Introduction to DPE CLI

This chapter describes licensing and authentication requirements for the Cisco Prime Cable Provisioning Device Provisioning Engine (DPE) and how you can access the command-line interface (CLI) of the DPE.

DPE Licensing

Licensing controls the number of DPEs that you can use. To configure the DPE from the CLI, you must have a valid license. If you run the commands described in this guide on an unlicensed DPE, the following message appears:

```
This DPE is not licensed. Your request cannot be serviced. Please check with your
system administrator for DPE licenses.
```

For details on how to obtain the license file, see the *Cisco Prime Cable Provisioning 5.3 User Guide*.

Once you receive your license file, install Prime Cable Provisioning. Then, from the Admin UI, use the following procedure to install the licenses that you purchased:

Note Before installing your license, ensure that you back it up in case you have to reinstall Prime Cable Provisioning.

Step 1 Once you receive your license file, save each file on the system from which you intend to launch the Prime Cable Provisioning Admin UI.

Step 2 Launch your web browser on that system.

Step 3 Enter the administrator's location using this syntax:

`https://machine_name:port_number/`

- *machine_name*—Identifies the computer on which the RDU is running.
- *port_number*—Identifies the computer port on which the server side of the administrator application runs.

The default port number is:

- 8100 for HTTP over TCP
- 8443 for HTTP over SSL

The main login page appears.

Step 4 Enter the default username (**admin**) and default password (**changeme**).

Note If you are logging in for the first time, the Change Password screen appears. Enter a new password and confirm it. The password that you enter must have at least eight characters.

Step 5 Click **Login**.

The Main Menu page appears.

Step 6 Click the license link at the top of the Main Menu page, or choose **Configuration > License Keys**.

The Manage License Keys page appears.

Step 7 In the License File field, enter the complete path to the location of the license file on your local system. Remember to include the name of the license file while specifying the pathname. Or, click **Browse**.

The details regarding the license file appear. For details on licensing in this release, see the *Cisco Prime Cable Provisioning 5.3 User Guide*.

Accessing the DPE CLI

To access the DPE CLI, open a Telnet session to port 2323 from a local or remote host. Before you proceed, however, familiarize yourself with the access levels on the DPE.

Prime Cable Provisioning specifies a certain access level to authorize DPE access. Table 1-1 identifies the two access levels, which are also known as command modes. Each mode provides access to a specific set of commands.

Table 1-1 Command Modes on the DPE CLI

Mode	Description	Prompt
Login	Enables user commands for viewing the system configuration which requires PRIV_DPE_READ. In addition, to view device configuration PRIV_DEVICE_READ is required.	`bac_dpe>`
Enable	Enables privileged user commands for viewing, setting, and changing the system configuration, state, and data. Enable mode is controlled by PRIV_DPE_UPDATE and PRIV_DPE_SECURITY privileges.	`bac_dpe#`

Use the enable, page 2-5, and disable, page 2-4, commands to switch between the two modes.

You can access the DPE CLI following the steps described in:

- Accessing the DPE CLI from a Local Host, page 1-3
- Accessing the DPE CLI from a Remote Host, page 1-4

DPE CLI Privileges

Privileges required to access DPE CLI are:

Table 1-2 DPE CLI Privileges

Privilege	Description
PRIV_DPE_READ	Allows you to enter into login mode and view DPE status and settings.
PRIV_DPE_UPDATE	Allows you to enter into enable mode and set DPE properties and controlling of DPE lifecycle.
PRIV_DPE_SECURITY	Enables all security related Admin operations including changing DPE admin password, configuring authentication and shared secrets.
PRIV_DEVICE_READ	Enables viewing of device properties, searching for devices, and selecting devices. Also permits use of show device-config command in the DPE CLI.

For the complete list of default privileges in Prime Cable Provisioning see the Default Privileges section of the *Cisco Prime Cable Provisioning 5.3 User Guide*.

Accessing the DPE CLI from a Local Host

To access the CLI from a local host, you can use:

```
# telnet local_hostname 2323
```

where *local_hostname* specifies the name of the local host.

Or, you can use:

```
# telnet 0 2323
```

Defaults

Once you access the CLI, enter the DPE username and password to continue. The default login username is **admin** and password is **changeme**. Unlike the earlier releases of Prime Cable Provisioning, there is no need for second challenge (entering of password) to enter into enable mode. User can enter into enable mode based on the assigned privileges. For the list of DPE CLI privileges, see DPE CLI Privileges, page 1-3.

Note Although the default DPE username is admin and password is **changeme**, it is not the same as the one that you use to access the Prime Cable Provisioning Admin UI. The default admin user in DPE and RDU are two different users.

For information on how to change the login password, see password, page 2-7.

Examples

This result occurs when you access the DPE from a local host specifying its hostname.

```
bac_host# telnet local_bac_dpe 2323
Trying 10.10.2.25...
Connected to local_bac_dpe.example.com.
Escape character is '^]'.
```

```
Cisco Prime Cable Provisioning 5.1 (SOL_BAC5_1_0_00000000_0000)
Device Provisioning Engine local_bac_dpe

User Access Verification
Username: admin
Password: <changeme>

local_bac_dpe> enable
local_bac_dpe#
```

This result occurs when you access the DPE from a local host without specifying its hostname.

```
bac_host# telnet 0 2323
Trying 0.0.0.0...
Connected to 0.
Escape character is '^]'.

Cisco Prime Cable Provisioning 5.1 (SOL_BAC5_1_0_00000000_0000)
Device Provisioning Engine local_bac_dpe

User Access Verification
Username: admin
Password: <changeme>

bac_dpe> enable
bac_dpe#
```

Accessing the DPE CLI from a Remote Host

To access the CLI from a remote host, enter:

```
# telnet remote_hostname 2323
```

where *remote_hostname* specifies the name of the remote host.

Note If you cannot establish a Telnet connection to the CLI, the CLI server is probably not running. You may need to start the server. To start the server, enter:

```
# /etc/init.d/bprAgent start cli
```

Defaults

Once you access the CLI, you must enter the DPE username and password to continue. The default login username is **admin** and password is **changeme**.

Note Although the default DPE username is admin and password is changeme, it is not the same as the one that you use to access the Prime Cable Provisioning Admin UI. The default admin user in DPE and RDU are two different users.

For information on how to change the login password, see password, page 2-7.

Examples

This result occurs when you access the DPE from a remote host specifying its hostname.

```
bac_host# telnet remote_bac_dpe 2323
Trying 10.10.2.10...
```

```
Connected to remote_bac_dpe.example.com.
Escape character is '^]'.

Cisco Prime Cable Provisioning 5.1 (SOL_BAC5_1_0_00000000_0000)
Device Provisioning Engine remote_bac_dpe

User Access Verification
Username: admin
Password: <changeme>

remote_bac_dpe> enable
remote_bac_dpe#
```

Authentication Support

DPE CLI supports RADIUS and TACACS+ protocols for authenticating a user. Also the local user **admin** can be used to log into DPE CLI. You cannot configure both RADIUS and TACACS+ protocols together. Also, even when none of the protocols is configured, the local user **admin** can still be used for authentication. See Chapter 2, "System Commands" for details about the DPE CLI commands.

Local Authentication

This mode authenticates the default **admin** user in the local DPE and this mode is always enabled. In DPE CLI there is only one local account, admin. Users accessing the RDU cannot log into DPE CLI.

RADIUS Authentication

RADIUS is a UDP-based protocol used for enabling centralized authentication, authorization, and accounting for network access. It authenticates the users accessing the network services via the RADIUS server using the RADIUS standard protocol.

Cisco AV-pair needs to be configured in the RADIUS server to support authorization for DPE CLI RADIUS users. Cisco IOS/PIX 6.x is the RADIUS server that supports Cisco AV-pair in the Access Control Server (ACS) server. The Cisco AV-pair attribute value is:

cp:groups=<group-name>

For example:

cp:groups=Administrators

Here, Administrators is either the actual user group or user group mapping defined in the RDU. For more details, see the RADIUS Authentication section of the *Cisco Prime Cable Provisioning 5.3 User Guide*.

Note Any changes made to the user groups associated with the user will be reflected only in the next telnet session.

To enable backward compatibility, support of shell privileges priv-lvl=1 and priv-lvl=15 is continued.

Where, priv-lvl=1 is mapped to the privilege PRIV_DPE_READ and priv-lvl=15 is mapped to privileges PRIV_DPE_READ, PRIV_DEVICE_READ, PRIV_DPE_SECURITY, and PRIV_DPE_UPDATE.

Note Use of shell privileges is not a recommended method for authorizing DPE CLI RADIUS users. This method must be used only for backward compatibility.

TACACS+ Authentication

TACACS+ is a TCP-based protocol that supports centralized access control for several network devices and user authentication for the DPE CLI. Using TACACS+, a DPE supports multiple users (and their individual usernames) and the login password configured at the TACACS+ server. Here is how mapping of privileges is done in case of a TACACS+ server:

- The user must have priv-lvl=1 configured in the TACACS+ server for successful authentication. The user needs to have priv-lvl=15 configured in the TACACS+ server for entering into the enable mode.
- On successful authentication, user with priv-lvl=1 is assigned with the privilege PRIV_DPE_READ.
- On successful authorization in the enable mode, user with priv-lvl=15 is assigned with privileges PRIV_DPE_READ, PRIV_DEVICE_READ, PRIV_DPE_SECURITY, and PRIV_DPE_UPDATE.
- In the earlier release of Prime Cable Provisioning, user's password was required during login authentication and during the enable mode authentication. Now, password is not required during the enable mode authentication. Instead the password which has been entered during initial authentication is used for entering into the enable mode. Hence, the user should be configured with the same password for login authentication and enable mode authentication in the TACACS+ server.
- While logging into DPE CLI, if you enter the username as **admin**, the CLI falls back to local authentication mode. In this mode, you must enter both username and password. Once DPE CLI enters into local authentication mode, if wrong credentials are provided, the CLI prompts for the credentials again, now if TACACS+ username is entered, log in will not work. To log in using a TACACS+ username, the telnet session must be initiated again.
- If TACACS+ authentication is enabled in DPE CLI, but the server is not reachable, the CLI falls back to local authentication mode.
- When TACACS+ authentication is enabled in DPE CLI, if you enter wrong credentials accidentally, CLI prompts for username and password again. However, if you enter the username as **admin**, the CLI falls back to local authentication mode.