TAP-005

Clear Command Privileges Errors (Pxxx)

PURPOSE

Provides procedures for clearing command privileges errors (Pxxx)

GENERAL

A command privileges error is generated when unauthorized entrance is made by a user or an interface.

Procedure

1. ***NOTE:*** *See TAP-001 for assistance in analyzing alarms and isolating alarms to specific Network Elements (NEs).*

   Are you logged on to the alarmed NE?
   If yes, go to step 3.
   If no, go to step 2.

2. Log on to the NE (DLP-117).

3. ***NOTE:*** *For additional information on Security/User Authorization, see TNG-510.*

NOTE: *The ability to download to an NE requires SUPERUSER status for all 1603 SM software releases prior to R05.00.00. For R05.00.00 and later releases, all security categories for user must be equal to seven.*
From Table A, find the error code received and go to the step indicated.
Table A. Privilege Error Codes

CODE	DESCRIPTION	STEP
PICC	Privilege, invalid command code. The command entered is not executable because the	4

	session or user is not allowed to use the command that received the error.	
PIMA	Privilege, invalid memory address. The address is not accessible by the session or user.	25
PIUC	Privilege, illegal user code. The user is trying to change own authorization levels with an ENT/ED command, or the stated user code is illegal.	28
PIUI	Privilege, illegal user identity. The user ID or password is not acceptable (illegal, wrong format, or password already used).	38
PLNA	Privilege, logon not active. A command requiring logon was entered, but no logon session is active.	42

Code - PICC

1. The security categories are PCMAINT (Maintenance Privilege Code with levels 0-7), PCPROV (Provisioning Privilege Code, 0-7), PCSECU (Security Privilege Code, 0-7), and PCTEST (Test Privilege Code, 0-7).

2. From the context menu, select the following menu items:

    Security>Command

3. Set Privilege Filter values to desired value and click on Retrieve. Scroll to the command desired (per the corresponding path that was executed).

4. Record the four command privilege codes.

5. From the Security - Command screen (arrived at in step 5), click on User tab key at top of the screen.

6. In the Security - User screen, click on the Retrieve button.

7. Record the four user privilege codes.

8. Align the codes of User (step 10) above Command (step 7). See Table B for example.

Table B. Comparison Between User and Command Privilege Codes

SCREEN	PRIVILEGE CODES			
	MAINTENANCE	PROVISIONING	SECURITY	TEST
User (step 10)	5	5	4	5
Command (step 7)	0	0	7	0

1. Is there a category in which there is comparison between non-zeroes?

   If yes, go to step 15.
   If no, go to step 13.

2. Execution is denied. See the system administrator.

3. STOP. This procedure is complete.

- 15 Are any command categories higher than corresponding user categories?

If yes, go to step 13.
If no, go to step 16.

- 16 From the Security - User screen (arrived at in step 8), click on Port Access tab key at top of the screen.

- 17 In the Security - Port Access screen, click on Retrieve. Note the Access Type for the port through which you are logged on to the NE.

- 18 Record the Maint, Prov, Secu, and Test Privilege Codes for the port through which you are logged on to the NE.

- 19 Align the codes of Port Access (step 18) above Command (step 7). Refer to Table C for an example.

Table C. Comparison Between Port Access and Command Privilege Codes

SCREEN	PRIVILEGE CODE			
	MAINTENANCE	PROVISIONING	SECURITY	TEST
Port Access (step 18)	4	4	4	4

Command (step 7)	0	0	7	0

1. Is there a category in which there is a comparison between non-zeroes?

   If yes, go to step 21.
   If no, go to step 22.

2. Are any command categories higher than corresponding port access categories?

   If yes, go to step 22.
   If no, go to step 24.

3. Execution is denied. See the system administrator or go to another Access Type port.

4. STOP. This procedure is complete.

5. 24 If the user and port access are higher in all categories that are compared, then execution should not be denied.

Look for other alarms that may prevent an execution. Go to TAP-001.

Code - PIMA

1. The user is inhibited from accessing a memory location.

2. Contact the system administrator.

3. STOP. This procedure is complete.

Code - PIUC

1. From the context menu, select the following menu items:

   Security>User

2. In the Security - User screen, click on the Retrieve button.

3. Record the levels of the Maint, Prov, Secu, and Test Privilege Codes.

4. Are the codes correct (0-7)?

If yes, go to step 35.
If no, go to step 32.

5. Have the system administrator log on and select the following menu items:

   Security>User

6. In the Security - User screen, have the system administrator add or modify the data, and click on the appropriate button (use Add or Modify buttons at bottom of the screen).

7. STOP. This procedure is complete.

8. If you are authorized to enter an ED/ENT-SECU command, you may be demoting your code levels.

   Compare command input data from the command that was alarmed to that retrieved (step 30).

9. System administrator must enter correct data.

10. STOP. This procedure is complete.

Code - PIUI

1. The probabilities include the following:

   ○ The User ID, with the password used, may not be correct.

   ○ The password may have been assigned to someone else.

   ○ The password entered has illegal characters (6 to 10 alphanumeric characters with minimum of one numeric and one non-TL1 symbolic character; e.g., ~ @ # $ % ^ + - _ =).

   ○ The User ID Aging Interval or Password Aging Interval has expired.

● Have the system administrator log on and select the following menu items:

Security>User

- In the Security - User screen, have the system administrator add or modify the data, and click on the appropriate button (use Add or Modify buttons at bottom of the screen).

- STOP. This procedure is complete.

Code - PLNA

1. PLNA error encountered. Command requiring a logon session entered, but no logon session active.

2. Log on to the NE ([DLP-117](#)).

3. STOP. This procedure is complete.