



ACT Commands

This chapter provides ACT (activate) commands for the Cisco ONS 15454 SDH.

1.1 Activate User

Usage Guidelines

This command opens a session with the Network Element (NE).



Note

- Passwords are masked for the following security commands: ACT-USER, COPY-RFILE, COPY-IOSCFG, ED-PID, ENT-USER-SECU and ED-USER-SECU. Access to a transaction language 1 (TL1) session via any means will have the password masked. The Cisco Transport Controller (CTC) Request History and Message Log will also show the masked commands. When a password-masked command is reissued by double-clicking the command from CTC Request History, the password will still be masked in the CTC Request History and Message Log. The actual password that was previously issued will be sent to the NE. To use a former command as a template only, single-click the command in CTC Request History. The command will be placed in the Command Request text box, where you can edit the appropriate fields prior to reissuing it.
- For the ACT-USER command:
ACT-USER:[TID]:[STRING]:CTAG::[STRING]
 - The syntax of the userid (first [STRING]) and the password (second [STRING]) are not checked.
 - Invalid syntax for both the userid and password is permitted, but the user can only log in if the userid/password match what is in the database.
 - The userid and password cannot exceed 10 characters.
- For the ACT-USER command, it is required that no error code be transmitted except to convey that the login is granted or denied. Per TR-835, Appendix A, Section A.2:
“... the error codes corresponding to ACT ... do not apply to the ACT-USER command because this command requires that no error code be provided to the session request except to indicate that it has been denied. Before a session is established, a specific error code might reveal clues to an intruder attempting unauthorized entry.”
- The following feature can be turned on or off, and the default is off: A new user must change his or her password after establishing a session for the first time before continuing. All TL1 commands except for ED-PID and CANC-USER will be denied until the password is changed. Once the

password has been changed, a user can execute any command that his security level allows. If the user logs out without changing his password, each following session will DENY all commands, except ED-PID and CANC-USER, until the password is changed.

Category Security

Security N/A

Input Format ACT-USER:[<TID>]:<UID>:<CTAG>[::<PID>];

Input Example ACT-USER:PETALUMA:TERRI:100::MYPASSWD;

Input Parameters

Table 1-1 ACT-USER Input Parameters

Parameter and Values	Description
UID	The user identifier (userid) of the person logged in. UID can be any combination of up to 10 alphanumeric characters. String. Must not be null
PID	The user password. PID is any combination of up to 10 alphanumeric characters. Passwords are encrypted for security reasons and will appear as asterisks (*). String. Must not be null

Output Format SID DATE TIME
M CTAG COMPLD
“<UID>:<LASTLOGINTIME>,<UNSUCCESSFULLOGINS>”
;

Output Example TID-000 1998-06-20 14:30:00
M 001 COMPLD
“TERRI:2003-01-02 14-04-49,0”
;

Output Parameters**Table 1-2** *ACT-USER Output Parameters*

Parameter and Values	Description
UID	The user identifier (userid) of the person logged in. UID can be any combination of up to 10 alphanumeric characters. String. Must not be null
LASTLOGINTIME	The date and time of the last successful connection to the NE (not including current login). String
UNSUCCESSFULLOGINS	The number of unsuccessful login attempts since the last successful login. Integer

