



## Managing the Prime Network Software Image, Features, and Backups

---

These topics explain how to manage the Prime Network software image—the base image, patches, and device updates (VNE driver jar files)—and how to backup and restore the software image and Prime Network data.

- [Getting Basic Information About the Prime Network Image, page 2-1](#)
- [Updating the Prime Network Image, page 2-4](#)
- [Backing Up and Restoring Data, page 2-5](#)
- [Tracking Changes to the Product Image and VNEs, page 2-14](#)



### Note

In Prime Network 4.2, the current existing support for third-party devices and related services is removed. Support for existing third-party devices and newly-required third-party devices is going to be enabled through Advanced Service engagement. For customer with third-party support in Prime Network 4.0, upgrading to Prime Network 4.2, please involve your sales representative to enable a smooth transition to Advanced Service engagement. Please involve your sales representative for additional details on the Advanced Service offering.

---

## Getting Basic Information About the Prime Network Image

These topics explain how you to get information about your existing product image version and VNE driver files that are installed on your gateway server:

- [Checking the Prime Network Home Directory and Software Image Version, page 2-2](#)
- [Checking Which VNE Drivers and Device Packages Are Installed, page 2-4](#)

## Checking the Prime Network Home Directory and Software Image Version

To identify your installed version of Prime Network, choose **Help > About** from any of the GUI clients.

By default, Prime Network is installed in `/export/home/pnuser`. The `pnuser` account is the operating system user account for the Prime Network application. An example of `pnuser` is **pn41**. The `pnuser` is an important account and is used in several ways:

- The default Prime Network installation directory is `/export/home/pnuser`. If you defined `pnuser` as **pn41** and used the default installation directory, the Prime Network installation directory would be `/export/home/pn41`.
- The ANAHOME environment variable for `pnuser` is set to the Prime Network installation directory. For example:

```
# echo $ANAHOME
/export/home/pn41
```

In general, the Prime Network installation directory is referred to as `NETWORKHOME`.

You can also connect to the gateway, get version information, and get general system status using the **networkctl** command. Before this your gateway must be installed. For information on installing the gateway and client software, refer to the [Cisco Prime Network 4.3 Installation Guide](#).

---

**Step 1** Log into the gateway server as `pnuser`.

**Step 2** Enter the following:

```
# networkctl status
```

```
-----
.-= Welcome to sjcn-sysm, running Cisco Prime Network gateway (v4.3 (build 347)) =-.
-----
...
```

---

The **networkctl** command is located in `NETWORKHOME/Main`. It takes the following options:

**networkctl [ start | stop | status | restart ]**

Options/Arguments	Description
<b>start</b>	Starts the gateway process. With no options, this command starts the gateway and all component processes.
<b>stop</b>	Stops the gateway process. With no options, this command stops the gateway and all component processes. If AVM protection (watchdog protocol) is enabled, Prime Network will try to restart the process after a few minutes. If you do not want the process to be restarted, stop the AVM using the GUI; see <a href="#">Moving and Deleting AVMs, page 3-34</a> .

Options/Arguments	Description
<b>status</b>	Displays the status of the gateway processes.
<b>restart</b>	Stops and starts the gateway processes. With no options, this command stops and restarts the gateway and all component processes.  By default, Prime Network automatically starts if the gateway is rebooted. To disable this behavior, see <a href="#">Managing Configurations with Firewalls (Device Proxy)</a> , page 3-24.

The following example shows the full output of a **networkctl status** command. In the following example, the user has created AVM 789 and AVM 850. AVMs number 1-100 are reserved for use by Prime Network and are described in [Table 3-2 on page 3-9](#).

```
# networkctl status
-----
.-= Welcome to sjcn-sysm, running Cisco Prime Network gateway (v4.3 (build 347)) =-.
-----

+ 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                 [UP]
- Checking Compliance Engine Status                         [UP]
+ Detected AVM99 is up, checking AVMs
- Checking for AVM789's status                             [OK 0/11983]
- Checking for AVM83's status                             [OK 0/83]
- Checking for AVM100's status                             [OK 0/823]
- Checking for AVM786's status                             [OK 4/2108]
- Checking for AVM555's status                             [OK 53/2519]
- Checking for AVM333's status                             [OK 43/5179]
- Checking for AVM800's status                             [OK 0/6804]
- Checking for AVM810's status                             [OK 9/5090]
- Checking for AVM156's status                             [OK 10/4098]
- Checking for AVM19's status                              [DISABLED]
- Checking for AVM112's status                             [OK 103/26822]
- Checking for AVM76's status                              [OK 0/104]
- Checking for AVM432's status                             [OK 133/24113]
- Checking for AVM11's status                              [OK 382/12304]
- Checking for AVM750's status                             [OK 0/40843]
- Checking for AVM777's status                             [OK 0/20287]
- Checking for AVM45's status                              [DISABLED]
- Checking for AVM123's status                             [OK 5/322]
- Checking for AVM0's status                               [OK 0/204]
- Checking for AVM850's status                             [OK 0/46489]
- Checking for AVM25's status                              [OK 0/1319]
- Checking for AVM111's status                             [DISABLED]
- Checking for AVM999's status                             [DISABLED]
- Checking for AVM35's status                              [OK 761/47795]
- Checking for AVM888's status                             [OK 146/7593]
- Checking for AVM444's status                             [OK 69/3547]
- Checking for AVM345's status                             [OK 98/10195]
- Checking for AVM768's status                             [OK 0/6206]
- Checking for AVM44's status                              [OK 3/78]
- Checking for AVM666's status                             [OK 16/1564]
- Checking for AVM78's status                              [OK 0/152]
- Checking for AVM84's status                              [OK 0/44]
+ Checking for latest installed device packages:
- Cisco: PrimeNetwork-4.3-DPO
- Third party: No third party device package installed.
```

**networkctl** could display any of the following status indicators:

Status	Description
OK	Service or AVM is up and running.
DOWN	Service or AVM is down.
LOADED	Service is down, but the system is trying to start (load) it.
DISABLED	AVM has been stopped.

## Checking Which VNE Drivers and Device Packages Are Installed

VNE drivers are jar files that contain support for specific device series or families. The type of support includes support for different software versions, physical and logical entities (modules or technologies), syslogs, traps, and configuration scripts. A complete set of VNE drivers is provided with the base releases of Prime Network. However, jar file updates are provided between Prime Network releases. The updated jar files are provided in VNE Device Packages (DPs) that you can download from [Prime Network Software Download site](#) on Cisco.com and install on your gateway. Updated DPs are provided on a monthly basis.

To find the latest Device Package that is installed on your gateway, run the **status** command as *pnuser*, which will display the latest DP version installed on the gateway.



### Note

The following DPs are hypothetical examples.

Log into the gateway server as *pnuser* and enter the following:

```
# networkctl status
```

The end of the output will display information similar to the following:

```
+ Checking for latest installed device packages:
- Cisco:      PrimeNetwork-4.3-DP1411
- Third party: PrimeNetwork-4.3-TPDP1409
(Need to check whether the version changed is correct)
```

For more information on DPs, use the **ivne** command. It can list *all* installed DPs (instead of only the latest one) and you can also use it to install new DPs. See [Adding New Device Support with Device Packages, page 4-27](#).

## Updating the Prime Network Image

These topics explain how to update the product image by applying patches and updating VNE driver jar files.

- [Installing Prime Network Patches, page 2-5](#)
- [Installing Prime Network Device Packages to Add New Device Support, page 2-5](#)

## Installing Prime Network Patches

Prime Network patches are posted to the external software download site for Prime Network software, as they become available. This procedure explains how to get to the download site to find patches, and how to start the installation process. Because the installation process sometimes changes (depending on patch contents), this procedure does not include the complete procedure, but instead points you to the Readme file that contains the complete information.

- 
- Step 1** Log into Cisco.com and go to the Prime Network [software download site](#).
  - Step 2** Click the link for the Prime Network release in which you are interested.
  - Step 3** Under Select a Software Type, click Prime Network **Patches**. If any patches are available, they are listed here.
  - Step 4** If you want to install a patch, click the Readme file link at the upper right corner of the download table and download the Readme. Then follow the Readme instructions on how to install the patch.
- 

## Installing Prime Network Device Packages to Add New Device Support

Device Packages are downloadable packages that contain a group of VNE driver jar files. When you add a device to Prime Network, Prime Network identifies the NE by vendor, device family, device subfamily, device type and software version. This is done by matching the device with its appropriate VNE driver jar file. The driver jar file contains information about software versions, physical and logical entities, syslogs, traps, and command scripts, all of which enable Prime Network to properly model and monitor the device.

Rather than make you wait for a new Prime Network release, updates are made available between releases. They are packaged together and delivered in Device Packages (DPs). As newer versions become available, DPs are placed on Cisco.com. The following procedure shows you how to check Cisco.com for new DPs. If you want to install a DP, see [Adding New Device Support with Device Packages, page 4-27](#).

- 
- Step 1** Log into Cisco.com and go to the Prime Network [software download site](#).
  - Step 2** Click the link for the Prime Network release in which you are interested.
  - Step 3** Under Select a Software Type, click Prime Network **VNE Drivers**.
  - Step 4** If you want to install a DP, follow the instructions in [Downloading and Installing New Driver Files, page 4-31](#).
- 

## Backing Up and Restoring Data

Backup and restore processes manage two categories of data used by Prime Network:

- Information stored on the gateway—Registry data, encryption keys, reports, etc.
- Information stored in the embedded Oracle database—Faults, events, inventory information, command scripts, device software images, device configuration files, etc.

If you have an external Oracle database, you must back it up as described in your Oracle documentation. The following topics explain the backup and restore mechanism, its configurable points, and how to use the tools provided with Prime Network:

- [Checking Backup Mechanism Defaults, page 2-6](#)
- [Backing Up and Restoring Data Stored on the Gateway, page 2-7](#)
- [Backing Up and Restoring the Embedded Oracle Database, page 2-10](#)

## Checking Backup Mechanism Defaults

Prime Network performs regular backups for Prime Network gateway data and the embedded Oracle database.



### Note

External Oracle databases are not backed up; use your vendor documentation to set up this type of backup. For information on the Infobright database used by Operations Reports, refer to the [Cisco Prime Network 4.3 Operations Reports User Guide](#).

The schedule, number of backups saved, and backup location for Prime Network gateway data and embedded Oracle database are described in [Table 2-1](#).

**Table 2-1** Default Backup Characteristics

Characteristic	Gateway Data	Embedded Oracle Database Data
What is backed up	Registry data, encryption keys, reports, user-specified data (see <a href="#">Table 2-2</a> ).	All active and archived data.
Backup schedule	Data is backed up every 12 hours at 4:00 a.m. and 4:00 p.m., as defined in the crontab file.  To modify this schedule see, <a href="#">Changing the Gateway Data Backup Schedule, page 2-8</a> .	Depends on the profile selected at installation: <ul style="list-style-type: none"> <li>• 1-20 actionable events<sup>1</sup> per second—Full backup is performed every Saturday at 1:00 a.m.; incremental backups are performed Sunday-Friday at 1:00 a.m.</li> <li>• 21-250 actionable events per second—Full backup is performed every Tuesday and Saturday at 1:00 a.m.</li> </ul> To modify this schedule see, <a href="#">Changing the Embedded Oracle Database Backup Schedule, page 2-12</a> .

R

**Table 2-1** Default Backup Characteristics (continued)

Characteristic	Gateway Data	Embedded Oracle Database Data
Number of saved backups	16 backups for a system installed with an embedded Oracle database. 5 backups for a system installed with an external Oracle database	Backups taken in last two days. <b>Note</b> You should back up this information to tape on a daily basis.
Backup location	<i>NETWORKHOME</i> /backup ( <i>NETWORKHOME</i> is the installation directory). You can change this setting by editing the registry. See <a href="#">Changing the Backup Location for Gateway Data</a> , page 2-8.	Depends on the location specified at installation time. You cannot modify the location.

1. *Actionable events* are events that are of interest to Prime Network. For more details about actionable events, see [How Prime Network Handles Incoming Events](#), page 9-1.

## Backing Up and Restoring Data Stored on the Gateway

Prime Network gateway information consists of registry data, encryption keys, reports, and any other user-specified data stored on the gateway server. To back up *only* the gateway data, use the **backup.pl** and **restore.pl** commands. (For embedded Oracle database installations, the **emdbctl** command cannot be used to backup or restore only the gateway.)

Prime Network backs up its registry data, encryption keys, and reports using the operating system cron mechanism. [Table 2-2](#) lists the directories that are backed up.

You can manually back up this data using the **backup.pl** command or, if you have an embedded Oracle database, the **emdbctl --backup** command. (If you use **emdbctl --backup**, Prime Network will also back up the embedded Oracle database.)

**Table 2-2** Gateway Directories Backed Up by Prime Network

Type of Data	Location	Description
Registry information	<i>NETWORKHOME</i> /Main/registry	Prime Network registry, which includes changes made since the installation (new soft properties, Command Manager and Command Builder command scripts, alarm customizations, and so forth)
General information	<i>NETWORKHOME</i> /Main/.encKey	SSH encryption key files
	<i>NETWORKHOME</i> /Main/to_backup	Other user-specified data
	<i>NETWORKHOME</i> /Main/reportfw/rptdocument	Prime Network reports <sup>1</sup>

1. Some report data is stored in the Oracle database, so you must back up both the Oracle database and the Prime Network data to capture all report information.

These topics describe how to use **backup.pl** and **restore.pl**:

- [Changing the Backup Location for Gateway Data](#), page 2-8
- [Changing the Gateway Data Backup Schedule](#), page 2-8

- [Performing a Manual Backup of Gateway Data, page 2-9](#)
- [Restoring Gateway Data, page 2-9](#)

## Changing the Backup Location for Gateway Data

If you need to change the backup directory for the Prime Network gateway data, use the **runRegTool** script to change the setting in the registry.

Make sure that *pnuser* has the necessary write permissions for the new backup directory, as in the following:

```
drwx-----  2 pn41  pn41  512 Sep 24 02:54
```

To change the default backup directory, log into the gateway server as *pnuser* and execute the following command, specifying a complete directory path for *new-directory*:

```
# ./runRegTool.sh -gs 127.0.0.1 set 0.0.0.0
"site/mmvm/agents/integrity/backup/backupOutputFolder" new-directory
```



### Note

- Do not locate the backup directory under /tmp, since this directory is deleted whenever the server is rebooted, and the backed-up content would be lost.
- To maximize data safety, copy the backed-up directory to an external storage location, such as a DVD or a disk on a different server.

## Changing the Gateway Data Backup Schedule

Prime Network runs backups and integrity tests according to the settings in the system crontab file.



### Note

If you change the schedule, it will affect when other system stability tests are run. See [How the Data Purging Mechanism Works, page 8-4](#).

The integrity service runs regular backups, along with other integrity tests, according to the settings in the system crontab file. Registry backups are controlled according to commands in the crontab file. The crontab file consists of lines, where each line contains six fields:

*min hour day-of-month month-of-year day-of-week command*

The fields are separated by spaces or tabs. The first five integer patterns can contain the following values:

Field	Acceptable Values
min	Minute in range 0-59
hour	Hour in range 0-23
day-of-month	Day in range 1-31
month-of-year	Month in range 1-12
day-of-week	Day in range 0-6 (0=Sunday).
command	Command



To specify days using only one field, set the other fields to \*. For example, `0 0 * * 1` runs a command only on Mondays.

In the following example, core files are cleaned up every weekday morning at 3:15 a.m.:

```
15 3 * * 1-5 find $HOME -name core 2>/dev/null | xargs rm -f
```

The sequence `0 0 1,15 * 1` runs a command on the first and fifteenth of each month as well as every Monday.

To change when Prime Network backs up its data:

- 
- Step 1** Log into the gateway as *pnuser*.
- Step 2** Edit the cron table as follows:
- ```
# crontab -e
```
- Step 3** Make your changes to the crontab file and save them.
- 

## Performing a Manual Backup of Gateway Data

This procedure explains how to perform an on-demand backup of the Prime Network gateway data. This procedure does not back up any database information. (If you want to perform a manual backup of *both* gateway and embedded Oracle database information, see [Performing a Manual Backup of the Embedded Oracle Database, page 2-12](#).) To backup an external Oracle database, see your Oracle documentation; Prime Network does not provide tools to back up an external Oracle database.

- 
- Step 1** Log into the gateway as *pnuser* and change to the Main/scripts directory:
- ```
# cd $ANAHOME/Main/scripts
```
- Step 2** Start the backup:
- ```
# backup.pl backup-folder
```



**Note** It is normal for null to appear in response to this command.

---

## Restoring Gateway Data



**Note** To restore an external Oracle database, refer to your Oracle documentation.

---

Use this procedure to restore Prime Network gateway data from a backup. If you have an embedded Oracle database, you can restore both the Prime Network data *and* the embedded Oracle database data at the same time using the **emdbctl** command (see [Restoring Prime Network Embedded Oracle Database \(With or Without Gateway Data\), page 2-13](#)).

- 
- Step 1** Log into the gateway as *pnuser* and change to the Main directory.
- ```
# cd $ANAHOME/Main
```
- Step 2** Stop the gateway server and all units:
- ```
# networkctl stop
# rall.csh networkctl stop
```
- Step 3** From the *NETWORKHOME/Main* directory, change to the directory *NETWORKHOME/Main/scripts*:
- ```
# cd NETWORKHOME/Main/scripts
```
- Step 4** Execute the restoration script:
- ```
# restore.pl backup-folder
```
- Step 5** Once the restoration is successful, initialize the Prime Network gateway by running the following commands:
- ```
# cd Main
# networkctl restart
```
- 

## Backing Up and Restoring the Embedded Oracle Database



### Note

If you have an external Oracle database, you must perform the backup as described in your Oracle documentation.

---

Prime Network provides native tools for managing an embedded Oracle database. Once you have enabled the backup mechanism, Prime Network backs up the embedded Oracle database and gateway data on a regular basis according to your database profile. (If you do not remember your profile setting, see [Retrieving Your Embedded Oracle Database Profile Setting from the Registry](#), page 8-19.)

The **emdbctl** command is the main tool you use to manage an embedded Oracle database. Whenever you perform a manual backup of the embedded Oracle database using **emdbctl**, Prime Network also backs up the Prime Network gateway data—that is, registry data, encryption keys, reports, and any other user-specified data stored on the gateway server. If you want to back up *only* the Prime Network gateway data, see [Performing a Manual Backup of Gateway Data](#), page 2-9.

You can also use the **emdbctl** command to:

- Restore *only* the embedded Oracle database
- Restore the embedded Oracle database *and* gateway data

See these topics for more information:

- [Enabling Embedded Oracle Database Backups](#), page 2-11
- [Changing the Embedded Oracle Database Backup Schedule](#), page 2-12
- [Performing a Manual Backup of the Embedded Oracle Database](#), page 2-12
- [Restoring Prime Network Embedded Oracle Database \(With or Without Gateway Data\)](#), page 2-13

## Enabling Embedded Oracle Database Backups

When you enabled the backup mechanism for an embedded Oracle database deployment, Prime Network schedules automated backups of both the embedded Oracle database *and* gateway data. The **emdbctl** command will call the **backup.pl** command to back up the gateway data. Backups are normally enabled during installation, but if you did not enable them, use this procedure to do so. You must enable this mechanism regardless of whether you want to perform backups manually or automatically. You can verify whether the backup mechanism is already enabled by checking the backup directory for recent backups.



### Note

This procedure requires both Oracle and Prime Network to be restarted.

### Before You Begin

The script will prompt you for the following information:

- The destination folders for the backup files and the archive log
- Your database profile. If you do not remember it, you can retrieve it as described in [Retrieving Your Embedded Oracle Database Profile Setting from the Registry](#), page 8-19.

To enable the backup mechanism for an embedded Oracle database deployment:

- Step 1** If you did not specify a backup location at installation time, do the following:
- a. Create the folders for the backup files and the archive logs.
  - b. Verify that the OS database user (**oracle**, by default) has write permission for the folders, or run the following command as the operating system root user:

```
chown -R os-db-user:oinstall path
```

- Step 2** Log into the gateway as *pnuser* and change the directory to the Main/scripts/embedded\_db directory:

```
# cd $ANAHOME/Main/scripts/embedded_db
```

- Step 3** Start the backup.

```
# emdbctl --enable_backup
```

The following is an example of a complete **--enable\_backup** session.

```
# emdbctl --enable_backup
```

```

Reading Prime Network registry
- Enter the destination for the backup files: /export/home/oracle/backup
You must create the target destination (path-to-backup-dir) before you continue
Verify user oracle has writing permissions on this destination or run the following
command as the OS root user:
chown -R <database-OS-user>oinstall <path>
Hit the 'Enter' key when ready to continue or 'Ctrl C' to quit
- Enter the destination for the archive log: /export/home/oracle/arch
- How would you estimate your database profile?
-----
1) 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 - 7) [default 1] 1
Updating Prime Network registry
Stopping Prime Network
Stopping NCCM DM Server...
- DM server is up, about to shut it down
Stopping AVMs...Done.
Configuring the database's automatic backup procedure
Starting Prime Network
Starting MVM.....Done.
```

---

## Changing the Embedded Oracle Database Backup Schedule

Use this procedure to change the embedded Oracle database backup time using **emdbctl** command.

**Step 1** Log into the gateway as *pnuser* and change the directory to the `Main/scripts/embedded_db` directory:

```
# cd $ANAHOME/Main/scripts/embedded_db
```

**Step 2** Change the embedded Oracle database backup time from 1:00 a.m. (the default) to 3:19 a.m.:

```
# emdbctl --change_backup_time
Reading Prime Network registry
Configuring the DB backup time
Please enter the new hour for the DB Backup      (0..23)   :3
Please enter the new minute for the DB Backup    (0..59)   :19
DB backup time was changed successfully
```

---

For more information on the **emdbctl** command, see [Stopping, Starting, and Changing Oracle Embedded Database Settings \(emdbctl Utility\)](#), page 8-17.

---

## Performing a Manual Backup of the Embedded Oracle Database



### Note

If you have an external Oracle database, you must perform the backup as described in your Oracle documentation.

---

This procedure explains how to perform an on-demand backup of a Prime Network embedded Oracle database using the **emdbctl** command. Whenever you use **emdbctl** to do a manual backup, Prime Network also backs up the Prime Network gateway data—that is, registry data, encryption keys, reports, and any other user-specified data stored on the gateway server (by calling the **backup.pl** command.) If you want to back up *only* the Prime Network gateway data, see [Performing a Manual Backup of Gateway Data](#), page 2-9.

### Before You Begin

The automatic backup mechanism must be enabled. If you did not enable it during the installation, follow the directions in [Enabling Embedded Oracle Database Backups](#), page 2-11.

**Step 1** Log into the gateway as *pnuser* and change the directory to the `Main/scripts/embedded_db` directory:

```
# cd $ANAHOME/Main/scripts/embedded_db
```

**Step 2** Start the backup:

```
# emdbctl --backup
  Reading Prime Network registry
  Backing up the database
  Backing up Prime Network
```

For more information on the `emdbctl` command, see [Stopping, Starting, and Changing Oracle Embedded Database Settings \(emdbctl Utility\)](#), page 8-17.

## Restoring Prime Network Embedded Oracle Database (With or Without Gateway Data)



### Note

If you have an external Oracle database, you must restore data as described in your Oracle documentation.

This procedure explains how to perform an on-demand restore of a Prime Network embedded Oracle database using the `emdbctl` command. When you perform a manual restore using `emdbctl`, you can restore both the embedded Oracle database *and* gateway data (`emdbctl --restore`), or *only* the embedded Oracle database (`emdbctl --restore_db`). If you want to restore *only* the gateway data, see [Restoring Gateway Data](#), page 2-9.

If you are going to restore both the Oracle database and gateway data, remember that embedded Oracle database backups are scheduled according to the database size. They can be restored to any hour within the last 8 days, as described in [Table 2-1 on page 2-6](#). However, Prime Network gateway data is backed up twice a day at 4:00 a.m. and 4:00 p.m. and can be restored to *only* those points in time. (The `emdbctl` command actually calls the `backup.pl` command to back up gateway data, and the `restore.pl` command to restore gateway data.) Therefore, find out the time and date of the latest Prime Network *data* backup, and restoring the data and your Oracle database to that time.

You do not have to stop Prime Network, the Oracle database, or any other processes before performing the restore operation. The script will do this for you. You can use this restore procedure even if the Oracle database is down.

**Step 1** Log into the gateway as *pnuser* and change to the directory `NETWORKHOME/Main/scripts/embedded_db`:

```
# cd $ANAHOME/Main/scripts/embedded_db
```

**Step 2** Run the restoration script as follows:

Command	Restores:
<code>emdbctl --restore</code>	Embedded Oracle database and gateway data
<code>emdbctl --restore_db</code>	Embedded Oracle database only

```
# ./emdbctl --restore
```

This example restores the embedded Oracle database and all Prime Network data to the state it was in on January 10, 2013 at 4:00 a.m.

```

Please enter the date and time information for the restore process
Restore year (YYYY) :2013
Restore month (1..12) :1
Restore day (1..31) :10
Restore hour (0..23) :4
Restore minute (0..59) :00
Selected Restore time (MM-DD-YYYY HH:MI): 01-10-2013 04:00
In case of a wrong or impossible date for restore, the DB will be restored to the latest
possible point in time
Do you want to continue (Y/N) ?Y
Stopping Prime Network
Stopping AVMs...Done.
Restoring the database to 01-10-2013 04:00
Successfully restored the database!
Restoring Prime Network
Enter Prime Network's backup directory (the default location is
$ANAHOME/backup/date+time): /export/home/pn41/backup/20130110040
Checking that the system is down...
Prime Network not running on the gateway
Backup_dir: /export/home/pn41/backup/201301100400
Backing-up current registry to /export/home/pn41/backup_before_restore.jar
Restoring registry
Restoring to_backup
Before restoring encryption key, backing up last installation encryption key
Restoring encryption key
Before restoring reports, backing up current reports
Restoring reports
Setting Main/registry ownership
Setting Main/reportfw/rptdocument ownership
Done
Would you like to start Prime Network? (yes,no) [default yes] no

```

**Step 3** Once all of your data is restored, restart the gateway.

## Tracking Changes to the Product Image and VNEs

The following table shows from where you can get historical information concerning changes to the product image and VNEs.

For historical events related to:	See:
Installation-related changes, including changes to VNEs	AVM and other appropriate log files (see <a href="#">Log Files Reference, page C-3</a> )
Backup and restore operations	The following reports, which you can launch from the main menu by choosing <b>Reports &gt; Run Report &gt; Events Reports &gt; Detailed Non-Network Events:</b>
Enable/disable feature operations	
	<ul style="list-style-type: none"> <li>Detailed System Events</li> <li>Detailed Security Events</li> </ul>