Installing and Upgrading Cisco Prime Network Registrar

This chapter contains the following sections:

Installing Cisco Prime Network Registrar

Starting from Cisco Prime Network Registrar 11.0, there are no configuration questions asked during the installation. Also, it no longer asks for admin credentials and licensing details. You must provide these details when you connect to Cisco Prime Network Registrar for the first time (see Using Cisco Prime Network Registrar).

Note that the following paths are used:

- Program files—/opt/nwreg2/{local | regional}

Warning You should NOT add or modify files in the /opt/nwreg2/* directories as these will be overwritten during upgrades or installations. You should add or modify the files only in the /var area. For example, you should add the extensions in the /var/nwreg2/local/extensions area and not in the /opt area.

- Data files—/var/nwreg2/{local | regional}/data
- Log files—/var/nwreg2/{local | regional}/logs
- cnr.conf file—/var/nwreg2/{local | regional}/conf

Also, Cisco Prime Network Registrar 11.1 installation configures the following by default:

- Type of web security—HTTPS only (default port, 8443 for local and 8453 for regional)
- Web services—REST API enabled (on HTTPS port, no separate port)
- Security mode—Required
- SCP Port number—CCM on default port (1234 for local and 1244 for regional)
- Run as root—Cisco Prime Network Registrar always runs as root, but with reduced permissions.
- Type of installation (local, regional, or client-only)—Depends on the RPM kit used. Following RPM kits are available for Cisco Prime Network Registrar 11.1:

Table 1: RPM Kits

	RHEL/CentOS 7.3 and later	**RHEL 8.x/AlmaLinux 8.6**
Regional cluster	cpnr-regional-11.1.x-1.el7*.x86_64.rpm	cpnr-regional-11.1.x-1.el8*.x86_64.rpm
Local cluster	cpnr-local-11.1.x-1.el7*.x86_64.rpm	cpnr-local-11.1.x-1.el8*.x86_64.rpm
Client only	cpnr-client-11.1.x-1.el7*.x86_64.rpm	cpnr-client-11.1.x-1.el8*.x86_64.rpm
x in the kit name indicates the Cisco Prime Network Registrar minor version. * in the kit name indicates the RHEL minor version that the package was forked from.		

- Create a superuser administrator during first login (see Using Cisco Prime Network Registrar).

The following steps are applicable for the new installations. To upgrade from earlier versions of Cisco Prime Network Registrar to 11.1, see Upgrading Cisco Prime Network Registrar, on page 5.

To install Cisco Prime Network Registrar, do the following:

Step 1 Log in to the target machine.

Caution Many distributions of Red Hat, AlmaLinux or CentOS come with a firewall and connection tracking installed and enabled by default. Running a stateful firewall on the DNS server's operating system causes significant decrease in the server performance. Cisco strongly recommends **NOT** to use a firewall on the DNS server's operating system. If disabling the firewall is not possible, then connection tracking of DNS traffic MUST be disabled. For more information, see the *"DNS Performance and Firewall Connection Tracking" section in the Cisco Prime Network Registrar 11.1 Administration Guide*.

Step 2 Install the OpenJDK 11 if you have not already done so. Use the following command:

```
# yum install java-11-openjdk
```

Note that on some systems, you must use the **dnf install** command.

Step 3 Download the distribution file (RPM kit) from Cisco.com as per your requirement. For the list of RPM kits available for Cisco Prime Network Registrar 11.1, see Table 1: RPM Kits above.

Cisco Prime Network Registrar 11.1 installs both client and server by default. For client only installation, use the appropriate kit as listed in Table 1: RPM Kits above.

Note Choose client only installation in a situation where you want the client software running on a different machine than the protocol servers. You must then set up a connection to the protocol servers from the client.

Step 4 Navigate to the directory in which you saved the downloaded distribution file.

Step 5 Install Cisco Prime Network Registrar using any of the following commands:

```
# yum install filename
```

OR

```
# rpm -i filename
```

OR

```
# dnf install filename
```

Where *filename* is the RPM kit name as listed in Table 1: RPM Kits, on page 2.

Note that the RHEL/CentOS 7.3 and later kits have "el7*" in the name and the RHEL 8.x kits have "el8*", where * is the RHEL minor version that the package was forked from.

For example, to install the regional cluster on RHEL/CentOS 7.3 and later, use any of the following commands:

```
# yum install cpnr-regional-11.1-1.el7_9.x86_64.rpm
```

OR

```
# rpm -i cpnr-regional-11.1-1.el7_9.x86_64.rpm
```

OR

```
# dnf install cpnr-regional-11.1-1.el7_9.x86_64.rpm
```

Note Since a regional server is required for license management, install the regional server first so that you can register the local to the regional.

Step 6 Start the Cisco Prime Network Registrar server agent using the following commands (or reboot the system as Cisco Prime Network Registrar is configured to start automatically):

For the local cluster:

```
# systemctl start nwreglocal
```

For the regional cluster:

```
# systemctl start nwregregional
```

During start-up, the /var/nwreg2/{local | regional} folder is created. The keystore file is created in the /var/nwreg2/{local | regional}/conf/priv folder and the keystore details are updated in the cnr-priv.conf file.

If you want to use your own certificate, see Installing Your Own Certificate for Web UI Access, on page 10.

Step 7 Verify the status of the Cisco Prime Network Registrar servers. Run either of the following commands:

`# ./cnr_status` (available in the *install-path*/usrbin directory)

OR

`# systemctl status nwreglocal` (for the local cluster)

`# systemctl status nwregregional` (for the regional cluster)

After the installation is complete, follow the steps in Using Cisco Prime Network Registrar to start using Cisco Prime Network Registrar. Make sure NOT to modify or add anything in the /opt folder as these files may be overwritten by a future upgrade. You can make changes in the /var folder.

Upgrade Considerations

Cisco Prime Network Registrar 11.1 supports direct upgrades from 9.0 and later.

Cisco Prime Network Registrar 11.1 can run on Red Hat/CentOS 7.3 and later, or on RHEL 8.x/AlmaLinux 8.6. If you are using an earlier version of the operating system, you will first need to upgrade your system to a supported version.

When you install the software, the installation program automatically detects an existing version and upgrades the software to the latest release. Archive the existing Cisco Prime Network Registrar data. If the upgrade fails and fails to start, then you should recover the backup that you made (and perhaps install the old Cisco Prime Network Registrar version). You can also find the backup of the data in the /var/nwreg2/{local | regional} directory, called **upgrade-backup-***date***.tar.gz**. If you did not create your own backup, you can use this backup to restore the databases.

The eventstore is no longer used to track the pending DNS updates. DHCPv4 lease objects are used for this purpose, similar to DHCPv6 DNS updates where leases are used. Therefore, when upgrading from Cisco Prime Network Registrar 10.x or earlier, it is best to upgrade when the DNS update backlog is low as any pending DHCPv4 DNS updates will be lost. The DHCP server logs the DNS update events that it drops using the log message 19669. This will report the lease, pending action, FQDNs, and DNS Update Configuration objects involved for each pending event. These are only logged once as the server removes these events from the eventstore.You can determine the DNS update backlog using the **dhcp getRelatedServers** command and by examining the "requests" count for the DNS servers.

Using Smart Licensing

Cisco Prime Network Registrar 11.x regional, working in Smart License mode, does not support pre-11.0 local clusters. Hence, you must perform the following steps to move to Smart Licensing:

Step 1 Upgrade the Cisco Prime Network Registrar regional cluster to 11.x and disable Smart Licensing (post upgrade). To disable Smart Licensing, see the *"Disabling Smart Licensing" section in the Cisco Prime Network Registrar 11.1 Administration Guide*.

Step 2 Load the required traditional licenses on the Cisco Prime Network Registrar 11.x regional cluster.

Step 3 Re-register or resync all the local clusters with the upgraded regional cluster.

Warning You must upgrade the Cisco Prime Network Registrar 10.x local clusters to 10.1.1 (or later version) before registering them with the 11.x regional cluster. The 10.x local clusters with lower than 10.1.1 version, have issues registering with the 11.x regional cluster.

Step 4 Upgrade all the local clusters to 11.x as per your schedule.

Step 5 After all the clusters are upgraded to 11.x, you can Enable Smart Licensing on regional if you want to move to Smart Licensing. You should perform this step only if you have required licenses in your Smart Account on the CSSM or Satellite. To enable Smart Licensing, see the *"Enabling Smart Licensing" section in the Cisco Prime Network Registrar 11.1 Administration Guide*.

Upgrading Cisco Prime Network Registrar

One major change introduced starting with Cisco Prime Network Registrar 11.0 is to better separate the distributed files (that is, those installed by the RPM) from those that are data and configuration files specific to your installation. Basically, the /opt/nwreg2 area should not include files that are not provided as part of the installation. Everything that is specific to your installation, should now be in the /var/nwreg2 area.

If you used the default paths when previously installing earlier versions of Cisco Prime Network Registrar, the following files will be automatically relocated the first time you start Cisco Prime Network Registrar after installing Cisco Prime Network Registrar 11.1:

- /opt/nwreg2/{local | regional}/conf/cnr.conf will be moved to /var/nwreg2/{local | regional}/conf
- /opt/nwreg2/{local | regional}/conf/priv (and its contents) will be moved to /var/nwreg2/{local | regional}/conf/priv
- /opt/nrweg2/{local | regional}/conf/cert (and its contents) will be moved to /var/nrweg2/{local | regional}/conf/cert
- Any paths in the cnr.conf and cnr-priv.conf will be updated to reflect this move

If the Cisco Prime Network Registrar data area is not in /var/nwreg2/{local | regional}/data, similar moves are done but the resulting paths will use a new conf directory in the parent directory of the data directory. Or, the files may be left where they are.

Note that after upgrading from earlier versions to Cisco Prime Network Registrar 11.1, the following changes will also occur in addition to the above mentioned changes:

- The nwreglocal.env (for local) or nwregregional.env (for regional) file in the /usr/lib/systemd/system directory is used instead of the /opt/nwreg2/{local | regional}/bin/cnr.env file. Therefore, after installing (before starting Cisco Prime Network Registrar), you may need to review if cnr.env changes (such as for LD_LIBRARY_PATH for extensions) need to be applied to the new .env file.
- The web UI keystore is used if one exists or a new one is generated. The existing priv/cnr-priv.conf is used and relocated to /var/nwreg2/{local | regional}.
- HTTPS is used for web UI and REST instead of HTTP. If no port was previously configured for HTTPS, the default (regional | local) ports are used.
- If REST was disabled in the previous install, it gets enabled after the upgrade. If you want to disable REST API, follow the steps in Disabling REST API after upgrading. If REST was previously using a different port than HTTPS, it is no longer supported and the same port is used for HTTPS (web UI) and REST.

Note From Cisco Prime Network Registrar 10.1 onwards, the keystore password is encrypted by default. Therefore, you do not have to encrypt the keystore password if you are upgrading from 10.1 to 11.0 and later. However, if you are upgrading from pre-10.1 version to 11.0 and later, then you must encrypt the keystore password manually.

To generate the encrypted password, use the encrypt script (**encrypt -s** <*plain-text password*>) present in the *install-path*/usrbin directory. You must update this encrypted password in server.xml and after making the change, you must restart Cisco Prime Network Registrar.

To upgrade to Cisco Prime Network Registrar 11.1:

Step 1 Ensure that your environment meets the current system requirements (see System Requirements).

Step 2 Remove the existing installation using the procedure described in Uninstalling Cisco Prime Network Registrar. Ensure NOT to do the cleanup operations mentioned at the end (that is, retain the data, cnr.conf, and so on).

Step 3 If the old cnr.conf is in *install-path*/conf, you can upgrade without doing anything. If the old cnr.conf is elsewhere, then create a cnr.conf file in the *install-path*/conf directory that contains the following line:

cnr.confdir=*location of the old cnr.conf file*

Step 4 To avoid issues with Java upgrades, we recommend that you set JAVA_HOME variable correctly in your environment. Starting Cisco Prime Network Registrar 11.1.1, if JAVA_HOME is not set the rpm installer will try to search the best possible java by looking into packages in the environment and set that. To further reduce issues with Java upgrades, we highly recommend that you edit your cnr.conf file to replace the cnr.java-home entry path with /usr/bin/java (if this is the path that has the version of Java specified in cnr.conf). You can test this by doing:

```
/usr/bin/java -version
```

and

```
cnr.java-home-path/bin/java -version
```

If the two report the same result, you should change the cnr.java-home path to specify /usr/bin/java. If you do this, updates to Java will not require you to update the cnr.java-home path.

Step 5 Install Cisco Prime Network Registrar 11.1. For installation instructions, see Installing Cisco Prime Network Registrar, on page 1.

Step 6 Start the Cisco Prime Network Registrar server agent using the following commands:

- For the local cluster:

```
# systemctl start nwreglocal
```

- For the regional cluster:

```
# systemctl start nwregregional
```

The upgrade process may take some time depending on the size of the configuration and lease/resource record data, and the version from which you are upgrading. You can view the status using the **systemctl status nwreglocal** (for the local cluster) or **systemctl status nwregregional** (for the regional cluster) command. If this shows "trampoline startup, local mode" (for the local cluster) or "trampoline startup, regional mode" (for the regional cluster), it indicates that the services are up or have started. Follow the steps in Using Cisco Prime Network Registrar to start using Cisco Prime Network Registrar.

If the upgrade fails, you can revert to the earlier Cisco Prime Network Registrar version. For details about reverting to the earlier version, see the Reverting to an Earlier Product Version, on page 7.

Reverting to an Earlier Product Version

The Cisco Prime Network Registrar installation program archives the existing product configuration and data when you upgrade to a newer version. If the upgrade process fails, use the following procedure to revert to the earlier product version and configuration:

Caution To complete this process, you must have access to the product installer and license key or license file for the earlier Cisco Prime Network Registrar version. Any attempt to proceed otherwise may destabilize the product.

If the installer had successfully performed the upgrade but you want to roll back to the earlier version at some later point, this procedure can result in network destabilization and data loss; for example, you will lose updates made to the Cisco Prime Network Registrar database after the upgrade, including DHCP lease data and DNS dynamic updates.

Step 1 Ensure that the archive file **upgrade-backup-***date***.tar.gz** is available in the /var/nwreg2/{local | regional} directory.

Step 2 Uninstall Cisco Prime Network Registrar using the procedure described in the Uninstalling Cisco Prime Network Registrar.

Step 3 Other than the contents of the archive file, delete any remaining files and directories in the Cisco Prime Network Registrar installation paths.

Step 4 Restore the backup (either the one that you created or the archive file that is created in Step 7).

Step 5 Reinstall the original version of Cisco Prime Network Registrar. Ensure that you follow the reinstallation procedure described in *Cisco Prime Network Registrar Installation Guide* that is specific to the original product version.

Step 6 After the installation ends successfully, stop the Cisco Prime Network Registrar server agent:

- For the local cluster:

```
# systemctl stop nwreglocal
```

- For the regional cluster:

```
# systemctl stop nwregregional
```

Step 7 Extract the contents of the backup file to the reinstalled version of Cisco Prime Network Registrar.

a) Change to the root directory (/) of the filesystem.

b) Using the fully qualified path to the archive directory, extract the archive.

- Change to the root directory of the filesystem using **cd /**.
- Using the fully qualified path to the archive directory containing the **upgrade-backup-***date***.tar.gz** file, extract the archive.

```
tar xzf /var/nwreg2/{local | regional}/upgrade-backup-date.tar.gz
```

The above command creates the **opt** and **var** folders. The **opt** folder contains only the conf directory.

Step 8 Verify if the previous configuration, including scopes and zones, is intact.

Moving a Local Cluster to a New Machine

Before you begin, ensure that the new machine meets the current system requirements (see System Requirements).

The following steps can be used to upgrade the cluster to a later Cisco Prime Network Registrar version (that is, it is not required that the same version of Cisco Prime Network Registrar be installed in Step 5; a later version that supports upgrades from the earlier version can be installed).

To move an existing Cisco Prime Network Registrar installation to a new machine on the same platform:

Step 1 Stop the server agent on the old local server.

```
# systemctl stop nwreglocal
```

Step 2 Tar up /var/nwreg2/local, except /var/nwreg2/local/tomcat. You can also skip the /var/nwreg2/local/data.bak if you prefer not to copy over the latest backup.

Step 3 Copy the tar file to the new server, and untar the files into the same location (/var/nwreg2/local). Ensure that there is no /var/nwreg2/local/tomcat directory (if so, remove it and anything in it).

Note The Step 2 and Step 3 apply to Cisco Prime Network Registrar 11.0 and later. For earlier releases, refer to the documentation of that version.

Step 4 Move the /usr/lib/systemd/system/nwreglocal.env file to the new system.

Step 5 Install Cisco Prime Network Registrar (local cluster) on the new server. The installation will detect an upgrade and will do so based on the copied data.

This procedure preserves your original data on the old machine.

Re-apply any custom configuration changes (such as those outlined in Enhancing Security for Web UI) after the installation.

Step 6 Log in to the web UI and navigate to the **Licenses** page under the **Administration** menu to open the List Licenses page.

Step 7 Edit the regional server information as necessary. Ensure that the regional server information provided is where you would like to register your new machine.

Step 8 Click the **Register** button to register with the regional server.

Step 9 If the IP address of the machine has changed, you may need to also update the failover/HA DNS partner to assure it also has the new address of the server. For DHCP, you may need to update the relay agent helper addresses and DNS server addresses.

Note An address change can prevent DHCP clients from renewing promptly (they may not be able to renew until they reach the rebinding time) and can prevent DNS queries from being resolved until clients or other DNS servers receive the updated information.

Moving a Regional Cluster to a New Machine

License management is done from the regional cluster when Cisco Prime Network Registrar is installed. The regional server is installed first and all licenses are loaded in the regional server. When the local cluster is installed, it registers with the regional server to obtain its license.

When you want to move a regional cluster to a new machine, you need to back up the data on the old regional cluster and copy the data to the same location on the new machine.

Note When the regional server goes down or is taken out of service, the local cluster is not aware of this action. If the outage lasts for less than 24 hours, it results in no impact on the functioning of the local clusters. However, if the regional cluster is not restored for more than 24 hours, the local cluster may report warning messages that the local cluster is not properly licensed (in the web UI, CLI, or SDK). This does not impact the operation of the local clusters and the local clusters continue to work and service requests.

The following steps can be used to upgrade the cluster to a later Cisco Prime Network Registrar version (that is, it is not required that the same version of Cisco Prime Network Registrar be installed in Step 5; a later version that supports upgrades from the earlier version can be installed).

To move an existing Cisco Prime Network Registrar installation to a new machine:

Step 1 Stop the server agent on the old regional server:

```
# systemctl stop nwregregional
```

Step 2 Tar up /var/nwreg2/regional, except /var/nwreg2/regional/tomcat. You can also skip the /var/nwreg2/regional/data.bak if you prefer not to copy over the latest backup.

Step 3 Copy the tar file to the new server, and untar the files into the same location (/var/nwreg2/regional). Ensure that there is no /var/nwreg2/regional/tomcat directory (if so, remove it and anything in it).

Note The Step 2 and Step 3 apply to Cisco Prime Network Registrar 11.0 and later. For earlier releases, refer to the documentation of that version.

Step 4 Move the /usr/lib/systemd/system/nwregregional.env file to the new system.

Step 5 Install Cisco Prime Network Registrar (regional cluster) on the new server. For more information, see Installing Cisco Prime Network Registrar, on page 1.

The installation will detect an upgrade and will do so based on the copied data. This procedure preserves your original data from the old regional server.

Re-apply any custom configuration changes (such as those outlined in Enhancing Security for Web UI) after the installation.

Note When you install Cisco Prime Network Registrar on the new machine, you must choose the data directory on which you have copied the data from the old regional server.

Step 6 Start the Cisco Prime Network Registrar web UI or CLI. For more information, see Using Cisco Prime Network Registrar.

Step 7 Log in as superuser to the CLI for the new regional cluster.

Step 8 To list the local clusters, use the following command:

```
nrcmd-R> cluster listnames
```

Step 9 To synchronize the data as well as the license information, use the following command:

```
nrcmd-R> cluster cluster-name sync
```

Installing Your Own Certificate for Web UI Access

If you want to use your own certificate for web UI access, do the following:

Step 1 Create a keystore file with self-signed certificate by using **openssl** or **keytool**. Use the utility to define a self-signed certificate, or to request and later import a certificate from an external signing authority:

- To create a keystore file containing a self-signed certificate, run this command and respond to the prompts:

```
> keytool -genkey -alias tomcat -keyalg RSA -keystore k-file
Enter keystore password: password
What is your first and last name? [Unknown]: name
What is the name of your organizational unit? [Unknown]: org-unit
What is the name of your organization? [Unknown]: org-name
What is the name of your City or Locality? [Unknown]: local
What is the name of your State or Province? [Unknown]: state
What is the two-letter country code for this unit? [Unknown]: cc
Is CN=name, OU=org-unit, O=org-name, L=local, ST=state, C=cc correct? [no]: yes
Enter key password for <tomcat> (RETURN if same as keystore password):
```

Note You must use 128-bit SSL to disable weak ciphers in the web UI. For more information, see Enhancing Security for Web UI.

- To create a Certificate Signing Request (CSR) that you will submit to the Certificate Authority (CA) when you request a certificate, create the keystore file as in the previous step, then execute this command:

```
> keytool -certreq -keyalg RSA -alias tomcat -file certreq.cer -keystore k-file
```

Submit the resulting certreq.cer file to the CA. Once you receive the certificate from the CA, first download the Chain Certificate from the CA, then import the Chain Certificate and your new Certificate into the keystore file, as follows:

```
> keytool -import -alias root -keystore k-file -trustcacerts -file chain-cert-file
> keytool -import -alias tomcat -keystore k-file -trustcacerts -file new-cert-file
```

For details on the **keytool** utility, see the documentation at the Java website of Oracle. For details on the **keystore** file and Tomcat, see the documentation at the website of the Apache Software Foundation.

- To create a self-signed certificate using openssl, use the following command:

```
> openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365
```

For more information on certificate management in Cisco Prime Network Registrar, see the *"Certificate Management" section in the Cisco Prime Network Registrar 11.1 Administration Guide*.

Step 2 Edit the cnr-priv.conf file (in /var/nwreg2/{local | regional}/conf/priv) as required to point to the new keystore and then specify the password (encrypted). To generate the encrypted password, use the encrypt script (**encrypt -s** <*plain-text password*>) present in the *install-path*/usrbin directory.

Step 3 Restart Cisco Prime Network Registrar.

Whenever Cisco Prime Network Registrar is restarted, the keystore details are applied to the Tomcat configuration.

Troubleshooting the Installation

The log directory is set to these locations by default:

- Local cluster: /var/nwreg2/local/logs
- Regional cluster: /var/nwreg2/regional/logs

If the installation or upgrade does not complete successfully, then:

- Check the contents of the above log files to help determine what might have failed. Some examples of possible causes of failure are:
  - An incorrect version of Java is installed.
  - Insufficient disk space is available.
  - Inconsistent data exists for an upgrade.
- Check the status of the service using the following commands:
  - For the local cluster:

    ```
    # systemctl status -l nwreglocal.service
    ```

  - For the regional cluster:

    ```
    # systemctl status -l nwregregional.service
    ```

- Check the systemd journal using the following commands:
  - For the local cluster:

    ```
    # journalctl -u nwreglocal --since=today
    ```

  - For the regional cluster:

    ```
    # journalctl -u nwregregional --since=today
    ```

  You can change the time interval used in since. For more details, use the **man journalctl** command.

Troubleshooting Local Cluster Licensing Issues

If your regional cluster and local cluster are located in isolated networks, are separated by a firewall, or the time skew between the regional and local clusters is more than five minutes, then the local cluster may be

unable to register with the regional server. The firewall may block the return connection used to validate the local cluster admin credentials that are sent from the local cluster to the regional cluster.

To register a local cluster with the regional cluster:

Step 1 Install Cisco Prime Network Registrar (local cluster) on the server and create the admin user for the local cluster. For more information, see Installing and Upgrading Cisco Prime Network Registrar, on page 1.

When you try to log in for the first time (either in the web UI or CLI) after installing Cisco Prime Network Registrar on the local cluster, you will be prompted to create the superuser and to register with a regional cluster.

Step 2 Log in to the regional cluster and add the new local cluster to the regional cluster with the admin credentials. For more information, see the *"Adding Local Clusters" section in the Cisco Prime Network Registrar 11.1 Administration Guide*.

Step 3 To synchronize the data as well as the license information, click the **Resynchronize** icon.