



Installation Overview

This chapter describes how you can access the software image and also describes the high-level installation steps.

This chapter contains the following sections:

- [Downloading the Prime Cable Provisioning Software Image, on page 1](#)
- [High-level Installation Flow and Startup, on page 1](#)

Downloading the Prime Cable Provisioning Software Image

You can download the Prime Cable Provisioning software image either through the product DVD or from the [Download Software](#) page for Prime Cable Provisioning.

To compare the checksum of the downloaded image with that available in the download software page use the below command:

```
md5sum BAC_613_LinuxK9.gtar.gz  
d03fa51fa9b539c43b87cc693e6448ab BAC_613_LinuxK9.gtar.gz
```

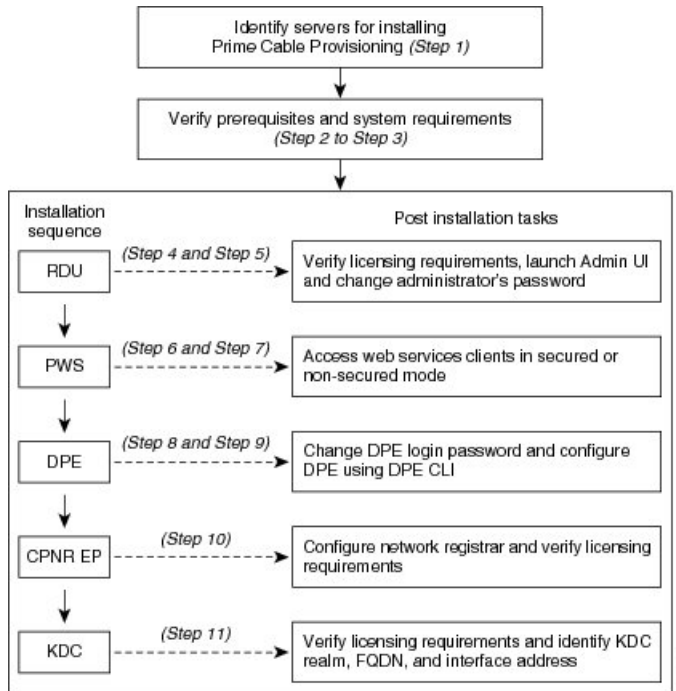
By comparing the checksum values, you can verify if the correct image has been downloaded

High-level Installation Flow and Startup

This section provides the general flow to complete the Prime Cable Provisioning 6.1.3 installation. For details about the complete installation, see [Installing Prime Cable Provisioning](#).

The following figure provides a high level flow for installing Prime Cable Provisioning 6.1.3:

Figure 1: High-level Installation Flow and Startup



To set up Prime Cable Provisioning 6.1.3 in your network infrastructure:

Procedure

- Step 1** Determine the servers on which you are installing the Prime Cable Provisioning components. The components can be installed on the same host server or on different host servers, though the recommendation is to have separate servers for each component.
- Note** In Linux, if RDU and Prime Network Registrar are installed on the same host server, then the lease query will not work.
- Step 2** Verify the file-system block size of the directory in which you intend to install the Prime Cable Provisioning database and the database transaction log files. See [File-System Block Size](#).
- Step 3** Review the [Installation Checklist](#).
- Step 4** Install the RDU. Ensure that you know the location for the Home directory, Data directory, and Database logs directory.
- Step 5** After installing the RDU, ensure that you:
- Obtain a valid Prime Cable Provisioning license to provision devices. For details on obtaining and installing your license file, see [Obtaining a Permanent License](#).
- You still require separate licenses for the following Prime Cable Provisioning components:
- The DPE
 - The KDC, if you configure your network to support secure PacketCable voice technology

- b) Verify whether the RDU is running by:
- Checking RDU logs from the location `BPR_DATA/rdu/logs`.
 - Checking the status of the `bprAgent` using the command `/etc/init.d/bprAgent status` (for RHEL/CentOS 6.x) or `systemctl status bpragent` (for RHEL/CentOS 7.x)

- c) Launch the Admin UI.

`//server_name:port_number/`

where,

- `server_name`—Identifies the server on which the RDU is running.
- `port_number`—Identifies the server port on which the server side of the RDU is running. By default, this port number is:
 - 8100 for HTTP
 - 8443 for HTTPS

The main login screen appears.

- d) Login to PCP using the login credentials

1. Enter the username and password.
2. Click **Login**
3. To change the password:
 - Enter a new password; ensure that this password has at least 8 alphanumeric characters, without any special characters.
 - Click **Login**.

Step 6 Install the PWS. Ensure that you know:

- The RDU server information; hostname, port, username, and password.

Note You can also configure the RDU server(s) after the PWS installation using the `ws-cli.sh` tool. The `ws-cli.sh` tool is used to change key PWS configuration properties like adding or deleting the RDU accounts and changing the log severity level. For information about the `ws-cli.sh` tool, see the [Cisco Prime Cable Provisioning User Guide](#).

- The secured port and nonsecured port for web services or API clients.

Step 7 After installing the PWS, ensure that you can access the web services or API clients in secured mode using HTTPS or nonsecured mode using HTTP. You can use the default port 9443 for secured mode, and 9100 for nonsecured mode for PWS using SOAP. For REST PWS, default ports for secured mode is 9790 and nonsecured mode is 9101.

Note If you have configured multiple RDU servers on the same PWS, ensure that the PWS can communicate with all the RDU servers.

Step 8 Install DPE.

Step 9

After installing the DPE, ensure that you:

- a) Change the DPE login password and the privileged password from the command-line interface (CLI).

- To change the login password, access the CLI in the privileged mode, and enter:

```
bac_dpe# password password
```

where, *password* identifies the new DPE password.

- To change the DPE privileged password, enter:

```
bac_dpe# enable password password
```

where, *password* identifies the local configured password currently in effect or, optionally, provides a new password. If this parameter is omitted, you are prompted for the password. **Note:** The **enable password** is disabled by default.

For more information, see the [Cisco Prime Cable Provisioning DPE CLI Reference Guide](#).

- b) Configure the DPE from the CLI as required. For configuration instructions, see the [Cisco Prime Cable Provisioning DPE CLI Reference Guide](#).

Step 10

Install and configure Prime Network Registrar, if it is not already installed on your system. We recommend that you use Prime Network Registrar 9.x. For more information on installing Prime Network Registrar, see the [Cisco Prime Network Registrar Installation Guide](#).

Note In Linux, if RDU and Prime Network Registrar are installed on the same server, then the lease query will not work.

- When you install the Prime Network Registrar Local Cluster (LCCM), ensure that you:
 - a. Install Prime Cable Provisioning extensions on all Prime Network Registrar local cluster servers. See [Installing Prime Cable Provisioning](#).
 - b. Configure Prime Network Registrar, including its extensions. Specifically, you need to configure scopes, policies, client classes, and selection tags. See [Configuring Extensions](#). Also see the [Cisco Prime Network Registrar User Guide](#).
 - c. Configure the Prime Network Registrar syslog for alerts and debugging information. For information on configuring syslog file for alerts, see the [Cisco Prime Cable Provisioning User Guide](#).
 - d. Validate the installation by connecting to the Prime Network Registrar web UI and viewing it.
- When you install Prime Network Registrar Regional Cluster (RCCM), ensure that you:
 - a. Identify the master server for Prime Network Registrar Regional Installation, which administers all the configured Prime Network Registrar local clusters. This server can be Solaris, Windows, or Linux.
 - b. Obtain a valid central-cluster license file for the Prime Network Registrar Regional Server.
 - c. After you install the Prime Cable Provisioning extensions on all Prime Network Registrar local servers, replicate the local data into regional and pull the replica address space. For more information, see the [Cisco Prime Network Registrar User Guide](#).

Alternatively, you can also create subnets, client classes, policies, and so on at RCCM and push them to the required LCCM DHCP server. For more information, see the [Cisco Prime Network Registrar User Guide](#).

After you complete Prime Network Registrar installation, install Prime Network Registrar Extension Points. For more information see, [Installing Prime Network Registrar Extension Points in Interactive Mode](#).

Step 11

Install and configure the KDC. When you install the KDC, ensure that you:

- Obtain a valid Prime Cable Provisioning license. The KDC license is proprietary and is licensed during Prime Cable Provisioning installation. For information on installing the KDC license, see [Licensing Prime Cable Provisioning](#).
- Have the following information at hand:
 - KDC realm—Identified by a unique name, the KDC realm consists of a KDC and the clients and servers registered to that KDC.
Note The realm must match the certificate chain at the KDC.
 - KDC FQDN—Identifies the fully qualified domain name on which the KDC server is located.
 - KDC interface address—Identifies the interface (generally the IP address of the KDC server) on which the KDC listens for requests.

Step 12

Optionally, configure the syslog file for alerts. You can set up the syslog file on any Prime Cable Provisioning component server. For information on configuring syslog file for alerts, see the [Cisco Prime Cable Provisioning User Guide](#)
