CHAPTER 15

Security

Revised: July 24, 2009, OL-3743-42

Security tables are used to report user activities and manage user accounts.

Note In this chapter, an asterisk preceding a token name means the token is mandatory. A token without an asterisk is optional.

Activity Summary

See Chapter 9, "History."

Command Level

The Command Level (command-level) table identifies the ten command levels and their descriptions.

Table Name: COMMAND-LEVEL

Table Containment Area: OAMP

Command Types

Show and change

Examples

```
show command-level id=10;
change command-level id=10; description=This is the highest level administration access;
```

Usage Guidelines

Primary Key Token(s): id

Change Rules: None.

Syntax Description

* ID	Primary key. Command level number. NUMERIC: 1–10.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DESCRIPTION (EMS-only field)	Mandatory for change command; optional for show command. Described by the service provider. VARCHAR(64): 1–64 ASCII characters.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).

Command Table

The Command Table (command-table) table allows a system administrator to show, change, and reset the command privilege level (CPL) of a specific noun-verb pair. Higher command privilege levels are granted all lower level privileges.

Table Name: COMMAND-TABLE

Table Containment Area: OAMP

Command Types

Show, change, and reset

Examples

```
show command-table noun=mgw; verb=add;
change command-table noun=mgw; verb=add; sec-level=9;
reset command-table noun=mgw; verb=add;
```

Usage Guidelines

Primary Key Token(s): noun

Change Rules: Noun and verb must exist.

Syntax Description

* NOUN	Primary key. The table or command name, such as User, MGW, CA, TGN-ID. VARCHAR(65): 1–65 ASCII characters.
* VERB	Verb used in the reported command. Valid verbs are add, audit, change, clear, control, delete, report, reset, show, and status. VARCHAR(8): 1–8 ASCII characters.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.

ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
SEC-LEVEL	Mandatory for change command. Security level. Used only in the change command. NUMERIC: 1–10.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).
WORK-GROUPS	Assigns a command to a given workgroup. A workgroup is a logical collection of commands created by the service provider. Valid only for the change command. Use the equal sign (=) to add a command to a workgroup for the first time, or to replace all existing workgroups of that command with one or more new workgroups. A plus sign (+) before the work-groups name adds one or more workgroups to a command. A minus sign (–) before the work-groups name removes one or more workgroups from a command. For example: change command-table noun=somenoun; verb=someverb; work-groups=newworkgroup; VARCHAR(64): 1–64 ASCII characters.

Password

The Password command allows the system administrator to reset any user's password. It also allows setting the number of days that the password is valid and the number of days before password expiration that the user is warned. It also forces the system administrator to enter a new password. Once the user logs in for the first time, the user should execute this command again to change the password.

Users can only reset their own passwords. Users are allowed to reset the days a password is valid, the number of days before password expiration, and the user must enter a new password when executing this command.

This command is not directly associated with any table. It checks if a user exists and manages the system password attributes.

Command Types

Reset

Examples

```
reset password name=wilburwabash; days-valid=15; warn=2; new-password=table1R;
```

Usage Guidelines

Primary Key Token(s): name

Reset Rules: User must exist.

You must construct passwords to meet the following UNIX standards:

- A password must have at least six characters. If it is longer than six characters, only the first eight characters are significant.
- A password must contain at least two alphabetic characters and at least one numeric or special character. In this case, *alphabetic* refers to all upper- or lowercase letters.
- A password must differ from the user's login name and any reverse or circular shift of that login name. For comparison purposes, an uppercase letter and its corresponding lowercase letter are equivalent.
- New passwords must differ from the old by in the first three characters. For comparison purposes, an uppercase letter and its corresponding lowercase letter are equivalent.

Syntax Description

* NAME	Primary key. Username, entered into the system by the system administrator. VARCHAR(16): 1–16 ASCII characters.
* NEW-PASSWORD	Specifies a password for a user. VARCHAR(12): 6–12 ASCII characters.
DAYS-VALID	Number of days a password is valid. NUMERIC: 0–364 (Default = 30).
WARN	Number of days before password expiration to start warning the user. NUMERIC: 0–10 (Default = 4).

Security Summary

The Security Summary (security-summary) command provides a summary report of security infractions by source and start/stop times from the Security Log (securitylog) table. The table logs at least 30 days of infractions. It writes and deletes only when infractions occur. For example, if a security infraction occurred 10 days ago, and none since, that infraction will show up in the database today when a show is performed. On the next infraction, all security violations 7 days prior to the current infraction are lost.

Table Name: SECURITYLOG

Table Containment Area: OAMP

Command Types

Report

Examples

```
report security-summary start-time=2002-03-27 00:00:00; end-time=2002-03-27 00:00:00;
source=all;
```

Note If this command is entered without any tokens, the report shows all security infractions.

Usage Guidelines Primary Key Token(s): None.

Syntax Description

START-TIME	Starting time for a security summary. Enter all 19 ASCII characters as shown. If you enter a start-time—but not an end-time— the report will show security infractions from the start-time to the present. Start-time must occur before end-time. Security items are available for the current and previous calendar days only (up to a maximum of 48 hours of events). If you enter this command without any tokens, the report returns all security infractions. DATE and TIME: yyyy-mm-dd hh:mm:ss.
END-TIME	Ending time for security summary. Enter all 19 ASCII characters as shown. If you enter an end-time—but not a start-time—the report returns all security infractions up to the end-time. DATE and TIME: yyyy-mm-dd hh:mm:ss.
SOURCE	Source of the infraction—name in the Users table. Source is actually the username. If you enter source without a start-time or end-time, all infractions are shown. VARCHAR(16): 1–16 ASCII characters.
AUTO-REFRESH	Specifies whether to display cached data on the screen. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DISPLAY	Specifies what token information to display on the screen. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
LIMIT	Specifies the number of rows to display on the screen. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
START-ROW	Specifies to begin displaying data on the screen at a specific row. INTEGER: 1–100000000 (Default = 1).

Users

The User (user) command identifies each user with the designated command level in the Security Level (securitylevels) table. The system administrator enters the command level for each user.

Table Name: SECURITYLEVELS

Table Containment Area: OAMP

Command Types

Show, add, change, and delete

Examples

```
show user name=john smith;
add user name=john smith; command-level=1;work-groups=thisworkgroup, thatworkgroup;
```

Note As of Release 4.5, setting a user password is done in one step by using the new mandatory password token in the add user command. For example:

```
add user name=UserABC;command_level=9;warn=5;days-valid=50;shell=CLI;password=secret01;
```

```
change user name=john smith; command-level=5;
```

Note To change a user's shell, delete the user and re-add specifying **shell=maint** or **cli**.
To change a password, use the **reset password** command. See the Password section for more information.

As of Release 4.5, it is possible to change user attributes days-valid and warn by using the change user command. For example:

```
change user name=john; command-level=5;warn=1;
change user name=jobh; command-level=5;warn=2;days-valid=45;
change user name=john; command-level=1;days-valid=4;
```

```
delete user name=john smith;
```

Usage Guidelines

Primary Key Token(s): name

Add Rules:

- user must not exist in the User table.
- name and command-level must both be entered in the add command.
- password must be entered.

Change Rules: User must exist in the User table. Name and command-level must both be entered in the change command.

Delete Rules: User must exist in the User table.

Note A user's actual password is stored in the Cisco BTS 10200 Softswitch EMS. It is not included here. A new user is not prompted to change a new password at first login. Users must change their password themselves at first login. Thereafter, they enter that password upon login to the EMS.

Syntax Description

* COMMAND-LEVEL	User command level, entered into the system by the system administrator. This token is optional for the show command; it is mandatory for the add and change commands. NUMERIC: 1–10.
* NAME	Primary key. Username, entered into the system by the system administrator. VARCHAR(16): 1–16 ASCII characters.
* PASSWORD (Release 4.5)	User password. See the Password section for user password creation requirements. VARCHAR(12): 6–12 ASCII characters.
AUTO-REFRESH	Specifies whether to display cached data on the screen. Valid only for the show command. CHAR(1): Y/N (Default = Y). Y—Queries the database for the most current data. N—Queries the database for the most current data only if the cached data is unavailable.
DAYS-VALID	Number of days a password is valid. NUMERIC: 0–364 (Default = 30).
DISPLAY	Specifies what token information to display on the screen. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all tokens are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.
FIRST	Not provisionable. Indicates whether an account has been used more than once. On a second login, the “true” indicator of a new account is changed to “false.” CHAR(1): T/F (Default = T).
LIMIT	Specifies the number of rows to display on the screen. Valid only for the show command. INTEGER: 1–100000000 (Default = 100000000). **Note** The actual maximum number of rows displayed is currently lower than 100000000 due to software limitations.
ORDER	Specifies whether to display data on the screen in a sorted order. Valid only for the show command. VARCHAR(1024): 1–1024 (Default = all rows are displayed). Permitted values are any valid token that can be shown for this command. Multiple tokens can be entered by separating with a comma.

SHELL	Specifies the type of interface for the user. This token is valid only for the add command. Delete and then re-add the user to change the type of shell. VARCHAR(5): CLI or MAINT (Default = CLI). CLI—User interface for entering commands and their parameters in command-line format. A user must log in to the active EMS. The session terminates if it is idle for a provisionable number of minutes (see the idle-time parameter in the Session table, default = 30 minutes) or if there is an EMS switchover from active to standby. This shell displays the CLI> prompt. MAINT—Maintenance interface for CLI commands that does not time out or disconnect on switchover. This shell can be used, when necessary, for maintenance and recovery purposes. The MAINT user can login to either the active or standby EMS. This interface displays a prompt based on the username, rather than a CLI> prompt. **Caution** The MAINT shell is not intended for normal provisioning activities. Use it only if the CLI shell is unusable in a maintenance or recovery scenario. An unattended MAINT session does not autodisconnect.
START-DATE	Not provisionable. Specifies the date the account was first used. Used to track and age idle accounts. DATE: YYYY-MM-DD.
START-ROW	Specifies to begin displaying data on the screen at a specific row. Valid only for the show command. INTEGER: 1–100000000 (Default = 1).
WARN	Number of days before password expiration to start warning the user. NUMERIC: 0–10 (Default = 4).

WORK-GROUPS	Logical collection of commands created by the service provider. Valid only for the change command. Use the equal sign (=) to add a user to a work-group for the first time, or to replace all existing workgroups of that user with one or more new workgroups. A plus sign (+) before the work-group name adds one or more workgroups to an existing user via the change command. This does not replace any already existing workgroups. A minus sign (–) before the work-group name removes one or more workgroups from an existing user via the change command. The following examples show the ways to specify values for the work-group token: • Specifying work-groups = +somewkgrp adds the user somewkgrp to the workgroups. • Specifying work-groups = -someoldwkgrp deletes the user someoldwkgrp from the work-groups. • Specifying work-groups = somenewworkgroup either adds somenewworkgroup for the first time, or replaces any previously existing work-groups with somenewworkgroup. **Note** The plus or minus sign is not allowed when adding a new user. Use the plus or minus sign only with the change command. VARCHAR(64): 1–64 ASCII characters.