



CHAPTER 2

Managing BTS Users and Commands using EMS

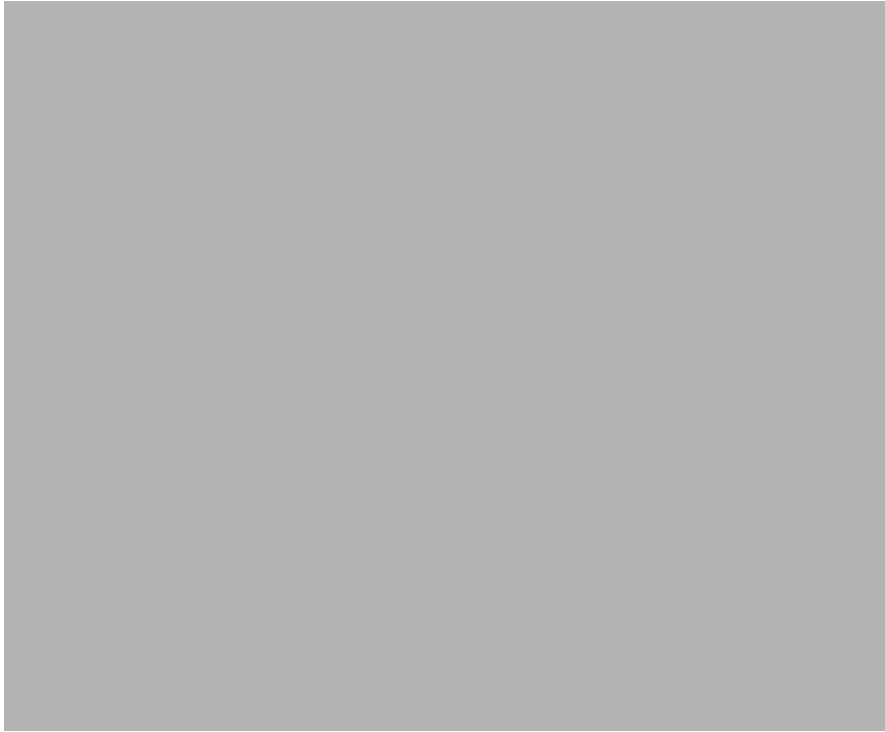
Revised: September 25, 2009, OL-12797-09

Introduction

This chapter describes operator interfaces to the BTS and how to manage access and users. The Element Management System (EMS) database holds up to 256 logins and up to 50 active user sessions.

Accessing the EMS

Using CLI you can locally connect to the EMS in an interactive session.

Figure 2-1 EMS Operator Interfaces

The EMS system administrator can:

- Add a new user.
- Assign a user's privilege level—10 is for the system administrator. BTS has predefined user accounts:
 - btsadmin—Username=btsadmin and password=btsadmin—like secadmin, MAINT shell user (MAINT shell is an enhanced CLI interface and does not log off an idle user)
 - secadmin—Username=secadmin and password=secadmin—like btsadmin, MAINT shell user (MAINT shell is an enhanced CLI interface and does not log off an idle user)
 - btsuser—Username=btsuser and password=btsuser—lower access permissions than btsadmin and secadmin, good for generic provisioning access
- Reset a user's password.
- Enter a description for each security class and privilege level.
- Manage security log reporting.

Logging into the EMS Using CLI

SSH is a way to access the BTS CLI or maintenance (MAINT) modes. SSH provides encrypted communication between a remote machine and the EMS/CA for executing CLI or MAINT commands. The SSH server runs on EMSs and CAs. To connect the client and server sides run the secure shell daemon (SSHD). With SSH, new users must enter a new password and reenter that password during the first login. In future logins they are prompted once for a password only.

When logging in for the first time, system administrators log in as `btsadmin` (the default password is `btsadmin`). Change the password.

Step 1 To log in from the client side for the first time: `ssh btsadmin@<ipaddress>`.



Note If you are logged in to the system as `root`, enter: `btsadmin@0`

On the first SSH login from the client side, expect a message like this:

```
The authenticity of host [hostname] can't be established.
Key fingerprint is 1024 5f:a0:0b:65:d3:82:df:ab:42:62:6d:98:9c:fe:e9:52.
Are you sure you want to continue connecting (yes/no)?
```

Step 2 Enter `yes`.

The password prompt appears, now all communications are encrypted.

Step 3 Enter your password.

The system responds with a CLI> prompt. You can now send commands to the EMS.

Step 4 Enter provisioning commands.

Step 5 To log off, enter `exit`.

Managing Users

You must have a user privilege level of 9 or higher to add, show, change, or delete a user.



Caution

Do not add, change, or delete username `root`, this prevents proper EMS access.

Table 2-1 Managing Users

Task	Sample Command
Adding a user	<ol style="list-style-type: none"> <code>add user name=UserABC; command-level=9; warn=10; days-valid=30; work-groups=somegroup; password=secret01;</code> <p>Note The name, command-level, and password tokens are mandatory tokens for the command 'add user'.</p> <ol style="list-style-type: none"> Supply a default password: <code>reset password name=<user name>; new-password=<user password>;</code>
Viewing a user	<code>show user name=UserABC;</code>
Viewing user activity	<code>show ems;</code>
Changing a user	<code>change user name=UserABC; command-level=1; work-groups=somegroup;</code>

Table 2-1 Managing Users (continued)

Task	Sample Command
Deleting a user	<pre>delete user name=UserABC;</pre> <p>You cannot delete <i>optiuser</i>.</p>
Changing a user's password	<pre>reset password name=username; days-valid=<number of days the new password will be valid>; warn=<number of days before password expiration to warn user>;</pre> <pre>reset password name=username; days-valid=30; warn=4;</pre> <p>A password must:</p> <ul style="list-style-type: none"> • Have 6-8 characters • Have at least two alphabetic characters • Have at least one numeric or special character • Differ from the user's login name and any combination of the login name • Differ from the old password by at least three characters <p>Change the password for user <i>optiuser</i> on each BTS.</p>
Adding a new work-group	<pre>change command-table noun=mgw; verb=add; work-groups=latex;</pre>
Adding a user to a work-group	<pre>change user name=trs80nut; work-groups=+rubber;</pre>
Removing a user from a work-group	<pre>change user name=trs80nut; work-groups=-latex;</pre>
Viewing all currently active users	<pre>show session</pre>
Viewing an active user	<pre>show session terminal</pre>

Table 2-1 Managing Users (continued)

Task	Sample Command
Blocking an active user	<p>1. Select operation mode:</p> <ul style="list-style-type: none"> • MAINTENANCE—(default) for regular maintenance • UPGRADE—for upgrades <p>2. <code>block session terminal=USR16;</code></p> <p>Note You cannot block the session of a user with higher privileges than yours.</p> <p>Prevent BTS provisioning during an upgrade or maintenance window from the following interfaces:</p> <ul style="list-style-type: none"> • CLI • FTP • CORBA • SNMP <p>Note The software will support blocking HTTP interfaces in a future release.</p> <p>If you block provisioning before performing an SMG restart or EMS reboot, blocking is still enforced when these applications return to in-service state.</p> <p>There are two levels of blocking:</p> <ul style="list-style-type: none"> • PROVISION—Prevents all provisioning commands from executing • COMPLETE—Prevents all commands from executing <p>Only terminal type MNT users can use these blocking and unblocking commands. MNT users are never blocked. MNT users issue these commands from either active or standby EMS.</p> <p>A blocking command applies to all non-MNT users on terminals on either active or standby EMS. Commands do not execute for:</p> <ul style="list-style-type: none"> • Logged-in users • Users who login after the block command <p>Commands are not queued for execution after unblock. The CLI user prompt changes when blocked, notifying the user their commands will not execute.</p>
Unblocking a user	<p><code>unblock session terminal=USR16;</code></p> <p>Note You cannot unblock the session of a user with higher privileges.</p>
Resetting a user's idle time	<p>Idle time is how many minutes (1-30) a user can be idle before being logged off the BTS.</p> <p><code>change session idle-time=30;</code></p>
Stopping a user's session	<p><code>stop session terminal=USR16;</code></p>

**Note**

All commands should be assigned to a work-group. If a command is not assigned to a work-group, a user will be able to execute that command, which is not recommended. You can also assign users and the commands to multiple work-groups.

Managing Commands

Each command (verb-noun combination) has a security class of 1-10; 1 is lowest, 10 is highest. Each time a user enters a command, the system compares the user's privilege level to the command's security class. EMS denies the command if the user level is less than the command level.

The Command Level (command-level) table shows the 10 command security classes. BTS has the following presets:

- 1 (lowest level)
- 5 (mid-level)
- 10 (highest level)—These commands require a system administrator with a security level of 10 to execute.

Table 2-2 Managing Commands

Task	Sample Command
Viewing a command's security class	<code>show command-level id=10;</code>
Adding a description to a command's security class	<code>change command-level id=10; description=This is the highest level administration access;</code>
Changing a command's privilege level	<code>change command-table noun=mgw; verb=add; sec-level=9;</code>
Resetting a command's privilege level	<code>reset command-table noun=mgw; verb=add;</code>
Viewing all executed commands	<code>show history;</code>
Sending all executed commands to a report file	<code>report history;</code>
Viewing the report of all executed commands	<ol style="list-style-type: none"> 1. In a web browser enter <code>http://server name</code>. 2. Click Reports. 3. Click <code>history.html</code>.
Viewing a security summary	<code>report security-summary start-time=2002-09-26 00:00:00; end-time=2002-09-27 00:00:00; source=all;</code>
Viewing security summary reports	In a web browser enter <code>https:// <ems ip addr></code> .

Restricting Command Access Using Workgroups

This section discusses about how to restrict access and secure commands by defining workgroups. As discussed earlier, a user privilege level (UPL) is assigned by the system administrator for a user's login. Each command has a preset command level (CL) for each noun-verb combination. A user could successfully execute a command if the privilege level assigned to the user is higher than or equal to the command level which is being executed.

The concept of allowing access by setting user privilege level higher than command privilege level allows any user with higher user privilege level to execute some critical commands, which we do not want. For example, special handling is provided for CALEA to prevent any user from accessing the wiretap and ESS tables. As a result, if a user has higher privilege level than the command level used in CALEA, the user can execute the commands and fetch critical data.

To restrict a user to only a certain set of commands, assign the user and the relevant commands to a workgroup 'X'. As a result, the user belonging to workgroup 'X' can only execute the commands which are having SEC_LEVEL <= User COMMAND_LEVEL and which are assigned to workgroup 'X'. For more details, see [Table 2-3](#).

To restrict a user for example "USER0" to only a certain set of commands:

Step 1 Assign 'USER0' to work_group 'X'.

Step 2 Assign all the commands to a workgroup 'cli_all_workgroup'. No commands must be left out without workgroup assignment.



Note

If any command is left without workgroup assignment, the USER0 would be able to execute the command which we do not want.

Step 3 Assign the specific commands for which you want to allow access to USER0 to the workgroup 'X'.



Tip

For example, to allow access for the command 'change subscriber', assign the command 'change subscriber' to the workgroup 'X'. Earlier 'change subscriber' was not assigned to any workgroup. This way 'change subscriber' command was executable by any user, having User COMMAND_LEVEL >= SEC_LEVEL of command. Now after 'change subscriber' is assigned to workgroup 'X', not "every" user can now execute the 'change subscriber' command even if that user's, User COMMAND_LEVEL >= SEC_LEVEL of the command.

Table 2-3 Restricting Command Access Through Workgroups

Task	Sample Command
Add and assign a user to a workgroup. The workgroup is also created using the same command.	<code>add user name=USER0; command-level=9; password=secret01; work-groups=X;</code>
Assign all the commands to a workgroup. No commands should be left without workgroup assignments.	<code>change command-table noun=mgw; verb=add; sec-level=8; work-groups=cli_all_workgroup;</code>
Assign only the specific commands to the workgroup for which you want to restrict access for other users. Only the users assigned to the workgroup can access these commands.	<code>change command-table noun=subscriber; verb=change; sec-level=8; work-groups=X;</code>