Preparing for Installation

This chapter covers the tasks that you must perform before installing Prime Cable Provisioning.

This chapter contains:

Users and Groups (for Solaris only)

The Prime Cable Provisioning root user can create users and groups, and assign appropriate privileges to the users.

A non-root user should be assigned with the following privileges to run Prime Cable Provisioning:

- file_chown
- file_link_any
- file_owner
- net_privaddr
- proc_exec
- proc_fork
- proc_info
- proc_owner
- proc_session
- proc_setid
- net_access

Note The Prime Cable Provisioning non-root user can run any process associated with socket connection, only if the net_access privilege is assigned to the non-root user. The net_access privilege is available only in Solaris 10 (update 9 and 10) platform.

Note During installation, it may be necessary to install several Solaris patches on your computer. Should patch installation become necessary, see the Sun Microsystems support site to download these patches. For a list of recommended patches, see System Requirements, page 2-1.

A root user should perform the following pre-installation steps:

Procedure

Step 1 Create groups and users. Assign users to the groups.

Note You must have system administrator privileges to create groups and users and assign users to groups.

If you are installing each of the Prime Cable Provisioning components in different servers, then you must create groups and users in all the different servers.

To create a group, run the following command.

```
groupadd –g 1110 baceng
```

where, -g—is the argument for representing group ID. This creates a group named *1110 baceng*.

To create a user, run the following command:

```
useradd -u 102 -g 1110 -d /home/user -m -s /bin/sh -c "Test User" user
```

where, -u—is the argument for representing user ID, -g is the group ID, -d is the directory location.

Step 2 Assign privileges to users using the command:

```
usermod -K defaultpriv=file_chown,file_link_any,file_owner,net_privaddr,proc_exec,proc_fork,
proc_info,proc_owner,proc_session,proc_setid user
```

Step 3 Set password for the user using the command:

```
passwd <user_name>
New Password:
Re-enter new Password:
passwd: password successfully changed for user
```

where, <user_name>—Specifies the name of the root or non-root user.

Installation Checklist

This section explains the procedures you must follow to install Prime Cable Provisioning.

Before you install Prime Cable Provisioning, ensure that you are ready by reviewing the checklist that the following table describes.

Table 1: Installation Checklist

Task	Checkoff
1. Verify if your system meets the minimum system hardware and software requirements described in Installation Requirements.	❑
2. Ensure that you have access to the servers on which you intend to install Prime Cable Provisioning components.	❑
3. Save your license file on the system from which you intend to launch the Prime Cable Provisioning Admin UI via a web browser. You need a valid license file to configure Prime Cable Provisioning licensing.	❑
4. Determine the home directory (*BPR_HOME*) in which you want to install the Prime Cable Provisioning component or components. The default directory is */opt/CSCObac*. Ensure that the target installation directory has enough disk space. **Note** We recommend that you have at least 1 GB of disk space available in *BPR_HOME* otherwise launching the Admin UI might result in some errors.	❑
5. For the RDU, determine where you want to install the data directory (*BPR_DATA*) and the database logs (*BPR_DBLOG*). The default directory is */var/CSCObac*. Ensure that the target installation directory has enough disk space. **Note** The RDU and the DPE database directory must be empty or manually cleaned up before proceeding with the Prime Cable Provisioning installation. A warning message is displayed. If you click OK, the database directory is deleted. **Note** We recommend that you locate the data directory on a different physical disk than the home directory; for example, */var/disk0/CSCObac*. The disk should have at least 8 GB and up to 30 GB of free space. The installation program, by default, installs the data directory, the database transaction logs directory, and the logs directory in the same location. We recommend that you locate the database transaction logs directory on the fastest disk on the system. Also, ensure that 8 GB of disk space is available. The minimum required free space may be greater than 8 GB, depending on the number of devices and the required log level.	❑
6. Verify that you have minimum 500 MB of free space available in the /tmp directory for successful installation.	❑
7. The RDU uses an interface (listening port number) to communicate with other Prime Cable Provisioning components. Ensure that this port is not used by any other processes. The default port is 49187 for non-secured communication, and 49188 for secured communication.	❑

Task	Checkoff
8. Determine the certificate details to generate the certificates for RDU, Admin UI, and PWS, used for SSL or HTTPS communication. **Note** You can also generate the certificates after installing Prime Cable Provisioning, and create a Certificate Signing Request (CSR) for an un-signed certificate. For information on how to generate certificates, import certificates in key store, and create a CSR, see the Cisco Prime Cable Provisioning User Guide.	❑
9. Determine the location of the certificate files and enter it correctly when prompted. The default location is */tmp*. If you enter an incorrect location, it falls back to the nonsecure mode.	❑
10. Determine the shared secret for the RDU. The Prime Cable Provisioning components (DPE and Prime Network Registrar Extension Points) use shared secret as a token to authenticate with the RDU. Ensure that you configure the same shared secret while installing the Prime Cable Provisioning components.	❑
11. Determine the secret key that is used to encrypt the shared secret for the RDU. The Prime Cable Provisioning components (DPE and Prime Network Registrar Extension Points) use the secret key for double encryption, apart from the shared secret. Ensure that you configure the same secret key while installing the Prime Cable Provisioning components.	❑
12. Determine the key store password to be used for the key store. The key store stores the certificate keys. For more information about key store, see the Cisco Prime Cable Provisioning User Guide.	❑
13. Determine the key password used for storing the private keys for the Admin UI, PWS, and the RDU.	❑
14. Determine the ports used to access the Admin UI using HTTP or HTTP over SSL (HTTPS). The default ports are: • 8100—Listening port on Admin UI web server for HTTP communication • 8443—Listening port on Admin UI web server for HTTPS communication	❑
15. Determine the ports used to access the PWS using HTTP or HTTP over SSL (HTTPS). The default ports are: • 9100—Listening port on PWS web server for HTTP communication • 9443—Listening port on PWS web server for HTTPS communication	❑

Task	Checkoff
16. For the DPE, ensure that 2 GB of disk space is available in the data directory.	❑
17. For the PWS, ensure that 500 MB of disk space is available in the data directory.	❑
18. The PWS can communicate only with the Prime Cable Provisioning 5.3 RDU. It is not compatible with the RDUs of earlier versions. If you configure multiple RDU servers with PWS, ensure that the information of all the RDU servers is available.	❑
19. The web server for PWS and Admin UI must be configured and functioning normally.	❑
20. Ensure that Prime Network Registrar 8.x is installed and running on the servers on which you are installing Prime Cable Provisioning extensions, that is, the Prime Network Registrar Extension Points.	❑
21. For the Prime Network Registrar extensions, determine the name of the provisioning group for the Prime Network Registrar server.	❑
22. For the Prime Network Registrar extensions, determine the location to install the data directory *(BPR_DATA)*. The default directory is */var/CSCObac*.	❑
23. Verify that you have the necessary Prime Network Registrar configuration files. For an example of these configuration files, see the Cisco Prime Network Registrar Configurations.	❑
24. Verify that you have the KDC servers available, if you want to configure your network to support secure PacketCable voice technology.	❑

25. Enable your server to support IPv6.
To enable IPv6, login as root, and run:
`# ifconfig intf inet6 plumb up`
`# /usr/lib/inet/in.ndpd`
`# touch /etc/hostname6.intf`
where, intf—identifies the interface on which you want to enable IPv6.
	❑

In case of Linux, perform the following extra steps	

Task	Checkoff
26. Modify the *config* file to disable SELinux using the following command: `# vi /etc/selinux/config` where, config—File that controls the state of SELinux on the system. In this file, set the value of SELINUX to *disabled*.	❑
27. Disable iptables using the following command: `# chkconfig iptables off` **Note** The Admin UI page will not open if iptables is in enabled state on the system.	❑
28. Reboot the Prime Cable Provisioning host using the following command: `# reboot`	❑
29. Wait till the server boots up and re-login to continue with the installation.	❑

Installation Worksheet

During the installation of Prime Cable Provisioning, you are prompted for configuration information. The following table is a worksheet that you can use to record the information specific to your installation.

Table 2: Prime Cable Provisioning Installation Parameters

Prompt	Description	Default Value	Your Value
Home directory	Root directory to install Prime Cable Provisioning component	*/opt/CSCObac*	
Data directory	Root directory to install the data directory for Prime Cable Provisioning component	*/var/CSCObac*	
Database logs directory	Root directory to install the database transaction logs for Prime Cable Provisioning component	*/var/CSCObac/rdu/dblog*	
Logs directory	Root directory to install the general transaction logs for Prime Cable Provisioning components	• For RDU: */var/CSCObac/rdu/logs* • For DPE: */var/CSCObac/dpe/logs* • For PWS: */var/CSCObac/pws/logs*	
RDU host	Hostname of the server on which the RDU is installed	None	

Prompt	Description	Default Value	Your Value
RDU port number for nonsecured communication	Port number through which the RDU communicates with other Prime Cable Provisioning components in nonsecured mode	49187	
RDU port number for secured communication	Port number through which the RDU communicates with other Prime Cable Provisioning components in secured mode using SSL	49188	
Prime Network Registrar Extension Points provisioning group name	Name of the provisioning group for Prime Network Registrar Extension Points	None	
KDC realm name	Name of the Kerberos realm required by the KDC component	None	
KDC service key	Service key that the KDC server uses for communication with the provisioning FQDNs of DPEs	None	
Response file	Name and location of the response file that you generate to install these components during a noninteractive installation: • RDU • PWS • DPE • Prime Network Registrar Extension Points • KDC	None	
Port number of Admin UI	Port number through which you access the Prime Cable Provisioning Admin UI using HTTP	8100	
	Port number through which you access the Prime Cable Provisioning Admin UI using HTTP over SSL (HTTPS)	8443	

Prompt	Description	Default Value	Your Value
Port number of web services and API clients	Port number through which you access the web services or API clients using HTTP	9100	
	Port number through which you access the web services or API clients using HTTP over SSL (HTTPS)	9443	
Admin UI user password	Password using which you access the Prime Cable Provisioning Admin UI	changeme	
Web UI password	Password using which you access the Prime Network Registrar Admin UI	changeme	
Shared Secret password	Password using which you can encrypt the communication between Prime Cable Provisioning components and RDU	None	
Shared Secret key	Key using which you can encrypt the shared secret password	None	
Key Store password	Password using which you can encrypt the key store	None	
Key password	Password using which you can encrypt the certificate keys added in the key store	None	
Certificate files location	The location of the certificate files.	Default location (certificate is stored in these files): /opt/CSCObac/lib/security/rootCA.crt /opt/CSCObac/lib/security/rootCA.pem	
Certificate details	The inputs to generate the RDU certificate, Admin UI certificate, and the PWS certificate. The certificate is used for authentication during SSL communication	Unknown	
DPE password	Password using which you access the DPE in the login mode	changeme	
	Password using which you access the DPE in the privileged mode	None	
User and Group	Name of a root or non-root user	root/user1	
	Name of a root or non-root group	root/group1	