Installing and Uninstalling Prime Cable Provisioning

This chapter describes how to work with the installation program.

This chapter contains the following sections:

- Installing Prime Cable Provisioning, on page 1
- Uninstalling Prime Cable Provisioning, on page 20
- Post-Uninstallation Task, on page 21

Installing Prime Cable Provisioning

To install Prime Cable Provisioning 7.0:

Note To configure Prime Cable Provisioning in SSL mode post installation, refer to the section **Configuring SSL Post Installation** in Cisco Prime Cable Provisioning 7.0 User Guide

Procedure

Step 1 Log into the intended Prime Cable Provisioning host as *root*.

Step 2 At the system prompt, change directory to your CD-ROM drive or other installation media.

Ensure that the **gzip** and **gtar** utilities are available on your system to decompress and unpack the Prime Cable Provisioning 7.0 installation file, and:

a. Change to the directory in which you will decompress and extract the installation file.

b. Extract the file with the *.gtar.gz* extension. Enter:

For Linux:

```
# <install_path>/gtar -zxvf BAC_70_LinuxK9.gtar.gz
```

The utility creates the *BAC_70_LinuxK9* directory into which the installation program is extracted.

Note If the program displays a checksum error while unpacking, specify the path to the GNU tar on your machine.

Step 3 After the installation program is extracted, you can choose to install the components either in interactive or in non-interactive mode.

- Installing Components in Interactive Mode, on page 2
- Installing Components in Non-interactive Mode, on page 18

Installing Components in Interactive Mode

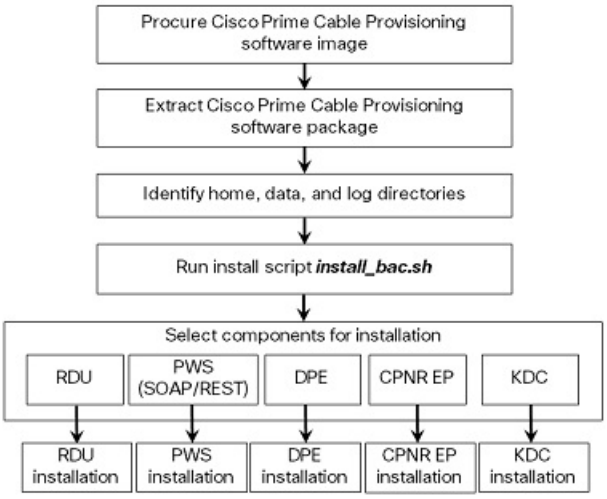
This section explains how to install Prime Cable Provisioning 7.0 components interactively from the command line.

Note Before you begin any of these procedures, you must complete the initial procedure described in Installation Checklist.

Common Steps for all Components

Perform the following steps to start the installation program. The following figure describes the workflow of installation steps that are common for all Prime Cable Provisioning components.

Figure 1: Common Installation Steps



To install Prime Cable Provisioning:

Procedure

Step 1 Enter the following command:

On Linux:

```
# <install-path>/BAC_70_LinuxK9/install_bac.sh
```

where, <*install-path*>—Specifies the complete path to the directory in which the *BAC_70_LinuxK9* directory has been created.

The installation program checks for the Prime Cable Provisioning components installed on the host server. When the check ends, a message appears informing the possible installation modes; interactive and non-interactive, and the location where the response file is to be stored for non-interactive mode.

The installation program prompts you to select whether to proceed with the non-interactive mode or the interactive mode. The default value is set as **n** to proceed with interactive mode.

Step 2 Press **Enter** to proceed with interactive mode.

Step 3 Enter the JDK home directory path.

Note You must have the Java Development Kit (JDK) 1.8 installed on your system.

Step 4 Press **Enter** to continue.

In case IPv6 is not enabled in the system, a warning message is displayed. You can either enable your machine to support IPv6 and continue with the installation, or just continue with the installation without enabling IPv6.

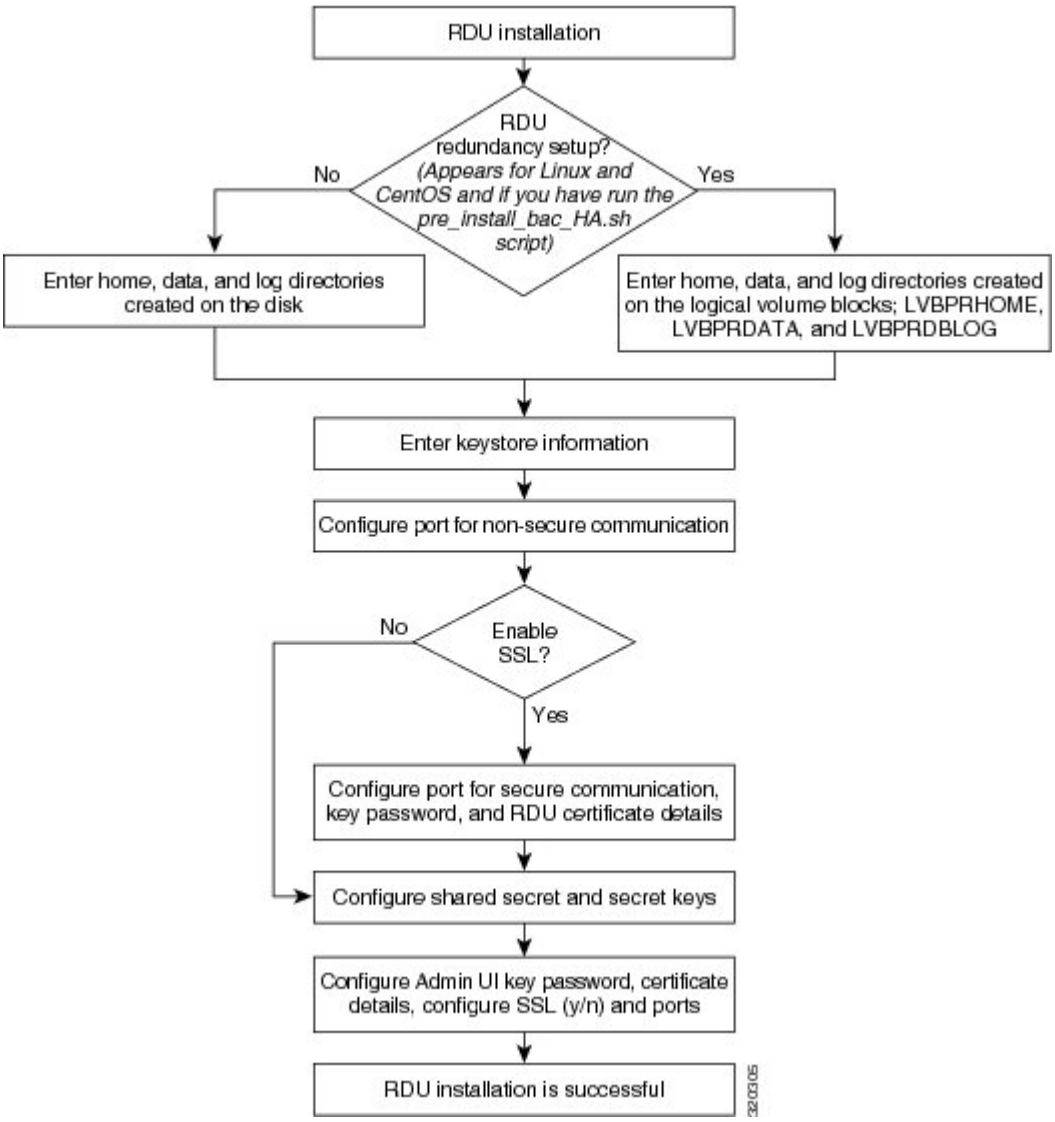
Installing the RDU in Interactive Mode

Install the RDU on a server that meets the requirements described in System Requirements. You should install the RDU on a high-end system that is the most reliable server in your network.

Note We recommend that you configure the RDU server to use a static IP address.

The following figure provides a high level RDU installation workflow.

Figure 2: RDU Installation



To install the RDU:

Procedure

Step 1 Perform steps 1 to 4 from Common Steps for all Components , on page 2.

Step 2 From the installer, select RDU as the component.

Prime Cable Provisioning performs lease query requests by binding to the IP addresses and ports that are described in the following table.

Table 1: Lease Query Address for Binding

Protocol	IP Address	Port
IPv4	Wildcard[1]	67
IPv6	Wildcard	547

[1] The wildcard is a special local IP address. It usually means "any" and can only be used for bind operations.

If the installation program detects that either of these ports is being used by another process, it recommends that you use the dynamic ports that the operating system selects.

If you have run the pre-installation script **pre_install_bac_HA.sh** with the operating system as Linux 6.5, the installation program prompts you to select whether to proceed with the RDU redundancy setup or not.

Step 3 Enter **y** to proceed with the RDU redundancy setup and **n** to proceed with RDU non-redundancy setup. The default is **y**.

Step 4 To accept the default home, data, and database log directories, press **Enter** for each directory prompt; or enter different directory locations.

Note For RDU redundancy feature, the default home, data, and database log directories exist on the logical volume blocks. For example, the default home, data, and database log directories may exist on the logical volume blocks; **LVBPRHOME** mounted on */bprHome*, **LVBPRDATA** mounted on */bprData*, and **LVBPRLOG** mounted on */bprLog*. You can also enter different directory locations.

Step 5 Enter the key store password, and confirm the key store password. The key store password is used to encrypt the key store.

Step 6 To accept the default listening port number, 49187, press **Enter**; or enter another port number. The listening port is the port number that the RDU uses to communicate with other Prime Cable Provisioning components.

Caution If you change the default listening port value, ensure that the new value does not conflict with any existing port assignments. Also, ensure that you configure all DPEs with the correct RDU port number. For details on configuring the DPE, see the Cisco Prime Cable Provisioning DPE CLI Reference Guide.

Step 7 To enable RDU secure mode communication, enter **y**. For nonsecure communication, enter **n**.

Note The default is secure mode.

If you have enabled the RDU secure communication, the installation program prompts you to enter the default port for secure communication, key password, and RDU certificate details. For nonsecure communication, the installation program skips these prompts.

Step 8 To accept the default port number for secure communication, 49188, press **Enter**; or enter another port number. Ensure that you enter the port number that is created for secure communication in RDU.

Step 9 Enter the key password and confirm the key password. The key password is used to encrypt the RDU certificate key in the key store.

Step 10 Enter the RDU certificate details used for SSL communication.

Step 11 Enter the shared secret password that you want to use for authentication among Prime Cable Provisioning servers, and confirm the password. The shared secret password is used to encrypt the information shared between Prime Cable Provisioning servers.

Note You must use the same shared secret password for the RDU, all DPEs, and Prime Network Registrar Extension Points in your network.

Step 12 Enter the secret key password that you want to use for shared secret authentication, and confirm the secret key password. The secret key password is used to encrypt the shared secret password.

Step 13 Enter the key password for Admin UI certificate, and confirm the password. The key password is used to encrypt the Admin UI certificate key in the key store.

Step 14 Enter the Admin UI certificate details used for SSL communication.

Step 15 Store the certificate details and enter **y**.

The installation program prompts you to select whether to enable the secure mode communication between RDU and API clients. The default value is set as **n** to proceed with nonsecure mode communication

Step 16 Enter **y** to enable the secure communication mode.

The installation program adds the certificate to the key store. This certificate is used for authentication during SSL communication.

Step 17 To accept the default port, 8100, press **Enter**; or enter another port number.

Step 18 To accept the default HTTPS port, 8443, press **Enter**; or enter another port number.

Step 19 To accept the default value y, press Enter; or enter n to disable SNMP agent.

Step 20 The RDU component of Prime Cable Provisioning is installed on the host.

After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

Installing PWS in Interactive Mode

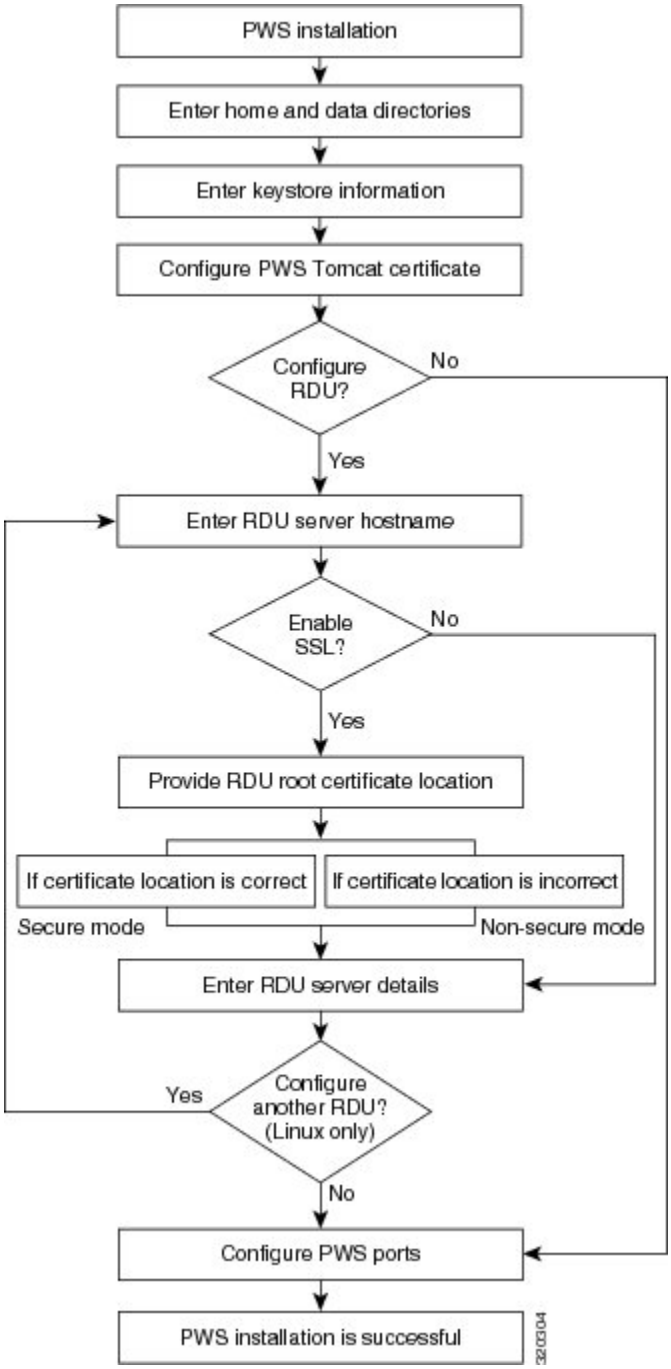
Install the PWS (Provisioning Web Services) on a server that meets the requirements described in System Requirements.

Note If you are installing both RDU and PWS on the same server, the installation configurations chosen for PWS take precedence over the Admin UI configurations. For example, if you have chosen secured mode of communication for Admin UI and non-secured mode for PWS, non-secured mode is chosen for both Admin UI and PWS.

Note We recommend that you configure the PWS server to use a static IP address.

The following figure provides a high level PWS installation workflow.

Figure 3: PWS Installation



To install the PWS:

Procedure

Step 1 Perform steps 1 to 4 from Common Steps for all Components , on page 2.

From the installer, select PWS as the component.

Step 2 To accept the default home directory, */opt/CSCObac*, press **Enter**; or enter another directory.

Step 3 To accept the default data directory, */var/CSCObac*, press **Enter**; or enter another directory.

Step 4 Enter the key store password, and confirm the key store password. The key store password is used to encrypt the key store.

Step 5 Enter the key password, and confirm the key password. The key password is used to encrypt the PWS certificate key in the key store.

Step 6 Enter the PWS certificate details used for SSL communication.

Step 7 Store the certificate details; enter **y** to continue.

The installation program prompts you to enter the PWS information.

The installation program prompts you to select whether to support the PWS instance with a load balancer. The default value is set as **n**.

Step 8 Enter **y** to enable the load balancer support, and enter the REST PWS cluster name.

Note Load Balancer is supported only for the REST PWS component.

The installation program prompts you to enter the RDU information.

Step 9 To add RDU information, enter **y**.

Step 10 Enter RDU hostname.

The installation program prompts you to select whether to enable the secure mode communication between RDU and PWS web server. The default value is set as **n** to proceed with nonsecure mode communication.

Step 11 To enable secure communication, enter **y**. For nonsecure communication, enter **n**.

If you have enabled secure communication, the installation program prompts you to enter the RDU certificate location. For nonsecure communication, the installation program skips this prompt.

Step 12 To accept the default RDU certificate location, [*/tmp/rootCA.crt*], press **Enter**; or enter another location. Ensure that you enter the location where the RDU certificate is placed else the communication mode falls back to nonsecured mode. If PWS is installed on a separate web server, ensure that you copy the RDU certificate from the location *$BPR_HOME/lib/security/* on the PWS web server.

Note For every RDU added, certificates must be placed in separate locations.

The installation program adds the certificate to the trust store. This certificate is used for authentication during SSL communication.

The installation program prompts you to enter the RDU information.

Step 13 Enter RDU information; port, username, and password, and press **Enter** to continue.

The installation program prompts you to confirm the RDU information.

Step 14 Enter **y** and press **Enter** to continue.

The installation program prompts you to add the second RDU.

Step 15 On Linux, repeat step 9 to 13 to add multiple RDUs, else enter **n**. The PWS component can communicate with multiple RDUs.

Note You can also configure RDUs 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 on how to run the ws-cli.sh tool, see the Cisco Prime Cable Provisioning User Guide.

Step 16 To accept the default PWS HTTP port for the API clients, 9100 (SOAP) / 9101 (REST), press **Enter**; or enter another port number.

Step 17 To accept the default PWS HTTPS port for the API clients, 9443 (SOAP) / 9790 (REST), press **Enter**; or enter another port number.

Step 18 Confirm the PWS installation information; enter **y** and press **Enter.**

Step 19 Press **Enter** to continue. The PWS component of Prime Cable Provisioning is installed on the host.

After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

Installing REST PWS in Interactive Mode

For installing the REST PWS, see Installing PWS in Interactive Mode, on page 6.

Note PWS RESTful can communicate with PCP 6.1.3 or above RDU versions only. It is not compatible with RDUs of earlier releases of Prime Cable Provisioning.

Note During Upgrade procedure, after successful upgrade of REST PWS to Prime Cable Provisioning 7.0, the installation program prompts you for enabling Load Balancer support.

Installing DPE in Interactive Mode

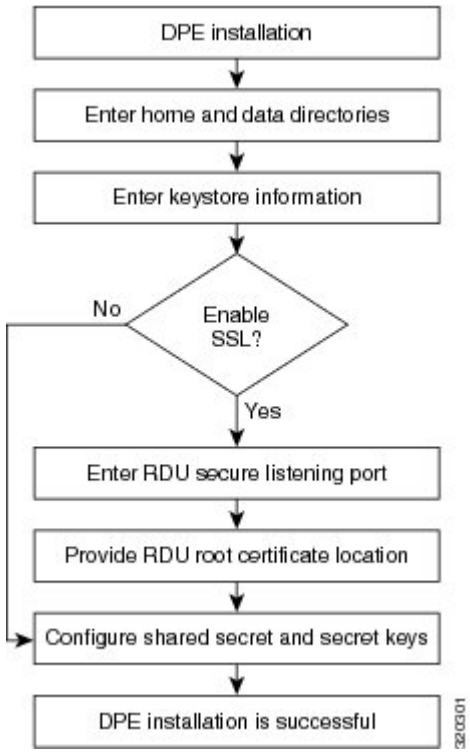
Install the DPE on a server that meets the requirements described in System Requirements.

Note We recommend that you configure the DPE server to use a static IP address.

During DPE installation, if the program detects a TFTP server or a ToD server running on the same server as the DPE, the installation displays an error message and quits. To stop the TFTP or ToD server, carry out the steps that the error message lists.

The following figure provides a high level DPE installation workflow.

Figure 4: DPE Installation



To install the DPE:

Procedure

Step 1 Perform steps 1 to 4 from Common Steps for all Components , on page 2.

From the installer, select DPE as the component.

Step 2 To accept the default home directory, */opt/CSCObac*, press **Enter**; or enter another directory.

Step 3 To accept the default data directory, */var/CSCObac*, press **Enter**; or enter another directory.

Note A message is displayed in case there is not enough space in the directory.

Step 4 Enter the key store password, and confirm the key store password. The key store password is used to encrypt the key store.

The installation program prompts you to select whether to enable the secure mode communication between RDU and DPE. The default value is set as **n** to proceed with nonsecure mode communication.

Step 5 To enable secure communication, enter **y**. For nonsecure communication, enter **n**.

Note The default is secure mode.

If you have enabled secure communication, the installation program prompts you to enter the default port for secure communication and RDU certificate location. For nonsecure communication, the installation program skips these prompts.

Step 6 To accept the default port number for secured communication, 49188, press **Enter**; or enter another port number. Ensure that you enter the port number that is created for secure communication in RDU.

Step 7 Confirm the listening port number for secured communication; enter **y** to continue.

Step 8 To accept the default RDU certificate location, [*/tmp/rootCA.crt*], press **Enter**; or enter another location. Ensure that you enter the location where the RDU certificate is placed else the communication mode falls back to nonsecured mode. If DPE is installed on a separate server, ensure that you copy the RDU certificate from the location *$BPR_HOME/lib/security/* to the DPE server.

The installation program prompts you to enter the authentication password for Prime Cable Provisioning servers.

Step 9 Enter the shared secret password that you want to use for authentication among Prime Cable Provisioning servers, and confirm the password. The shared secret password is used to encrypt the information shared between Prime Cable Provisioning servers.

Note You must use the same shared secret password for the RDU, all DPEs, and Prime Network Registrar extension points in your network.

Step 10 Enter the secret key password that you want to use for shared secret authentication, and confirm the secret key password. The shared secret key password is used to encrypt the shared secret password.

Step 11 To accept the default value y, press Enter; or enter n to disable SNMP agent.

Step 12 Press **Enter** to continue. The DPE component of Prime Cable Provisioning is installed on the host.

After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

Note After you install the DPE, you must configure the DPE with the RDU. For details, see Setting Up a Device Provisioning Engine.

Installing Prime Network Registrar Extension Points in Interactive Mode

Install Prime Cable Provisioning extensions on all Prime Network Registrar servers in your network infrastructure. If you are deploying Prime Cable Provisioning in a failover environment, you must also install the extensions on the failover servers. After you install extensions, you must configure them. This section explains how to install, configure, and validate these extensions.

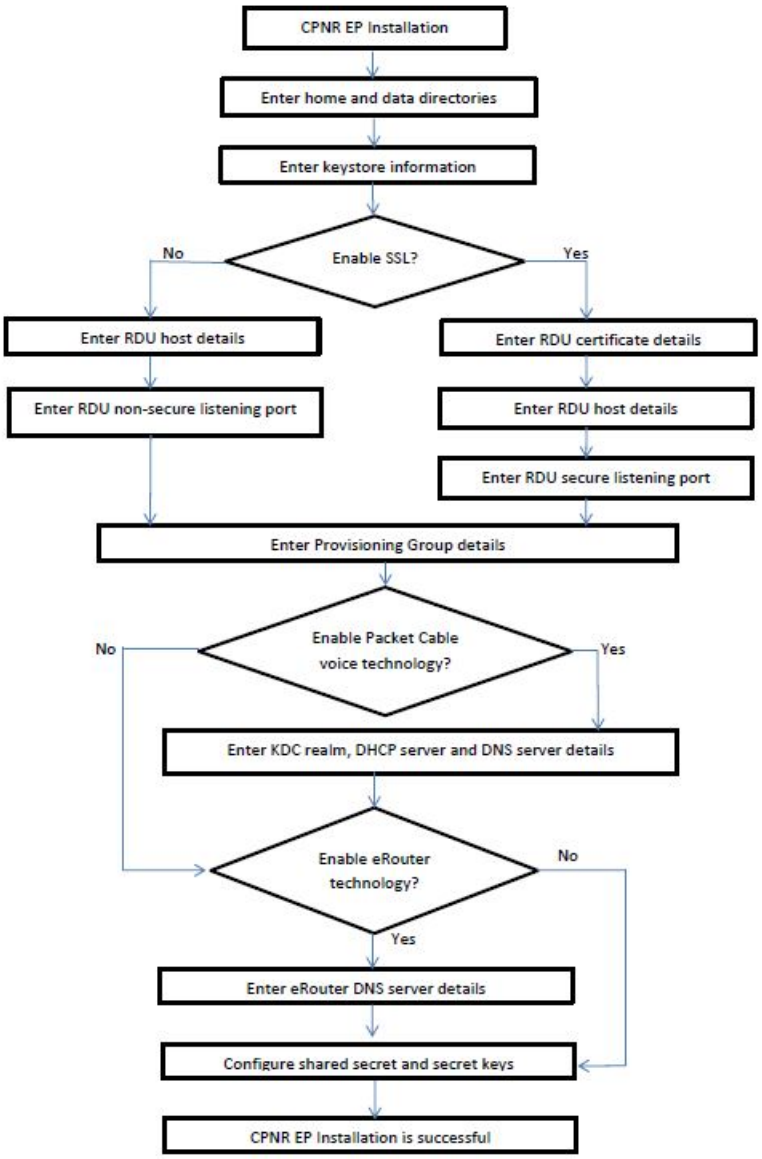
Note We recommend that you configure the Prime Network Registrar server to use a static IP address.

Before you install Prime Network Registrar Extension Points, complete the initial installation described in Installation Checklist. Ensure that Prime Network Registrar is installed and running. To install Prime Network Registrar, see the Cisco Prime Network Registrar 11.x Installation Guide.

Note For SSL to work on a fresh installation of Prime Cable Provisioning, you must install Prime Network Registrar 10.x or higher and then install the extension points.

The following figure provides a high level Prime Network Registrar extension point installation workflow.

Figure 5: Prime Network Registrar Extension Point Installation



To install Prime Network Registrar extension points:

Procedure

Step 1 Perform steps 1 to 4 from Common Steps for all Components , on page 2.

From the installer, select CPNR EP as the component.

Step 2 To accept the default home directory, */opt/CSCObac*, press **Enter**; or enter another directory.

Step 3 To accept the default data directory, */var/CSCObac*, press **Enter**; or enter another directory.

Step 4 Enter the key store password, and confirm the key store password. The key store password is used to encrypt the key store.

The installation program prompts you to select whether to enable the secure mode communication between RDU and Prime Network Registrar extension point. The default is set as **n** to proceed with nonsecure mode communication.

Step 5 To enable secure communication, enter **y**. For nonsecure communication, enter **n**.

Note The default is secure mode.

If you have enabled secure communication, the installation program prompts you to enter the RDU certificate location and default port for secure communication. For nonsecure communication, the installation program skips these prompts.

Step 6 To accept the default RDU certificate location, [*/tmp/rootCA.pem*], press **Enter**; or enter another location. Ensure that you enter the location where the RDU certificate is placed else the communication mode falls back to nonsecured mode. If Prime Network Registrar is installed on a separate server, ensure that you copy the RDU certificate from the location *$BPR_HOME/lib/security/* on the Prime Network Registrar server.

The installation program prompts you to enter the RDU's IP address or hostname.

Step 7 To accept the default RDU's IP address or hostname, press **Enter**; or enter another RDU's IP address or hostname.

Step 8 To accept the default listening port number for secure communication, 49188, press **Enter**; or enter another port number. You must enter the port number that is created for secure communication in RDU.

Step 9 Enter the appropriate provisioning group name, and press **Enter** to continue.

The installation program prompts you to select whether the support for packet cable voice technology is required. The default value is set as n to proceed without support of packet cable voice technology.

Step 10 To accept the default value n, press **Enter**; or enter **y** to enable support of packet cable voice technology.

If you enter y to enable packet cable support, the installation program prompts you to enter the packet cable configuration information:

a. Enter details on the KDC realm name, the IP addresses for the primary and secondary DHCP servers, and the primary and secondary DNS servers.

b. Confirm the information; enter **y** and press **Enter**.

c. Press **Enter** to continue.

Step 11 To accept the default value n, press Enter; or enter y to enable support of eRouter technology.

If you enter y to enable eRouter support, the installation program prompts you to enter the eRouter configuration information:

a. Enter details of the DNS server. Enter a single IP Address or a list of comma separated IP Addresses.

For example: 192.168.4.3 (or) 192.168.5.1,192.168.4.3

b. Confirm the information; enter "Y" and press Enter.

c. Press Enter to continue.

Step 12 Enter the shared secret password that you want to use for authentication among Prime Cable Provisioning servers, and confirm the password. The shared secret password is used to encrypt the information shared between Prime Cable Provisioning servers.

Note You must use the same shared secret password for the RDU, all DPEs, and Prime Network Registrar extension points in your network.

Step 13 Enter the secret key password that you want to use for shared secret authentication, and confirm the secret key password. The shared secret key password is used to encrypt the shared secret password.

Step 14 Confirm the details entered for RDU IP address or hostname, listening port number for secured communication, provisioning group, and packet cable voice technology support selection.

The Prime Network Registrar extension points component of Prime Cable Provisioning is installed on the host.

After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

Configuring Extensions

After you install the Prime Network Registrar extension points, you must configure the extensions. The procedure described in this section assumes that:

- The Prime Cable Provisioning component is installed in */opt/CSCObac*.
- Prime Network Registrar is installed in */opt/nwreg2*.
- The Prime Network Registrar username and password are known.

Note Before you can use the Prime Network Registrar server, you must configure client classes, scope-selection tags, policies, and scopes. In an IPv6 environment, you must configure links and prefixes as well. For details, see the Cisco Prime Cable Provisioning User Guide.

To configure extensions:

Procedure

Step 1 Log into the Prime Network Registrar server, with *root* access.

Step 2 At the command line, enter:

```
# NR_HOME/local/usrbin/nrcmd -N username -P password -b <
BAC_HOME/cnr_ep/bin/bpr_cnr_enable_extpts.nrcmd
```

Step 3 To reload the Prime Network Registrar server, enter:

```
# systemctl stop nwreglocal
# systemctl start nwreglocal
```

Alternatively, to reload the DHCP server alone, enter:

```
# NR_HOME/local/usrbin/nrcmd -N username -P password "dhcp reload"
```

Validating Extensions

To validate the extensions installed on the Prime Network Registrar server, from the Prime Network Registrar Command Line Tool (**nrcmd**), run:

Note Depending on whether you installed a local or regional cluster, the **nrcmd** tool is located in:

- Local—*/opt/nwreg2/local/usrbin*
- Regional—*/opt/nwreg2/regional/usrbin*

```
nrcmd> extension list
100 Ok
dexdropras:
    entry = dexdropras
    file = libdexextension.so
    init-args =
    init-entry =
    lang = Dex
    name = dexdropras
preClientLookup:
    entry = bprClientLookup
    file = libbprextensions.so
    init-args = BPR_HOME=/opt/CSCObac,BPR_DATA=/var/CSCObac
    init-entry = bprInit
    lang = Dex
    name = preClientLookup
prePacketEncode:
    entry = bprExecuteExtension
    file = libbprextensions.so
    init-args =
    init-entry = initExtPoint
lang = Dex
    name = prePacketEncode

nrcmd>
```

Note The *$BPR_HOME* and *$BPR_DATA* values may be different in your installation.

Also, in the **nrcmd** program, run:

```
nrcmd> dhcp listextensions
100 Ok
post-packet-decode: dexdropras
pre-packet-encode: prePacketEncode
pre-client-lookup: preClientLookup
post-client-lookup:
```

```
post-send-packet:
pre-dns-add-forward:
check-lease-acceptable:
post-class-lookup:
lease-state-change:
generate-lease:
environment-destructor:
pre-packet-decode:
post-packet-encode:

nrcmd>
```

Configuring Prime Network Registrar Extension Points Properties File

After you install the Prime Network Registrar extension points, depending on the Prime Network Registrar provided libraries for SSL and Crypto, you must modify the *cnr_ep.properties* file located in *<BAC_HOME>/cnr_ep/conf/* directory to include the appropriate SSL and Crypto libraries version.

For example:

If the SSL and Crypto libraries shipped with Prime Network Registrar are 1.0.1d, ensure that you remove the patch character d while loading the SSL and Crypto libraries.

To load the SSL and Crypto libraries, enter the SSL and Crypto libraries in the *cnr_ep.properties* file as:

```
/lib/cpcp/cryptolib=/opt/nwreg2/local/lib/libcrypto.so.1.0.1
/lib/cpcp/ssllib=/opt/nwreg2/local/lib/libssl.so.1.0.1
```

Note Prime Network Registrar does not ship SSL and Crypto libraries as part of CPNR **9.1.3 and above**, **10.1 and above**, instead it uses the system libraries. Modify the *cnr_ep.properties* file located in *<BAC_HOME>/cnr_ep/conf/* directory to include the appropriate SSL and Crypto system libraries.

To identify the SSL and Crypto libraries used by CPNR execute the below command:

```
ldd /opt/nwreg2/local/bin/dhcp
```

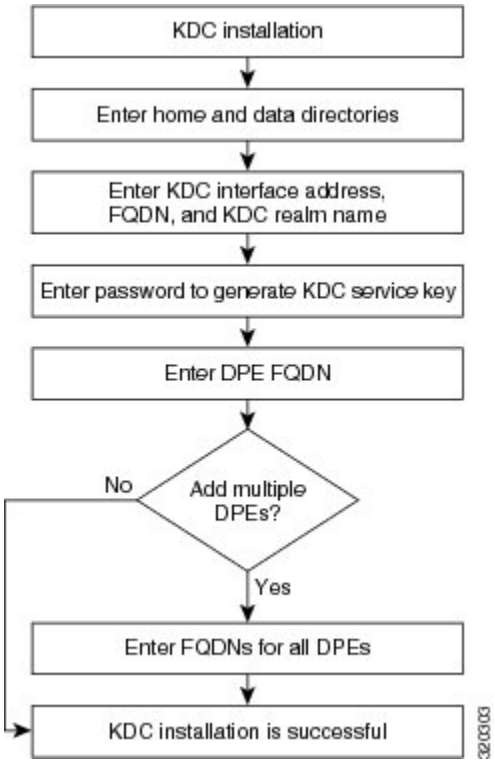
Note You must modify cnr_ep.properties file with the appropriate details, whenever you change the library files.

Installing KDC in Interactive Mode

You must install the KDC (Key Distribution Center) only when configuring a system to support voice technology operations.

Install the KDC on a server that meets the requirements described in System Requirements. For performance reasons, you should install the KDC on a separate server. The following figure provides a high level KDC installation workflow.

Figure 6: KDC Installation



To install the KDC:

Procedure

Step 1 Perform steps 1 to 4 from Common Steps for all Components , on page 2.

From the installer, select KDC as the component.

Step 2 To accept the default home directory, */opt/CSCObac*, press **Enter**; or enter another directory.

Step 3 To accept the default data directory, */var/CSCObac*, press **Enter**; or enter another directory.

Step 4 Enter the KDC interface address, the fully qualified domain name (FQDN), and the Kerberos realm name. The realm name should be consistent with the realm you give to the DPEs that belong to this provisioning group.

Step 5 To confirm your entry and continue, enter **y** and press **Enter**.

The installation program prompts you to enter a password to generate the KDC service key.

Step 6 For each DPE, enter a password from 6 to 20 characters. The KDC service key mentioned here is one that you must generate on the DPE and the KDC to enable communication between the two components. To generate this service key, the password that you enter for the KDC must match the one that you enter for the corresponding DPE; otherwise, the DPE does not function.

Note To generate the service key on the:

- DPE, use the **service packetcable** *1* **registration kdc-service-key** command from the DPE CLI. For details, see the Cisco Prime Cable Provisioning DPE CLI Reference Guide.
- KDC, use the KeyGen tool. For details, see the Cisco Prime Cable Provisioning User Guide.

Step 7 To confirm and continue, enter **y** and press **Enter.**

The installation program prompts you to enter the DPE FQDN.

Step 8 Enter the FQDN of the DPE, and press **Enter**.

Step 9 Enter **y** and press **Enter** to confirm and continue.

Step 10 To add another DPE, enter **y** and press **Enter**, or enter **n** and press **Enter**. The installation program uses the same voice technology shared key for all DPEs.

Step 11 Enter **y** and press **Enter**. The KDC component of Prime Cable Provisioning is installed on the host.

After a successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

Caution After installing the KDC, install the licenses and the chain of certificates; otherwise, you cannot launch the KDC.

Installing Components in Non-interactive Mode

The non-interactive mode installation is similar to that of the interactive mode with just a few exceptions. This section explains the exceptions that you follow to install the components from the command line in non-interactive mode.

In order to install Prime Cable Provisioning 7.0 in non-interactive mode, you must first generate a response file, in which you store values for installing a component. You then use the response file as input while installing that component. For subsequent installations of the same component, you only need to use a single command, which removes all installation prompts and installs the component using the values contained in the response file.

To install Prime Cable Provisioning 7.0 in non-interactive mode, you must perform these steps:

1. Generating the Response File, on page 18
2. Installing a Component Using the Response File, on page 19

Generating the Response File

To generate the response file:

Procedure

Step 1 Generate a response file, using:

For Linux:

```
#<install-path>/BAC_70_LinuxK9/install_bac.sh -response
```

Note In Linux environment, the response file is generated in the installation directory.

Running the command does not install Prime Cable Provisioning on your system; it only generates the response file in which you store values for installation.

Note that there can only be one response file. As a result, you can use the response file only to install the component for which you generate the response file. If you want to install another component, you must generate a response file for that component and install that component using the response file generated for it.

Example:

You cannot use the response file that you generated to install the DPE, to install Prime Network Registrar extensions.

The installation program verifies that you have installed the required patches of the operating system. When the verification ends, the welcome information appears.

Step 2 Carry out the steps as listed in Installing Components in Interactive Mode, on page 2.

Installing a Component Using the Response File

After you generate the response file, you can install the component in noninteractive mode.

To install the component in noninteractive mode:

Procedure

Step 1 Enter the following command to start the installation program:

On Linux:

```
#<install-path>/BAC_70_LinuxK9/install_bac.sh
```

where, install-path—Specifies the complete path to the directory in which the *BAC_70_LinuxK9* directory has been created.

The installation program checks for the Prime Cable Provisioning components installed on the host server. When the check ends, a message appears informing the possible installation modes; interactive and non-interactive, and the location where the response file is to be stored for non-interactive mode.

The installation program prompts you to select whether to proceed with the non-interactive mode. The default value is set as n to proceed with interactive mode.

Step 2 Enter **y** and press **Enter** to proceed with noninteractive mode.

After the successful installation, the following message appears:

```
Installation of <CSCObac> was successful.
```

Adding Components

This section describes how you can add one component of Prime Cable Provisioning to a system on which other components have already been installed. This situation arises largely in a deployment similar to a lab installation, where, for the purposes of testing, more than one component is installed on a single machine. The definitions file (*bpr_definitions.sh*) is updated whenever you add new components. The procedures for adding a component are similar to those for a fresh installation.

When the installation program detects the presence of one component on your system, it does not allow you the option of adding that particular component. It prompts you to add or install other components only.

Note You cannot reinstall a component that you have already installed. If you must carry out a reinstallation, first uninstall that component, and then install it again.

Uninstalling Prime Cable Provisioning

The procedure described in this section uninstalls the RDU, Prime Network Registrar extensions, the DPE, the PWS and the KDC, but it does not uninstall the Prime Network Registrar application. Before removing Prime Cable Provisioning, manually remove the Prime Cable Provisioning configuration on Prime Network Registrar.

The uninstallation program removes all files found in the installation directory (the default directory is */opt/CSCObac*). The program also shuts down and removes these processes, if they are detected: RDU, KDC, SNMP Agent, Tomcat, Prime Cable Provisioning agent, and DPE.

The uninstallation program does not remove files that were placed outside the installation directory. For example, a component installation places the database and database logs directories under */var/CSCObac*. These files must be removed manually. (Subsequent sections describe how to delete these files.) Also, the program does not remove any files found in the Prime Network Registrar directory

If you have installed Prime Cable Provisioning extensions on Prime Network Registrar, you must first uninstall it for a complete uninstallation of the Prime Cable Provisioning program; otherwise, an error message similar to the following appears:

```
Error: Unable to uninstall until the CNR extension points are disabled

To disable, use the NRCMD file /opt/CSCObac/cnr_ep/bin/bpr_cnr_disable_extpts.nrcmd
and then delete the extensions library, for example:

/opt/nwreg2/local/usrbin/nrcmd -b <
/opt/CSCObac/cnr_ep/bin/bpr_cnr_disable_extpts.nrcmd
/opt/nwreg2/local/usrbin/nrcmd dhcp reload
rm /opt/nwreg2/local/extensions/dhcp/dex/libbprextensions.so
```

The path to the Prime Network Registrar extensions differs based on the location where you have installed Prime Network Registrar; the default location is */opt/nwreg2*.

If the uninstallation program fails to uninstall Prime Cable Provisioning, an error message appears.

After uninstalling Prime Cable Provisioning, manually remove the data and database logs directories. See Post-Uninstallation Task, on page 21.

To uninstall Prime Cable Provisioning from the command line:

Procedure

Step 1 Log into the Prime Cable Provisioning server as the *root* user.

Step 2 Manually remove the configuration of the Prime Cable Provisioning extensions on the Prime Network Registrar server. You can do this from any server that has nrcmd installed and connectivity with Prime Network Registrar.

a. To uninstall the Prime Cable Provisioning extensions from your Prime Network Registrar configuration, enter:

```
# NR_HOME/local/usrbin/nrcmd -N <username> -P <password> -b
<$BPR_HOME/cnr_ep/bin/bpr_cnr_disable_extpts.nrcmd
```

b. To reload your DHCP server, enter:

```
# systemctl stop nwreglocal
```

```
# systemctl start nwreglocal
```

Alternatively, enter:

```
# NR_HOME/local/usrbin/nrcmd -N <username> -P <password> "dhcp reload"
```

c. To remove the Prime Cable Provisioning extensions from the Prime Network Registrar extensions directory, enter:

```
# rm -rf NR_HOME/local/extensions/dhcp/dex/libbprextensions.so
```

Step 3 To uninstall Prime Cable Provisioning run the following command:

On Linux:

```
# install-path/BAC_70_LinuxK9/uninstall_bac.sh
```

Step 4 Enter **y**, and press **Enter** to start uninstalling.

Post-Uninstallation Task

After you have uninstalled Prime Cable Provisioning, manually remove the data and database logs directories.

Note Back up the important files before removing the data.

To remove these directories:

Procedure

Step 1 Log in as *root*.

Step 2 Remove the data and the database logs directories. The default directory for both is */var/CSCObac*.

For example, enter:

```
# rm -rf /var/CSCObac
```

The data and the database logs directories are deleted.