



CHAPTER 2

Using Cisco E-DI

This chapter details how to configure and use Cisco E-DI features:

- [Setting up the Terminal](#)
- [Customizing the Default Prompt](#)
- [Keyboard Shortcuts](#)
- [Cisco E-DI Services](#)
- [Commonly Used Commands](#)
- [Using Session Based Device Authentication](#)
- [File System Commands](#)
- [Restarting the Server or a Device](#)
- [Restarting the Server or a Device](#)

Setting up the Terminal

The commands used to set up the terminal are detailed in [Table 2-1](#). You can enter the commands in server or network mode.

Table 2-1 *Commands to Setup the Terminal*

Action	Command
To set the terminal color mode. You can also use the key combination Ctrl-T from the server EXEC level to toggle between gray and color modes.	[SRV:/server NET:/network]# terminal color
The terminal display settings can be configured to use either hostname, DNS name, or the IP address of the device.	[SRV:/server NET:/network]# terminal device-id { dns-name dns-name-short ip name }
To define the FTP Authentication credentials. The credentials created using this command are used for downloading a file from an FTP site and for data backup and restore using FTP.	[SRV:/server NET:/network]# terminal ftp-auth username { word } Password
To define the HTTP Authentication credentials. The credentials created using this command are used for downloading a file from a website.	[SRV:/server NET:/network]# terminal http-auth username { word } Password

Table 2-1 **Commands to Setup the Terminal (continued)**

Action	Command
To make the session interactive.	[SRV:/server NET:/network] # terminal interactive
To specify the number of lines that are displayed on the terminal.	[SRV:/server NET:/network] # terminal length {0-1} {2-256}
When terminal monitor is enabled, any action on the Cisco E-DI server carried out on another session is displayed on the terminal.	[SRV:/server NET:/network] # terminal monitor message filter {word}
To disable the relevant terminal mode.	[SRV:/server NET:/network] # terminal no {color http-auth interactive monitor monitor message-filter skip-locked skip-unauth status-codes suppress-repeats}
To enable cursor wrap to next line on reaching the end of the line (in some terminals, for example Putty).	[SRV:/server NET:/network] # terminal [no] cursor-wrap
To set the terminal environment variable value.	[SRV:/server NET:/network] # terminal set {word} {word}
To skip all devices locked by some other user.	[SRV:/server NET:/network] # terminal skip-locked
To skip all devices that are not authorized to be included in a task.	[SRV:/server NET:/network] # terminal skip-unauth
To display the status code after command implementation.	[SRV:/server NET:/network] # terminal status-codes
To set the terminal stream control type. The xml-data-channel option converts the terminal from CLI mode to XML mode (NETCONF). See <i>Cisco Enhanced Device Interface Programmer's Guide, 2.2</i> for more details on establishing XML sessions with Cisco E-DI.	[SRV:/server NET:/network] # terminal stream-ctl {xml-data-channel {word}}
To turn the toggle options using the Ctrl key on and off.	[SRV:/server NET:/network] # terminal supress-repeats
To unset the terminal environment variable.	[SRV:/server NET:/network] # terminal unset {word}
To specify the text width displayed on the screen. The default terminal width is 80. The default terminal length is 24.	[SRV:/server NET:/network] # terminal width {16-256}
To format the output of show commands with pre-defined column width (default setting).	[SRV:/server NET:/network] # terminal format-report
To disable the pre-defined column width based formatting for reports. This command is useful in scripting.	[SRV:/server NET:/network] # terminal no format-report

Customizing the Default Prompt

The commands used to customize the default Cisco E-DI prompt are detailed in [Table 2-2](#). The commands can be given in server mode.

Table 2-2 **Commands to Customize the Default Cisco E-DI Prompt**

Action	Command
To customize the default Cisco E-DI prompt. This prompt is configured by the system administrator, and will be applicable for all users. It is saved to the running configuration. The prompt can include characters and function names as follows: • ServerName—Hostname of Cisco E-DI Server • User—Login ID of user • DIR—Current directory (ex: ~/) • ContextType—SRV or GRP or DEV or NET (entire network) • Context—Device IP address/name or Group name (existing prompt component) with status (when color is enabled) • Status—Alarm Code for the context (OK, Offline, P1, P2 .. P5) • DeviceIP—Device IP address (for single device) • DeviceName—Device Hostname (for single device) • PartialDir—Part of the directory (In device context, “/network/devices/” and “/network/groups/” in the current directory replaced with ~/.) The maximum length of the prompt is 75 characters. Ctrl characters are not allowed. A function is contained within %{ and } in the prompt definition. After the prompt expression is defined the functions are evaluated and displayed in the prompt. Any character that is not enclosed within %{ and } will be displayed in the terminal prompt. For example, if the prompt is customized as terminal prompt %{DeviceIp}-on- EDI-%{ServerName} and the DeviceIP (1.1.1.1) and ServerName (Dev-1) are the functions to be applied, the customized prompt will be 1.1.1.1-on-EDI-Dev-1. To include a space in the prompt, you should specify the <prompt expression> in double quotes (“ ”).	<pre>[SRV:/server] (config)# system prompt <prompt expression></pre>
To clear the customized prompt, and return to the default Cisco E-DI prompt.	<pre>[SRV:/server] (config)# no system prompt</pre>
To customize the default terminal prompt. This prompt is user defined, and applicable for that terminal only. It is valid for that session only. The prompt can include the characters and functions described above. This prompt has the highest priority. It will override the default Cisco E-DI prompt and the system defined prompt.	<pre>[SRV:/server]# terminal prompt <prompt expression></pre>

Table 2-2 *Commands to Customize the Default Cisco E-DI Prompt (continued)*

Action	Command
To clear the customized terminal prompt, and return to the default prompt.	[SRV:/server]# terminal no prompt
To save the terminal preferences set in the current session to a profile that will be stored in the user's home directory. Terminal properties like prompt, color, suppress-repeats, width, and length are saved to the profile. Other terminal properties such as auth-type and skip-unauth are not saved.	[SRV:/server]# terminal save properties

Keyboard Shortcuts

[Table 2-3](#) gives the keyboard shortcuts available in Cisco E-DI.

Table 2-3 *Keyboard Shortcuts and Associated Actions*

Shortcut	Action
?	Opens context sensitive help
Ctrl A	The cursor goes to the beginning of the line
Ctrl B	The cursor moves one character to the left
Ctrl C	Discards the current line
Ctrl D	Deletes the character at the cursor
Ctrl E	The cursor goes to the end of line
Ctrl F	The cursor moves one character to the right
Ctrl G	Displays the devices selected, the knowledge base applied and the applicability of the command to the devices selected in device configuration mode
Ctrl K	Deletes all characters from the cursor to the end of the command line
Ctrl N	Returns more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key
Ctrl P	Recalls commands in the history buffer, beginning with the most recent command
Ctrl R	Refreshes the current line
Ctrl T	Toggles between terminal color display
Ctrl U	Deletes all characters before the cursor to the beginning of the command line
Ctrl W	Deletes the word to the left of the cursor
Ctrl X	Deletes all characters before the cursor to the beginning of the command line
Ctrl Z	Exit from configuration mode
Enter	For paginated messages (more than one page), message scrolls one line up
Space bar	For paginated messages (more than one page), message scrolls one page up (equal to terminal length)
Tab	Completes a partial command

Cisco E-DI Services

Cisco E-DI includes a number of services, see [Table 2-4](#). To enable these services, see [Table 2-5](#).

You can configure services in Cisco E-DI according to the category of inventory data required, see [Table 7-1](#).

Table 2-4 Cisco E-DI Services

Service	Default	Description
asset	Enabled	Device asset collection service. Periodically collects information on device hardware assets such as chassis, cards, slot, power-supply, and fans.
editor	Enabled	Text editor service for CLI. Allows you to edit and create files on Cisco E-DI using a vi editor.
exec-cmd	Enabled	Direct network EXEC command service. Enables implementing commands on a device using exec-cmd command.
ftp-server	Disabled	FTPD server service. Enables or disables Cisco E-DI accessibility through FTP.
perl-scripting	Disabled	Perl scripting service for CLI. Enables implementation of perl scripts using perl command.
telnet	Disabled	Enables or disables Telnet service. Enables login to the Cisco E-DI server using Telnet.
trap-receiver	Enabled	SNMP trap receiver service. Enables the receiving and processing of SNMP traps. E-DI trap service listens on port 162 which is the default port to receive traps.

You can enable services in Cisco E-DI with these commands. See [Table 2-5](#)

Table 2-5 Commands to Enable Cisco E-DI Services

Action	Command
To enable the device asset collection service	[SVR:/server] (config)# service asset
To enable the text editor service for the CLI	[SVR:/server] (config)# service editor
To enable the direct network EXEC command service The behavior of this command changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-7 for a full explanation of the command behavior.	[SVR:/server] (config)# service exec-cmd
To enable the FTP server service	[SVR:/server] (config)# service ftp-server
To enable perl-scripting for the CLI	[SVR:/server] (config)# service perl-scripting

Table 2-5 *Commands to Enable Cisco E-DI Services (continued)*

Action	Command
To enable the telnet service	[SVR:/server] (config)# service telnet
To enable the SNMP trap receiver service	[SVR:/server] (config)# service trap-receiver E-DI trap service listens on port 162 which is the default port to receive traps.

Commonly Used Commands

[Table 2-6](#) details commands which are commonly used in Cisco E-DI.

Table 2-6 *Commonly Used Commands*

Action	Command
To enter the configure setup mode. The behavior of this command changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-7 for a full explanation of the command behavior.	config setup
To enter the configure terminal mode.	config t
To perform various diagnostic activities on the network.	diag
To download files using HTTP or FTP onto Cisco E-DI.	download
To exit out of the configuration mode. You can also use Ctrl-Z	end
To exit from the current configuration view and move to the parent view.	exit
To find the managed devices that match a certain criteria.	find
To show help on different topics based on the text input.	help
To put the discovered devices into the managed state.	import
To collect device(s) inventory. Used in network mode. The behavior of this command changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-7 for a full explanation of the command behavior.	inventory
To logout of the server.	logout
To query a DNS server to lookup and find IP address information for a host or device.	dnslookup
To ping a element in the network using its IP address or name.	ping

Table 2-6 Commonly Used Commands (continued)

Action	Command
To check the status of management operations in Cisco E-DI when session based device authentication is enabled. This command displays the status of the credentials for performing different management operations. It can be used to find out why an operation is not happening. These credentials are not validated with the device, instead the status indicates whether the required credentials are configured by the user or not.	<code>show devices manageability</code>
To synchronize the file system, device configuration and archives on the devices and the server.	<code>sync</code>
To trace a route to a network element using its IP address or name.	<code>traceroute</code>
To save the server running configuration to start-up configuration.	<code>write</code>

Click **Launch Visual Config Editor** or **Launch File Editor** to open the applications. See [Chapter 6, “Configuring Devices”](#) for information about managing configuration files using the GUI.

Using Session Based Device Authentication

Session based device authentication is used in an environment where there is an external AAA server. This mode requires a user to enter a login and password when running the commands in [Table 2-7](#). The behavior of these commands changes when session based device authentication is enabled, see [Table 2-7](#) for details.

If session based device authentication has been disabled, it can be enabled by entering the following command in server configuration mode:

```
[SVR:/server] (config) # device-auth session-based
```

To disable session based device authentication, enter the following command in server configuration mode:

```
[SVR:/server] (config) # no device-auth session-based
```

To specify the session credentials after session based device authentication is enabled, enter the following command in either server or network mode:

```
[NET:/network] # terminal device-auth login <login val>
```



Note

We do not recommend that you change the device authentication mode after you have started managing devices. If you need to change the mode, you should first clear all previous connections, enter the command **clear status connections**. Then change the authentication mode.

Table 2-7 Command Behavior When Session Based Device Authentication Is Enabled

Commands	Command Behavior When Session Based Device Authentication is Enabled
In EXEC Mode	
diag connectivity	If the command is run within a scheduled job, the Telnet/SSH connectivity test fails. When the command is run, the Telnet/SSH connectivity test uses the session's credential set for login and password. The enable password is taken from the credential set used to manage the device. If the session is not configured with device credentials, the following message appears for the login test: <pre>Device credentials are not configured for this session</pre> Configure the device credentials for this session, enter terminal device-auth
diag device	If the command is run within a scheduled job, the Telnet/SSH connectivity test fails. When the command is run, the Telnet/SSH connectivity test uses the session's credential set for login and password. The enable password is taken from the credential set used to manage the device. If the session is not configured with device credentials, the following message appears for the login test: <pre>Device credentials are not configured for this session</pre> Configure the device credentials for this session, enter terminal device-auth
config setup	If the device credentials for the session are not configured, the following message appears before entering config-setup mode: <pre>%WARNING: System is setup to use session based device authentication. Your current session is not configured with device credentials.</pre> Configure the device credentials for this session, enter terminal device-auth If you proceed with the configuration, the commit command will display the following error message: <pre>%System is configured to use session based device authentication. Your current session is not configured with device credentials</pre> Configure the device credentials for this session, enter terminal device-auth If the session is configured with device credentials, the commit operation would use the session's credential to establish a Telnet/SSH connection with the device and issue a copy tftp://ediserver/running-config command on the device. In session based device authentication mode, device configuration cannot be scheduled as a job.
sync config {fg bg}	If this command is run within a scheduled job, it will use SNMP Write operation to synchronize the configuration. If the SNMP Write community is not configured, this command will fail. The command uses the session's device credentials to establish a Telnet/SSH connection and downloads the configuration of the device to Cisco E-DI using TFTP transport. If the device credentials for the session are not configured, the command fails with the following message: <pre>%System is setup to use session based device authentication. Your current session is not configured with device credentials.</pre> Configure the device credentials for this session, enter terminal device-auth

Table 2-7 **Command Behavior When Session Based Device Authentication Is Enabled (continued)**

Commands	Command Behavior When Session Based Device Authentication is Enabled
sync filesystem {fg bg}	If this command is run within a scheduled job, it will fail. The command will use the session's device credentials to establish a Telnet/SSH connection and retrieve the device file system. If the device credentials for the session are not configured, the command fails with the following message: <pre>%System is setup to use session based device authentication. Your current session is not configured with device credentials.</pre> Configure the device credentials for this session, enter terminal device-auth
inventory	There is no change to basic inventory and asset inventory. The inventory command internally issues sync config and sync filesystem commands, the behavior of those commands within the inventory job is similar to the behavior describe above.
connect exec-mode exec-cmd <cmd>	These commands cannot be run from a scheduled job. These commands use the session's device credentials to establish a Telnet/SSH connection and run the specified command. If the device credentials for the session are not configured, the command fails with the following message: <pre>%System is setup to use session based device authentication. Your current session is not configured with device credentials.</pre> Configure the device credentials for this session, enter terminal device-auth
more <device-filename> copy <from-device> <to-server>	If this command is run within a scheduled job, it uses the SNMP Write operation to synchronize downloading the file from the device to Cisco E-DI using TFTP transport. If the SNMP Write community is not configured, this command will fail. The command uses the session's device credentials to establish a Telnet/SSH connection, and downloads the file from the device to Cisco E-DI using TFTP transport. If the device credentials for the session are not configured, the command fails with the following message: <pre>%System is setup to use session based device authentication. Your current session is not configured with device credentials.</pre> Configure the device credentials for this session, enter terminal device-auth
copy <from-server> <to-device>	If this command is run within a scheduled job, it will fail. The command uses the session's device credentials to establish a Telnet/SSH connection and downloads the file from Cisco E-DI to the device using TFTP transport. If the device credentials for the session are not configured, the command fails with the following message: <pre>%System is setup to use session based device authentication. Your current session is not configured with device credentials.</pre> Configure the device credentials for this session, enter terminal device-auth

Table 2-7 Command Behavior When Session Based Device Authentication Is Enabled (continued)

Commands	Command Behavior When Session Based Device Authentication is Enabled
write mem	If the device credentials for the session are not configured, the command fails with the following message: <pre>%WARNING: System is setup to use session based device authentication. Your current session is not configured with device credentials. You must use 'terminal device-auth' command to configure device credentials before executing this command.</pre> The command uses the session's device credentials to establish a Telnet/SSH connection and tftp transport to transfer files between Cisco E-DI and the device.
reload device	This is applicable in the network EXEC mode. If the device credentials for the session are not configured, the command fails with the following message: <pre>%WARNING: System is setup to use session based device authentication. Your current session is not configured with device credentials. You must use 'terminal device-auth' command to configure device credentials before executing this command.</pre> The command uses the session's device credentials to establish a Telnet/SSH connection to reload the managed device.
In Config mode	
login <login>	If the user attempts to configure any of these parameters in credential-set submode, Cisco E-DI will generate the following warning message: <pre>% Warning: This parameter is not applicable when session based device authentication is enabled</pre>
password <passwd>	
enable-password <enpassword>	
subscribe syslog	Syslog auto subscription cannot be enabled in session based device authentication mode. When the user enters the device-auth session-based command, syslog auto subscription will be turned off. Note The subscribe syslog feature will remain off if the user switches the mode back to non-session based authentication.

File System Commands

Cisco E-DI creates a virtual file system to represent the file systems on the managed devices. The virtual file system contains server, network and users directories in the root of the file system:

- **/server** directory contains directories and files related to Cisco E-DI such as directories for storing configuration archives, images and temporary files.
- **/network** directory contains the virtual file system representing file systems for all the devices currently managed.

This is a read-only file system. Files can be read from the devices, but cannot be written or deleted. The file systems of the devices are learned when the device is managed and are kept current with the device whenever a device inventory is performed. The file systems can also be updated with the **sync filesystem** command.

- **/users** directory contains one directory for each user of Cisco E-DI, which can be used to store user specific files.

Table 2-8 details commands to manage the file system.

Table 2-8 **Commands to Manage the File System**

Action	Command
To change the current directory.	[SVR:/server NET:/network]# cd {/} [name{/name/name...}]
To switch to the server root directory.	[SVR:/server]# cd /
To switch to the user's home directory.	[SVR:/server]# cd
To display the current working directory.	[SVR:/server NET:/network]# pwd
To create a directory with a specified name.	[SVR:/server NET:/network]# mkdir /{server/ network/} name
To remove the specified directory.	[SVR:/server NET:/network]# rmdir /{server/ network/} name
To show the contents of the current directory. If the filesystem service is disabled, the dir command under the device context shows the following warning message, Warning: filesystem service is disabled. Enter sync filesystem fg to manually synchronize the data.	[SVR:/server NET:/network]# dir
To view the contents of the specified file.	[SVR:/server NET:/network]# more /{server/ network/} name
To delete the specified file.	[SVR:/server NET:/network]# delete {/force /recursive name}
To copy a file. The behavior of this command changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-7 for a full explanation of the command behavior.	[SVR:/server NET:/network]# copy {source file destination file}
To rename a file.	[SVR:/server NET:/network]# rename name
To synchronize the file system on the server with the file system on the device. You can choose to synchronize the device in the background or the foreground. The behavior of this command changes when session based device authentication is enabled. See Using Session Based Device Authentication, page 2-7 for a full explanation of the command behavior.	[NET:/network]# sync filesystem {bg fg}



Note

You can also manage the file system using perl scripts. See [Chapter 10, “Using Perl Scripts”](#).

Restarting the Server or a Device

The command to restart the Cisco E-DI device is detailed in [Table 2-9](#).

Table 2-9 **Commands to Restart Devices**

Description	Command
Restart the specified devices.	[SVR:/server]# reload device ip-address1 [ip-address2..... .]