Command: ED-SECU-USER

Message category: Security Administration
Application: Add/Drop, Rings

Definition:

Edit security level for user.

Restrictions:

All parameters in this command are position-defined except the *uid_nblk* parameter, which contains name-defined parameters. The session user cannot raise any user's privilege code to a level greater than or equal to his/her own security privilege code. Only the superuser can edit a user to have a privilege code equal to his own privilege code.

Function:

To edit the security level(s), the PID, the UID, the DBCHG parameter, the timeout disable parameter, and the password aging parameters for the specified user.

Command Format:

ED-SECU-USER:[tid]:uid:[ctag]::[nuid],[npid],,[pcmaint],[pcprov],[pcsecu],
[pctest]:[uid_nblk];

Command Parameters	
PARAMETER	**EXPLANATION**
[tid]	Identification of the target NE (1...20 characters). The NE's SID code is the recommended value. The default value is null.
uid	The user identification code which is used to identify the user whose password is to be changed. The parameter may be preceded by "AID=", although it is not required. Input of alpha characters is case-sensitive. The length of the name is 1...10 characters.
[ctag]	Correlation tag (1...6 characters) that links an input command with associated output responses. The default is 0.
[nuid]	New user identification code (1...10 characters). The value can be preceded by NUID=, but this is not required. Input is case-sensitive.

[npid]	New password (6...10 characters) for the user. The new password must be different from the old one and must include at least one digit, one letter, and one non-alphanumeric character. Input is case-sensitive. If the non-alphanumeric character is one of those interpreted by the parser as symbolic operators, the password must be enclosed in double quotes. See Table B (Syntactical Operators) in Appendix B (TL1 Language).
[pcmaint]	Authorization level (0...7) for the maintenance function. The value can be preceded by PCMAINT=, but this is not required. 1 indicates the least privileged level, and 7 the most privileged. 0 disables security checking for this category.
[pcprov]	Authorization level (0...7) for the provisioning function. The value can be preceded by PCPROV=, but this is not required. 1 indicates the least privileged level, and 7 the most privileged. 0 disables security checking for this category.
[pcsecu]	Authorization level (0...7) for the security function. The value can be preceded by PCSECU=, but this is not required. 1 indicates the least privileged level, and 7 the most privileged. 0 disables security checking for this category.
[pctest]	Authorization level (0...7) for the testing function. The value can be preceded by PCTEST=, but this is not required. 1 indicates the least privileged level, and 7 the most privileged. 0 disables security checking for this category.
[uid_nblk]	Named parameter block for user identification. The block consists of the following parameters in any order, separated by commas. Each parameter name is followed by an equal sign and a valid value.
	DBCHMSG= Whether database change messages are enabled for the specifed user. The generation of database change messages is enabled/disabled (for the entire NE) by the DBCHMSG parameter of the SET-NE-ALL command. Valid values are: Y Enabled. Database change messages are sent to the user session (Alcatel factory default). N

	Disabled. Database change messages are suppressed for the specified user. ***NOTE:*** *For X.25 connections, database change messages are not sent to NMA or TEST OS. Database change messages are always sent to CAMR concentrators.*
	PAGE= Length of time (0...999 days) until the password expires and must be changed. A value of zero disables the feature.
	UAGE= Length of time (0...999 days) until the UID is disabled if no successful logon session has occured. A value of zero disables the feature.
	TMDIS= Whether inactivity timeout is disabled. Valid values are: Y TMOUT disabled. Timeout interval is ignored. N TMOUT not disabled. Logon session is terminated when the timeout interval (set by the TMOUT parameter of the ED-SECU-CID command) expires. ***NOTE:*** *A TMOUT value of 0 for the* ED-SECU-CID *command also disables the timeout feature.*

Response Format:

Acknowledgment:

If, in less than 2 seconds, a normal or error response cannot be sent, the following acknowledgment response is sent:

```
IP <ctag>
```

After the above response, a new command input may be generated.

Normal Response:

```
    sid yy-mm-dd hh:mm:ss
M   c COMPLD
    /* ED-SECU-USER:[tid]:uid:[ctag]::[nuid],[npid],,[pcmaint], */
    /* [pcprov],[pcsecu],[pctest]:[uid_nblk] */
;
```

Error Response:

```
    sid yy-mm-dd hh:mm:ss
M   c DENY
    /* ED-SECU-USER:[tid]:uid:[ctag]::[nuid],[npid],,[pcmaint], */
    /* [pcprov],[pcsecu],[pctest]:[uid_nblk] */
```

```
    errcde
;
```

Response Parameters	
PARAMETER	EXPLANATION
sid	Source NE identification
yy-mm-dd	Year (2 digits), month, and day
hh:mm:ss	Hour (00...23), minute, and second
M	Message generated in response to an input command
c	If provided, ctag, otherwise 0
COMPLD	Completed
DENY	Input command is denied
/* */	Enclosed are human readable comments - unspecified format
errcde	Error code (See Appendix C)

Example:

Change the user ID, DANIEL, to a new ID of DAN with password of LION#1, with the highest privileges, good for one year on UID, but one week on PID, and port time-out interval disabled. The report database change feature is enabled for this user.

ENT-SECU-USER:RAL:DANIEL:656::DAN,LION#1,,7,7,7,7:DBCHMSG=Y,PAGE=7, UAGE=365,TMDIS=Y;

```
    RAL 99-11-16 14:10:04
M  656 COMPLD
    /* ENT-SECU-USER:RAL:DANIEL:656::DAN,LION#1,,7,7,7,7:DBCHMSG=Y, */
    /* PAGE=7,UAGE=365,TMDIS=Y */
;
```


Related Commands:

ED-SECU-CID	ENT-SECU-USER	RTRV-SECU-UPC
ED-SECU-CMD	RTRV-SECU-CID	RTRV-SECU-USER
ED-SECU-PID	RTRV-SECU-CM	