. See the *Windows Supplemental Configuration Setup Guide*.

Ensure that the virtual machine is powered down.

Procedure:

1 Insert the *Motorola Windows Box Profile* media into the optical drive of the Windows-based device.

2 Open the PowerShell command prompt.

   a From **Start**, click **Search**.

   b In the search field, type: `powershell`

   c Right-click **Windows PowerShell** and select **Run as administrator**.

   d If the **User Account Control** window appears, click **Yes**.

   If you are not logged on with an administrative account, enter the Administrator's credentials.

3 At the PowerShell prompt, enter:
```
cd 'C:\Program Files\Motorola\Motorola VM Automation Tools\bin'
```

4 At the PowerShell prompt, enter: `.\Execute_VM_Resource_Config.ps1`

5 At the `ESXi_IP` prompt, enter the IP address of the ESXi host.

6 At the `ESXi_acct` prompt, enter: `root`

7 At the `ESXi_password` prompt, enter the ESXi host password for the root account.

8 At the `VMName` prompt, enter the name of the virtual machine that you want to configure.

9 At the `VMResourceFile` prompt, enter the path to the `xml` file with resource configuration:

   For the Private Network Management (PNM) Client: ***<cdrom>*****:**`\VM_Resource_Config\NM_Client_Resource.xml`

   where ***<cdrom>*** is the drive letter, for example: `E:`

10 Verify that there are no error messages in the output of the script.

11 At the PowerShell prompt, enter: `exit`

3.7
PNM Client Windows OS Installation

This section covers the installation of the Windows operating system.

3.7.1
Windows OS Software Media

Table 5: Media Software Required for Installation

Required Media	Description
Motorola Windows 10 OS Image	Installs Windows® on Z420/Z440.

3.7.2
Installing Windows

To install the Windows Operating System (OS), use the Motorola Windows 10 OS Image media that came with your system (see Windows OS Software Media on page 25), or use an updated version of this installation media, if appropriate. The media supports Windows OS installation and configuration (local) by minimizing the amount of wait time normally experienced to install.

NOTICE: PCs purchased from Motorola Solutions are shipped with Windows 10 IoT Enterprise. Certified workstations marked with a yellow sticker contain a genuine copy of the Microsoft operating system that does not require Windows Activation.

Procedure:

1 Insert Motorola Windows 10 OS Image into DVD drive.

2 Make sure device is booting from DVD drive.

3 On the Common Operating System boot prompt select Install Windows option and confirm with **Enter**.

4 Windows Preinstallation Environment starts. Choose one option from the 3 buttons that are available for 30 seconds:

   - **Preserve partitions** - removes only partition C:
   - **Delete all partitions** - removes all partitions (including partition D:)
   - **Reboot** - no action is taken

5 Wait until OS image in unpacked and restored.

3.8 Applying OS-Level Identity on the PNM Client

Perform this procedure to apply Operating System (OS) configuration to the PNM Client.

Prerequisites: Obtain the *Motorola Windows CommonOS Box Profile* media.

When and where to use: If the PNM Client is a virtual machine: If the message `Click Cancel to continue without the hostcfg.ini` appears in the VM console window, click **Cancel** and wait for an OS reboot.

Procedure:

1. Insert the *Motorola Windows CommonOS Box Profile* media into the optical drive.

   The **Common OS Reconfigurator** launches automatically.
2. In the **Common OS Reconfigurator** attention window, at the **Do you want to configure computer and apply Box Profile** prompt, click **Yes**.
3. In the **Common OS Settings** window, from the **Computer Type** drop-down list, select the **Network Management Client** in the appropriate location.

   The following locations (as displayed on screen) are available:

   - **Backup UCS Subnet**
   - **Backup Zone ZNM Subnet**
   - **CSub location**
   - **non T-Sub Console Site**
   - **Primary UCS Subnet**
   - **Primary Zone ZNM Subnet**
   - **T-Sub Console Site**
4. Select the appropriate values for Astro Settings (if available).
5. Enter the appropriate values in the **Full Computer Name**, **Primary Lan**, and **Time Synchronization** fields.

   Some fields may be already filled in. If so, make sure that the values are correct.
6. Make the appropriate selections from the **Time Zone** and **Keyboard Layout** drop down lists.
7. Click **Execute**.
8. Wait for an OS reboot.

3.9 Installing the Motorola PRNM Suite of Applications

The **Motorola PRNM Suite** is typically installed on a PNM Client when shipped from Motorola Solutions.

Prerequisites:
Ensure that the date, time, and time zone are set correctly.

Obtain the *Private Network Management (PRNM) Suite Client Application CD*.

Procedure:

1. Log on to the PNM Client using an account with administrative privileges.
   - If using a domain administrative account, make sure that the Active Directory domain is entered before the user name in the format ***`<domain>`*****\*****`<user name>`***.

- If using a local administrative account, make sure to enter the host name before the user name in the format ***<host name>\<user name>***.

2 Insert the *Private Network Management (PRNM) Suite Client Application CD* into the optical drive of the client.

To learn how to use CD/DVD drive in virtual environment, see the “Installing or Transferring Files to a Virtual Machine” section in the *Virtual Management Server Software* manual.

3 Navigate to the CD and double-click the `PrnmSuite_install.bat` file.

If a **User Account Control** dialog box displays, click **Allow** or **Yes** or **Continue**.

The WIF execution log window appears.

- Installation of software prerequisites starts. The WIF execution log displays the status of prerequisites installation.
- When installation is complete, the **Motorola – InstallShield Wizard** dialog box appears.

4 Click **Next**.

5 In the **License Agreement** dialog box, select **I accept the terms in the license agreement**. Click **Next**.

6 In the **Ready to Install the Program** dialog box, click **Install**.

7 Perform one of the following actions:

- If the critical data backup is detected, you are asked if you would like InstallShield to restore the data. Go to step 8.
- If not, go to step 9.

8 Perform one of the following actions:

- If you want to restore the critical data, click **Yes**.
  - The Installing Motorola Private Radio Network Management Suite dialog box appears. The progress bar on the dialog box indicates installation progress.
  - When installation is complete, the **InstallShield Wizard Completed** dialog box appears.
- If not, click **No**.

9 Click **Finish**.

10 Click **OK** to close the WIF execution log.

11 Remove the *Private Network Management (PRNM) Suite Client Application CD* from the optical drive.

If installing in virtual environment, disconnect the CD-DVD drive. See the “Installing or Transferring Files to a Virtual Machine” section in the *Virtual Management Server Software* manual.

12 Reboot the PNM Client. See Rebooting the PNM Client on page 28.

3.10 Centralized Event Logging Client and Backup and Restore Client Installation

For information on installing the Centralized Event Logging client and the Backup and Restore client, see “Installing Components Located on the Windows Supplemental Media” in the *Windows Supplemental Configuration* manual and use their respective parameters.

3.11 ASTRO 25 System Release Documentation Set Installation

ASTRO® 25 system documentation from Motorola Solutions is delivered on a USB drive or other media when the system is commissioned. Follow the instructions provided with the media to install the documentation on the network management client workstation.

Your system must have Adobe Reader and a web browser installed to access the documentation. If your system does not have Adobe Reader, install the application using the option provided during the installation procedure.

3.12 Rebooting the PNM Client

Procedure:

1. From the taskbar, select **Start** → **Power**.
2. Select **Restart**.

   The PNM Client reboots.

Chapter 4

PNM Client Configuration

After the initial configuration, all procedures assume that you are already accessing PNM Client.

For procedures and related information on virtual environment, see the *Virtual Management Server Software* manual.

4.1 Network Time Protocol (NTP) as the ASTRO 25 Time Source

The Domain Controllers are time sources for Windows-based devices that are joined to the Active Directory domain.

Whenever a device that is part of a Windows Active Directory domain interacts with a Domain Controller, the time from the device is included in the messages. If the time the device supplies in the message differs by a certain amount of time compared to the time on the DC, that message is considered invalid.

The Domain Controllers get their time from the ASTRO® 25 system Network Time Protocol (NTP) servers. The hostnames of the NTP servers for the Domain Controllers depend on whether Dynamic System Resilience (DSR) is implemented:

Table 6: Domain Controller NTP Elements and Configuration

Location of the Domain Controller:	Non-DSR 1st NTP Source	Non-DSR 2nd NTP Source	DSR 1st NTP Source	DSR 2nd NTP Source
Primary Core	N/A	N/A	`ntp02.zone`***<Z>****	`ntp03.zone`***<Z>***
Backup Core	N/A	N/A	`ntp05.zone`***<Z>***	`ntp06.zone`***<Z>***
Zone Core	`ntp02.zone`***<Z>***	`ntp03.zone`***<Z>***	N/A	N/A
Tsub Prime Site**	`ntp02.zone`***<Z>***	`ntp03.zone`***<Z>***	`ntp02.zone`***<Z>***	`ntp05.zone`***<Z>***

* where ***<Z>*** is the zone to which the DC belongs

** For the Trunking Subsystem (Tsub) Domain Controllers, while there is no backup Tsub when a system is DSR-enabled, the time source configuration is dependent on the DSR configuration of the host zone core. The non-DSR configuration applies to Tsub DC when the host zone core is non-DSR. The DSR configuration applies to Tsub DC when the host zone core is DSR.

The Domain Controller configuration script specifies the NTP servers that Domain Controllers use (you do not need to enter this information when installing and configuring Domain Controllers.)

For more information about NTP configuration in an ASTRO® 25 system, see the following manuals:

- *Network Time Protocol Server*
- *Virtual Management Server Software*

If the time source needs to be configured before configuring RADIUS, see the *Network Time Protocol Server* manual and the appropriate manual for the configured device.

4.2 Windows Login Warning Banners

Change the Windows Login Warning Banner only if it is required by your organization's policies.

For information on how to change the Windows Login Warning Banner using Windows, see the "Changing Logon Banners Locally" section in the *Windows Supplemental Configuration* manual.

4.3 Printer Installation

If a printer (local or network) is present in your system, follow the printer's vendor documentation to install it on PNM Client.

4.4 MOTOPATCH for Windows

The *MOTOPATCH for Windows DVD* may contain patches applicable to your system. Be sure to thoroughly review the `README.txt` file on the MOTOPATCH media as it contains information on system preparation and operating instructions for MOTOPATCH installation.

Before installing in the virtual environment, connect the virtual machine to the DVD drive where you want to insert the software media. For information about connecting DVD drives to virtual machines, see the *Virtual Management Server Software* manual.

The *MOTOPATCH for Windows DVD* is a dynamic product, which changes each month in response to new security vulnerabilities. Your system was shipped with the latest version of the *MOTOPATCH for Windows DVD* available at that time. Use its latest version and review the `README.txt` file as it may include new information pertaining to your specific system. For information on obtaining the latest version, contact the Motorola Solution Support Center (SSC).

4.5 Common Windows Procedures

Follow the procedures in the "Common Windows Procedures" chapter of the *Windows Supplemental Configuration* manual.

4.6 Changing Password for Windows User Account

Use this procedure to change the password for a Windows uer account.

Procedure:

1. Log on to the PNM Client using the account that needs a password change.
   - If using a domain account, make sure that the Active Directory domain is entered before the user name in the format ***<domain>\<user name>***.
   - If using a local account, make sure that the hostname is entered before the username in the format ***<hostname>\<user name>***.
2. Perform the following actions:
   a. Press CTRL + ALT + DELETE.
   b. Click **Change Password**.

   If you are accessing a Windows-based virtual machine using VMware vSphere Client, pressing CTRL + ALT + DELETE displays the Windows Security dialog box for the Windows-based device hosting the vSphere application, even if the cursor is in the console for the Windows-based virtual machine.

For more information about interacting with virtual machines, see the *Virtual Management Server Software* manual.

The **Change Password** window appears.

3 Perform the following actions:

   a In the **Old Password** field, enter the current password.

   b In the **New Password** field, enter the new password.

   c In the **Confirm Password** field, enter the new password again.

   A confirmation message appears.

4 To exit, click **OK**.

4.7
PTP Certificates

You can launch the PTP web management application from the UEM within each PNM Client. However, first install the valid certificates into each PNM Client. Currently, there is a set of default certificates that have been installed as part of PNM Client installation to enable users to launch PTP web management application successfully:

- `root_cert astro-ca.crt` is a default PTP ASTRO®25 system root certificate installed to allow the browser to validate the default PTP public certificate. Without it, the browser displays an “untrusted certificate” warning every time a user launches PTP web application.
- `public_cert ptp-astro.der` is the default PTP public certificate for use in ASTRO® 25 systems. It is not tied to a specific device, so a web browser indicates an “invalid certificate”. It is not secure and is used for a bootstrapping purpose only.

If full IA capabilities are available (example: users have a valid Certificate Authority), then a unique certificate should be generated for each PTP radio. Example: you can create a PTP ASTRO® 25 Root Certificate (one for all PNM Clients) along with a PTP public certificate for each PTP radio.

To install the certificates, see Installing PTP Certificates on PNM Client for Each PTP Radio on page 31.

4.7.1
Installing PTP Certificates on PNM Client for Each PTP Radio

Procedure:

1 Generate the root certificate and PTP public certificate through a valid Certificate Authority (CA) and place them into PNM Client.

   Step example: Save them on the Desktop of the PNM Client.
   The certificates for your organization are stored locally.

2 Right-click a certificate file and select **Install certificate**.

3 At the **Certificate Import Wizard** window, click **Next**.

4 At the **Certificate Store** window, select the **Automatically select the certificate store based on the type of certificate** option. Click **Next**.

5 At the **Completing the Certificate Import Wizard** window, click **Finish**.

NOTICE: The certificates should be installed under the following sections within the **Certificates** section under the **Contents** tab within the **Internet Options** window of the browser.

- ***`<root certification file>`*** – “Trusted Root Certificate Authorities” section
- ***`<public PTP certificate file>`*** – “Intermediate Certificate Authorities” section

The **Success** window appears.

After the installation of certificates completes, you are able to access the PTP web application securely. For more information, see the *Unified Event Manager* manual.

Chapter 5

PNM Client Operations

This chapter details tasks that you perform once the PNM Client is installed and operational on your system.

5.1 Creating a PRNM Suite Application Shortcut

Follow this procedure to create desktop shortcuts for **Motorola PRNM Suite** applications and web-launched applications.

Application shortcuts are generated for all installed **Motorola PRNM Suite** applications and web-launched applications upon login to Windows, based on zones provided by Active Directory (depending on policies in your organization).

The system manager assigns permissions to each user in the system. These permissions determine which applications, security groups, and objects you can access. However, each application shortcut can be opened by a user with different permissions (example: through the `runas` command).

Procedure:

1. Double-click the **Motorola PRNM Suite** icon on your desktop.
2. From the **Explorer** window, select one of the following items:
   - A system-level application from the content pane.
   - A zone from the navigation pane, and then a zone-level application from the content pane.
   - Open the Primary Master Site folder.
   - Open the Primary Zone Core folder, and then open a zone folder.
   - Only if the Dynamic System Resilience feature is enabled, open the Backup Master Site folder.
   - Only if the Dynamic System Resilience feature is enabled, open the Backup Zone Core folder and then open a zone folder.
3. Drag the application icon where you want it to appear on the desktop.

   NOTICE: Creating a desktop shortcut removes the application from the Explorer window. To leave the application icon in the window, copy the application icon to the desktop by holding down the CTRL key and dragging the icon to where you want it to appear.

   The application icon appears on the desktop.

5.2 Opening Applications from the Explorer Window

Procedure:

1. Double-click the **Motorola PRNM Suite** icon on your desktop.
2. From the Windows Explorer window, perform one of the following steps:
   - If you want to run a system-level application from the primary master site, open the **Primary Master Site** folder.

- If you want to launch a zone-level application, open the **Primary Zone Core** folder and then open a zone folder.
- If the Dynamic System Resilience feature is enabled and you want to run a system-level application from the backup master site, open the **Backup Master Site** folder.
- If the Dynamic System Resilience feature is enabled and you want to run a zone-level application from the backup master site, open the **Backup Zone Core** folder and then open a zone folder.

The selected folder opens.

3 Double-click an icon of an application you want to run.

The application opens.

5.3
Checking the User Identity

When and where to use: Perform this procedure to locate the list of **Motorola PRNM Suite** user IDs.

NOTICE: User IDs are the same for both Windows and the **Motorola PRNM Suite**.

Procedure:

1 To access the Run command dialog box, press the WINDOWS + R.

2 Enter: `sysdm.cpl`

3 Optional: If a **User Account Control** dialog box appears, click **Allow**, **Yes**, or **Continue**.

4 On the **Advanced** tab, in the **User Profiles** field, click **Settings**.

The list of users is displayed.

5.4
Run Command

The Run command is an efficient way to open programs, files, or web sites.

To access the Run command dialog box, press WINDOWS + R.

For more information on the Run command, see the “Start a program by using the Run command” topic in your operating system online help.

5.5
Centralized Backup and Recovery for PNM Clients

This section provides information about centralized backup and recovery for Private Network Management (PNM) clients in an ASTRO® 25 system that includes a Backup and Recovery Server (BAR server), if implemented in your system.

NOTICE: If secure protocols are used for communication with the BAR server, then correctly configure secure protocols, provision SSH keys, and register the device. See the SSH configuration process for centralized backup and restore in the *Securing Protocols with SSH* manual.

5.5.1
Restoring Critical Data to a PNM Client from the Backup and Recovery Server

Back up a PNM Client whenever critical data on the client changes. Critical data types for a PNM Client include SSH keys, password vault, and configuration (including secure settings).

To back up a PNM Client, schedule a backup to the Backup and Recovery Server (BAR server), selecting the PNM Client for backing up. For details see the *Backup and Restore Services* manual.

Procedure:

1. Connect to the Backup and Recovery Server (BAR server) and log on using the administrative account for the Backup and Restore (BAR) Service.
2. Execute a client data restore, selecting the PNM Client as the client for restoring.
3. Verify the successful completion of the restore. See “Reporting Restore Results” in the *Backup and Restore Services* manual.

Chapter 6

PNM Client Maintenance

This chapter describes the periodic maintenance procedures relating to PNM Client.

There are no serviceable parts in the PC client or PNM Client that require maintenance or calibration. Exterior cleaning by the user using a clean, lint-free cloth, or soft brush is sufficient. It is also advisable to do periodic interior cleaning of the cooling fan, power supply, and boards by using a low-suction vacuum cleaner.

Since PNM databases are not on the PNM Client PC and the PNM Client application does not consume much space on the hard drive, regular PC maintenance is enough for the PNM Client. The PNM Client PC should solely be used for PNM Client activity. If you install any extra applications, they can cause the PNM Client to malfunction.

Keep a minimum of 5 GB free space on the hard drive at all times.

6.1 Uninstalling the PRNM Suite of Applications

Do not uninstall common components that apply to NM Client from the system. You can remove them only after you uninstall the PRNM Suite. For details on how to check which components apply to the NM Client, see “Installing Components Located on the Windows Supplemental Media” in the *Windows Supplemental Configuration* manual.

Use this procedure to uninstall the **Motorola PRNM Suite** applications. This procedure does not uninstall other components installed from the Windows Supplemental Media as prerequisites in step 6 of Installing the PNM Client on page 19.

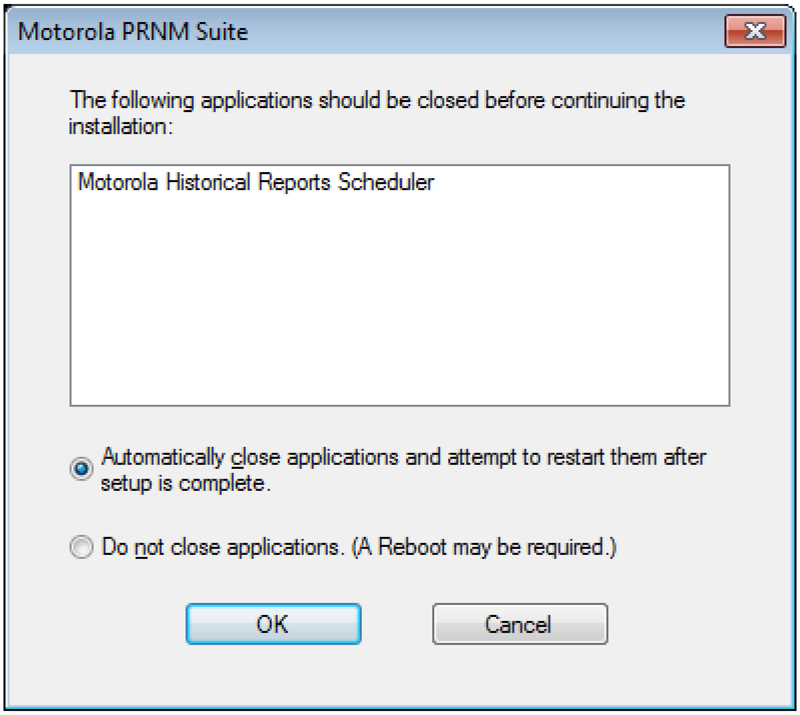
Prerequisites:
Close **Motorola PRNM Suite** applications.

Procedure:

1. Log on to Windows using a local administrative account (the account name set up by Motorola is secmoto for Windows-based devices), or Active Directory administrative account.
   - If using a domain account, make sure that the Active Directory domain is entered before the user name in the format ***<domain>\<user name>***.
   - If using a local account, make sure that thehost name is entered before the user name in the format ***<host name>\<user name>***.
2. To open the **Run** dialog box, press WINDOWS ICON + R.
3. In the **Run** dialog box, enter: `appwiz.cpl`
4. Right-click **Motorola PRNM Suite**. From the context menu, select **Uninstall**.
5. When prompted to confirm that you want to unistall the suite, click **Yes**.

   If a **User Account Control** dialog box appears, click **Allow**, **Yes**, or **Continue**.

   The following messages may appear:
   ```
   The setup must update files or services that cannot be updated while
   the system is running. If you choose to continue, a reboot will be
   required to complete the setup.
   ```
   or;



Motorola PRNM Suite

The following applications should be closed before continuing the installation:

Motorola Historical Reports Scheduler

● Automatically close applications and attempt to restart them after setup is complete.

○ Do not close applications. (A Reboot may be required.)

Click **OK**.

6 When the message appears: `Would you like InstallShield to back up your critical data? The backup may be used while installing PRNM Suite next time to restore or migrate the data.`

perform one of the following actions:

- To back up the critical data, click **Yes**.
- To skip backing up the critical data, click **No**.

A dialog box may appear asking you to close the Java Platform SE binary application.

7 If a dialog box asking you to close the Java Platform SE binary application appears, click **Yes**.

8 If a popup window with information about a necessary reboot appears, click **Yes**.

Chapter 7

PNM Client Troubleshooting

This chapter contains information on PNM Client troubleshooting procedures.

For detailed information on the Operating System, see the Windows help and the specific Network Management application manuals within the ASTRO® 25 system documentation set for more information on those applications.

7.1

Embedded Passwords

Embedded accounts have passwords that must match on all peer devices. Motorola Solutions sets up default passwords that match on all peer devices. However, problems may occur when, on all peer devices, the embedded passwords are:

- not changed all at the same time
- not set to the same value

For detailed information, see the "Embedded Password Management" appendix in the *Authentication Services* manual.

7.2

Regenerating Invalid Applications Shortcut

Shortcuts are being regenerated only in the native "Motorola PRNM Suite" windows explorer window.

In case an invalid applications` shortcut is generated (the shortcut does not work, and the ↗ icon shows), perform the following:

Procedure:

1. Remove the shortcut.
2. Close the window.
3. Open **Motorla PRNM Suite** again.

Chapter 8

PNM Client FRU Information

This chapter lists the Field Replaceable Units (FRUs).

8.1

PNM Client Field Replaceable Units

Table 7: PNM Client Field Replaceable Units

Item Description	Part Number
Certified Network Management ASTRO® 25 System Workstation (Z420 or Z440)	N/A (see the Motorola model number)
HP DL380 Gen8 HC Virtual Server without Software (for L1 system configuration)	DLN6863A
HP DL380 Gen8 HC – DAS 300 Virtual Server without Software (for L2 system configuration)	DLN6822A
HP DL380 Gen9 HC Virtual Server without Software	DLN6974A
HP DL380 Gen9 HC – DAS 900 Virtual Server without Software	DLN6975A

Chapter 9

PNM Client Disaster Recovery

This chapter provides references and information that enable you recovering PNM Client in the event of a failure.

9.1 Recovering the PNM Client

Process:

1. Back up data. See Backing Up the PNM Client SSH Data on page 42.
2. **If you replace your PC hardware:** If Media Access Control (MAC) Port Lockdown is enabled, unlock the HP Switch Port corresponding to the failed client.

   Perform steps related to disabling the MAC Port Lockdown from the “Unlocking/Locking HP Switch Ports When Replacing Connected Devices” in the *MAC Port Lockdown* manual.
3. Optional: If you replace your PC hardware, set up the new hardware and connect the PC to the switch.
4. If MAC Port Lockdown was enabled at the beginning of the device recovery, verify that the new MAC address has been learned by the HP Switch, then re-enable MAC Port Lockdown.

   a Obtain the MAC address of the recovered PNM Client. Verify that the HP Switch has learned the new MAC address before locking down the port again.

      1. Log on to the PNM Client using the valid administrator account.
      2. To open the **Run** dialog box, press WINDOWS ICON + R.
      3. Enter: `ipconfig /all`
      4. Under **Ethernet Adapter Local Area Connection**, in the **Physical Address** field, locate the MAC address.

   b Enable MAC Port Lockdown.

      See “Unlocking/Locking HP Switch Ports When Replacing Connected Devices” in the *MAC Port Lockdown* manual. Complete the portion of the procedure to enable MAC Port Lockdown and validate that the MAC address on the switch port matches the MAC address from the previous step.
5. Reinstall the PNM Client software. See: Installing the PNM Client on page 19. (If needed, see Table 3: PNM Client Software Installation Media on page 18.)
6. To restore the data, perform one of the following procedures:
   - If a BAR server is present in a system, see Executing a BAR Client Data Restore on page 41.
   - If a BAR server is not used in a system, perform a local restore. See: Restoring the PNM Client SSH Data on page 42.

9.1.1 Executing a BAR Client Data Restore

This procedure restores the Backup and Restore (BAR) client data to the staging directory on the BAR client.

Prerequisites: Provision Secure Shell (SSH) keys to the BAR client before initiating the restore. See procedures for SSH host key provisioning for the centralized Backup and Restore feature in the *Securing Protocols with SSH* manual.

Procedure:

1. Log on to the BAR server using your Active Directory account.
2. At the command prompt, enter: `admin_menu`

   The administrative menu appears. To select menu items in the following steps, type the number that corresponds to each menu item, then press Enter.

3. Select **Application Administration**.
4. Select **Restore Administration**.
5. Select **Initiate Client Restore**.
6. When prompted to enter the client name or name prefix, perform one of the following actions:
   - Press Enter for a list of all registered BAR clients.
   - Enter the first few characters of the BAR client name. Press Enter for a list of BAR client names that start with those characters.
7. To select a BAR client, perform one of the following actions:
   - If a list of BAR clients does not appear, press Enter. Only one BAR client matched your query, so the BAR client has already been selected for you.
   - If a list of BAR clients appears, perform the following actions:
     1. Enter the menu number for the selected client.
     2. Press Enter.
   - If more than 25 BAR clients appear, BAR clients scroll off the top of the screen. You can page up to see them by pressing Shift + Page Up, then return to the prompt by pressing Shift + Page Down.

   A menu of backup dates and times appears for the selected BAR client.

8. Enter the number for the backup you want to restore.

   The following prompt appears: `Restore operation in progress`. The **Restore Administration** menu reappears.

Appendix A

Local Backup/Restore of PNM Client SSH Data

To learn how to perform PNM Client backup and restore, see Centralized Backup and Recovery for PNM Clients on page 34. This appendix should not be used for a regular backup/restore of PNM Client. However, it can be useful in some specific cases (such as PNM Client Disaster Recovery when your Backup/Restore Server is not accessible).

A.1

Backing Up the PNM Client SSH Data

Procedure:

1 Log on to the PNM Client using your Active Directory account, a member of the Active Directory Network Security Administrator group (secadm). If needed, see the “Logging on to Network Management Clients to Configure SSH” in the *Securing Protocols with SSH* manual.

   NOTICE: If using a domain account, make sure that the Active Directory domain is entered before the user name in the format ***<domain>\<user name>***.

2 Using **Run As Administrator**, select **Start** → **All Apps** → **Motorola** → **backupSshSettings** (**Programs** in the Windows classic menu)

   If the destination folder does not exist, a message appears informing that the folder will be created.

   A **Status** window opens with the status of the backup. When successful, there are no errors reported.

3 To acknowledge the backup status, click **OK**.

   NOTICE: All backed up settings are stored within the `D:\Upgrade Data Store \Motorola PRNM Suite` folder. Additionally, you may copy this folder to a safe external location. Remember to copy it back to the folder before a restore, if for any reason the folder was removed or emptied.

   The **Status** window closes.

A.2

Restoring the PNM Client SSH Data

Procedure:

1 Log on to the PNM Client using your Active Directory account being a member of the Active Directory Network Security Administrator group (secadm). If needed, see the “Logging on to Network Management Clients to Configure SSH” in the *Securing Protocols with SSH* manual.

   NOTICE: If using a domain account, make sure that the Active Directory domain is entered before the user name in the format ***<domain>\<user name>***.

2 Verify that the backup files are available within the `D:\Upgrade Data Store\Motorola PRNM Suite` folder.

3 Using **Run As Administrator**, select **Start** → **All Apps** → **Motorola** → **restoreSshSettings** (**Programs** in the Windows classic menu).

If a **User Account Control** dialog box displays, select **Allow**, **Yes**, or **Continue**.

A **Status** window opens with the status of the restore. When successful, there are no errors reported.

4 Click **OK**.

The **Status** window closes.

Appendix B

PNM Printer Security Configuration

This chapter describes configuration of the HP LaserJet 500 color M553dn printer.

Procedures apply only to PNM Printers that are connected to the system as Network Printers through LAN, not USB.

B.1 Configuring the PNM Printer Security

You must configure the printer security settings before you add the printer to the PNM Client.

While using the Web Administration Panel you may see the following warning messages:

- `Certificate Error: There is a problem with this website's security certificate`. Click **Continue to this website…** to proceed.
- `Security Alert: You are about to view pages over a secure connection`. Click **OK** to proceed.
- `A script is accessing some software (an ActiveX control) on this page which has been marked safe for scripting. Do you want to allow this?` Click **Yes** to proceed.

When and where to use:
Perform this process **before** you add the printer to the PNM Client.

Process:

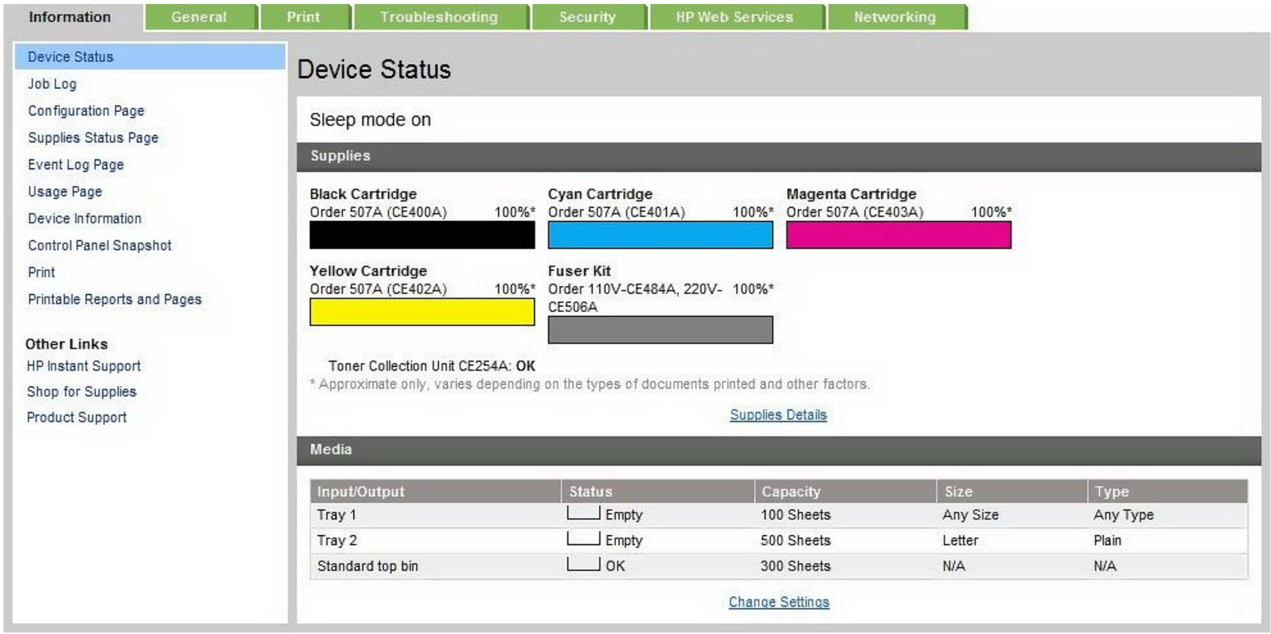
1. Perform the following initial configuration procedures:
   a. Accessing PNM Printer Web Administration Panel on page 44
   b. Disabling Printer SNMP Management and Unnecessary PNM Printer Services on page 45
   c. Configuring PNM Printer Static IP Address on page 47
   d. Disabling PNM Printer Management Protocols (Except for HTTPS) on page 48
   e. Disabling PNM Printer Firmware Upgrade Sent as Print Jobs on page 50
   f. Restricting PNM Printer Print Services to Port 9100 and LPD (port 515) on page 51
   g. Restricting PNM Printer Configuration Access to Administrators Only on page 52
2. Perform the periodical maintenance procedures in PNM Printer Periodical Maintenance on page 53.

B.1.1 Accessing PNM Printer Web Administration Panel

Prerequisites:
For the default IP address, see the printer's manual.

This figure shows proper settings.

Figure 1: PNM Printer Device Status



Device Status

Sleep mode on

Supplies

Black Cartridge
Order 507A (CE400A) 100%*

Cyan Cartridge
Order 507A (CE401A) 100%*

Magenta Cartridge
Order 507A (CE403A) 100%*

Yellow Cartridge
Order 507A (CE402A) 100%*

Fuser Kit
Order 110V-CE484A, 220V-CE506A 100%*

Toner Collection Unit CE254A: **OK**

* Approximate only, varies depending on the types of documents printed and other factors.

Supplies Details

Media

Input/Output	Status	Capacity	Size	Type
Tray 1	Empty	100 Sheets	Any Size	Any Type
Tray 2	Empty	500 Sheets	Letter	Plain
Standard top bin	OK	300 Sheets	N/A	N/A

Change Settings

Procedure:

Log in to the **Web Administration Panel** of the Printer by entering its IP address in the Web Browser on the PC with network access to the PNM printer.

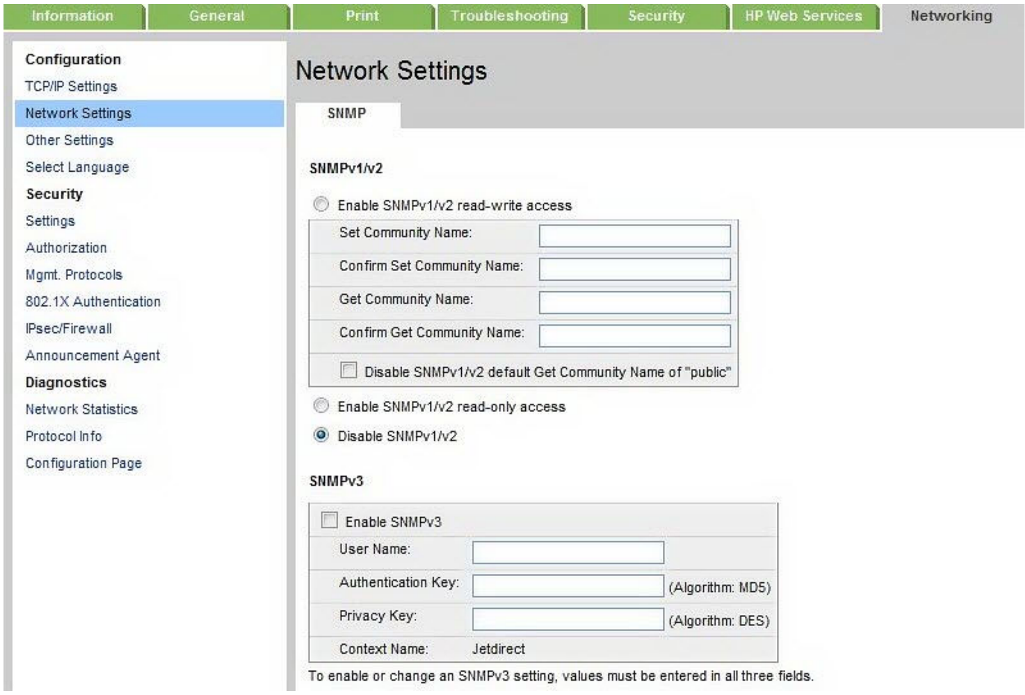
The **Device Status** window appears. See Figure 1: PNM Printer Device Status on page 45.

Postrequisites: Return to the Configuring the PNM Printer Security on page 44.

B.1.2
Disabling Printer SNMP Management and Unnecessary PNM Printer Services

Figures show proper settings.

Figure 2: PNM Printer Network Settings



Network Settings

SNMPv1/v2

○ Enable SNMPv1/v2 read-write access

Set Community Name:

Confirm Set Community Name:

Get Community Name:

Confirm Get Community Name:

□ Disable SNMPv1/v2 default Get Community Name of "public"

○ Enable SNMPv1/v2 read-only access

● Disable SNMPv1/v2

SNMPv3

□ Enable SNMPv3

User Name:

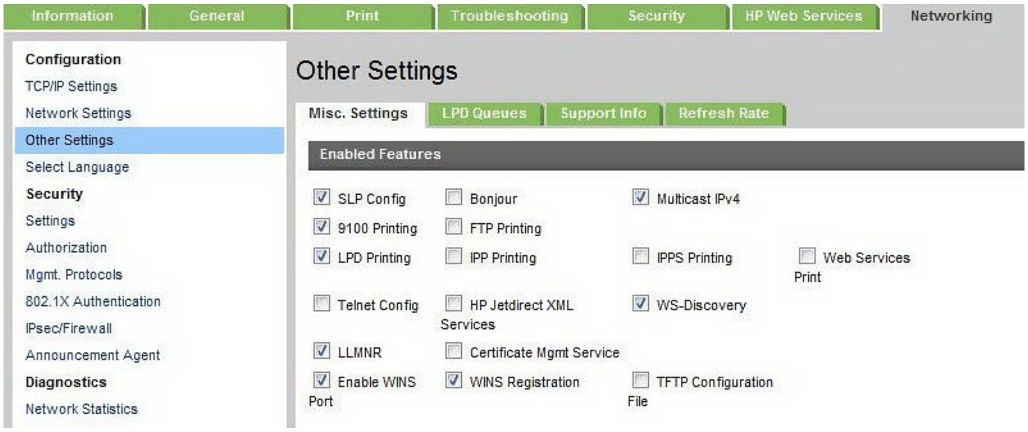
Authentication Key: (Algorithm: MD5)

Privacy Key: (Algorithm: DES)

Context Name: Jetdirect

To enable or change an SNMPv3 setting, values must be entered in all three fields.

Figure 3: PNM Printer Other Settings



Other Settings

Enabled Features

☑ SLP Config □ Bonjour ☑ Multicast IPv4

☑ 9100 Printing □ FTP Printing

☑ LPD Printing □ IPP Printing □ IPPS Printing □ Web Services Print

□ Telnet Config □ HP Jetdirect XML Services ☑ WS-Discovery

☑ LLMNR □ Certificate Mgmt Service

☑ Enable WINS Port ☑ WINS Registration □ TFTP Configuration File

Procedure:

1. Perform the following steps:
   - a On the **Networking** tab, select **Network Settings** → **Disable SNMPv1/v2**.
   - b Remove the selection for **Enable SNMPv3**.
   - c See Figure 2: PNM Printer Network Settings on page 46.
2. Scroll down, click **Apply** → **OK**.
3. Perform the following steps:
   - a On the **Networking** tab, select **Other Settings** → **Misc. Settings**.
   - b Remove the selection for the following:
   - **Bonjour**
   - **FTP Printing**

- **Telnet Config**
- **TFTP Configuration File**

  See Figure 3: PNM Printer Other Settings on page 46.

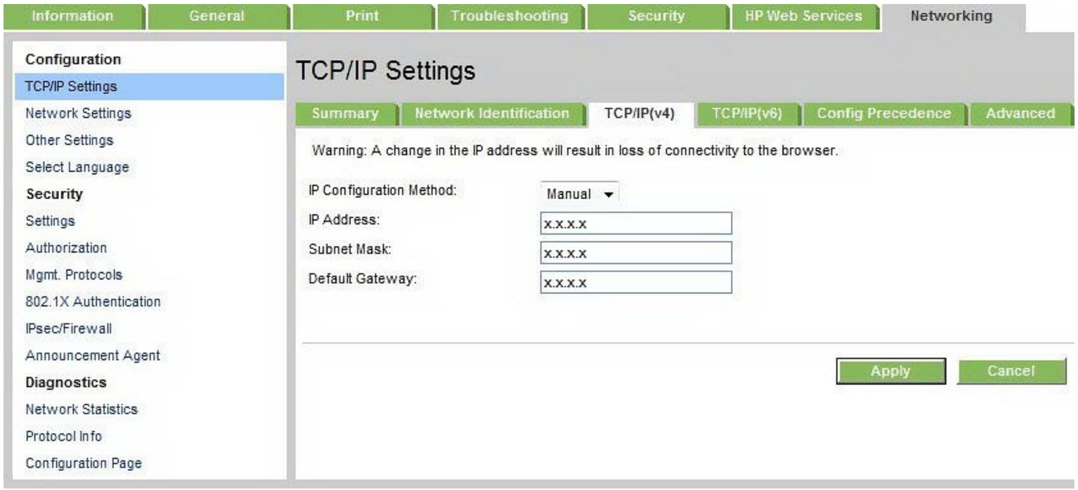
4 Scroll down, click **Apply** → **OK**.

Postrequisites: Return to the Configuring the PNM Printer Security on page 44.

B.1.3 Configuring PNM Printer Static IP Address

Prerequisites: Obtain the IP plan from your system administrator.
Figures show proper settings.

Figure 4: PNM Printer TCP/IP(v4) Settings



Warning: A change in the IP address will result in loss of connectivity to the browser.

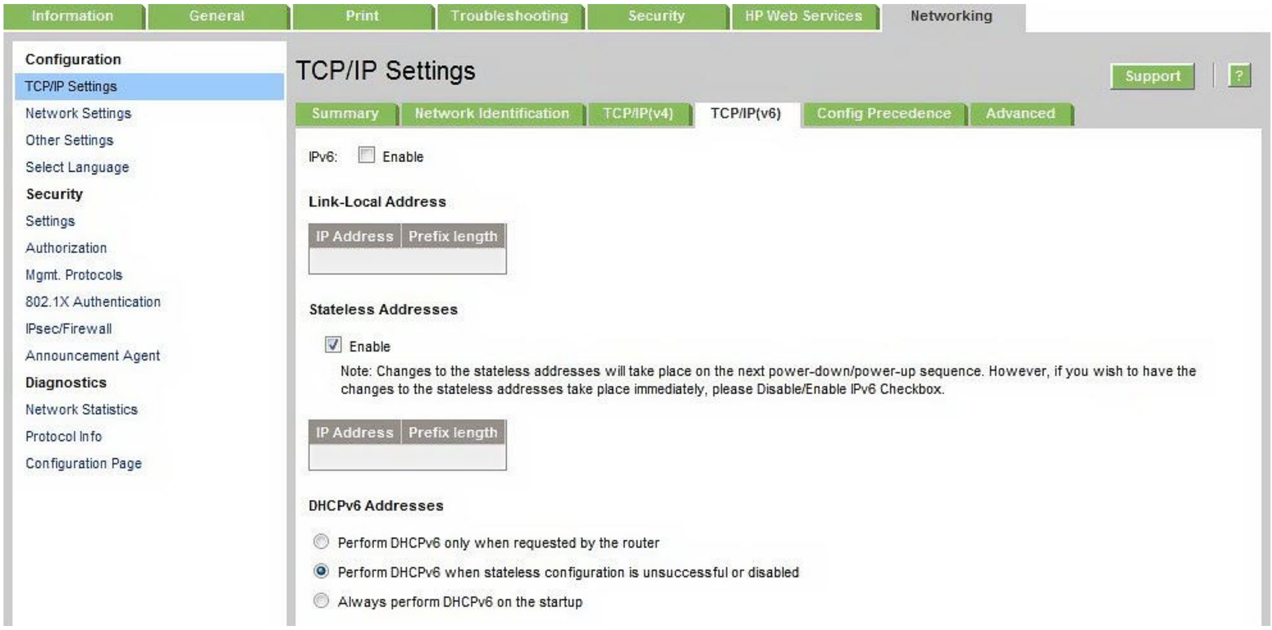
IP Configuration Method: Manual

IP Address: x.x.x.x

Subnet Mask: x.x.x.x

Default Gateway: x.x.x.x

Figure 5: PNM Printer TCP/IP(v6) Settings



IPv6: □ Enable

Link-Local Address

IP Address	Prefix length

Stateless Addresses

☑ Enable

Note: Changes to the stateless addresses will take place on the next power-down/power-up sequence. However, if you wish to have the changes to the stateless addresses take place immediately, please Disable/Enable IPv6 Checkbox.

IP Address	Prefix length

DHCPv6 Addresses

○ Perform DHCPv6 only when requested by the router

● Perform DHCPv6 when stateless configuration is unsuccessful or disabled

○ Always perform DHCPv6 on the startup

Procedure:

1. On the **Networking** tab, select **TCP/IP Settings** → **TCP/IP(v4)**. See Figure 4: PNM Printer TCP/IP(v4) Settings on page 47.

   The TCP/IP(v4) tab appears.

2. Set the **IP Configuration Method** to **Manual**.
3. Complete the following fields, according to the *System IP Plan*:
   - **IP Address:**
   - **Subnet Mask:**
   - **Default Gateway:**
4. Scroll down, click **Apply** → **OK**.
5. On the **TCP/IP(v6)** tab, uncheck **Enable** for IPv6. See Figure 5: PNM Printer TCP/IP(v6) Settings on page 47.
6. Scroll down, click **Apply** → **OK**.

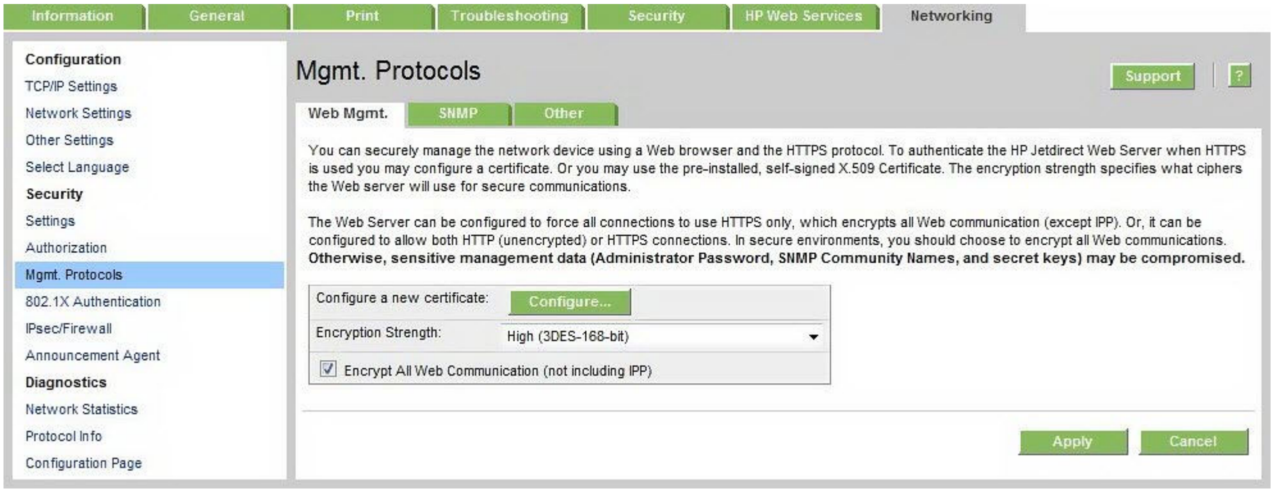
Postrequisites: Return to the Configuring the PNM Printer Security on page 44.

B.1.4

Disabling PNM Printer Management Protocols (Except for HTTPS)

Figure 6: PNM Printer Management Protocols – Web Management on page 48 , Figure 7: PNM Printer Management Protocols – Other on page 49 and Figure 8: PNM Printer Device Announcement Agent on page 49 show proper settings.

Figure 6: PNM Printer Management Protocols – Web Management



Mgmt. Protocols

You can securely manage the network device using a Web browser and the HTTPS protocol. To authenticate the HP Jetdirect Web Server when HTTPS is used you may configure a certificate. Or you may use the pre-installed, self-signed X.509 Certificate. The encryption strength specifies what ciphers the Web server will use for secure communications.

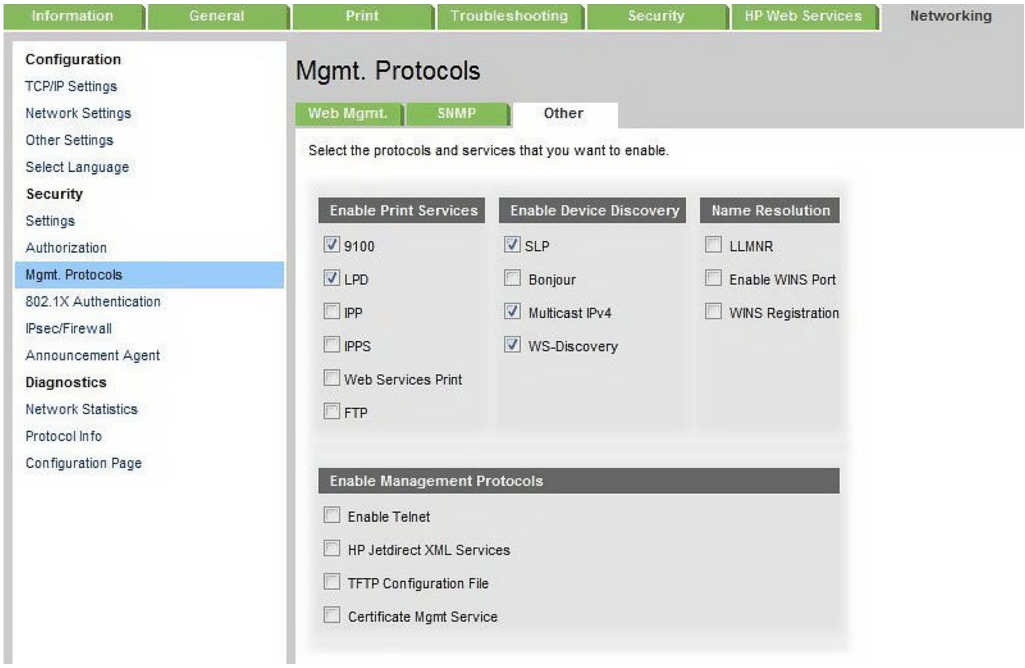
The Web Server can be configured to force all connections to use HTTPS only, which encrypts all Web communication (except IPP). Or, it can be configured to allow both HTTP (unencrypted) or HTTPS connections. In secure environments, you should choose to encrypt all Web communications. **Otherwise, sensitive management data (Administrator Password, SNMP Community Names, and secret keys) may be compromised.**

Configure a new certificate: Configure...

Encryption Strength: High (3DES-168-bit)

☑ Encrypt All Web Communication (not including IPP)

Figure 7: PNM Printer Management Protocols – Other



Mgmt. Protocols

Select the protocols and services that you want to enable.

Enable Print Services

- ☑ 9100
- ☑ LPD
- □ IPP
- □ IPPS
- □ Web Services Print
- □ FTP

Enable Device Discovery

- ☑ SLP
- □ Bonjour
- ☑ Multicast IPv4
- ☑ WS-Discovery

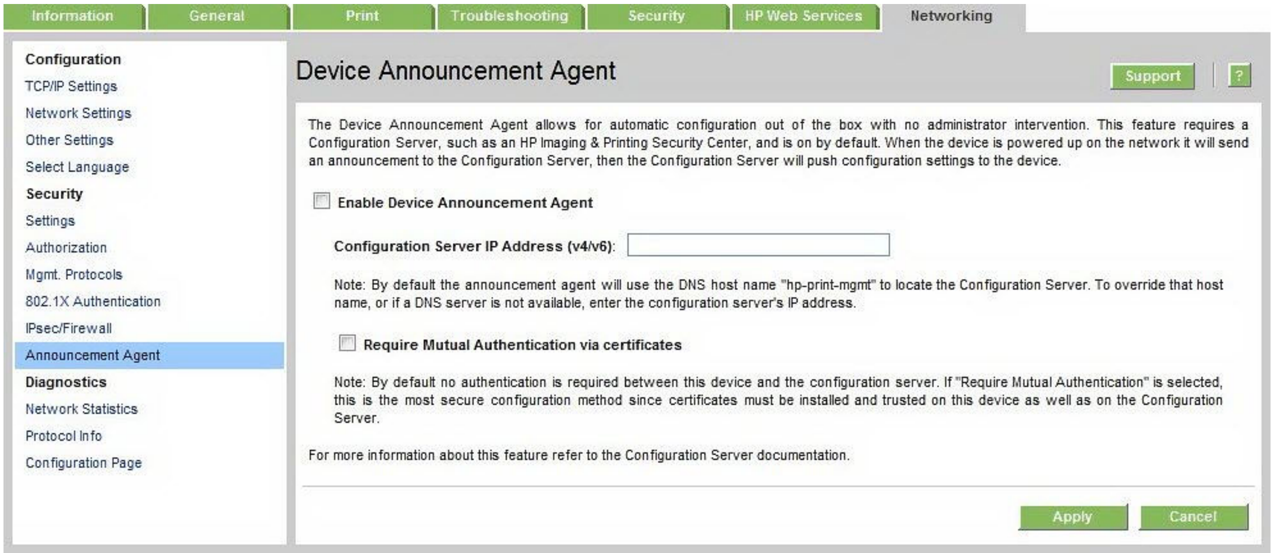
Name Resolution

- □ LLMNR
- □ Enable WINS Port
- □ WINS Registration

Enable Management Protocols

- □ Enable Telnet
- □ HP Jetdirect XML Services
- □ TFTP Configuration File
- □ Certificate Mgmt Service

Figure 8: PNM Printer Device Announcement Agent



Device Announcement Agent

The Device Announcement Agent allows for automatic configuration out of the box with no administrator intervention. This feature requires a Configuration Server, such as an HP Imaging & Printing Security Center, and is on by default. When the device is powered up on the network it will send an announcement to the Configuration Server, then the Configuration Server will push configuration settings to the device.

□ Enable Device Announcement Agent

Configuration Server IP Address (v4/v6):

Note: By default the announcement agent will use the DNS host name "hp-print-mgmt" to locate the Configuration Server. To override that host name, or if a DNS server is not available, enter the configuration server's IP address.

□ Require Mutual Authentication via certificates

Note: By default no authentication is required between this device and the configuration server. If "Require Mutual Authentication" is selected, this is the most secure configuration method since certificates must be installed and trusted on this device as well as on the Configuration Server.

For more information about this feature refer to the Configuration Server documentation.

Procedure:

1 On the **Networking** tab, select **Mgmt. Protocols** → **Web Mgmt.**. See Figure 6: PNM Printer Management Protocols – Web Management on page 48.

The **Web Mgmt.** window appears.

2 Select the **Encrypt All Web Communication** check box.

NOTICE: Make sure to set **Encryption Strength** to **High**.

3 Scroll down, click **Apply** → **OK**.

4 On the **Networking** tab, select **Mgmt. Protocols** → **Other**. See Figure 7: PNM Printer Management Protocols – Other on page 49.

   The **Other** window displays.

5 Remove the selection for the following:
   - **LLMNR**
   - **Enable WINS Port**
   - **WINS Registration**
   - **Enable Telnet**
   - **HP Jetdirect XML Services**
   - **TFTP Configuration File**
   - **Certificate Mgmt Service**

6 Scroll down, click **Apply** → **OK**.

7 On the **Networking** tab, select **Announcement Agent**. See Figure 8: PNM Printer Device Announcement Agent on page 49.

   The **Device Announcement Agent** window displays.

8 Remove the selection for **Enable Device Announcement Agent**.

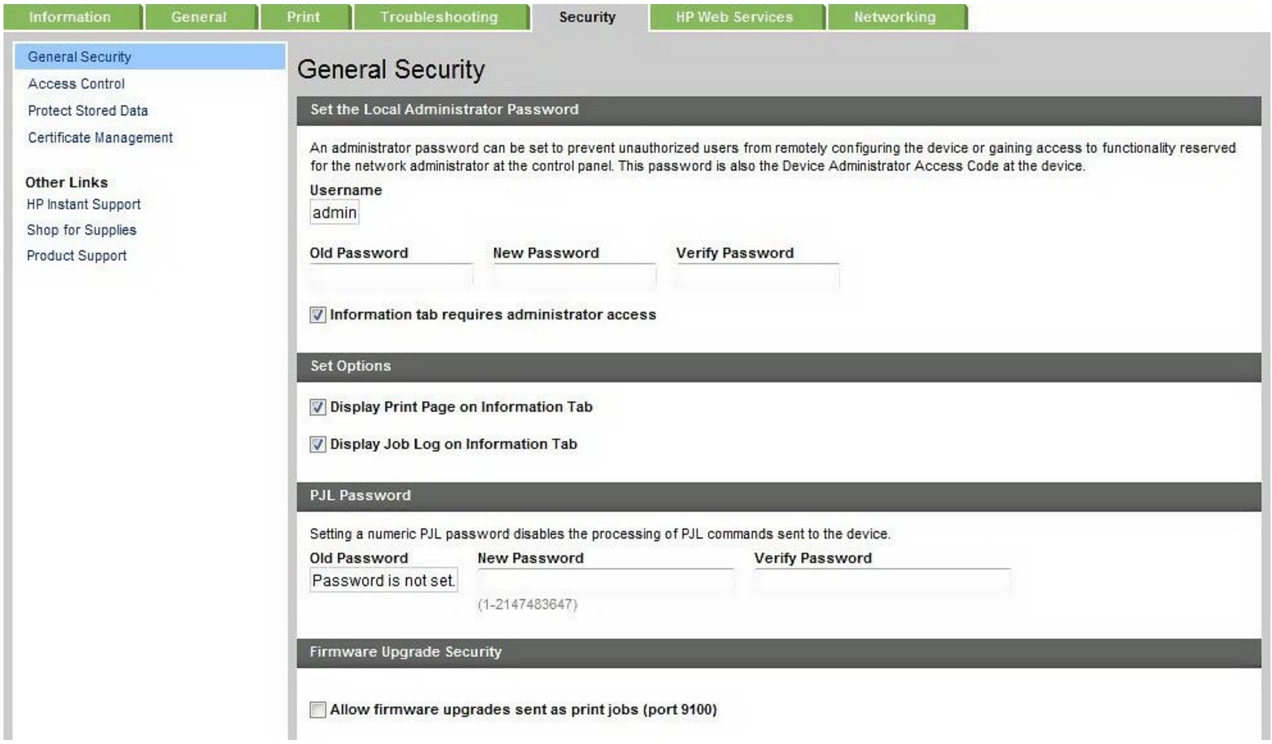
9 Scroll down, click **Apply** → **OK**.

Postrequisites: Return to the Configuring the PNM Printer Security on page 44.

B.1.5 Disabling PNM Printer Firmware Upgrade Sent as Print Jobs

This figure shows proper settings.

Figure 9: PNM Printer General Security



General Security

Set the Local Administrator Password

An administrator password can be set to prevent unauthorized users from remotely configuring the device or gaining access to functionality reserved for the network administrator at the control panel. This password is also the Device Administrator Access Code at the device.

Username: admin

Old Password | New Password | Verify Password

☑ Information tab requires administrator access

Set Options

☑ Display Print Page on Information Tab

☑ Display Job Log on Information Tab

PJL Password

Setting a numeric PJL password disables the processing of PJL commands sent to the device.

Old Password: Password is not set. | New Password (1-2147483647) | Verify Password

Firmware Upgrade Security

☐ Allow firmware upgrades sent as print jobs (port 9100)

Procedure:

1. On the **Security** tab, select **General Security**. See Figure 9: PNM Printer General Security on page 51.

   The **General Security** window appears.

2. Remove the selection for the **Allow firmware upgrades sent as print jobs (port 9100)** check box.
3. Scroll down, click **Apply**.

Postrequisites: Return to the Configuring the PNM Printer Security on page 44.

B.1.6 Restricting PNM Printer Print Services to Port 9100 and LPD (port 515)

Procedure:

1. On the **Networking** tab, select **Mgmt. Protocols** → **Other**. See Figure 7: PNM Printer Management Protocols – Other on page 49.

   The **Other** window appears.

2. Under **Enable Print Services**, remove the selection the following:
   - **IPP**
   - **IPPS**
   - **Web Services Print**
   - **FTP**
3. Scroll down, click **Apply** → **OK**.

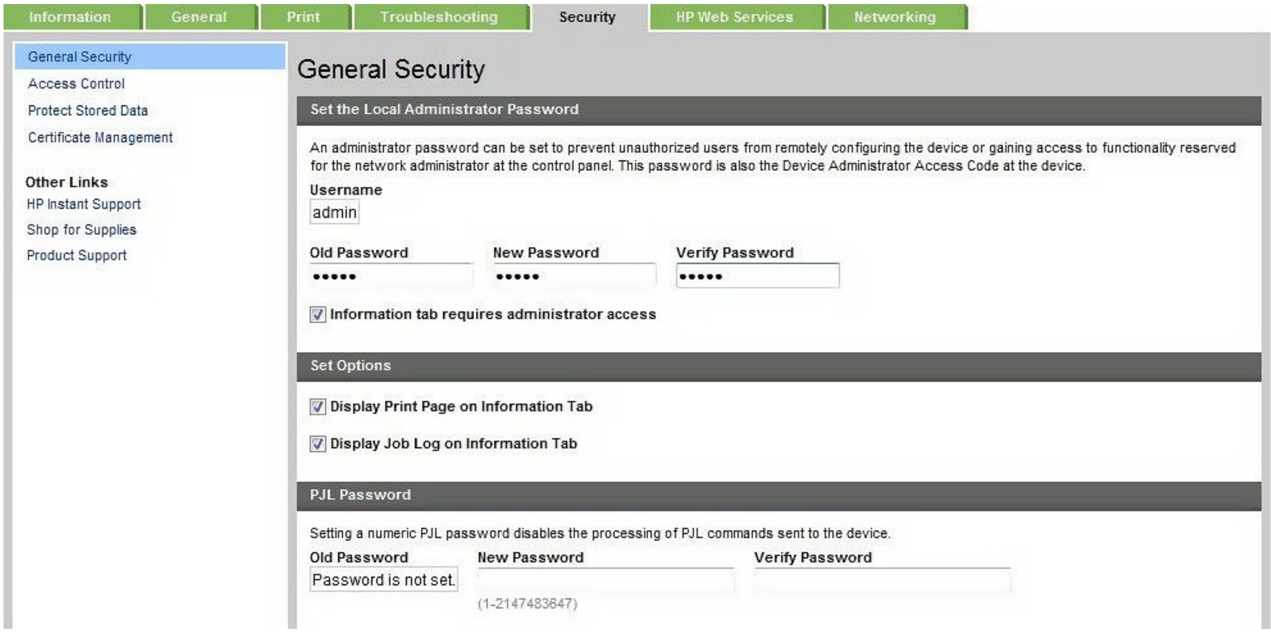
Postrequisites: Return to the Configuring the PNM Printer Security on page 44.

B.1.7

Restricting PNM Printer Configuration Access to Administrators Only

Figures show proper settings.

Figure 10: PNM Printer General Security Set Password



General Security

Set the Local Administrator Password

An administrator password can be set to prevent unauthorized users from remotely configuring the device or gaining access to functionality reserved for the network administrator at the control panel. This password is also the Device Administrator Access Code at the device.

Username: admin

Old Password: ••••• New Password: ••••• Verify Password: •••••

☑ Information tab requires administrator access

Set Options

☑ Display Print Page on Information Tab

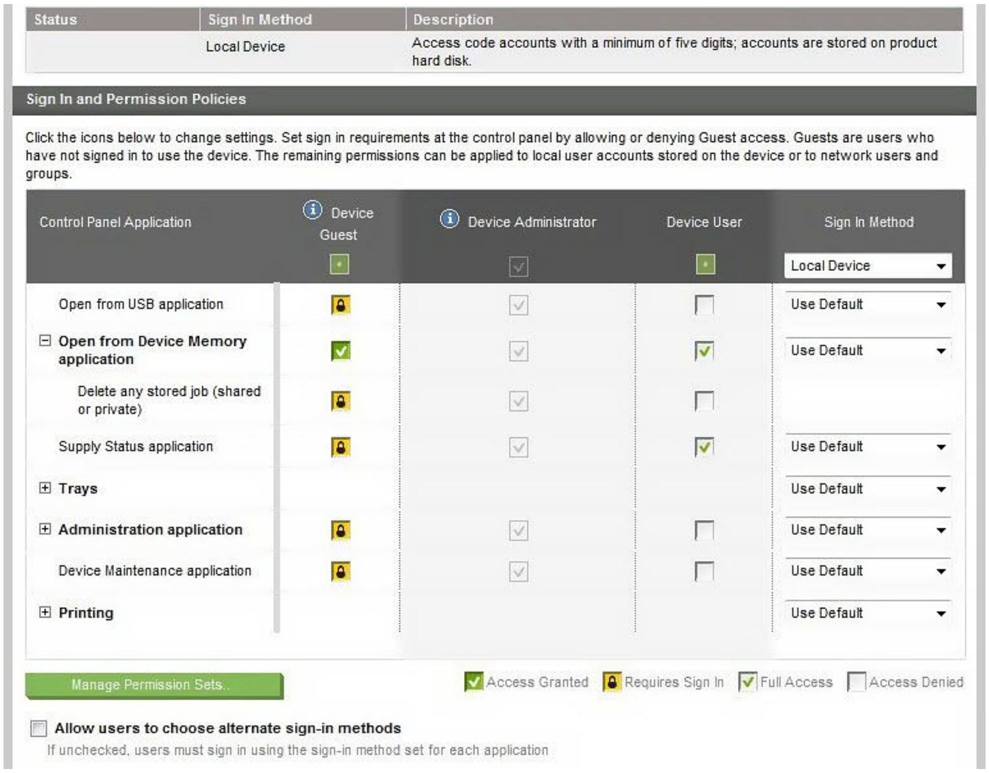
☑ Display Job Log on Information Tab

PJL Password

Setting a numeric PJL password disables the processing of PJL commands sent to the device.

Old Password: Password is not set. New Password: (1-2147483647) Verify Password:

Figure 11: PNM Printer Permission Policies



Status	Sign In Method	Description
	Local Device	Access code accounts with a minimum of five digits; accounts are stored on product hard disk.

Sign In and Permission Policies

Click the icons below to change settings. Set sign in requirements at the control panel by allowing or denying Guest access. Guests are users who have not signed in to use the device. The remaining permissions can be applied to local user accounts stored on the device or to network users and groups.

Control Panel Application	Device Guest	Device Administrator	Device User	Sign In Method
	🟩	☑	🟩	Local Device
Open from USB application	🔒	☑	□	Use Default
⊟ Open from Device Memory application	☑	☑	☑	Use Default
Delete any stored job (shared or private)	🔒	☑	□	
Supply Status application	🔒	☑	☑	Use Default
⊞ Trays				Use Default
⊞ Administration application	🔒	☑	□	Use Default
Device Maintenance application	🔒	☑	□	Use Default
⊞ Printing				Use Default

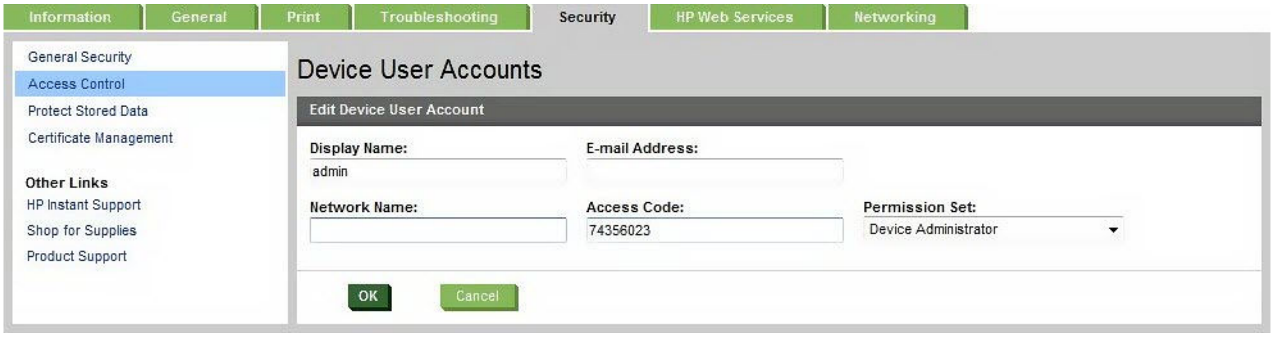
Manage Permission Sets...

☑ Access Granted 🔒 Requires Sign In ☑ Full Access □ Access Denied

□ Allow users to choose alternate sign-in methods

If unchecked, users must sign in using the sign-in method set for each application

Figure 12: PNM Printer Device User Accounts



Device User Accounts

Edit Device User Account

Display Name: admin

E-mail Address:

Network Name:

Access Code: 74356023

Permission Set: Device Administrator

Procedure:

1 On the **Security** tab, select **General Security**. See Figure 10: PNM Printer General Security Set Password on page 52.

The **General Security** window appears.

2 Set up the **Local Administrator Password** by entering credentials.

NOTICE: Make sure that the password meets complexity requirements.

3 Select the **Information tab requires administrator access** check box.

4 Scroll down, click **Apply**.

5 To disable guest configuration access from the Local Device (Panel on the Printer) on the Security tab, select **Access Control**.

The **Access Control** window displays.

6 Configure the **Sign In and Permissions Policies** table as shown in Figure 11: PNM Printer Permission Policies on page 52.

7 Remove selection for the **Allow users to choose alternate sign-in methods** check box.

8 Scroll down, click **Apply**.

9 Create a User/Admin Device account in the **Device User Accounts** window. See Figure 12: PNM Printer Device User Accounts on page 53.

10 Click **New…**, then perform the following:

a In the **Display Name**, enter the name for the account.

b Enter at least 8-digit-long **Access Code**.

c Click **OK**.

You can use this access code to configure from the Device Panel.

Postrequisites: Return to the Configuring the PNM Printer Security on page 44.

B.1.8

PNM Printer Periodical Maintenance

This section describes periodical maintenance actions required for the PNM Printer.

B.1.8.1

Applying PNM Printer Firmware

Procedure:

1. Download the latest firmware from the HP Support web page for your PNM printer model.
2. Copy the downloaded Printer Firmware File to a PNM Client that has network access to the Printer. The typical recommended methods to transfer the Firmware File to the PNM Client are:
   - CD/DVD Media
   - USB Memory/Disk Device
   - Remote Desktop Copy

   Depending on your organization's policies, choose the appropriate transfer method. For example, use of USB drives may be prohibited.
3. On the PNM Printer Web Administration Panel, go to the General Tab, select **Firmware Upgrade**.
4. Verify the **Firmware Version and Date**.

   You can do that by printing a configuration page to determine the version of firmware currently installed in this product.
5. If the firmware installed is older than the one downloaded, click **Browse…**, select the firmware file and click **Open** → **Install**.
6. Restart the PNM printer after upgrade is completed.

B.1.8.2

Reviewing Event and Job Logs

Procedure:

To review the logs periodically, go to the **Information** tab, **Job Log** or **Event Log** Page.