



Cisco Prime Network 5.0 Installation Guide

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number:

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

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

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

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

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

© 2018 Cisco Systems, Inc. All rights reserved.



iii

Installation Overview 1-1

Installation Options 1-1

Installation DVDs 1-2

Installation Requirements 2-1

Sample Network Sizes Used in This Document 2-1

Hardware and Software Requirements 2-2

Prime Network Gateway and Database Requirements 2-2

Gateway: Minimum Hardware and Software Requirements 2-3

Gateway: CPU and Memory Requirements for Different Network Sizes 2-3

Gateway: IOPS (Input/Output Operations Per Second) for Different Network Sizes 2-5

Storage Requirements for Different Network Sizes 2-7

Remote Embedded Database Requirements 2-9

External Database Requirements 2-9

Prime Network Unit Requirements 2-10

Unit: Minimum Hardware and Software Requirements 2-10

Unit: Recommended Hardware for Different Network Sizes 2-10

Requirements for Gateway and Unit on a Single Server 2-12

Prime Network Client Requirements 2-12

Clients: Minimum Hardware and Software Requirements 2-12

Required Red Hat Services and RPMs 2-16

Required RPMs for Red Hat 6.5 2-16

Required RPMs for Red Hat 6.7 2-17

Required RPMs for Red Hat 6.8 2-20

RPMS Dependent on Above Listed Packages 2-22

Required RPMs for Red Hat 7.2 2-23

Required RPMs for Oracle Database 12c 2-24

Required Ports for Prime Network 2-25

Prime Network Server, HTTP, TCP, and UDP Ports 2-25

Prime Network Integration Layer Ports 2-29

Preparing for the Installation	3-1
Gateway Preinstallation Tasks—Embedded Database	3-1
Gateway Preinstallation Tasks—External Database	3-3
Unit Preinstallation Tasks	3-5
Verifying the Installed Operating System	3-6
Verifying the RPMs Required on Red Hat for Prime Network	3-6
Starting the Oracle Listener (External Database)	3-7
Configuring the Network Timing Protocol	3-7
Finding NTP Process in Server	3-8
Killing NTP Process in Server	3-9
IPv4 and IPv6 Compliance Considerations	3-9
UNIX Services and Components Used by Prime Network	3-10
Preparing the Oracle External Database	4-1
Using an External Database: General Guidelines	4-1
Creating an External Oracle Database	4-2
Configuring the External Database	4-5
Configuring the cursor_sharing System Parameter	4-5
Retaining Partitioning Storage Behavior	4-6
Configuring the job_queue_processes System Parameter	4-6
Configuring the audit_trail System Parameter	4-6
Disabling the Recycle Bin Option	4-7
Setting the open_cursors Parameter	4-7
Disabling Automatic Maintenance Jobs	4-8
Changing Database Ports	4-8
Configuring the Database Size and Disk Structure	4-9
Configuring Oracle to Start Automatically When Prime Network Restarts	4-9
Preventing Passwords in the Default Profile from Expiring	4-10
Maintaining the External Database	4-11
Maintaining Archive Log File Disk Space	4-11
Adding Data Files to the Tablespace	4-11
Installing the Prime Network Gateway and Units Using the Installation Wizard	5-1
Prerequisites for Using the Installation Wizard	5-1
Launching the Installation Wizard	5-2
Installing the Gateway with Embedded Database Using the Installation Wizard	5-3
Installing the Gateway with External Database Using the Installation Wizard	5-7
Installing a Unit Using the Installation Wizard	5-11

Installing the Prime Network Gateway Using CLI	6-1
Installation Overview	6-1
Installing the Prime Network Gateway With an Embedded Database	6-2
Installing the Prime Network Gateway With an External Database	6-6
Manually Creating Prime Network Database Schemas	6-11
Post Installation Tasks For the Gateway	6-13
Starting the Prime Network Gateway	6-13
Verifying Connectivity	6-15
Verifying the Connectivity to the Database	6-15
Configuring Prime Network Post-Installation	6-16
Verifying the Redirected Ports	6-17
Verifying the Drools Rules Configuration	6-17
Verifying the Monitoring (Graphs) Configuration	6-17
Verifying the Installation of Registry Directories	6-18
Adding Oracle Database Files	6-18
Updating the Database Host in the Registry for NAT	6-19
Environment Variables, Aliases, and Folders Created During Installation	6-20
Product Services Installed with Prime Network	6-21
Troubleshooting	6-22
Installing Prime Network Units	7-1
Installing a Unit	7-1
Configuring Dual Listeners	7-3
Post Installation Tasks For Units	7-4
Verifying the Prime Network Version and the Unit Processes	7-4
Verifying the Unit Configuration	7-5
Installing the Vision, Events, and Administration Clients	8-1
Launching the Clients From the Web Start Page	8-1
Installing the Prime Network Clients on Your Computer	8-3
Installing Prime Network Clients in a Remote Personal Computer	8-5
Troubleshooting Clients	8-6
Installing the Prime Network Integration Layer	9-1
Prerequisites for Installing the PN-IL	9-1
Installing the PN-IL Using the Installation Wizard	9-2
Installing the PN-IL (CLI Method)	9-4
Enabling and Disabling the PN-IL Health Monitor	9-5
Managing FTP for Prime Network Integration Layer Server	9-5

- Storage Location for PN-IL Replicated Files 9-6
- Clearing the FTP Configuration for the Standalone Integration Layer Server 9-7
- Changing the Ports Used by the PN-IL 9-7
 - Changing the NIO and SSL Ports 9-7
 - Changing the MTOSI Web Services Port 9-7
 - Changing the 3GPP Web Services Port 9-8
 - Changing the Alarm Web Services Port 9-8
- Migrating the PN-IL from Standalone Mode to Suite Mode 9-8

Upgrading and Rolling Back Prime Network 10-1

- Prime Network Upgrade Overview 10-2
- Preparing to Upgrade Prime Network (Pre-Upgrade Checklist) 10-5
 - Supported Prime Network Upgrade and Rolling back versions 10-8
- Upgrading to Prime Network 5.0 from 4.3.2, 4.3.1, 4.3, 4.2.3, 4.2.2 (Intermediate Steps) 10-8
- Upgrading to Prime Network 5.0 and Oracle 12.1.0.2 10-11
 - In-line Upgrade of RHEL 6.5, 6.7, 6.8, or 6.9¹ with Prime Network 5.0 and Oracle 12.1.0.2 10-11
 - Upgrading from RHEL 5.8 to RHEL 6.x or RHEL 7.2 with Prime Network 5.0 and Oracle 12.1.0.2 10-12
- Upgrading to Prime Network 5.0 in Suite Mode 10-13
- Upgrading or Downgrading OS in HA Environment 10-14
 - Upgrade of OS in HA Environment 10-14
 - Downgrade OS in HA Environment 10-16
- Configuring Clusters for Pacemaker and Corosync Setup 10-17
- Rolling Back to Earlier Prime Network Version 10-20
- Upgrading the Prime Network Integration Layer (PN-IL) 10-22
 - Upgrading PN-IL in Standalone Mode 10-22
 - Upgrading PN-IL in Suite Mode 10-23
- Prime Network Post-upgrade Tasks 10-24
 - Enable Units to Restart Automatically After they are Rebooted 10-24
 - Restoring Customized Crontabs 10-25
 - Restarting Crontab Jobs for NAT Units 10-25
 - Fixing the Database Entry for Vision Clients with NAT 10-25
 - Updating the Port Watchdog (AVM Protection) Scripts 10-26
 - Restore Links Between Devices and Cloud VNEs 10-26
 - Support for Third-Party VNEs 10-26
 - Command Builder Scripts 10-26
 - Gathering DB Statistics in First 24 Hours 10-27
 - Integration Changes 10-27
 - Adding Managed Elements to the Database Manually for PC-FM Resync 10-27
- Upgrading the Embedded Database to Oracle 12.1.0.2 10-28

Example-Upgrading the Embedded Database to Oracle 12.1.0.2 10-29

Upgrading the Embedded Database to Oracle 12.1.0.2 in a HA Setup with Geographical Redundancy and Oracle ADG 10-31

Example-Upgrading the Embedded Database to Oracle 12.1.0.2 in a HA Setup with Geographical Redundancy and Oracle ADG 10-32

Uninstalling Prime Network 11-1

Uninstalling a Prime Network Gateway 11-1

Uninstalling a Gateway with an Embedded Database 11-2

Uninstalling Cisco Prime Network Units 11-2

Uninstalling the Cisco Prime Network Clients 11-3

Uninstalling Prime Network Manually 11-3

Uninstalling the PN-IL Using CLI 11-3

Uninstalling the PN-IL Using the Wizard 11-4

Uninstalling Pacemaker Corosync Configuration 11-4

Next Steps 12-1

Launching the Prime Network GUI Clients 12-1

Verifying That Backups Are Set Up 12-3

Enabling Network Discovery 12-4

Setting Up Transaction Manager 12-5

Setting Up VMware vCenter to Forward Events 12-5

Integration with Cisco Multicast Manager (CMM) 12-5

Setting Up Integration with Cisco Multicast Manager 12-6

Setting Up Traps for CMM 12-6

Removing Cisco Multicast Manager Integration from Prime Network 12-7

Using Chinese Characters with Oracle A-1

Using Chinese Characters with Windows Clients A-3

Displaying Chinese Characters in the GUI A-3



Installation Overview

This chapter provides an overview of the Prime Network installation process:

- [Installation Options, page 1-1](#) lists the installation options and provides links to available information for each option.
- [Installation DVDs, page 1-2](#) lists the DVDs that contain the Prime Network software and the contents of each DVD.

Installation Options

The Prime Network installation includes the installation of the following components in a Linux environment:

- Gateway (with an embedded or external database). The gateway installation is supported on physical servers or on VMware.
- One or more units.
- GUI clients.
- Prime Network Integration Layer (PN-IL), which can be installed to allow Prime Network to be used with Multi-Technology Operations Systems Interface (MTOSI) and 3GPP northbound interfaces. The PN-IL is mandatory if Prime Network is being installed in suite mode, that is integrated with Prime Central.

The following table shows where you will find the information you need for the various installation options.

Table 1-1 **Where to Find Information for the Prime Network Installation Options**

For this Option...	Go To...
Install the gateway with an embedded database	For CLI installation: Chapter 6, “Installing the Prime Network Gateway Using CLI.” For GUI installation: Chapter 5, “Installing the Prime Network Gateway and Units Using the Installation Wizard.”
Install the gateway with an external Oracle database	<ul style="list-style-type: none"> • Chapter 4, “Preparing the Oracle External Database,” • For CLI installation: Chapter 6, “Installing the Prime Network Gateway Using CLI.” or For GUI installation: Chapter 5, “Installing the Prime Network Gateway and Units Using the Installation Wizard.”

Table 1-1 Where to Find Information for the Prime Network Installation Options (continued)

For this Option...	Go To...
Install the gateway with local or geographic high availability	Cisco Prime Network 5.0 Gateway High Availability Guide
Install a unit	For CLI installation: Chapter 7, “Installing Prime Network Units.” For GUI installation: Chapter 5, “Installing the Prime Network Gateway and Units Using the Installation Wizard.”
Launching the Prime Network GUI Clients	Chapter 12, “Launching the Prime Network GUI Clients.”
Install Prime Network Integration Layer (PN-IL)	Chapter 9, “Installing the Prime Network Integration Layer, page 9-1”
Upgrade from a previous Prime Network release with RHEL 5.5-5.8, and 6.4	Chapter 10, “Upgrading and Rolling Back Prime Network.”
Pre-installation tasks	Chapter 2, “Installation Requirements” and Chapter 3, “Preparing for the Installation”
Post-installation tasks	Next Steps, page 12-1

Installation DVDs

[Table 1-2](#) lists the contents of the DVDs that contain the Prime Network 5.0 installation files.

Table 1-2 Contents of Cisco Prime Network 5.0 Installation DVDs

Disk	DVD Components
Disk 1: New Install	
Files for a new Prime Network 5.0 gateway and unit installation, including Red Hat High Availability.	
Server	<ul style="list-style-type: none"> • Prime Network 5.0 gateway and unit installation files: <ul style="list-style-type: none"> – install.bin (GUI installation) – install.pl – install.properties – ivne-drivers.tar • RH_ha.zip and install_ha.pl—High availability installation files • jws directory
Disk 2: Software and Documentation	
Client Installation Files	<ul style="list-style-type: none"> • Cisco Prime Network Vision • Cisco Prime Network Administration • Cisco Prime Network Events
Integration	<ul style="list-style-type: none"> • Standalone Integration Layer ESB tar files (sil-esb-2.0.0.tar.gz) • PNIntegrationLayer_v2.0.bin (GUI installation)

Table 1-2 Contents of Cisco Prime Network 5.0 Installation DVDs (continued)

Disk	DVD Components
Documentation	Cisco Prime Network Documentation Overview, 5.0
Disk 3: Upgrade files	
Upgrade from Prime Network , 4.2.2, 4.2.3 4.3, 4.3.1, 4.3.2 to 5.0	<ul style="list-style-type: none"> • Prime_Network_upgrade directory that has upgrade and rollback dependent scripts • ivne-drivers.tar file • PNIntegrationLayerUpgrade_1.0.0.0-2.0.0.tar.gz • embedded_upgrade_12.1.zip
Disk 4: Database Binaries	
Embedded database installation	<ul style="list-style-type: none"> • linuxamd64_12c_database_1of2.zip • linuxamd64_12c_database_2of2.zip
Operations Reports	
<p>Installation of Prime Network Operations Reports and the Infobright database on the Prime Network gateway.</p> <p>Note Operations Reports are only available to customers with Operations Reports license prior to May 2018. For re-installation of Operations Reports contact a Cisco customer support representative.</p>	<ul style="list-style-type: none"> • infobright_integ.zip



Installation Requirements

This chapter provides the hardware, software, database, and other requirements that must be met before installing Prime Network 5.0.

- [Sample Network Sizes Used in This Document, page 2-1](#)
- [Hardware and Software Requirements, page 2-2](#)
- [Required Red Hat Services and RPMs, page 2-16](#)
- [Required Ports for Prime Network, page 2-25](#)

Sample Network Sizes Used in This Document

[Table 2-1](#) provides specifications for different Prime Network deployments based on network size. Use one of these network sizes as a guide for defining your requirements.

The deployment sizing for Prime Network assumes that the devices are distributed as follows for Carrier Ethernet (CE), MPLS, or IP Radio Access Network (RAN):

- CE: 2% Ps, 8% N-PEs, 80% U-PEs, 10% CEs.
- MPLS: 5% core routers, 95% CPE.
- IP RAN: 15% aggregation, 30% cell sites, 55% L2 switches.

Table 2-1 **Network Size Specifications**

Network Size	Maximum No. of Devices	Maximum No. of Events Per Second (EPS)
Small	200	5
Medium	2000	20
Large	5000	50

Hardware and Software Requirements

These topics describe the gateway, unit, and client requirements:

- [Prime Network Gateway and Database Requirements, page 2-2](#)
- [Prime Network Unit Requirements, page 2-10](#)
- [Requirements for Gateway and Unit on a Single Server, page 2-12](#)
- [Prime Network Client Requirements, page 2-12](#)

**Note**

- Consult with your Cisco account representative for specific hardware and configuration details for your gateway and units before you acquire or use Prime Network.
- Hardware requirements assume that Prime Network does not share the hardware with additional applications. (This is the recommended installation.)

Prime Network Gateway and Database Requirements

Prime Network supports installation of the gateway on both bare metal and virtual machine (VM). The requirements listed in this section are the same for both of these options.

The gateway can be installed with a fully integrated, embedded Oracle 12c database or it can be configured to connect to and interact with an external Oracle database. In addition, if the Operations Reports component is installed, it incorporates the Infobright database.

This section lists the requirements for gateway installation with the embedded Oracle database, with and without the Infobright database (Operations Reports component). If you are using an external database, see the [External Database Requirements, page 2-9](#).


These topics provide the gateway requirements:

- [Gateway: Minimum Hardware and Software Requirements, page 2-3](#)
- [Gateway: CPU and Memory Requirements for Different Network Sizes, page 2-3](#)
- [Gateway: IOPS \(Input/Output Operations Per Second\) for Different Network Sizes, page 2-5](#)
- [Storage Requirements for Different Network Sizes, page 2-7](#)
- [Remote Embedded Database Requirements, page 2-9](#)
- [External Database Requirements, page 2-9](#)

Gateway: Minimum Hardware and Software Requirements

Table 2-2 identifies the minimum software and hardware requirements for Prime Network gateways.

Table 2-2 Minimum Requirements for Gateways

Item	Specifications
System hardware	Intel Xeon E5-2600 or equivalent. Also see Gateway: CPU and Memory Requirements for Different Network Sizes, page 2-3 .
Operating System	Red Hat 6.5, Red Hat 6.7, Red Hat 6.8, and Red Hat 7.2 64-bit Server Edition (English language) are supported in Prime Network 5.0 and run in a virtual environment. Red Hat is supported on VMWare ESXi version 5.5, and 6.0, and also on the Openstack kernel-based virtual machine (KVM) hypervisor version 2.6. Certain Red Hat services and RPMs are required. See Required Red Hat Services and RPMs, page 2-16 .
	 <p>Note Prime Network must be installed on a dedicated operating system. We cannot guarantee compatibility with external components running on the operating system together with Prime Network.</p>

Gateway: CPU and Memory Requirements for Different Network Sizes

Table 2-3 lists the gateway CPU and memory requirements for networks of different sizes. See [Sample Network Sizes Used in This Document, page 2-1](#).

Table 2-3 CPU and Memory Requirements for Different Network Sizes

Network Size (No. of Devices and Events Per Second (EPS))	No. of CPU Cores (VMware or Bare Metal)	Minimum RAM (without Operations Reports ¹¹ or PN-IL)	RAM (Gateway + Operations Reports)	Minimum RAM (Gateway + Operations Reports + PN-IL)
Small: 200 devices or less 5 EPS	5	32 GB	48 GB	52 GB
Medium: 200 - 2000 devices 20 EPS	8	64 GB	96 GB	100 GB

Table 2-3 CPU and Memory Requirements for Different Network Sizes

Network Size (No. of Devices and Events Per Second (EPS))	No. of CPU Cores (VMware or Bare Metal)	Minimum RAM (without Operations Reports¹ or PN-IL)	RAM (Gateway + Operations Reports)	Minimum RAM (Gateway + Operations Reports + PN-IL)
Large: 2000 - 5000 devices 50 EPS	10	96 GB	128 GB	132 GB
More than 50 EPS	1 actionable events per second (POC/LAB deployment) 2) Up to 5 actionable events per second 3) Up to 20 actionable events per second 4) Up to 50 actionable events per second 5) Up to 100 actionable events per second 6) Up to 200 actionable events per second 7) Up to 250 actionable events per second			

1. *Operations Reports are only available to customers with Operations Reports license prior to May 2018. For re-installation of Operations Reports contact a Cisco customer support representative.

Gateway: IOPS (Input/Output Operations Per Second) for Different Network Sizes

This section provides IOPS tables for the different network sizes:

- [Table 2-4](#) lists the IOPS for Oracle and Infobright databases.
- [Table 2-5](#) provides a breakdown of IOPS for the Oracle database.
- [Table 2-6](#) provides a breakdown of IOPS for the Infobright database.



Note

Infobright database specifications are only relevant if you intend to install the Operations Reports component.

Table 2-4 Total IOPS for Oracle and Infobright Databases

Network Size (No. of Devices and Events Per Second (EPS))	IOPS for Oracle Datafiles	IOPS for Infobright Database	Total IOPS for Oracle and Infobright Databases
Small: 200 devices or less 5 EPS	600	85	685
Medium: 200 - 2000 devices 20 EPS	1200	170	1370
Large: 2000 - 5000 devices 50 EPS	2250	340	2590
More than 50 EPS			



Note

Prime Network supports more than 5000 NEs. For specific hardware requirement contact the Cisco Representative.

Table 2-5 Breakdown of Oracle Database IOPS

Network Size (No. of Devices and Events Per Second (EPS))	Oracle Datafiles	Oracle Redo Logs	Oracle Archive	Oracle Backup
Small: 200 devices or less 5 EPS	500	40	40	20
Medium: 200 - 2000 devices 20 EPS	1000	80	80	40
Large: 2000 - 5000 devices 50 EPS	2000	100	100	50

Table 2-6 Breakdown of Infobright Database IOPS

Network Size (No. of Devices and Events Per Second (EPS))	Infobright Data Directory (raid 5/10)	Infobright Cache Directory (raid 5/10)	Gateway DLP Directory	Total
Small: 200 devices or less 5 EPS	40	20	25	85
Medium: 200 - 2000 devices 20 EPS	80	40	50	170
Large: 2000 - 5000 devices 50 EPS	160	80	100	340

Storage Requirements for Different Network Sizes

This section provides storage requirements (in GB) for the different network sizes:

- [Table 2-7](#) lists the storage required for Oracle and Infobright databases.
- [Table 2-8](#) provides a breakdown of storage requirements for the Oracle database.
- [Table 2-9](#) provides a breakdown of storage requirements for the Infobright database.

Table 2-7 Total Storage (GB) for Oracle and Infobright Databases

Network Size (No. of Devices and Events Per Second (EPS)) ¹	Storage for Oracle Database	Storage for Infobright Database	Swap Space	Total Storage for Oracle and Infobright Databases
Small: 200 devices or less 5 EPS	419	77	16	512
Medium: 200 - 2000 devices 20 EPS	1616	306	16	1938
Large: 2000 - 5000 devices 50 EPS	3947	765	16	4728

1. The EPS numbers in the table refer to actionable events. We assume that there is a ratio of approximately 1:3 between actionable and standard events, i.e., for 50 actionable EPS, there will be an additional 150 standard EPS.

Table 2-8 Breakdown of Storage for Oracle Database

Network Size (No. of Devices and Events Per Second (EPS))	Oracle Datasize	Oracle Backup	Oracle Archive Logs ¹	Online Redo Logs	Total
Small: 200 devices or less 5 EPS	82	41	290	6	419
Medium: 200 - 2000 devices 20 EPS	299	149	1162	6	1616
Large: 2000 - 5000 devices 50 EPS	690	345	2904	8	3947

1. The archive log storage requirements are based on the default 14 days that events are retained in the archive before they are purged. This setting can be changed in the Administration GUI client to reduce the archive logs storage requirements.

Table 2-9 Breakdown of Storage for Infobright Database

Network Size (No. of Devices and Events Per Second (EPS))	Infobright Database Server	Infobright Storage Gateway DLP	Total
Small: 200 devices or less 5 EPS	75	2	77
Medium: 200 - 2000 devices 20 EPS	298	8	306
Large: 2000 - 5000 devices 50 EPS	745	20	765

Guidelines for Location of Oracle Files

Storage is required for the Oracle database data files, redo logs, archive log, and backup file.

- A *data file* is a physical file on disk that contains data structures such as tables and indexes. The optimal location is an external disk array (preferably RAID 10). The data files are created under the directory that you specify during installation.
- Online *redo logs* are a set of files that contain records of changes made to data. Redo log files should not reside on the same disk as the data files. Use ext3 mounted with the default mount options. The redo logs are created under the directory that you specify during installation.
- An *archive log* is a member of an online redo log that has been archived by the Oracle database. Archived log files should not reside on the same disk as the data files. The archived redo log files can be applied to a database backup for media recovery. The archive logs are created under the directory that you specify during installation.



Note If the embedded database mount points for network data, archive logs, or control files are set outside the local disks (for example, on a storage area network), make the corresponding entry in `/etc/fstab` (Linux) so the mount points can be accessed during reboots. If this is not done, the embedded database and gateway will not start.

- A *backup file* stores a copy of the database data, which can be used to reconstruct data. Backup files should not reside on the same disk as the data files. The backup files are created under the directory that you specify during installation.

Disk Partitions

Table 2-10 lists the required partitions and space for Prime Network 5.0 .



Note Do not use the `-override_diskspace` flag to add or free up space.

Use this information in conjunction with the gateway and unit requirements listed in [Prime Network Gateway and Database Requirements, page 2-2](#).

Table 2-10 Disk Partitions

Partition	Space (in MB)
/root	<ul style="list-style-type: none"> Database and gateway on same server—1.5 GB Database and gateway on different servers—4 GB <p>This space is required because the installer copies the Oracle installation files to the remote server under the home directory of the SSH user. This is especially important if the home directory is root (/) where over-consumption could cause the server to crash.</p>
Prime Network 5.0 installation directory	5 GB Note By default, Prime Network is installed in /export/home/pnuser
(Embedded DB only) \$NETWORKHOME/oracle (\$NETWORKHOME: /export/home/<user_name>)	6 GB (minimum) for Oracle binaries.
/tmp	100 MB (minimum) of disk space available.

Remote Embedded Database Requirements

For remote embedded database installations:

- Perl version 5.8.6 or later must be installed on the root user.
- The installation script copies the Oracle installation files to the remote server under the home directory of the user connecting to the workstation through SSH. The home directory must have at least 4 GB of space available for the installation files. This is especially important if the home directory is root (/), because over consumption might cause the server to crash.
- In addition to the list of UNIX shells required for Prime Network (see [UNIX Services and Components Used by Prime Network, page 3-10](#)), the remote embedded database also requires BASH (/bin/bash & /usr/bin/bash).

External Database Requirements

If the Prime Network gateway will be connecting to an external database, the Oracle version shown in [Table 2-11](#) must be installed with the Oracle JVM and partitioning options. The partitioning options are required because Prime Network uses partitioning for event management.

Table 2-11 Supported Oracle Versions and Required Patches

Oracle Version	Required Linux Patch(es)
Oracle Database 12c Enterprise Edition Release 12.1.0.2	---

Prime Network Unit Requirements

These topics provide the unit requirements:

- [Unit: Minimum Hardware and Software Requirements, page 2-10](#)
- [Unit: Recommended Hardware for Different Network Sizes, page 2-10](#)

Unit: Minimum Hardware and Software Requirements

[Table 2-12](#) identifies the minimum software and hardware requirements for units. The unit must have connectivity to the database.

Table 2-12 Minimum Requirements for Units

Item	Specifications
System hardware	Xeon E5-2600 or equivalent. Also see Unit: Recommended Hardware for Different Network Sizes, page 2-10 .
Software	Red Hat 6.5, Red Hat 6.8, and Red Hat 7.2 64-bit Server Edition (English language) are supported in Prime Network 5.0 and run in a virtual environment. Red Hat is supported on VMware ESXi version 5.5, and 6.0, and also on the Openstack kernel-based virtual machine (KVM) hypervisor version 2.6. Certain Red Hat services and RPMs are required. See Required Red Hat Services and RPMs, page 2-16 .

Unit: Recommended Hardware for Different Network Sizes

Before you choose the machines that will serve as your units, you need to know the total memory requirements, based on your network size (number of devices and events per second). The total memory will be distributed across your unit machines and will determine the CPU requirements for each unit.

You might choose to use several relatively small units (common in a VM environment) or fewer large units (more common with bare metal). Either way, your calculations must begin with identifying the total amount of memory required.



Note

Contact your Cisco account representative if you need assistance calculating your memory requirements.

Following is an example of total memory requirements for the different network sizes. This example is based on the following percentage distribution of device types in a Carrier Ethernet deployment:

2% Ps, 8% N-PEs, 78% U-PEs, 12% CEs

Table 2-13 Example of Total Unit Memory Requirements

Network Size	Maximum No. of Devices	Maximum No. of Events Per Second (EPS)	Total Memory Required for All Units (GB RAM)
Small	200	5	10
Medium	2000	20	100
Large	5000	50	250

The number of units you require depends on the type of servers you choose. Following are some examples of potential unit servers:

Table 2-14 **Examples of Unit Servers**

Unit Server Type	Memory (GB)	CPU Cores
VM	32	2
VM	96	6
Bare Metal (UCS-B)	256	10
Bare Metal (UCS-B)	512	20



Note

- An additional 10 - 20 GB storage is required for DLP processing
- If you are using the Operations Reports component, an additional 3% RAM is required per unit server.

Example combinations of unit servers for a large network (250 GB RAM required):

- 1 UCS-B with 256 GB RAM
- 2 VMs with 96 GB RAM each, 2 VMs with 32 GB RAM each

Disk Space Requirements

Each unit server requires a minimum of 30 GB disk space (which includes swap space and Operations Reports storage requirements).

Requirements for Gateway and Unit on a Single Server

The one-server setup, where the gateway, unit, and database run on the same server, is suitable for small-medium deployments of up to 1000 devices, supporting up to 50 actionable events and 150 standard events per second (200 EPS total).

Requirements for the one-server setup are as follows:

- 10 CPU cores
- 64 - 96 GB RAM, depending on the number of devices. 96 GB is recommended.
- 6.5 TB disk space



Note Disk space requirements increase proportionally as the number of supported events per second increases. The system has been tested for a maximum of 750 events per second (50 actionable plus 700 standard events), which would require 15 TB disk space. See [Storage Requirements for Different Network Sizes, page 2-7](#).

- 1200 IOPS (Read 300/Write 900).

If you install Operations Reports, you need an additional:

- 291 GB disk space
- 32 GB RAM
- 170 IOPS

Prime Network Client Requirements

These topics provide the client requirements:

- [Clients: Minimum Hardware and Software Requirements, page 2-12](#)
- [Using Prime Network Clients with Citrix, page 2-14](#)
- [Accessing Prime Network Clients Using Citrix Environment, page 2-14](#)


Clients: Minimum Hardware and Software Requirements

[Table 2-15](#) identifies the minimum hardware and software requirements for Prime Network clients.

Table 2-15 Prime Network Client Minimum Installation Requirements

Item	Specifications
Minimum Hardware Requirements	
IBM PC or PC-compatible workstation	<ul style="list-style-type: none"> • Pentium IV, 2.66-GHz or higher processor • 1 GB RAM • 2 GB free disk space • 512 MB free nonvirtual memory per running instance
Screen	<ul style="list-style-type: none"> • Screen resolution optimized for 1024 x 768 pixels or higher • True color (32-bit) setting

Table 2-15 Prime Network Client Minimum Installation Requirements (continued)

Item	Specifications
Minimum Software Requirements	
Operating system	<ul style="list-style-type: none"> Windows 2000, Windows XP, Windows Vista, or Windows 7 <p>Note For a Windows 32 bit system, reduce the memory allocation to 512MB in the jnlp file for launching Network Vision.</p> <ul style="list-style-type: none"> Citrix XenApp 6.0 with the Citrix Hotfix patch CTX120923, available at http://support.citrix.com/article/CTX120923, and Citrix XenApp 6.0. <p>Note The Citrix Hotfix patch requires an upgraded Citrix License Server (version 11.6.1). A single Citrix server supports multiple Citrix clients, each of which can run Cisco Prime Network clients. See Using Prime Network Clients with Citrix, page 2-14</p>
Other Software	<ul style="list-style-type: none"> Java 8 update 60. <p> Note Prime Network was tested on Java 8 update 60, however it is expected to work with lower Java 8 updates as well.</p>
Browser Requirements	
Bandwidth	1.5 MB per second bandwidth (to download)
Supported browsers for Prime Network web-based GUI applications	<ul style="list-style-type: none"> Mozilla Firefox 24, ESR 24, 26, 27, 29, 30, 49, 52, 54, 55 <p>Note Users might not be able to connect to the Prime Network Web server to use features such as VCB, Network Discovery, and CCM using Firefox if the gateway IP address is a raw IPv6 address. This is due to a Firefox defect. To avoid this issue, log into Prime Network using a hostname instead of an IP address.</p> <ul style="list-style-type: none"> Google Chrome version 31, 33, 60 Internet Explorer versions 9, 10, 11 <p>Note Network Discovery might not display properly and the Discovery Profile page might take longer than usual to load.</p>
Required browser support	<ul style="list-style-type: none"> JavaScript—Required Cookies—Enabled Pop-ups—Enabled (Firefox and Internet Explorer) Security—SSL/Certificates required for access to restricted resources
Flash Player	<ul style="list-style-type: none"> Adobe Flash player 9.0 or higher for optimal display of advanced graphics and complex UI components.

Using Prime Network Clients with Citrix

When using Prime Network with Citrix you might have issues establishing SSL connection or creating a cache folder to the Prime Network client.

Establishing SSL connection

If you are using Prime Network with Citrix and you cannot establish an SSL connection, complete the following steps:

-
- Step 1** Right-click an application in the Citrix Management Console (server side) and choose **Modify application properties > Modify all Properties**.
 - Step 2** Click the **Client Options** window.
 - Step 3** Uncheck the **Enable SSL and TLS protocols** check box.
-

Updating Permissions on Citrix

If you cannot create a cache folder or download .jar files to the Prime Network client, there might be a problem with permission definitions on Citrix. Complete the following steps to update permissions:

-
- Step 1** Right-click the client installation folder (usually C:\Cisco Systems\Prime Network\) and choose **Properties**.
 - Step 2** Click the **Security** tab.
 - Step 3** Click the **Users** group and check the **Allow** check box to modify permissions.
 - Step 4** Click **OK**.

Accessing Prime Network Clients Using Citrix Environment

Prerequisites

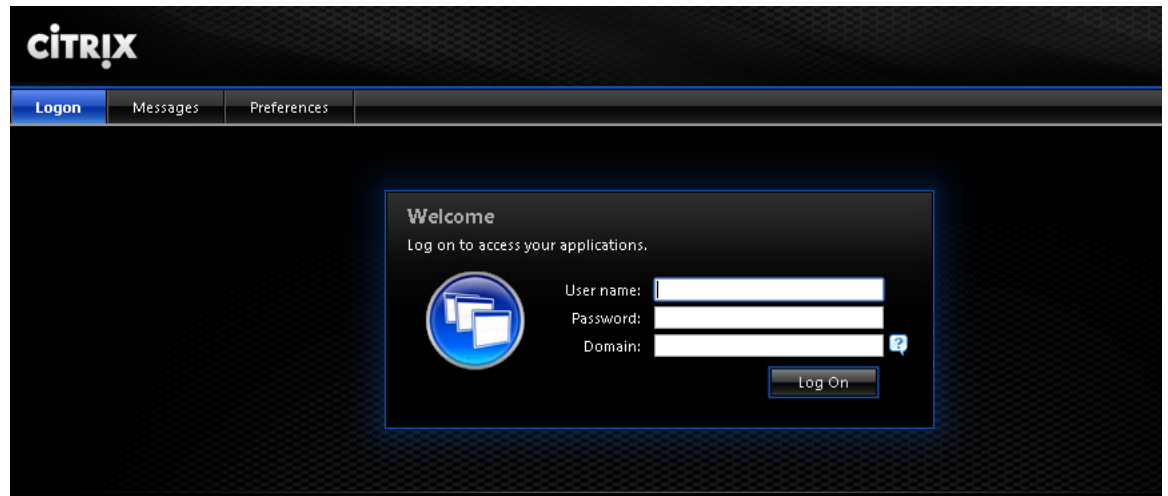
- Click the below link to install and configure the Citrix XenApp 6.0

http://docwiki.cisco.com/wiki/Citrix_XenApp_Server_6.0_Installation_for_Accessing_Prime_Network_in_Standalone_and_Suite_Modes

- Ensure that the server on which the Citrix XenApp is installed is configured with correct time and the time zone. Example for IST, the zone should be configured as (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi.

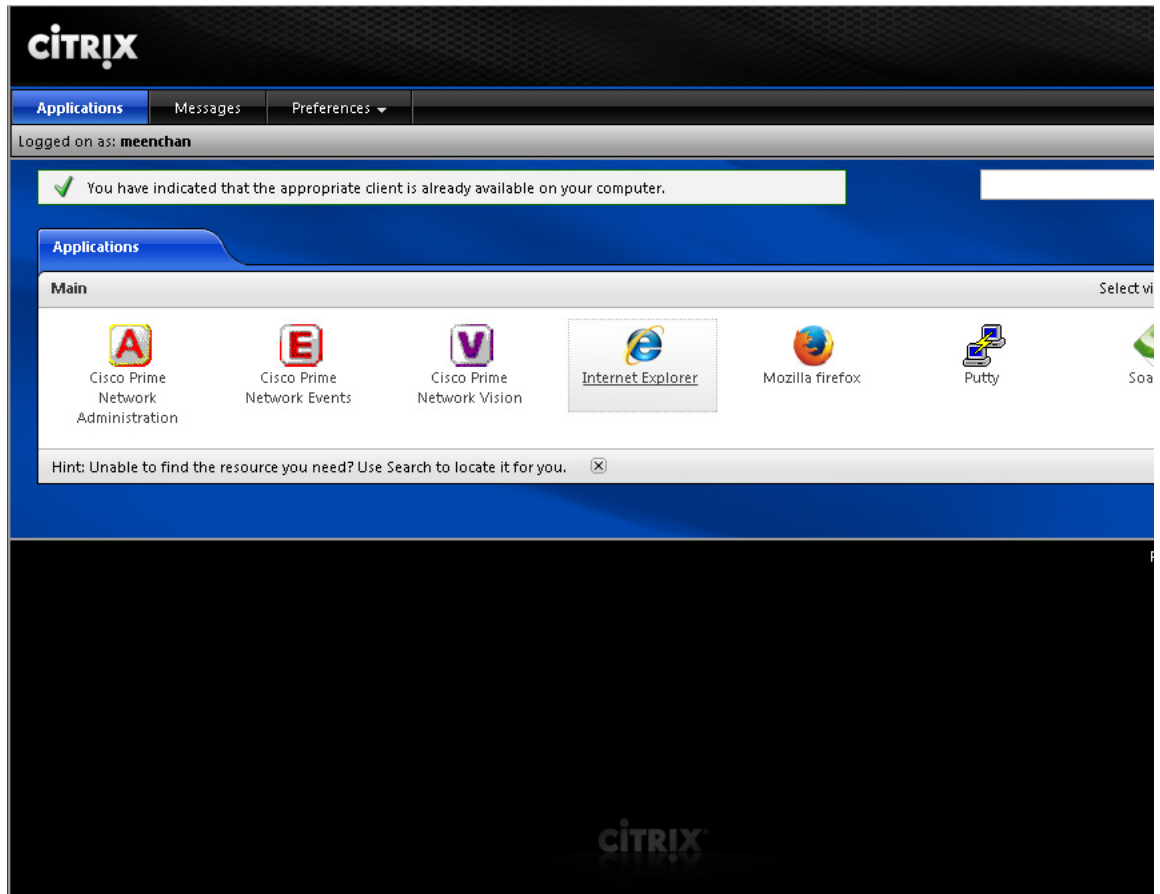
Once the Citrix online plugin and receiver are installed on client machine, the Prime Network features are enabled to be accessed in a Citrix environment. The user is provided with a Citrix enabled URL with login credentials.

Figure 2-1 Citrix Login Screen



Once logged in, the Prime Network applications are displayed and can be accessed by the user.

Figure 2-2 Viewing Prime Network Applications in Citrix Environment



Required Red Hat Services and RPMs

The following sections list the required Red Hat services and RPMs:

- [Required RPMs for Red Hat 6.5, page 2-16](#)
- [Required RPMs for Red Hat 6.7, page 2-17](#)
- [Required RPMs for Red Hat 6.8, page 2-20](#)
- [Required RPMs for Red Hat 7.2, page 2-23](#)
- [Required RPMs for Oracle Database 12c, page 2-24](#)

Required RPMs for Red Hat 6.5

The following RPMs must be downloaded from the Red Hat website and installed on the gateway and unit servers.

Required 32-bit packages

- compat-libstdc++-33-3.2.3-69.el6.i686
- glibc-2.12-1.132.el6.i686

- libgcc-4.4.7-4.el6.i686
- libstdc++-4.4.7-4.el6.i686
- libaio-devel-0.3.107-10.el6.i686
- libXtst-1.2.1-2.el6.i686(Required for GUI installation)
- libgcj-4.4.7-4.1.el6_5.i686(Required for GUI installation)

Minimum Required 64-bit packages

- binutils-2.20.51.0.2-5.36.el6.x86_64
- libXtst-1.2.1-2.el6.x86_64 (Required for GUI installation)
- libgcj-4.4.7-4.1.el6_5.x86_64(Required for GUI installation)
- compat-libcap1-1.10-1.x86_64
- compat-libstdc++-33-3.2.3-69.el6.x86_64
- openssl098e-0.9.8e-17.el6_2.2.x86_64 (Required for installing Operations Reports)
- gcc-c++-4.4.7-4.el6.x86_64
- glibc-devel-2.12-1.132.el6.x86_64
- numactl-2.0.7-8.el6.x86_64
- ksh-20120801-10.el6.x86_64
- libgcc-4.4.7-4.el6.x86_64
- libstdc++-devel-4.4.7-4.el6.x86_64
- libaio-devel-0.3.107-10.el6.x86_64
- make-3.81-20.el6.x86_64
- sysstat-9.0.4-22.el6.x86_64
- expect-5.44.1.15-5.el6_4.x86_64
- openssh-server-5.3p1-94.el6.x86_64
- openssh-5.3p1-94.el6.x86_64
- telnet-0.17-47.el6_3.1.x86_64
- dos2unix-3.1-37.el6.x86_64
- openssl-1.0.1e-30.el6_6.11

For high availability, the following packages are required:

- elfutils-libelf
- elfutils-libelf-devel
- numactl-devel

Required RPMs for Red Hat 6.7

The following RPMs must be downloaded from the Red Hat website and installed on the gateway and unit servers.

Required 32-bit packages

- libgcc-4.4.7-17.el6.i686

- nss-softokn-freebl-3.14.3-23.3.el6_8.i686
- compat-libstdc++-33-3.2.3-69.el6.i686
- glibc-2.12-1.192.el6.i686
- libstdc++-4.4.7-17.el6.i686

Required 64-bit packages

- gpg-pubkey-fd431d51-4ae0493b
- libgcc-4.4.7-17.el6.x86_64
- gcc-c++-4.4.7-17.el6.x86_64
- psc-lite-libs-1.5.2-15.el6.x86_64
- telnet-0.17-48.el6.x86_64
- glibc-2.12-1.192.el6.x86_64
- compat-libcap1-1.10-1.x86_64
- cpp-4.4.7-17.el6.x86_64
- nspr-4.11.0-1.el6.x86_64
- nss-tools-3.21.3-2.el6_8.x86_64
- mpfr-2.4.1-6.el6.x86_64
- ksh-20120801-33.el6.x86_64
- expect-5.44.1.15-5.el6_4.x86_64
- nss-softokn-freebl-3.14.3-23.3.el6_8.x86_64
- cloog-ppl-0.15.7-1.2.el6.x86_64
- ntp-4.2.6p5-10.el6.1.x86_64
- nss-sysinit-3.21.3-2.el6_8.x86_64
- java-1.7.0-openjdk-devel-1.7.0.121-2.6.8.1.el6_8.x86_64
- libstdc++-4.4.7-17.el6.x86_64
- libstdc++-devel-4.4.7-17.el6.x86_64
- ppl-0.10.2-11.el6.x86_64
- telnet-server-0.17-48.el6.x86_64
- gpg-pubkey-2fa658e0-45700c69
- tcl-8.5.7-6.el6.x86_64
- tzdata-2016j-1.el6.noarch
- glibc-headers-2.12-1.192.el6.x86_64
- glibc-devel-2.12-1.192.el6.x86_64
- ntpdate-4.2.6p5-10.el6.1.x86_64
- nss-3.21.3-2.el6_8.x86_64
- java-1.7.0-openjdk-1.7.0.121-2.6.8.1.el6_8.x86_64
- dos2unix-3.1-37.el6.x86_64
- glibc-common-2.12-1.192.el6.x86_64
- libaio-devel-0.3.107-10.el6.x86_64

- libgomp-4.4.7-17.el6.x86_64
- nss-util-3.21.3-1.el6_8.x86_64
- xinetd-2.3.14-40.el6.x86_64
- compat-libstdc++-33-3.2.3-69.el6.x86_64
- gcc-4.4.7-17.el6.x86_64
- lksctp-tools-1.0.10-7.el6.x86_64

For high availability, the following packages are required:

- binutils.x86_64
- cluster-cim.x86_64
- cman.x86_64
- compat-libcap1.x86_64
- compat-libstdc++-33.i686
- compat-libstdc++-33.x86_64
- dos2unix.x86_64
- elfutils-libelf-devel.x86_64
- elfutils-libelf.x86_64
- expect.x86_64
- gcc-c++.x86_64
- gcc.x86_64
- glibc-common.x86_64
- glibc-devel.x86_64
- glibc-devel.x86_64
- glibc-headers.x86_64
- glibc.i686
- glibc.x86_64
- ksh.x86_64
- libaio-devel.i686
- libaio.i686
- libaio.x86_64
- libgcc.i686
- libgcc.x86_64
- libgej.i686
- libstdc++-devel.i686
- libstdc++-devel.x86_64
- libstdc++.i686
- libstdc++.x86_64
- libX11.i686
- libX11.x86_64

- libXau.i686
- libXau.x86_64
- libxcb.i686
- libxcb.x86_64
- libXext.i686
- libXext.x86_64
- libXi.i686
- libXi.x86_64
- libXtst.i686
- libXtst.x86_64
- luci.x86_64
- make.x86_64
- modcluster.x86_64
- numactl-devel.x86_64
- numactl.x86_64
- openais.x86_64
- openssh-clients.x86_64
- openssh-server.x86_64
- openssh.x86_64
- openssl098e.x86_64
- rgmanager.x86_64
- ricci.x86_64
- sysstat.x86_64
- sysstat.x86_64
- telnet.x86_64

Required RPMs for Red Hat 6.8

The following RPMs must be downloaded from the Red Hat website and installed on the gateway and unit servers.

Required 32-bit packages

- compat-libstdc++-33-3.2.3-69.el6.i686.rpm
- glibc-2.12-1.192.el6.i686.rpm
- libgcc-4.4.7-17.el6.i686.rpm
- nss-softokn-freebl-3.14.3-23.el6_7.i686.rpm

Required 64-bit packages

- ksh-20120801-33.el6.x86_64.rpm
- expect-5.44.1.15-5.el6_4.x86_64.rpm

- tcl-8.5.7-6.el6.x86_64.rpm
- telnet-0.17-48.el6.x86_64.rpm
- dos2unix-3.1-37.el6.x86_64.rpm
- compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm
- compat-libcap1-1.10-1.x86_64.rpm
- libaio-devel-0.3.107-10.el6.x86_64.rpm
- libstdc++-devel-4.4.7-17.el6.x86_64.rpm
- cloog-ppl-0.15.7-1.2.el6.x86_64.rpm
- cpp-4.4.7-17.el6.x86_64.rpm
- gcc-4.4.7-17.el6.x86_64.rpm
- gcc-c++-4.4.7-17.el6.x86_64.rpm
- mpfr-2.4.1-6.el6.x86_64.rpm
- ppl-0.10.2-11.el6.x86_64.rpm
- libgcj-4.4.7-17.el6.x86_64.rpm

For GUI Installation, the following packages are required:

Required 64-bit package

- libgcj-4.4.7-17.el6.x86_64

Required 32-bit package

- libgcj.i686

For Operations Reports installation, the following package is required:

Required 64-bit packages

- openssl098e-0.9.8e-20.el6_7.1.x86_64

For high availability, the following packages are required:

RPMs	Dependencies
ksh.x86_64	compat-libxcb-1.9-1.el7.i686
libstdc++.i686	compat-libstdc++-33.x86_64
expect.x86_64	compat-libxcb-1.9-1.el7.x86_64
libstdc++.x86_64	gcc-c++.x86_64
dos2unix.x86_64	compat-libstdc++-33.i686 0:3.2.3-72.el7
glibc-devel-2.12	compat-libstdc++-33-3.2.3-72.el7.x86_64
redhat-lsb-core.x86_64	libstdc++.x86_64
gcc-4.4.4	compat-libf2c-34.x86_64
compat-libstdc++-33-3.2.3-72.el7.x86_64	compat-libgfortran-41.x86_64
libaio-devel-0.3.107	compat-libtermcap.x86_64
compat-libstdc++-33-3.2.3	compat-libxcb.x86_64
binutils.x86_64	libstdc++-devel-4.4.4.x86_64

RPMs	Dependencies
libXext.x86_64	libXxf86vm.x86_64
compat-libcap1-1.10.x86_64	gcc-c++-4.4.4.x86_64
libxcb.x86_64	compat-libcap1.x86_64
compat-libstdc++-33-3.2.3-72.el7.i686	libdmx.x86_64
libXxf86dga.x86_64	gcc.x86_64
perl-Data-Dumper-2.145-3.el7.x86_64	make.x86_64
libX11.x86_64	nfs-utils.x86_64
glibc-devel.x86_64	libXi.x86_64
xorg-x11-utils.x86_64	libXau.x86_64
libgcc.x86_64	libXxf86misc.x86_64
libXv.x86_64	smartmontools.x86_64
libstdc++-devel.x86_64	glibc.x86_64
libXt.x86_64	elfutils-libelf-devel.x86_64
libXtst.x86_64	iptables-1.4.21-18.2.el7_4.x86_64
sysstat.x86_64	libaio.x86_64
numactl-devel.x86_64	compat-libgmp-4.3.1-1.sl7.x86_64 (for GUI installation)
xorg-x11-xauth.x86_64	compat-libmpfr-2.4.1-1.sl7.x86_64 (for GUI installation)
iptables-services-1.4.21-18.2.el7_4.x86_64	libgcj-2.96-28.i386 (for GUI installation)
gmp-4.3.1-12.el6.i686 (for GUI installation)	libgcj3-3.0.1-3.i386 (for GUI installation)
libgcj-2.96-27.i386 (for GUI installation)	libgcj3-devel-3.0.1-3.i386 (for GUI installation)
libgcj-4.4.7-4.1.el6_5.i686 (for GUI installation)	libgcj-devel-2.96-27.i386 (for GUI installation)
libpng12-1.2.50-10.el7.x86_64(Graph)	
libpng-1.5.13-7.el7_2.x86_64(Graph)	

RPMS Dependent on Above Listed Packages

- cloog-ppl.x86_64 0:0.15.7-1.2.el6
- cpp.x86_64 0:4.4.6-4.el6
- glibc-headers.x86_64 0:2.12-1.80.el6
- kernel-2.6.32-573.el6.x86_64
- mpfr.x86_64 0:2.4.1-6.el6
- ppl.x86_64 0:0.10.2-11.el6

Required RPMs for Red Hat 7.2

The following RPMs must be downloaded from the Red Hat website and installed on the gateway and unit servers.

Required 64-bit packages

RPMs	
ksh.x86_64	
expect.x86_64	libstdc++.i686
dos2unix.x86_64	glibc-devel-2.12.x86_64
redhat-lsb-core.x86_64	gcc-4.4.4.x86_64
compat-libstdc++-33-3.2.3.x86_64	compat-libstdc++-33-3.2.3-72.el7.x86_64
libaio-devel-0.3.107.x86_64	binutils.x86_64
compat-libxcb-1.9-1.el7.i686	compat-libstdc++-33.x86_64
compat-libxcb-1.9-1.el7.x86_64	gcc-c++.x86_64
compat-libstdc++-33.i686 0:3.2.3-72.el7.x86_64	ksh.x86_64
compat-libstdc++-33-3.2.3-72.el7.x86_64	libstdc++.x86_64
compat-lib*.x86_64	libXext.x86_64
compat-libcap1-1.10.x86_64	libXxf86dga.x86_64
compat-libstdc++-33-3.2.3-72.el7.i686	libX11.x86_64
perl-Data-Dumper-2.145-3.el7.x86_64	libXxf86vm.x86_64
libstdc++-devel-4.4.4.x86_64	compat-libcap1.x86_64
gcc-c++-4.4.4.x86_64	gcc.x86_64
libdmx.x86_64	glibc-devel.x86_64
make.x86_64	libgcc.x86_64
xorg-x11-utils.x86_64	libstdc++-devel.x86_64
libXv.x86_64	libXtst.x86_64
libXt.x86_64	libXi.x86_64
nfs-utils.x86_64	libXxf86misc.x86_64
libXau.x86_64	smartmontools.x86_64
glibc.x86_64	elfutils-libelf-devel.x86_64
sysstat.x86_64	numactl-devel.x86_64
xorg-x11-xauth.x86_64	iptables-1.4.21-18.2.el7_4.x86_64
libaio.x86_64	compat-libgmp-4.3.1-1.sl7.x86_64 (for GUI installation)
iptables-services-1.4.21-18.2.el7_4.x86_64	compat-libmpfr-2.4.1-1.sl7.x86_64 (for GUI installation)
gmp-4.3.1-12.el6.i686 (for GUI installation)	libgcj-2.96-28.i386 (for GUI installation)
libgcj-2.96-27.i386 (for GUI installation)	libgcj3-3.0.1-3.i386 (for GUI installation)

RPMs	
libgcj-4.4.7-4.1.el6_5.i686 (for GUI installation)	libgcj3-devel-3.0.1-3.i386 (for GUI installation)
libpng12-1.2.50-10.el7.x86_64(Graph)	libgcj-devel-2.96-27.i386 (for GUI installation)
libpng-1.5.13-7.el7_2.x86_64(Graph)	

Required RPMs for Oracle Database 12c

The following packages, or later versions of them, are required for the Oracle 12c database on Red Hat.

RPMs	
compat-libcogl12-1.14.0-3.el7.x86_64	compat-libxcb-1.9-1.el7.x86_64
compat-libcogl-pango12-1.14.0-3.el7.x86_64	compat-libmediaart0-0.7.0-1.el7.x86_64
compat-libmpc-1.0.1-3.el7.x86_64	compat-libgweather3-3.8.2-1.el7.x86_64
libmediaart-1.9.1-1.el7.x86_64	compat-libpackagekit-glib2-16-0.8.9-1.el7.x86_64
compat-libgnome-bluetooth11-3.8.2.1-2.el7.x86_64	compat-libgdata13-0.13.3-1.el7.x86_64
compat-libgnome-desktop3-7-3.8.4-2.el7.x86_64	compat-libgfortran-41-4.1.2-44.el7.x86_64
compat-libcolord1-1.0.4-1.el7.x86_64	libXau-1.0.8-2.1.el7.i686
compat-libtiff3-3.9.4-11.el7.x86_64	libxcb-1.12-1.el7.i686
compat-libupower-glib1-0.9.20-1.el7.x86_64	compat-libxcb-1.9-1.el7.i686
compat-libf2c-34-3.4.6-32.el7.x86_64	libmediaart-0.7.0-1.el7.x86_64
compat-libgfortran-41-4.1.2-44.el7.x86_64	compat-libcogl12-1.14.0-3.el7.x86_64
compat-libgdata13-0.13.3-1.el7.x86_64	compat-libmediaart0-0.7.0-1.el7.x86_64
compat-libpackagekit-glib2-16-0.8.9-1.el7.x86_64	compat-libxcb-1.9-1.el7.x86_64
compat-libgweather3-3.8.2-1.el7.x86_64	compat-libf2c-34-3.4.6-32.el7.x86_64
compat-libcogl-pango12-1.14.0-3.el7.x86_64	compat-libupower-glib1-0.9.20-1.el7.x86_64
compat-libtiff3-3.9.4-11.el7.x86_64	libxcb-1.12-1.el7.i686
compat-libcolord1-1.0.4-1.el7.x86_64	compat-libgnome-bluetooth11-3.8.2.1-2.el7.x86_64
compat-libgnome-desktop3-7-3.8.4-2.el7.x86_64	libmediaart-1.9.1-1.el7.x86_64
libXau-1.0.8-2.1.el7.i686	compat-libxcb-1.9-1.el7.i686
compat-libmpc-1.0.1-3.el7.x86_64	libXau.i686
libmediaart-0.7.0-1.el7.x86_64	libmediaart.x86_64
compat-libstdc++-33-3.2.3	

Required Ports for Prime Network

These topics list the required ports for Prime Network.

- [Prime Network Server, HTTP, TCP, and UDP Ports, page 2-25](#)
- [Prime Network Integration Layer Ports, page 2-28](#)

If a firewall is enabled on the system, use this command to open required ports:

```
iptables -A INPUT -p <protocol> --dport <destination port> -j ACCEPT
```

Prime Network Server, HTTP, TCP, and UDP Ports

[Table 2-16](#) lists the default ports used by the various Prime Network server and client applications. It also lists the HTTP, TCP, and UDP ports and directions.

You can check the status of the listed ports by executing the following command:

```
# netstat -tulnap | grep port-number
```

Table 2-16 Prime Network Server, HTTP, TCP, and UDP Ports

Port No.	Source	Destination	Used for:
21 and 22(TCP)	Gateway	Remote FTP/SFTP server	Exporting Change and Configuration Management configurations to remote FTP server when the gateway is hosting user-created VNEs Note This is not a recommended configuration. Unit servers, not the gateway server, should host device VNEs.
22	Unit	Network elements	Default port for SSHv1 or SSHv2
23 (TCP)	Unit	Network elements (VNEs)	Telnet collector
25 (TCP)	Gateway	SMTP server	SMTP port (recommended for embedded database, and optional for external database)
25 (TCP)	Database server	SMTP server	SMTP port recommended for an embedded database If gateway server and database server are different, keep port 25 open on both. Note If you do not want to receive e-mail notifications, you do not have to configure the SMTP server.
69 (UDP)	Network element	Unit	<ul style="list-style-type: none"> • Default TFTP server on units • AVM 83, which is the TFTP server used by Change and Configuration Management Note To use AVM 83, you must disable the default TFTP server such that the port is free and available. Otherwise, Change and Configuration Management operations will fail. Note Do not block the port number 1069. Prime Network uses this port to listen the TFTP traffic flow.
69 (UDP)	Gateway	Network elements	Transferring images to and from network elements

Table 2-16 Prime Network Server, HTTP, TCP, and UDP Ports (continued)

Port No.	Source	Destination	Used for:
123 (UDP)	Unit	Gateway	NTP synchronization between gateway and units
123 (UDP)	Gateway	NTP server 1	NTP synchronization for gateway
161 (UDP) 1161 (UDP, Linux only)	Unit	Network elements	For units with VNEs , these ports are used for SNMP polling by the VNEs. For units with AVM100 , you need these ports only if you use SNMPv3, for engine discovery.
161 (UDP) 1161 (UDP, Linux only)	Network Elements	Unit	For Units with AVM100 , if you use SNMP v3. Note For 161 (UDP), if AVM100 resides on the gateway, the Network Elements sends to the gateway.
162 (UDP) 1162 (UDP, Linux only)	Network Elements	Unit	For Units with AVM100 , these ports are used for traps. Note For 162 (UDP), if AVM100 resides on the gateway, the Network Elements sends to the gateway.
162 (UDP) 1162 (UDP, Linux only)	Unit	Network elements	SNMP v3 inform replies
162 (TCP/UDP)	Gateway	Northbound NMS	EPM MIB notifications
514 (UDP)	Network elements (VNEs)	Unit Note If AVM100 resides on the gateway, the Network Elements sends to the Gateway.	Syslog Note If port 514 is occupied when you install Prime Network, you are prompted to make the port available. However, you are given the option to continue with port 514 occupied, and the installation completes successfully.
1101 (TCP)	Unit	Gateway	Prime Network user exclusive bidirectional hardened SSH connection for system administration operations
1101 (TCP)	Gateway	Unit	
1102 (TCP)	Gateway	Database server	Prime Network user exclusive bidirectional hardened SSH connection for system administration operations Note This SSH port is mandatory only for an embedded database.
1102 (TCP)	Database server	Gateway	
1311 (TCP)	Prime Network clients	Gateway	Prime Network monitoring system (SSL over HTTP)
1521 (TCP)	Prime Network clients	Database server	Prime Network Events database access
1521 (TCP)	Unit	Database server	Event persistency
1521 (TCP)	Gateway	Database server	Gateway persistency services

Table 2-16 Prime Network Server, HTTP, TCP, and UDP Ports (continued)

Port No.	Source	Destination	Used for:
2148 (TCP)	Local Geographical Redundant server	Remote geographical redundancy server	If you implement the Veritas gateway high availability solution, port 2148 is used by Veritas, and AVM 148 cannot be used.
2148 (TCP)	Remote Geographical Redundant server	Local geographical Redundancy server	
38751	Unit	Network elements	Default Telnet port
38752	Unit	Network elements	Default SSL port
9605 (TCP) 42607 (TCP)	WEB UI Server/Tomcat	Compliance Audit Engine	Compliance Audit Engine default connection port.
5029	Unit	DB server	Operations Reports database (Infobright)
6080 (TCP)	Client	Gateway	HTTP for web access and web start. Used to download the client from the gateway server, client updates (jar files), and online help files.
6081 (TCP)	Client	Gateway	HTTP over SSL for web access and web services such as Operations Reports
6081 (TCP)	Unit	Gateway	HTTP over SSL for key exchange during unit configuration
8000 (TCP)	Unit	Unit	Local management over http
	Gateway	Gateway	
8009 (TCP)	Client	Gateway	Tomcat server AJP connector port, used for Change and Configuration Management and Operations Reports. ¹
8011 (TCP)	Unit	Unit	Local management over http
	Gateway	Gateway	
8024	Client	Gateway	Operations Reports
8043 (HTTPS)	Client	Gateway	Secure HTTP port for Change and Configuration Management, Network Discovery, and VCB web clients.
8080 (HTTP)	Client	Gateway	<p>HTTP port for Change and Configuration Management, VCB, and Network Discovery web clients.</p> <p>By default, this port is disabled and the secure 8043 HTTP port is enabled for these clients. To use port 8080, you must enable it manually, as follows:</p> <pre># cd \$NCCM_HOME/scripts/ # ./nccmHTTP.csh enable # dmctl stop # dmctl start</pre>
8092	AVM 76	AVM 77	CCM NBI service
8099 (TCP)	Unit	Unit	Local management over HTTP
	Gateway	Gateway	

Table 2-16 Prime Network Server, HTTP, TCP, and UDP Ports (continued)

Port No.	Source	Destination	Used for:
8445 (HTTPS)	Client	Prime Network Operations Reports BA Console	Secure HTTP port for Prime Network Operations Reports web client.
9002 (TCP)	Gateway	Gateway	Prime Network BQL Note Port 9002 is a local port only.
9003 (SSL)	Prime Network clients	Gateway	Prime Network BQL over SSL
9005 (TCP)	Client	Gateway	Web GUI server port, used for Change and Configuration Management
9009 (TCP)	Client	Gateway	Web GUI server AJP connector port, used for Change and Configuration Management
9080 (TCP)	Client	Gateway	Web GUI server HTTP connector port, used for Change and Configuration Management
9443 (TCP)	Client	Gateway	Web GUI server HTTPS connector port, used for Change and Configuration Management
9390 (TCP)	Gateway	Unit	Transport internal processes.
9490 (TCP)	Unit	Gateway	Prime Network secured SSL transport
9770 (TCP) and 9771 (TCP)	Prime Network clients	Gateway	Prime Network Vision, Administration, Events.
9875 (TCP)	Client	Gateway	Spring JMX console port, used for Change and Configuration Management

Prime Network Integration Layer Ports

[Table 2-17](#) lists the ports used by the Prime Network Integration Layer (PN-IL). The PN-IL allows Prime Network to expose Multi-Technology Operations Systems Interface (MTOSI) APIs over Simple Object Access Protocol (SOAP).

Table 2-17 SIL Ports

Port No.	Source	Destination	Used for:
1100 (TCP) - Private	Integration Layer Framework	Integration Layer Framework	Karaf JMX RMI registry (Integration layer management). Note Allow access to this port from local host.
9500 (TCP) - Private (localhost)			Karaf SSH Shell Note Make sure this application is not in use by another application or process.
9095		-	Auditlog NBI Web Service
9020		-	Alarm Management NBI Web Service
9229		-	3GPP Notification Consumer WSDL will be exposed
9201		-	MTOSI Notification Consumer WSDL will be exposed

Table 2-17 SIL Ports (continued)

Port No.	Source	Destination	Used for:
9110 (TCP) - Public	MTOSI adapter	Integration Layer Framework	MTOSI web service implementation (MTOSI WS-SOAP NBI)
9220 (TCP) - Public	3GPP adapter	Integration Layer Framework	3GPP web service implementation (3GPP WS-SOAP NBI)
32768 - 61000 (TCP) - Private/Public	Integration Layer Framework	Integration Layer Framework	Ephemeral Ports Note Allow access to this port from the local host, unless the integration layer uses a distributed installation with JMS SSL transport.
44445 (TCP) - Private			Karaf JMX RMI server (Prime Network integration layer management). Note Allow access to this port from localhost.
61615(TCP) - Private/Public			JMS SSL transport Note Allow access to this port from the local host, unless the integration layer uses a distributed installation with JMS SSL transport.
61616 (TCP) - Private/Public			JMS NIO transport Note Allow access to this port from the local host, unless integration layer uses a distributed installation with JMS NIO transport.



CHAPTER 3

Preparing for the Installation

This chapter provides preinstallation tasks that must be performed and verified before proceeding with the Prime Network installation.

- [Gateway Preinstallation Tasks—Embedded Database, page 3-1](#)
- [Gateway Preinstallation Tasks—External Database, page 3-3](#)
- [Unit Preinstallation Tasks, page 3-5](#)
- [IPv4 and IPv6 Compliance Considerations, page 3-9](#)
- [UNIX Services and Components Used by Prime Network, page 3-10](#)



Note

All procedures in this chapter are performed as the root user.

Gateway Preinstallation Tasks—Embedded Database

[Table 3-1](#) shows the tasks that you must perform before installing Prime Network on a gateway that uses an embedded database. All procedures should be performed as the root user.

Table 3-1 Gateway Preinstallation tasks Using an Embedded Database


	Task	Refer to (or perform):
Step 1	Verify that the Disk 1: New Install DVD is available.  Note If the Installation DVD is not available, mount the build server on the gateway and access the required build for PN installation.	Installation DVDs, page 1-2
Step 2	Verify that the server machines meet the system requirements.	Installation Requirements, page 2-1

Table 3-1 Gateway Preinstallation tasks Using an Embedded Database (continued)

	Task	Refer to (or perform):
Step 3	<p>Ensure you have the following SSH connectivity as root:</p> <ul style="list-style-type: none"> • Gateway to unit • Unit to gateway • Unit to localhost • Gateway to localhost 	—
Step 4	<p>Verify that the server machines meet the Oracle database requirements.</p>	<p>Prime Network Gateway and Database Requirements, page 2-2</p> <p>The following steps are applicable only for RHEL 7.2.</p> <p>Before you begin to Install Prime Network 5.0, ensure to:</p> <ol style="list-style-type: none"> 1. Edit the file in the following path: <code>/etc/systemd/logind.conf</code> 2. Uncomment the <code>RemoveIPC=no</code> by removing the leading #, for example, <code>#RemoveIPC=no</code> to <code>RemoveIPC=no</code>. 3. Stop the Firewall: <code>systemctl stop firewalld.service</code>
Step 5	<p>Verify the installed operating system.</p>	<p>Verifying the Installed Operating System, page 3-6</p>
Step 6	<p>Disable SELinux.</p>	<p>In <code>/etc/selinux/config</code>, configure <code>SELINUX=disabled</code>, then reboot the machine.</p>
Step 7	<p>Verify the RPM files required for Prime Network on Red Hat are installed.</p>	<p>Verifying the RPMs Required on Red Hat for Prime Network, page 3-6</p>
Step 8	<p>Verify that all the ports designated for Prime Network are free.</p>	<p>Required Ports for Prime Network, page 2-25</p>
Step 9	<p>Allocate the storage for the Oracle database files. By default, Prime Network supports an archive size of 14 days.</p> <p>Contact your Cisco account representative for assistance.</p>	<p>Also see the database requirements in Breakdown of Oracle Database IOPS.</p>
Step 10	<p>Verify that the time of the servers is synchronized.</p>	<p>Configuring the Network Timing Protocol, page 3-7.</p>
Step 11	<p>Enable the <code>jar</code> command in the root user path on all machines where you will install Prime Network.</p>	<p>Run <code>which jar</code> to verify that the <code>jar</code> command is available.</p>
Step 12	<p>Verify that the user has root privileges on the gateway.</p>	—
Step 13	<p>Verify that DNS is enabled on the Prime Network gateway, unit, and client machines.</p>	—

Table 3-1 Gateway Preinstallation tasks Using an Embedded Database (continued)

	Task	Refer to (or perform):
Step 14	Verify that the hosts file (/etc/hosts) is configured to include the machine's local hostname and its IP address.	Do not put the hostname and local host address on the same line, as shown in the bad /etc/hosts example. Valid /etc/hosts file: <pre>127.0.0.1 localhost.localdomain localhost ::1 localhost6.localdomain localhost6 10.56.117.131 pnqa-ha-p2 pnqa-ha-p2.cisco.com</pre> Invalid /etc/hosts file: <pre>127.0.0.1 localhost.localdomain localhost hostname1 ::1 localhost6.localdomain localhost6</pre>
Step 15	Verify the minimum Swap file memory size is 8GB	If the installation fails because of missing swap file check the swap file minimum allowed size. The minimum allowed swap file size is 8192000.

Gateway Preinstallation Tasks—External Database

Table 3-2 lists the tasks that you must perform before installing Prime Network on a gateway that uses an external database. All procedures should be performed as the root user.

Table 3-2 Gateway Preinstallation Tasks Checklists For External Database

	Task	Refer to (or perform):
Step 1	Verify that the Disk 1: New Install DVD is available.	Installation DVDs, page 1-2
Step 2	Verify that the server machines meet the system requirements.	Installation Requirements, page 2-1
Step 3	Ensure you have the following SSH connectivity as root: <ul style="list-style-type: none"> • Gateway to unit • Unit to gateway • Unit to localhost • Gateway to localhost 	—

Table 3-2 Gateway Preinstallation Tasks Checklists For External Database (continued)

	Task	Refer to (or perform):
Step 4	Verify that the server meets the Oracle database requirements.	Prime Network Gateway and Database Requirements, page 2-2 Before you begin to Install Prime Network 5.0, ensure to: <ol style="list-style-type: none"> 1. Edit the file in the following path: /etc/systemd/logind.conf 2. Change the value to <i>Set RemoveIPC=no</i> 3. Remove the following comment: Reboot Server 4. Stop the Firewall: service firewalld stop
Step 5	Verify the installed operating system.	Verifying the Installed Operating System, page 3-6
Step 6	Disable SELinux.	In /etc/selinux/config, configure SELINUX=disabled, then reboot the machine.
Step 7	Verify the RPM files required for Prime Network on Red Hat are installed.	Verifying the RPMs Required on Red Hat for Prime Network, page 3-6
Step 8	Verify that all the ports designated for Prime Network are free.	Required Ports for Prime Network, page 2-25.
Step 9	Verify that the Oracle database is configured before proceeding with the installation.	Preparing the Oracle External Database, page 4-1.
Step 10	Start the Oracle listener after installing the database.	Starting the Oracle Listener (External Database), page 3-7
Step 11	(Optional) Collect the following details: <ul style="list-style-type: none"> • Port number • SID • Data file location 	Required if you do <i>not</i> want Prime Network to auto-configure your database during the installation. Note Confirm the absolute path and location of the Oracle data files with your database administrator. The location can be under the <i>ORACLEHOME</i> directory or under any other pre-allocated, mounted directory that has oracle:oinstall or oracle:dba permissions.
Step 12	Pre-allocate the storage for the Oracle database files.	See Prime Network Gateway and Database Requirements, page 2-2. Note Contact your Cisco account representative if you need assistance.
Step 13	Verify that the time of the servers is synchronized.	Configuring the Network Timing Protocol, page 3-7
Step 14	Verify that the time zone setting on all Prime Network servers is GMT (with 0 offset). Prime Network stores events in the database in GMT format. The Prime Network clients convert events to the time zone that is configured on the client workstation.	—
Step 15	Enable the jar command in the root user path on all machines where you will install Prime Network.	Run which jar .
Step 16	Verify that the user has root privileges on the gateway.	—

Table 3-2 Gateway Preinstallation Tasks Checklists For External Database (continued)

	Task	Refer to (or perform):
Step 17	Verify that DNS is enabled on the Prime Network gateway, unit, and client machines.	—
Step 18	Verify that the hosts file (/etc/hosts) is configured to include the machine's local hostname and its IP address.	<p>Do not put the hostname and local host address on the same line, as shown in the bad /etc/hosts example.</p> <p>Valid /etc/hosts file:</p> <pre>ip_address1 hostname1.domain hostname1 127.0.0.1 localhost.localdomain localhost ::1 localhost6.localdomain localhost6</pre> <p>Invalid /etc/hosts file:</p> <pre>ip_address1 hostname1.domain hostname1 localhost 127.0.0.1 localhost.localdomain localhost hostname1 ::1 localhost6.localdomain localhost6</pre>

Unit Preinstallation Tasks

Table 3-3 shows the tasks that you must verify or perform before proceeding with Prime Network unit installation. All procedures should be performed as the root user.

Table 3-3 Unit Preinstallation Tasks Checklists

	Task	Refer to:
Step 1	Verify that the Disk 1: New Install DVD is available.	Installation DVDs, page 1-2
Step 2	Verify that the unit machines meet the system hardware and software requirements.	Prime Network Unit Requirements, page 2-10
Step 3	Verify that the time on all units in the setup is synchronized. Note The maximum difference allowed between different clocks is 4 minutes.	—
Step 4	Verify that all the ports designated for Prime Network are free.	Required Ports for Prime Network, page 2-25

Verifying the Installed Operating System

Prime Network 5.0 is supported on Red Hat 6.5, Red Hat 6.7, Red Hat 6.8, and Red Hat 7.2 64-bit Server Edition (English language).

To verify that you have installed a supported Linux version, as the root user, enter:

```
# cat /etc/redhat-release
```

The command output should list a supported version, as in this example:

```
Red Hat Enterprise Linux Server release 6.5
```

Verifying the RPMs Required on Red Hat for Prime Network

As root user, verify all required RPMs are installed. For a list of required RPMs, see [Required Red Hat Services and RPMs, page 2-16](#).

To verify which required RPMs are installed, use the `rpm -q` command followed by the required RPMs, as in the following example (which is for Red Hat 6.5):

```
rpm -q binutils-2.20.51.0.2-5.36.el6.x86_64 compat-libcap1-1.10-1.x86_64
compat-libstdc++-33-3.2.3-69.el6.x86_64 gcc-4.4.7-4.el6.x86_64 gcc-c++-4.4.7-4.el6.x86_64
glibc-2.12-1.132.el6.x86_64 glibc-2.12-1.132.el6.x86_64 ksh-20120801-10.el6.x86_64
libgcc-4.4.7-4.el6.x86_64 libstdc++-4.4.7-4.el6.x86_64 libstdc++-devel-4.4.7-4.el6.x86_64
libaio-0.3.107-10.el6.x86_64 libaio-devel-0.3.107-10.el6.x86_64 make-3.81-20.el6.x86_64
sysstat-9.0.4-22.el6.x86_64 expect-5.44.1.15-5.el6_4.x86_64
openssh-clients-5.3p1-94.el6.x86_64 openssh-server-5.3p1-94.el6.x86_64
openssh-5.3p1-94.el6.x86_64 telnet-0.17-47.el6_3.1.x86_64 openssl-1.0.1e-16.el6.x86_64
compat-libstdc++-33.x86_64 dos2unix-3.1-37.el6.x86_64 --qf '%{name} %{arch} \n' | sort
```

The output of this command will list the RPMs and will indicate which RPMs are not installed.

Example output:

```
binutils-2.20.51.0.2-5.36.el6.x86_64
package compat-libcap1-1.10-1.x86_64 is not installed
compat-libstdc++-33-3.2.3-69.el6.x86_64
package gcc-4.4.7-4.el6.x86_64 is not installed
gcc-c++-4.4.7-4.el6.x86_64
glibc-2.12-1.132.el6.x86_64
ksh-20120801-10.el6.x86_64
libgcc-4.4.7-4.el6.x86_64
libstdc++-4.4.7-4.el6.x86_64
libstdc++-devel-4.4.7-4.el6.x86_64
libaio-0.3.107-10.el6.x86_64
libaio-devel-0.3.107-10.el6.x86_64
make-3.81-20.el6.x86_64
sysstat-9.0.4-22.el6.x86_64
expect-5.44.1.15-5.el6_4.x86_64
openssh-clients-5.3p1-94.el6.x86_64
openssh-server-5.3p1-94.el6.x86_64
openssh-5.3p1-94.el6.x86_64
telnet-0.17-47.el6_3.1.x86_64
openssl-1.0.1e-16.el6.x86_64
compat-libstdc++-33.x86_64
dos2unix-3.1-37.el6.x86_64
```


Starting the Oracle Listener (External Database)

After the external database has been created, start the Oracle listener so that the **network-conf.pl** configuration script can connect to the database.

Step 1 As the root user, to determine if the Oracle listener is up, enter:

```
ps -ef | grep ora
```

The following output should be displayed (in this example, *ORACLEHOME* is set to */export/home/oracle*):

```
oracle 17327      1    0   Aug 02 ?        0:00 /export/home/oracle/product/11.2.3/bin/tnslsnr
LISTENER -inherit
```

Step 2 If the Oracle listener is down, complete the following steps:

- a. Log in as user oracle.
- b. Enter **lsnrctl start**.

Configuring the Network Timing Protocol

It is recommended to use your organization's NTP server for timing synchronization, however, if necessary, you could use the Prime Network gateway.

**Note**

If gateway high availability is configured, you must use your organization's NTP server for timing.

To use your organization's NTP server for timing synchronization:

Step 1 Locate the **ntp.conf** file, which is usually located under */etc/ntp.conf*. (Check the file location with the NTP system administrator.)

Step 2 Enter the following in *ntp.conf*, where *NTP_SERVER_IP* is the IP address of your organization's NTP server.

- For IPv4, enter:

```
###
server NTP_SERVER_IP prefer
###
```

- For IPv6, enter:

```
###
server -6 NTP_SERVER_IP prefer
###
```

Step 3 Restart the NTP service:

```
service ntpd restart
```

To use the Prime Network gateway for timing synchronization:

Step 1 On the Prime Network gateway, create a file with the following contents and save it as `/etc/ntp.conf`:

```
###
server 127.127.1.0 prefer
fudge 127.127.1.0 stratum 10
restrict default noquery
driftfile /var/lib/ntp/ntp.drift
statsdir /var/lib/ntp/ntpstats/
filegen peerstats file peerstats type day enable
filegen loopstats file loopstats type day enable
filegen clockstats file clockstats type day enable
###
```

Step 2 Create a drift file:

```
touch /var/lib/ntp/ntp.drift
```

Step 3 Restart the NTP service:

```
service ntpd restart
```

Step 4 Configure the units and database to be NTP clients by creating a file with the following contents, and save it as `/etc/ntp.conf`:

a. Create an `/etc/ntp.conf` with the following contents:

For IPv4, enter:

```
###
server GW_SERVER_IP prefer
###
```

For IPv6, enter:

```
###
server -6 GW_SERVER_IP prefer
###
```

b. Restart the NTP service:

```
service ntpd restart
```

c. Verify connectivity to the NTP server, enter:

```
ntpq -p
```



Note

If you find two NTP processes running on the server, kill one of them.

Finding NTP Process in Server

To find an NPT process running in the server, follow the command provided below:

```
[root@ast-nms-cpn ~]# ps -ef | grep -v grep | grep "ntp"
ntp 2040 1 0 Jan23 ?    00:00:01 ntpd -u ntp:ntp -p /var/run/ntpd.pid -g
root 2051 2040 0 Jan23 ?    00:00:01 ntpd -u ntp:ntp -p /var/run/ntpd.pid -g
```

Killing NTP Process in Server

To kill an NTP process running in the server, follow the command provided below:

```
[root@ast-nms-cpn ~]# kill -9 2051
[root@ast-nms-cpn ~]# ps -ef | grep -v grep | grep "ntp"
ntp    2040  1 0 Jan23 ?    00:00:01 ntpd -u ntp:ntp -p /var/run/ntpd.pid -g [
root@ast-nms-cpn ~]#
[root@ast-nms-cpn ~]# ps -ef | grep -v grep | grep "ntp" | wc -l
1
```

IPv4 and IPv6 Compliance Considerations

Prime Network 5.0 supports monitoring and communication over IPv4 and IPv6 interfaces. Units can hold and manage VNEs from different interface types. Prime Network IPv4 and IPv6 installation options are shown in [Table 3-4](#). Variations in the options are possible, for example, a gateway with a dual-stack interface can connect to one unit with an IPv4 interface and another with an IPv6 interface.



Note

If Gateway is installed with IPv6 interface then OR is not supported.

Table 3-4 Supported IPv4 and IPv6 Installations

Interface	IPv4	IPv6	IPv4 + IPv6
Gateway	Yes	Yes	Yes
Client	Yes	Yes	Yes
Unit	Yes	Yes	Yes
Cisco Embedded Oracle	Yes	No	Yes Note For Dual Stack environments IPv6 is supported. However, it is recommended to select IPv4 as the DB interface during network-conf execution and select IPv6 as the backend interface.
User-purchased Oracle	Yes	No	Yes
Operations Reports	Yes	No	Yes
Note Operations Reports are only available to customers with Operations Reports license prior to May 2018. For re-installation of Operations Reports contact a Cisco customer support representative.			

While Prime Network 5.0 allows for flexible IPv4 and IPv6 installations, do not install Prime Network in an IPv4 and IPv6 network until you review the following points:

- Units configured in a redundant relationship must have the same interface type, that is, either IPv4 or IPv6.
- Installation sets the interface type between a unit and a gateway. Upgrading to Prime Network 5.0 does *not* automatically add a new interface type between an existing unit and its gateway, even if the IPv6 connectivity already exists. Contact Cisco Technical Support for assistance.
- The client must have the same connectivity type to the database machine as the Prime Network gateway. For example, if the gateway is configured to access the database using IPv4, the client must also be able to access the database using IPv4.
- Only Oracle version 12cR2 and later are IPv6-compliant. If you plan to install a gateway or unit with only IPv6 interface types, verify that the Oracle database is version 12cR2 or later. (The Prime Network embedded Oracle database is version 12c[12.1.0.2].)
- You can install the Prime Network 5.0 embedded database on an IPv4-only server or on a dual stack server (IPv4 and IPv6). You cannot install the embedded database on an IPv6-only server.
- You can install Prime Network 5.0 Operations Reports on an IPv4-only server or on a dual stack server (IPv4 and IPv6). You cannot install the tool on an IPv6-only server.



Note The distribution of Operations Reports is no longer available. Operations Reports are only available to customers with Operations Reports license prior to May 2018. For re-installation of Operations Reports contact a Cisco customer support representative.

- When using Change and Configuration management, make sure your device can communicate both over IPv4 and IPv6. If your device cannot communicate over IPv4, then the Unit from which the VNE of that device is configured can only manage devices over IPv6. This is valid only in case the device does not have dual stack.
- If the units are installed with interface type that differs from the interface on which the database is installed, then database must be configured for dual listener. To configure dual listener, complete the procedure in [Configuring Dual Listeners, page 7-3](#) after the installation.

UNIX Services and Components Used by Prime Network

[Table 3-5](#) lists the Linux services and components that are used by the Prime Network system. Do not remove them.

Table 3-5 Required Linux Services and Components

Name	Function	Configuration Information	TCP or UDP Port No.	Traffic Classification
xntpd	Time server	/etc/inet/ntp.conf	123 (UDP)	ntp
ntp4	Time server	/etc/inet/ntp.conf	123 (UDP)	ntp
ntpd ¹	Time server	/etc/inet/ntp.conf	123 (UDP)	ntp
/bin/tcsh	UNIX shell	None	None	None
/usr/bin/tcsh	UNIX shell	None	None	None
Perl	Scripting language	None	None	None
/bin/sh	UNIX shell	None	None	None

Table 3-5 Required Linux Services and Components (continued)

/bin/ksh	UNIX shell	None	None	None
/usr/bin/ksh	UNIX shell	None	None	None
ntpd	Time server	/etc/inet/ntp.conf	123 (UDP)	ntp

1. IPv6 support, installed package



Preparing the Oracle External Database

This chapter describes how to configure an external Oracle database for use with Prime Network. Make sure you have the most recent version of the Oracle software documentation (see the [Oracle Corporation website](#)).

Using an External Database: General Guidelines

- Installation and sizing:
 - The external Oracle server can be installed on the Prime Network gateway or on any other remote workstation.
 - Preallocate the database storage by creating all required data files to their full sizes in advance. With the exception of *pnuser* and *pnuser_admin*, Prime Network tablespace data files are generated in 1 GB sizes with autoextend set to 256 MB and no size limit. (The data file can grow to 32 GB.)
 - If the Oracle server is installed on the Prime Network gateway, no Oracle services can be installed on port 2100. If an Oracle listener is installed on port 2100, you must disable it or change the port number (see [Table 4-2](#)). By default, this port is used by the Oracle XML DB service.
 - The mount directory should be available in both the active and standby nodes. If the mount folder directory does not exist in the standby node, then the installation fails.
 - For deployment information and recommendations, contact your Cisco account representative.
- Starting and stopping processes:
 - Prime Network does not manage the starting and stopping of Oracle processes for an external database. The database administrator is responsible for automatically restarting Oracle processes in the event of a power failure.
 - If your system is configured for gateway high availability, start and stop Prime Network and Oracle using CLI commands. Stopping the applications using the regular application commands (without the awareness of the cluster software) can cause a failover.
 - If you restart Oracle, you must also restart AVM 25 on both the gateway and units.
- Usernames:
 - The Oracle user should be called **oracle**, and it should be part of a group called **dba**.
 - The database username and password that are related to the Prime Network application are created automatically during installation.

- Clocks: In Prime Network, the clocks on the gateway and units must be synchronized. If Oracle is running on a separate workstation, that remote database workstation's clock must be synchronized with the gateway and unit clocks.

Creating an External Oracle Database

The database instance installation can be performed as part of the Oracle installation or separately using the Oracle database configuration assistant (DBCA) utility. This section describes how to create an Oracle database instance using the DBCA utility (in *ORACLEHOME/bin*).

Download the Oracle patches from <http://metalink.oracle.com>.



Note

After installing an Oracle patch, you must change the permissions for the newly installed files to enable all OS users to use Oracle on the workstation. You can do this by running the script *ORACLEHOME\install\changePerm.sh*.

The Prime Network database size is determined by the usage patterns and the expected load in your deployment. Contact your Cisco account representative for assistance in determining your database load profile and calculating your database memory and storage size requirements.

Prime Network provides sizing estimates for the following usage profiles, which vary according to the maximum expected rate of actionable events per second that your deployment can support:

- Up to 250—Represents a high-scale production environment with a maximum supported rate of database operations, including up to 250 actionable events per second, a maximum amount of services, and the highest rate of configuration archive and provisioning operations.
- Up to 200—Represents a high-scale production environment with a maximum supported rate of database operations, including up to 200 actionable events per second, a maximum amount of services, and the highest rate of configuration archive and provisioning operations.
- Up to 100—Represents a high-scale production environment with a maximum supported rate of database operations, including up to 100 actionable events per second, a maximum amount of services, and the highest rate of configuration archive and provisioning operations.
- Up to 50—Represents a medium- to high-scale production environment with a medium rate of database operations, including up to 50 actionable events per second, a medium amount of services, and a medium rate of configuration archive and provisioning operations.
- Up to 20—Represents a medium- to small-scale production environment with a low rate of database operations, including up to 20 actionable events per second, a small amount of services, and a low rate of configuration archive and provisioning operations.
- Up to 5—Represents a small environment with a low rate of database operations, including up to 5 actionable events per second, a small amount of services, and a low rate of configuration archive and provisioning operations.
- Up to 1—Represents a very small test or proof-of-concept environment with a single machine acting as a gateway, unit, and database (or with a separate unit), with no more than 50 VNEs and a low rate of events.

When installing a database instance, use the values in [Table 4-1](#) for the Oracle initialization parameters. The values are in bytes.

Table 4-1 Database Initialization Parameters

Profile Name	Up to 5 Actionable Events per Second	Up to 20 Actionable Events per Second	Up to 50 Actionable Events per Second	Up to 100 Actionable Events per Second	Up to 200-250 Actionable Events per Second
sga_max_size	4412407808	6509559808	6509559808	10301210624	10301210624
shared_pool_size	1258291200	2147483648	2147483648	2147483648	2147483648
large_pool_size	134217728	134217728	134217728	134217728	134217728
java_pool_size	218103808	335544320	335544320	335544320	335544320
pga_aggregate_target	1048576000	1887436800	1887436800	1887436800	1887436800
sga_target	0	0	0	0	0
memory_target	0	0	0	0	0
memory_max_target	0	0	0	0	0
db_cache_size	1048576000	2684354560	2684354560	2684354560	2684354560
db_keep_cache_size	318767104	872415232	872415232	3690987520	3690987520
db_recycle_cache_size	167772160	167772160	167772160	838860800	838860800
db_file_multiblock_read_count	16	16	16	16	16
open_cursors	2000	2000	2000	2000	2000
optimizer_index_cost_adj	10	10	10	10	10
optimizer_index_caching	50	50	50	50	50

For better performance, make sure you generate statistics for all tables in the database. Prime Network issues alerts if no statistics are generated, or if the current statistics are more than 2 weeks old.



Note

The *pnuser_admin* user is a user with database administrator permissions who can run maintenance tasks—such as gathering statistics—on the other Prime Network database schemas. After the *pnuser_admin* user is created, a cron job runs every 24 hours to gather statistics on the *pnuser* (Fault Database). You no longer have to gather statistics manually.

If you expect a high scale in the first 24 hours, it might be necessary to manually force statistics gathering twice during the first day, 1 and 5 hours after noise start. To force statistics gathering, enter the following command as *pnuser*:

```
cd $NETWORKHOME/Main/scripts; ./call_update_ana_stats.pl >& /dev/null
```

[Table 4-2](#) describes the steps involved in creating an Oracle 12c database using DBCA.

If you are using an Oracle 12c database, please refer to the Cisco Prime Network 5.0 Installation Guide.

Table 4-2 Creating an Oracle database Using DBCA

	Procedure	Recommended Action
Step 1	In the Operations window, select the operation that you want to perform.	Choose Create a Database .
Step 2	Select a creation mode in the Creation Mode window.	Choose Advanced Mode .
Step 3	In the Database Template window, select the template.	Choose Custom Database .
Step 4	In the Database Identification window, enter the Global Database Name and SID field.	Enter mcdb . Do not check the Create As Container Database check box, and do not fill in any of the related data. Note Do not modify the default Service, instead, you can add additional Service (s) along with the default service.
Step 5	In the Management Options window, configure the fields in Enterprise Manager as required.	Do not set any of the fields in Enterprise Manager and Automatic Maintenance task, and proceed to the next step.
Step 6	Enter the passwords for the Oracle administrative accounts	Enter passwords for SYS and SYSTEM users.
Step 7	In the Listener Selection window, check the relevant listener check box.	Enter the name and port.
Step 8	In Database File Locations window, specify the storage type and location for the database. Set recovery settings if you intend to configure a database backup policy.	<ol style="list-style-type: none"> 1. Select Storage Type as File System. 2. For Storage Location, browse for the common location for all database files (Example: /export/home/oracle/oradata/mcdb). 3. In Recovery Related Files, choose File System as the Storage Type. 4. Check the Enable Archiving check box. 5. Click Edit Archive Mode Parameters to set the location for archive logs.
Step 9	In the Database Options window, use the default options.	Make sure that the Oracle Label Security and Oracle Database Vault check boxes are not checked. The rest of the check boxes should be checked.

Table 4-2 Creating an Oracle database Using DBCA (continued)

	Procedure	Recommended Action
Step 10	In the Initialization Parameters window, configure the memory settings for the database.	<ol style="list-style-type: none"> 1. Select Custom. 2. For the Memory Management field, select the Manual Shared Memory Management from the drop down. 3. Configure other initialization parameters. Refer to Table 4-1 for the values of various database initialization parameters based on profiles. 4. In the Sizing tab, change processes to 1000. 5. In the Character Sets tab, choose your preferred character set (AL32UTF8 is recommended). 6. In the Connection Mode tab, choose Dedicated Server Mode.
Step 11	In the Creation Options window, select the database creation options.	<p>Choose Create Database and click Customize Storage Locations to configure redo log settings.</p> <p>Contact your Cisco account representative for assistance in estimating the database size.</p> <p>To support high event rates, redo log files must be six online 2 GB files on raw devices or on a dedicated disk partition mounted with the directio option. The redo log files must reside on a physical disk separate from the Oracle data files.</p>

Configuring the External Database

This section includes details on configuring the database, such as the Oracle initialization parameters, ports, database size, and so forth.

Configuring the cursor_sharing System Parameter

The cursor_sharing system parameter must be set to FORCE. To configure the cursor_sharing system parameter:

Step 1 As the SYS user, enter the following command:

```
ALTER SYSTEM SET cursor_sharing='FORCE' SCOPE=BOTH;
```

Step 2 Enter the following SQL*PLUS command to verify that the parameter is set correctly:

```
SQL> show parameter cursor_sharing
```

In the command output, you should see:

```
NAME                TYPE        VALUE
-----                -
cursor_sharing      string      FORCE
```

Retaining Partitioning Storage Behavior

To ensure that partitioning storage behavior is retained, ensure that the partitions are created with an extent size of 64 KB. To create partitions with extent size of 64 KB, set the hidden parameter (`_partition_large_extents`) to false.

Enter the following command as the SYS user:

```
ALTER SYSTEM SET "_partition_large_extents" =FALSE SCOPE=BOTH;
```



Note

The partitioning storage behavior is not retained if the partitions are created with the default extent size (8 MB).

Configuring the `job_queue_processes` System Parameter

The `job_queue_processes` parameter specifies the maximum number of processes that can be created for the execution of jobs. It must be set to 1000. To configure the `job_queue_processes` parameter:

Step 1 As the SYS user, enter the following command:

```
alter system set job_queue_processes=1000 scope=both;
```

Step 2 Enter the following SQL*PLUS command to verify that the parameter is set correctly:

```
SQL> show parameter job_queue_processes
```

In the command output, you should see:

NAME	TYPE	VALUE
-----	-----	-----
job_queue_processes	integer	1000

Configuring the `audit_trail` System Parameter

Disable Oracle auditing by setting the `audit_trail` system parameter to NONE. To configure the `audit_trail` system parameter:

Step 1 As the SYS user, enter the following command:

```
ALTER SYSTEM SET audit_trail=NONE SCOPE=spfile;
```

Step 2 As the SYS user, enter the following command to start the database:

```
Startup
```

Step 3 As the SYS user, enter the following SQL*PLUS command to verify that the parameter is set correctly:

```
SQL> show parameter audit_trail
```

In the command output, you should see:

NAME	TYPE	VALUE
-----	-----	-----
audit_trail	string	NONE

Disabling the Recycle Bin Option

If enabled, the Oracle recycle bin feature retains a version of each dropped object, which can lead to an accumulation of junk information in the Prime Network DB Segments table. To disable the recycle bin option:

Step 1 As the SYS user, enter the following command:

```
ALTER SYSTEM SET recyclebin = OFF DEFERRED scope=both;
```

Step 2 Enter the following SQL*PLUS command to verify that the parameter has been disabled:

```
SQL> show parameter recyclebin
```

In the command output, you should see:

NAME	TYPE	VALUE
-----	-----	-----
recyclebin	string	OFF DEFERRED

Step 3 (Optional) As *pnuser*, enter the following command to see the objects that are currently saved in the recycle bin:

```
show recyclebin
```

Step 4 (Optional) As *pnuser*, enter the following command to empty the recycle bin:

```
purge recyclebin;
```

Setting the open_cursors Parameter

Open cursors enable the reading and writing of data between the Oracle database and Cisco Prime Network. The `open_cursors` parameter defines the maximum number of cursors that can be opened concurrently, per session. The recommended maximum number of open cursors for use with Cisco Prime Network is 2000. An error is generated if the number of open cursors in a session exceeds the specified number.

To set the `open_cursors` parameter:

Step 1 To check the value of the `open_cursors` parameter, enter:

```
SQL> show parameter open_cursors
```

In the command output, you should see:

```
open_cursors integer 2000
```

Step 2 If the integer value is less than 2000, enter:

```
SQL> ALTER SYSTEM SET open_cursors = 2000 SCOPE=BOTH;
```

Step 3 To verify that the value has changed, enter:

```
SQL> show parameter open_cursors
```

**Note**

If the `open_cursors` integer value is still less than 2000, contact your local database administrator.

Disabling Automatic Maintenance Jobs

If you deploy Prime Network to handle a high event rate, it is recommended that you disable Oracle's automatic maintenance jobs. Automatic maintenance significantly affects Oracle performance and increases event processing time.

**Caution**

These commands disable *all* scheduler maintenance activities. Complete the following procedure after implementing an alternative method of gathering database statistics. Some of the commands will fail in some versions of Oracle; you can ignore any failures.

Connect to the Oracle database as the SYS user and enter the following commands:

```
execute DBMS_SCHEDULER.disable (name => 'GATHER_STATS_PROG',force => TRUE);
execute DBMS_SCHEDULER.disable (name => 'AUTO_SPACE_ADVISOR_PROG',force => TRUE);
execute dbms_scheduler.disable(name =>'GATHER_STATS_JOB',force => TRUE);
execute dbms_scheduler.disable(name =>'BSLN_MAINTAIN_STATS_JOB',force => TRUE);
execute DBMS_SCHEDULER.disable(name => 'SYS.MAINTENANCE_WINDOW_GROUP', force => TRUE);
execute DBMS_SCHEDULER.disable(name => 'SYS.ORA$AT_WGRP_SA', force => TRUE);
execute DBMS_SCHEDULER.disable(name => 'SYS.ORA$AT_WGRP_SQ', force => TRUE);
execute DBMS_SCHEDULER.disable(name => 'SYS.ORA$AT_WGRP_OS', force => TRUE);
EXECUTE DBMS_SCHEDULER.disable (name =>'SYS.MONDAY_WINDOW', force => TRUE);
EXECUTE DBMS_SCHEDULER.disable (name =>'SYS.TUESDAY_WINDOW', force => TRUE);
EXECUTE DBMS_SCHEDULER.disable (name =>'SYS.WEDNESDAY_WINDOW', force => TRUE);
EXECUTE DBMS_SCHEDULER.disable (name =>'SYS.THURSDAY_WINDOW', force => TRUE);
EXECUTE DBMS_SCHEDULER.disable (name =>'SYS.FRIDAY_WINDOW', force => TRUE);
EXECUTE DBMS_SCHEDULER.disable (name =>'SYS.SATURDAY_WINDOW', force => TRUE);
EXECUTE DBMS_SCHEDULER.disable (name =>'SYS.SUNDAY_WINDOW', force => TRUE);
EXECUTE DBMS_SCHEDULER.disable (name =>'SYS.WEEKNIGHT_WINDOW', force => TRUE);
EXECUTE DBMS_SCHEDULER.disable (name =>'SYS.WEEKEND_WINDOW', force => TRUE);
```

Changing Database Ports

If Oracle is installed on the Prime Network gateway, the Oracle services will be installed on port 2100. If an Oracle listener was installed on port 2100, you must disable it or change the port number. By default, this port is used by the Oracle XML DB service.

**Note**

You must change the FTP port number if an Oracle listener was installed by default on port 2100.

Use this procedure to change the port numbers of the XML DB listeners, if required. This procedure applies only if you installed the Oracle XML DB service. If you disabled the Oracle XML DB service, skip this section.

Step 1 To log into Oracle SQL, enter:

```
sqlplus user/password
```

Step 2 To change the HTTP port from 8080 to 8083, enter:

```
sql> call dbms_xdb.cfg_update(updateXML(dbms_xdb.cfg_get(),
'/xdbconfig/sysconfig/protocolconfig/httpconfig/http-port/text()', 8083));
```

Step 3 To change the FTP port from 2100 to 2111, enter:

```
sql> call dbms_xdb.cfg_update(updateXML(dbms_xdb.cfg_get(),
'/xdbconfig/sysconfig/protocolconfig/ftpconfig/ftp-port/text()' , 2111));
```

Step 4 To commit the update, enter:

```
sql> COMMIT;
```

Step 5 To refresh the settings, enter:

```
sql> exec dbms_xdb.cfg_refresh
```

Step 6 To exit SQL Command Line, enter:

```
sql> exit
```

Configuring the Database Size and Disk Structure

The size of the stored data is determined mainly by the number of stored events. By default, Prime Network is configured to archive events for up to 14 days. The archive size, the supported event rates, and the average event size dictate the expected database growth on a daily basis. Events that are archived for a long time cause a significant load on the database and require additional disk space. You can change the default archive period using the Administration GUI, if necessary (see the [Cisco Prime Network 5.0 Administrator Guide](#)). Contact your Cisco account representative for assistance with sizing calculations.

Recommended Disk Structure

Following is the recommended disk structure for an Oracle server based on the number of disks that the server holds:

- Oracle data files—The optimal location is an external disk array (preferably RAID 10).
- Online redo log files—The optimal location is an internal disk partition. The redo log files should not reside on the same disk as the data files.
- Archive files—Should not reside on the same disk as the data files.
- Backup files—Should not reside on the same disk as the data files.

Configuring Oracle to Start Automatically When Prime Network Restarts

By default, the Oracle application does not start automatically when Prime Network is rebooted. This is because the best practice is for the system database administrator to manually start the database in a controlled environment. However, if you want Oracle to start when the system is rebooted, there are multiple ways to accomplish this task. The following is one example; see the [Oracle documentation](#) for other implementations.

As the Oracle UNIX root user, create a file in the /etc/rc2.d directory named S99OracleDB, with the following contents:

```
ORA_OWNER=oracle
DBLOG=$INSTALL_DIR/log/dbop.log
TZ=GMT
if [ -f /var/opt/oracle/oratab ]; then
    orahome=`grep -v "^#" /var/opt/oracle/oratab | grep . | sed -ne 'lp' | awk -F: '{print $2}'`
else
    echo "/var/opt/oracle/oratab file doesn't exist. Please check if Oracle is installed "
>> $DBLOG
    echo "dbora $1 aborted..." >> $DBLOG
    exit
fi
ORA_HOME=$orahome
TNS_ADMIN=$ORA_HOME/network/admin
if [ ! -f $ORA_HOME/bin/dbstart -o ! -d $ORA_HOME ]
then
echo "Oracle startup cannot start"
exit
fi

if [ ! -d $INSTALL_DIR/log ]; then
    mkdir $INSTALL_DIR/log
    chmod 777 $INSTALL_DIR/log
fi
if [ ! -f $DBLOG ]; then
    touch $DBLOG
fi

#start the Oracle databases
echo "Invoking dbstart at `date` " >> $DBLOG
echo >> $DBLOG
su - $ORA_OWNER -c $ORA_HOME/bin/dbstart
echo "Invoking Listener start at `date`" >> $DBLOG
echo >> $DBLOG
su - $ORA_OWNER -c "lsnrctl start"
echo "Listener started." >> $DBLOG
echo >> $DBLOG
```

Preventing Passwords in the Default Profile from Expiring

When you create a database, passwords of users that belong to the default profile expire after 180 days. Because Prime Network database users receive the default profile, their database password will expire after 180 days. To prevent this from occurring, complete the following steps:

Step 1 Log into the Oracle SQL as the sysdba.

Step 2 Enter:

```
alter profile default limit PASSWORD_LIFE_TIME unlimited;
```

Maintaining the External Database

After installation, maintaining the database can involve:

- [Maintaining Archive Log File Disk Space](#)—Ensure that there is sufficient space on a disk to store a large volume of archive logs caused by the large number of Cisco Prime Network updates to the database.
- [Adding Data Files to the Tablespace](#)—Add data files to enable the storage of event history logs for a longer period of time.



Note

Refer to your Oracle documentation for instructions on how to back up the Oracle database.

Maintaining Archive Log File Disk Space

The large number of Prime Network updates to the database causes the size of the archive log to expand rapidly and consume a large amount of space on the disk partition. To maintain space on the disk partition, an Oracle database administrator should delete the archive log files periodically.

Adding Data Files to the Tablespace

After you install Prime Network and its database, you might need to add more data files, depending on the event rate per second. Here is an example showing how to add a data file to the existing tablespace:

```
alter tablespace tablespace-name add datafile 'new-data-file-full-path' size 32G
autoextend off;
```

where *tablespace-name* is *pnuser_TABLESPACE*, *dwe_TABLESPACE*.

The size can be changed and is subject to actual needs and availability.



Note

With the exception of *pnuser* and *pnuser_admin*, Prime Network tablespace data files are generated in 1 GB sizes with autoextend set to 256 MB and no size limit. (The data file can grow to 32 GB.) It is recommended that you preallocate the database storage by creating all required data files to their full sizes in advance.



Installing the Prime Network Gateway and Units Using the Installation Wizard

This chapter describes how to install the gateway and units using the GUI installation wizard, which is an alternative (and preferred) installation method to the CLI installation.

The following topics are covered in this section:

- [Prerequisites for Using the Installation Wizard, page 5-1](#)
- [Launching the Installation Wizard, page 5-2](#)
- [Installing the Gateway with Embedded Database Using the Installation Wizard, page 5-3](#)
- [Installing the Gateway with External Database Using the Installation Wizard, page 5-7](#)
- [Installing a Unit Using the Installation Wizard, page 5-11](#)

The installation wizard does not include installation of Operations Reports and the Prime Network Integration Layer.

Prerequisites for Using the Installation Wizard

Before you begin, verify that the following prerequisites are met:

- An X client application, such as Xming, is installed on the local machine on which you plan to launch the wizard.
- A Telnet/SSH client, such as PuTTY, is installed on the local machine on which you plan to launch the wizard, and X11 forwarding is enabled.
- All preinstallation tasks for the gateway and unit are completed. See [Preparing for the Installation](#).
- The database files (`linuxamd64_12c_database_1of2.zip` and `linuxamd64_12c_database_2of2.zip`) are available in the Cisco Prime Network 5.0 disk 4. The files required for upgrading to Prime Network 4.0 are available in Prime Network 4.0 DVD.
- Use only Oracle 12.1.0.2. This is because all Prime Network 5.0 fresh installation will support only Oracle 12.1.0.2.

Launching the Installation Wizard

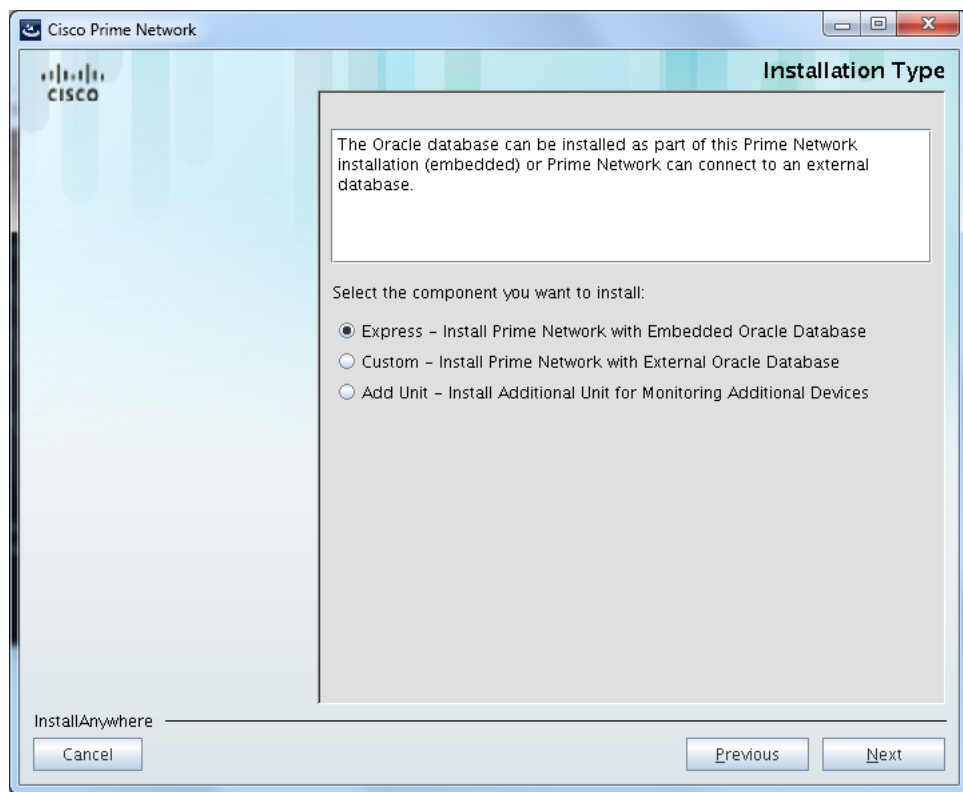
To launch the installation wizard:

-
- Step 1** Launch the X client application (for example, Xming).
 - Step 2** As the root user, launch a terminal on the server where you want to install the Prime Network gateway.
 - Step 3** Insert **Disk 1: New Install** in the DVD drive. (See [Installation DVDs, page 1-2](#)).
 - Step 4** Mount the inserted DVD using the **mount** command, and move to the mount directory.
 - Step 5** In the mount directory, locate the install.bin file and run it:

```
./install.bin
```

This launches the installation wizard.

- Step 6** Read the introduction and click **Next**. In the Installation Type window, you can choose the relevant installation:
 - Prime Network gateway with an embedded database. See [Installing the Gateway with Embedded Database Using the Installation Wizard, page 5-3](#).
 - Prime Network gateway with an external database. See [Installing the Gateway with External Database Using the Installation Wizard, page 5-7](#).
 - Unit. See [Installing a Unit Using the Installation Wizard, page 5-11](#)



Installing the Gateway with Embedded Database Using the Installation Wizard

The following procedure describes how to install a Prime Network gateway and an embedded database using the GUI installation wizard.

- Step 1** Launch the installation wizard using the install.bin file on Disk 1: New Install. See [Launching the Installation Wizard, page 5-2](#).
- Step 2** Read the introduction and click **Next**.
- Step 3** In the Installation Type window, select **Express - Install Prime Network with Embedded Oracle Database** and click **Next**.
- Step 4** In the next four windows, provide the required user and installation folder information, as follows:

Field	Enter:	Notes
Operating System User Name Window		
New Operating System user	A username for the Prime Network operating system. This username will be used when connecting to the gateway using SSH and for other administrative purposes.	This username is used as the basis for the installation directory and the database schema names. We recommend you use pn50 . In the documentation, we use <i>pnuser</i> to represent the operating system user variable.
Password	A password for the Prime Network operating system user.	—
Prime Network User Window		
Password	A password for the Prime Network root user.	The root username and password are used to log into the Prime Network GUI applications. Enter a password that complies with the password requirements listed in the text box at the top of the screen.
Operating System "root" Password Window		
Password	A password for the operating system root user.	—
Installation Folder Window		
Please choose a folder	Select an installation folder or use the default folder.	The default installation directory is /export/home/OS-User. We recommend you use the default directory. In the documentation, we use <i>\$NETWORKHOME</i> to represent the installation directory.

- Step 5** Click **Next**.
- Step 6** Check the Prerequisites Summary window for items that are not marked [OK] and rectify them as needed (for example, add more disk space). Click **Next**.

Step 7 In the Gateway Installation Embedded Oracle Database window, enter the gateway IP address to be used for communication with the units, if it is different from the IP address that was automatically identified by the system.

Step 8 Select **Suite-Integrated** (if you are using Prime Network with Prime Central), or **Standalone**.



Note For suite-integrated systems, Prime Network Integration Layer must be installed. See [Chapter 9, “Installing the Prime Network Integration Layer”](#).

Step 9 Provide the following information in the Embedded Database windows.

Embedded Database Field	Enter:	Notes
Embedded Database Window (1)		
Database username	Username for the Oracle database user, if you do not want to use the default username.	Default is oracle .
Database Server IP Address	IP address of the database server (IPv4 or IPv6). The database server could be the gateway or a remote server.	Default is the IP address of the gateway.
Choose a database profile	Select the database profile that represents your setup.	See Creating an External Oracle Database, page 4-2 for guidelines (the information also applies to embedded databases). Prime Network calculates memory and storage requirements based on this entry.
Would you like to enable database auto-backup?	[yes no]	If you enter No , you can enable automatic backups later using the emdbctl command. See the Cisco Prime Network 5.0 Administrator Guide .
Embedded Database Window (2)		
Database Zip Files Path	Path to the directory in which the database zip files are located.	Default is / . These files must be copied from Disk 4 of the Prime Network 5.0 installation DVDs.
Database Home Directory	Path to the database home directory.	Default is /export/home/oracle . Must have a minimum of 6 GB of disk space for oracle binaries. Should not reside under the installation directory (\$NETWORKHOME).
Database Data Files Path	Path to the directory containing the datafiles (<i>oracle-datafiles-dir</i>)	Default is /export/home/oracle/oradata/anadb .
Redo Logs File Path	Path to the directory containing the redo files.	Should not reside on the same disk as <i>oracle-datafiles-dir</i> . Use ext3 partition mounted with the default mount options.

Embedded Database Field	Enter:	Notes
Archive Logs Files Path	Path to the directory containing the archive log files.	Should not reside on the same disk as <i>oracle-datafiles-dir</i> .
Backup Data Files Path	Path to the directory containing the backup data files.	Should not reside on the same disk as <i>oracle-datafiles-dir</i> .

Step 10 If you selected Suite-Integrated, you will be required to enter information enabling communication with Prime Central, including the Prime Central database server IP address, database port, database SID, database username and password. Click **Next**.

Step 11 In the Operations Reports Database (Infobright) windows, enter the information that will enable connection to the server on which the Infobright database is located and the folders for the Infobright data, then click **Next**.

Field	Enter:	Notes
Operations Reports Database (Infobright) Window		
Infobright Database Server IP Address		
Root user password for SSH connection		
Infobright database server port		
Archive history size		
Backup history size		
Would you like to enable backup files creation?		
Operations Reports Database (Infobright) Folders Window		
Path to folder for Infobright database data		
Path to folder for Infobright database cache data		
Path to folder for Infobright database backup data		
Path to folder for Infobright DLP staging area		

**Note**

Operations Reports are only available to customers with Operations Reports license prior to May 2018. For re-installation of Operations Reports contact a Cisco customer support representative.

Step 12 In the Installation Setup Summary window, review and verify the information.

Step 13 Click **Install**. The installation procedure will take between 20-50 minutes to complete.

Step 14 When the installation is complete, you will receive a message indicating this. If the installation fails, you will receive a message with details about the failure.

The following logs are available after the installation:

- Installation logs—/var/adm/cisco/prime-network/logs/.
- Embedded database configuration logs—\$NETWORKHOME/local/scripts/embedded_oracle.
- Prime Network configuration logs—\$NETWORKHOME/Main/logs.

**Note**

Before launching Prime Network in the Windows 2008 server from Prime central, ensure that the host file is updated with correct host IP address to resolve the hostname. If hostname is not configured properly, then the Prime Network installation fails.

Installing the Gateway with External Database Using the Installation Wizard

The following procedure describes how to use the GUI installation wizard to install a Prime Network gateway that is connected to an external database.

- Step 1** Launch the installation wizard using the `install.bin` file on Disk 1: New Install. See [Launching the Installation Wizard, page 5-2](#).
- Step 2** Read the introduction and click **Next**.
- Step 3** In the Installation Type window, select **Custom: Install Prime Network with External Oracle Database** and click **Next**.
- Step 4** Provide the required user and installation folder information.

Field	Enter:	Notes
Operating System Username Window		
New Operating System User	A username for the Prime Network operating system. This username will be used when connecting to the gateway using SSH and for other administrative purposes.	This username is used as the basis for the installation directory and the database schema names. We recommend you use pn50 . In the documentation, we use <i>pnuser</i> to represent the operating system user variable.
Password	A password for the Prime Network operating system user.	—
Prime Network User Window		
Password	A password for the Prime Network root user.	The root username and password are used to log into the Prime Network GUI applications. Enter a password that complies with the password requirements listed in the text box at the top of the screen.
Operating System "root" Password Window		
Password	A password for the operating system root user.	—
Installation Folder Window		
Please choose a folder	<i>pn-installation-dir</i>	The default installation directory is <code>/export/home/OS-User</code> . We recommend you use the default directory. This default home directory is referred to as <code>\$NETWORKHOME</code> .

- Step 5** Click **Next**.
- Step 6** Check the Prerequisites Summary window to see if any items do not say [OK] and rectify them as needed (for example, add more disk space). Once verified, click **Next**.

Step 7 In the Gateway Installation window, enter the gateway IP address to be used for communication with the units, if it is different from the IP address that was automatically identified by the system.

Step 8 Select **Suite-Integrated** (if you are using Prime Network with Prime Central), or **Standalone**.



Note For suite-integrated systems, Prime Network Integration Layer must be installed. See [Chapter 9, “Installing the Prime Network Integration Layer.”](#)

Step 9 Provide the following information in the External Database window.

External Database Field	Enter:	Notes
Database Server IP Address	IP address of the database server.	—
Database Port	<i>oracle-listener-port</i>	Default port is 1521.
SID	<i>oracle-SID</i>	—
Database Administrator User Name	<i>oracle-admin-user</i>	Database user who can perform administrative tasks.
Database Administrator Password	<i>oracle-admin-password</i>	—
Database Data Files Path	<i>oracle-datafiles-dir</i>	—
Does your database require an encrypted connection?	[yes no]	If you answer yes , you will be prompted for encryption method and algorithm after clicking Next .
Do you want Prime Network to create the users?	[yes no]	If you answer yes , Prime Network will create the database users with default usernames.

Step 10 If you specified that your database needs encryption, you are prompted for an encryption method and algorithm:

- Encryption Method—Accepted, Requested, or Required (default is Required).
- Encryption Algorithm—Choose from the drop-down list.

Step 11 If you specified that you did *not* want Prime Network to create the database users, the External Database User Configuration window opens.

External Database User Configuration Field	Enter	Notes
Database schema “main” Username	<i>name</i> , e.g., PN5.0	
Database schema “dwe” Username	<i>name_dwe</i>	For example, PN5.0_dwe
Database Administrator Username	<i>name_admin</i>	Name for admin database schema
Database Reports main username	<i>name_rep</i>	Name for reports database schema

External Database User Configuration Field	Enter	Notes
Database schemes passwords	<i>password</i>	Password used for all schemas except the Event Archive
Database EP schema username	<i>name_ep</i>	Name for Event Archive database schema
Database EP Reports username	<i>name_ep_rep</i>	Name for older reports database schema
Database EP Schema Password	<i>ep-password</i>	Password for Event Archive schema

Step 12 If you selected Suite-Integrated, you will be required to enter information enabling communication with Prime Central, including the Prime Central database server IP address, database port, database SID, database username and password.

Step 13 In the Operations Reports Database (Infobright) windows, enter the information that will enable connection to the server on which the Infobright database is located and the folders for the Infobright data, then click **Next**.

Field	Enter:	Notes
Operations Reports Database (Infobright) Window		
Infobright Database Server IP Address		
Root user password for SSH connection		
Infobright database server port		
Archive history size		
Backup history size		
Would you like to enable backup files creation?		
Estimate your database profile	Select the database profile that represents your setup.	See Creating an External Oracle Database, page 4-2 for guidelines.
Operations Reports Database (Infobright) Folders Window		
Path to folder for Infobright database data		
Path to folder for Infobright database cache data		
Path to folder for Infobright database backup data		
Path to folder for Infobright DLP staging area		

**Note**

Operations Reports are only available to customers with Operations Reports license prior to May 2018. For re-installation of Operations Reports contact a Cisco customer support representative.

Step 14 In the Installation Setup Summary window, review and verify the information.

Step 15 Click **Install**. The installation procedure will take between 20-50 minutes to complete. When the installation is complete, you will receive a message indicating this. If the installation fails, you will receive a message with details about the failure. The following logs are available:

- Installation logs—`/var/adm/cisco/prime-network/logs/`.
 - Configuration logs—`$NETWORKHOME/Main/logs`.
-

Installing a Unit Using the Installation Wizard

The following procedure describes how to install an additional unit using the GUI installation wizard.


Note

Ensure that the OS version of unit and gateway is same while adding the unit to the gateway.


Note

Before starting the unit installation, ensure that the gateway to which the unit will be connected is up and running.

- Step 1** Launch the installation wizard using the install.bin file on Disk 1: New Install. See [Launching the Installation Wizard, page 5-2](#).
- Step 2** Read the introduction and click **Next**.
- Step 3** In the Installation Type window, select **Add Unit** and click **Next**.
- Step 4** Provide the required user and installation folder information.

Field	Enter:	Notes
Set OS User Window		
Operating System User Name	The same operating system username as is configured for the gateway.	—
Password	<i>OS-User-password</i>	—
PN Administrator User Window		
PN Administrator User Name	<i>admin-username</i>	User name of the administrator user for access to the various Prime Network applications.
Password	<i>admin-password</i>	This is the password for the Prime Network admin user, which is used to log into the Prime Network applications.
Installation Folder Window		
Please choose a folder	The path to the installation directory.	This should be the same installation folder as was specified for the gateway.

- Step 5** Check the Prerequisites Summary window to see if any items do not say [OK] and rectify them as needed (for example, add more disk space). Once verified, click **Next**.
- Step 6** In the Unit Installation window, enter the following:

Unit Installation Field	Enter:	Notes
Gateway IP Address	The gateway IP address to be used for communication with the units.	Make sure the gateway is up and running before proceeding.
Prime Network User OS Password on Gateway	<i>OS-User-password</i>	—
Unit IP Address	<i>unit-ip-address</i>	—

Unit Installation Field	Enter:	Notes
Mode	[Active Unit Standby Unit]	Active units are started after they are added; standby units start when a failover occurs.
Unit Protection	[Enable Disable]	Enable or disable unit high availability protection.
Unit Name	<i>unit-name</i>	—
Unit Protection Group	<i>unit-protection-group</i>	The protection group to which the unit belongs.
Main Schema Database IP Address (optional)	<i>FaultDatabase-ip-address</i>	Providing this information protects against incompatible gateway and database interface types.

Step 7 In the Pre-installation Summary window, verify the information.

Step 8 Click **Install** to start the Unit installation.

Step 9 When the installation is complete, click **Done**.

The following logs are available:

- Installation logs—`/var/adm/cisco/prime-network/logs/`.
- Configuration logs—`$NETWORKHOME/Main/logs`.



Installing the Prime Network Gateway Using CLI

This chapter explains how to install the Prime Network gateway and Operations Reports using CLI commands. If you want to use the installation wizard, see [Chapter 5, “Installing the Prime Network Gateway and Units Using the Installation Wizard”](#).

The following topics are covered in this chapter:

- [Installation Overview, page 6-1](#)
- [Installing the Prime Network Gateway With an Embedded Database, page 6-2](#)
- [Installing the Prime Network Gateway With an External Database, page 6-6](#)
- [Post Installation Tasks For the Gateway, page 6-13](#)
- [Environment Variables, Aliases, and Folders Created During Installation, page 6-20](#)
- [Product Services Installed with Prime Network, page 6-21](#)
- [Troubleshooting, page 6-22](#)

Installation Overview

The Prime Network gateway can be installed using either an embedded database or an external database. For the embedded database, Prime Network 5.0 uses a fully-integrated Oracle 12c database that allows Prime Network to manage and monitor data. This Oracle database version is also supported for the external database.



Note

All Prime Network 5.0 fresh installation will support only Oracle 12.1.0.2.

The Prime Network installation script (**install.pl**) automatically performs the following:

- Checks some system prerequisites, such as required disk space
- Backs up and removes older versions of Prime Network software (if any exist)
- Creates the Prime Network user *pnuser*, which is the operating system user for the Prime Network application.
- Copies all required files from the installation DVD to the server under the Prime Network user home directory (*/export/home/pnuser* by default), also called *\$NETWORKHOME*.
- Extracts and creates the required directories. For information on folders created after installation, see [Environment Variables, Aliases, and Folders Created During Installation, page 6-20](#).
- Installs the Prime Network software

- Configures the Prime Network registry
- Sets the Prime Network environment variables and aliases (.cshrc file)

Installing the Prime Network Gateway With an Embedded Database

Before You Begin

- Verify that all preinstallation tasks have been completed. See [Gateway Preinstallation Tasks—Embedded Database, page 3-1](#).

To install the gateway with an embedded database (on the same or separate server):

-
- Step 1** As the root user, launch a terminal on the server where you want to install the Prime Network gateway.
- Step 2** Insert **Disk 1: New Install** in the DVD drive. (See [Installation DVDs, page 1-2](#)).
- Step 3** Mount the inserted DVD using the **mount** command, and move to the mount directory.
- Step 4** In the mount directory, locate the install.pl script and move to its parent directory.
- Step 5** Start the installation with the install.pl script. (The installation procedure is automatic and requires no user input.) The **-user** flag creates the operating system user account for the Prime Network application, and the **-dir** option specifies the installation directory:

```
perl install.pl -user pnuser [-dir directory]
```



Note *pnuser* must start with a letter and contain only the characters shown in brackets: [A-Z a-z 0-9]. It cannot contain a [.] character. For example, pn50 is permitted, but network 5.0 is not.

For example, the following command creates a *pnuser* named pn50, and installs Prime Network in the /export/home/pn50 directory:

```
perl install.pl -user pn50 -dir /export/home/pn50
```



Note The installation might take a while. You will be notified when the installation has completed successfully.

- Step 6** After the installation is complete, you will be prompted to configure Prime Network. Enter **yes** to continue with the configuration and proceed to [Step 8](#), or enter **no** to configure Prime Network later using the **network-conf** command.



Note If you choose to configure Prime Network at a later stage (not during the initial installation process), you must manually enable the network discovery functionality, as described in [Enabling Network Discovery, page 12-4](#).

- Step 7** Copy the following Oracle installation .zip files from **Prime Network 5.0, Disk 6: Database Binaries** to the embedded_oracle directory (\$NETWORKHOME/local/scripts/embedded_oracle):
- linuxamd64_12c_database_1of2.zip
 - linuxamd64_12c_database_2of2.zip

Step 8 Select **Set machine as Prime Network gateway**, then press **Enter**. The Prime Network configuration utility configures the system by running a number of procedures, including generation of SSH keys.



Note If you are notified that NTP is stopped or not configured, restart or configure NTP and then proceed with the rest of the configuration. See [Configuring the Network Timing Protocol](#), page 3-7.

Step 9 Enter a password for all built-in users (root, bosenable, bosconfig, bosusermgr, web monitoring user). This password will be used to access the various Prime Network system components, and will also be used as the database schema password.

The password must:

- Contain at a minimum 9 characters.
- Contain both upper and lower case letters.
- Start with a letter.
- Contain at least one number.
- Contain at least one of the allowed special characters: ~!#%^ (no other special characters to be used)
- Not contain the username or the username in reverse.
- Not contain cisco, cisco in reverse, or any variation.
- Not repeat the same character three or more times.

Step 10 When asked if Prime Network should install the database for you, select **Yes**. This is the embedded database option.

Step 11 During the configuration, you will be requested to provide some information. Enter the required information at the prompts. The following table lists the prompts that appear at various stages of the configuration and their required settings.

Table 6-1 Gateway Installation Prompts and Input Using Embedded Database

Prompt for...	Enter...	Notes
Database installation on a remote server.	yes/no	<p>This guide assumes that the database will be installed locally on the gateway server.</p> <p>If you want to install the embedded database on a remote server, enter yes. The next few prompts will ask you to enter the remote server details (IP address, username and password to connect to the remote server, and OS root user password (if not provided earlier)).</p> <p>Note If the IP address you enter is not the default one, the database installation software updates the hostname in the database listener's files. Verify that /etc/hosts is updated with the correct IP address and hostname. If more than one hostname is attached to the selected IP address, the first hostname is used.</p>
Selecting a single interface for the database services. Note This prompt appears only if more than one interface is detected during the network-conf process.	NIC to use for database connection	Because Prime Network 5.0 supports dual NICs, the installation may detect that the server is configured with multiple NICs. Specify the NIC to use for the database connection.
OS root user password	Unix root password	Prime Network uses the root password to set machine-level settings and to execute scripts.
OS username	—	The username of the Unix database user. The default is oracle.
OS user home directory	Path to the Oracle user home directory	OS user home directory by default is /export/home/oracle. The directory must have a minimum of 6 GB of disk space for oracle binaries, and should not reside under Prime Network user home directory.
Removing previous installation of Oracle.	yes	<p>Default is yes. If you already have Oracle installed with the same user and home directory, enter yes to remove it before installing the new database.</p> <p>If you enter no, the installation will quit.</p>
Selecting Prime Network database profile.	The number corresponding to the estimated profile.	<p>Select from 1-7 based on the actionable events per second.</p> <p>For more information on database profiles, see Creating an External Oracle Database, page 4-2.</p>
Database's datafiles location	Path to the directory containing the datafiles.	Location of the database datafiles (/export/home/oracle/oradata/anadb by default).
Redo logs location	Path to the directory containing the redo files.	<p>Location of the redo logs. They should not be on the same disk as the data files. Example: /export/home/oracle/redo.</p> <p>Note Use ext3 partition mounted with the default mount options.</p>

Table 6-1 Gateway Installation Prompts and Input Using Embedded Database (continued)

Prompt for..	Enter..	Notes
Prime Network to run automatic database backups?	yes	The default is yes . If you entered no at this prompt, you can enable automatic backups later with the emdbctl --enable_backup command. See the Cisco Prime Network 5.0 Administrator Guide for information on the emdbctl utility.
Destination for archive logs	Path to the directory containing the archive logs.	Location of the archive logs. They should not reside on the same disk as the data files.
Destination for backup files	Path to the directory containing the backup files.	Location of the backup files. They should not reside on the same disk as the data files.
SMTP server IP/hostname	Company e-mail server IP address or host name.	Port 25 must be available. You must have SMTP server access from the gateway in order to receive e-mail notifications. If you enter an invalid server, you can change the SMTP server later using emdbctl -set_smtp_server as described in the Cisco Prime Network 5.0 Administrator Guide . Note Prime Network validates the SMTP server only on installations where the gateway and embedded database reside on the same server.
Selecting a single interface for Prime Network backend services. Note This prompt appears only if more than one interface is detected during the network-conf process.	The number corresponding with the IP address of the back-end interface to be used for gateway-to-unit communication.	Because Prime Network 5.0 supports dual NICs, the installation may detect that the server is configured with multiple NICs. Specify the NIC to use for back-end services (such as transport, http, and so on) for gateway-to-unit communication. Dual NICs let you isolate the northbound interface from the back-end interface.
Installing Prime Network as part of a Prime suite of products.	no	Default is no . If you enter yes , additional prompts on suite installation appears, as shown in Prime Suite Prompts , page 6-6. Note If you use Prime Network in suite mode, you must additionally install the Prime Network Integration Layer (PN-IL). Integration of Prime Network should have been done before installing the operations report. See Installing the Prime Network Integration Layer , page 9-1. Refer to the Cisco Prime Central Quick Start Guide to see how to integrate and configure the PN-IL in suite mode. Once the PN is integrated to PC, the PN and the PN-IL status should be up in the PC portal.
E-mail ID for receiving alerts	username@company-name.com	E-mail address to receive notification when database errors occur. You can enter a single email address or a comma separated list of email addresses.

Table 6-1 Gateway Installation Prompts and Input Using Embedded Database (continued)

Prompt for...	Enter...	Notes
Disabling Low and Medium strength Ciphers	yes/no	<p>Choose either one of the following option:</p> <ul style="list-style-type: none"> no —No change happens in Prime Network security configurations. yes —Disables Low and Medium strength Ciphers. <p>If you disable Low and Medium strength Ciphers, you must ensure that all network connections are using High Strength Ciphers before disabling.</p> <p>Note The standalone script updateciphers.pl and the install flows do not allow to set the cipher strength to low and medium. The updateciphers.pl script only allows to configure the setting to High (not visa-versa) after the restart of services.</p>
Starting the Prime Network gateway at the end of the installation.	yes	Default is yes . If you enter no , you can start Prime Network later using the procedure in Starting the Prime Network Gateway , page 6-13.
Prime Suite Prompts		
Prime Central database server IP address	IP Address	After providing these inputs, Prime Network will be launched in <i>suite mode</i> . To integrate Prime Network with Prime Central, see Cisco Prime Central Quick Start Guide .
Prime Central database SID	primedb	
Prime Central database username	username	
Prime Central database password	password	
Prime Central database port	port number	

After the installation is complete, the following logs are available:

- Installation logs are available at `/var/adm/cisco/prime-network/logs`.
- Configuration logs are available at `$NETWORKHOME/Main/logs`.
- Network Discovery logs are available at `$NETWORKHOME/XMP_Platform/logs/existenceDiscovery.log`

Installing the Prime Network Gateway With an External Database

This procedure describes installation of Prime Network gateway using an external database. Before installing the gateway make sure the external Oracle database is set up as described in [Preparing the Oracle External Database](#), page 4-1.

**Note**

Change and Configuration Management (CCM) does not support encrypted databases. CCM can be installed on a Prime Network gateway that uses an encrypted connection to the database, but the connection used by CCM will not be encrypted.

Before You Begin

Verify that all preinstallation tasks have been completed. See [Gateway Preinstallation Tasks—External Database, page 3-3](#).

To install the gateway with an external database:

- Step 1** (Optional) Obtain the Prime Network ISO image files from Download Software page on Cisco.com, and burn the ISO image files to DVDs.

**Note**

Perform this step only if you are downloading the Prime Network ISO image files from Cisco.com.

- Step 2** As the root user, launch a terminal on the server where you want to install Prime Network gateway.
- Step 3** Insert **Disk 1: New Install** in the DVD drive.(See [Installation DVDs, page 1-2](#)).
- Step 4** Mount the inserted DVD using the **mount** command, and move to the mount directory.
- Step 5** In the mount directory, locate the install.pl script and move to its parent directory.
- Step 6** Start the installation with the install.pl script. (The installation procedure is automatic and requires no user input.) The **-user** flag creates the operating system user account for the Prime Network application, and the **-dir** option specifies the installation directory:

```
perl install.pl -user pnuser [-dir directory]
```

**Note**

pnuser must start with a letter and contain only the characters shown in brackets: [A-Z a-z 0-9]. It cannot contain a [.] character. For example, pn50 is permitted, but network 5.0 is not.

For example, the following command creates a *pnuser* named pn50, and installs Prime Network in the /opt/primenetwork50 directory:

```
perl install.pl -user pn50 -dir /opt/primenetwork50
```

**Note**

The installation might take a while. For information on the Cisco Prime Network environment created during installation, see [Table 6-5](#).

- Step 7** After the installation is complete, you will be asked if you want to proceed directly to the configuration of Prime Network. Enter **yes** to continue with the configuration or enter **no** to configure Prime Network later using the **network-conf** command (as *pnuser*).

**Note**

If you choose to configure Prime Network at a later stage (not during the initial installation process), you must manually enable the network discovery functionality, as described in [Enabling Network Discovery, page 12-4](#)

- Step 8** Select **Set machine as Prime Network gateway**, then press **Enter**. The Prime Network configuration utility configures the system by running a number of procedures, including generation of SSH keys.
- Step 9** Enter the required information at the prompts. [Table 6-2](#) lists the prompts that appear at various stages of the configuration and their required settings.

Table 6-2 Gateway with External Database Installation Prompts and Input

Prompt for...	Enter...	Notes
Password for all built-in users (root, bosenable, bosconfig, bosusermgr, web monitoring user)	The password that will be used to access the various Prime Network system components.	<p>The three login levels defined to connect to the Prime Network shell. This password will also be used as the database schemas password.</p> <p>You can change the password for each of these users at a later stage. See the Cisco Prime Network 5.0 Administrator Guide for changing the passwords.</p> <p>The password must:</p> <ul style="list-style-type: none"> • Contain at a minimum 9 characters. • Contain both upper and lower case letters. • Start with a letter. • Contain at least one number. • Contain at least one of the allowed special characters: ~!#%^ (no other special characters to be used) • Not contain the username or the username in reverse. • Not contain cisco, cisco in reverse, or any variation. • Not repeat the same character three or more times.
Prime Network to install the database?	no	After you enter no , the setup will configure the Prime Network default schema. You can manually create the database schemas, as described in Manually Creating Prime Network Database Schemas , page 6-11.
Oracle server IP address/host name	IP address/hostname	
Oracle admin username	<i>username</i>	Default is system.

Table 6-2 Gateway with External Database Installation Prompts and Input (continued)

Prompt for..	Enter..	Notes
Oracle admin password	password	Password for the database administrator.
Allowing Prime Network to auto-configure the database	yes	<p>If you enter yes, the <i>pnuser</i> database is configured automatically with the following default values:</p> <ul style="list-style-type: none"> • Port 1521 • SID: mcdb • No encryption • Prime Network-created users <p>The <i>pnuser_ep</i> (Event Archive) schema uses the same settings.</p> <p>If you enter no, alternative database server is used to install EP schema. You need to provide the Port number, SID and whether you require an encrypted connection to the database server. If you select encrypted connection, enter the values as shown in Table 6-4. If you have manually created the database schemas, as described in Manually Creating Prime Network Database Schemas, page 6-11, you need to provide these schemas details.</p>

Step 10 The installer then installs the Change and Configuration Management application as a part of the installation.



Note The installation of Change and Configuration Management will abort if your Oracle account is locked during the installation process. You must unlock the account and then run the `setup_xmp_nccm.cmd` command to install the Change and Configuration Management components.

Step 11 Enter the input for the remaining prompts as shown in the [Table 6-3](#).

Table 6-3 Gateway Installation Prompts and Input Using External Database

Prompt for...	Enter...	Notes
Selecting a single interface for the database services. Note This prompt appears only if more than one interface is detected during the network-conf process.	NIC to use for database connection	Because Prime Network 4.3.2 supports dual NICs, the installation may detect that the server is configured with multiple NICs. Specify the NIC to use for the database connection.
Installing Prime Network as part of a Prime suite of products.	no	Default is no . If you enter yes , additional prompts on suite installation appear, as shown in Prime Suite Prompts, page 6-6 . Note If you use Prime Network in suite mode, you must install the Prime Network Integration Layer (PN-IL). See Installing the Prime Network Integration Layer, page 9-1 . Refer to the Cisco Prime Central Quick Start Guide to see how to integrate and configure the PN-IL in suite mode.
Starting Prime Network at the end of the installation.	yes	Default is yes . If you enter no , you can start Prime Network later using the procedure in Starting the Prime Network Gateway, page 6-13 .

Prime Suite Prompts

Prime Central database server IP address	IP address	These prompts appear if you decided to install Prime Network as part of the suite.
Prime Central database SID	primedb	
Prime Central database username	username	
Prime Central database password	password	
Prime Central database port	port number	

Table 6-4 shows the parameters displayed for a remote database installation that uses an encrypted connection.

Table 6-4 Parameters For An Encrypted Connection

Prompt for..	Enter..	Notes
Oracle's listener port	<i>port-number</i>	Default is 1521
Oracle's SID	SID	Prime Central Database SID
Encrypted connection for database	yes	Default is yes .
Type of encryption method	Enter option (1-3)	Number corresponding to the encryption method you would like to use.
Type of encryption algorithm	Enter option (1-9)	Number corresponding to the encryption algorithm you would like to use.

After the installation is completed following logs are available:

- Installation logs are available at `/var/adm/cisco/prime-network/logs`.
- Configuration logs are available at `$NETWORKHOME/Main/logs`.
- Network Discovery logs are available at `$NETWORKHOME/XMP_Platform/logs/existenceDiscovery.log`

Manually Creating Prime Network Database Schemas



Note

This topic applies only if you are using Prime Network with external database.

Use the procedure in this section if you want to create database schemas manually. You can choose any name for the schema. By default, Prime Network uses *pnuser* to name the schemas. In the following table, *pnuser* is

Schema Name	Description	Example
<i>pnuser</i>	Fault Database—Active and archived network and non-network events and tickets (<i>archived events and tickets</i> are events and tickets that were moved to an archive partition in the Fault Database)	pn50
<i>pnuser_ep</i>	Event Archive—Raw traps and syslogs received from devices	pn50_ep
<i>pnuser_rep</i>	Used by reports mechanism	pn50_rep
<i>pnuser_ep_rep</i>		pn50_ep_rep

Schema Name	Description	Example
<i>pnuser_xmp</i>	Change and Configuration Management (CCM), Compliance Manager, Compliance Audit, Command Manager, Transaction Manager	pn50_xmp
<i>pnuser_admin</i>	Database administrator for maintenance tasks—such as gathering statistics—on the other Prime Network database schemas	pn50_admin

To manually create database schemas:

Step 1 Log into the database as the system user.

Step 2 Enter the following commands to create the database schemas. You can choose any name for the usernames and filenames. The password must be identical for the schemas.

- For *pnuser*, *pnuser_dwe*, *pnuser_ep*, *pnuser_xmp*, execute the following command:

```
create tablespace user datafile 'file-location/user.dbf' size 1024M autoextend on next
256M;
create temporary tablespace user_temp tempfile 'file-location/user_temp.dbf' size 100m
autoextend on next 5m maxsize 5000m;
create user user identified by "default-password" default tablespace user
temporary tablespace user_temp;
grant connect to user;
grant resource to user;
grant SELECT_CATALOG_ROLE to user;
```

- For *pnuser_rep* and *pnuser_ep_rep*, execute the following command:

```
create user user identified by "default-password" default tablespace pnuser temporary
tablespace pnuser_temp;
grant connect to user;
grant resource to user;
grant SELECT_CATALOG_ROLE to user;
grant CREATE SYNONYM to user;
```

- For *pnuser_admin*

```
create tablespace user datafile 'file-location/user.dbf' size 100M autoextend on next
100M maxsize 500m;
create user user identified by "default-password" default tablespace user temporary
tablespace pnuser_temp profile default;
GRANT RESOURCE TO user;
GRANT DBA TO user;
GRANT CONNECT TO user;
GRANT SELECT ANY DICTIONARY TO user;
GRANT ANALYZE ANY TO user;
GRANT SELECT ANY TABLE TO user;
GRANT EXECUTE ON DBMS_LOCK TO user WITH GRANT OPTION;
GRANT ALTER SYSTEM TO user;
ALTER USER user QUOTA UNLIMITED ON user;
```

Enabling the *pnuser_admin* user to run maintenance tasks on other schemas

To enable the *pnuser_admin* user to run maintenance tasks, such as gathering statistics, on the other Prime Network database schemas, complete the following steps:

-
- Step 1** As the Oracle UNIX user, use SQL*Plus to log into user sys as sysdba.
- Step 2** Enter one of the following commands:
- If the *pnuser_admin* user does not exist, enter:

```
SQL> grant execute on dbms_lock to system with grant option;
```
 - If the *pnuser_admin* user already exists, enter:

```
SQL> grant execute on dbms_lock to pnuser_admin with grant option;
```
- Step 3** Verify that your database contains the temporary TEMP tablespace, which is required by the new Prime Network admin database user. If this tablespace does not exist, create the TEMP tablespace.

Post Installation Tasks For the Gateway

After installing the gateway, perform these post-installation tasks.

- [Starting the Prime Network Gateway, page 6-13](#)
- [Verifying Connectivity, page 6-15](#)
- [Configuring Prime Network Post-Installation, page 6-16](#)
- [Verifying the Redirected Ports, page 6-17](#)
- [Verifying the Drools Rules Configuration, page 6-17](#)
- [service iptables save, page 6-17](#)
- [Verifying the Monitoring \(Graphs\) Configuration, page 6-17](#)
- [Verifying the Installation of Registry Directories, page 6-18](#)
- [Adding Oracle Database Files, page 6-18](#)
- [Updating the Database Host in the Registry for NAT, page 6-19](#)

Starting the Prime Network Gateway

-
- Step 1** As a Prime Network user, if you did not start the gateway at the end of the installation process, start it by entering the following command:

```
networkctl start
```

The gateway may require a few minutes to load.



Note

Prime Network 5.0 will automatically restart whenever the gateway server is restarted. If you want to disable this behavior (so that Prime Network has to be manually started after a gateway restart), see the [Cisco Prime Network 5.0 Administrator Guide](#).

-
- Step 2** As a Prime Network user, check the status of all processes and daemons by entering the following command:

```
status
```

The output lists all processes. For each AVM process that is checked, the **status** command displays, in brackets, the number of exceptions found in the total number of log file lines for that process. For example, the information for AVM 0 is [OK 0/39]; that is, 0 exceptions in the 39 log file lines that were checked.

The **status** command shows the version of the Prime Network installed and also verifies that the gateway processes are up and running. The processes are listed in the following table.

AVM Number	Process
AVM 0	High Availability/Switch
AVM 11	Gateway
AVM 19	Auto-Add
AVM 25	Fault Agent
AVM 35	Service Discovery
AVM 41	Compliance Manager
AVM 44	Operations Reports
AVM 76	Job scheduler AVM.
AVM 77	Change and Configuration Management (CCM)
AVM 78	VNE topology
AVM 83	TFTP Server (CCM)
AVM 84	Reports AVM
AVM 99	Management AVM
AVM 100	Event Collector
—	webserver daemon (client connection)
—	secured connectivity daemon



Note Check the log files for each AVM if there are any problems. The log files are located under `$NETWORKHOME/Main/logs`.

Verifying Connectivity

Verify the connectivity between the components as follows:

- Gateway and units— The gateway must have connectivity to all units. The gateway communicates frequently with the units to exchange information. Some unit-to-unit (VNE-to-VNE) communication may pass through the gateway. The units, managed devices, and gateway may not be located on separate networks.
- Gateway and clients— IP connectivity is required between the clients and the gateway. The Events and Vision GUIs also require IP connectivity to the database. The Events GUI is the only client application that communicates directly with the database.
Clients support automatic client updates from the gateway and, depending on the upgrade, the data can be up to 30 MB.
- Units and NEs—Unit host VNEs and therefore require SNMP/Telnet connectivity to the network elements.
- Gateway to Oracle database and unit to Oracle database—Required if you are installing an external database. See [Verifying the Connectivity to the Database, page 6-15](#).
- Gateway and units to Infobright database server—Required if you are installing Operations Reports.

Verifying the Connectivity to the Database



Note

This section is applicable only if you are using Prime Network with external database.

To confirm that your database is configured correctly:

Step 1 As *pnuser*, connect to SQLPLUS by entering the following command:

```
sqlplus username/'password'@'(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = host)(PORT = port)))(CONNECT_DATA =(SID = sid)))'
```

The password is the same as the root built-in password, *host* is the server where Oracle is installed, *port* is the listener's port (default is 1521) and *sid* is the database's name (default is mcdb).

Step 2 Confirm that the SQL client can connect to the database. If you see the a prompt similar to the following, the connection was successful:

```
SQL*Plus: Release 12.1.0.2 Production on Fri Sep 26 13:58:48 2014
```

```
Copyright (c) 1982, 2013, Oracle. All rights reserved. (please review, the date has to be changed)
```

```
Last Successful login time: Fri Sep 26 2014 13:58:28 +03:00
```

```
Connected to:
```

```
Oracle Database 12c Enterprise Edition Release 12.1.0.2 - 64bit Production  
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options
```

If the test fails, contact your local database administrator and repeat the test.

Configuring Prime Network Post-Installation

The standard Prime Network installation process includes the configuration phase. However, you can choose to configure Prime Network at a later stage.


Note

Do *not* rerun the **network-conf** script after AVMs or units are added. Rerunning the **network-conf** script could cause problems with the Prime Network registry.

To access the Prime Network configuration:

-
- Step 1** Make sure the database and listener are up, and as *pnuser*, enter the following command:
- ```
network-conf
```
- Step 2** The first time you log in, you are prompted to change the default password. It is recommended that you do so. To change the default user password, enter:
- ```
passwd pnuser
```
- Step 3** Provide the necessary information at the prompts, as described in [Installing the Prime Network Gateway With an Embedded Database, page 6-2](#) and [Installing the Prime Network Gateway With an External Database, page 6-6](#).

Changing a System Account of the OS User Name or/and Database User Name

To change the OS user or/and database user name from the Standalone mode or from the gateway unit, change of Prime Network user requires FTP configurations on the devices.


Note

The change of user name is not applicable for HA environment.

To change the Prime Network user name and database user name, follow the below steps:

1. Log in to the Prime Network client.
2. Run the following script,


```
~/PNHOME/local/scripts/changePrimeNetworkOSAndOracleUser.pl
execute as a root user
file location
/tmp
```
3. Enter the user name to change either a Prime Network user name or Oracle user name after Prime Network installation. Make sure to follow the below mentioned points:
 - a. Prime Network user name must be same in Gateway and unit.
 - b. The `changePrimeNetworkOSAndOracleUser.pl` script cannot be executed in the integrated setup. To execute the script, disintegrate Prime Network and re-integrate it.
 - c. If required, configure the devices with new Prime Network user name, which is similar to previous Prime Network user name, after the script execution is completed. If VNE's are configured with ftp protocol, the new Prime Network username should be updated in the device to work in CCM.

**Note**

After changing the SSH user name if you are unable to dis-integrate Prime Network from Prime Central, reintegration is required. Refer the [Troubleshooting Clients](#) section for more information.

Verifying the Redirected Ports

Prime Network redirects some ports (161, 162, 514, 69) during the installation for receiving the traps and messages. Verify that these ports were redirected by entering the following as the root user:

```
iptables -L -t nat
```

The result should contain the following rows:

```
REDIRECT udp -- anywhere anywhere udp dpt:snmptrap redir ports 1161
REDIRECT udp -- anywhere anywhereudp dpt:snmptrap redir ports 1162
REDIRECT udp -- anywhere anywhereudp dpt:syslog redir ports 1514
REDIRECT udp -- anywhere anywhereudp dpt:tftp redir ports 1069
```

If not, enter the following:

```
iptables -t nat -A PREROUTING -p udp --dport 161 -j REDIRECT --to-port 1161
iptables -t nat -A PREROUTING -p udp --dport 162 -j REDIRECT --to-port 1162
iptables -t nat -A PREROUTING -p udp --dport 514 -j REDIRECT --to-port 1514
iptables -t nat -A PREROUTING -p udp --dport 69 -j REDIRECT --to-port 1069
ip6tables -t mangle -A PREROUTING -p udp --dport 69 -j TPROXY --on-port 1069
ip6tables -t mangle -A PREROUTING -p udp --dport 514 -j TPROXY --on-port 1514
ip6tables -t mangle -A PREROUTING -p udp --dport 161 -j TPROXY --on-port 1161
ip6tables -t mangle -A PREROUTING -p udp --dport 162 -j TPROXY --on-port 1162
service iptables save
```

Verifying the Drools Rules Configuration

To confirm that the Drools rules file was created correctly, check the `$NETWORKHOME/Main/data` directory and verify that the `post.drl` file exists. If it does not exist, rerun the installation.

Verifying the Monitoring (Graphs) Configuration

To confirm that the Monitoring (graphs) tool is working correctly:

- Step 1** Open a web browser on a client that is connected to the gateway.
- Step 2** Enter the following URL to connect to the Cisco Prime Network graph:

```
https://gateway-IP-address:1311/graphs/
```

**Note**

The username and password for the graphs were configured during installation. For changing the password for monitoring (graphs) tool, see [Cisco Prime Network 5.0 Administrator Guide](#).

- Step 3** If you cannot log in, the tool may not be enabled. You can enable and disable the tool by logging in as *pnuser* and running **webcontrol start** or **webcontrol stop**.
-

Verifying the Installation of Registry Directories

To confirm that the registry directories are installed on the gateway:

- Step 1** On the server, browse to the directory `~/Main/registry/ConfigurationFiles`.
- Step 2** Verify that the directory contains the following subdirectories:
- 127.0.0.1
 - 0.0.0.0
- Step 3** Verify that the webserver daemon is up and running by executing **networkctl status**.
-

Adding Oracle Database Files



Note

This topic is applicable only if you are using Prime Network with embedded database.

Use the **add_emdb_storage.pl** script (or **add_emdb_storage.pl -ha** for deployments with gateway high availability) to add database files according to the database size you estimate that you will need. For usage of **add_emdb_storage.pl -ha** script, see [Cisco Prime Network 5.0 High Availability Guide](#).

When using this script, you are prompted to provide the database profile, the estimated database capacity and the history size for events and workflows. This enables the script to calculate the maximum size of the database, and to create the data files, temp files, and redo logs. See [Prime Network Gateway and Database Requirements, page 2-2](#) for information on database sizing.

Before You Begin

If you need assistance estimating the database size, contact your Cisco account representative.

- Step 1** Log into the gateway as *pnuser*.
- Step 2** Change directories to `$NETWORKHOME/Main/scripts/embedded_db` and enter the following command:
- ```
./add_emdb_storage.pl
```
- Step 3** Enter the number corresponding to the estimated database profile that meets your requirement.
- Step 4** Enter the event and workflow archiving size in days.



### Note

If you enter incorrect values—such as the wrong database profile estimate—you can rerun the script with different inputs.

---



If you encounter any errors, messages similar to the following examples are displayed.

- If there is not enough disk space to create the additional database files or redo logs, enter another location.
- If the files or redo logs cannot be created for any reason, you will see an error message and the following prompt:

```
- How would you like to continue?

1) Retry
2) Skip (move to the next in list)
3) Abort
(1 - 3) [default 1]
```

For example, if the correct permissions were not set, you would see the following.  
Failed to add datafile for pn50:  
-1119: ORA-01119: error in creating database file '/2del/pn50\_DATA11.dbf'  
ORA-27040: file create error, unable to create file  
Linux-x86\_64 Error: 13: Permission denied

The menu choices provide with you with an opportunity to fix the permissions and retry creating the file or log.

The log file is located in `$NETWORKHOME/Main/logs/emdb/add-storage-time-stamp.log`.

## Updating the Database Host in the Registry for NAT

If you are using NAT with the Events client, update the database host in the registry so it contains the hostname instead of the IP address. Complete the following steps after the gateway installation is complete and the system is up and running.



### Note

If you already use a hostname instead of an IP address, you do not have to repeat this procedure.

**Step 1** Verify that the Windows client workstations have the correct Domain Name System (DNS) mapping.

**Step 2** From `~/Main`, enter the following commands:

```
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/persistence/nodes/main/Host database-server-hostname
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/persistence/nodes/ep/Host database-server-hostname
```

**Step 3** Enter the following command to restart the Prime Network system:

```
networkctl restart
```

# Environment Variables, Aliases, and Folders Created During Installation

The Prime Network installation script creates environment variables, folders, aliases, and services on the Prime Network gateway.

Table 6-5 defines the *pn-user* environment variables defined by the installation script.

**Table 6-5** *pn-user Environment Variables Defined by the Installation Script*

| Variable Name                                                                                                                                                                            | Default                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| NETWORKHOME                                                                                                                                                                              | /export/home/pnuser        |
| <b>Note</b> At the command line, enter \$PRIME_NETWORK_HOME for this variable. For compatibility with previous Cisco Active Network Abstraction releases, this variable was not changed. |                            |
| JAVA_HOME                                                                                                                                                                                | NETWORKHOME/java           |
| NCCM_HOME                                                                                                                                                                                | NETWORKHOME/NCCMComponents |
| XMP_HOME                                                                                                                                                                                 | NETWORKHOME/XMP_Platform.  |



## Caution

Do not change permissions on the *NETWORKHOME* directory. If the permissions are too lax, SSH communication problems can occur and the gateway might not start.

Table 6-6 lists the aliases defined by the installation script.

**Table 6-6** *Aliases Defined by the Installation Script*

| Table Alias | Content                                              |
|-------------|------------------------------------------------------|
| reg         | Changes the directory to \$NETWORKHOME/Main/registry |
| main        | Changes the directory to \$NETWORKHOME/Main          |
| logs        | Changes the directory to \$NETWORKHOME/Main/logs     |

Table 6-7 lists the folders created in Prime Network 5.0.

**Table 6-7** *Folders Created in Prime Network*

| Folder                           | Contents                                                                                                       |
|----------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Folders in NETWORKHOME.</b>   |                                                                                                                |
| Main/bosconfig                   | Prime Network configuration files (syntax of the commands, supported errors, and the connection configuration) |
| Main/bosconfig/bos_shell_scripts | User-created scripts                                                                                           |
| Main/data                        | Drools configuration files and user-defined scripts.                                                           |
| Main/logs                        | Log output files ( <i>AVM-ID.out</i> ; for example, 0.out or 11.out)                                           |

**Table 6-7 Folders Created in Prime Network (continued)**

|                                  |                                                                                         |
|----------------------------------|-----------------------------------------------------------------------------------------|
| Main/registry                    | Local copy of registry files                                                            |
| Main/registry/ConfigurationFiles | <i>Golden source</i> (master registry) configuration files in the Prime Network gateway |
| Main/registry/templates          | Registry file templates used by the Prime Network gateway for global system changes     |
| local/scripts                    | Scripts on the gateway and units                                                        |
| Main/scripts                     | Scripts on the gateway and units                                                        |
| Third_Party                      | Third-party files                                                                       |
| Main/unix                        | UNIX maintenance scripts and utilities                                                  |
| Main/reportfw/rptdocument        | Reports                                                                                 |
| Main/drivers                     | VNE driver files                                                                        |
| prime_integrator                 | Integrating Prime Network into Prime Central                                            |
| NCCMComponents                   | Configuration and Change Management (CCM)                                               |
| XMP_Platform                     | Contains XMP platform components used by CCM                                            |
| pentaho                          | Operations Reports                                                                      |

## Product Services Installed with Prime Network

Table 6-8 lists the product services that are installed with the Prime Network system.

**Table 6-8 Product Services Installed with Prime Network**

| Name                    | Function                                                  | Configuration Information            | TCP or UDP Port Number                                                                            | Dynamic TCP or UDP Port Ranges   | Interdependencies with Other Features, Services, and Applications | Traffic Classification |
|-------------------------|-----------------------------------------------------------|--------------------------------------|---------------------------------------------------------------------------------------------------|----------------------------------|-------------------------------------------------------------------|------------------------|
| avm[1-999]              | Main application                                          | Main/registry/Av<br>m[NUM].xml       | 8000+AVM<br>number for<br>secured XML<br>RPC<br><br>2000+AVM<br>number for<br>local<br>management | 2000-3000,<br>8000-9000<br>(TCP) | Java, Perl, Tcsh                                                  | Inner protocol         |
| sheer_secured<br>daemon | Secured<br>connectivity<br>between<br>gateway and<br>unit | local/sheer_secured/<br>sheer_config | 1101 (TCP)                                                                                        | —                                | —                                                                 | SSH                    |

**Table 6-8** *Product Services Installed with Prime Network (continued)*

| Name                          | Function                                                              | Configuration Information      | TCP or UDP Port Number | Dynamic TCP or UDP Port Ranges | Interdependencies with Other Features, Services, and Applications | Traffic Classification |
|-------------------------------|-----------------------------------------------------------------------|--------------------------------|------------------------|--------------------------------|-------------------------------------------------------------------|------------------------|
| webserver daemon              | Serves the client Web Start and the diagnostics tool with graphs      | utils/apache/conf / sheer.conf | 1311 (TCP)             | —                              | —                                                                 | HTTP                   |
| Machine interface             | BQL machine-to-machine interface                                      | —                              | 9002 (TCP)             | —                              | Java                                                              | —                      |
| Secure machine interface      | Secured (SSL) BQL machine-to-machine interface                        | —                              | 9003 (TCP)             | —                              | Java                                                              | —                      |
| Transport switch              | Gateway/unit internal message bus.                                    | —                              | 9390 (TCP)             | —                              | Java                                                              | —                      |
| Client Applications Transport | Client/gateway message bus.<br>This PTP connection is secured by SSL. | —                              | 9771 (TCP)             | —                              | Java                                                              | —                      |

## Troubleshooting

The following troubleshooting tips help you to solve common problems in Prime Network Installation.

| Problem/Message                                                                           | Solution/Action Required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Problem</b> Swap file entry error                                                      | <p><b>Solution</b> Increase the swap file size in two ways:</p> <p>Enter the keyword “-override_swap” along with the installation command.</p> <p>For example. <code>perl install.pl -user pn43 -override_swap</code></p> <pre>dd if=/dev/zero of=/swapfile bs=1024 count=65536 (based on the requirement size, the bs &amp; count entry will differ) mkswap /swapfile chmod 0600 /swapfile swapon /swapfile</pre> <p>To enable it at boot time:</p> <p>Edit /etc/fstab to include the following entry:</p> <pre>/swapfile swap swap defaults 0 0</pre>                                           |
| <b>Problem</b> Error in deploying fetch_expect or RRDs or Embedded database (on RHEL 5.8) | <p><b>Solution</b> Remove the “=” symbol from the following file:</p> <pre>Cat /etc/profile.d/proxy.csh</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Problem</b> Host file entry error                                                      | <p><b>Solution</b> Check the host file for local host entry:</p> <pre>Cat /etc/hosts 127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4 ::1 localhost localhost.localdomain localhost6 localhost6.localdomain6 Local host IP hostname hostname.domainname For eg, if the hostname is pn-dev-u-008 and its ip add is 172.25.98.208, then the entry should be 127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4 ::1 localhost localhost.localdomain localhost6 localhost6.localdomain6 172.25.98.208 pn-dev-u-008 pn-dev-u-008.cisco.com</pre> |
| <b>Problem</b> SMTP TIME OUT Error (on both RHEL 5.8 & 6.5)                               | <p>This occurs when there is SMTP time out error.</p> <p><b>Solution</b></p> <ol style="list-style-type: none"> <li>1. Get to the following file:<br/><code>/etc/opt/quest/vas/vas.conf</code></li> <li>2. Edit the following entry:</li> </ol> <pre>prompt-local-pw = From "This is your UNIX password: " to "Password:" prompt-vas-ad-pw = From "This is your UNIX password: " to "Password:"</pre>                                                                                                                                                                                             |

| Problem/Message                                                                                                                                                                                                                                                                                                                           | Solution/Action Required                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Problem</b> COMPACT LSB error</p>                                                                                                                                                                                                                                                                                                   | <p><b>Solution</b> While installing any RPM, update the LSB core with the following command:</p> <pre>yum install redhat-lsb-core or yum update redhat-lsb-core</pre>                                                                                                                                                                   |
| <p><b>Problem</b> It is time consuming to install multiple RPMs individually</p>                                                                                                                                                                                                                                                          | <p><b>Solution</b> To install Multiple RPM's simultaneously:</p> <ol style="list-style-type: none"> <li>1. Create a txt file and copy all the RPM names.</li> <li>2. Enter the following command:</li> </ol> <pre>yum install `awk '{print \$1}' ./rpm.txt` -y</pre> <p>where, "rpm.txt" is name of the text file that you created.</p> |
| <p>During installation or upgrade you may encounter the following errors:</p>                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                         |
| <p><b>Problem</b> Unable to establish master SSH connection: master process exited unexpectedly at reader<br/>PrimeNetwork::DB::Oracle::_ssh</p>                                                                                                                                                                                          | <p>This occurs when master process exited unexpectedly at reader<br/>PrimeNetwork::DB::Oracle::_ssh</p> <p><b>Solution</b> Check whether the Openssh or Openssl got installed and updated.</p>                                                                                                                                          |
| <p><b>Solution</b> Failed to backup the database with the following error<br/>ORA-27369: job of type EXECUTABLE failed with exit code: Operation not permitted<br/>ORA-06512: at "SYS.DBMS_ISCHED", line 198<br/>ORA-06512: at "SYS.DBMS_SCHEDULER", line 594<br/>ORA-06512: at line 1 (DBD ERROR: OCISmtExecute) .<br/>ABORTING. ***</p> | <p><b>Solution</b><br/>Enable the backup and give proper permission to the folder for both backup and archive, which are under Oracle home folder.</p>                                                                                                                                                                                  |
| <p><b>Problem</b> Error: Failed on creating inventory logical tables</p>                                                                                                                                                                                                                                                                  | <p>This occurs when there is a SQL syntax error.</p> <p>For example: check the log and get into that location to check the syntax. In this case,<br/>/export/home/pn43/Main/plugins/newalarm/deployment/infobrightdeployment/inventory/logical</p>                                                                                      |

| Problem/Message                                                                                                                                                   | Solution/Action Required                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Problem</b> Failed to copy ssh keys from gateway error (during unit adding)</p>                                                                             | <p>Check the following:</p> <ul style="list-style-type: none"> <li>• proxy settings and file permissions of /\$PNHOME/local/ana_secured and /\$PNHOME/</li> <li>• RHEL version. If the RHEL version is 6.5, make sure the openssl rpm is updated (to 57 version).<br/> <pre>openssl-1.0.1e-57.el6.i686.rpm openssl-1.0.1e-57.el6.x86_64.rpm</pre> </li> <li>• Make sure that firewall is configured properly or in stopped state.</li> </ul> |
| <p><b>Problem</b> Prime Network failed to start with the following error:<br/><br/>This unit (10.104.63.97) is not connected to 10.104.63.96 gateway anymore.</p> | <p>Check if both Unit and GW got installed on the same directory path. For example, either in /export/home or /home.</p>                                                                                                                                                                                                                                                                                                                     |
| <p><b>Problem</b> Unable to launch the CCM application</p>                                                                                                        | <p>Check for the following:</p> <ul style="list-style-type: none"> <li>• Web server should be up</li> <li>• Tomcat should be up</li> <li>• dmctl status</li> </ul>                                                                                                                                                                                                                                                                           |

| Problem/Message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Solution/Action Required                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Problem</b> Receiving the following error entries:</p> <pre>Unzipping p23054354_121010_Linux-x86-64.zip on the database server  Stopping the database and listener /export/home/anaoracle/product/12.1.0/db_1/bin/dbshut: line 160: /export/home/oracle/product/12.1.0/db_1/shutdown.log:Permission denied  Installing p23054354_121010_Linux-x86-64.zip on the database server. This may take a while  Starting the database and listener touch: cannot touch `/export/home/oracle/product/12.1.0/db_1/startup.log': Permission denied  chmod: changing permissions of `/export/home/oracle/product/12.1.0/db_1/startup.log': Operation not permitted  /export/home/anaoracle/product/12.1.0/db_1/bin/dbstart: line 346: /export/home/oracle/product/12.1.0/db_1/startup.log:Permission denied</pre> | <p>This occurs when there is no proper permission to ivne-drivers.tar file &amp; oracle home folder.</p> <p><b>Solution</b> Check the permissions of copied ivne-drivers.tar file and oracle home folder.</p> |
| <p><b>Problem</b> Unit AVM failed / unreachable to start the Prime Network after Rollback</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <p><b>Solution</b> Check if the hostname entry on /etc/hosts is appropriate.</p>                                                                                                                              |
| <p><b>Problem</b> Receiving errors during XMP platform and Web server installation process.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <p><b>Solution</b> Make sure all the Required RPMs for Oracle Database 12c got installed. Ensure that two mandatory RPMS; libXext-1.1 (x86_64) and libXtst-1.0.99.2 (x86_64) are installed properly.</p>      |

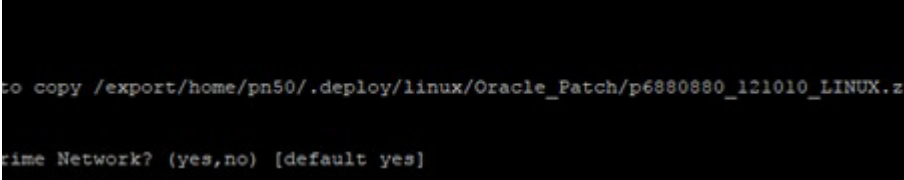


| Problem/Message                                                                                                                                                                       | Solution/Action Required                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Problem</b> The following ports are unreachable on the Prime Network Gateway (ipadd): 6081, 9490, 1101".while adding unit with gateway. (using either ipv4 or ipv6 address)</p> | <p><b>Solution</b></p> <p>Make sure that:</p> <ul style="list-style-type: none"> <li>• Ports such as 6081, 9490, 1101 are in listening state.</li> <li>• iptables (for both ipv4 and ipv6) got turned off.</li> <li>• Selinux got disabled or in permissive mode.</li> </ul>                                                         |
| <p><b>Problem</b> Compliance engine status is down</p>                                                                                                                                | <p><b>Solution</b> Check the ComplianceService.log under:<br/>PNHOME/XMP_Platform/logs and nccm.log under PNHOME<br/>utils/independent/compliance/bin</p> <p><b>Solution</b> Check the DB ip address entry in the following folder path:<br/>PNHOME/utils/independent/compliance/resources/server/global/nccmDatabase.properties</p> |
| <p><b>Problem</b> Compliance Engine not starting:<br/>.</p>                                                                                                                           | <p>Before upgrading to 5.0, take the backup file "nccmDatabase.properties" that is located in:<br/>PNHOME/utils/independent/compliance/resources/server/global/nccmDatabase.properties</p>                                                                                                                                           |
| <p><b>Problem</b> Could not open '/tmp/ana_db_properties.properties' for reading No such file or directory</p>                                                                        | <p><b>Solution</b> Check the oracle 12c files permissions.</p>                                                                                                                                                                                                                                                                       |

| Problem/Message                                                                                                                                                                                                                                                                                                                                                                                            | Solution/Action Required                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Problem</b> Unit servers shows Virtual IP address during Network configuration.</p> <p><b>Figure 6-1 Unit Servers</b></p> <hr/> <pre> All Servers   Gateway 10.76.82.101   Unit 0.0.0.1 (unit-2)   Unit 0.0.0.2 (unit-3)   Unit 0.0.0.3 (unit-5)   Unit 0.0.0.4 (unit-6)   Unit 0.0.0.5 (unit-7)   Unit 10.76.82.206 (unit-1)   Unit 10.76.82.209 (unit-4) Event Notification Global Settings </pre> | <p><b>Solution</b> This occurs when either gateway or Unit server is not installed on the same directory. For example:/export/home/pnuser.</p> <p>Make sure to install the Unit servers with the same directory path in which the Gateway is installed.</p> |

**Problem** Receiving errors ending with number 256.

**Figure 6-2 Errors ending with 256**



```

to copy /export/home/pn50/.deploy/linux/Oracle_Patch/p6880880_121010_LINUX.z
ime Network? (yes,no) [default yes]

```

**Solution** This occurs when the oracle is not uninstalled properly.



## Installing Prime Network Units

This chapter covers the installation and post installation tasks for Prime Network units.

- [Installing a Unit, page 7-1](#)
- [Post Installation Tasks For Units, page 7-4](#)

### Installing a Unit

Complete the following steps to install the Prime Network unit and the tools that are required for unit functionality, including JDK 1.7.0\_25 and Perl 5.16.



#### Note

Ensure that the OS version of unit and gateway is same while adding the unit to the gateway. Also, make sure that the home directory of the unit or the redundant unit is the same as the home directory of the gateway.

- 
- Step 1** Before starting with the installation, check the unit prerequisites in [Prime Network Unit Requirements, page 2-10](#) and make sure you have completed all the unit preinstallation tasks in [Unit Preinstallation Tasks, page 3-5](#).
- Step 2** Insert **Disk 1: New Install** in the DVD drive. (See [Installation DVDs, page 1-2](#).)
- Step 3** Open a Telnet or SSH session to the unit and log in as root.
- Step 4** Back up and remove the old version of the unit (if an older version exists). For backup procedures, see the [Cisco Prime Network 5.0 Administrator Guide](#).
- Step 5** To change directories to the CD directory, enter:
- ```
cdCisco Prime Network 5.0 Installation Guide /cdrom/cdrom0/Server
```
- Step 6** To install the Cisco Prime Network unit, complete one of the following steps:
- a. For a new Prime Network 5.0 installation, enter the following command.
- ```
perl install.pl -user pn50 -dir /export/home/pn50
-uninstall_previous_versions -override_swap -override_ports
```

You must enter the same *pnuser* and directory path that you used when you installed the gateway. (If the gateway and unit have different usernames and directory paths, the unit will not start.)

For example, if the name of the user is pn50, enter the above command.

The installation of the unit starts.



**Note** This process might take a while.

- Step 7** After the installation is complete, you will be prompted to configure Prime Network. Enter **yes** to continue to [Step 8](#) or **no** to continue to the next step and configure later using the **network-conf** command. (You can run **network-conf** by opening a Telnet or SSH to the unit, logging in as *pnuser*, and running **network-conf**.)
- Step 8** Select **Set machine as Prime Network unit**, then press **Enter**. The Prime Network configuration utility configures the system by running a number of procedures.
- Step 9** Enter the required information at the prompts. The following table lists the prompts that appears at various stages of the unit configuration and their required settings

**Table 7-1 Prompts A**

| Unit Field                                                                                                                                                                       | Enter:                                                                                                               | Notes                                                                                                                                                                                     |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Checking NTP configuration on machine.                                                                                                                                           | yes                                                                                                                  | Default is <b>yes</b> .                                                                                                                                                                   |
| Gateway IP address                                                                                                                                                               | IP address of the gateway                                                                                            | Make sure the gateway is up and running before proceeding.                                                                                                                                |
| OS root user password                                                                                                                                                            | The Unix root password.                                                                                              | Prime Network uses the root password for machine-level settings and to execute as “root”.                                                                                                 |
| Selecting a single interface for Prime Network backend services.<br><b>Note</b> This prompt appears only if more than one interface is detected during the network-conf process. | The number corresponding with the IP address of the back-end interface to be used for gateway-to-unit communication. | This prompt appears if more than one interface is detected during the network-                                                                                                            |
| Proceeding with installation for unit behind NAT.<br><b>Note</b> This prompt appears if the unit does not have connectivity to the gateway.                                      | yes                                                                                                                  | If the unit is connected to a gateway with IPv4 and IPv6 interfaces (dual stack), a second listener must be added to the unit. See <a href="#">Configuring Dual Listeners, page 7-3</a> . |
| Prime Network administrator username and password                                                                                                                                | username and password                                                                                                | Prime Network internal admin user, used for secure communication with the gateway.                                                                                                        |
| Selecting the unit protection group name                                                                                                                                         | Choose from the listed options.                                                                                      | —                                                                                                                                                                                         |
| Checking if the unit is a standby unit.                                                                                                                                          | no                                                                                                                   | Default is <b>no</b> .                                                                                                                                                                    |
| Unique name for the unit                                                                                                                                                         | Unit name                                                                                                            | —                                                                                                                                                                                         |
| Enabling unit protection.                                                                                                                                                        | yes                                                                                                                  | Default is <b>yes</b> . When this option is enabled, high availability is enabled on the unit.                                                                                            |
| Entering the database interface accessible from the unit.                                                                                                                        | Oracle listener IP                                                                                                   | This appears when the unit's IP version is different from the Oracle listener IP version.                                                                                                 |

- Step 10** When configuring the unit, if the SSH keys are not retrieved automatically within 60 seconds, the following message is displayed: “Connection to *gateway-IP-address* failed. 60 seconds timeout exceeded.” To resolve this issue, verify that the unit can reach port 6081 on the gateway.
- 

## Configuring Dual Listeners

If the unit connects to a gateway with multiple interfaces (dual stack), the installer asks you to specify the interface that should be used. This happens when the gateway has multiple interfaces (dual stack) and the unit is installed with interface type that differs from the interface on which the database is installed. For example, the gateway and database are installed on an IPv4 interface. The gateway also has an IPv6 interface, and the unit only has an IPv6 interface. To add the unit, the database must be configured with dual listeners and an interface that allows the unit to communicate with the database.

### For Embedded Database

To add a listener to an Oracle embedded database installation:

---

- Step 1** As *pnuser*, log into the Prime Network gateway.

- Step 2** Change to the embedded database directory:

```
cd Main/scripts/embedded_db
```

- Step 3** Run the following perl script:

```
add_oracle_listener.pl
```

- Step 4** Answer the script's questions.

```
Is the database installed on a remote server? (yes,no)
```

If you enter **yes**, the following response appears:

```
Provide the new IP Address to be supported by the listener.
```

Enter the database IP address that the new listener should use.

If you enter **no**, the following response appears:

```
The following network interfaces were detected on this host. Please select a single interface to be used by the new listener:
```

Select the address to be added to the listener.

---

### For External Database

To add a listener to an Oracle external database installation:

---

- Step 1** As the Oracle user, log into the Oracle database.

- Step 2** Change to the Oracle home directory:

```
cd $ORACLEHOME/network/admin
```

- Step 3** Add the new address to the listener.ora file.

For example:

```

LISTENER =
 (DESCRIPTION_LIST =
 (DESCRIPTION =
 (ADDRESS = (PROTOCOL = TCP) (HOST = 10.56.22.55) (PORT = 1521))
 (ADDRESS = (PROTOCOL = TCP) (HOST = 2001:420:44ff:b8:221:28ff:fe04:bba7) (PORT = 1521))
)
)
ADR_BASE_LISTENER = /export/home/oracle

```

**Step 4** Stop and then start the listener by executing the following command:

```

lsnrctl stop
lsnrctl start

```



**Note**

In dual-stack gateway installation, redundant units must be of same IP type as the unit. In other words, an IPv4 redundant unit cannot replace an IPv6 unit.

## Post Installation Tasks For Units

The following sections describe post installation tasks to verify the Prime Network unit installation:

- [Verifying the Prime Network Version and the Unit Processes, page 7-4](#)
- [Verifying the Unit Configuration, page 7-5](#)

## Verifying the Prime Network Version and the Unit Processes

The **networkctl status** command verifies that the following unit processes are up and running:

- AVM 0—High availability/switch process
- AVM 25—Event persistence
- AVM 83—Internal use; used as a TFTP server by Change and Configuration Management
- AVM 99—Management process
- AVM 100—Prime Network Event Collector (AEC) process



**Note**

AVM 100 is disabled by default. To enable it, refer to the “Enabling a Single Event Collector on a Gateway or a Unit” section in the [Cisco Prime Network 5.0 Administrator Guide](#).

- secured connectivity daemon

At this point in the installation, no AVMs have been added. When you add AVMs and assign VNEs to them, they appear as *AVM ID*, where *ID* is the number assigned to the AVM.

As a Prime Network user, to check the status of all processes and daemons, enter:

```
networkctl status
```

The output lists all processes. For each AVM process that is checked, the **status** command displays, in brackets, the number of exceptions found in the total number of log file lines for that process. For example, the information for AVM 0 is [OK 0/45]; that is, 0 exceptions in the 45 log file lines that were checked:

```

.-= Welcome to server-name, running Prime Network unit (pn50 (build 347)) =-.

+ Checking for services integrity:
 - Checking if host's time server is up and running [DOWN]
 - Checking if secured connectivity daemon is up and running [OK]
+ Detected AVM99 is up, checking AVMS
 - Checking for AVM103's status [OK 0/857]
 - Checking for AVM83's status [OK 0/45]
 -Checking for AVM101's status [OK 0/857]
 -Checking for AVM0's status [OK 0/57]
 - Checking for AVM100's status [DISABLED]
 - Checking for AVM25's status [OK 0/35]
```

## Verifying the Unit Configuration

Use this procedure to verify that the *golden source* registry was configured correctly on the unit.

- 
- Step 1** On the server, locate and open the `$NETWORKHOME/Main/registry/avm99.xml` file.
- Step 2** Confirm that the file contains an entry for the key *parent*, which is the value of the IP address of the gateway. If it does not contain the entry, rerun the installation.
-







# Installing the Vision, Events, and Administration Clients

There are two methods for installing/launching the clients:

| Client Installation Method    | Description                                                                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Java Web Start technology     | The clients are launched from the gateway by entering a URL in the browser. No manual installation is required, and client upgrades are fully automated. |
| Installation executable files | The clients are manually installed using the executables from the DVD or the gateway server.                                                             |

This chapter covers the following:

- [Launching the Clients From the Web Start Page, page 8-1](#)
- [Installing the Prime Network Clients on Your Computer, page 8-3](#)
- [Troubleshooting Clients, page 8-6](#)



**Note**

The client installation methods in this chapter are only relevant if Prime Network is installed as a standalone product. If you installed Prime Network as part of a suite, see [Configuring the Prime Network, Prime Optical, and Prime Fulfillment Servers as Suite Components](#) in the *Cisco Prime Central Quick Start Guide*.

## Launching the Clients From the Web Start Page

Prime Network enables you to access all its GUI clients from the Web Start page on the gateway. It provides single sign-on (SSO) for all GUI clients. After you enter your credentials, you can access any of the clients.

### Before You Begin

Verify the following:

- All the client requirements are met. For more information on the requirements, see [Prime Network Client Requirements, page 2-12](#).

- Java 8 update 60 is installed on your computer. If not, download it from the Java download site: <http://www.java.com>.



**Note** Prime Network was tested on Java 8 update 60, however it is expected to work with lower Java 8 updates as well.

- Ports 6080 and 6081 are open. For other ports required for Prime Network, see [Required Ports for Prime Network, page 2-25](#).

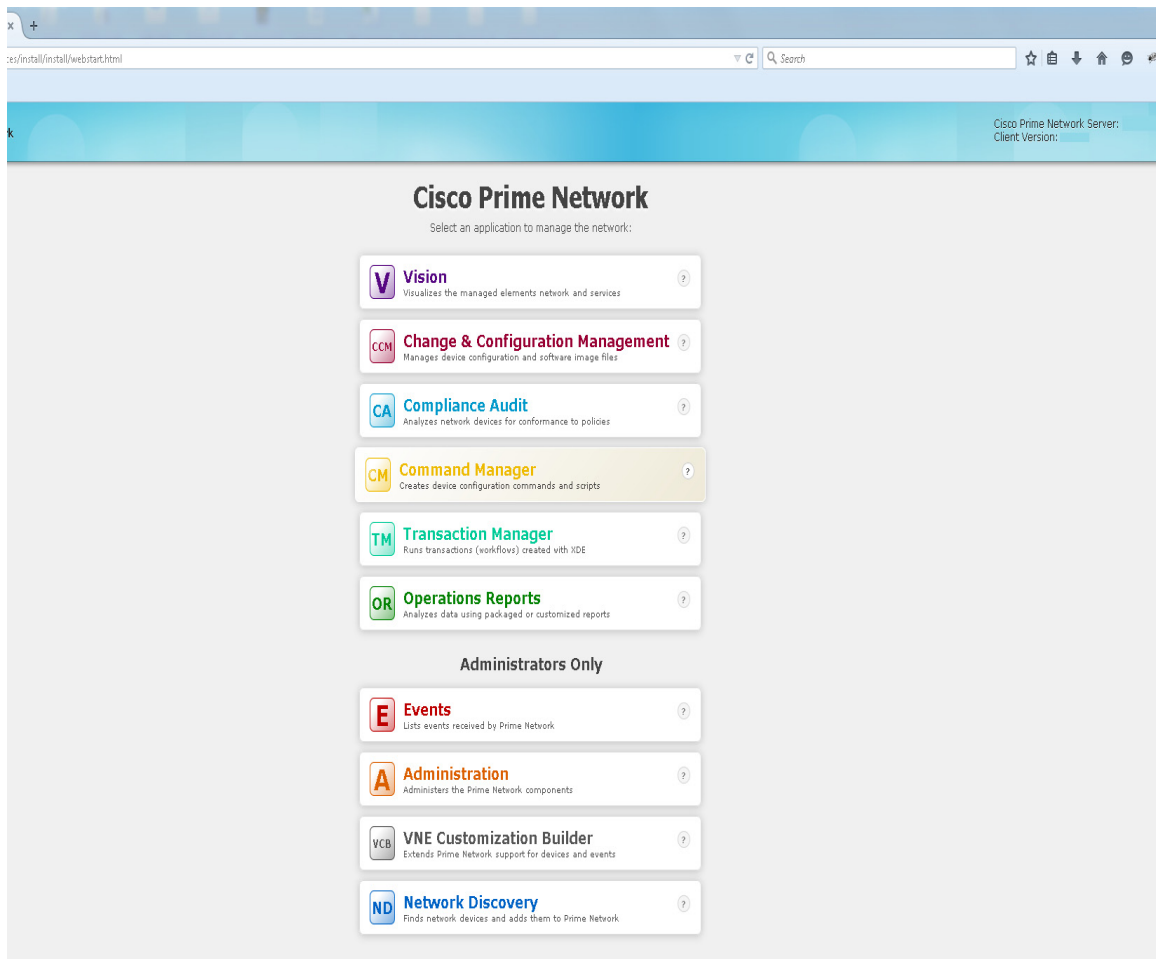
To access the clients using Java Web Start technology:

**Step 1** Log into the gateway by entering:

**`http://gateway-host-ip:6080/ana/services/install/install/webstart.html`**

where *gateway-host-IP* is the gateway host name or IP address.

The Prime Network applications launch page is displayed and provides access to all of the Prime Network GUI clients.



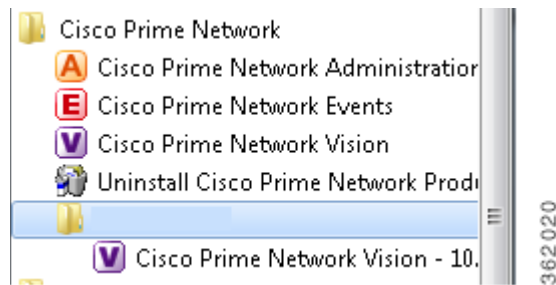
**Step 2** Enter your user name and password in the Prime Network login window and click **Login**.

- Step 3** Click on the Prime Network application you want to access. A .jnlp file is downloaded.
- Step 4** Click **Continue** in the Security Warning screens. The client application jar files are downloaded and the Prime Network application starts.
- Step 5** Enter the gateway username and password, then click **OK**.



**Note** If you want to launch a client from a different gateway, repeat this procedure from the other gateway.

After the first Java Web Start application launch, a shortcut menu is added to the Start menu under the gateway IP address or hostname. Use this shortcut menu to launch the application for subsequent usage.



## Installing the Prime Network Clients on Your Computer

This section provides procedures for installing the Prime Network client from the DVD or by downloading the client executable from the gateway server.

### Before You Begin

Verify the following:

- All the client requirements are met. For more information on the requirements, see [Prime Network Client Requirements, page 2-12](#).
- **Disk 2: Client, Integration Layer, and Documentation** is available. (See [Installation DVDs, page 1-2](#).)
- There is IP connectivity between the gateway and the client workstation that you are about to install.
- Ports 6080 and 6081 are open. For other ports required for Prime Network, see [Required Ports for Prime Network, page 2-17](#).
- Make sure that you do not have any outdated client files.

The client installation wizard guides you step-by-step through the client installation process.

- Step 1** Use either of the following options to begin the client installation:
- Insert **Disk 2: Client, Integration Layer, and Documentation** in the DVD drive. The client installation wizard launches automatically and the Welcome window is displayed.

If the client installation wizard does not launch automatically, browse to the DVD directory and launch the client executable (CiscoPrimeNetwork.exe for 32-bit systems or CiscoPrimeNetwork\_64bit.exe for 64-bit systems).

- Open a web browser and download the client installation executable from the gateway using this URL:

`http://gateway-IP-address:6080/ana/services/install/install/index.html`

where *gateway-IP-address* is the IP address of the gateway.

The system makes a best effort to detect whether your operating system is 32-bit or 64-bit and indicates the recommended download. Click on the relevant link to download the exe file. You can also download Vision, Events, and Admin clients.

**Cisco Prime Network Client Download**  
Download Cisco Prime Network for Windows

Download  
**Prime Network 64-bit**  
Recommended\*

Download  
**Prime Network 32-bit**

You will be able to download these Cisco Prime Network GUI clients:

**V** **Vision**  
Visualizes the managed network elements and services

**E** **Events**  
Lists events received by Prime Network

**A** **Administration**  
Administers the Prime Network components

- \* The recommended download is based on the detection of a 64-bit OS.
- \* Please verify that your computer meets the minimum client requirements as listed in the [Installation Guide](#).
- \* **For Windows 7 only:** We recommend that you do *not* install the Cisco Prime Network GUI clients in the Program Files folder. Only Windows Administrators can run the GUI clients if they are installed in that folder.

- After the download is complete, launch the downloaded file. The client installation wizard launches and the Welcome window is displayed.

**Step 2** Click **Next**. The Destination Location window is displayed. Click **Browse** to change the installation directory, if you do not want to use the default, then click **Next**.

**Note**

The default installation location is C:\Cisco Systems\Prime Network\. If you are installing on Windows 7, do not install the Prime Network clients in the Program Files folder. Only Windows administrators can run the clients if they are installed in that folder.

**Step 3** In the Select Components window, select the clients you want to install (Vision, Events, and/or Administration) and click **Next**.

**Step 4** If you want to change the default Program Manager group, enter your preference and click **Next**.

**Note**

Cisco Prime Network is the default Program Manager group. Cisco Prime Network overwrites any existing icons. If you choose to have multiple client installations, you should add a version number to the Program Manager group; for example, Prime Network 5.0.

**Step 5** Click **Next** to start the installation.

**Step 6** When the installation is complete, choose the options displayed in the final installation window, according to your preference:

- Create “Quick Launch” icons—Create a Quick Launch icon for Prime Network Vision and Cisco Prime Network Administration on the Quick Launch toolbar.
- Launch Cisco Prime Network Vision—Immediately launch Prime Network Vision.

**Step 7** Click **Finish**.

## Installing Prime Network Clients in a Remote Personal Computer

This section provides procedure for installing the Prime Network client in a remote Personal Computer (PC).

**Before You Begin**

- Ensure that the following System requirements are set:
  - Operating System-Windows 10
  - Memory (RAM)-8GB
  - Processor-Intel Core i5 CPU @ 2.30GHz

**Step 1** Connect two Windows 10 machine to the network (local machine and Remote machine).

**Note**

Do not install Prime Network GUI clients in a local machine.

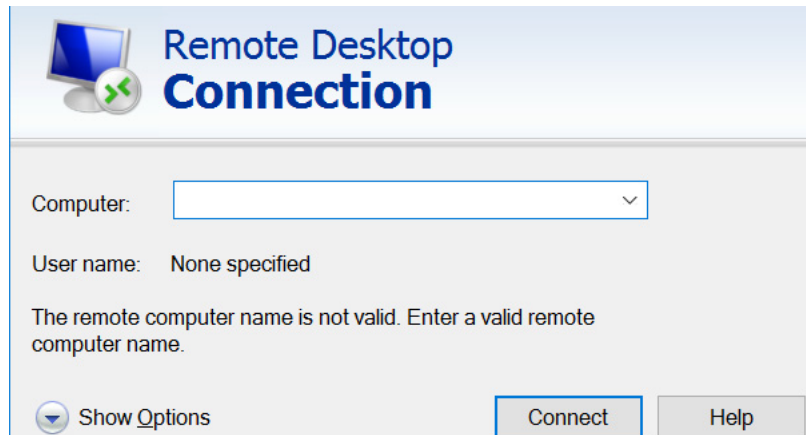
**Step 2** Install Prime Network GUI clients (Administration, Vision, Events and so on) in a remote machine. Make a note of the IP address of the remote machine.

**Step 3** In the Client, open the **Remote Desktop Connection** application.



**Note** Click **Search** for Remote Desktop Connection in Windows 10 and you can see the Application in Search results. Click on it and open that application in Windows 10.

**Figure 8-1 Remote Desktop Connection**



- Step 4** In the **Computer** field, enter the IP address and click **Connect**.
- Step 5** Now, you will be asked to enter credentials of the remote machine. Once you enter correct credentials, you can access the remote machine from local machine.
- Step 6** After accessing the remote machine, launch the Prime Network Administration GUI, Vision GUI client, or Events GUI client.

After the client installation is finished, use Cisco Prime Network Administration to complete the deployment of Cisco Prime Network. For information, see the [Cisco Prime Network 5.0 Administrator Guide](#).

## Troubleshooting Clients

This table explains how to troubleshoot typical client problems and respond to client messages.

| Problem/Message                                                                                                                                                            | Action Required                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Latency problems                                                                                                                                                           | Close any other applications running on the desktop.                                                                                                                                                    |
| Citrix problems                                                                                                                                                            | There may be issues establishing SSL connection or creating a cache folder to the Prime Network client. Follow the instructions in <a href="#">Using Prime Network Clients with Citrix, page 2-14</a> . |
| Message: An automatic upgrade of the Prime Network installer is required to connect to the specified server. The application will restart after the upgrade has completed. | The server and client have different versions of the launcher. Let the automatic upgrade continue.                                                                                                      |

| Problem/Message                                                                                                                                                                                                          | Action Required                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Message: Client not compatible                                                                                                                                                                                           | <p>You are trying to launch a client that is not compatible with the gateway. Install updated clients as described in:</p> <ul style="list-style-type: none"> <li>• <a href="#">Launching the Clients From the Web Start Page, page 8-1</a></li> <li>• <a href="#">Installing the Prime Network Clients on Your Computer, page 8-3</a></li> </ul>                                                                                                                                                                                                                                                      |
| Message: Another Prime Network client accessing a different server is open on your computer. This additional Prime Network client will open using the same installer version as the currently open Prime Network client. | <p>This occurs when another Prime Network application is running and is connected to a different gateway—For example, a client is already connected to <i>gateway1</i> and you are trying to connect to <i>gateway2</i>.</p> <p>Click <b>OK</b>. The client will connect to <i>gateway2</i> but will use the client launcher from <i>gateway</i>. Consequently, the GUI might not match the host code.</p>                                                                                                                                                                                             |
| You cannot open any clients.                                                                                                                                                                                             | <p>If you encounter a problem in opening a Prime Network application, try to regenerate the application files at the Prime Network server by logging in Prime Network gateway and execute the script <b>clientregpacker.sh</b> located at <i>NETWORKHOME/ Main/Scripts</i></p>                                                                                                                                                                                                                                                                                                                         |
| After the execution of <b>ChangePrimeNetworkAndOracleUser.sh</b> script, unable to dis-integrate Prime Network from Prime Central.                                                                                       | <p>This occurs when you change the SSH user name.</p> <p>After the execution of <code>ChangePrimeNetworkAndOracleUser.sh</code> script, follow the re-integration process of the script in the Prime Network-Prime Central setup.</p> <ol style="list-style-type: none"> <li>1. In Prime Network-Prime Central setup before executing <code>ChangePrimeNetworkAndOracleUser.sh</code> script, dis-integrate Prime Network from Prime Central.</li> <li>2. Execute the <code>ChangePrimeNetworkAndOracleUser.sh</code> script.</li> <li>3. Integrate Prime Network with Prime Central again.</li> </ol> |







# Installing the Prime Network Integration Layer

Prime Network can be used with Multi-Technology Operations Systems Interface (MTOSI) and 3rd Generation Partnership Project (3GPP) northbound interfaces. To enable this, you must install the Prime Network Integration Layer (PN-IL) along with the MTOSI and 3GPP bundles.



**Note**

---

The PN-IL must be installed if you intend to use Prime Network in suite mode.

---

The PN-IL server allows Prime Network to expose MTOSI and 3GPP APIs over Simple Object Access Protocol (SOAP). The integration layer exposes MTOSI and 3GPP interfaces to enable clients to register and receive notifications. For information on interfaces exposed by the integration layer for MTOSI and 3GPP, refer to the [Cisco Prime Network OSS Guide](#). An OSS client can use these standard and vendor extension APIs to integrate with Prime Network.

There are two methods for installing the PN-IL—using the GUI wizard (preferred method) or using CLI commands.

The following topics guide you through these PN-IL tasks:

- [Installing the PN-IL Using the Installation Wizard, page 9-2](#)
- [Installing the PN-IL \(CLI Method\), page 9-4](#)
- [Enabling and Disabling the PN-IL Health Monitor, page 9-5](#)
- [Managing FTP for Prime Network Integration Layer Server, page 9-5](#)
- [Changing the Ports Used by the PN-IL, page 9-7](#)



**Note**

---

If the integration layer is installed and you want to upgrade to the current version, refer to the section [Upgrading the Prime Network Integration Layer \(PN-IL\), page 10-22](#).

---

## Prerequisites for Installing the PN-IL

Before you start installing the PN-IL:

- Make sure Prime Network is completely installed.
- Verify that the ports required by PN-IL are available. See the [Prime Network Integration Layer Ports, page 2-29](#). To change the default ports used by PN-IL, see the section [Changing the Ports Used by the PN-IL, page 9-7](#).
- Verify that the system has at least 4 GB of RAM available using the `top` command.

- Verify that the system has minimum of 1 GB free space in the temp directory.
- To use the GUI method (installation wizard), make sure that:
  - An X client application, such as Xming, is installed on the local machine where you plan to launch the wizard.
  - A Telnet/SSH client, such as PuTTY, is installed on the local machine where you plan to launch the wizard, and X11 forwarding is enabled.
  - Max user processes value on the machine is higher than 2048. Check this by executing:
 

```
command ulimit -a
```

## Installing the PN-IL Using the Installation Wizard

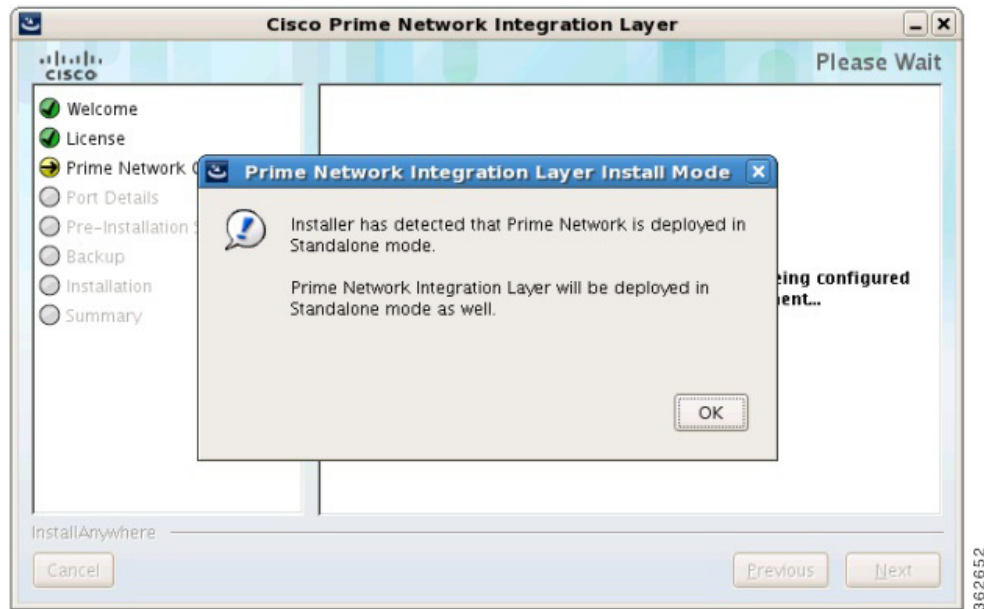
The PN-IL can be quickly and easily installed using the GUI installation wizard.

### Before you Begin

Make sure that all the prerequisites for installing the PN-IL are met. See [Prerequisites for Installing the PN-IL, page 9-1](#).

- 
- Step 1** Launch the X client application (for example, Xming).
- Step 2** As the root user, launch a terminal to the Prime Network gateway server.
- Step 3** Insert **Disk 2: Software and Documentation** in the DVD drive. (See [Installation DVDs, page 1-2](#)).
- Step 4** Mount the inserted DVD using the **mount** command, and move to the mount directory.
- Step 5** In the mount directory, locate the PNIntegrationLayer\_v2.0.0.bin file and run it. This will launch the installation wizard.
- ```
./PNIntegrationLayer_v2.0.0.bin
```
- Step 6** Read the introduction in the Welcome page and click **Next**.
- Step 7** In the License page, accept the terms of the License Agreement and click **Next**.
- Step 8** In the Prime Network Credentials page, provide the following information, then click **Next**.
- Operating System user—The username for the Prime Network operating system that was defined during installation of the Prime Network gateway.
 - Prime Network Root User—The username for the root user that was defined during installation of the Prime Network gateway.
 - Prime Network Root User Password—Password for the root user.
- Step 9** After you have entered the Prime Network credentials, the installation checks the disk space and RAM and identifies whether Prime Network is installed in standalone or suite mode. Click **OK** to proceed with the installation.

Figure 9-1 PN-IL Installation Wizard - Prime Network Credentials



- Step 10** The Port Details page lists the ports used by the PN-IL. Verify that they are available. Click **Next**.
- Step 11** Review the pre-installation summary. If you need to change any of the user inputs, click **Previous**, otherwise click **Install** to continue.
- Step 12** To run 3GPP services in Prime Network, use the following command to enable the NBI script:

```
cd $PRIMEHOME
install/scripts/accessconfig.sh nbi enable
```

- Step 13** Restart the PN-IL:

```
$PRIMEHOME/bin/itgctl restart
```



Note For successful installation of PNIL, karaf process should be running. If the process is not running try *itgctl restart*.

- Step 14** When the installation is complete, click **Done** to close the wizard.
- Step 15** Verify the PN-IL installation by logging into the Prime Network bin directory on the gateway as the Prime Network user (e.g., pn50) and executing this command:

```
cd $PRIMEHOME/bin
itgctl status
```

The integration layer status should be “Restarted”.



Note After the PN-IL installation is complete, a new environmental variable \$PRIMEHOME is created and points to the PN-IL installation directory.

Installing the PN-IL (CLI Method)

Before you Begin

Make sure that all the prerequisites for installing the PN-IL are met. See [Prerequisites for Installing the PN-IL, page 9-1](#).

To install PN-IL:

Step 1 As the root user, open a terminal on the Prime Network gateway server where you want to install PN-IL.

Step 2 Insert **Disk 2: Software and Documentation** in the DVD drive.

Step 3 Mount the inserted DVD using the **mount** command and change to the mount location.

Step 4 Change to the *pnuser*:

```
su - pnuser
```

Step 5 Create an installation directory for PN-IL (pnil in this example).

```
mkdir -p $PRIME_NETWORK_HOME/pnil
```

Step 6 Copy the PN-IL installation tar file from the mount location to this directory.

```
cp /mnt/**/Integration/sil-esb-x.x.x.tar.gz $PRIME_NETWORK_HOME/pnil-directory
```

Step 7 Move to the directory in which the tar file was copied and extract the PN-IL installation tar:

```
cd $PRIME_NETWORK_HOME/pnil-directory
tar -zxvf sil-esb-x.x.x.tar.gz
```

Step 8 Move to the directory in which the installation tar files were extracted and run the installation script:

```
cd sil-esb-x.x.x./install/packages/
./installAndConfigureEsb.sh
```

Step 9 Reload user profile using the following command:

```
source $PRIME_NETWORK_HOME/.cshrc
```

The installation does the following:

- Sets the \$PRIMEHOME variable to the PN-IL home directory.
- Sets up a PN-IL health monitor that checks the PN-IL status every 3 minutes.

Step 10 Configure PN-IL in standalone mode by running the following command as *pnuser*.



Note If you installed Prime Network in suite mode, you must configure PN-IL to run in suite mode after Prime Network has been integrated with Prime Central. Refer to the [Cisco Prime Central Quick Start Guide](#).

Step 11 Go to the path `cd $PRIMEHOME/bin`.

```
itgctl config 1 --anaPtpServer ana_host_ip --anaPtpUser user --anaPtpPw password --authURL
pnetwork-authentication-URL
```

where:

- *user* is the Prime Network root user (usually **root**)
- *password* is the Prime Network root user password

- *pnetwork-authentication-URL* is the URL used to authenticate Prime Network calls; usually `https://localhost:6081/ana/services/username`

Step 12 To run 3GPP services in Prime Network, use the following command to enable the NBI script:

```
cd $PRIMEHOME
install/scripts/accessconfig.sh nbi enable
```

Step 13 Restart the PN-IL:

```
$PRIMEHOME/bin/itgctl restart
```



Note For successful installation of PNIL, karaf process should be running. If the process is not running try *itgctl restart*.

Enabling and Disabling the PN-IL Health Monitor

The PN-IL health monitor checks the PN-IL status every 3 minutes. If the services are down for any reason, the health monitor brings the PN-IL back up.

If you do not want PN-IL to be automatically restarted (such as for a maintenance window), manually disable the health monitor. As *pnuser*, enter the following:

```
$PRIMEHOME/local/scripts/il-watch-dog.sh disable
```

To re-enable the health monitor:

```
$PRIMEHOME/local/scripts/il-watch-dog.sh enable
```



Note

By default, the PN-IL health monitor is disabled.

Managing FTP for Prime Network Integration Layer Server

Each PN-IL FTP server has a primary and a secondary FTP server setup with a failover option or a replication option

- **Failover**—If the primary server is not reachable, files are transferred to the secondary FTP server. If the secondary server is also not reachable, files are copied to the configured directory on the local machine.
- **Replication**—Files are transferred to both the primary and the secondary FTP servers.

The PN-IL directory contains a script (`ftpConfig.sh`) that is available in the PN-IL installation directory. The default location is `$PRIMEHOME/esb/bin`.

Use the `ftpConfig.sh` script with the following options to modify the file transfer component:

```
ftpConfig.sh [-help] [-ftp enable | disable] [-localDir new-location] [-replication enable | disable] [-clearConfig] [-display]
```

Options	Description
-help	View the FTP options for standalone integration layer.
-ftp enable disable	Enables and disables the FTP service.
-localDir <i>new-location</i>	Changes the storage directory that is used on the local machine when file transfer is disabled (the default is /tmp).
-replication enable disable	Enables and disables replication of XML and status files on both primary and secondary FTP servers. To see where files are stored, see Storage Location for PN-IL Replicated Files, page 9-6 .
-clearConfig	Clears the FTP configuration. See Clearing the FTP Configuration for the Standalone Integration Layer Server, page 9-7
-display options	Displays the FTP configurations, with the following <i>options</i> :
im [-hostOption primary secondary]	Displays all servers configured for Inventory Management interface type for 3GPP. Use -hostOption to specify the primary or secondary server.
global	Displays FTP configurations for primary and secondary servers across all management interface type for 3GPP.
all	Displays global FTP configurations

Storage Location for PN-IL Replicated Files

Table 9-1 shows where the files are stored when the replication is enabled/disabled. Tick mark indicates ftp details are configured for the particular FTP server.

Table 9-1 FTP Configuration with Replication Enabled/ Disabled

Primary FTP	Secondary FTP	Replication	Files Stored Under:
✓	X	X	Primary
✓	✓	X	Primary
X	✓	X	Secondary
✓	X	✓	Primary
✓	✓	✓	Primary, Secondary

Clearing the FTP Configuration for the Standalone Integration Layer Server

Use one of these command to clear the configuration depending on the server type:

- Global primary server:

```
./ftpConfig.sh -clearConfig true -hostOption primary -mgmtDataType global
```
- Global secondary server:

```
./ftpConfig.sh -clearConfig true -hostOption secondary -mgmtDataType global
```
- IM primary server:

```
./ftpConfig.sh -clearConfig true -hostOption primary -mgmtDataType im
```
- IM secondary server:

```
./ftpConfig.sh -clearConfig true -hostOption secondary -mgmtDataType im
```

Changing the Ports Used by the PN-IL

This section explains how to change the default ports listed in [Prime Network Integration Layer Ports, page 2-29](#).

**Note**

These procedures stop the PN-IL. If you do not want the health monitor to automatically restart the PN-IL after 3 minutes, disable it as described in [Enabling and Disabling the PN-IL Health Monitor, page 9-5](#).

Changing the NIO and SSL Ports

By default, the NIO and SSL transport ports are 61616 and 61615. To change the port numbers:

-
- Step 1** Edit the `$PRIMEHOME/esb/etc/activemq.broker.cfg` as follows:
 - Change the `nioTransportPort` value to a port number that is not in use, such as 61614.
 - Change the `sslTransportPort` value to a port number that is not in use, such as 61613.
 - Step 2** Edit the `$PRIMEHOME/esb/etc/com.cisco.prime.esb.jms.cfg` file and change the `prime.connection.port` value to the value of `nioTransportPort` from [Step 1](#).
 - Step 3** Save and close the `activemq.broker.cfg` and `com.cisco.prime.esb.jms.cfg` files.
 - Step 4** From the `$PRIMEHOME/bin` directory, stop the integration layer server by invoking `itgctl stop`.
-

Changing the MTOSI Web Services Port

By default, the MTOSI web services implementation port is 9110. To change the port number:

-
- Step 1** Open the `$PRIMEHOME/esb/etc/com.cisco.prime.esb.mtosi.cfg` file and change the **mtosiPort** value to a port number that is not in use.
 - Step 2** Save and close the `com.cisco.prime.esb.mtosi.cfg` file.
 - Step 3** From the `$PRIMEHOME/bin` directory, stop the integration layer server by invoking **itgctl stop**.
-

Changing the 3GPP Web Services Port

By default, the 3GPP web services implementation port is 9220. To change the port number:

-
- Step 1** Open the `$PRIMEHOME/esb/etc/com.cisco.prime.esb.tgpp.cfg` file and change the **tgppPort** value to a port number that is not in use.
 - Step 2** Save and close the `com.cisco.prime.esb.tgpp.cfg` file.
 - Step 3** From the `$PRIMEHOME/bin` directory, stop the integration layer server by invoking **itgctl stop**.
-

Changing the Alarm Web Services Port

By default, the Alarm web services implementation port is 9020. To change the port number:

-
- Step 1** Open the `$PRIMEHOME/esb/etc/com.cisco.prime.esb.alarm.cfg` file and change the **alarmMgmtPort** value to a port number that is not in use.
 - Step 2** Save and close the `com.cisco.prime.esb.alarm.cfg` file.
 - Step 3** From the `$PRIMEHOME/bin` directory, stop the integration layer server by invoking **itgctl stop**.
-

Migrating the PN-IL from Standalone Mode to Suite Mode

If Prime Network was originally installed in standalone mode and was subsequently migrated to work as part of a suite, you need to migrate the PN-IL to suite mode as well. You can do this using the installation wizard.

During the installation, the system automatically detects that the migration to suite mode is required and, after receiving your confirmation, proceeds with the relevant installation and configuration.

To migrate the PN-IL to suite mode:

-
- Step 1** Log in to the Prime Network gateway as the Prime Network user.
 - Step 2** Stop the PN-IL instance and then disable PN-IL Health checker, as follows:

```
$PRIMEHOME/bin/itgctl stop
$PRIMEHOME/local/scripts/il-watch-dog.sh disable
```


- Step 3** Launch the installation wizard and follow Steps 1 through 8 in [Installing the PN-IL Using the Installation Wizard, page 9-2](#).
- Step 4** After you have provided the Prime Network credentials, the system identifies that Prime Network is installed in suite mode. Click **Continue Migration** in the displayed message:

Figure 9-2 Migration to Suite Mode



- Step 5** Click **Next** in the Port Details page.
- Step 6** In the Pre-Installation Summary page, check that the installation mode is Suite Mode Deployment, then click **Install**.
- Step 7** When the installation is complete, click **Done** to close the wizard.



Upgrading and Rolling Back Prime Network

This section covers tasks on how to upgrade from Prime Network 4.2.2, 4.2.3, 4.3, 4.3.1, 4.3.2 to 5.0 or roll back from Prime Network 5.0 to 4.3.2, 4.3.1, 4.3, 4.2.3, or 4.2.2. If you want to upgrade from an earlier version of Prime Network, you must first upgrade to Prime Network 4.0 and then you can upgrade to Prime Network 5.0.

To upgrade 4.0 from earlier versions of Prime Network, refer Prime Network 4.0 DVD contents. For the upgrade procedure, see [Cisco Prime Network 4.0 Installation Guide](#).

This section contains the following topics:

- [Prime Network Upgrade Overview](#), page 10-2
- [Preparing to Upgrade Prime Network \(Pre-Upgrade Checklist\)](#), page 10-4
- [Upgrading to Prime Network 5.0 from 4.3.2, 4.3.1, 4.3, 4.2.3, 4.2.2 \(Intermediate Steps\)](#), page 10-8
- [Upgrading to Prime Network 5.0 and Oracle 12.1.0.2](#), page 10-11
 - [In-line Upgrade of RHEL 6.5, 6.7, 6.8, or 6.9¹ with Prime Network 5.0 and Oracle 12.1.0.2](#), page 10-11
 - [Upgrading from RHEL 5.8 to RHEL 6.x or RHEL 7.2 with Prime Network 5.0 and Oracle 12.1.0.2](#), page 10-12
 - [Upgrading to Prime Network 5.0 in Suite Mode](#), page 10-13
- [Rolling Back to Earlier Prime Network Version](#), page 10-19
- [Upgrading the Prime Network Integration Layer \(PN-IL\)](#), page 10-21
- [Prime Network Post-upgrade Tasks](#), page 10-23
- [Upgrading the Embedded Database to Oracle 12.1.0.2](#), page 10-27
- [Configuring Clusters for Pacemaker and Corosync Setup](#), page 10-16

Prime Network Upgrade Overview

The upgrade procedure backs up the existing user directory and then adds any new Prime Network 5.0 libraries, files, and code to the existing installation. Any changes to the database are made automatically as part of the upgrade. The majority of your customizations and user-defined information remain intact

and available after upgrading. A list of what is migrated is provided in [Table 10-1 on page 10-2](#).

If Operations Reports is installed, it will be upgraded automatically during the upgrade process.

The amount of time required to upgrade Prime Network depends on your deployment size and system performance. During upgrade, the system will be down. Contact your Cisco account representative for an estimated upgrade duration.

[Table 10-1](#) shows the components affected by the Prime Network upgrade and whether those components are upgraded automatically. If they are not updated automatically, the manual procedure you must perform is provided.

Table 10-1 Components Affected by the Prime Network Upgrade

Component	Description	Upgraded Automatically?	Comments
VNE AVMs	avm*.xml files with managed element definitions	Yes	—
Third-party VNE support	Support for non-Cisco VNEs	No	Prime Network supports third-party devices through Cisco Advanced Services engagement. As of release 5.0, Prime Network will not natively support third-party devices, and a Cisco Advanced Services contract will be required for their enablement and support.
Database schema changes	Add, change, or remove database schema tables to meet the Cisco Prime Network 5.0 schema definition	Yes	—
Database data preservation	Migrates the old data representation to the Cisco Prime Network 5.0 representation, where applicable	Yes	All tickets and events are available after upgrading. All other data (such as maps, users, and so on) are preserved and migrated.
Database (general)	—	No	You must retain the same database type after migration. In other words, you cannot upgrade from: <ul style="list-style-type: none"> • A database located on the gateway server to a database located on a remote server (and vice versa) • A customer-provided database to an embedded database.
Users and scopes	—	Yes	All users and scopes are maintained.
Northbound API trap forwarding and SNMP	Out-of-box support for the SNMP trap forwarding mechanism	Yes	The Cisco-EPM-NOTIFICATION-MIB structure includes a running index in the object identifier (OID) suffix, instead of a constant number as in previous releases. The cenAlarmType content was changed in Prime Network 3.8. For more information, contact Cisco Advanced Services.
Northbound API: IMO and BQL	Changes made to information model objects (IMOs)	Yes	Note IMOs might change between versions to support new features. For more information, contact Cisco Advanced services.

Table 10-1 Components Affected by the Prime Network Upgrade (continued)

Component	Description	Upgraded Automatically?	Comments
Customizations: Business objects	—	Yes	Review IMO changes to verify that the OID associated with the business object did not change.
Customizations: Soft properties	Soft properties remain backward compatible and are available in Prime Network 5.0 after upgrading.	Yes	—
Customizations: Command Builder	User-defined commands	Yes	—
Built-in Command Builder scripts	Prime Network built-in activation scripts	Yes	The upgrade procedure updates the built-in changes and removes scripts that are no longer part of the product. See Prime Network Post-upgrade Tasks, page 10-23 to understand which commands require installation after the upgrade.
Customizations: Drools rules	—	Yes	The Post.drl rule is available after upgrading.
Customizations: crontab files	Prime Network crontabs are configured as part of the installation	Yes, if in proper location	If you have user-defined cron jobs, place them in <code>NETWORKHOME/local/cron/crontab.user.list</code> . The upgrade will automatically add the user-defined cron jobs. User-defined cron jobs that are not placed in this directory will be removed. See Prime Network Post-upgrade Tasks, page 10-23 .
Customizations: External launch points	External launch configuration	Yes	Review IMO changes to verify that the OID associated with the launch command did not change.
Customizations: Message of the Day	Message of the Day configuration	Yes	
Registry	—	Yes	New Prime Network 5.0 registry files are available automatically after the upgrade. Customizable registry files, including <code>avm+.xml</code> and <code>site*</code> , are available and upgraded automatically. Review any customized registry configurations in <code>site.xml</code> and <code>avm*.xml</code> to understand whether they are relevant to Prime Network 5.0. Contact your Cisco account representative, if necessary.
<code>pnuser_admin</code> user	User with database administrator permissions who can run maintenance tasks—such as gathering statistics—on the other Prime Network database schemas.	Yes	—

Table 10-1 Components Affected by the Prime Network Upgrade (continued)

Component	Description	Upgraded Automatically?	Comments
Security: SSH and SSL keys	Prime Network SSL keystore and truststore keys, SSH keys, and registry encryption keys	Yes	Prime Network SSL keystore and truststore keys are maintained. These keys are used by all SSL sockets, including BQL and PTP clients. Prime Network SSH keys and registry encryption keys are also maintained.
Prime Network persistency files	Inventory, events, and link persistency data	Yes	All persistency files are available after the upgrade.
Standby units	—	Yes	Standby units complete their upgrade when they are restarted by the gateway (when an active unit goes down and the standby unit is brought online).
GUI client	—	No	If you had an installed client, you need to reinstall it after upgrade. If you access the clients via Web Start, no action is required.
Network Service Activation (NSA)	—	No	Cisco Prime Network Activation functionality is no longer available in Prime Network 5.0. Transaction Manager replaces the Prime Network Workflow and Activation features that were available in previous releases. For details on setting up Transaction Manager, see Setting Up Transaction Manager, page 12-5 . For information on how to use Transaction Manager, see the <i>Cisco Prime Network 5.0 Customization Guide</i> .
Change and Configuration Management	Software image and device configuration files	Yes	All the software and device configuration changes are retained as part of the upgrade.
High availability configuration	Upgrades for RHCS/Oracle Active Data Guard gateway high availability	No	If you have gateway high availability, move the Prime Network and Oracle services to maintenance mode before you run the upgrade, then move them back to normal mode after it.
Operations Reports	User-defined reports	Yes	All user defined reports created prior to the upgrade will be available post-upgrade. Note Operations Reports are only available to customers with Operations Reports license prior to May 2018. For re-installation of Operations Reports contact a Cisco customer support representative.

Preparing to Upgrade Prime Network (Pre-Upgrade Checklist)

Table 10-2 shows the pre-upgrade tasks that must be performed before upgrading to Prime Network 5.0.

Table 10-2 Gateway Pre-Upgrade Tasks

	Task	Referred Topic/Action Required
Step 1	If you are managing third-party devices, make note of them. You will need to give this information to your Cisco representative to enable the support after the upgrade.	Prime Network supports third-party devices through Cisco Advanced Services engagement. As of release 5.0, Prime Network will not natively support third-party devices, and a Cisco Advanced Services contract will be required for their enablement and support.
Step 2	Insert Disk 3: Upgrade Files into the DVD drive.	Copy these files from the DVD to the temporary upgrade directory you created: <ul style="list-style-type: none"> • ivne-drivers.tar file • Prime_Network_upgrade directory and its dependent contents
Step 3	Insert Disk 4: Database Binaries into the DVD drive.	
Step 4	Familiarize yourself with the upgrade process and identify areas that may require manual changes.	Components affected by upgrade are listed in Table 10-1 .
Step 5	<p>Back up your database and files stored on the gateway.</p> <p>Note You will need this data in case you perform a rollback.</p> <p>You can use the script <code>nccmjobstore.csh</code> from the installation DVD to obtain the scheduled job information in CSV or HTML format.</p>	<p>External database:</p> <ul style="list-style-type: none"> • Back up your gateway data by logging into the gateway and running this command from <code>NETWORKHOME/Main/scripts</code>: <code>backup.pl backup-folder</code> • Back up the Oracle database using your Oracle documentation. <p><i>Embedded database:</i></p> <ol style="list-style-type: none"> Log in to the gateway as <code>pnuser</code>. Change to the embedded database directory: <code># cd \$PRIME_NETWORK_HOME/Main/scripts/embedded_db</code> Execute the backup script: <code># emdbctl --backup</code> <p>For information on <code>emdbctl</code> utility used in the above procedure, refer to the Cisco Prime Network 5.0 Administrator Guide.</p>
Step 6	Apply the database configurations and recommendations.	Preparing the Oracle External Database, page 4-1
Step 7	Verify that the server machines comply with the system hardware and software requirements.	Installation Requirements, page 2-1 Gateway: CPU and Memory Requirements for Different Network Sizes, page 2-3
Step 8	Verify that the backup directory has at least 6000 MB of free space for <code>pnuser</code> .	Example: <code>df -k /backup_dir</code>
Step 9	Verify that the database has at least 8 GB of RAM available (the minimum requirement).	For the database storage sizing guidelines, contact your Cisco account representative.
Step 10	Verify that all required ports are free.	Required Ports for Prime Network, page 2-25 .

Table 10-2 Gateway Pre-Upgrade Tasks (continued)

	Task	Referred Topic/Action Required
Step 11	Make sure all database sessions (such as TOAD, SQL, and so on) are closed.	Other TOAD/SQL sessions apart from Prime Network established session should be closed.
Step 12	Place any customized crontab files in <i>NETWORKHOME</i> /local/cron/crontab.user.list. User-defined cron jobs that are not placed in this directory will be removed.	—
Step 13	(External database only) Restart Prime Network and the Oracle database.	<ol style="list-style-type: none"> As <i>pnuser</i>, stop Prime Network: <code>networkctl stop</code> As <i>oracle user</i>, stop and restart Oracle: <code>sqlplus</code> <code>shutdown immediate</code> <code>startup</code> As <i>pnuser</i>, restart Prime Network: <code>networkctl start</code>
Step 14	Verify that the gateway and units are powered up and connected by opening an SSH session between gateway and all units.	—
Step 15	Verify that Oracle and the Oracle listener are running.	Starting the Oracle Listener (External Database), page 3-7
Step 16	Drop the TMP_BIG_TICKET2 table if it is already created.	<p>Prior to Prime Network 5.0 upgrade, run the below query in Data base (DB):</p> <ol style="list-style-type: none"> Log in to the Prime Network DB and do the following: <ol style="list-style-type: none"> As <i>pnuser</i>, execute <code>sqlplus <PN Username>/<PN User Password>@[<Gateway IP>]:1521/<SID></code> Example: <code>sqlplus</code> <code>pn43/Admin123#[10.76.80.19]:1521/mcdb</code> <p>Note mcdb - SID is the value that is set for environment variable ORACLE_SID)</p> <ol style="list-style-type: none"> Execute the below query: <pre> BEGIN EXECUTE IMMEDIATE 'DROP TABLE TMP_BIG_TICKET2'; EXCEPTION WHEN OTHERS THEN IF SQLCODE != -942 THEN RAISE; END IF; END; / </pre>

Table 10-2 Gateway Pre-Upgrade Tasks (continued)

	Task	Referred Topic/Action Required
Step 17	(Only for NAT units) Stop the Prime Network application and remove the current crontab.	Enter the following commands on each of the NAT units: <pre>networkctl stop; crontab -r;</pre> <p>Note To restart the crontab later, see Restarting Crontab Jobs for NAT Units, page 10-24.</p>
Step 18	(Local and geographic gateway high availability) Verify that the gateways and units with Red Hat installed have rsync 3.0.6 or newer.	Verify the rsync version installed on the gateway/units using the command: <pre>[root@primebgl01-lnx ~]# rpm -qa rsync rsync-3.0.6-9.el6_4.1.x86_64 [root@primebgl01-lnx ~]#</pre>
Step 19	If using an external database, verify your database settings. Note Prime Network 5.0 requires the Oracle JVM and partitioning options.	See Chapter 4, “Preparing the Oracle External Database”

Supported Prime Network Upgrade and Rolling back versions

Refer the following table for supported Prime Network Upgrade and rolling back versions.

Table 10-3 Supported Prime Network Upgrade and Rolling back versions

Upgrade from	Upgrade to	Rollback to
PN 3.x -> 4.0	4.3 -> 5.0	4.3
PN 4.0	4.3 -> 5.0	4.3
PN 4.1	4.3 -> 5.0	4.3
PN 4.2	4.3 -> 5.0	4.3
PN 4.2.1	4.3 -> 5.0	4.3
PN 4.2.2	5.0	4.2.2
PN 4.2.3	5.0	4.2.3
PN 4.3	5.0	4.3
PN 4.3.1	5.0	4.3.1
PN 4.3.2	5.0	4.3.2

Upgrading to Prime Network 5.0 from 4.3.2, 4.3.1, 4.3, 4.2.3, 4.2.2 (Intermediate Steps)



Note

The steps provided below are intermediate steps that are to be followed while [Upgrading to Prime Network 5.0 and Oracle 12.1.0.2, page 10-11](#) from Prime Network 4.1 with RHEL 6.4 or other lower versions of Prime Network with RHEL 5.5-5.8.

If you are upgrading from lower versions of Prime Network / RHEL to Prime Network 5.0 / RHEL 7.2, it is mandatory to use Oracle 12.1.0.2 release version.

If you are using earlier versions of RHEL 6.5, 6.7, 6.8 during the upgrade of Prime Network 5.0, it is highly recommended to use Oracle 12.1.0.2 version. In case, if you want to use 12.1.0.1 Oracle version, then upgrade only Prime Network, do not upgrade the Oracle.

Use the procedure described in this section to upgrade from Prime Network 4,3,2, 4.3.1, 4.3, 4.2.3, or 4.2.2, to Prime Network 5.0.



Caution

Do *not* apply any service patches during any phase of the upgrade to Prime Network 5.0. Apply them after the upgrade is completed.

Before You Begin

Before you begin the upgrade, perform the pre-upgrade tasks in [Preparing to Upgrade Prime Network \(Pre-Upgrade Checklist\), page 10-4](#).



Note

While upgrading Prime Network in a HA setup, you should always start the upgrade from the Primary gateway as active gateway. The active gateway should not be the secondary gateway when starting the upgrade process

To upgrade the Prime Network gateway:

Step 1 Create a temporary upgrade directory on the gateway.



Note

Make sure that upgrade directory is not a subdirectory of \$PRIME_NETWORK_HOME (which is `/export/home/pnuser` by default).

Step 2 Insert **Disk 3: Upgrade Files** into the DVD drive.

Step 3 Copy these files from the DVD to the temporary upgrade directory you created:

- `ivne-drivers.tar` file
- `Prime_Network_upgrade` directory and its dependent contents

Step 4 Give the `Prime_Network_upgrade` directory and its contents `pnuser:pngroup` owner permissions:

```
chown -R pnuser:pngroup Prime_Network_upgrade
```

Step 5 To verify the group name, run the following command as `pnuser`: `id --group --name`

Step 6 As `pnuser`, move to the following location in your temporary upgrade directory:

```
cd Prime_Network_upgrade
```

Step 7 If you have not upgraded from fresh install of Prime Network **4.3.2, 4.3.1, 4.3, 4.2.3, or 4.2.2 to Prime Network 5.0**, as Prime Network user, run *status* command to check if Compliance Manager is UP, if not, run:

```
cmctl start
```

```
For example, pn50@imeir-pn50-01 [~]% cmctl status
Up
```

Step 8 Start the upgrade:

```
perl upgrade.pl
```



Note Compliance server should be up and running for performing the upgrading process.



Note While exporting custom policies, if you are prompted with the following message, **Export failed, Do you want to continue (YES/NO)**, then you can follow the below conditions based on your requirements: Choose **NO** to stop the upgrading process and exit, or **YES** to continue. When you choose YES, the following message appears: **Warning ! All the custom policies has been wiped out, Do you want to continue (YES/NO)**. Choose **NO** to stop the upgrading process and exit, or **YES** to continue the upgrade process.

Step 9 Enter the required information as shown in the following table.

Prompt for...	Enter...	Notes
Password for OS root user	Operating system root password	Linux root password In a high availability environment, you will be required to enter the OS root user for each machine in the setup.
Verifying whether you have completed database backup	yes	This prompt is to check whether you have recently completed database backup. Default is yes . If you enter no , the upgrade process will stop and will ask you to back up the database. For information on backing up your database, see Step 5 in the pre-upgrade checklist.
Destination location for backing up the existing installation tar file	<i>directory</i>	Specify a directory with at least 6000 MB of free space. Verify that the backup directory is available for <i>pnuser</i> . The backup directory needs write permission. Enter the following command to add write permission to the backup directory: chmod 777 <directory>
Disabling Configuration Audit	yes	Configuration Audit is deprecated and replaced by Compliance Audit. If you still want to use Configuration Audit, enter no and it will remain available from Change and Configuration Management.
Path to the ivne-drivers.tar file	<i>full pathname</i>	Provide the full pathname to the temporary upgrade location from Step 1 .
Prime Network root password	root password	The root password used to log into the Prime Network GUI applications.

Step 10 After the upgrade is complete, Prime Network restarts. Log in as *pnuser* for the environment changes to take effect.

**Note**

While importing the custom policies, if the number of custom policies exported is zero, then the importing process is skipped with a message **No Custom Policies to import**. If the custom policies exported is not zero and if the compliance server is up, then the importing process begins. If the compliance server is not up within 30 seconds, the following message is prompted to the user:
Failed : Run <PN_Home>/utils/independent/compliance/bin/importPolicies.sh manually

Step 11 If any of the preceding steps fail, the following error message is shown:

```
Failed to execute hook-type for hook-name. See log for further details.
- Hook hook-name terminated with failure
- Please choose one of the following:
1. Abort the upgrade process
2. Re-run the hook
```

In the error message, *hook-type* and *hook-name* are the type and name of the procedure that failed.

- Check the upgrade log (*NETWORKHOME/Main/upgrade-timestamp.log*) to identify the reason for the failure.
- If you can identify the problem and fix it manually, do so; then, choose option **2** to rerun the hook. The upgrade procedure continues from the procedure that failed.
- If you cannot fix the problem, choose option **1** to cancel the upgrade. After canceling the upgrade, Prime Network cannot be started. Contact your Cisco account representative to fix the problem; then, rerun the upgrade. The upgrade procedure continues from the procedure that failed.

**Note**

If you decide not to rerun the upgrade, you must roll back to your base Prime Network environment, including rolling back the database. See [Rolling Back to Earlier Prime Network Version, page 10-19](#).

Step 12 If you upgraded a gateway configured with local high availability, take the ana and oracle_db services out of maintenance mode:

```
clusvcadm -U ana
clusvcadm -U oracle_db
```

Step 13 Clear the web browser cache.

Step 14 Perform the necessary tasks listed in [Prime Network Post-upgrade Tasks, page 10-23](#).

**Note**

To remove previous device package reference errors in avm file: 11.out, execute the following command as a Prime Network user: **networkctl restart -avm 11**.

After the upgrade of Prime Network, you can implement SNMPv2 protocol on all devices. Follow the below steps to run the script:

- Navigate to '*<PNHome>/local/scripts*' directory in the GateWay (GW).
- Run the script as *pnuser* from the GW.

**Note**

To run script, Prime Network should be down in both GW and Units. This condition is applicable for all VNEs and not applicable to a specific VNE.

- Run the script file using the below command.GW.

```
perl updateSNMPver.pl <currentSnmpver> <newSnmpVer>
```

```
Ex1: perl updateSNMPver.pl v2 v2only
```

```
Ex2: perl updateSNMPver.pl v1 v2only
```



Note Valid SnmpVer parameters for the above script are v1,v2,v2 only and the parameters are case sensitive. The log files are available in the following path; '<PNHome>/SnmpVerchange_logs' in the GW.

4. Start the Prime Network to reflect the changes.

Upgrading to Prime Network 5.0 and Oracle 12.1.0.2

In-line Upgrade of RHEL 6.5, 6.7, 6.8, or 6.9¹ with Prime Network 5.0 and Oracle 12.1.0.2

To perform the in-line upgrade of RHEL 6.5, 6.7, 6.8, or 6.9 with Prime Network 5.0 and Oracle 12.1.0.2, follow the procedure provided below:

- Step 1** Upgrade to Prime Network 5.0 using **Prime_Network_upgrade** directory from Disk 3 to the temporary upgrade directory you created. See [Upgrading to Prime Network 5.0 from 4.3.2, 4.3.1, 4.3, 4.2.3, 4.2.2 \(Intermediate Steps\)](#), page 10-8.
- Step 2** Upgrade embedded Oracle 12 using the **embedded_upgrade_12.1.zip** file from Disk 3. See [Upgrading the Embedded Database to Oracle 12.1.0.2](#), page 10-27.
- Step 3** To perform the in-line upgrade from 6.x to 6.5, 6.7, 6.8 with latest Open ssl package, contact your System Admin for RHEL in-line upgrade.



Note In Prime Network 5.0, In-line upgrade is supported from RHEL 6.8 to RHEL 6.9. For support on fresh RHEL 6.9 installation with Prime Network 5.0, contact the account manager and the Advance Services representative.

- Step 4** After upgrading the RHEL, login with *pnuser* and verify the web server status and the compliance engine status.
- Step 5** Login as *pnuser* and restart AVM11 using **\$ANA_HOME# anactl restart -avm 11**.



Note If you have Unit server attached with Gateway, first upgrade the Gateway as mentioned in the above steps and then upgrade the unit server.

1. *RHEL 6.9 is supported when upgraded from RHEL 6.8.

Upgrading from RHEL 5.8 to RHEL 6.x or RHEL 7.2 with Prime Network 5.0 and Oracle 12.1.0.2

To perform a major upgrade from RHEL5.8 to 6.x, or 7.2 with Prime Network 5.0, backup the database and Prime Network, and save it to any other local machine. After which, you need to re-image the system with RHEL 6.x or 7.2, fresh install the Prime Network 5.0 and restore the previous data backup from the location where you saved it.



Note

If you have RHEL 5.8 and do not wish to re-image to RHEL 6.x or 7.2, you can continue to upgrade PN 5.0 with RHEL 5.8

To upgrade the RHEL, follow the below steps:

- Step 1** Note down the *pnuser* name and Password, and Oracle username and Database profile that you had selected while installing Prime Network lower version.
- Step 2** Upgrade to Prime Network 5.0 from Prime Network lower version using **Prime_Network_upgrade** directory from Disk 3. See [Upgrading to Prime Network 5.0 from 4.3.2, 4.3.1, 4.3, 4.2.3, 4.2.2 \(Intermediate Steps\)](#), page 10-8.
- Step 3** Upgrade embedded Oracle 12 using the **embedded_upgrade_12.1.zip** file. See [Upgrading the Embedded Database to Oracle 12.1.0.2](#), page 10-27.
- Step 4** Login as Prime user and Backup the Embedded oracle database **\$PNHOME/Main/scripts/embedded_db# emdbctl --backup**. Please refer the [Cisco Prime Network 5.0 Administration Guide](#) for knowing how to back up the Gateway data and the Embedded Database.



Note

If you have operations reports in Gateway, Uninstall it before performing PN Database backup.

- Step 5** Copy the latest backup folder in **\$ANA_HOME/backup#** to your local server (for example, other than the server you are currently using).
- Step 6** Re-image the Gateway server to RHEL 6.5 or RHEL 6.7 or 6.8 or RHEL 7.2. If you have a Unit server attached in the Gateway, re-image the Unit server to RHEL6.5 or RHEL 6.7 or 6.8 or 7.2.



Note

After you complete the re-imaging of the Gateway server to RHEL 6.x or 7.2, ensure to restore the backup data.

- Step 7** Install the Prime Network 5.0 Gateway, Oracle 12.1.0.2 and the Unit server. If you have unit Gateway setup in Prime Network lower version, use the *pnuser* name and Password, and Oracle username and Database profile that you had chosen while installing Prime Network Gateway lower version.



Note

If you have installed the embedded Oracle in remote server for Prime Network lower version, install embedded database 12.1.0.2 on the same server for Prime Network 5.0.

- Step 8** Once installation is complete, login as a Prime user, back up the Prime network Gateway data and embedded database **\$PNHOME/Main/scripts/embedded_db # emdbctl --backup**. Please refer [Prime Network 5.0 Administrator guide](#) to know more on how to back up the Gateway data and the embedded database.

- Step 9** Navigate to `$ANA_HOME/backup` location, and remove the back up file folder in the location.
- Step 10** Paste the backup file folder which you already have in your local machine to the location `$ANA_HOME/backup`.
- Step 11** Provide the group owner permissions to the backup file directory and its contents as follows:
- ```
chown -R pnuser: pngroup.
Example: chown -R pn50:ana
```
- Step 12** Login as Prime user and restore the embedded database with Prime network gateway data by using the command `$PNHOME/Main/scripts/embedded_db # emdbctl --restore`. Please refer [Prime Network 5.0 Administration guide](#) to know more on how to restore the gateway data and the embedded database.
- Step 13** Once the restoring process is completed, check the status of Prime Network.
- Step 14** Ensure that the status of both compliance engine and web server is up.
- Step 15** Start the Unit server as a Prime user using the command `$ANA_HOME# anactl start`, if it is attached with the Gateway.
- Step 16** Restart the Prime Network as Prime user using the command `$ANA_HOME# anactl restart`.
- 

## Upgrading to Prime Network 5.0 in Suite Mode

To upgrade to Prime Network 5.0 in suite mode, follow the procedure provided below:

- Step 1** Follow the upgrade procedures described below:
- [Upgrading to Prime Network 5.0 from 4.3.2, 4.3.1, 4.3, 4.2.3, 4.2.2 \(Intermediate Steps\), page 10-8](#)
  - [In-line Upgrade of RHEL 6.5, 6.7, 6.8, or 6.9<sup>1</sup> with Prime Network 5.0 and Oracle 12.1.0.2, page 10-11](#)
  - [Upgrading from RHEL 5.8 to RHEL 6.x or RHEL 7.2 with Prime Network 5.0 and Oracle 12.1.0.2, page 10-12](#)
- Step 2** Integrate Prime Network in suite mode with Prime Central 2.0. Refer to the Integrating Prime Network with Prime Central topic of the [Cisco Prime Central Quick Start Guide](#).
- Step 3** Upgrade to Prime Network Integration Layer 2.0.0 from PN-IL earlier release. Refer to the [Appendix 10, “Upgrading PN-IL in Standalone Mode”](#) topic of the Cisco Prime Network 5.0 Installation Guide
- Step 4** Integrate Prime Network Integration Layer 2.0.0 in suite mode with Prime Central 2.0. Refer to the Integrating the Prime Network Integration Layer with Prime Central topic of the [Cisco Prime Central Quick Start Guide](#).
- 

## Upgrading or Downgrading OS in HA Environment

You can upgrade or downgrade RHEL version on the local cluster and install HA on all VMs. For example, you can install VM1 and VM2 in a local cluster and VM3 as Geo/DR in a Local with Geographical setup or Install VM1 in a local cluster and VM3 as Geo/DR in a Geo only setup. VM1 is considered as Local or Primary VM, VM2 as secondary local cluster VM where both Prime Network and oracle services not running, and VM3 as standby and distant Geo/DR.

## Upgrade of OS in HA Environment

To perform the upgrade, follow the steps:

- Step 1** Install HA on a Local cluster VM with Geographical setup or Geographical only setup that has RHEL5.8 or 6.x on all VMs.
- Step 2** Shutdown the Primary VM (VM1) in case of both Local+HA local clusters without loss of generality.
- Step 3** Execute the following script on the StandBy VM (VM3):

```
#perl primeha-fail
```



**Note** After execution, VM3 will be your new Primary, and either VM1 or VM2 will be your new Geo/DR.

- Step 4** Upgrade the RHEL from 5.8 to 6.x or 7.2 on the local cluster.

-or-

Upgrade the RHEL from 6.x to 7.2 on the local cluster.

Complete the below steps:

- a. Take the backup of Prime Network, re-image the server with RHEL 6.x or RHEL7.2, install the Prime Network 5.0, and then restore the Prime Network backup.
- b. In case, if you are re-imaging the server with RHEL 7.2, ensure to configure the cluster with Pacemaker. For more information, see [Configuring Clusters for Pacemaker and Corosync Setup](#).



**Note** In Prime Network 5.0, in-line upgrade is supported from RHEL 6.8 to RHEL 6.9. For support on new RHEL 6.9 installation with Prime Network 5.0, contact the account manager and the Advance Services representative.

- Step 5** Setup VM cluster (VM1 or VM2) for HA installation as shown below:
- a. Create */etc/hosts* file
  - b. Set permissions for both */tmp* and */etc/shadow*
  - c. Mount build locations
  - d. Mount again various 4 disk partitions without loss of generality on the primary VM as shown below:
    - *mount/dev/sdb1/export1/ana-home/ana*
    - *mount/dev/sdb2/ora/opt/ora1*
    - *mount/dev/sdb3/directio*
    - *mount/dev/sdb4/datafiles/dbf*

- Step 6** Log in to the Primary VM (VM1) without loss of generality, and then navigate to */tmp path* to unzip RH\_ha.zip.



**Note** Your new Geo/DR VM will be the new DR.

- Step 7** Navigate to */tmp/RH\_ha* path and then execute the following script on VM1:



```
#"perl resumeFromFailOver.pl -- reinstall_setup" from /tmp/RH_ha on the primary VM
```



**Note** When the script fails, do the following:

- Add `OVERRIDE_SWAP=true` to the file `/tmp/RH_ha/auto_install_RH.ini`
- Execute `perl install_Prime_HA.pl-autoconf auto_install_RH.ini`

- Step 8** Execute `perl resumeFromFailOver.pl --reconfigure_setup` also on the primary VM1.
- Step 9** Log in to standby VM (VM3) and navigate to `/tmp/RH_ha` path.
- Step 10** Execute `"perl resumeFromFailOver.pl --setup_replication"` on the standby VM (VM3).
- Step 11** To upgrade OS on your new primary VM(VM3) to RHEL 6.5 or 6.7 or 6.8 or 7.2, repeat steps 2 through 10.
- Shutdown VM3 and execute `perl primeha -fail` script on Local VM (VM1).
  - Upgrade OS on VM3 to RHEL 6.5 or 6.7 or 6.8 or 7.2.



**Note** In Prime Network 5.0, in-line upgrade is supported from RHEL 6.8 to RHEL 6.9. For support on new RHEL 6.9 installation with Prime Network 5.0, contact the account manager and the Advance Services representative.

- Setup VM3 to install HA If VM3
- Execute the scripts `perl resumeFromFailOver.pl --reinstall_setup` and `perl resumeFromFailOver.pl --reconfigure_setup` on VM3
- Execute `perl resumeFromFailOver.pl --setup_replication` on VM1.

## Downgrade OS in HA Environment

To perform the downgrade follow the steps:

- Step 1** Install HA on a Local cluster VM with Geographical setup or Geographical only setup that has RHEL 6.5, 6.7, 6.8 or 7.2 on all VMs.
- Step 2** Shutdown the Primary VM without loss of generality in case of both Local +HA clusters.
- Step 3** Execute the following script on the StandBy VM (VM3):

```
#perl primeha-fail
```



**Note** After execution, VM3 will be your new Primary, and either VM1 or VM2 will be your new Geo/DR.

- Step 4** Downgrade the RHEL from 7.2 to 6.x on the local cluster.



**Note** Downgrade to RHEL 5.8 is not supported.

- Step 5** Setup VM cluster for the HA installation as shown below:
- Create `/etc/hosts` file

- b. Set permissions for both */tmp* and */etc/shadow*
- c. Mount build locations
- d. Mount again various 4 disk partitions without loss of generality on the primary VM as shown below:
  - *mount/dev/sdb1/export1/ana-home/ana*
  - *mount/dev/sdb2/ora/opt/ora1*
  - *mount/dev/sdb3/directio*
  - *mount/dev/sdb4/datafiles/dbf*

**Step 6** Log in to the Primary VM without loss of generality, and then navigate to */tmp path* to unzip *RH\_ha.zip*.




---

**Note** Your new Geo/DR VM will be the new DR.

---

**Step 7** Navigate to */tmp/RH\_ha* path and then execute the following script:

```
#"perl resumeFromFailOver.pl -- reinstall_setup" from /tmp/RH_ha on the primary VM
```




---

**Note** When the script fails, do the following:

- a. Add *OVERRIDE\_SWAP=true* to the file */tmp/RH\_ha/rf\_auto\_install\_RH.ini*
- b. Execute *perl install\_Prime\_HA.pl-autoconf rf\_auto\_install\_RH.in*

---

**Step 8** Execute *perl resumeFromFailOver.pl --reconfigure\_setup* also on the primary VM.

**Step 9** Log in to standby VM and navigate to */tmp/RH\_ha* path.

**Step 10** Execute *perl resumeFromFailOver.pl--setup\_replication* on the standby VM.

**Step 11** To downgrade OS on your new primary VM to RHEL6.x, repeat steps 2 through 10.

- a. Shutdown VM3 and execute *perl primeha -fail* script on Local VM (VM1)
  - b. Downgrade OS on VM3 to RHEL 6.x
  - c. Setup VM3 to install HA
  - d. Execute the scripts *perl resumeFromFailOver.pl --reinstall\_setup* and *perl resumeFromFailOver.pl --reconfigure\_setup* on VM3
  - e. Execute *perl resumeFromFailOver.pl --setup\_replication* on VM1.
- 

## Configuring Clusters for Pacemaker and Corosync Setup

From RHEL7.2 onwards Pacemaker is the default cluster resource manager. Pacemaker provides maximum availability for your cluster services and resources by detecting and recovering node and resource-level failures. It uses messaging and membership capabilities provided by Corosync to keep the resource availability on any of the cluster nodes.

Corosync is the open source cluster engine that manages cluster interconnect and maintains the same cluster configuration across all the cluster nodes. All the configuration changes will be replicated to other node using corosync cluster engine. Pacemaker and Corosync are powerful open source technologies that completely replaces the CMAN and RGManager technologies from previous Redhat cluster releases.

Use the following procedure to configure clusters:

**Step 1** Install the required packages for Pacemaker on both nodes.

```
yum-config-manager --enable rhel-7-server-optional-rpms
yum install pcs fence-agents-all
yum install lvm2-cluster gfs2-utils
yum install nfs-utils rpcbind
yum install pacemaker pcs
```

**Step 2** (Optional) Verify Pacemaker /Corosync /pcs is available or not-`a | grep pacemaker`.

```
rpm -q -a | grep corosync
rpm -q -a | grep pcs
```

**Step 3** Stop the firewalld services and Network Manager on both nodes.

```
systemctl disable firewalld.service
systemctl stop firewalld.service
systemctl stop NetworkManager.service
```

**Step 4** Disable selinux on both nodes.

```
update SELINUX=enforcing ? permissive
[root@pn50-qa-ha-01 /]# setenforce 0
[root@pn50-qa-ha-01 /]# getenforce
permissive
OR
Configure SELINUX=disabled in the /etc/selinux/config file:
vi /etc/selinux/config
```

**Step 5** (Optional) Verify Hostnames on both nodes.

```
[root@pn50-qa2-ha-01 /]# cat /etc/hostname
pn50-qa2-ha-01
```

```
[root@pn50-qa2-ha-02 /]# cat /etc/hostname
pn50-qa2-ha-02
```

**Step 6** (Optional) Verify system configurations.

```
cat /etc/sysconfig/network-scripts/ifcfg-ens192
```

**Step 7** Add Hostnames, IP addresses and Virtual IPs on both nodes (Vi /etc/hosts)

```
[root@pn50-qa2-ha-01 /]# vi /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
```

```
10.56.57.204 pn50-qa2-ha-01 pn50-qa2-ha-01.cisco.com
10.56.57.205 pn50-qa2-ha-02 pn50-qa2-ha-02.cisco.com
10.56.57.212 ana-cluster-ana
10.56.57.211 ana-cluster-oracle
```

```
[root@pn50-qa2-ha-02 /]# vi /etc/hosts
```

**Step 8** Set the cluster password on both the nodes.

```
passwd hacluster
```

**Step 9** Start and enable the pcsd service on both nodes.

```
systemctl start pcsd.service
systemctl enable pcsd.service
```

**Step 10** Authenticate and authorize the nodes, any one node

```
pcs cluster auth <Node1> <Node2> (Proper "HOSTNAME" should be given as it is case sensitive)
```

Eg: pcs cluster auth pn50-qa2-ha-01 pn50-qa2-ha-02.

**Step 11** Start the cluster on one of the nodes. Execute the below command:

```
pcs cluster setup --start --name <Cluster_Name> <Node1> <Node2>
```



**Note** Node1 and Node2 can accept hostname and is case sensitive. For example, pcs cluster setup --start --name hacluster pn50-qa2-ha-01 pn50-qa2-ha-02

**Step 12** Enable a cluster with the specified command on both nodes.

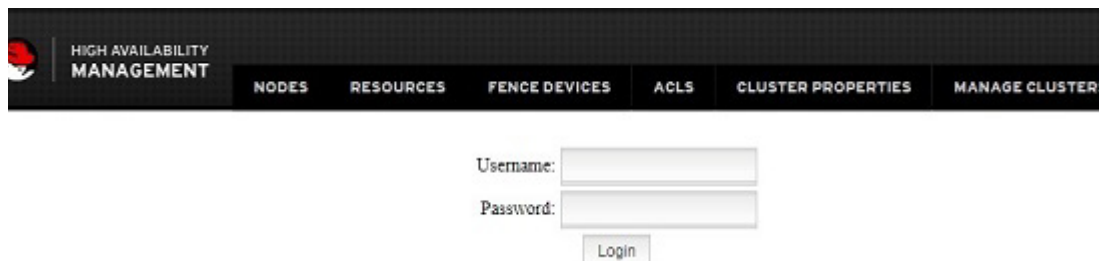
```
pcs cluster enable - all
```

**Step 13** Log in to the Cluster GUI.

For example, https:// <Anynode>:2224;https://10.56.57.204:2224

- Enter the username and password.
- Click Login to access the HAcluster. The High Availability Management window appears.

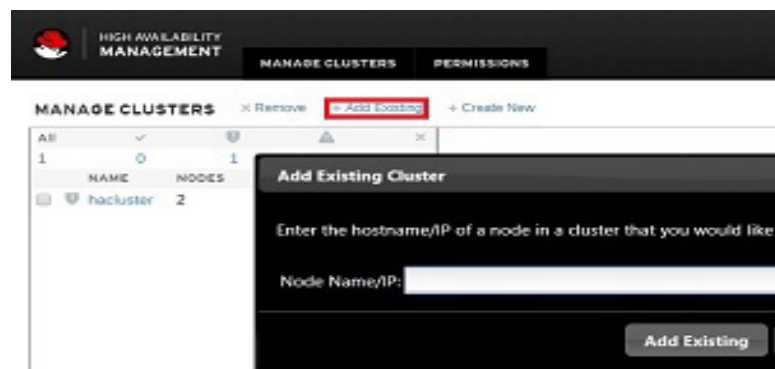
**Figure 10-1** High Availability Login Screen



**Step 14** To add a Hostname to an existing Cluster GUI, follow the below steps:

- Click the **MANAGE CLUSTERS** tab, and then click **Add Existing**.

**Figure 10-2** Add Existing Clusters



- b. In the Add Existing Cluster dialog box, enter the relevant hostname/IP of a node, and then click **Add Existing**.



**Note** To create a new cluster, click **Create New**.

**Step 15** To view individual Cluster information, follow the below steps:

- a. In the Left pane, check a cluster name to view the nodes, resources, and fence-devices information of the selected cluster.



**Note** Prime Network installation does not support fencing. Fencing can be configured manually as per the instructions in RHEL documentation.

**Step 16** In the right pane, under the Nodes area, click any one node and view the Cluster Status in GUI or in CLI.

## Rolling Back to Earlier Prime Network Version

Rollback to Prime Network 4.3.2, 4.3.1, 4.3, 4.2.3, 4.2.2, 4.2.1, or 4.2 is available if you encounter problems during the upgrade, or if you want to roll back to the previous version after the upgrade completes.

### Before You Begin

- Verify that the gateway and units are powered up and connected; that is, you can open an SSH session between the gateway and all units.
- Disconnect standby and NAT units from the gateway using the Administration GUI.
- Verify that the Prime Network application is *not* running with **networkctl status**.
- Before performing the rollback, stop Prime Network integration layer and watchdog monitoring process. For stopping the Integration layer, refer [Chapter 9, “Installing the Prime Network Integration Layer”](#).

After upgrading from RHEL 6.4 or RHEL 5.5 - 5.8 to Prime Network 5.0 with RHEL 6.7, or 6.5 and Oracle 12, you cannot rollback to the previous versions of Prime Network.

To Roll back Prime Network gateway:

- 
- Step 1** If your deployment has units that are connected to the gateway, roll back the units (before rolling back the gateway). The rollback will remove redundant units from the registry and the golden source.
- Step 2** Configure all units using the following command:
- network-conf -rollback**
- Step 3** Enter **no** at the prompt to start the unit.
- Step 4** Restore the backed-up database and start the database services and the listener. Because the database table structure changes after the upgrade, the database is backed up as part of the upgrade process. The old table structure must be recovered.




---

**Note** If you have a gateway high availability deployment, the services ana and oracle\_db services should be moved to maintenance state.

---

- *To restore an external database, contact your database administrator.*
- *To restore an embedded database:*
  - Log into the gateway as *pnuser*.
  - Change to the directory *NETWORKHOME/Main/scripts/embedded\_db*:
 

```
cd $PRIME_NETWORK_HOME/Main/scripts/embedded_db
```
  - Execute the restoration script for restoring the embedded database:
 

```
emdbctl --restore_db
```

For more information on prompts that appear while restoring an embedded database, see the [Cisco Prime Network 5.0 Administrator Guide](#).

After restoring the database, enter **no** at the prompt to start Prime Network.

- Step 5** As *pnuser*, move to the temporary upgrade directory (created in [Step 1](#) of the procedure in [Upgrading to Prime Network 5.0 from 4.3.2, 4.3.1, 4.3, 4.2.3, 4.2.2 \(Intermediate Steps\)](#), page 10-8).
- Step 6** Enter the following command to change to the upgrade directory:
- ```
cd Prime_Network_upgrade
```
- Step 7** Enter the following command on the gateway (only):
- ```
perl rollback.pl
```
- Step 8** Perform the rollback by entering the required information as shown in the following table.

| Prompt for...                               | Enter: | Notes                                                                                                                                                                                       |
|---------------------------------------------|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Confirm that you have restored the database | yes    | Confirm that you performed <a href="#">Step 2</a> .<br><b>Note</b> If you have <i>not</i> restored the database, enter <b>no</b> and exit the script. Restore the database and begin again. |
| Confirm whether you have reinstalled units  | yes    | Confirm that you performed <a href="#">Step 5</a> .<br><b>Note</b> If you have <i>not</i> rolled back the units, enter <b>no</b> and exit the script. Rollback the units and begin again.   |

| Prompt for...                                              | Enter:               | Notes                                                                                                                                        |
|------------------------------------------------------------|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Confirm whether you want to roll back to the older version | yes                  | —                                                                                                                                            |
| Full path to the backup file                               | <i>full pathname</i> | Location of the backup file (it is not deleted during the rollback). An example is:<br><br>/export/home/PrimeNetworkBackUp_XXXXXXXXXX.tar.gz |

**Step 9** When the rollback is complete, log in as the *pnuser* to apply the environment changes.

**Step 10** Start the unit:

- **networkctl start** (without running **network-conf** again)

**Step 11** Reconnect standby and NAT units to the gateway using the Administration GUI.



**Note** Rollback logs can be found in the Prime\_Network\_upgrade folder under *NETWORKHOME*.

## Upgrading the Prime Network Integration Layer (PN-IL)

If the PN-IL is installed on your system, you can upgrade using the instructions in these topics:

- [Upgrading PN-IL in Standalone Mode, page 10-21](#)
- [Upgrading PN-IL in Suite Mode, page 10-22](#)



**Note** If the PN-IL is not installed on your system, you can install it using the instructions in [Installing the PN-IL \(CLI Method\), page 9-4](#)

### Upgrading PN-IL in Standalone Mode

#### Before You Begin

Perform these tasks as *pnuser*:

- Disable the health monitor to disable the PN-IL services permanently otherwise the services will start automatically after a delay of 3 minutes.

```
$PRIMEHOME/local/scripts/il-watch-dog.sh disable
```

- Back up the \$PRIMEHOME directory.

For example, `./ilUpgradeUtility.sh backup`

- Stop the PN-IL using the following command:

```
itgctl stop
```

To upgrade a standalone PN-IL:

**Step 1** As the root user, launch a terminal on the Prime Network gateway server where you want to install PN-IL.

- Step 2** Insert **Disk 3: Upgrade Files** in the DVD drive.
- Step 3** Mount the inserted DVD using **mount** and move to the mount location.
- Step 4** Log in as *pnuser*:
- ```
su - pnuser
```
- Step 5** Create a temporary PN-IL upgrade directory.
- ```
mkdir -p $PRIME_NETWORK_HOME/pnilupgrade
```
- Step 6** Copy the PN-IL upgrade tar file from the mount location to the **pnilupgrade** directory.
- ```
cp /mnt/**/Upgrade/PNIntegrationLayerUpgrade_1.0.0.0-2.0.0.tar.gz
$PRIME_NETWORK_HOME/pnilupgrade
```
- Step 7** Navigate to the directory in which the tar file was copied and extract the PN-IL upgrade tar.
- ```
cd $PRIME_NETWORK_HOME/pnilupgrade
tar -xzf PNIntegrationLayerUpgrade_1.0.0.0-2.0.0.tar.gz
```
- Step 8** Navigate to the extracted files directory.
- ```
cd PNIntegrationLayerUpgrade_1.0.0.0-2.0.0
```
- Step 9** Run the upgrade script
- ```
./upgradeIntegrationLayer.sh
```
- Step 10** Enter **yes** at the prompt to continue the upgrade process. The upgrade process is completed and the log file directory changes based on the PNIL versions changes.
- Step 11** Perform the following post-upgrade tasks:
- As *pnuser*, reload the user profile:
 

```
source $PRIME_NETWORK_HOME/.cshrc
```
  - Configure the PN-IL in standalone mode:
 

```
itgctl config 1
```
  - Start the PN-IL:
 

```
$PRIMEHOME/bin/itgctl start
```
  - Enable the health monitor:
 

```
$PRIMEHOME/local/scripts/il-watch-dog.sh enable
```
- 

## Upgrading PN-IL in Suite Mode

If you have been working with Prime Network 5.0, you will have PN-IL 2.0 installed on your system. The procedure for upgrading to PN-IL 2.0 in suite mode is the same as upgrading in standalone mode. See [Upgrading PN-IL in Standalone Mode, page 10-21](#).



If you have been working with a release prior to Prime Network 5.0, follow the instructions below to upgrade to PN-IL 2.0.

- 
- Step 1** Upgrade PN-IL in standalone mode as described in [Upgrading the Prime Network Integration Layer \(PN-IL\)](#).
- Step 2** Perform these tasks on the Prime Central Server to create a backup of the PN-IL configuration data.
- Log in to the Prime Central server as root.  

```
ssh root@Prime-Central-host-IP-address
su - prime-central-user
```
  - Create Prime Central upgrade directory  

```
mkdir -p $PRIMEHOME/upgrade
```
  - Copy the PN-IL upgrade tar file (example: PNIntegrationLayerUpgrade\_1.0.0.0-2.0.0.tar.gz) from the upgrade directory on the Prime Network server to the upgrade directory on the Prime Central server.
  - Extract the files.  

```
tar -zxvf PNIntegrationLayerUpgrade_1.0.0.0-2.0.0.tar.gz
```
  - Run the PN-IL upgrade utility script to create a backup tar file in \$PRIMEHOME/backup.  

```
./ilUpgradeUtility.sh backup
```
- Step 3** Perform these tasks on the Prime Network server to restore the PN-IL configuration.
- As *pnuser*, copy the backup tar from the Prime Central upgrade directory to Prime Network server.
  - Extract the files:  

```
tar -zxvf il_backup_2.0.0.0.tar.gz
```
  - Run the PN-IL utility script to restore the PN-IL configuration:  

```
./ilUpgradeUtility.sh restore untar-files-directory
```
- Step 4** Perform these tasks on Prime Central as described in [Cisco Prime Central Quick Start Guide](#).
- Upgrade Prime Central
  - Integrate Prime Network and PN-IL with Prime Central
- Step 5** Start the upgraded PN-IL:  

```
$PRIMEHOME/bin/itgctl start
```
- 

## Prime Network Post-upgrade Tasks

After the upgrade to Prime Network 5.0 is complete, perform the post-upgrade tasks that apply to your deployment.

- [Enable Units to Restart Automatically After they are Rebooted, page 10-24](#)
- [Restoring Customized Crontabs, page 10-24](#)
- [Restarting Crontab Jobs for NAT Units, page 10-24](#)
- [Fixing the Database Entry for Vision Clients with NAT, page 10-25](#)

- [Updating the Port Watchdog \(AVM Protection\) Scripts, page 10-25](#)
- [Restore Links Between Devices and Cloud VNEs, page 10-25](#)
- [Support for Third-Party VNEs, page 10-26](#)
- [Command Builder Scripts, page 10-26](#)
- [Gathering DB Statistics in First 24 Hours, page 10-26](#)
- [Integration Changes, page 10-27](#)

## Enable Units to Restart Automatically After they are Rebooted

After upgrade, you need to perform the following steps on each unit in your setup otherwise the units will not restart automatically after they are rebooted.

---

**Step 1** Log into the unit as *pnuser*.

**Step 2** Copy `rootdeploy.cmd` from the gateway, as follows:

```
remote_copy.cmd "<Gateway_IP>:./deploy/independent/on_boot/rootdeploy.cmd"
"./deploy/independent/on_boot/rootdeploy.cmd"
```

**Step 3** Switch to the root user:

```
su - root
```

As the root user, execute the root deploy command:

```
cd $PRIME_NETWORK_HOME/./deploy/independent/on_boot ; ./rootdeploy.cmd
```

---

## Restoring Customized Crontabs

If you saved user-defined cron jobs in `NETWORKHOME/local/cron/crontab.user.list`, they are restored. User-defined cron jobs that are not placed in this directory must be manually recreated.

## Restarting Crontab Jobs for NAT Units

Cron jobs on NAT units must be manually restarted.

---

**Step 1** Log into the unit as *pnuser*.

**Step 2** Copy the `upgrade_restart_crons.pl` script from the gateway, as follows:

```
remote_copy.cmd [gw-ip]:$PRIME_NETWORK_HOME/Main/scripts/upgrade_restart_crons.pl
Main/scripts
```

**Step 3** Run the `upgrade_restart_crons.pl` script. It will display output similar to the following:

```
./Main/scripts/upgrade_restart_crons.pl
+ Updating the unit's cronjobs
- Writing log to ~/Main/logs/upgrade_crons.log
- Copying the files from the gateway (gateway's_ip)
- Restarting the cronjobs
+ Please wait while the unit is being updated.....Done.
```

**Step 4** Verify that the crontab list is not empty:

```
crontab -l
```

**Step 5** The upgrade is now complete. Run the **status** command and check the version number to make sure that the upgrade has been successful.

---

## Fixing the Database Entry for Vision Clients with NAT

If you are using network address translation (NAT) with the Prime Network Vision client, update the database host in the Prime Network registry to contain the hostname instead of the IP address.

If you already use a hostname instead of an IP address, you do not have to repeat this procedure.

---

**Step 1** Make sure Prime Network is running.

**Step 2** Verify that the client workstations have the correct Domain Name System (DNS) mapping.

**Step 3** From *NETWORKHOME/Main*, run the following commands:

```
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/persistency/nodes/main/Host
database-server-hostname
./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0 site/persistency/nodes/ep/Host
database-server-hostname
```

**Step 4** Enter the following command to restart Prime Network:

```
networkctl restart
```

---

## Updating the Port Watchdog (AVM Protection) Scripts

After upgrading to Prime Network 5.0, copy the port watchdog scripts to */var/adm/cisco/prime-network/scripts*. Enter the following commands as the root user:

```
mkdir -p /var/adm/cisco/prime-network/scripts
cp NETWORKHOME/Main/scripts/port_watchdog.pl /var/adm/cisco/prime-network/scripts
cp NETWORKHOME/Main/scripts/keep_alive_port_watchdog.pl
/var/adm/cisco/prime-network/scripts
chmod -R 700 /var/adm/cisco/prime-network/scripts
chown -R pnuser:network /var/adm/cisco/prime-network/scripts
```

## Restore Links Between Devices and Cloud VNEs

If your deployment had cloud VNEs that were connected to devices with static links, the connection between the cloud VNE and the device may be lost after the upgrade. Delete and recreate the link using the Administration GUI.

## Support for Third-Party VNEs

Prime Network supports third-party devices through Cisco Advanced Services engagement. As of release 5.0, Prime Network will not natively support third-party devices, and a Cisco Advanced Services contract will be required for their enablement and support.

## Command Builder Scripts

If you had customized Command Builder scripts (which you should have uninstalled), you may need to update your scripts if your deployment:

- Executes command scripts using the Prime Network northbound APIs (for example, BQL)
- Includes references to IMOs or to the Prime Network internal model

Verify whether the command names, parameters, or IMO references have changed, in which case you must update your scripts. The reinstall your customized scripts.

## Gathering DB Statistics in First 24 Hours

The *pnuser\_admin* user performs maintenance tasks—such as gathering statistics—on the other Prime Network database schemas. After this user is created, a cron job runs every 24 hours to gather statistics on the Fault Database tables.

However, if you expect a high scale in the first 24 hours, you might need to manually force statistics gathering twice during the first day, 1 and 5 hours after noise start. To force statistics gathering, enter the following UNIX command as *pnuser*:

```
cd $PRIME_NETWORK_HOME/Main/scripts ; ./call_update_ana_stats.pl >& /dev/null
```

If you deploy Prime Network to handle a high event rate, disabling Oracle's automatic maintenance jobs is recommended. Automatic maintenance significantly affects Oracle performance and increases event processing time. See [Disabling Automatic Maintenance Jobs, page 4-8](#).

Prime Network supports the *resetVneSSHv2Algorithms.pl* to clean up the 'algorithms' key in avm registry files.

It is recommended to run this script if you are managing the VNE's from ANA3.7 or earlier.

To run the script, follow the below steps:

---

**Step 1** Navigate to '<PNHome>/local/scripts' directory in GW.

Ensure the following:

- Script runs as PN user from the GW.
- PN should be down in both GW and Units.

**Step 2** Run the script file using the below command:

```
perl resetVneSSHv2Algorithms.pl
```

**Step 3** Start the PN in GW and Units to reflect the changes.

## Integration Changes

### Adding Managed Elements to the Database Manually for PC-FM Resync

After upgrading Prime Network, you can execute BQL commands to invoke a VNE insert operation in a new MANAGED ELEMENTS table for all the existing MANAGED ELEMENTS.

Execute the below BQL commands, which has a VNE name “CopyAllManagedElementsToDB” and IP “0.0.0.0”.



**Note**

Make sure to execute the BQL command before restarting PNIL. BQL execution will not introduce any new VNE, but only performs DB refreshing for all the existing VNE’s; inserts all Managed Elements to DB.

```
<?xml version="1.0" encoding="UTF-8"?>
<command name="Create">
 <param name="imobject">
 <value>
 <management.IElementManagement type="management.IElementManagement "
instance_id="0">
 <ID
type="Oid">{ [MCNetwork] [MCMV(IP=X.X.X.X)] [ElementManagement (Key=CopyAllManagedElementsToDB
)]}</ID>
 <IP type="com.sheer.types.IPAddress">0.0.0.0</IP>
 <ElementName type="String">CopyAllManagedElementsToDB</ElementName>
 </management.IElementManagement>
 </value>
 </param>
 </command>
". "
```



**Note**

Replace X.X.X.X in the above BQL with Gateway IP Address.

To terminate the further processing of BQL, an Exception that will be returned as part of the response to the BQL must be invoked (Invocation of this Exception is an already available approach used for Validating the input values while creating a new VNE through Modelling tabs.)



**Note**

The below exception message is expected after executing the BQL:

```
"<Description type="String">ERROR (5133): The VNE's name contains invalid characters. valid chars
are: A-Z, a-z, 0-9, _, '@', '!', '~', '!', '!.</Description>"
```

For details on BQL and other integrations after the upgrade, refer to the Cisco Developer Network at <https://developer.cisco.com/site/prime-network/>.

## Upgrading the Embedded Database to Oracle 12.1.0.2

You must upgrade the embedded Oracle database to version 12.1.0.2 if:

- You have been using Prime Network 4.1 or a lower version and you want to upgrade to Prime Network 5.0.  
AND
- You are planning to upgrade your operating system to Red Hat 6.

If the conditions specified are not met, there is no need to upgrade to Oracle 12.1.0.2 and the upgraded Prime Network 5.0 can run with Oracle 12.1.0.2 as well.

While upgrading to Oracle 12.1.0, follow the steps:

1. First upgrade to Prime Network 4.1.
2. Upgrade Oracle from earlier version to Oracle 12.1.0.2.
3. Upgrade your Operating System.
4. Upgrade from Prime Network 4.1 to Prime Network 5.0.
5. Upgrade to Oracle 12.1.0.2

#### Before you Begin

- Copy the following Oracle installation.zip files from **Prime Network 5.0, Disk 4: Database Binaries** to a directory on the machine on which the embedded database is installed (either on the local gateway server or a remote server):
  - linuxamd64\_12c\_database\_1of2.zip
  - linuxamd64\_12c\_database\_2of2.zip




---

**Note** These database files are available in the Prime Network 5.0 Disk.

---

- Ensure that there is a minimum of 12 GB free disk space. This space is freed up after the upgrade has completed successfully.
- Ensure that database backup and restore are enabled. See the “Enabling Embedded Oracle Database Backups” section in the [Cisco Prime Network 5.0 Administrator Guide](#).

---

**Step 1** As the root user, locate the **embedded\_upgrade\_12.1.zip file** on **Disk 3** and copy it to a directory on the machine on which the embedded database is installed (either on the local gateway server or a remote server).

**Step 2** Unzip the file:

```
unzip embedded_upgrade_12.1.zip
```

**Step 3** If your setup has cluster, freeze the cluster configured services (ana and oracle\_db) using the following command:

```
clusvcadm -Z service
```

**Step 4** Start the database upgrade by entering the following command:

```
perl upgrade_embedded_oracle_12.pl
```

## Example-Upgrading the Embedded Database to Oracle 12.1.0.2

**Step 1** In the database server, perform the following steps:

a. Unzip the **embedded\_upgrade\_12.1.zip** to **/tmp/upg12c** by entering the following command:

```
chmod a+x /tmp/upg12c/*.pl
```

b. Copy the following two zip files to **/tmp/upg12c**.

- linuxamd64\_12c\_database\_1of2.zip
- linuxamd64\_12c\_database\_2of2.zip

c. Create the staging directory by entering the following commands:

```
mkdir /export/home/stg
cd /tmp/upg12c
```

d. Upgrade to Oracle 12.1.0.2 by entering the following command:

```
perl upgrade_embedded_oracle_12.pl
```

```
Enter the name of the OS user of the database [oracle]
Enter the staging/upgrade directory. This directory should have at least 9GB free space
[/export/home/stg]
Running pre-upgrade validations
Extracting /tmp/upg12c/linuxamd64_12c_database_2of2.zip
Extracting /tmp/upg12c/linuxamd64_12c_database_1of2.zip
Diagnosing the database status
Installing the software
Running pre-upgrade tasks
Copying files to new Oracle home
Verifying no files needs media recovery and no backup is running
Before proceeding with the upgrade, this procedure will take a backup of the database. you
may choose between
 1. Offline (Cold) backup (requires database downtime) [default]
 2. Online (Hot) backup
 Enter option: (1-2) 1

The database is about to be shutdown. Please stop PrimeNetwork and any other application
using the database.
Hit the 'Enter' key when ready to continue

Stopping the database & listener
Backing up the database.
Stopping the database & listener
Backing up system files
Upgrading the database. This step may take at least 40 minutes.
Executing post upgrade tasks.
Upgrading timezone file
Identifying new invalid objects
Copying PrimeNetwork scripts to new Oracle home
Restarting Oracle cronjobs
Upgrade completed successfully. Logs can be found under /opt/ora/oracle/ana_logs/upgrade
To complete the upgrade, enter the following command as the Prime Network user:
cd ~/Main/scripts/embedded_db ; emdbctl --update_oracle_home
You have new mail in /var/spool/mail/root
```

**Step 2** Enter the required information as shown in the following table.

Prompt for...	Enter...	Notes
OS username	Username for the Oracle database user.	Default is <b>oracle</b> .
Staging/upgrade directory	Path to the directory from which the upgrade will run and to which the database zip files will be extracted.	Default is /export/home/stg
Location of zip files	<i>Path to the directory to which the Oracle zip files were copied.</i>	—
Database backup method	Offline (Cold) backup or Online (Hot) backup	With cold backup, the database is down during the backup. With hot backup, the database continues to run until the upgrade starts. Downtime is shorter but the backup might take longer. Default is cold backup.

**Step 3** Login to Oracle, and restart the embedded Oracle by following command:

```
#lsnrctl stop
#lsnrctl start
```

## Upgrading the Embedded Database to Oracle 12.1.0.2 in a HA Setup with Geographical Redundancy and Oracle ADG

You must upgrade the embedded Oracle database to version 12.1.0.2 if:

- You have been using Prime Network 3.9 or a lower version and you want to upgrade to Prime Network 5.0.  
AND
- You are planning to upgrade your operating system to Red Hat 6.

If the conditions specified are not met, there is no need to upgrade to Oracle 12.1.0, and the upgraded Prime Network 5.0 can run with Oracle 12.1.0.2 as well.

While upgrading to Oracle 12.1.0.2, follow the steps:

1. First upgrade to Prime Network 4.1.
2. Upgrade Oracle from earlier version to Oracle 12.1.0.2.
3. Upgrade your Operating System.



4. Upgrade from Prime Network 4.1 to Prime Network 5.0.
5. Upgrade to Oracle 12.1.0.2

#### Before you Begin

- Copy the following **Oracle installation.zip** files from **Prime Network 5.0** Disk to a directory on the machines on which the embedded database is installed (both the primary and standby gateway servers):
  - linuxamd64\_12c\_database\_1of2.zi
  - linuxamd64\_12c\_database\_2of2.zip



**Note** These database files are available in the Prime Network 5.0 Disk.

- Ensure that there is a minimum of 12 GB free disk space on each of the servers. This space is freed up after the upgrade has completed successfully.
- Verify that database replication works properly prior to starting the database upgrade by performing the geographical redundancy verification tests described in the [Cisco Prime Network 5.0 Gateway High Availability Guide](#).

- 
- Step 1** To be performed on both primary and standby gateway servers.  
As the root user, locate the **embedded\_upgrade\_12.1.zip** file on **Disk 3** and copy it to a directory on the machines on which the embedded database is installed.
- Step 2** To be performed on both primary and standby gateway servers.  
As the root user, unzip the file:
- ```
unzip embedded_upgrade_12.1.zip
```
- Step 3** On the standby gateway server, run the Oracle software upgrade and prepare the standby server for database upgrade.
Navigate to the upgrade scripts directory and enter the following command:
- ```
perl standby_db_prepare_for_upgrade_12.1.pl
```
- Step 4** On the primary gateway server, start the database upgrade by entering the following command:
- ```
# perl upgrade_embedded_oracle_12.pl
```
- Step 5** Enter the required information as shown in the following table.

| Prompt for... | Enter... | Notes |
|---------------------------|---|----------------------------|
| OS user name | Username for the Oracle database user. | Default is oracle . |
| Staging/upgrade directory | Path to the directory to which the upgrade zip file was copied. | — |

| Prompt for... | Enter... | Notes |
|------------------------|---|---|
| Location of zip files | <i>Path to the directory to which the Oracle zip files were copied.</i> | — |
| Database backup method | Offline (Cold) backup or Online (Hot) backup | With cold backup, the database is down during the backup and the gateway is stopped. With hot backup, the database continues to run until the upgrade starts. Downtime is shorter but the backup might take longer. Default is cold backup. |

Step 6 On the primary gateway server, verify that the Oracle listener is running by entering the following command as the root user:

```
su - oracle -c "lsnrctl status"
```

Step 7 On the standby gateway server, set back the replication redo apply by running the **standby_post_upgrade.pl** to **perl ./standby_db_post_upgrade12.1.pl**.

Example-Upgrading the Embedded Database to Oracle 12.1.0.2 in a HA Setup with Geographical Redundancy and Oracle ADG

Step 1 Stop the Prime Network.

Step 2 Verify if the replication between databases work.

Step 3 In the STANDBY database server, perform the following steps:

- a. Navigate to the location where the embedded Oracle software is available.
- b. Unzip the **embedded_upgrade_12.1.zip** to a location **/tmp/upg12c** by entering the following command:

```
chmod a+x /tmp/upg12c/*.pl
```

- c. Copy the two zip files to **/tmp/upg12c**:
 - linuxamd64_12c_database_1of2.zip
 - **linuxamd64_12c_database_2of2.zip**

- d. Create the staging directory by entering the following commands:

```
mkdir /export/home/stg
cd /tmp/upg12c
```

- e. Upgrade to Oracle 12.1.0 by entering the following command:

```
# perl standby_db_prepare_for_upgrade_12.1.pl
```

```
- Enter the name of the OS user of the database [oracle]
- Enter the staging/upgrade directory. This directory should have at least 9GB free space
[/export/home/stg]
- Running pre-upgrade validations
- Extracting /tmp/upg12c/linuxamd64_12c_database_2of2.zip
- Extracting /tmp/upg12c/linuxamd64_12c_database_1of2.zip
```

- Installing the software
- Copying files to new Oracle home
- Enter the name of the prime network user :pn400
- Upgrade Opatch
- Install Oracle Patch
- Backing up system files
- Starting the standby database in mount mode.
- Copying PrimeNetwork scripts to new Oracle home
- Restarting Oracle cronjobs

Standby database is ready for upgrade. Please run the upgrade procedure for the primary database. Logs can be found under /opt/ora/oracle/ana_logs/upgrade

Step 4 In the PRIMARY database server, perform the following steps:

- a. Navigate to the location where the embedded Oracle software is available.
- b. Unzip the **embedded_upgrade_12.1.zip** to **/tmp/upg12c** by entering the following command:

```
chmod a+x /tmp/upg12c/*.pl
```

- c. Copy the two zip files to **/tmp/upg12c**:
 - linuxamd64_12c_database_1of2.zip
 - linuxamd64_12c_database_2of2.zip

- d. Create the staging directory by entering the following commands:

```
mkdir /export/home/stg
cd /tmp/upg12c
```

- e. Upgrade to Oracle 12.1.0.2 by entering the following command:

```
# perl upgrade_embedded_oracle_12.pl

- Enter the name of the OS user of the database [oracle]
- Enter the staging/upgrade directory. This directory should have at least 9GB free space
[/export/home/stg]
- Running pre-upgrade validations
- Extracting /tmp/upg12c/linuxamd64_12c_database_2of2.zip
- Extracting /tmp/upg12c/linuxamd64_12c_database_1of2.zip
- Diagnosing the database status
- Installing the software
- Running pre-upgrade tasks
- Copying files to new Oracle home
- Verifying no files needs media recovery and no backup is running
- Before proceeding with the upgrade, this procedure will take a backup of the database.
you may choose between
1. Offline (Cold) backup (requires database downtime) [default]
2. Online (Hot) backup
   Enter option: (1-2) 1
The database is about to be shutdown. Please stop PrimeNetwork and any other application
using the database.
Hit the 'Enter' key when ready to continue
- Stopping the database and listener
- Backing up the database
- Stopping the database and listener
- Backing up system files
- Upgrading the database. This step may take at least 40 minutes.
- Executing post upgrade tasks
- Upgrading timezone file
- Enter the name of the prime network user :pn400
- Running Oracle patch installation
- Identifying new invalid objects
- Copying PrimeNetwork scripts to new Oracle home
- Restarting Oracle cronjobs
```

```
Upgrade completed successfully. Logs can be found under /opt/ora/oracle/ana_logs/upgrade
To complete the upgrade, enter the following command as the Prime Network user:
cd ~/Main/scripts/embedded_db; emdbctl --update_oracle_home
You have new mail in /var/spool/mail/root.
Welcome to Prime Network
```

```
-----
.-= Welcome to pn-ha-p1-s5, running Cisco Prime Network gateway (v5.0 (build 119)) =-.
-----
```

```
+ Checking for services integrity:
- Checking if host's time server is up and running           [DOWN]
- Checking if webserver daemon is up and running            [OK]
- Checking if secured connectivity daemon is up and running [OK]
- Checking Prime Network Web Server Status                  [DOWN]
- Checking Compliance Engine Status                          [DOWN]
- Detected AVM99 is down, skipping AVMs check
+ Checking for latest installed device packages:
- Cisco: PrimeNetwork-5.0-DP0
- Third party: No third party device package installed.
```

Step 5 In the STANDBY database server, perform the following steps:

a. Enter the following command:

```
cd /tmp/upg12c
```

b. Upgrade the Oracle version by entering the following command:

```
# perl standby_db_post_upgrade12.1.pl

- Enter the name of the OS user of the database [oracle]
- Setting standby DB for redo apply
- Enter the staging/upgrade directory, same one that was provided earlier
[/export/home/stg]
- Enter the name of the prime network user :pn400
- Upgrade Opatch
- Install Oracle Patch
- Starting the STANDBY database in mount mode.
- Standby database is ready. Please verify replication.
```



Uninstalling Prime Network

This chapter describes how to uninstall Prime Network gateways, units, and clients. For instructions on how to uninstall Prime Network in a gateway high availability deployment, see the [Cisco Prime Network 5.0/ Gateway High Availability Guide](#).

- [Uninstalling a Prime Network Gateway, page 11-1](#)
- [Uninstalling Cisco Prime Network Units, page 11-2](#)
- [Uninstalling the Cisco Prime Network Clients, page 11-3](#)
- [Uninstalling Prime Network Manually, page 11-3](#)
- [Uninstalling the PN-IL Using CLI, page 11-3](#)
- [Uninstalling the PN-IL Using the Wizard, page 11-4](#)
- [Uninstalling Pacemaker Corosync Configuration, page 11-4](#)

Uninstalling a Prime Network Gateway

The following procedure describes how to uninstall a Prime Network gateway with an external database either locally on the gateway or on a remote server. If the uninstallation script fails during the uninstallation process, you can do it manually as described in [Uninstalling Prime Network Manually, page 11-3](#).



Note

During uninstallation process Prime Network does not remove `hidepid=2` entry on the `/etc/fstab` automatically if updated during installation. You need to manually remove the `hidepid` entry from `/etc/fstab` and reboot the system to disable `Hidepid=2`.

To uninstall a gateway:

Step 1 To retain customized information (such as user-created AVMs and VNEs and soft properties), back up `$/NETWORKHOME/Main/registry` and its subfolders and save the data to an external device or folder.

- a. Log on to the gateway as `pnuser` and run the following commands from the `$/NETWORKHOME` directory:

```
mkdir /tmp/avmFiles
cp Main/registry/ConfigurationFiles/127.0.0.1/avm* /tmp/avmFiles
```

The files are copied to the /tmp/avmFiles folder.

- b. Copy the files to another file system.

Step 2 Log on to the gateway server as root, and use the following command to uninstall Prime Network.

```
[root@pn-d-rh-10-lnx ~]# perl /var/adm/cisco/prime-network/reg/pn50/uninstall.pl
```

Step 3 (Optional) Use the dbca utility to remove the database schemas. For more information, see [Table 4-2](#).

Step 4 After the uninstallation procedure is complete, reboot the server.

The uninstallation log is available at
/var/adm/cisco/prime-network/logs/uninstall-log-mmddyy_hhmmss.

Uninstalling a Gateway with an Embedded Database

The embedded database is automatically uninstalled when you uninstall Cisco Prime Network.

Step 1 Log on to the gateway server as root and move to the correct directory.

```
cd /var/adm/cisco/prime-network/reg/pnuser
```

Step 2 Start the uninstallation:

```
./uninstall.pl
```

Step 3 Enter **yes** at the prompt to uninstall Prime Network (and Operations Reports, if installed). The uninstallation begins.

Step 4 If the embedded database is on a remote server, provide the remote server details such as the IP address, username, OS admin, and OS root user password.

Step 5 If the uninstallation fails, uninstall the database manually:

- a. As root, enter the following commands:

```
cd $NETWORKHOME/local/scripts
perl uninstall_ana_db.pl pnuser NETWORKHOME
```

- b. Press **Enter** to finish the uninstallation.

Uninstalling Cisco Prime Network Units

Before you uninstall a unit, make sure it is deleted from the gateway (you can do this from the Administration GUI). To uninstall a unit:

Step 1 Log on to the unit as root, and move to the correct directory:

```
cd /var/adm/cisco/prime-network/reg/pnuser
```

Step 2 Begin the uninstallation:

```
./uninstall.pl
```

- Step 3** At the prompt to uninstall, enter **yes**.
- Step 4** The uninstaller checks if the unit is connected to a gateway. If it is, you are prompted to stop the uninstallation and delete from the gateway.
- Step 5** Delete the working directory:
- ```
cd ..
rm -Rf /var/adm/cisco/prime-network/reg/pnuser
```
- Step 6** After the uninstallation procedure is complete, reboot the unit.
- 

The uninstallation log is available at  
`/var/adm/cisco/prime-network/logs/uninstall-log-mmddyy_hhmmss`.

## Uninstalling the Cisco Prime Network Clients

If you have upgraded from a previous version of Prime Network to Prime Network 5.0, you might want to uninstall the old GUI clients, but this is not mandatory.

To uninstall the clients:

- 
- Step 1** Choose **Start > All Programs > Cisco Prime Network > Uninstall Cisco Prime Network Products**.
- Step 2** In the Select Uninstall Method window, choose Automatic and click **Next**. (We recommend you do not use the Custom uninstall option.)
- Step 3** When the Finish Perform Uninstall window is displayed, click **Finish**. The progress bar reflects the status of the files being uninstalled.
- 

If you click **Cancel** at any time, the uninstallation process stops. Some stranded files might remain on your computer, and you will have to uninstall the software again.

## Uninstalling Prime Network Manually

To manually uninstall Prime Network, log in as root and remove the user and the user installation registry folder:

```
userdel -r username
rm -Rf /var/adm/cisco/prime-network/reg/pnuser
```

To remove information that was migrated, use the following command:

```
userdel -r username_old
```

## Uninstalling the PN-IL Using CLI

This procedure will only uninstall the Prime Network Integration Layer (PN-IL). To unregister PN-IL from Prime Central, see the [Cisco Prime Central Quick Start Guide](#).

To uninstall the PN-IL:

- 
- Step 1** As the root user, open a terminal on the Prime Network gateway server where the PN-IL is installed.
- Step 2** Change to the *pnuser*:
- ```
su - pnuser
```
- Step 3** Start the uninstallation:
- ```
$PRIMEHOME/uninstall/uninstall.sh
```
- Step 4** At the prompt to uninstall, enter **yes**.
- Step 5** After the uninstallation procedure is complete, login to a fresh session.
- 

## Uninstalling the PN-IL Using the Wizard

This procedure will only uninstall the PN-IL. If the PN-IL was configured with Prime Central, after uninstalling the PN-IL, you must manually delete the PN-IL entry from the Prime Central portal.

To uninstall the PN-IL using the wizard:

- 
- Step 1** Launch the X client application (for example, Xming).
- Step 2** As the root user, open a terminal on the Prime Network gateway server where the PN-IL is installed.
- Step 3** Move to the below directory and execute the uninstaller.
- ```
cd/var/adm/cisco/pnintegrationlayer/Uninstaller/  
./PNILUninstaller
```
- Step 4** Click **Uninstall** to continue the uninstallation process.
- Step 5** When the uninstallation is complete, click **Done** to close the wizard.

Uninstalling Pacemaker Corosync Configuration

This procedure will only uninstall the pacemaker Corosync configuration setup in Prime Network.

-
- Step 1** In Prime Network, remove all resources from cluster using below commands

Disable all running resources (Run any one node)

```
Pcs resource disable Oracle  
Pcs resource disable PrimeNetwork  
Pcs resource cleanup
```

Delete resources once all in stopped state (Run any one Node)

```
Pcs resource delete Oracle  
Pcs resource delete PrimeNetwork
```


Destroy Cluster entirely (Run on both nodes)

```
Pcs cluster destroy
```

Step 2 Uninstall PN and Oracle (in all nodes)

```
Perl /var/adm/cisco/prime-network/reg/current/uninstall.pl
```



Next Steps

This chapter provides some steps you should perform after installing the product. After you perform these steps, you can move on to use the Prime Network Administration GUI to add users, create device scopes, and so forth.

- [Launching the Prime Network GUI Clients, page 12-1](#)
- [Verifying That Backups Are Set Up, page 12-3](#)
- [Enabling Network Discovery, page 12-4](#)
- [Setting Up Transaction Manager, page 12-5](#)
- [Setting Up VMware vCenter to Forward Events, page 12-5](#)
- [Integration with Cisco Multicast Manager \(CMM\), page 12-5](#)

Launching the Prime Network GUI Clients

Prime Network enables you to access all its GUI clients from the Web Start page on the gateway. It provides single sign on for all GUI clients. After you enter your credentials, you can access any of the clients.

Before You Begin

Verify the following:

- All the client requirements are met. For more information on the requirements, see [Prime Network Client Requirements, page 2-12](#).
- Java 8 update 60 is installed on your computer. If not, download it from the Java download site: <http://www.java.com>.



Note Prime Network was tested on Java 8 update 60, however it is expected to work with lower Java 8 updates as well.

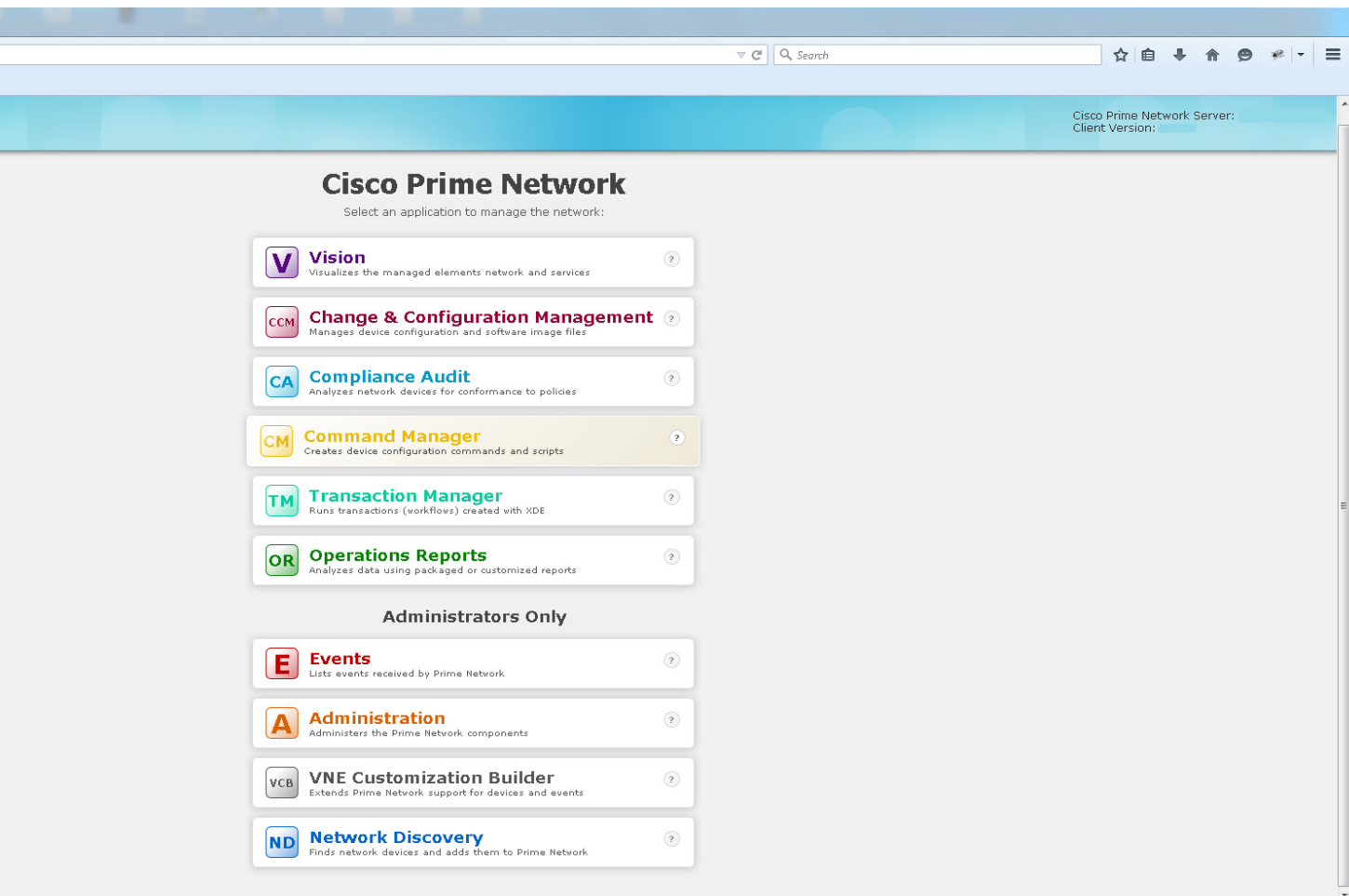
- Ports 6080 and 6081 are open. For other ports required for Prime Network, see [Required Ports for Prime Network, page 2-25](#).

To access the clients using Java Web Start technology:

Step 1 Log into the gateway by entering:

```
http://gateway-host-ip:6080/ana/services/install/install/webstart.html
```

where *gateway-host-IP* is the gateway host name or IP address.



362019

- Step 2** Enter your user name and password in the Prime Network login window and click **Login**. The Prime Network applications launch page is displayed and provides access to all of the Prime Network GUI clients.

- Step 3** Click on the Prime Network application you want to access. A .jnlp file is downloaded.
- Step 4** Click **Continue** in the Security Warning screens. The client application jar files are downloaded and the Prime Network application starts.
-

Verifying That Backups Are Set Up

The Prime Network backup and restore process includes:

- Data backup of the registry data, encryption keys, and reports using the operating system cron mechanism. This data is backed up regardless of whether you have an embedded or external database.
- Embedded database backup. For external database, refer to Oracle documentation.

Prime Network performs backups on a regular schedule. The schedule and data that is backed up depends on whether you have a system with an embedded database or an external database.

**Note**

Back up to tape on a daily basis.

Verifying the Prime Network Data Backup (Gateway Data)

To verify that Prime Network is backing up your data, check the backup directory after you expected a backup to occur. By default the data is saved in `$NETWORKHOME/backup`. For information on changing the backup schedule or location, or performing a manual backup, see the [Cisco Prime Network 5.0 Administrator Guide](#).

Verifying the Embedded Database Backup

Embedded database backups are normally enabled during installation. If you did not enable them, use the procedure in [Cisco Prime Network 5.0 Administrator Guide](#). You must enable this mechanism if you want to perform a backup of the embedded database, regardless of whether the backup is manual or automatic.

Embedded database is backed up according to the profile selected at installation:

- **1-50 actionable events per second** —Full backup is performed every Saturday at 1:00 a.m.; and incremental backups are performed every Sunday-Friday at 1:00 a.m.
- **51-250 actionable events per second** —Full backup is performed every Tuesday and Saturday at 1:00 a.m.

To verify that backups are happening, after a sufficient amount of time has lapsed, check the backup directory you specified during installation.

Operations Reports Data Backup

For information on performing a reports data backup, see the [Cisco Prime Network 5.0 Administrator Guide](#).

Enabling Network Discovery

If you did not configure Prime Network during the initial installation process, you must enable the network discovery functionality manually, as follows:

Step 1 As the root user, navigate to the Prime Network home directory/`local/scripts/`. Be sure to enter the full path to the home directory.

Step 2 Execute `setFpingPermissions.tcsh`.

Example:

```
/export/home/pn50/local/scripts/setFpingPermissions.tcsh
```

Setting Up Transaction Manager

Transaction Manager replaces the Prime Network Workflow and Activation functionality that was available in previous releases of Prime Network. Transactions are activation workflows that you can create using the XDE Eclipse SDK, and then execute from Transaction Manager.

For information on the Transaction Manager GUI and how to use it, see the [Cisco Prime Network 5.0 Customization Guide](#).

To install the XDE Eclipse SDK, contact Advanced Services.

Setting Up VMware vCenter to Forward Events

Prime Network uses the VMware vCenter to obtain information about virtualization inventory and events information by modeling the vCenter as an individual VNE. The XMP Datacenter component retrieves events from the VMware vCenter, normalizes them into the CISCO-EPM-NOTIFICATION-MIB trap format, and forwards them to the Event Collector (AVM 100).

To receive events from the VMware vCenter, you must perform one of the following procedures so that the XMP Datacenter will send UCS events to the correct Event Collector location.

| If the Event Collector (AVM 100) is running on: | You must do the following (as Linux root user): |
|---|---|
| A different server from XMP_DATACENTER | <ol style="list-style-type: none"> 1. Go to <code>\$NETWORKHOME/Main/XMP_DATACENTER/conf</code>. 2. In the <code>datacenterevent.properties</code> file, set the value of the following property to the IP address of the server running AVM 100:
datacenterevent.destAddress0 |
| The same server as XMP_DATACENTER | iptables -t nat -A OUTPUT -p udp -d localhost --dport 162 -j REDIRECT --to-port 1162 |

Integration with Cisco Multicast Manager (CMM)

Prime Network provides multicast support by enabling integration with Cisco Multicast Manager 3.3.2 (CMM). This involves installing CMM on the Prime Network gateway server, and then manually creating the menu options that will enable cross-launching CMM from the Prime Network Administration and Vision GUI clients.



Note

In an installation scenario, where the Cisco Prime Network is installed first followed by the Cisco Prime Network Operations Reports and the CMM on a gateway server, the application might shutdown. In such case, restart the CMM application and then enter the following system command as a root user: **service mysqld-ib start**.

Setting Up Integration with Cisco Multicast Manager

To integrate Prime Network with CMM:

-
- Step 1** Install CMM on the Prime Network gateway server. Refer to the [Installation Guide for Cisco Multicast Manager](#).
 - Step 2** Log into the gateway as *pnuser*.
 - Step 3** Change directories to `$NETWORKHOME/Main/` and enter the following command:

```
installCMMLaunchMenu.pl
```
 - Step 4** At the prompt, enter the port to be used by CMM (default 8080 but this might have been changed during CMM installation).
 - Step 5** When the registry files have been updated, you will be notified that the CMM launch menu has been added successfully.
 - Step 6** Restart the Prime Network Administration and Vision GUI clients.
 - Step 7** In Prime Network Administration, verify that the CMM Configuration menu option appears in the Tools menu. In Prime Network Vision, verify that the CMM Dashboard menu option appears in the Tools menu.

Setting Up Traps for CMM

To receive CMM traps in the **Trap Viewer** page:

-
- Step 1** View the status of IP tables, and verify if the 2162 port is configured by entering the following command:

```
#iptables -t nat -L -n -v
```
 - Step 2** Change the rules in IP tables in the `/usr/sbin` directory by enter the following CLI command:

```
#iptables -t nat -A PREROUTING -p UDP --dport 162 -j REDIRECT --to-port 2162
```
 - Step 3** In the `snmptrapd.conf` file, under `/usr/local/netman/mmtsyst/share/snmp` directory, enter the following command in the first line and save.

```
snmpTrapdAddr udp:<server-ip>:<port-no>
```

For example, `snmpTrapdAddr udp:10.106.214.116:2162`



-
- Note** Ensure that the port number is provided as 2162.
-

- Step 4** Restart CMM by entering the following commands:

```
#!/usr/local/netman/K98mmt  
#!/usr/local/netman/S98mmt
```
 - Step 5** Launch the CMM GUI and verify if the CMM traps are received in the **Trap Viewer** page.
-

Removing Cisco Multicast Manager Integration from Prime Network

To remove CMM integration from Prime Network:

-
- Step 1** Log into the gateway as *pnuser*.
- Step 2** Change directories to `$NETWORKHOME/Main/` and enter the following command:
`uninstallCMMLaunchMenu.pl`
- Step 3** Restart the Prime Network Administration and Vision GUI clients.
- Step 4** In Prime Network Administration, verify that the CMM Configuration menu option is removed from the Tools menu. In Prime Network Vision, verify that the CMM Dashboard menu option is removed from the Tools menu.
-



Using Chinese Characters in Business Tags

Prime Network Vision lets you attach business tags (customer labels) to the following network objects using traditional and simplified Chinese characters:

- Location
- Node name
- Router name
- Map aggregation

The following business tag functions support Chinese characters:

- Creating business tags for network objects
- Searching for business tags
- Generating a list of business tags
- Editing business tag details
- Removing business tags
- Exporting business tags through the northbound interface (NBI)
- Writing business tag notes

Complete the following sections to use Chinese characters with Prime Network.

Using Chinese Characters with Oracle

If you are using Chinese characters, make sure the database parameter `NLS_CHARACTERSET` is set to a value that supports UTF8. Otherwise, Chinese characters will not display correctly after you install or upgrade to Prime Network 5.0.

Step 1 Stop Cisco Prime Network before changing the character set of your database.

```
networkctl stop
```

Step 2 To check the value of the `NLS_CHARACTERSET` parameter, enter the following SQL*PLUS command:

```
sql> SELECT parameter, value FROM v$nls_parameters WHERE parameter='NLS_CHARACTERSET';
```

If the value is UTF8 or AL32UTF8, no further action is required.

Step 3 Check the `job_queue_processes` and `aq_tm_processes` parameters and record the current values (you will restore them later in this procedure). Complete the following steps:

- a. To check the `job_queue_processes` value, enter the following command:

```
SQL> show parameter job_queue_processes
```

In the command output, you should see:

| NAME | TYPE | VALUE |
|---------------------|---------|-------|
| ----- | ----- | ----- |
| job_queue_processes | integer | 10 |

- b. To check the `aq_tm_processes` value, enter the following command:

```
SQL> show parameter aq_tm_processes
```

In the command output, you should see:

| NAME | TYPE | VALUE |
|-----------------|---------|-------|
| ----- | ----- | ----- |
| aq_tm_processes | integer | 0 |

Step 4 Use the Oracle CSALTER script to change the character set to UTF8 or AL32UTF8. The CSALTER script is part of the Oracle Database Character Set Scanner utility. Complete the following steps to change the database character set. For details, see the *Oracle Database Globalization Support Guide*, section “Migrating a Character Set Using the CSALTER Script.”

- Use either a **SHUTDOWN IMMEDIATE** or a **SHUTDOWN NORMAL** statement to shut down the database.
- Perform a full backup of the database (the CSALTER script cannot be rolled back). See the *Cisco Prime Network 5.0 Administrator Guide* for database backup procedures.
- Start the database.
- Run the Oracle Database Character Set Scanner utility (the `csscan` script). The new character set must be UTF8 or AL32UTF8.
- Run the CSALTER script.
- Use either a **SHUTDOWN IMMEDIATE** or a **SHUTDOWN NORMAL** statement to shut down the database.
- Start the database.

Step 5 If the CSALTER script returns the error “Sorry, only one session is allowed to run this script,” do the following:

- Log into the database with SQL*PLUS.
- Use a **SHUTDOWN IMMEDIATE** statement to shut down the database.
- Use **startup restrict** to start the database instance in restricted mode.
- Rerun the CSALTER script.

Step 6 Enter the following commands to restore the values that you recorded in [Step 3](#) for the `job_queue_processes` and `aq_tm_processes` parameters:

```
sql> alter system set job_queue_processes=10 SCOPE=BOTH; # value
sql> alter system set aq_tm_processes=0 SCOPE=BOTH; # value
```

Step 7 Start Prime Network:

```
networkctl start
```

Using Chinese Characters with Windows Clients

If you are using Chinese characters, East Asian languages must be installed on the Windows client workstation (where the Prime Network clients are installed). Also, the regional options must support Chinese.

-
- Step 1** In the Windows Control Panel, choose **Regional and Language Options**.
 - Step 2** Click the **Languages** tab.
 - Step 3** Insert the Windows CD.
 - Step 4** Check the **Install files for East Asian languages** check box.
 - Step 5** Click **OK**.
 - Step 6** Reopen the Windows Control Panel and choose **Regional and Language Options**.
 - Step 7** Click the **Regional Options** tab.
 - Step 8** In the drop-down list, choose **Chinese (PRC)**.
 - Step 9** Click **OK**.
 - Step 10** Restart your Windows client workstation.
-

Displaying Chinese Characters in the GUI

If Chinese characters are not displayed correctly in the GUI, it is because the **synth.xml** file contains a physical font (such as Tahoma) that does not support Chinese characters.

To modify the synth.xml file:

-
- Step 1** Navigate to the `$NETWORKHOME/Main/webstart/jars/xmp-laf` directory and open the Cues.jar file.
 - Step 2** Modify the synth.xml file as follows:
 - a. Access the synth.xml file from the directory, `com/cisco/plaf`.
 - b. Change all instances of “font name=” and/or “font id=” to the desired font. In the below example, the font is set to “Tahoma”.



Note Prime Network was tested with the “Dialog” font.

```
<style id="default">
<object id="graphicsUtils" class="com.cisco.plaf.CUESGraphicsUtils"/>
<graphicsUtils idref="graphicsUtils"/>

<object id="syntheticaPainter"
class="de.javasoft.plaf.synthetica.painter.SyntheticaPainter"/>
```

```

<state>
<!-- CUES: <font id="SyntheticaDefaultFont" name="Segoe UI" size="12"/>
<color type="FOREGROUND" value="#333333"/>-->
<font id="SyntheticaDefaultFont" name="Tahoma" size="11"/>
<color type="FOREGROUND" value="#222222"/>
</state>

```

Step 3 To change the font on the title pane, do the following:

```

<style id="internalFrameTitlePane">
  <imageIcon id="internalFrameCloseIcon"
path="/com/cisco/plaf/images/closeIcon.png"/>
  <imageIcon id="internalFrameMaximizeIcon"
path="/com/cisco/plaf/images/maximizeIcon.png"/>
  ....

  <state>
<property key="InternalFrameTitlePane.closeIcon" value="internalFrameCloseIcon"/>
<property key="InternalFrameTitlePane.minimizeIcon" value="internalFrameMinimizeIcon"/>
<property key="InternalFrameTitlePane.maximizeIcon" value="internalFrameMaximizeIcon"/>
<property key="InternalFrameTitlePane.iconifyIcon" value="internalFrameIconifyIcon"/>

    <!-- <font name="Tahoma" size="11" style="BOLD" /> -->
    <!-- CUES: <font name="Tahoma" size="14" style="PLAIN"/> -->
    <!-- <font name="Tahoma" size="13" style="BOLD"/> -->
    <font name="Tahoma" size="13" style="BOLD"/>

```

Step 4 Save and exit the `synth.xml` file.
