CHAPTER 2

Manage the Prime Network Software Image and Backups

These topics explain how to manage the Prime Network software. This includes the base image, licenses, patches, and VNE driver jar files. These topics also describe how to use the backup and restore mechanism for both embedded and external databases.

Get Information About the Basic Image and Licenses

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

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 **pn310**. 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 **pn310** and used the default installation directory, the Prime Network installation directory would be /export/home/pn310.
- The ANAHOME environment variable is set to the Prime Network installation directory. For example:

```
# echo $ANAHOME
/export/home/pn310
```

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, see *Cisco Prime Network 3.10 Installation Guide*.

Step 1 Log into the gateway server as *network user*.

Step 2 Enter the following:

```
# networkctl status

------------------------------------------------------------------------------
.-= Welcome to sjcn-sysm, running Cisco Prime Network gateway (v3.10.0 (build583)) =-.
------------------------------------------------------------------------------
...
```

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

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

Options/Arguments	Description
start	Starts the gateway process. With no options, this command starts the gateway and all component processes.
stop	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 Change AVM Status (Start or Stop), page 3-33.
status	Displays the status of the gateway processes.
restart	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 Disable Prime Network Automatic Restarts, page 3-23.

This example shows the full output of a **networkctl status** command. In the following example, the user has created AVM 751 and AVM 851. (AVMs number 1-100 are reserved for use by Prime Network.)

```
# networkctl status

------------------------------------------------------------------------------
.-= Welcome to sjcn-sysm, running Cisco Prime Network gateway (v3.10.0 (build583)) =-.
------------------------------------------------------------------------------

+ Checking for services integrity:
  - Checking if host's time server is up and running                [OK]
  - Checking if webserver daemon is up and running                  [OK]
  - Checking if secured connectivity daemon is up and running       [OK]
  - Checking if license server is up and running                    [OK]
  - Checking Prime Network Web Server Status                        [UP]
+ Detected AVM99 is up, checking AVMs
  - Checking for AVM19's status                                     [DISABLED]
  - Checking for AVM76's status                                     [OK 0/129]
  - Checking for AVM66's status                                     [OK 6/232]
```

```
- Checking for AVM11's status                                    [OK 0/987]
- Checking for AVM851's status                                   [OK 29/10618]
- Checking for AVM83's status                                    [OK 0/108]
- Checking for AVM751's status                                   [OK 0/16410]
- Checking for AVM55's status                                    [DISABLED]
- Checking for AVM100's status                                   [OK 0/69]
- Checking for AVM0's status                                     [OK 0/178]
- Checking for AVM25's status                                    [OK 0/488]
- Checking for AVM35's status                                    [OK 0/118]
- Checking for AVM82's status                                    [DISABLED]
- Checking for AVM78's status                                    [OK 0/111]
- Checking for AVM84's status                                    [OK 0/72]
```

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.
EVAL	License service is running with an evaluation license.
DISABLED	AVM has been stopped.

Installed Licenses

Note This feature is disabled if Prime Network is installed with Cisco Prime Central.

Licenses contain keys that are associated with a specific gateway server. The keys cannot be used by any other machines. Licenses are encrypted and are stored on the gateway server in the gateway directory $FLEXNET_HOME (an environment variable which is set at installation). You do not need to copy license files to unit servers.

When the gateway starts, Prime Network validates the license keys on the gateway. The gateway server keeps track of the licenses by communicating with the license validation server (FlexNet server), which is provided with the Prime Network image. Table 2-1 lists the general licensing requirements per Prime Network installation.

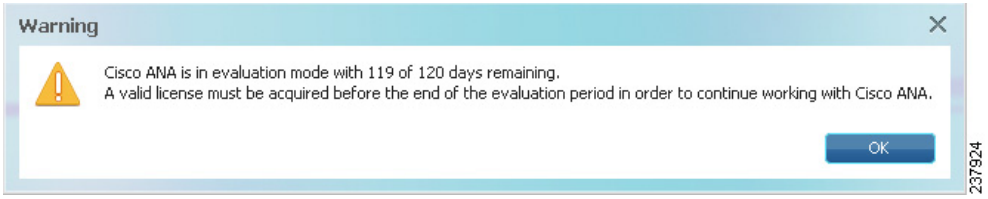
Table 2-1 License Requirements for Different Installation Types

Installation Type	License Requirements
New	Use the PAK number to request the required license keys. See Obtain and Apply Prime Network Licenses, page 2-7.
Upgrade	From Cisco ANA 3.7.x—Reuse the same license keys. From Cisco ANA 3.6.x—Requires a new license file; contact your account representative to get a new license file. You must install it within 120 days of the upgrade.
Gateway High Availability	Purchase the required additional part numbers; contact your Cisco account representative. **Note** For information on gateway high availability licensing requirements, see the *Cisco Prime Network 3.10 Gateway High Availability Guide*.

License Violations

If Prime Network detects a license violation, a warning message is displayed, as illustrated in Figure 2-1.

Figure 2-1 License Warning Message at GUI Login



Check Installed Licenses

To check the status of installed licenses, choose **Global Settings > License Report** from the Administration GUI client. The License Report window provides the following basic license information:

Field	Description	
Date	License Report generation time	
Basic License	License type	
	Production	For production networks (also called a Base license).
	Lab	For lab or staging environments. Supports an unrestricted number of devices (within the product limits). At UI login, the user is notified that the installation is a Lab installation.
	Unlicensed Evaluation	For time-based evaluation period (120 days). At UI login, the number of days remaining in the evaluation period is displayed. If the evaluation period expires and a permanent license is not installed, the gateway will reject all connection requests. When no licenses are installed, the system is treated as an unlicensed evaluation version.

Field	Description
Evaluation Days Remaining	For Unlicensed Evaluation, the number of days remaining (out of 120)

To check the status of the license manager daemon and whether any licenses are installed, log into the Prime Network gateway as *pnuser* and run the **liccontrol** command. (This command does not perform any validation; it just checks for the existence of licenses.)

```
# liccontrol status
Operation requested -> status
License server is up
```

If no license is installed (as in unlicensed evaluation versions), you will see a message similar to the following:

```
# liccontrol status
No license files found in /export/home/ana310/utils/linux/FlexNet/licenses/
```

If you are experiencing licensing problems:

- Check the licensing log file in $FLEX_NET/logs/flexnet.log.
- Try stopping and restarting the license manager and AVM 11. See Stop, Start, and Check the License Server, page 2-9, and Change AVM Status (Start or Stop), page 3-33.
- If you know that licenses are installed but they were not found when using the **liccontrol** command, contact your Cisco account representative. The license file may be corrupted.

Installed VNE Drivers and Device Packages

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 command 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.

Step 1 Log into the gateway server as *network user*.

Step 2 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-3.10-DP0
  - Third party:  No third party device package installed.
```

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 Add New Device Support by Installing Device Packages, page 4-26.

Update the Prime Network Image, Database, and Licenses

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

Install 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.

Install Prime Network Device Packages

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 activation 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.

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**. (Drivers for non-Cisco devices are also provided on this site.)

Step 4 If you want to install a DP, follow the instructions in Download and Install New Driver Files, page 4-30.

Obtain and Apply Prime Network Licenses

Note This feature is disabled if Prime Network is installed with Cisco Prime Central.

The Prime Network licensing mechanism is described in Installed Licenses, page 2-3. These topics explain how to obtain and install license files and check the health of the licensing feature.

- Obtain a License File with Keys, page 2-7
- Install and Apply Licenses, page 2-8
- Stop, Start, and Check the License Server, page 2-9

Note If you are using gateway high availability, see the licensing information in the *Cisco Prime Network 3.10 Gateway High Availability Guide*.

Obtain a License File with Keys

Note This topic only applies to new installations.

To obtain a license file with the required license keys, register your Prime Network software on Cisco.com.

Step 1 Go to the licensing web page at http://www.cisco.com/go/license and enter your Cisco.com user credentials to enter the Product License Registration process. (If you are not a registered Cisco.com user, create an account.)

Step 2 Enter the following information:

Required Information	Description
PAK number	Product Authorization Key which is listed on the Software License Claim Certificate. A PAK number is an automatically-generated identification key that represents the specific software and hardware covered by the license.
Gateway server name	Name returned when you run the **hostname** command on the Prime Network gateway server.
Gateway server host ID	ID returned when you run the **hostid** command on the Prime Network gateway server. **Note** For systems running Linux, use the primary MAC address.
Operator e-mail	E-mail address where the license information should be sent.

Step 3 Click **Submit**. When you receive the file, follow the procedure in Install and Apply Licenses, page 2-8.

Caution Do not edit the contents of the .lic file in any way. The contents of the file are signed and must remain intact.

Install and Apply Licenses

When you receive the license file, install it on the Prime Network gateway server within 120 days after installation. The license file is held and managed by the FlexNet license validation server, which is provided with the Prime Network image. You do not need to install anything on your unit servers.

If you are using gateway high availability, see the licensing information in the *Cisco Prime Network 3.10 Gateway High Availability Guide*.

Use the following procedure to install and update license files.

Step 1 Log into the Prime Network gateway as *pnuser*.

Step 2 Copy the license file (*.lic) to $FLEXNET_HOME/licenses. (This environment variable is set at installation time.)

```
# cp licensefile.lic $FLEXNET_HOME/licenses
```

Step 3 Read and activate the license with the license manager.

```
# liccontrol reread
```

Step 4 Apply the license to the Prime Network gateway process (which runs on AVM 11):

```
# networkctl -avm 11 restart
```

If you are experiencing licensing problems:

- Check the licensing log file in $FLEX_NET/logs/flexnet.log.
- Try stopping and restarting the license manager and AVM 11. See Stop, Start, and Check the License Server, page 2-9, and Change AVM Status (Start or Stop), page 3-33.
- If you know that licenses are installed but they were not found when using the **liccontrol** command, contact your Cisco account representative. The license file may be corrupted.

Stop, Start, and Check the License Server

The **liccontrol** command manages the FlexNet license validation server. To stop and restart the license server, use **liccontrol stop** and **liccontrol start**. If no license files installed, the license server will not start.

You can also get general information using the **networkctl status** command. Prime Network will return a line similar to the following:

```
Checking if license server is up and running     [ status ]
```

status can be any of the following:

Status	Description
OK	A license file was found and the license server is up and running.
LOADED	The license server is starting. If it remains LOADED and does not change to OK, there might be a problem with the license file. Contact your Cisco account representative.
NO LICENSE	No license file exists; the license server is not started.
ERROR	A problem occurred while starting the license server.

Back Up and Restore Process

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 database—Faults, events, workflows, activations, device software images, device configuration files, etc.

Prime Network performs regular backups of gateway and database information—but *databases* are only backed up by Prime Network if they are embedded (not external). If you have an external 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:

- Overview of the Backup Mechanism, page 2-10
- Gateway Backup and Restore, page 2-10, explains how to manage backup and restore for information stored on the gateway (external database installations).
- Prime Network Embedded Database Backup and Restore, page 2-14, explains how to manage backup and restore for a Prime Network embedded database.

Overview of the Backup Mechanism

Prime Network performs regular backups for both Prime Network data and, if installed, an embedded database.

Note External databases are not backed up; use your vendor documentation to set up this type of backup.

The schedule, number of backups saved, and backup location for Prime Network and database backup are described in Table 2-2.

Table 2-2 Default Backup Characteristics

Characteristic	Embedded Database Data	Gateway Data
What is backed up	Database and archive files	Registry data, encryption keys, reports, user-specified data (see Table 2-3)
Backup schedule	Depends on the profile selected at installation: • 1-50 actionable events per second—Full backup is performed every Saturday at 1:00 a.m.; incremental backups are performed Sunday-Friday at 1:00 a.m. • 51-250 actionable events per second—Full backup is performed every Tuesday and Saturday at 1:00 a.m. To modify this schedule see, Change the Embedded Database Backup Schedule, page 2-15.	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, Change the Gateway Data Backup Schedule, page 2-12.
Number of saved backups	Backups taken in last 8 days. **Note** You should back up this information to tape on a daily basis.	5 backups for a system installed with an external database, and 16 backups for a system installed with an embedded database.
Backup location	Depends on the location specified at installation time. You cannot modify the location.	*NETWORKHOME*/backup (*NETWORKHOME* is the installation directory). You can change this setting by editing the registry. See Change the Backup Location for Gateway Data, page 2-11.

Gateway Backup and Restore

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 database installations, the **embdctl** command cannot be used to backup or restore only the gateway.) These topics describe how to use **backup.pl** and **restore.pl**:

- Prime Network Data That is Backed Up, page 2-11
- Change the Backup Location for Gateway Data, page 2-11
- Change the Gateway Data Backup Schedule, page 2-12
- Perform a Manual Backup of Gateway Data, page 2-13
- Restore Gateway Data, page 2-13

Prime Network Data That is Backed Up

Prime Network backs up its registry data, encryption keys, and reports using the operating system cron mechanism. Table 2-3 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 database, the **embdctl --backup** command. (If you use **embdctl --backup**, Prime Network will also back up the embedded database.)

Table 2-3 Directories Backed Up by Prime Network

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

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

Change 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 pn310    pn310    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.

Change the Gateway Data Backup Schedule

Prime Network runs the backup according to the settings in the system crontab file. To change the backup time, edit the 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 8-6.

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 contain 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 are integer patterns that 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* (where *pnuser* is the operating system account for the Prime Network application, created when Prime Network is installed; for example, **pn310**).

Step 2 Edit the cron table as follows:

```
# crontab -e
```

Step 3 Make your changes to the crontab file and save them.

Perform 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 database information, see Perform a Manual Backup of the Embedded Database, page 2-16.) To backup an external Oracle database, see your Oracle documentation; Prime Network does not provide tools to backup an external database.

Step 1 Log into the gateway as *pnuser* and change the directory 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.

Restore Gateway Data

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

Use this procedure to restore Prime Network gateway data from a backup. If you have an embedded database, you can restore both the Prime Network data *and* the embedded database data at the same time using the **emdbctl** command (see Restore Prime Network Embedded Database Alone or With Gateway Data, page 2-16).

Step 1 Log into the gateway as *pnuser*.

Step 2 Stop the gateway server and all units:

```
# cd $ANAHOME/Main
# 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
```

Prime Network Embedded Database Backup and Restore

The Prime Network **emdbctl** command provides backup and restore tools for deployments with embedded databases. Once you have enabled the backup mechanism, Prime Network backs up the embedded database and gateway data on a regular basis according to your database profile.

Whenever you perform a manual backup of the embedded database using **emdbctl**, Prime Network also backups 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 Perform a Manual Backup of Gateway Data, page 2-13.

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

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

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

- Enable Embedded Database Backups, page 2-14
- Change the Embedded Database Backup Schedule, page 2-15
- Perform a Manual Backup of the Embedded Database, page 2-16
- Restore Prime Network Embedded Database Alone or With Gateway Data, page 2-16

Enable Embedded Database Backups

When you enabled the backup mechanism for an embedded database deployment, Prime Network schedules automated backups of both the embedded 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 will 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.

To enable the backup mechanism for an embedded 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.
```

Change the Embedded Database Backup Schedule

Use this procedure to change the embedded 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 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 **embdctl** command, see Stop, Start, and Change Embedded Database Settings (embdctl Utility), page 8-18.

Perform a Manual Backup of the Embedded Database

Note If you have an external 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 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 Perform a Manual Backup of Gateway Data, page 2-13.

Before You Begin

The automatic backup mechanism must be enabled. If you did not enable it during the installation, follow the directions in Enable Embedded Database Backups, page 2-14.

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 **embdctl** command, see Stop, Start, and Change Embedded Database Settings (embdctl Utility), page 8-18.

Restore Prime Network Embedded Database Alone or With Gateway Data

Note If you have an external 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 database using the **emdbctl** command. When you perform a manual restore using **emdbctl**, you can restore the database and gateway data (**emdbctl --restore**), or only the database (**emdbctl --restore_db**). If you want to restore *only* the gateway data, see Restore Gateway Data, page 2-13.

If you are going to restore both the database and gateway data, remember that embedded 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 2-2 on page 2-10. 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 **embdctl** 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 database to that time.

You do not have to stop Prime Network, the 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 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:
embdctl --restore	Embedded database and gateway data
embdctl --restore_db	Embedded database only

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

This example restores the embedded database *and* all Prime Network data to the state it was in on May 10, 2012 at 4:00 a.m.

```
Please enter the date and time information for the restore process
Restore year (YYYY) :2012
Restore month (1..12) :5
Restore day (1..31) :10
Restore hour (0..23) :4
Restore minute (0..59) :00
Selected Restore time (MM-DD-YYYY HH:MI): 05-10-2012 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 05-10-2012 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/pn310/backup/20120510040
Checking that the system is down...
Prime Network not running on the gateway
Backup_dir: /export/home/pn310/backup/201205100400
Backing-up current registry to /export/home/pn310/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.

Track 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.

Information Type	Refer to:
Installation-related changes, including changes to VNEs	The appropriate logs. (A complete list of logs is provided in Log Files, page B-3
Backup and restore operations Licensing events	Detailed Non-Network Events reports (choose **Reports > Run Report > Events Reports** from main menu).