CHAPTER 4

Managing Security

The Cisco E-DI security features are described in detail in Security in Cisco E-DI, page 1-4.

Security in Cisco E-DI also includes the following features:

- Locking a Device
- Monitoring Changes in the Network

Locking a Device

Device locking prevents multiple users making concurrent changes to a device by limiting the write access to the owner of the lock. As long as the lock is held by you, all the other users will only have read access for the locked NEs. An administrator can override the locks, and clear them when desired.

A device will be locked as long as the user intends to hold it. Locks can be cleared when the user intends to relinquish the control of the entity.

A device lock does not prohibit configuration read access.

Table 4-1 details the commands used for working with device locking.

Device locks are one of the features that can be set up in the Cisco E-DI XML Programmatic Interface. See the *Cisco Enhanced Device Interface Programmer's Guide, 2.2* for more details.

Table 4-1 Commands to Lock Devices

Action	Command
To create a server lock.	`[SVR:/server]# lock reason text {message, message ..}`
To lock an individual device preventing any other user making any changes to the device.	`[NET:/network] (network ip_address)# lock reason text {message, message ..}`
To lock all the devices simultaneously at the network level, preventing any other user making any changes to the devices.	`[NET:/network]# lock reason text {message, message ..}`
To lock all devices in a group simultaneously to prevent any other user making any changes to the devices;	`[NET:/network] (network group name)# lock reason text message, message ..}`
To view all the locks currently held in the current context.	`[SVR:/server]# show locks`

Table 4-1 Commands to Lock Devices (continued)

Action	Command
To clear all the locks currently held in the current context. Use the option override to clear the locks held by other user (requires administrator privileges).	`[SVR:/server]# clear lock [ override ]`
To skip all devices locked by some other user, while performing any network level operations.	`[SRV:/server|NET:/network]# terminal skip-locked`

Monitoring Changes in the Network

The network administrator can monitor changes performed on the network through Cisco E-DI. Each user session is monitored, and all activities are logged against a pre-defined priority level (see Table 4-2).

All the tasks that can be performed on a Cisco E-DI server go through a change-log management system which checks the task's priority and logs it into the database. Detailed information about the task, the user, and the commands used to perform the task are logged.

You can configure what tasks should be logged based on a configuration setting. See Table 4-3.

Table 4-2 Task Priorities

Domain	Task Name	Priority Level
Any	View Devices	3
Any	View Alarms	3
Any	View Events	3
Any	XML Connection	3
Network	View Interfaces	3
Any	View Locks	4
Network	Show Network Connections	4
Network	View Network Reports	4
Server	View Server Reports	4
Server	View Server Lines	4
Server	Read Server Files	4
Any	Raise Alarm	5
Network	View Network Configuration	5
Network	Read Network Files	5
Server	View Server Config	5
Server	View Server History	5
Server	View Server Logs	5
Server	Modify Server Files	5
Network	Update Network Locks	6
Network	Implement Network Diagnostics	6

Table 4-2 Task Priorities (continued)

Domain	Task Name	Priority Level
Server	Update Server Lock	6
Server	Delete Server Files	6
Server	Backup Database	6
Server	Discover Devices	6
Network	Update Network Locks (Override)	7
Network	Collect Inventory From Devices	7
Network	Clear Network Reports	7
Network	Connect Exec-Mode To Devices	7
Network	Clear Network Events	7
Network	Clear Network Alarms	7
Network	Clear Network History	7
Network	Network Debug Logging	7
Server	Update Server Lock (Override)	7
Server	Clear Server Events	7
Server	Clear Server Alarms	7
Server	Clear Server Lines	7
Network	Change Network Configuration	8
Network	Change Network Configuration (From Terminal)	8
Network	Write Network Files	8
Server	Clear Server Logs	8
Server	Clear Server History	8
Network	Delete Network Files	9
Network	Restart Network Devices	9
Network	Install Software on Devices	9
Network	Clear Network Connections	9
Server	Clear Database	9
Server	Restore Database	9
Server	Change Server Configuration	9
Server	Restart Server	9
Server	Server Maintenance	9

Table 4-3 Commands to Setup Change Logs

Action	Command
To configure change-log logging level. Server related tasks and network related tasks are logged according to the task logging level. See Table 4-2. The administrator configures the change-log so that all tasks with priority greater than or equal to the level configured will be logged.	`[SVR:/server](config)# change-log level {1-10}`
To view the change-log. The change-log tasks can be filtered based on the username option or the number of tasks performed.	`[SVR:/server]# show change-log {user-name} { last <1-100000> }`
To clear the change-log. This will clear all change-log entries or entries older than a specified number of hours or days.	`[SVR:/server]# clear change-log [older-than { days <1-240> | hours <1-240> } ]`