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 6-21
- Product Services Installed with Prime Network, page 6-23
- Troubleshooting, page 6-24

Installation Overview

The Prime Network gateway can be installed using either an embedded database or an external database. For the embedded database, Prime Network 5.2 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 5.2 fresh installation will support only Oracle 12.2.0.1.

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 $*PRIME_NETWORK_HOME*.
- Extracts and creates the required directories. For information on folders created after installation, see Environment Variables, Aliases, and Folders Created During Installation, page 6-21.
- 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.
- Its know issue that when enabled security hardening, the operation reports connects to PN-GW:8445 with TLSV11.0 because Operations Report does not support SSL

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, pn52 is permitted, but network 5.2 is not.

For example, the following command creates a *pnuser* named pn52, and installs Prime Network in the /export/home/pn52 directory:

```
perl install.pl -user pn52 -dir /export/home/pn52
```

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 12-3.

Step 7 Copy the following Oracle installation .zip files from **Prime Network 5.2**, **Disk 4: Database Binaries** to the embedded_oracle directory ($*PRIME_NETWORK_HOME*/local/scripts/embedded_oracle):

- linuxx64_12201_database.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 3-6.

Step 9 Enter a password for all built-in users (root, bosenable, bosconfig, bosusermngr, 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	This guide assumes that the database will be installed locally on the gateway server. 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). **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.
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 5.2 supports dual NICs, the installation may detect that the server is configured with multiple NICs. Specify the NIC to use for the database connection.
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	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. If you enter **no**, the installation will quit.
Selecting Prime Network database profile.	The number corresponding to the estimated profile.	Select from 1-7 based on the actionable events per second. For more information on database profiles, see Creating an External Oracle Database, page 4-2.
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.	Location of the redo logs. They should not be on the same disk as the data files. Example: /export/home/oracle/redo. **Note** Use ext3 partition mounted with the default mount options.

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 5.2 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 5.2 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 5.2 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 Prime Network is integrated to Prime Central, the Prime Network and the PN-IL status should be up in the Prime Central 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	**Choose either one of the following option:** • **no** —No change happens in Prime Network security configurations. • **yes** —Disables Low and Medium strength Ciphers. If you disable Low and Medium strength Ciphers, you must ensure that all network connections are using High Strength Ciphers before disabling. **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.
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 *suite mode*. 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 $*PRIME_NETWORK_HOME*/Main/logs.
- Network Discovery logs are available at $*PRIME_NETWORK_HOME*/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, pn52 is permitted, but network 5.2 is not.

For example, the following command creates a *pnuser* named pn52, and installs Prime Network in the /opt/primenetwork51 directory:

```
perl install.pl -user pn52 -dir /opt/primenetwork52
```

Note The installation might take a while. For information on the Cisco Prime Network environment created during installation, see Table 6-6.

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 12-3

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, bosusermngr, web monitoring user)	The password that will be used to access the various Prime Network system components.	The three login levels defined to connect to the Prime Network shell.This password will also be used as the database schemas password. You can change the password for each of these users at a later stage. See the Cisco Prime Network 5.2 Administrator Guide for changing the passwords. 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.
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	*username*	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	If you enter **yes**, the *pnuser* database is configured automatically with the following default values: • Port 1521 • SID: mcdb • No encryption • Prime Network-created users The *pnuser*_ep (Event Archive) schema uses the same settings. 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.

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 5.2 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 your 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 appears 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	*port-number*	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 $*PRIME_NETWORK_HOME*/Main/logs.
- Network Discovery logs are available at $*PRIME_NETWORK_HOME*/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
pnuser	Fault Database—Active and archived network and non-network events and tickets (*archived events and tickets* are events and tickets that were moved to an archive partition in the Fault Database)	pn52
***pnuser*_ep**	Event Archive—Raw traps and syslogs received from devices	pn52_ep
***pnuser*_rep**	Used by reports mechanism	pn52_rep
***pnuser*_ep_rep**		pn52_ep_rep

Schema Name	Description	Example
***pnuser*_xmp**	Change and Configuration Management (CCM), Compliance Manager, Compliance Audit, Command Manager, Transaction Manager	pn52_xmp
***pnuser*_admin**	Database administrator for maintenance tasks—such as gathering statistics—on the other Prime Network database schemas	pn52_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 6-15
- Verifying the Redirected Ports, page 6-18
- Verifying the Drools Rules Configuration, page 6-19
- `service iptables save`, page 6-19
- Verifying the Monitoring (Graphs) Configuration, page 6-19
- Verifying the Installation of Registry Directories, page 6-19
- Adding Oracle Database Files, page 6-19
- Updating the Database Host in the Registry for NAT, page 6-21

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 5.2 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 5.2 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 $*PRIME_NETWORK_HOME*/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 12.2.0.1.0 Production on Tue Jan 22 11:59:18 2019

Copyright (c) 1982, 2016, Oracle. All rights reserved.

Connected to:
Oracle Database 12c Enterprise Edition Release 12.2.0.1.0 - 64bit Production
```

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 System Account of the Prime Network OS User Name or/and Database User Name

To change the Prime Network OS user or/and database user name from the gateway and unit, follow these steps.

1. Log in to the Prime Network server.

Warning **When you execute the ChangePrimeNetworkAndOracleUser.sh script the Prime Network application on both the gateway and unit will be down.**

2. Run the following script as root user,

```
$PRIME_NETWORK_HOME/local/scripts/ChangePrimeNetworkAndOracleUser.sh
Log can be found at /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. 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.

Changing a System Account in the Local HA Configuration Setup

To change the Prime Network OS user name, Database user name, or both Oracle and Prime Network OS user name:

Step 1 Log in to the primary node that is configured at the time of installation.

Warning **When you execute the ChangePrimeNetworkAndOracleUserLocalHA.sh script both the active and standby Prime Network application will be down.**

Step 2 As root user execute **ChangePrimeNetworkAndOracleUserLocalHA.sh** that is available under $PRIME_NETWORK_HOME/local/scripts.

Note If your setup has unit added to it then execute the **ChangePrimeNetworkAndOracleUser.sh script,** which is available under $PRIMEHOME/local/scripts.

Step 3 Use the following table values to change the Prime Network OS username, Oracle Database username or both Oracle and Prime Network OS user name.

.

Table 6-5 Changing OS User Name, Database User Name or Both Oracle and Prime Network OS User Name

Action	Prompt for...	Enter...	Notes
To Change Prime Network OS User Name, select the **Change Prime Network OS Username only** option	Secondary Cluster node IP	IP address of the secondary node	The Script displays the curent Prime Network user. Press Enter to continue or provide the prime network user name in case it is different
	Entering new user name	New Prime Network user name	On successful completion the script displays the following message `Requested users has been changed and activated successfully.`
	Unfreeze the services after the execution of the script		To Un-freeze the services, use the following • **clusvcadm -U <service-name>** (RHEL 6.x) • **pcs resource manage <service-name>** (RHEL 7.x)
To change Oracle database username, select the **Change Oracle Database Username only** option	Secondary Cluster node IP	IP address of the secondary node	The script displays the current Oracle user. Press Enter to coninue or provide the Oracle user name in case it is different.
	Entering new Oracle Database user name	New Oracle user name	On successful completion the script displays the following message: `Requested users has been changed and activated successfully.`
	Unfreeze the services after the execution of the script		To Un-freeze the services, use the following • **clusvcadm -U <service-name>** (RHEL 6.x) • **pcs resource manage <service-name>** (RHEL 7.x)

Table 6-5 Changing OS User Name, Database User Name or Both Oracle and Prime Network OS User Name (continued)

Action	Prompt for...	Enter...	Notes
To change both Oracle and Prime Network OS Username, select the **Change both Prime Network OS Username & Oracle Database Username** option	Secondary Cluster node IP	IP address of the secondary node	The script displays the current Prime Network user. Press Enter to continue or provide the Prime Network user name in case it is different.
	Enter the new Prime Network user name	New Prime Network user name	The script displays the current Oracle user name, Press Enter to continue or provide the Oracle Database user name in case it is different.
	Enter the new Oracle user name	New Oracle user_name	On successful completion the script displays the following message: `Requested users has been changed and activated successfully`
	Unfreeze the services after the execution of the script		To Un-freeze the services, use the following • **clusvcadm -U <service-name>** (RHEL 6.x) • **pcs resource manage <service-name>** (RHEL 7.x)

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 $*PRIME_NETWORK_HOME /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 5.2 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 5.2 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 $*PRIME_NETWORK_HOME*/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 pn52:
-1119: ORA-01119: error in creating database file '/2del/pn52_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 $*PRIME_NETWORK_HOME*/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/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 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 6-6 defines the *pn-user* environment variables defined by the installation script.

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

Variable Name	Default
PRIME_NETWORK_HOME **Note** 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.	/export/home/*pnuser*
JAVA_HOME	*PRIME_NETWORK_HOME*/java
NCCM_HOME	*PRIME_NETWORK_HOME*/NCCMComponents
XMP_HOME	*PRIME_NETWORK_HOME*/XMP_Platform.

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

Table 6-7 lists the aliases defined by the installation script.

Table 6-7 Aliases Defined by the Installation Script

Table Alias	Content
reg	Changes the directory to *$PRIME_NETWORK_HOME*/Main/registry
main	Changes the directory to $*PRIME_NETWORK_HOME*/Main
logs	Changes the directory to *$PRIME_NETWORK_HOME*/Main/logs

Table 6-8 lists the folders created in Prime Network 5.2.

Table 6-8 Folders Created in Prime Network

Folder	Contents
Folders in *PRIME_NETWORK_HOME*.	
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 (*AVM-ID*.out; for example, 0.out or 11.out)
Main/registry	Local copy of registry files
Main/registry/ConfigurationFiles	*Golden source* (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 6-9 lists the product services that are installed with the Prime Network system.

Table 6-9 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/Avm[NUM].xml	8000+AVM number for secured XML RPC 2000+AVM number for local management	2000-3000, 8000-9000 (TCP)	Java, Perl, Tcsh	Inner protocol
sheer_secured daemon	Secured connectivity between gateway and unit	local/sheer_secured/sheer_config	1101 (TCP)	—	—	SSH
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. 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

Problem Swap file entry error	**Solution** Increase the swap file size in two ways:
	Enter the keyword "-override_swap" along with the installation command.
	`For example. perl install.pl –user pn52 –override_swap`
	`dd if=/dev/zero of=/swapfile bs=1024 count=65536 (based on the requirement size, the bs & count entry will differ)`
	`mkswap /swapfile`
	`chmod 0600 /swapfile`
	`swapon /swapfile`
	To enable it at boot time:
	Edit /etc/fstab to include the following entry:
	`/swapfile swap swap defaults 0 0`

Problem Error in deploying fetch_expect or RRDs or Embedded database (on RHEL 5.8)	**Solution** Remove the "=" symbol from the following file: `Cat /etc/profile.d/proxy.csh`

Problem Host file entry error	**Solution** Check the host file for local host entry:
	`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`

Problem/Message	Solution/Action Required

Problem SMTP TIME OUT Error (on both RHEL 5.8 & 6.5)	This occurs when there is SMTP time out error.
	Solution
	1. Get to the following file:
	/etc/opt/quest/vas/vas.conf
	2. Edit the following entry:
	`prompt-local-pw = From "This is your UNIX password: " to "Password:"`
	`prompt-vas-ad-pw = From "This is your UNIX password: " to "Password:"`

Problem COMPACT LSB error	**Solution** While installing any RPM, update the LSB core with the following command:
	`yum install redhat-lsb-core`
	or
	`yum update redhat-lsb-core`

Problem It is time consuming to install multiple RPMs individually	**Solution** To install Multiple RPM's simultaneously: 1. Create a txt file and copy all the RPM names. 2. Enter the following command: `yum install `awk '{print $1}' ./rpm.txt` -y` where, "rpm.txt" is name of the text file that you created.
During installation or upgrade you may encounter the following errors:	
Problem Unable to establish master SSH connection: master process exited unexpectedly at reader PrimeNetwork::DB::Oracle::_ssh	This occurs when master process exited unexpectedly at reader PrimeNetwork::DB::Oracle::_ssh **Solution** Check whether the Openssh or Openssl got installed and updated.
Solution Failed to backup the database with the following error ORA-27369: job of type EXECUTABLE failed with exit code: Operation not permitted ORA-06512: at "SYS.DBMS_ISCHED", line 198 ORA-06512: at "SYS.DBMS_SCHEDULER", line 594 ORA-06512: at line 1 (DBD ERROR: OCIStmtExecute) . ABORTING. ***	**Solution** Enable the backup and give proper permission to the folder for both backup and archive, which are under Oracle home folder.

Problem/Message	Solution/Action Required
Problem Error: Failed on creating inventory logical tables	This occurs when there is a SQL syntax error. `For example: check the log and get into that location to check the syntax. In this case, /export/home/pn43/Main/plugins/newalarm/deployment/infobrightdeployment/inventory/logical`

Problem Failed to copy ssh keys from gateway error (during unit adding)	Check the following:
	• proxy settings and file permissions of /$PRIME_NETWORK_HOME/local/ana_secured and /$PRIME_NETWORK_HOME/
	• RHEL version. If the RHEL version is 6.5, make sure the openssl rpm is updated (to 57 version).
	`openssl-1.0.1e-57.el6.i686.rpm`
	`openssl-1.0.1e-57.el6.x86_64.rpm`
	• Make sure that firewall is configured properly or in stopped state.

Problem Prime Network failed to start with the following error: This unit (10.104.63.97) is not connected to 10.104.63.96 gateway anymore.	Check if both Unit and GW got installed on the same directory path. For example, either in /export/home or /home.
Problem Unable to launch the CCM application	Check for the following: • Web server should be up • Tomcat should be up • dmctl status

Problem/Message	Solution/Action Required
Problem Receiving the following error entries: Unzipping p23054354_121010_Linux-x86-64.zip on the database server Stopping the database and listener /export/home/anaoracle/product/12.2.0/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/12.2.0/db_1/startup.log': Permission denied chmod: changing permissions of `/export/home/oracle/product/12.2.0/db_1/startup.log': Operation not permitted /export/home/anaoracle/product/12.2.0/db_1/bin/dbstart: line 346: /export/home/oracle/product/12.2.0/db_1/startup.log:Permission denied	This occurs when there is no proper permission to ivne-drivers.tar file & oracle home folder. **Solution** Check the permissions of copied ivne-drivers.tar file and oracle home folder.
Problem Unit AVM failed / unreachable to start the Prime Network after Rollback	**Solution** Check if the hostname entry on /etc/hosts is appropriate.
Problem Receiving errors during XMP platform and Web server installation process.	**Solution** 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.

Problem/Message	Solution/Action Required
Problem The following ports are unreachable on the PN Gateway (ipadd): 6081, 9490, 1101".while adding unit with gateway. (using either ipv4 or ipv6 address)	**Solution** Make sure that: • Ports such as 6081, 9490, 1101 are in listening state. • iptables (for both ipv4 and ipv6) got turned off. • Selinux got disabled or in permissive mode.

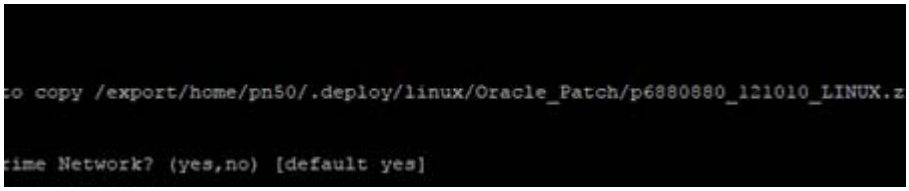
Problem Compliance engine status is down	**Solution** Check the ComplianceService.log under:
	`PRIME_NETWORK_HOME/XMP_Platform/logs and nccm.log under PRIME_NETWORK_HOME utils/independent/compliance/bin`
	Solution Check the DB ip address entry in the following folder path:
	`PRIME_NETWORK_HOME/utils/independent/compliance/resources /server/global/nccmDatabase.properties`

Problem Compliance Engine not starting: .	Before upgrading to 5.2, take the backup file "nccmDatabase.properties" that is located in: `PRIME_NETWORK_HOME/utils/independent/compliance/resources /server/global/nccmDatabase.properties`
Problem Could not open '/tmp/ana_db_properties.properties' for reading No such file or directory	**Solution** Check the oracle 12c files permissions.

Problem/Message	Solution/Action Required
Problem Unit servers shows Virtual IP address during Network configuration. ***Figure 6-1 Unit Servers*** 	**Solution** This occurs when either gateway or Unit server is not installed on the same directory. For example:/export/home/pnuser. Make sure to install the Unit servers with the same directory path in which the Gateway is installed.

Problem Receiving errors ending with number 256.

Figure 6-2 Errors ending with 256



Solution This occurs when the oracle is not uninstalled properly.