



Installation Requirements

This chapter provides the hardware, software, database, and other requirements that must be met before installing Prime Network 4.3.1.

- [Sample Network Sizes Used in This Document, page 2-1](#)
- [Hardware and Software Requirements, page 2-2](#)
- [Required Red Hat Services and RPMs, page 2-15](#)
- [Required Ports for Prime Network, page 2-22](#)

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 2-9](#)
- [Requirements for Gateway and Unit on a Single Server, page 2-11](#)
- [Prime Network Client Requirements, page 2-11](#)

**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.

**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.

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 2-8](#).


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 2-4](#)
- [Storage Requirements for Different Network Sizes, page 2-6](#)
- [Remote Embedded Database Requirements, page 2-8](#)
- [External Database Requirements, page 2-8](#)

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 5.8, Red Hat 6.5, and Red Hat 6.7 64-bit Server Edition (English language) are supported in Prime Network 4.3.1 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 2-15 .
	 <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 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
Large: 2000 - 5000 devices 50 EPS	10	96 GB	128 GB	132 GB

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



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 4.3.1.



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 4.3.1 installation directory	5 GB Note By default, Prime Network is installed in <code>/export/home/pnuser</code>
(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 3-9](#)), 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. 1.0.1	—

Prime Network Unit Requirements

These topics provide the unit requirements:

- [Unit: Minimum Hardware and Software Requirements, page 2-9](#)
- [Unit: Recommended Hardware for Different Network Sizes, page 2-9](#)

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 2-9 .
Software	Red Hat 5.8 and Red Hat 6.5 64-bit Server Edition (English language) are supported in Prime Network 4.3.1 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 2-15 .

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 2-6](#).

- 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 2-11](#)
- [Using Prime Network Clients with Citrix, page 2-13](#)
- [Accessing Prime Network Clients Using Citrix Environment, page 2-13](#)


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 2-13</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, 26, 27, 29, 30, std Ed 30, ESR 24¹ Google Chrome version 31, 33 Internet Explorer versions 9, 10, 11²
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.

- 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
- Network Discovery might not display properly and the Discovery Profile page might take longer than usual to load.

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

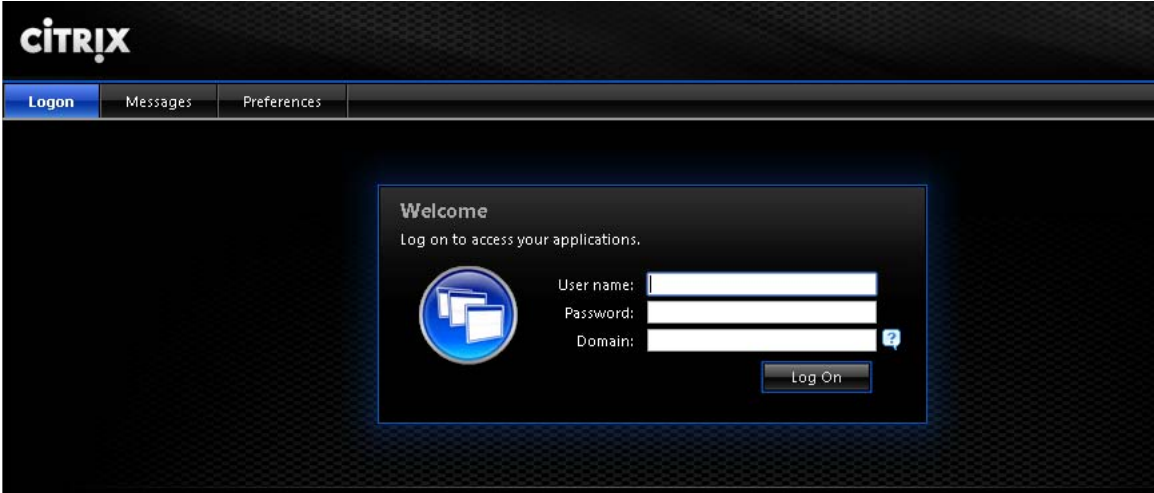
- Click the below link to install and configure the Citrix XenApp 6.0

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

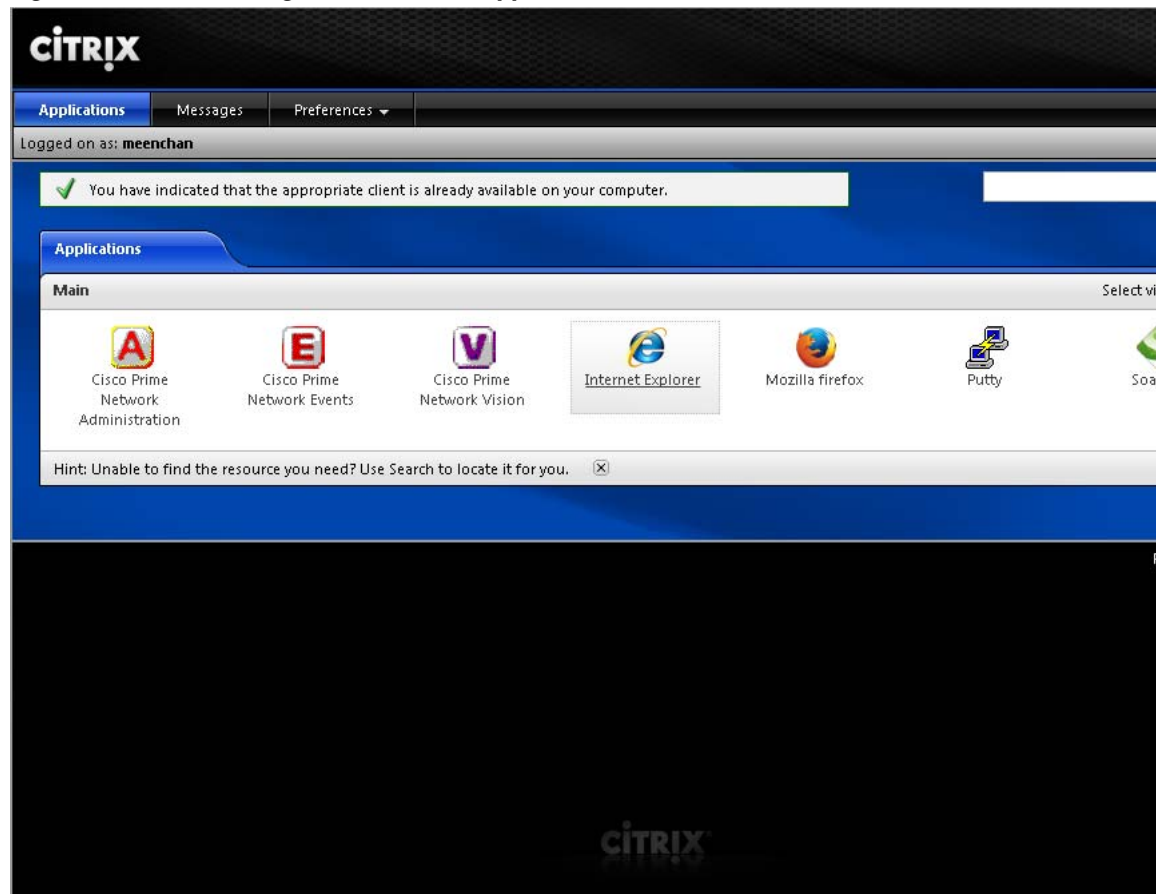
- Ensure that the server on which the Citrix XenApp is installed is configured with correct time and the time zone. Example for IST, the zone should be configured as (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi.

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 5.8](#)
- [Required RPMs for Red Hat 6.5, page 2-16](#)
- [Required RPMs for Oracle Database 12c, page 2-20](#)

Required RPMs for Red Hat 5.8

If you plan to run Prime Network 4.3.1 on gateways or units running Red Hat 5.8, you must download and install several RPM files from the Red Hat website. For more information, see the Red Hat openssh bug fix and enhancement update, Advisory RHRA-2011:0018-1 at:

<https://rhn.redhat.com/errata/RHBA-2011-0018.html>

To download and install the Red Hat RPMs:

-
- Step 1** Download the following Red Hat openssh bug fix and enhancement update RPM files from the Red Hat website to the gateway or unit installation directory:

- openssh-4.3p2-72.el5.x86_64.rpm
- openssh-clients-4.3p2-72.el5.x86_64.rpm
- openssh-server-4.3p2-72.el5.x86_64.rpm

Step 2 As a root user, enter the following commands:

```
rpm -Uhv openssh-4.3p2-72.el5.x86_64.rpm
rpm -Uhv openssh-clients-4.3p2-72.el5.x86_64.rpm
rpm -Uhv openssh-server-4.3p2-72.el5.x86_64.rpm
/etc/init/sshd stop
/etc/init/sshd start
```

Step 3 Repeat these steps for each gateway and unit running with Red Hat 5.8.

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
- libgcj.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 Oracle Database 12c

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

- binutils-2.20.51.0.2-5.11.el6 (x86_64)
- glibc-2.12-1.7.el6 (x86_64)
- libgcc-4.4.4-13.el6 (x86_64)
- libstdc++-4.4.4-13.el6 (x86_64)
- libaio-0.3.107-10.el6 (x86_64)
- libXext-1.1 (x86_64)
- libXtst-1.0.99.2 (x86_64)
- libX11-1.3 (x86_64)
- libXau-1.0.5 (x86_64)
- libxcb-1.5 (x86_64)
- libXi-1.3 (x86_64)
- make-3.81-19.el6
- sysstat-9.0.4-11.el6 (x86_64)
- compat-libcap1-1.10-1 (x86_64)
- compat-libstdc++-33-3.2.3-69.el6 (x86_64)
- gcc-4.4.4-13.el6 (x86_64)
- gcc-c++-4.4.4-13.el6 (x86_64)
- glibc-devel-2.12-1.7.el6 (x86_64)
- ksh (any version of ksh)
- libstdc++-devel-4.4.4-13.el6 (x86_64)
- libaio-devel-0.3.107-10.el6 (x86_64)

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 Ports for Prime Network

These topics list the required ports for Prime Network.

- [Prime Network Server, HTTP, TCP, and UDP Ports, page 2-22](#)
- [Prime Network Integration Layer Ports, page 2-25](#)

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	HTTP port for Change and Configuration Management, VCB, and Network Discovery web clients. 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: # cd \$NCCM_HOME/scripts/ # ./nccmHTTP.csh enable # dmctl stop # dmctl start
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.
8101 (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.