



**FORUM SYSTEMS SENTRY™ VERSION 8.7**  
**CLI REFERENCE GUIDE**

**Legal Marks**

No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.

FORUMOS™ Firmware, Forum Systems XMLSec™ WebAdmin, Forum Systems XML Security Appliance™, Forum Sentry™, Forum Presidio™, Forum XWall™ Forum Sentry™ Web Services Gateway, Forum Presidio™ OpenPGP Gateway, Forum FIA Gateway™, Forum XWall Type-PCI™, Forum XWall® Web Services Firewall and Forum XRay™ are trademarks and registered trademarks of Forum Systems, Inc.

All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2016 Forum Systems, Inc. – All Rights Reserved.

Forum Systems Sentry™ Version 8.7 CLI Reference Guide, published April 2016.

D-ASF-SE-02794

INTRODUCTION TO THE CLI REFERENCE .....	1
Audience for the CLI Reference .....	1
Conventions Used for the CLI Reference .....	1
ABOUT THE CLI MODES .....	3
Command Prompts .....	5
Summary of CLI Commands .....	7
COMMANDS DETAILS .....	12
access acl add .....	12
access acl remove .....	12
access group add .....	13
access group add-user .....	13
access group remove .....	14
access group remove-user .....	14
access user add .....	15
access user add-group .....	15
access user disable .....	16
access user dn-alias .....	17
access user email .....	17
access user enable .....	18
access user password .....	18
access user privileged-access .....	19
access user remove .....	19
access user remove-group .....	20
access user sign-key .....	20
connections .....	21
crypto hw-disable .....	21
crypto hw-enable .....	22
exit .....	22
hsm card changepp .....	23
hsm card checkpp .....	23
hsm card erase .....	24
hsm card replace .....	25
hsm import-world .....	26
install-wizard .....	27
log config key-pair .....	32
log config lifespan .....	32
log config log-level .....	33
log config wizard .....	33
log reset .....	34
management bootstrap export .....	35
management bootstrap import .....	36
management upgrade-software .....	36
network config dns .....	37
network config gateway .....	37
network config mgmt-filter .....	38
network config mgmt-iface .....	39
network config mgmt-ip .....	39
network config name .....	40
network config phy .....	40
network config two-device-iface .....	41
network config wan-ip .....	42
network config wizard .....	43
network static-host add .....	45
network static-host remove .....	46
network utils chkport .....	46

network utils dns-flush .....	46
network utils dns-lookup .....	47
network utils ntp-validate .....	47
network utils ping .....	48
network utils traceroute.....	49
ping .....	49
reboot.....	50
route host add.....	51
route host remove.....	52
route network add.....	52
route network remove.....	53
show acl-groups.....	54
show acls.....	54
show arp.....	55
show backup-settings.....	55
show connections.....	56
show crypto settings.....	57
show crypto stats.....	57
show email-config.....	58
show failover-config.....	58
show fips-mode.....	59
show general.....	59
show group-users.....	60
show groups.....	61
show hsm enquiry.....	61
show hsm security-world-id.....	62
show hsm stattree.....	62
show idle-timeout.....	63
show ifconfig.....	63
show interfaces.....	65
show listeners.....	65
show log access.....	67
show log audit.....	68
show log defaultav.....	69
show log defaultavupdate.....	70
show log opsec.....	70
show log system.....	71
show logging-settings.....	72
show max-threads.....	72
show network iptable.....	73
show routes.....	73
show snmp.....	74
show static-hosts.....	74
show statistics.....	76
show syslog-targets.....	77
show system-settings.....	77
show tibrv services.....	78
show tibrv statistics.....	78
show time.....	79
show user-advanced.....	80
show user-groups.....	80
show users.....	81
shutdown.....	82
syslog destination add.....	82
syslog destination disable.....	84
syslog destination enable.....	85

syslog destination remove .....	85
system config backup-enable .....	86
system config backup-test .....	86
system config backup-wizard.....	87
system config certificate-reset .....	89
system config enable-password-set .....	89
system config factory-reset.....	90
system config fips-mode .....	91
system config idle-timeout .....	93
system config ipacl-reset .....	93
system config max-threads.....	94
system config ntp.....	94
system config ports.....	95
system config session-timeout.....	95
system config smtp .....	96
system config tibrv multicast.....	96
system config time .....	97
system config time-zone .....	98
system failover config .....	99
system failover synchronize.....	100
traceroute.....	100
APPENDIX .....	102
Appendix A - CLI Key Bindings.....	102
Appendix B - Default Key Bindings in EMACS Mode .....	108
Appendix C - Default Key Bindings in VI Mode .....	110
Appendix D - Terminal-independent Key Bindings in VI Mode .....	111
Appendix E - Key Bindings for VI Command Mode.....	112
Appendix F - Entering Repeat Counts .....	116
Appendix G - CLI Routing Commands and Equivalent UNIX Commands .....	116
Appendix H - Output of show hsm stattree Command .....	117
Appendix I - Terms and Definitions for Output of show hsm stattree Command .....	117
Appendix J - Constraints in CLI Reference .....	122
INDEX .....	123



# INTRODUCTION TO THE CLI REFERENCE

## Audience for the CLI Reference

The *Forum Systems Sentry™ Command Line Interface Reference* is for IT professionals who will perform system configuration using the Command Line Interface (CLI).

## Conventions Used for the CLI Reference

In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all commands and parameters that must be entered are displayed in italicized boldface. Instructions for the CLI user are displayed in italicized boldface text inside brackets. Press the <enter> key after each command. Returned output from each command is also displayed.

Example:

```
login as: admin1 <enter>  
[Enter your User Name, then press <enter>.]
```

During any operation that involves tab completion with an LDAP group within the CLI, any spaces within an LDAP group name will be replaced by the '%' character to make tab completion easier. Groups and their sub-groups are separated by the '\$' character. For example: GroupParent\$sub-group.

## Overview

The Command Line Interface (CLI), or shell, is a command interpreter that you use to configure and troubleshoot the system. It is also used to configure enough information to bootstrap the WebAdmin UI.

The CLI has been designed with the following features:

- Command completion
- Command history
- Command options listings using "?".
- Easy to use.
- Displays any errors the user has caused through invalid inputs.
- Includes the Forum Systems Installation Wizard to facilitate initial installation of the system.
- Allows for access to system configuration via a serial port or network connection using SSH.
- Abort current command using the "exit" command.

At this point in the installation sequence, your IT Administrators or Network Administrators have run the Forum Systems Installation Wizard, where they have configured system settings and network interfaces for the system, the WebAdmin UI, and added the first Listener Network policy and an initial system User.

You could now add subsequent users, if desired, or allow Administrators to add subsequent system users. Administrators can add listeners by creating HTTP Listener Network policies.

**Note:** Assignment of IP addresses must be controlled by a central IT Administrator and must be unique. Except where otherwise noted, the parameters shown in this document are examples only.

## CLI Start Up Screen

Once your IT Administrator or Network Administrator has cycled through the Forum Systems Installation Wizard, the CLI user will see the following start-up screen after connecting the hyper terminal or other console emulation program to the console (com) port:

```
-----  
Forum OS - Command Shell  
-----  
Forum Systems Model: 456X  
  Serial Number: 0000  
    Licensed to: Unknown  
License Expiration: 12/31/99 12:00 AM  
  Firmware Version: 8.7  
  Product Version: 8.7  
    System Name: Value not set  
Server Start Date/Time: Wed, 30 August 2014 01:29:09 AM EDT  
  Server Up-Time: 0 years, 0 months, 4 days, 0 h, 25 min, 16 s, 54ms  
  Security World ID: N/A  
-----  
ForumOS>
```

## ABOUT THE CLI MODES

The CLI may be operated in one of three modes:

- Restricted mode
- Command mode
- Enable mode

### Restricted Mode

**Restricted mode** allows you to manage connecting, exiting, rebooting and shutting down the system. If you are in Restricted mode, there has been a failure condition. Restricted mode is apparent to you by the following display:

```
.....  
Failure connecting to server  
ForumOS: Could not connect to server.  
ForumOS: Entering restricted-mode.  
ForumOS(restricted-mode)>
```

### Show All Commands in Restricted Mode

View a listing of all available commands at any time, from any mode. This command displays the returned output from Restricted mode.

```
ForumOS(restricted-mode)> ? <enter>  
Restricted Mode:  
  
connections      View all network connections  
exit              Used to exit the system  
ping             Used to locate a host on the network  
factory-reset    Removes all configuration  
reboot           Reboot the system  
traceroute       Run a traceroute to a host  
  
ForumOS(restricted-mode)>
```

### Command Mode

**Command Mode** allows you to view settings on the system. Command mode is a listing of commands that do not require authentication on the system, therefore, the CLI user is restricted to only viewing a variety of statistics on the system. Command mode is apparent to you by the prompt displayed:

```
ForumOS>
```

## Show All Commands in Command Mode

View a listing of all available commands at any time, from any mode. This command displays the returned output from Command mode.

```
ForumOS> ? <enter>
```

```
Command Mode:
```

```
enable          Used to enter privileged mode
exit            Used to exit the system
network        Networking related commands
show           Used to display information on a given topic
system         System wide settings
ForumOS>
```

## Enable Mode

**Enable Mode** allows you to modify the configuration of the system. Enable mode is a privileged mode of operation in which users have the ability to modify system configuration settings. Additionally, Enable mode exposes low-level utilities to users along with all of the commands available in Command mode. Enable mode is apparent to you by the prompt displayed:

```
ForumOS#
```

## Show All Commands in Enable Mode

This command displays all available commands from Enable mode.

```
ForumOS# ? <enter>
```

```
Enable Mode:
```

```
access          Access control commands
crypto **       Cryptographic acceleration commands
exit            Used to exit enable mode
hsm**           HSM related functionality
install-wizard* Allows for initial system configuration
log             Logging related commands
management      Management related commands
network         Networking related commands
reboot          Reboot the system
route           Routing commands
show            Used to display information on a given topic
shutdown        Shutdown the system
syslog          Commands related to the syslog logging facility
system         System wide settings
ForumOS#
```

\* This command is not visible after the first CLI session or after performing the **system config factory-reset** command.

\*\* These commands are only available if the appropriate Cryptographic/HSM card is installed.

## Command Prompts

All commands are displayed with returned output from Enable mode, which is evident by the Enable mode cursor, `ForumOS#`, unless otherwise noted.

Commands with returned output from Restricted mode or Command mode are evident by the Restricted mode or Command mode cursor, `ForumOS>`.

## Example Command Hierarchy

An example of this hierarchy would be adding a new host route. At the Enable mode prompt, type the root command ***route***, followed by a ***space***, the ***<?>*** character, and end the command by pressing the ***<enter>*** key to reveal two sub-commands under ***route***.

```
ForumOS# route ? <enter>

host                Manage host routes
network            Manage network routes

ForumOS#
```

Type the sub-command ***host***, followed by a ***space***, the ***<?>*** character, and end the command by pressing the ***<enter>*** key to reveal two sub-commands under ***host***.

```
ForumOS# route host ? <enter>

add                Adds a new host route
remove            Removes a host route

ForumOS#
```

Therefore, to add a new host route, from the Enable mode prompt, type ***route***, followed by a ***space***, type ***host***, followed by a ***space***, type ***add***, and end the command by pressing the ***<enter>*** key. The CLI requests the IP of the new host route. Enter the host IP address, and then press the ***<enter>*** key. For convenience, a description of the input values that should be entered appear in a bracketed line of text.

```
ForumOS# route host add <enter>
#Please enter: Host
#The host for the route

> 10.5.5.100 <enter>
[Enter host IP address, and then press <enter>]

#Please enter: Gateway address
#The gateway for the host route

> 10.5.6.1 <enter>
[Enter gateway address, and then press <enter>]

Host route added

ForumOS#
```

## CLI Command Hierarchy

The commands in the CLI are hierarchical in structure. To display the hierarchy of a command, type the **command**, followed by a **space**, and then type the **<?>** character, and end the command by pressing the **<enter>** key. The CLI displays required parameters that must be entered. Always end a command by pressing the **<enter>** key, displayed as the **<enter>** character after each input.

## Tab Completion

Tab completion is available for the commands in the CLI. For example, to use tab completion with the command **access group add-user**, follow these steps:

1	From the CLI in enable mode, type	<b>ac &lt;tab&gt;</b>
2	Returned output is	ForumOS# access
3	Type	<b>g &lt;tab&gt;</b>
4	Returned output is	ForumOS# access group
5	Type	<b>a &lt;tab&gt;</b>
6	Returned output is	ForumOS# access group add add-user
7	Type	<b>- &lt;tab&gt;</b>
8	Returned output is	ForumOS# access group add-user
9	Type	<b>&lt;enter&gt;</b> (or <b>press &lt;enter&gt;</b> )
10	Returned output is	<b>ForumOS# access group add-user</b>

... and the command continues to prompt the user for input.

## Summary of CLI Commands

The following table displays the root commands with associated sub-commands. Root commands are listed in bolded text for easy recognition. Commands are also listed as available in Restricted mode [R], Command mode [C] and / or Enable mode [E] in the last three columns.

ROOT COMMAND	SUB-COMMAND	SUB-COMMAND	DESCRIPTION	R	C	E
<b>?</b>			View a list of all available commands	X	X	X
<b>access</b>			Access control commands			X
	acl		ACL management commands			X
		add	Used to add a new ACL to the system			X
		remove	Used to remove an ACL account			X
	group		Group management commands			X
		add	Used to add a new group to the system			X
		add-user	Used to associate a user with a group			X
		remove	Used to remove a group account			X
		remove-user	Used to disassociate a user from a group			X
	user		User management commands			X
		add	Used to add a new user to the system			X
		add-group	Used to associate a group with a user account			X
		disable	Used to disable a user account			X
		dn-alias	Used to set a DN alias for a user account			X
		email	Used to set an email alias for a user account			X
		enable	Used to enable a user account			X
		password	Used to modify a user password			X
		privileged-access	Enable or disable the privileged access			X
		remove	Used to remove a user account			X
		remove-group	Used to disassociate a group from a user account			X
		sign-key	Used to set a signing key for a user account			X
<b>connections</b>			View all network connections	X		
<b>crypto</b>			Cryptographic acceleration commands			X
	hw-disable *		Turn off crypto acceleration for the system			X
	hw-enable *		Turn on crypto acceleration for the system			X
<b>enable</b>			Used to enter privileged mode		X	
<b>exit</b>			Used to exit enable mode	X	X	X
<b>hsm</b>			HSM commands			X
	card	changepp	Change the passphrase on an Admin Card			X
		checkpp	Verify the passphrase on an Admin Card			X
		erase	Erase an Admin Card			X
		replace	Change the Admin Card set for a Security World			X
	import-world		Update the Security World information on system			X

ROOT COMMAND	SUB-COMMAND	SUB-COMMAND	DESCRIPTION	R	C	E
<b>install-wizard</b>			Allows for initial system configuration			X
<b>log</b>			Logging related commands.			X
	config		Configure log parameters			X
		lifespan	Max amount of days to keep archived logs			X
		log-level	Sets the log level			X
		wizard	Configure all the system logs			X
	reset		Resets the system log for today			X
<b>management</b>			Management related commands			X
	bootstrap		Manage bootstrap configuration files			X
		export	Exports a bootstrap configuration file			X
		import	Imports a bootstrap configuration file			X
	upgrade-software		Used to upgrade the system software			X
<b>network</b>			Networking related commands		X	X
	config		Configure network interfaces			X
		dns	Configures DNS settings			X
		gateway	Configures a default gateway			X
		mgmt-filter	Configures Management/Device port traffic filtering			X
		mgmt-iface	Interface where the management interface binds to			X
		mgmt-ip	Configures the management network ip address			X
		name	Configures the system's name			X
		phy	Sets the WAN and WAN Phy characteristics			X
		two-device-iface	Configures the WAN and LAN device interfaces			X
		wan-ip	Configures the wan IP address			X
		wizard	Configures all system net interface settings			X
	static-host		Updates static table lookup for host names.			X
		add	Associates an IP address with a host name.			X
		remove	Disassociates an IP address from a host name.			X
	utils		Network utilities		X	X
		dns-flush	Used to flush the DNS cache			X
		dns-lookup	Used to lookup the IP address if a host via DNS			X
		ntp-validate	Synchronize system time via NTP			X
		ping	Used to verify the presence of a host on the network		X	X
		traceroute	Used to determine the route packets take to network host		X	X
<b>ping</b>			Used to verify the presence of a host on the network	X		
<b>reboot</b>			Reboot the system	X		X

ROOT COMMAND	SUB-COMMAND	SUB-COMMAND	DESCRIPTION	R	C	E
<b>route</b>			Routing commands			X
	host		Manage host routes			X
		add	Adds a new host route			X
		remove	Remove a host route			X
	network		Manage network routes			X
		add	Adds a new network route			X
		remove	Removes a network route			X
<b>show</b>			Used to display information on a given topic		X	X
	acl-groups		Display the groups associated with a specific ACL		X	X
	acls		Displays all ACLs		X	X
	arp		Displays the system ARP table			X
	backup-settings		Displays backup settings		X	X
	connections		View all network connections		X	X
	crypto		Displays cryptographic acceleration settings		X	X
		settings *	Displays cryptographic acceleration settings		X	X
		stats *	Displays cryptographic acceleration statistics		X	X
	failover-config *		Displays the current failover configuration		X	X
	fips-mode		Displays whether FIPS mode is on or off			X
	general		Displays general statistics about the system		X	X
	group-users		Display the users associated with a specific group		X	X
	groups		Displays all groups		X	X
	hsm		Displays hardware security module information			X
		enquiry **	Displays information about the HSM server and module(s)			X
		security-world-id	Displays the Security World ID for this system			X
		stattree **	Displays statistics for the HSM server and module(s)			X
	idle-timeout		Displays the maximum idle timeout		X	X
	ifconfig		Displays statistics & configuration on all interfaces			X
	interfaces		Shows all network interface settings		X	X
	listeners		Shows all server policy listeners		X	X
	log		Logging related commands			X
		access	Display the internal access logs		X	X
		audit	Display the internal audit logs		X	X
		defaultav	Display the default AV log		X	X
		defaultavupdate	Display the default AV updater log		X	X
		opsec	Display the Check Point OPSEC log			
		system	Display the internal system logs		X	X
	logging settings		Display the current log configuration			X
	max-threads		Display the current maximum number of listener threads allowed.		X	X
	network		Displays network interface information		X	X

ROOT COMMAND	SUB-COMMAND	SUB-COMMAND	DESCRIPTION	R	C	E
		iptable	Displays system ip table information		X	X
<b>show</b>	routes		Shows all network and host routes		X	X
	snmp		Displays SNMP name, location and contact settings		X	X
	static-hosts		Displays the static table lookup for host names.		X	X
	statistics		Displays the systems statistics		X	X
	syslog-targets		Displays all remote syslog destinations		X	X
	system-settings		Display system wide configuration		X	X
	tibrv		Tibco Rendezvous commands		X	X
		services	Displays all registered services		X	X
		statistics	Shows Rendezvous statistics for a service		X	X
	time		Displays the system time and date		X	X
	user-advanced		Display the advanced options for a specific user		X	X
	user-groups		Display the groups associated with a specific user		X	X
	users		Displays all users		X	X
<b>shutdown</b>			Shutdown the system			X
<b>syslog</b>			Commands related to the syslog logging facility			X
	destination		Configures a remote destination			X
		add	Used to add a syslog remote destination			X
		disable	Used to disable a syslog remote destination			X
		enable	Used to enable a syslog remote destination			X
		remove	Used to remove a syslog remote destination			X
<b>system</b>			System wide settings		X	X
	config		Used to configure system wide settings		X	X
		backup-enable	Used to enable the automatic backup of the config file			X
		backup-test	Initiates a configuration file backup			X
		backup-wizard	Used to set ftp parameters for backup of the config file			X
		certificate-reset	Resets the SSL certificate			X
		enable-password-set	Used to set the enable mode password			X
		factory-reset ***	Reset all system settings		X	X
		fips-mode ****	Toggles FIPS mode			X
		idle-timeout	Set the maximum number of seconds to wait for the next request from the same client on the same connection. The timeout is also used as a listener read timeout.			X
		ipacl-reset	Resets the Web Admin IP ACL Policy			
		max-threads	Sets the maximum size of the listener pool.			X
		ntp	Used to configure an NTP time server			X

ROOT COMMAND	SUB-COMMAND	SUB-COMMAND	DESCRIPTION	R	C	E
<b>system</b>	config		Used to configure system wide settings		X	X
		ports	Used to set the system management ports			X
		session-timeout	Used to configure the inactive timeout for sessions			X
		smtp	Used to configure an SMTP mail server			X
		tibrv multicast	Configures IP multicast for a specific service			X
		time	Used to set the system time			X
		time-zone	Used to set the system time zone			X
	failover		Failover settings			X
		config	Used to configure failover			X
		synchronization	Schedules a synchronization to the server running in standby mode			X
<b>traceroute</b>			Used to run a traceroute to a host	X		

\* These commands are unavailable on the HSM-enabled system and the Type-PCI Card.

\*\* These commands are unavailable on the non-HSM system and the Type-PCI Card.

\*\*\* The system config factory-reset command is only available via the serial CLI in command mode. It is available via both SSH and serial CLI in enable mode

\*\*\*\* The system config fips-mode command is only available on systems with the FIPS license feature.

## COMMANDS DETAILS

The following section displays an alphabetical listing of the CLI commands and their details.

### access acl add

Command Availability		
Restricted	Command	Enable
		X

This command is used to add a new ACL to the system.

**Note:** ACL names must be unique, are case sensitive, may be from 1 to 255 alphanumeric characters, and may include underscores, dashes, spaces and the "@"character. However, ACL names cannot contain leading or trailing spaces.

```
ForumOS# access acl add <enter>

# Please enter: ACL name
# A unique ACL name

> Field Managers <enter>
[Enter ACL name, and then press <enter>]

ACL added
ForumOS#
```

### access acl remove

Command Availability		
Restricted	Command	Enable
		X

This command is used to remove an ACL account.

```
ForumOS# access acl remove <enter>

# Please enter: ACL name
# The acl to remove

> Trustees <enter>
[Enter ACL name, and then press <enter>]

ACL has been removed
ForumOS#
```

## access group add

Command Availability		
Restricted	Command	Enable
		X

This command is used to add a new Group to the system.

**Note:** Group names must be unique, are case sensitive, from 1 to 255 alphanumeric characters, and may include underscores and dashes, but cannot contain spaces. Furthermore, Group names cannot start, nor end, in a space.

```
ForumOS# access group add <enter>

# Please enter: Group name
# A unique group name

> Government_Sales <enter>
[Enter a Group name, and then press <enter>]

Group added
ForumOS#
```

## access group add-user

Command Availability		
Restricted	Command	Enable
		X

This command is used to associate a User with a Group.

```
ForumOS# access group add-user <enter>

# Please enter: Group name
# The group account to target

> InternalSales <enter>
[Enter Group name, and then press <enter>]

# Please enter: User
# The user to associate

> pjones <enter>
[Enter User name, and then press <enter>]

User pjones added to group InternalSales
ForumOS#
```

## access group remove

Command Availability		
Restricted	Command	Enable
		X

This command is used to remove a Group account.

```
ForumOS# access group remove <enter>

# Please enter: Group name
# The group account to remove

> government_sales <enter>
[Enter Group name, and then press <enter>.]

Group has been removed
ForumOS#
```

## access group remove-user

Command Availability		
Restricted	Command	Enable
		X

This command is used to disassociate a User from a Group.

```
ForumOS# access group remove-user <enter>

# Please enter: Group name
# The group account to target

> Marketing <enter>
[Enter Group name, and then press <enter>]

# Please enter: User <enter>
# The user to disassociate

> karenlittle <enter>
[Enter User name, and then press <enter>]

User karenlittle removed from group Marketing
ForumOS#
```

## access user add

Command Availability		
Restricted	Command	Enable
		X

This command is used to add a new User to the system. Additionally, this command requires that the user name and user password be unique per user.

**Note:** User names must be unique, are case sensitive, and may be from 1 to 80 alphanumeric characters. The '@' character, underscores, dashes and spaces are allowed; however, no leading or trailing spaces are allowed. User passwords must be unique, are case sensitive, may be from 6 to 255 alphanumeric characters, and may be any keyboard characters.

```
ForumOS# access user add <enter>

# Please enter: User name
# A unique user name

> pjones <enter>
[Enter a User name, and then press <enter>]

# Please enter: New password
# The new user password

> ***** <enter>
[Enter a Password, and then press <enter>]

# Please enter: Confirm password
# Confirm the new user password

> ***** <enter>
[Re-enter the Password, and then press <enter>]

# Please enter: Enable policy
# Enable the new policy
  Y to enable policy
  N to disable policy

> Y <enter>
[Press Enter to accept the default Y, or enter N, and then press <enter>]

User added
ForumOS#
```

## access user add-group

Command Availability		
Restricted	Command	Enable
		X

This command is used to associate a Group with a User account.

**Note:** Group names and sub-groups must be uniquely named at each group level. Group names must be unique, are case sensitive, may be from 1 to 255 alphanumeric characters, and may include underscores, dashes, spaces and the "@" character. However, Group names cannot contain leading or trailing spaces. Groups and sub-groups are separated by a '\$'. For example: GroupParent\$sub-group.

```
ForumOS# access user add-group <enter>
# Please enter: User name
# The user account to modify

> donstreeter <enter>
[Enter User name, and then press <enter>]

# Please enter: Group
# The group to associate

> Bus_Development$Architects <enter>
[Enter Group name, and then press <enter>]

Group added
ForumOS#
```

## access user disable

Command Availability		
Restricted	Command	Enable
		X

This command is used to disable a User account.

```
ForumOS# access user disable <enter>

# Please enter: User name
# The user account to disable

> pjones <enter>
[Enter User name, and then press <enter>]

User has been disabled
ForumOS#
```

## access user dn-alias

Command Availability		
Restricted	Command	Enable
		X

This command is used to set a DN alias for a User account.

```
ForumOS# access user dn-alias <enter>
```

```
# Please enter: User name  
# The user account to modify
```

```
> donald <enter>  
[Enter User name, and then press <enter>]
```

```
# Please enter: DN alias  
# A DN alias for the user account
```

```
> cn=Donald, ou=Quality Assurance, o="Forum Systems", l=Waltham,  
st=Massachusetts, c=US <enter>  
[Enter dn alias data, and then press <enter>]
```

```
User DN alias updated  
ForumOS#
```

## access user email

Command Availability		
Restricted	Command	Enable
		X

This command is used to set an email alias for a User account.

```
ForumOS# access user email <enter>
```

```
# Please enter: User name  
# The user account to modify
```

```
> donald <enter>  
[Enter a User name, and then press <enter>]
```

```
# Please enter: Email alias  
# An Email alias for the user account
```

```
> donald@test.forumsys.com <enter>
```

*[Enter email address, and then press <enter>]*

User email updated  
ForumOS#

## access user enable

Command Availability		
Restricted	Command	Enable
		X

This command is used to enable a User account.

ForumOS# *access user enable <enter>*

# Please enter: User name  
# The user account to enable

> *pjones <enter>*

*{Enter User name, and then press <enter>}*

Account has been enabled  
ForumOS#

## access user password

Command Availability		
Restricted	Command	Enable
		X

This command is used to modify a User password.

ForumOS# *access user password <enter>*

# Please enter: User name  
# The user account to target

> *pjones <enter>*

*[Enter User name, and then press <enter>]*

# Please enter: New password  
# The new user password

> *\*\*\*\*\* <enter>*

*[Enter Password, and then press <enter>]*

```
# Please enter: Confirm password
# Confirm the new user password

> ***** <enter>
[Re-enter Password, and then press <enter>]
```

```
User Modified
ForumOS#
```

## access user privileged-access

Command Availability		
Restricted	Command	Enable
		X

This command is used to modify a User privileged access setting.

```
ForumOS# access user privileged-access <enter>
```

```
# Please enter: User name
# The user account to modify
```

```
> pjones <enter>
[Enter User name, and then press <enter>]
```

Privileged access has been enabled

```
ForumOS#
```

## access user remove

Command Availability		
Restricted	Command	Enable
		X

This command is used to remove a User account.

```
ForumOS# access user remove <enter>
```

```
#Please enter: User Name
#The user account to remove
```

```
> pjones <enter>
[Enter User name, and then press <enter>]
```

User has been removed

ForumOS#

## access user remove-group

Command Availability		
Restricted	Command	Enable
		X

This command is used to disassociate a Group from a User account.

```
ForumOS# access user remove-group <enter>
```

```
# Please enter: User name  
# The user account to target
```

```
> pjones <enter>  
[Enter User name, and then press <enter>]
```

```
# Please enter: Group  
# The group to disassociate
```

```
> InternalSales <enter>  
[Enter Group name, and then press <enter>]
```

```
Group removed
```

```
ForumOS#
```

## access user sign-key

Command Availability		
Restricted	Command	Enable
		X

This command is used to set a signing key for a User account by entering a key pair alias. When setting a sign key in the CLI, and then navigating to the Users screen > USER DETAILS screen, the sign key may not be immediately visible. Select another User, then return to the User of the newly set signing key to see the Sign Key field populate with the key name.

```
ForumOS# access user sign-key <enter>
```

```
# Please enter: User name  
# The user account to modify
```

```
> jessica <enter>  
[Enter User name, and then press <enter>]
```

```
# Please enter: Signing key
# A signing key for the user account

> jessica_0_rsa <enter>
[Enter key pair alias, and then press <enter>]
```

```
Signing key has been updated
ForumOS#
```

## connections

Command Availability		
Restricted	Command	Enable
X		

This command is used to view all network connections.

```
ForumOS(restricted-mode)> connections <enter>
```

Active Internet connections

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	10.5.3.92:5060	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:7030	0.0.0.0:*	LISTEN
tcp	0	0	10.5.3.92:22	0.0.0.0:*	LISTEN
tcp	0	0	10.5.3.92:5050	0.0.0.0:*	LISTEN
udp	0	0	0.0.0.0:32797	0.0.0.0:*	
udp	0	0	0.0.0.0:32798	0.0.0.0:*	
udp	0	0	10.5.6.92:123	0.0.0.0:*	
udp	0	0	10.5.3.92:123	0.0.0.0:*	
udp	0	0	127.0.0.1:123	0.0.0.0:*	
udp	0	0	0.0.0.0:123	0.0.0.0:*	

```
ForumOS(restricted-mode)>
```

## crypto hw-disable

Command Availability		
Restricted	Command	Enable
		X

This command turns off cryptographic acceleration for the system.

```
ForumOS# crypto hw-disable <enter>
```

```
Cryptographic acceleration is disabled  
ForumOS#
```

**Note:** With the HSM-enabled system and the Type-PCI card product, this command is unavailable.

### crypto hw-enable

Command Availability		
Restricted	Command	Enable
		X

This command turns on cryptographic acceleration for the system.

```
ForumOS# crypto hw-enable <enter>
```

```
Cryptographic acceleration is enabled  
ForumOS#
```

**Note:** With the HSM-enabled system and the Type-PCI card product, this command is unavailable.

### exit

Command Availability		
Restricted	Command	Enable
X	X	X

This command is used to exit Enable mode. From Enable mode, when the CLI user exits Enable mode by typing *exit* <enter> , the CLI user is brought to Command mode. From Command mode, the CLI user may leave the shell by retyping *exit* <enter>.

**Note:** You may also use the *exit* <enter> command to cancel any command in Enable mode.

```
ForumOS# exit <enter>
```

```
Logged into command mode  
Type ? for a list of commands
```

```
ForumOS>
```

The CLI screen closes. Note that this command started with the Enable Mode prompt (ForumOS#) and ends with the Command Mode prompt (ForumOS>).

## hsm card changepp

Command Availability		
Restricted	Command	Enable
		X

This command allows the Administrator to change the passphrase on an Admin Card.

**Note:** HSM Administrator Card passphrases must be unique, are case sensitive, and may be from 6 to 128 printable characters (i.e., #, \$, %, &, etc. are valid). Spaces are allowed, but leading and trailing white space is ignored.

```
ForumOS# hsm card changepp <enter>
```

```
# Please insert an Administrator card (1-1) to change its passphrase and  
press enter.
```

```
[Enter an Admin Card, and then press <enter>]
```

```
> <enter>
```

```
# Please enter: a passphrase
```

```
# The passphrase for the current Administrator Card
```

```
[Enter the passphrase for current Admin Card, and then press <enter>]
```

```
> ***** <enter>
```

```
# Please enter: a passphrase
```

```
# A new passphrase for the current Administrator Card
```

```
[Enter the new passphrase for an Admin Card, and then press <enter>]
```

```
> ***** <enter>
```

```
# Please enter: a passphrase
```

```
# Please confirm the passphrase for the current Administrator Card
```

```
[Re-enter the new passphrase for an Admin Card, and then press <enter>]
```

```
> ***** <enter>
```

```
Passphrase changed
```

```
ForumOS#
```

## hsm card checkpp

Command Availability		
Restricted	Command	Enable
		X

This command allows the Administrator to verify the passphrase on an Admin Card. This command also determines if an Admin Card is part of a Security World.

### With Admin Card that is Part of a Security World

```
ForumOS# hsm card checkpp <enter>
```

```
# Please insert an Administrator card (1-1) to be loaded and press enter.  
[Enter an Admin Card, and then press <enter>]
```

```
> <enter>
```

```
# Please enter: a passphrase  
# The passphrase for the current Administrator Card  
[Enter the passphrase for the current Admin Card, and then press <enter>]
```

```
> ***** <enter>
```

```
Passphrase correct
```

```
ForumOS#
```

### With Admin Card that is Not Part of a Security World

```
ForumOS# hsm card checkpp <enter>
```

```
# Please insert an Administrator card (1-1) to be loaded and press enter.  
[Enter an Admin Card, and then press <enter>]
```

```
> <enter>
```

```
# Please enter: a passphrase  
# The passphrase for the current Administrator Card  
[Enter the passphrase for the current Admin Card, and then press <enter>]
```

```
> ***** <enter>
```

```
# Error: Provided card could not be identified
```

```
> Please insert an Administrator card (1-1) to be loaded and press enter.  
[Enter an Admin Card, and then press <enter>]
```

### hsm card erase

Command Availability		
Restricted	Command	Enable
		X

This command allows the Administrator to erase an Admin Card.

**Note:** The system will not allow you to erase an Admin Card which is in use by the currently loaded Security World.

**Warning:** Once an Admin Card is erased, there is no mechanism to recover it. Use this command with extreme care.

```
ForumOS# hsm card erase <enter>

# Please insert a smart card (1-1) to be erased and press enter.
[Enter an Admin Card, and then press <enter>]

> <enter>

% Error: The card in the card reader could not be identified.
# Would you like to overwrite it? (y/n)

> y <enter>

Card erased

ForumOS#
```

## hsm card replace

Command Availability		
Restricted	Command	Enable
		X

This command allows the Administrator to change the Admin Card set for a Security World.

The number of Administrator cards will remain the same. When this command is initially executed, only the system on which the command is executed is affected (i.e. only the old Admin Card set will continue to work on other systems in the same Security World). After the command is executed, the Administrator should propagate the change to all other systems in the same security world (see "hsm import-world" command).

**Note:** Initially, this command is only executed on the local system. In order to propagate the change to other systems, a bootstrap file should be exported from this system (see "management bootstrap export" command) and imported on to the other systems (see "hsm import-world" command).

HSM Administrator Card passphrases must be unique, are case sensitive, and may be from 6 to 128 printable characters (i.e., #, \$, %, &, etc. are valid). Spaces are allowed, but leading and trailing white space is ignored.

**Warning:** This method should rarely be needed, and when used, should be handled with extreme care. If the Administrator is not careful, the Administrator may end up with no valid Admin Card set from which to initialize a new HSM with the existing Security World.

```
ForumOS# hsm card replace <enter>
```

# Please insert an Administrator card (1/1) to be loaded and press enter.  
*[Enter an Admin Card, and then press <enter>]*

> <enter>

# Please enter: a passphrase  
# The passphrase for the current Administrator Card  
*[Enter the passphrase for the current Admin Card, and then press <enter>]*

> \*\*\*\*\* <enter>

# Please insert an Administrator card (1/1) to be initialized, and then press enter.  
*[Enter an Admin Card to be initialized, and then press <enter>]*

> <enter>

# Please enter: a passphrase  
# A new passphrase for the current Administrator Card  
*[Enter a new passphrase for the current Admin Card, and then press <enter>]*

> \*\*\*\*\* <enter>

# Please enter: a passphrase  
# Please confirm the passphrase for the current Administrator Card  
*[Re-enter the new passphrase for the current Admin Card, and then press <enter>]*

> \*\*\*\*\* <enter>

**Note:** The previous three prompts are repeated once per card being created for the new Admin Card set.

Admin card-set replaced

ForumOS#

## hsm import-world

Command Availability		
Restricted	Command	Enable
		X

This command allows the Administrator to update the Security World information on an system. The Security World contains more information than simply the Security World Key. It also contains information on which Administrator cards may be used to load the security world if an Administrator replaces an Admin Card set (using the "hsm card replace" command). Only the new Administrator cards will be

accepted on the system on which the command was executed. However, to propagate this change, the Administrator must load the Security World information from the original system to all others in that security world. The Administrator may do so by generating a bootstrap file on the original system (the one on which the "hsm card replace" command was executed) and then loading it onto other systems in the same security world using this command.

**Note:** This command will succeed only if the Security World ID in the bootstrap file matches the Security World ID on the target machine.

**Warning:** This method, if successful, will overwrite security world information on the target system, including references to the Security World Card set. Therefore, after this command is executed, only the Admin Card set specified in the Security World information in the bootstrap file will be accepted on this system (and the previously accepted Admin Card set will no longer be accepted on this system). This command must be executed with extreme care.

```
ForumOS# hsm import-world <enter>
```

```
Ready to receive file via zmodem...  
ŠB000000023be50
```

*[Initiate zmodem file upload from terminal emulation software]*

```
# Please enter: overwrite Security World information  
# Overwrites the system's current security world information with that  
# contained in the bootstrap (fsb) file. The security world information in  
# the bootstrap (fsb) file differs from that currently loaded possibly  
# because the Administrator card set has been replaced) on the system.  
# However, both sets of security world information were produced by an HSM  
# operating in the same security world.
```

```
# Warning: The Administrator Card set information is stored in the Security  
# World information. Before overwriting the system's Security World  
# information, it is highly recommended that a backup be made by either  
# exporting a configuration file (fsx) from the WebAdmin, or by exporting a  
# new bootstrap file (the latter method exports only the Security World  
# information and bootstrap fields, but none of the other application-key or  
# configuration information).
```

```
Y to overwrite security world information  
N keep existing security world information
```

*[Enter y to overwrite Security World information, or n to retain existing Security World information, and then press <enter>]*

```
> y <enter>
```

```
ForumOS#
```

## install-wizard

Command Availability		
Restricted	Command	Enable
		X

This command allows for initial system configuration.

**Note:** This command is available in the first CLI session or after performing the *system config factory-reset* command.

```
ForumOS# install-wizard <enter>
```

```
*****
* Welcome to the Forum Systems Installation Wizard      *
*                                                       *
* Before using the command line interface, some       *
* basic information will be needed to configure        *
* the management network interface. Type exit at      *
* the command prompt if you would like to defer      *
* this wizard until later.                             *
*                                                       *
* Once this information is collected you will be      *
* able to use the command line interface or the      *
* the web admin gui.                                  *
*                                                       *
*****

# Please enter: Data entry method
# Manual enter data or import an existing bootstrap file
  1 to manually enter data
  2 to import a bootstrap (fsb) file

> 1 <enter>
[Type (1) or (2), and then press <enter>.]
```

**Note:** If you have selected 2, then the “Ready to receive file via zmodem” message appears. You will now upload the bootstrap file, and then drop back into the CLI enable mode. If you have selected 1, then the Installation Wizard continues with the following prompts for various network values.

```
*****
* Management Interface Settings for the System      *
*                                                       *
* This includes the ip address and netmask that will *
* be used for managing the device.                 *
*****

# Please enter: Management Address
# The IP Address for management

> 10.5.3.92 <enter>
[Enter IP address or press <enter> to accept default]
```

```
# Please enter: Management Netmask
# The netmask for management
```

```
> 255.255.255.0 <enter>
```

```
[Enter management netmask or press <enter> to accept default]
```

```
*****
*                               *
*           Physical Network Topology           *
*                               *
* These are global settings for the device that *
* restrict all device communication policies to *
* either a one-port configuration, or inline with *
* separate IP addresses on the WAN and LAN      *
* interfaces.                                  *
*****
```

```
# Please enter: Topology Mode
# The network topology for the system
  1 for One-Port mode
  2 for Inline (Dual IP address) mode
```

```
> 1
```

```
[Enter (1) or (2) and then press <enter>]
```

```
*****
*                               *
*   Device Interface Settings for the System   *
*                               *
* This includes the ip address and netmask that will *
* be used for all system traffic. In a proxy *
* configuration this will be the address that clients *
* connect to.                                     *
*****
```

```
# Please enter: Device IP Address
# The default IP Address for the system
```

```
> 10.5.6.92 <enter>
```

```
[Enter default IP address for System or press <enter> to accept default]
```

```
# Please enter: Device Netmask
# The default device netmask for the system
```

```
> 255.255.255.0 <enter>
```

```
[Enter default device netmask or press <enter> to accept default]
```

```
*****
*                               *
*           Default Gateway Setting           *
*                               *
* This is an optional default gateway for the *
* system that applies to either the device setting *
* or the management interface.                *
*****
```

```
# Please enter: Device Gateway
# The default gateway for the system
  Enter blank value for none
```

```
> 10.5.3.1 <enter>
[Press <enter> to accept default or backspace to remove all pre-populated
value to enter a blank value]
```

```
# Please enter: Gateway Interface
# Interface directed to the gateway
  1 Let the System Choose for you
  2 for Virtual Interface
  3 for Management
```

```
> 1 <enter>
[Enter the gateway interface. Press 1 to let the system choose for you, or 2
for the Virtual Interface, or 3 for Management, and then press <enter>]
```

```
*****
*           DNS Name Server Configuration Settings           *
*                                                                 *
* These are optional DNS settings that can be applied *
* to the device. *
*****
```

```
# Please enter: Primary DNS
# The address of the primary DNS
  Enter blank value for none
```

```
> 10.5.2.11 <enter>
[Press <enter> to accept default or backspace to remove all pre-populated
value to enter a blank value]
```

```
# Please enter: Secondary DNS
# The address of a secondary DNS
  Enter blank value for none
```

```
> 10.5.2.12 <enter>
[Press <enter> to accept default or backspace to remove all pre-populated
value to enter a blank value]
```

```
*****
*           Enable Password           *
*                                                                 *
* Enable mode is a privileged mode of operation in *
* CLI that allows you to modify system settings. *
* These settings allow you to enter an enable mode *
* password that will allow an administrator to enter *
* enable mode. *
*****
```

```
# Please enter: New password
```

```
# The new enable mode password

> ***** <enter>
[Enter new enable password, and then press <enter>]
```

**Note:** The Enable mode password must be unique, is case sensitive, and may be from 6 to 32 alphanumeric characters.

```
# Please enter: Confirm password
# Confirm the new enable mode password

> ***** <enter>
[Re-enter new enable password, and then press <enter>]
```

**Note:** The command line will not echo "\*" characters.

```
*****
*                               *
*           Management User           *
*                               *
* The following settings allow you to enter a user *
* policy that can be used to gain access to other *
* user interfaces such as the Web Administration UI. *
*****
# Please enter: User name
# A unique user name

> admin1 <enter>
[Enter new user name, and then press <enter>]
```

**Note:** User names must be unique, are case sensitive, and may be from 1 to 80 alphanumeric characters. The '@' character, underscores, dashes and spaces are allowed; however, no leading or trailing spaces are allowed. User passwords must be unique, are case sensitive, may be from 6 to 255 alphanumeric characters, and may be any keyboard characters.

```
# Please enter: New password
# The new user password

> ***** <enter>
[Enter new user password, and then press <enter>]
```

**Note:** The command line will not echo "\*" characters.

```
# Please enter: Confirm password
# Confirm the new user password

> ***** <enter>
[Re-enter new user password, and then press <enter>]
```

Installation Wizard is now complete!

Logged into Command mode  
Type ? for a list of commands

ForumOS>

## log config key-pair

Command Availability		
Restricted	Command	Enable
		X

This command is used to set the key pair used to sign archived logs.

```
ForumOS# log config key-pair <enter>
```

```
# Please enter: Key pair  
# Key pair to sign archived logs
```

```
> DEFAULT <enter>
```

```
[Press <enter> to accept default, or enter the name of a key pair]
```

```
Key pair updated  
ForumOS#
```

## log config lifespan

Command Availability		
Restricted	Command	Enable
		X

This command is used to set the maximum amount of days to keep archived logs.

```
ForumOS# log config lifespan <enter>
```

```
# Please enter: Log type  
# Logs are classified in two: system and audit.  
Audit logs record configuration information.  
System logs record runtime/processing information.  
  0 for Audit  
  1 for System
```

```
> 0 <enter>
```

```
[Enter 1 or press <enter> to accept default (0)]
```

```
# Please enter: Lifespan  
# Lifespan (in days) for audit log
```

```
> 15 <enter>
```

```
[Enter a value for number of days or press <enter> to accept default (15)]
```

```
Log lifespan set to 15
```

ForumOS#

## log config log-level

Command Availability		
Restricted	Command	Enable
		X

This command is used to set the log level.

```
ForumOS# log config log-level <enter>
```

```
# Please enter: Log type
```

```
# Logs are classified in two: system and audit.
```

```
Audit logs record configuration information.
```

```
System logs record runtime/processing information.
```

```
0 for Audit
```

```
1 for System
```

```
> 1 <enter>
```

```
[Enter 1 or 2, and then press <enter>]
```

```
# Please enter: Logging level
```

```
# Logging level for system log
```

```
1. Debug
```

```
2. Info
```

```
3. Warning
```

```
4. Error
```

```
> 2 <enter>
```

```
[Enter 1, 3, or 4 or press <enter> to accept default (2)]
```

```
Log level set to Info
```

```
ForumOS#
```

## log config wizard

Command Availability		
Restricted	Command	Enable
		X

This command is used to configure all system logs.

**Note:** For information on importing your own corporate, self-signed SSL certificate on the system, refer to the Sample System Configuration Using Your Own SSL Key Pair appendix in the *Forum Systems Sentry™ Web-based Administration Guide*.

```
ForumOS# log config wizard <enter>
# Please enter: Key pair
# Key pair to sign archived logs

> DEFAULT <enter>
[Press the <tab> key to view other SSL key pairs available for selection or
or press <enter> to accept default (DEFAULT)]

# Please enter: Logging level
# Logging level for audit log
  1. Debug
  2. Info
  3. Warning
  4. Error

> 2 <enter>
[Enter 1, 3, or 4 or press <enter> to accept default (2)]

# Please enter: Lifespan
# Lifespan (in days) for audit log

> 15 <enter>
[Enter a value for number of days or press <enter> to accept default (15)]

# Please enter: Logging level
# Logging level for system log
  1. Debug
  2. Info
  3. Warning
  4. Error

> 2 <enter>
[Enter 1, 3, or 4 or press <enter> to accept default (2)]

# Please enter: Lifespan
# Lifespan (in days) for system log

> 15 <enter>
[Enter a value for number of days or press <enter> to accept default (15)]

Log configuration updated
ForumOS#
```

## log reset

Command Availability		
Restricted	Command	Enable
		X

This command is used to reset the system log for today.

```
ForumOS# log reset <enter>
```

```
System log has been reset
ForumOS#
```

### management bootstrap export

Command Availability		
Restricted	Command	Enable
		X

This command is used to export a bootstrap configuration file.

**Note:** Bootstrap export file names must be unique, are case sensitive, may be from 2 to 32 alphanumeric characters, may include underscores, dashes but no spaces. One period ( . ) character is allowed.

```
ForumOS# management bootstrap export <enter>
```

```
# Please enter: File Name
# The name of the export file to generate
[Enter bootstrap configuration file to export, and then press <enter>]
```

```
> fsconfig <enter>
```

```
# Please enter: Default User
# The default administrative user to include in the export file
 1 admin1
 2 admin2
 3 admin3
```

```
[Press <enter> to accept the default (1) or select another number, and then press <enter>]
```

```
> 1 <enter>
```

```
Starting zmodem transfer...
```

Once the “Starting zmodem transfer” message appears, if your hyperterminal or your emulation software does not automatically start up `zmodem receive`, then you will have to start it manually; otherwise, the file should start downloading.

ForumOS#

## management bootstrap import

Command Availability		
Restricted	Command	Enable
		X

This command is used to import a bootstrap configuration file.

```
ForumOS# management bootstrap import <enter>
```

Ready to receive file via zmodem...

You will now upload the bootstrap file via zmodem using your terminal emulation software, and then drop back into the CLI enable mode.

ForumOS#

## management upgrade-software

Command Availability		
Restricted	Command	Enable
		X

This command is used to upgrade the system software. CLI users are asked for the protocol to use for retrieving the upgrade package, the Server name or IP address for delivery of the upgrade package and the filename of the upgrade package. After these three values have been entered, please be patient as the package is being downloaded, the file fingerprint is checked for verification, and the upgrade is unpacked. After these events have occurred, the system will automatically reboot.

```
ForumOS# management upgrade-software <enter>
```

```
# Please enter: Protocol
```

```
# The protocol for retrieving
```

```
  Available options: Http or FTP
```

```
> ftp <enter>
```

```
[Enter http or ftp, and then press <enter>]
```

```
# Please enter: Server name
```

```
# The name or address of the server where the package can be found
```

```
> 10.5.2.90 <enter>
```

```
[Enter Server Name or IP Address, and then press <enter>]
```

```
# Please enter: Package (file) name
```

```
# The name of the file to download

> /dist/RPM-4.5/FS-ENVT-4.5-90.upgrade.bin <enter>
[Enter the filename for the Forum upgrade package, and then press <enter>]
```

**Note:** While the upgrade files download and verify, expect a long delay, with no screen output.

Upgrade successful. Rebooting.  
Please wait as the system reboots.

## network config dns

Command Availability		
Restricted	Command	Enable
		X

This command is used to configure DNS settings.

```
ForumOS# network config dns <enter>
```

```
# Please enter: Primary DNS
# The address of the primary DNS
  Enter blank value for none
```

```
[Enter Primary DNS Address. Press <enter> to accept default or enter blank
for no value]
```

```
> 10.5.2.11
```

```
# Please enter: Secondary DNS
# The address of a secondary DNS
  Enter blank value for none
```

```
[Enter Secondary DNS Address. Press <enter> to accept default or enter blank
for no value]
```

```
> 10.5.2.12
```

```
DNS updated.
```

```
Note: Changes will not take effect until the system is rebooted
```

```
ForumOS#
```

**Note:** When updating the DNS, you must reboot to enable the changes.

## network config gateway

Command Availability		
Restricted	Command	Enable

		X
--	--	---

This command is used to configure a default gateway.

```
ForumOS# network config gateway <enter>
```

```
#Please enter: Device Gateway
#The default gateway for the system
#Enter blank value for none
```

10.5.2.1

*[Enter Device Gateway. Press <enter> to accept default or enter blank for no value]*

```
# Please enter: Gateway Interface
# Interface directed to the gateway
  1 Let the System Choose for you
  2 for the Virtual Interface
  3 for Management
```

```
> 1 <enter>
```

*[Enter the gateway interface. Press 1 to let the system choose for you, or 2 for the Virtual Interface or 3 for Management, and then press <enter>]*

```
Gateway updated
```

```
ForumOS#
```

## network config mgmt-filter

Command Availability		
Restricted	Command	Enable
		X

Filters are used to guarantee that management traffic does not go onto the data network and data traffic does not go onto management network for security purposes. Common errors that are made with network configuration are:

- Putting the management network and device network on same subnet and forgetting to turn filters OFF.
- Putting the management network and device network on separate networks, but neglecting to configure routes properly.

**Note:** When placing the MANAGEMENT interface and WAN interface on same subnet, you must turn the filters OFF by setting filters to N.

This command is used to configure management/device port traffic filtering.

```
ForumOS# network config mgmt-filter <enter>
```

```
#Please enter: Filter Node
#Allows or disallows mgmt/dev port filtering
  Y for Filtering
  N for no Filtering
```

*[Enter N or press <enter> to accept the default Y]*

```
> Y <enter>
```

```
Filtering updated
ForumOS#
```

### network config mgmt-iface

Command Availability		
Restricted	Command	Enable
		X

This command is used to choose the interface where to bind the admin servers (the WebAdmin or GDM).

```
ForumOS# network config mgmt-iface <enter>
```

```
#Please enter: Management Listeners
# Interface used for binding the management listeners
```

```
  MGMT
  WAN
  LAN
```

*[Press <enter> to accept default (MGMT) or overwrite MGMT and enter WAN or LAN and then press <enter>]*

```
Management interface updated
```

```
ForumOS#
```

### network config mgmt-ip

Command Availability		
Restricted	Command	Enable
		X

This command is used to configure the management network IP address.

```
ForumOS# network config mgmt-ip <enter>
```

```
#Please enter: Management Address
```

#The IP Address for management

> *10.5.3.92* <enter>

[Enter Management IP Address or press <enter> to accept default]

#Please enter: Management Netmask

#The netmask for management

> *255.255.255.0* <enter>

[Enter Management Netmask or press <enter> to accept default]

Management ip address updated

ForumOS#

## network config name

Command Availability		
Restricted	Command	Enable
		X

This command is used to configure the system's name.

ForumOS# *network config name* <enter>

# Please enter: System name

# The system's name

> *hal* <enter>

[Enter the system name, and then press <enter>]

**Note:** System names must be unique, are case sensitive, may be from 1 to 64 alphanumeric characters, and may include underscores, dashes, spaces and the "@" character. However, system names cannot contain trailing spaces.

The system's name has been set

ForumOS#

## network config phy

Command Availability		
Restricted	Command	Enable

		X
--	--	---

**Note:** This command is available on the Forum 1502 and above.

This command is used to set the WAN and WAN physical characteristics.

```
ForumOS# network config phy <enter>
```

```
# Please enter: Ethernet Phy configuration
# Select the WAN/LAN Phy configuration
  1 Auto-Negotiate
  2 100Mbs Full Duplex
```

```
> 1 <enter>
```

*[Enter 1 to allow the system to negotiate the line speed, or 2 to allow the system to run in 100Mbs, and then press <enter>]*

Phy configuration updated.

```
ForumOS#
```

### **network config two-device-iface**

<b>Command Availability</b>		
<b>Restricted</b>	<b>Command</b>	<b>Enable</b>
		X

This command is used to configure the WAN and LAN device interfaces.

```
ForumOS# network config two-device-iface <enter>
```

```
# Please enter: LAN Device Address
# The IP Address for the LAN device interface
```

```
> 10.5.6.94 <enter>
```

*[Enter the LAN Device Address or press <enter> to accept default]*

```
# Please enter: LAN Device Netmask
# The netmask for the LAN device interface
```

```
> 255.255.255.0 <enter>
```

*[Enter the LAN Device Netmask or press <enter> to accept default]*

```
# Please enter: WAN Device Address
# The IP Address for the WAN device interface
```

```
> 10.5.6.92 <enter>
```

*[Enter the WAN Device Address or press <enter> to accept default]*

```
# Please enter: WAN Device Netmask
```

```

# The netmask for the WAN device interface

> 255.255.255.0 <enter>
[Enter the WAN Device Netmask or press <enter> to accept default]

*****
*           Two Port Inline Interface Route           *
*                                                                 *
* The WAN and LAN IP addresses are on the same         *
* subnet. The device route must exist only on a       *
* single interface.                                    *
*****
# Please enter: Interface for device route
# The interface (WAN/LAN) that will be used to route device traffic
  1 for Route Out LAN Interface
  2 for Route Out WAN Interface

> 2 <enter>
[Enter (1) for LAN or (2) for WAN]

WAN and LAN interfaces updated
ForumOS#

```

## network config wan-ip

Command Availability		
Restricted	Command	Enable
		X

This command is used to configure the WAN IP address.

```

ForumOS# network config wan-ip <enter>

# Please enter: WAN IP Address
#The IP Address for the WAN interface
<default> 10.5.6.92

> <enter>
[Press <enter> for default or enter the netmask, and then press <enter>]

# Please enter: WAN Netmask
#The netmask for the WAN interface
<default> 255.255.255.0

> <enter>
[Press <enter> for default or enter the netmask, and then press <enter>]

WAN IP address updated
ForumOS#

```

## network config wizard

Command Availability		
Restricted	Command	Enable
		X

When configuring the system network interface settings, the CLI user is prompted for a series of inputs. This command is used to configure all system network settings.

**Note:** You may accept the displayed default for each prompt by pressing the `<enter>` key. You may exit this command by typing `exit <enter>` at any time, at any prompt.

```
ForumOS# network config wizard <enter>
```

```
*****  
*      Management Interface Settings for the System      *  
*                                                        *  
* This includes the ip address and netmask that will    *  
* be used for managing the device.                      *  
*****
```

```
#Please enter: Management Address  
#The IP Address for management  
<default> 10.5.3.92
```

*[Press <enter> to accept default or enter the Management IP Address, and then press <enter>]*

```
#Please enter: Management Netmask  
#The management netmask for the system  
<default> 255.255.255.0
```

*[Press <enter> to accept default or enter the Management Netmask, and then press <enter>]*

```
*****  
*      Physical Network Topology                          *  
*                                                        *  
* These are global settings for the device that         *  
* restrict all device communication policies to         *  
* either a one-port configuration, or inline with       *  
* separate IP addresses on the WAN and LAN              *  
* interfaces.                                           *  
*****
```

```
# Please enter: Topology Mode  
# The network topology for the system  
  1 for One-Port mode  
  2 for Inline (Dual IP address) mode
```

> 1  
*[Enter (1) or (2) and then press <enter>]*

```
*****  
*           Device Interface Settings for the System           *  
*                                                                 *  
* This includes the ip address and netmask that will          *  
* be used for all system traffic. In a proxy                   *  
* configuration this will be the address that clients         *  
* connect to.                                                 *  
*****
```

# Please enter: Device IP Address  
# The default IP Address for the system

> 10.5.6.92  
*[Press <enter> to accept default or enter the System IP Address, and then press <enter>]*

# Please enter: Device Netmask  
# The default device netmask for the system

> 255.255.255.0  
*[Press <enter> to accept default or enter the System Netmask Address, and then press <enter>]*

```
*****  
*           Default Gateway Setting                             *  
*                                                                 *  
* This is an optional default gateway for the                 *  
* system that applies to either the device setting           *  
* or the management interface.                               *  
*****
```

# Please enter: Device Gateway  
# The default gateway for the system  
Enter blank value for none

> 10.5.3.1 <enter>  
*[Enter Device Gateway, and then press <enter>]*

# Please enter: Gateway Interface  
# Interface directed to the gateway  
1 Let the System Choose for you  
2 for Virtual Interface  
3 Management

> 1 <enter>  
*[Enter the gateway interface. Press 1 to let the system choose for you, or 2 for Virtual Interface, or 3 for Management, and then press <enter>]*

```
*****
```

```

*           DNS Name Server Configuration Settings           *
*                                                         *
* These are optional DNS settings that can be applied *
* to the device.                                         *
*****
# Please enter: Primary DNS
# The address of the primary DNS

> 10.5.2.11 <enter>
[Enter Primary DNS, and then press <enter>]

# Please enter: Secondary DNS
# The address of a secondary DNS

> 10.5.2.12 <enter>
[Enter Secondary DNS, and then press <enter>]

Network settings updated.
Note: DNS changes will not take effect until the system is rebooted
ForumOS#

```

## network static-host add

Command Availability		
Restricted	Command	Enable
		X

This command is used to associate an IP address to a host name. address with a host name.

```

ForumOS# network static-host add <enter>

# Please enter: Host name
# Fully qualified host name to be associated.
>
[Enter a fully qualified host name, and then press <enter>]
> test.ABCcompany.com <enter>

# Please enter: IP address
# IP address to be associated with a host name
>
[Enter an IP address to associate with the host name, and then press <enter>]
> 10.5.6.712 <enter>

Static host added
ForumOS#

```

## network static-host remove

Command Availability		
Restricted	Command	Enable
		X

This command is used to disassociate an IP address from a host name.

```
ForumOS# network static-host remove <enter>
# Please enter: Host name
# Host name to be removed.
>
[Enter the host name, and then press <enter>]
> test.forumsys.com <enter>
```

```
Static host removed
ForumOS#
```

## network utils chkport

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to perform a TCP connection to a port to determine if it is available. It is used in the same manner that a telnet request would be used to validate TCP communication ability to a target IP and Port.

```
ForumOS> network utils chkport 10.5.1.11 80

Can connect to ip/port
ForumOS> network utils chkport 10.5.1.11 801

Cannot connect to ip/port
ForumOS>
```

## network utils dns-flush

Command Availability		
Restricted	Command	Enable
		X

This command is used to flush the DNS cache.

```
ForumOS# network utils dns-flush <enter>
```

DNS cache have been flushed

```
ForumOS#
```

### network utils dns-lookup

Command Availability		
Restricted	Command	Enable
		X

This command is used to lookup the IP address if a host via DNS.

```
ForumOS# network utils dns-lookup <enter>
```

```
# Host name to lookup IP address  
[Enter host name, and then press <enter>]
```

```
> abc.com
```

```
199.181.132.250
```

```
ForumOS#
```

### network utils ntp-validate

Command Availability		
Restricted	Command	Enable
		X

This command is used to synchronize system time via NTP. The system uses *ntpd*, Network Time Protocol (NTP) daemon, for time synchronization and *ntpdate* to force a time synchronization.

**Note:** For more information on *ntpd*, refer to <http://www.cis.udel.edu/~mills/ntp/html/ntpd.html>.  
For more information on *ntpdate*, refer to <http://www.cis.udel.edu/~mills/ntp/html/ntpdate.html>.

```
ForumOS# network utils ntp-validate <enter>
```

```
Successfully synchronized with NTP server
```

```
ForumOS#
```

## network utils ping

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to locate a host on the network. You cannot ping the IP address of the device when the system is in In-Line mode.

```
ForumOS# network utils ping <enter>
```

```
#Please enter: Host Name
```

```
#The destination to ping
```

```
>10.5.2.90 <enter>
```

```
[Enter IP address to ping, and then press <enter>]
```

```
Pinging 10.5.2.90 [10.5.2.90] with 32 bytes of data:
```

```
Reply from: 10.5.2.90: bytes=32 time=2923 usec TTL=138
```

```
Reply from: 10.5.2.90: bytes=32 time=191 usec TTL=138
```

```
Reply from: 10.5.2.90: bytes=32 time=189 usec TTL=138
```

```
Reply from: 10.5.2.90: bytes=32 time=186 usec TTL=138
```

```
Reply from: 10.5.2.90: bytes=32 time=188 usec TTL=138
```

```
Reply from: 10.5.2.90: bytes=32 time=186 usec TTL=138
```

```
Reply from: 10.5.2.90: bytes=32 time=188 usec TTL=138
```

```
ForumOS#
```

## network utils traceroute

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to determine the route that packets take to network host.

```
ForumOS# network utils traceroute <enter>
```

```
# Please enter: Host Name  
# The destination to traceroute
```

```
[Enter the destination IP address to traceroute, and then press <enter>]
```

```
> 12.11.11.11 <enter>
```

```
# Please enter: Probe Wait  
# The time in seconds to wait for a response to a probe  
> 5 <enter>
```

```
[Press <enter> to accept the default of 5 seconds, or enter a value, and then press <enter>]
```

```
# Please enter: Max time-to-live (hops)  
# The maximum number of hops to attempt before reaching the target server
```

```
[Press <enter> to accept the default of 5 hops, or enter a value, and then press <enter>]
```

```
> 5 <enter>
```

```
1 10.5.3.1 0.757 ms 0.534 ms 0.507 ms  
2 67.96.115.193 1.618 ms 1.661 ms 1.549 ms  
3 65.89.226.249 28.719 ms 41.715 ms 59.791 ms  
4 216.140.10.17 24.209 ms 13.244 ms 18.801 ms  
5 192.205.32.105 14.733 ms 10.143 ms 22.680 ms
```

```
ForumOS#
```

## ping

Command Availability		
Restricted	Command	Enable
X		

This command is used to locate a host on the network. You cannot ping the IP address of the device when the system is in In-Line mode. Output is truncated.

```
ForumOS# ping <enter>
```

```
#Please enter: Host Name  
#The destination to ping
```

```
>10.5.2.90 <enter>
```

```
[Enter IP address to ping, and then press <enter>]
```

```
Pinging 10.5.2.90 [10.5.2.90] with 32 bytes of data:  
Reply from: 10.5.2.90: bytes=32 time=2923 usec TTL=138  
Reply from: 10.5.2.90: bytes=32 time=191 usec TTL=138  
Reply from: 10.5.2.90: bytes=32 time=189 usec TTL=138  
Reply from: 10.5.2.90: bytes=32 time=186 usec TTL=138  
Reply from: 10.5.2.90: bytes=32 time=188 usec TTL=138  
Reply from: 10.5.2.90: bytes=32 time=186 usec TTL=138
```

```
ForumOS#
```

**Note:** The CLI will timeout any request after two minutes. If ping is taking a long time, users can open a new CLI connection.

## reboot

Command Availability		
Restricted	Command	Enable
X		X

This command is used to reboot the system. The system will begin the reboot sequence, restart and re-initialize. When the system is available and ready, a prompt similar to the prompt below appears. This command is displayed truncated.

```
ForumOS# reboot <enter>
```

```
000090 I POLMASTR No Access Control Policies found  
000091 I POLMASTR Shutting down FileUtils  
000092 I FILEUTLS Found 0 temp files  
000093 I FILEUTLS xml-sec file utilities shutdown successfully  
000094 I POLMASTR Shutting down EncryptionEngine  
000095 I POLMASTR Shutting down SignatureEngine  
000096 I SECMANGR PolicyMaster shutdown successfully  
000097 I KEYMASTR Shutting down the KeyMaster  
000098 I KEYMASTR KeyStore saved to /forum/xmlserver/security/keystore  
000099 I KEYMASTR KeyStore is closed  
00009A I SECMANGR KeyMaster shutdown successfully
```

```
Sending all processes the TERM signal...
```

```
Sending all processes the KILL signal...
Syncing hardware clock to system time md: recovery thread got woken up ...
md: recovery thread finished ...
```

```
Turning off swap:
Unmounting file systems:
Please stand by while rebooting the system...
md: stopping all md devices.
md: updating md0 RAID superblock on device
md: hda2 [events: 00000653]<6>(write) hda2's sb offset: 5116608
md: hda1 [events: 00000653]<6>(write) hda1's sb offset: 5116544
md: md0 switched to read-only mode.
flushing ide devices: hda hdc
Restarting system.
```

## route host add

Command Availability		
Restricted	Command	Enable
		X

This command is used to add a new host route.

**Note:** The capacity of configured routes supported in the system is limited by the size of the kernel routing table.

```
ForumOS# route host add <enter>
#Please enter: Host
#The host for the route

> 10.5.5.100 <enter>
[Enter host IP address, and then press <enter>]

#Please enter: Gateway address
#The gateway for the host route

> 10.5.6.1 <enter>
[Enter gateway address, and then press <enter>]

Host route added
ForumOS#
```

## route host remove

Command Availability		
Restricted	Command	Enable
		X

This command is used to remove a host route.

```
ForumOS# route host remove <enter>
# Please enter: Host Address
#The host for the route

> 10.5.2.130 <enter>
[Enter host IP address, and then press <enter>]

# Please enter: Gateway Address
# The gateway for the host route

> 10.5.6.1 <enter>
[Enter gateway address, and then press <enter>]

Host Route Removed

ForumOS#
```

## route network add

Command Availability		
Restricted	Command	Enable
		X

This command is used to add a new network route that define the gateways for a range of addresses or if the Management console or your back end servers or clients are on a different subnet.

**Note:** The capacity of configured routes supported in the system is limited by the size of the kernel routing table.

```
ForumOS# route network add <enter>
#Please enter: Network Address
#The network address for the route

> 10.5.3.0 <enter>
[Enter IP Address, and then press <enter>]

#Please enter: Netmask
```

```

#The netmask for the route

> 255.255.255.0 <enter>
[Enter Netmask, and then press <enter>]

#Please enter: Route Type
#The route method to use
#1 for Gateway
#2 for Interface
<default> 1. Gateway

> 1 <enter>
[Press <enter> to accept default (1) or enter 2, and then press <enter>]

#Please enter: Gateway address
#The gateway for the network route

> 10.5.2.1 <enter>
[Enter Gateway Address, and then press <enter>]

Network route added
ForumOS#

```

## route network remove

Command Availability		
Restricted	Command	Enable
		X

This command is used to remove a network route.

```

ForumOS# route network remove <enter>
#Please enter: Network Address
#The network address for the route

> 10.5.5.0 <enter>
[Enter Network IP Address, and then press <enter>]

#Please enter: Netmask
#The netmask for the route

> 255.255.255.0 <enter>
[Enter netmask, and then press <enter>]

#Please enter: Route Type
#The route method used
1 for Gateway
2 for Interface
<default> 1. Gateway

[Press <enter> to accept default (1) or enter "2", and then press <enter>]

```

```
#Please enter: Gateway address
#The gateway for the network route

> 10.5.6.1 <enter>
[Enter Gateway address, and then press <enter>]
```

Removing network route

ForumOS#

## show acl-groups

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to display the Groups associated with a specific Access Control List (ACL).

**Note:** Groups and sub-groups are separated by a '\$'. For example: GroupParent\$sub-group.

```
ForumOS# show acl-groups <enter>

# Please enter: ACL name
# The acl to display

> Developers <enter>
[Enter the ACL name, and then press <enter>]
```

ACL: Developers

Groups

```
-----
Siteminder-SM100
Siteminder-SM700
Tivoli-Tiv_Capris
Tivoli-Tiv_Ventura_SSL
Vendors
```

ForumOS#

## show acls

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to displays all Access Control Lists (ACLs).

```
ForumOS# show acls <enter>
```

```
-----  
ACL Policy  
-----  
Administrators  
Developers  
Executives  
General_Users  
Managers  
Research_and_Devel...
```

```
ForumOS#
```

## show arp

Command Availability		
Restricted	Command	Enable
		X

This command is used to display the system ARP table.

```
ForumOS# show arp <enter>
```

```
-----  
                        ARP Table  
-----  
IP Address           Hardware Address      Interface  
10.5.6.1             00:06:D7:3C:C3:25     WAN  
10.5.3.114          00:0B:DB:82:F4:BE     Management  
10.5.6.82           00:04:23:06:DC:5A     WAN  
10.5.6.85           00:E0:81:23:18:CB     WAN  
10.5.6.86           00:E0:81:23:19:94     WAN
```

```
ForumOS#
```

## show backup-settings

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to display backup settings.

```
ForumOS# show backup-settings <enter>
```

```
-----  
Backup Settings  
-----  
Time: 13:19  
Server: 10.5.6.40  
Directory: /incoming  
Transfer Mode: Passive  
Username: ftp  
Password: *****  
Enabled: Yes  
ForumOS#
```

**Note: If the system config backup-wizard has not yet been run, the listed elements under the Backup Settings table will be blank.**

## show connections

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to view all network connections.

```
ForumOS# show connections <enter>
```

Active Internet connections

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	10.5.3.92:5060	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:7030	0.0.0.0:*	LISTEN
tcp	0	0	10.5.3.92:22	0.0.0.0:*	LISTEN
tcp	0	0	10.5.3.92:5050	0.0.0.0:*	LISTEN
udp	0	0	0.0.0.0:32797	0.0.0.0:*	
udp	0	0	0.0.0.0:32798	0.0.0.0:*	
udp	0	0	10.5.6.92:123	0.0.0.0:*	
udp	0	0	10.5.3.92:123	0.0.0.0:*	
udp	0	0	127.0.0.1:123	0.0.0.0:*	
udp	0	0	0.0.0.0:123	0.0.0.0:*	

```
ForumOS#
```

## show crypto settings

Command Availability		
Restricted	Command	Enable
	X	X

This command displays cryptographic hardware acceleration settings.

```
ForumOS# show crypto settings <enter>
```

```
Cryptographic acceleration enabled  
ForumOS#
```

**Note:** This command is unavailable on the HSM-enabled system and the Type-PCI card product.

## show crypto stats

Command Availability		
Restricted	Command	Enable
	X	X

This command displays cryptographic hardware statistics.

```
ForumOS# show crypto stats <enter>
```

```
                Crypto Statistics  
    Number of RSA Exp Operations : 0  
    Number of RSA CRT Operations : 0  
    Number of Paddings performed : 0  
    Number of signed results with high bit on : 0  
    Errors performing RSA Exp operations : 0  
    Errors performing RSA CRT operations : 0  
    Errors performing memory allocations : 0
```

```
ForumOS#
```

**Note:** This command is unavailable on the HSM-enabled system the Type-PCI card product.

## show email-config

Command Availability		
Restricted	Command	Enable
	X	X

This command displays the email configuration.

```
ForumOS# show email-config <enter>
```

```
SMTP server: 10.5.2.12
From email address: system@customer.com
Send system alert to email address: klittle@ABC.com
```

```
ForumOS#
```

## show failover-config

Command Availability		
Restricted	Command	Enable
	X	X

This command is used display the current failover configuration. This example displays the output after configuring a Master.

```
ForumOS# show failover-config <enter>
```

```
-----
                        Failover Configuration
-----
Configuration Mode: Master
Last synchronization: Wed June 28 13:41:45 EST 2006
Synchronization in progress: 100% completed
```

```
ForumOS#
```

**Note:** For an overview of Failover, refer to the Failover section of the *Forum Systems Sentry™ System Management Guide*. Failover is unavailable with the Type-PCI card product.

## show fips-mode

Command Availability		
Restricted	Command	Enable
		X

This command toggles FIPS mode.

```
ForumOS# show fips-mode <enter>
```

```
*****  
*                               Enable FIPS Mode                               *  
*                                                                           *  
* This will stops all current system traffic so      *  
* listeners and crypto settings can be reset        *  
*****
```

```
# Please enter: Confirm  
# Are you sure you want to turn FIPS mode on  
  Y to confirm  
  N to cancel
```

```
> y <enter>
```

```
[Backspace, and type Y or press <enter> to accept the default (N)]
```

```
FIPS mode has been changed to on  
ForumOS#
```

## show general

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to view general statistics about the system. This example displays the output on a model 1503.

```
ForumOS# show general <enter>
```

```
-----  
                          System Statistics  
-----  
      Model: 1503  
    Build Version: 6.3  
  Firmware Version: 6.3  
    System Name: Value not set
```

System Start Time: 11:43:03 AM EDT  
System Up Time: 0 years, 0 months, 0 days, 0 h, 9 min, 21 s, 628ms

```
-----  
                          System Memory  
-----  
      Total Memory: 1058693120  
      Free Memory: 854310912  
      Used Memory: 204382208  
Percent Free Memory: 81  
Percent Used Memory: 19  
-----
```

ForumOS#

**Note:** The Model field displayed in this command is the 1503. If you have an HSM-enabled or FIPS-certified system, that model number would be listed instead. The Type-PCI card platform displays model 500 Type-PCI.

### show group-users

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to display the users associated with a specific Group.

**Note:** Groups and sub-groups are separated by a '\$'. For example: GroupParent\$sub-group

```
ForumOS# show group-users <enter>  
  
# Please enter: Group name  
# The group to display  
  
> JamesGroup<enter>  
[Enter a Group name, and then press <enter>]  
  
Associated Users  
-----  
jamesmith  
  
ForumOS#
```

## show groups

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to display all Groups and their associated sub-groups.

**Note:** Sub-groups are displayed as nested groups. System groups (SNMPMonitor and SNMPTech) do not have sub-groups.

```
ForumOS# show groups <enter>
```

```
-----  
Group Policy  
-----  
Auditors  
East_Coast_Corporate  
Group1  
Group2  
JamesGroup  
NickGroup  
SNMPMonitor*  
SNMPTech*  
TomGroup  
West_Coast_Corporate  
* = System Groups
```

```
ForumOS#
```

## show hsm enquiry

Command Availability		
Restricted	Command	Enable
		X

**Note:** This command is available only on the HSM-enabled system.

This command is used to display information about the HSM server and module(s).

```
ForumOS# show hsm enquiry <enter>
```

```
Module #1:  
enquiry reply flags none  
enquiry reply level 6
```

```

serial number      F256-2DFB-54AC
mode              operational
version          6.0.1
speed index      1536
rec. queue       67..75
level one flags   Hardware HasTokens
version string    6.0.1 built on Jul 12 2005 10:41:42
checked in       000000003d2e9589 Fri Jul 12 04:38:33 EDT 2002
level two flags   none
max. write size  8192
level three flags KeyStorage
level four flags OrderlyClearUnit HasNSOPermsCmd ServerHasPollCmds
                  FastPollSlotList HasKLF HasShareACL HasFeatureEnable

module type code  7
product name     nC1003P/nC3023P
device name      #1 nFast PCI device, bus 6, slot 3.
EnquirySix version 1
impath kx groups DHPPrime1024
feature ctrl flags LongTerm
features enabled  StandardKM

```

ForumOS#

**Note:** If, in the unlikely event, the customer experiences problems with the hardware, they might be asked to run this command to provide Forum Systems Customer Support the information listed. .

### show hsm security-world-id

Command Availability		
Restricted	Command	Enable
		X

This command displays the Security World id for this system.

```

ForumOS# show hsm security-world-id <enter>

BE1EDEEA 38F0EF08 35DABDB6 FE585BBE 30080DF1

ForumOS#

```

### show hsm stattree

Command Availability		
Restricted	Command	Enable
		X

**Note:** This command is available only on the HSM-enabled system.

This command is used to display statistics for the HSM server and module(s). Output is truncated.

```
ForumOS# show hsm stattree <enter>
```

```
+ServerGlobals:  
-Uptime           692803  
-CmdCount         506449  
-CmdBytes         18981552
```

```
ForumOS#
```

**Note:** If, in the unlikely event, the customer experiences problems with the hardware, they might be asked to run this command to provide Forum Systems Customer Support the information listed. For more information about the output of `show hsm stattree`, refer to [Appendix H](#).

## show idle-timeout

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to show the idle timeout.

```
ForumOS# show idle-timeout
```

```
10
```

```
ForumOS#
```

## show ifconfig

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to show statistics and configuration on all interfaces.

```
ForumOS# show ifconfig <enter>
```



## show interfaces

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to show all network interface settings.

ForumOS# *show interfaces* <enter>

```
-----  
                        Network Interfaces  
-----  
Management IP Address: 10.5.3.92  
  Management NetMask: 255.255.255.0  
    Filter: Disabled  
Management Interface: MGMT  
  Topology Mode: Inline Mode (Dual IP address)  
Device IP Address Wan: 10.5.6.92  
  Device NetMask Wan: 255.255.255.0  
Device IP Address Lan: 11.12.1.2  
  Device NetMask Lan: 255.255.255.0  
  Default Gateway: 10.5.6.1  
    Primary DNS: 10.5.2.12  
    Secondary DNS: 10.5.2.11  
Wan/Lan Phy Setting: Auto-Negotiate
```

ForumOS#

## show listeners

Command Availability		
Restricted	Command	Enable
	X	X

Network policies (the listeners) cannot be set from the CLI, although CLI users may view port numbers and associated data. Listener and Remote Network policies are only set from the Web Admin UI in the Network Policies screen. This command is used to shows all Network policy listeners. Output is truncated.

ForumOS# *show listeners* <enter>

```
-----  
                        Listeners  
-----
```

Web Admin Port = 5050  
GDM Admin Port = 5070

-----  
Policy - FTP\_ABC  
-----

Enabled: true PolicyMode: One-Port  
Listener Ip: 10.5.6.92 Listener Port: 21  
Remote Host: 10.5.3.108 Remote Port: 21  
GET OpenPGP Policy: ABCPGP-encrypt PUT OpenPGP Policy: ABCPGP-decrypt  
Prevent User@Host: false Ftp User Mode: Ignored

-----  
Policy - SpireProxy  
-----

Enabled: true PolicyMode: One-Port  
Listener Ip: 10.10.10.10 Listener Port: 80  
Remote Host: 11.11.11.11 Remote Port: 80  
List. SSL Enable: false Remote SSL Enable: false  
List. SSL Policy: default SSL Initiation Policy: default

Min Thread Count: 1 Max Thread Count: 64

-----  
Policy - WorkGroupXML  
-----

Enabled: true PolicyMode: One-Port  
Listener Ip: 10.3.3.12 Listener Port: 8082  
Remote Host: 22.22.22.22 Remote Port: 8082  
List. SSL Enable: true Remote SSL Enable: true  
List. SSL Policy: SSL\_Bob\_Term SSL Initiation Policy: SSL\_Generic\_Init

Min Thread Count: 1 Max Thread Count: 64

ForumOS#

**Note:** The default port for the WebAdmin is 5050. If this port is modified, record the new port number and provide them to Administrators.

## show log access

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to display the internal audit logs. Output is truncated.

```
ForumOS# show log access <enter>
```

```
Please enter: Access logs
```

```
# List of access logs
```

```
> 7 <tab>
```

```
[Enter a numeric value for the month (7), and then press <tab>]
```

```
7/10/05 7/12/05 7/14/05 7/16/05 7/18/05 7/6/05 7/8/05
```

```
7/11/05 7/13/05 7/15/05 7/17/05 7/5/05 7/7/05 7/9/05
```

```
> 7
```

```
> 7/11 <tab>
```

```
[Enter a slash (/), a numeric value for the day (11), press <tab>, a remaining slash and the numeric value for the year (05) are added. Press <enter>]
```

```
> 7/11.05 <enter>
```

```
00B2B6 14:53:31.028 X0023BD 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
```

```
00B2B5 14:53:29.560 X0023BC 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
```

```
00B2B4 14:53:28.974 X0023BB 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
```

```
00B2B3 14:53:28.788 X0023BA 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
```

```
00B2B2 14:53:27.812 X0023B9 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
```

```
00B2B1 14:53:27.232 X0023B8 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
```

```
00B2B0 14:53:26.683 X0023B7 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
```

```
00B2AF 14:53:26.154 X0023B6 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
```

```
00B2AE 14:53:24.782 X0023B5 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
```

```
00B2AD 14:53:24.203 X0023B4 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
```

```

00B2AC 14:53:23.666 X0023B3 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
00B2AB 14:53:23.135 X0023B2 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
00B2AA 14:53:22.598 X0023B1 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
00B2A9 14:53:22.064 X0023B0 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
00B2A8 14:53:21.494 X0023AF 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
00B2A7 14:53:19.692 X0023AE 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
00B2A6 14:53:19.156 X0023AD 08409 I 192.168.7.11 POST / HTTP/1.1 200 345
00B2A5 14:53:18.619 X0023AC 08409 I 192.168.7.11 POST / HTTP/1.1 200 345

```

ForumOS#

## show log audit

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to display the internal audit logs. Output is truncated.

ForumOS# *show log audit* <enter>

Please enter: Audit logs

# List of audit logs

> 7 <tab>

*[Enter a numeric value for the month (7), and then press <tab>]*

7/10/05 7/12/05 7/14/05 7/16/05 7/18/05 7/6/05 7/8/05

7/11/05 7/13/05 7/15/05 7/17/05 7/5/05 7/7/05 7/9/05

> 7

> 7/11 <tab>

*[Enter a slash (/), a numeric value for the day (11), press <tab>, a remaining slash and the numeric value for the year (05) are added. Press <enter>]*

> 7/11.05 <enter>

```

000096 12:54:44.397 A0000216 13014 I Login succeeded - admin1 via WebAdmin
from
10.5.3.114 with Session ID A0000216

```

```

000097 12:55:56.011 A0000216 08001 I Add succeeded - Network policy:
      Policy Name: Resp_100
      Usage Type: SMTP Response
Remote Address or Host Name: 11.11.11.22:2522
      From Address: Mailer Daemon <mailer-daemon@10.5.6.92>
      To Address:
      Subject:
      Enabled: No
000098 12:55:56.013 A0000216 08007 I Enable succeeded - Network policy
'Resp_100
'
000099 12:56:05.245 A0000216 08001 I Add succeeded - Network policy:
      Policy Name: List_100
      Client IP Ranges:
System Listener: [Device IP]:25
      Response Policy: Resp_100
      Error Template: Special XML Template
      Enabled: No
00009A 12:56:05.256 A0000216 08007 I Enable succeeded - Network policy
'List_100
'

ForumOS#

```

## show log defaultav

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to display the default AV log. Output is truncated.

```

ForumOS# show log defaultav <enter>
Mon Mar 21 17:50:46 2005 -> +++ Started at Mon Mar 21 17:50:46 2005
Mon Mar 21 17:50:46 2005 -> Log file size limited to 2097152 bytes.
Mon Mar 21 17:50:47 2005 -> Protecting against 30736 viruses.
Mon Mar 21 17:50:47 2005 -> Bound to address 127.0.0.1 on port 3310
Mon Mar 21 17:50:47 2005 -> Setting connection queue length to 30
Mon Mar 21 17:50:47 2005 -> Archive: Recursion level limit set to 9.
Mon Mar 21 17:50:47 2005 -> Archive: Files limit set to 1000.
Mon Mar 21 17:50:47 2005 -> Archive: Compression ratio limit set to 250.
Mon Mar 21 17:50:47 2005 -> Archive support enabled.
Mon Mar 21 17:50:47 2005 -> Self checking every 1800 seconds.
Tue Mar 22 15:16:36 2005 -> Exiting (clean)
Tue Mar 22 15:16:36 2005 -> --- Stopped at Tue Mar 22 15:16:36 2005

```

ForumOS#

## show log defaultavupdate

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to display the default AV updated log. Output is truncated.

```
ForumOS# show log defaultavupdate <enter>
```

```
-----  
ClamAV update process started at Mon Mar 21 17:50:49 2005  
main.cvd updated (version: 30, sigs: 31086, f-level: 4, builder: tkojm)  
daily.cvd updated (version: 778, sigs: 710, f-level: 4, builder: diego)  
Database updated (31796 signatures) from database.clamav.net (IP:  
69.93.108.98)
```

```
-----  
ClamAV update process started at Mon Mar 21 18:06:31 2005  
main.cvd is up to date (version: 30, sigs: 31086, f-level: 4, builder: tkojm)  
daily.cvd is up to date (version: 778, sigs: 710, f-level: 4, builder: diego)
```

```
-----  
ClamAV update process started at Tue Mar 22 01:06:31 2005  
main.cvd is up to date (version: 30, sigs: 31086, f-level: 4, builder: tkojm)  
daily.cvd is up to date (version: 778, sigs: 710, f-level: 4, builder: diego)  
-----
```

ForumOS#

## show log opsec

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to display the OPSEC log.

```
ForumOS# show log opsec <enter>
```

ForumOS#

## show log system

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to display the internal system logs. Output is truncated.

```
ForumOS# show log system <enter>
```

```
# Please enter: System logs
```

```
# List of system logs
```

```
> 7 <tab>
```

```
[Enter a numeric value for the month (7), and then press <tab>.]
```

```
7/19/05 7/21/05 7/23/05 7/25/05 7/27/05 7/29/05 7/31/05 7/20/05  
7/22/05 7/24/05 7/26/05 7/28/05 7/30/05
```

```
[All available logs for the month entered are displayed. Enter a numeric value for the day (22) and then press <tab>. The year appears.]
```

```
>7/22 <tab>
```

```
[Press <enter> and the log for the given date appears.]
```

```
> 7/22/05 <enter>
```

```
0000AD 00:00:00.984 X0000000 0B006 I Sign succeeded - Signed System historic  
log for Jul 21, 2005  
0000AE 00:00:00.999 X0000000 0B00B I Log Archive succeeded - Created System  
historic log for Jul 21, 2005  
0000AF 10:12:09.876 X0000000 26010 I Verifying the signature in the license  
0000B0 10:12:09.918 X0000000 26011 I Signature in the license verified  
successfully  
0000BC 10:25:13.678 X0000000 00010 I Shutting down server  
0000BD 10:25:13.678 X0000000 0000F I Shutting down Web Admin Server  
0000BE 10:25:13.678 X0000000 00202 I Shutting down the web admin server  
0000BF 10:25:15.899 X0000000 00015 I Web Admin Server shutdown successfully
```

```
ForumOS#
```

## show logging-settings

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to display the current log configuration.

**Note:** For information on importing your own corporate SSL certificate on the system, refer to the Sample System Configuration User Your Own SSL Key Pair appendix in the *Forum Systems Sentry™ Web-based Administration Guide*.

```
ForumOS# show logging-settings <enter>
```

```
-----  
                        Internal Log Configuration  
-----  
      Audit Logging Level: Info  
  
      Audit Log Lifespan (in days): 15  
  
      System Logging Level: Info  
  
      System Log Lifespan (in days): 15  
  
      Access Logging Level: Info  
  
      Access Log Lifespan (in days): 15
```

```
ForumOS#
```

## show max-threads

Command Availability		
Restricted	Command	Enable
	X	X

This command displays the current maximum number of listener threads allowed.

```
ForumOS# show max-threads <enter>
```

128

ForumOS#

## show network iptable

Command Availability		
Restricted	Command	Enable
	X	X

This command displays the system IP table information.

```
ForumOS# show network iptable <enter>
```

```
# Please enter: IP Table Name
# The IP table to view
  1 for NAT
  2 for Input
  3 for Output
```

```
> 2 <enter>
```

```
[Enter 2, and then press <enter>]
```

```
Chain INPUT (policy ACCEPT 378K packets, packets, 413M bytes)
  pkts bytes target      prot opt in   out  source      destination
```

ForumOS#

## show routes

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to shows all network and host routes that make up the kernel IP routing table.

```
ForumOS# show routes <enter>
```

```

-----
                        Routing Table
-----
Destination      Gateway          Netmask          Type  Interface
192.168.2.0      *                255.255.255.0   NET   LAN
10.5.6.0         *                255.255.255.0   NET   Management
127.0.0.0        *                255.0.0.0       NET   Loopback

ForumOS#

```

## show snmp

Command Availability		
Restricted	Command	Enable
	X	X

This command shows the SNMP system name, location and contact.

```
ForumOS# show snmp <enter>
```

```
System name: Houston
System location: 3rd floor, Room 314, Bay 2, Rack 5, Slot 30
System contact: John Smith johnsmith@anywhere.com
```

```
ForumOS#
```

## show static-hosts

Command Availability		
Restricted	Command	Enable
	X	X

This command displays the static table lookup for host names.

```
ForumOS# show static-hosts <enter>
```

```

-----
                        Static Host Name Lookup Table
-----

test.ABCcompany.com          10.5.6.217

```

ForumOS#

## show statistics

Command Availability		
Restricted	Command	Enable
	X	X

This command displays system statistics. Output is truncated.

```
ForumOS# show statistics <enter>
```

```
System Statistics
```

```
Name,Group,Value:
```

```
-----
```

```
fsgsDocSizeAverage,Document_Processing,0  
fsgsDocSizeMin,Document_Processing,0  
fsgsDocSizeMax,Document_Processing,0  
fsgsDocProcessPass,Document_Processing,0  
fsgsDocProcessFail,Document_Processing,0  
fsgsDocChars,Document_Processing,0  
fsgsDocProxies,Document_Processing,0  
fsgsDocTotalErrors,Document_Processing,0  
fsgsDocSigCreatePass,Document_Processing,0  
fsgsDocSigCreateFail,Document_Processing,0  
fsgsDocSigVerifyPass,Document_Processing,0  
fsgsDocSigVerifyFail,Document_Processing,0  
fsgsDocElemEncryptPass,Document_Processing,0  
fsgsDocElemEncryptFail,Document_Processing,0  
fsgsDocContEncryptPass,Document_Processing,0  
fsgsDocContEncryptFail,Document_Processing,0  
fsgsDocArchiveChars,Document_Processing,0  
-----
```

```
By Group:
```

```
fsgsDocSizeAverage,Document_Processing,0  
fsgsDocSizeMin,Document_Processing,0  
fsgsDocSizeMax,Document_Processing,0  
fsgsDocProcessPass,Document_Processing,0  
fsgsDocProcessFail,Document_Processing,0  
fsgsDocChars,Document_Processing,0  
fsgsDocProxies,Document_Processing,0  
fsgsDocTotalErrors,Document_Processing,0  
fsgsDocSigCreatePass,Document_Processing,0  
fsgsDocSigCreateFail,Document_Processing,0  
fsgsDocSigVerifyPass,Document_Processing,0  
fsgsDocSigVerifyFail,Document_Processing,0  
fsgsDocArchPass,Document_Processing,0  
fsgsDocArchFail,Document_Processing,0  
fsgsDocArchiveChars,Document_Processing,0
```

ForumOS#

## show syslog-targets

Command Availability		
Restricted	Command	Enable
	X	X

This command displays all remote Syslog destinations.

ForumOS# *show syslog-targets* <enter>

```
-----  
Policy           Destination           Enabled  
-----  
Mgmt-1           9.9.9.9 : 514         True  
RedAlertLogs     10.7.4.23 : 514      True  
WebLogs5         9.9.9.9 : 515         True  
WebLogs6         9.9.9.9 : 516         False
```

ForumOS#

## show system-settings

Command Availability		
Restricted	Command	Enable
	X	X

This command displays system wide configuration.

ForumOS# *show system-settings* <enter>

```
-----  
System Settings  
-----  
Web Admin Port: 5050  
Global Device Management (GDM) Port: 5070  
NTP Time Server: 192.5.41.41  
Session Timeout (in minutes): 120
```

```
SSL Termination Policy: factory ssl termination policy
SSL Initiation Policy: factory ssl initiation policy
Web Admin Client IP ACL Policy: Unrestricted
```

-----  
Email Config  
-----

```
SMTP server: 10.5.2.12
From email address: klittle@ABC.com
Send system alert to email address: appliance@company.com
```

ForumOS#

**Note:** If the WebAdmin port number is changed, record the new port number and provide it to your Administrators. The WebAdmin port cannot be set to 0.

### show tibrv services

Command Availability		
Restricted	Command	Enable
	X	X

This command displays all Tibco/Rendezvous registered services.

ForumOS# *show tibrv services* <enter>

```
7501
7500
```

ForumOS#

**Note:** If the Tibco/Rendezvous feature is not licensed, this command will not be visible in the CLI.

### show tibrv statistics

Command Availability		
Restricted	Command	Enable
	X	X

This command displays all Tibco/Rendezvous statistics for a service after selecting one of the Tibco services.

```
ForumOS# show tibrv statistics <enter>
```

```
# Please enter: Service  
# The service to display statistics on  
> 7500 <enter>  
[Enter the service, and then press <enter>]
```

```
-----  
Rendezvous Daemon Statistics  
-----  
Service: 7500  
Network: 192.168.7.255  
Reliability: 60  
Creation: 2004-08-068 (09:09:59)  
Clients: 1  
Subscriptions: 2  
-----  
Inbound Rates (Per Sec) | Outbound Rates (Per Sec)  
-----  
msgs | bytes | pkts | msgs | bytes | pkts  
-----  
0.0   0.0   0.0   0.0   0.0   0.0  
-----  
Inbound Totals          | Outbound Totals  
-----  
msgs | bytes | pkts | msgs | bytes | pkts  
-----  
0     0     0     6     1033  34  
ForumOS>
```

**Note:** If the Tibco/Rendezvous feature is not licensed, this command will not be visible in the CLI.

## show time

Command Availability		
Restricted	Command	Enable
	X	X

This command displays the system time and date displayed as Greenwich Mean Time minus five hours, which is Eastern Standard Time.

```
ForumOS# show time <enter>
```

```
Tues Apr 27 15:17:22 GMT-05:00 2006  
ForumOS#
```

## show user-advanced

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to display the advanced options a specific User.

```
ForumOS# show user-advanced <enter>
```

```
# Please enter: User name  
# The user account to display
```

```
> robertwhite <enter>  
[Enter User name, and then press <enter>]
```

```
User:          robertwhite  
DN Alias:      CN=1024bit, OU=Quality Assurance, O=FORUM SYSTEM,  
               ST=Massachusetts, C=US  
E-Mail:       robert@test.forumsys.com  
Signing key:   robert_rsa
```

```
ForumOS#
```

## show user-groups

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to display the Groups associated with a specific User.

**Note:** Groups and sub-groups are separated by a '\$'. For example: GroupParent\$sub-group

```
ForumOS# show user-groups <enter>
```

```
# Please enter: User name  
# The user account to display
```

```
> donstreeter <enter>
[Enter User name, and then press <enter>]
```

```
User: donstreeter
```

```
Associated Groups
```

```
-----
```

```
Bus_Development
Bus_Development$Engineering
Bus_Development$Architects
```

```
ForumOS#
```

## show users

Command Availability		
Restricted	Command	Enable
	X	X

This command is used to displays all Users. A User policy identifies a registered user. User names (used for login) and User passwords are managed in the Users screen of the product.

```
ForumOS# show users <enter>
```

```
-----
User Policy      Enabled
-----
```

```
admin1          True
charleslee      True
gdmadmin        True
jamesmith       True
janeflower      True
jkantos         True
klittle         True
markcross       True
marysmith       True
nickthomas      True
tomwaters       True
walter          True
```

```
ForumOS#
```

**Note:** When adding, modifying and removing Users from the CLI, and toggling back to the Users screen of the WebAdmin, force a refresh in the Users screen by clicking on any other screen, then navigating back to the Users screen for an updated view.

## shutdown

Command Availability		
Restricted	Command	Enable
		X

This command is used to shut down the system. The system will complete the shutdown sequence. Press the soft power switch on the front of the system and hold for a few seconds.

```
ForumOS# shutdown <enter>
```

```
INIT: Switching to runlevel: 0
```

```
-----  
-----
```

```
Unmounting file systems:
```

```
Halting system...
```

```
Shutting down RAID
```

```
Flushing disk buffers
```

```
Power down.
```

```
—
```

**Note:** To re-engage the system, press the soft power switch on the front of the system. Refer to the system schematic that is appropriate for your system in the *Forum Systems Sentry™ Version 8.7 Hardware Installation Guide*. If moving the system from one location to another, press the main power switch on the back of the system before unplugging it.

## syslog destination add

Command Availability		
Restricted	Command	Enable
		X

This command configures a Syslog remote destination.

```
ForumOS# syslog destination add <enter>
```

```
#Please enter: Syslog Policy
```

```
#The policy name of the syslog policy to add
```

```
> WebLogs5 <enter>
```

```
[Enter syslog policy name, and then press <enter>]
```

```
#Please enter: Host Name or address
#The host name or address of the destination

> 9.9.9.29 <enter>
[Enter host name or address, and then press <enter>]

#Please enter: Port
#The port number of the destination

> 523 <enter>
[Enter port number, and then press <enter>]

#Please enter: Severe
#Redirect Severe messages to syslog destination
#Y to log Severe messages
#N to ignore Severe messages

> Y <enter>
[Enter N or press <enter> to accept the default]

#Please enter: Warning
#Redirect Warning messages to syslog destination
#Y to log Warning messages
#N to ignore Warning messages

> Y <enter>
[Enter N or press <enter> to accept the default]

#Please enter: Info
#Redirect Info messages to syslog destination
#Y to log Info messages
#N to ignore Info messages

> Y <enter>
[Enter N or press <enter> to accept the default]

#Please enter: Debug
#Redirect Debug messages to syslog destination
#Y to log Debug messages
#N to ignore Debug messages

> Y <enter>
[Enter N or press <enter> to accept the default]

#Please enter: Facility Code
#The syslog facility code to use in remote logs
0. General User
1. Daemon
2. Local 0
```

- 3. Local 1
- 4. Local 2
- 5. Local 3
- 6. Local 4
- 7. Local 5
- 8. Local 6
- 9. Local 7

<default> 0

> 2 <enter>

*[Enter 1, 2, 3, 4, 5, 6, 7, 8, 9 or press <enter> to accept default]*

#Please enter: Enable policy

#Enable the new policy

#Y to enable policy

#N to disable policy

<default> Y

> <enter>

*[Enter N or press <enter> to accept the default]*

Syslog Destination was added

ForumOS#

## syslog destination disable

Command Availability		
Restricted	Command	Enable
		X

This command disables a Syslog remote destination.

ForumOS# *syslog destination disable* <enter>

#Please enter: Syslog Policy

#The name of the syslog policy to disable

> *syslog-3* <enter>

*[Enter Syslog policy name, and then press <enter>]*

Syslog destination is now disabled

ForumOS#

## syslog destination enable

Command Availability		
Restricted	Command	Enable
		X

This command enables a Syslog remote destination.

```
ForumOS# syslog destination enable <enter>
```

```
#Please enter: Syslog Policy  
#The name of the syslog policy to enable
```

```
> syslog-3 <enter>  
[Enter Syslog policy name, and then press <enter>]
```

```
Syslog destination is now enabled  
ForumOS#
```

## syslog destination remove

Command Availability		
Restricted	Command	Enable
		X

This command removes a Syslog remote destination.

```
ForumOS# syslog destination remove <enter>
```

```
#Please enter: Syslog Policy  
#The name of the syslog policy to remove
```

```
> syslog-3 <enter>  
[Enter Syslog policy name, and then press <enter>]
```

```
Syslog destination was removed
```

```
ForumOS#
```

## system config backup-enable

Command Availability		
Restricted	Command	Enable
		X

This command is used to enable the automatic backup of the config file.

**Note:** To run this command, the `system config backup-wizard` command must have been executed before any of the other backup commands (`system config backup-enable` and `system config backup-test`) can be executed.

For more information about the system config backup commands, refer to the [system config backup-wizard](#) command.

```
ForumOS# system config backup-enable <enter>
```

```
# Please enter: Enable/Disable
```

```
# Enable/Disable the automatic backup of the config file
```

```
Y to enable backup
```

```
N to disable backup
```

```
> N
```

```
[Overwrite N with Y to enable automatic backup of the config file, or press  
<enter> to accept the default N which disables backing up the config file]
```

```
> Y <enter>
```

```
Backup settings updated.
```

```
ForumOS#
```

## system config backup-test

Command Availability		
Restricted	Command	Enable
		X

This command is used to initiate a configuration file backup immediately, and tests that the backup has occurred.

**Note:** To run this command, the `system config backup-wizard` command must have been executed before any of the other backup commands (`system config backup-enable` and `system config backup-test`) can be executed.

For more information about the system config backup commands, refer to the [system config](#)

## backup-wizard command.

```
ForumOS# system config backup-test <enter>
```

Backup has been performed

```
ForumOS#
```

## system config backup-wizard

Command Availability		
Restricted	Command	Enable
		X

This command is used to set ftp parameters for backup of the config file.

**Note:** This command must be executed before any of the other backup commands (system config backup-enable and system config backup-test) can be executed.

Forum Systems recommends that you execute:

- the system config backup-wizard command first (this command sets up configuration for how to perform backups.
- the system config backup-enable command second (this command determines whether backup is ON or OFF.
- the system config backup-test command last (this command performs an immediate run of the backup configuration.

```
ForumOS# system config backup-wizard <enter>
```

```
# Please enter: Backup time
```

```
# Time of day in which backup takes place
```

```
  e.g. 12 for 12PM, 00 for 12AM, 13 for 1PM, etc
```

```
>
```

```
[Enter backup time in format HH:MM, and then press <enter>]
```

```
> 00:00 <enter>
```

```
# Please enter: Server IP Address
```

```
# IP Address of the Backup Server
```

```
>
```

```
[Enter Server IP address of the Backup Server, and then press <enter>]
```

```
> 1.1.1.1 <enter>
```

```
# Please enter: Server directory
```

```
# Name of the directory to place the config file backups
```

```
>
```

```
[Enter the name of the directory to place the config file backups, and then
press <enter>]
> /ConfigBackupFiles/ <enter>

# Please enter: FTP Transfer Mode
# FTP Transfer Mode Configuration
  1 Passive Mode
  2 Active Mode
> 1 <enter>

[Enter 2 for Active Mode, or press <enter> for Passive Mode]

# Please enter: Server Username
# Username of FTP server
>
[Enter the Server username, and then press <enter>]
> Scotty <enter>

# Please enter: Server Password
# FTP server Password
>
[Enter the Server password, and then press <enter>]
> ***** <enter>

# Please enter: Confirm password
# Confirm the FTP server password
>
[Re-enter the Server password, and then press <enter>]
> ***** <enter>

# Please enter: Conf file password
# The configuration file password
>
[Enter the Config file password, and then press <enter>]
> ***** <enter>

# Please enter: Confirm password
# Confirm the configuration file password
>
[Re-enter the Config file password, and then press <enter>]
> ***** <enter>

Backup settings updated.
ForumOS#
```

## system config certificate-reset

Command Availability		
Restricted	Command	Enable
		X

This command resets the WebAdmin SSL Certificate.

```
ForumOS# system config certificate-reset <enter>
```

```
SSL Certificate has been reset
```

```
ForumOS#
```

## system config enable-password-set

Command Availability		
Restricted	Command	Enable
		X

This command is used to set the Enable mode password. This command displays the returned output from Command mode.

**Note:** The Enable mode password must be unique and is case sensitive, may be from 6 to 32 alphanumeric characters long, may include underscores and dashes, but not spaces.

```
ForumOS# system config enable-password-set <enter>
```

```
#Please enter: New Password  
#The new enable mode password
```

```
> boston <enter>
```

```
[Enter new Password, and then press <enter>] It will not be visible on the screen]
```

```
#Please enter: Confirm Password  
# Confirm the new enable mode password
```

```
> boston <enter>
```

```
[Re-enter Password, and then press <enter>] It will not be visible on the screen]
```

Password has been updated  
ForumOS#

## system config factory-reset

Command Availability		
Restricted	Command	Enable
		X

**Note:** On the Forum HSM-enabled or FIPS-certified system, you may either: 1) Retain the original HSM Security World after using the **system config factory-reset** command by replying Yes to “Would you like to keep the HSM's currently loaded security world key?”, or 2) erase the current HSM Security World by replying No.

**Warning:** The **system config factory-reset** command will delete all configuration data from the system including all policies, keys, users, groups, ACLs, Domains and Roles.

This command resets all system settings. The output of this command is truncated.

```
ForumOS# system config factory-reset <enter>
*****
*                               Factory Reset Requested                               *
*                                                                           *
* This will delete ALL configuration data from this system. This includes all policies, task lists *
* and keys.                                                                 *
*****
# Please enter: Confirm
# Are you sure you want to reset?
  Y to confirm reset
  N to cancel
> y <enter>
[Enter Y to confirm, or N to cancel, and then press <enter>]
```

Visible on  
all Forum  
systems  
and Type-  
PCI cards.

```
# Please enter: Save Security World Key
# Would you like to keep HSM's currently loaded security world key?
  Y to keep the currently loaded security world key
  N to erase the currently loaded security world key and
  reinitialize the HSM
```

Visible on  
Forum  
HSM-  
enabled  
and FIPS-  
certified  
system  
only.

### Retain Security World Key

```
> Y <enter>
[Enter Y to retain the HSM's currently loaded Security World Key,
and then press <enter>]
```

---

## Erase Security World Key

> *N* <enter>  
[Enter *N* to erase the HSM's currently loaded Security World Key,  
and then press <enter>]

# Please enter: Set HSM module switch to "I" mode  
# Set the HSM module switch to "I" mode and press enter to clear  
the # HSM module

The system will now reboot.

## system config fips-mode

Command Availability		
Restricted	Command	Enable
		X

This command toggles FIPS mode on a FIPS-certified system. The returned text of this command is truncated for brevity.

ForumOS# *system config fips-mode* <enter>

```
*****  
*                               Enable FIPS Mode                               *  
*                                                                           *  
* This will stop all current system traffic and *  
* perform a full reboot of the system *  
*****
```

# Please enter: Confirm  
# Are you sure you want to turn FIPS mode on  
Y to confirm  
N to cancel

> *Y* <enter>  
[Press <enter> to accept the default (*N*), or type *Y* for yes, and then press  
<enter>]

```
FIPS 0028BA 15:14:20.015 X0000000 00010 I Shutting down server  
FIPS 0028BB 15:14:20.049 X0000000 0000F I Shutdown succeeded - Web  
Admin Server has been shutdown successfully  
FIPS 002946 15:14:22.996 X0000000 00015 I Destination Manager shutdown  
successfully  
ForumOS#
```



## system config idle-timeout

Command Availability		
Restricted	Command	Enable
		X

This command is used to set the maximum number of seconds to wait for the next request from the same client on the same connection.

```
ForumOS# system config idle-timeout<enter>
```

```
# Please enter: Maximum idle timeout in seconds
```

```
# Number of seconds to wait for the next request from the same client on the same connection
```

```
> 10
```

```
[Press <enter> to accept the default (10), or backspace to overwrite 10 and enter new number of seconds to wait for next request from the same client on the same connection, and then press <enter>]
```

```
<enter>
```

```
Maximum idle timeout changed
```

```
ForumOS#
```

## system config ipacl-reset

Command Availability		
Restricted	Command	Enable
		X

This command is used to reset the IP ACL policy for the Web Admin

```
ForumOS# system config ipacl-reset
```

```
Web Admin IP ACL Policy has been reset
```

```
ForumOS#
```

## system config max-threads

Command Availability		
Restricted	Command	Enable
		X

This command sets the maximum size of the listener pool. Valid values are between 16 and 256. Default value is 128.

```
ForumOS# system config max-threads <enter>
```

```
# Please enter: Max Size
```

```
# The maximum number of threads
```

```
> 128
```

```
[Press <enter> to accept the current max number of threads, or backspace to overwrite 128 and then type 256. Then press <enter>]
```

```
> 256 <enter>
```

```
Maximum thread size changed
```

```
ForumOS#
```

## system config ntp

Command Availability		
Restricted	Command	Enable
		X

This command configures an NTP time server.

```
ForumOS# system config ntp <enter>
```

```
# Please enter: NTP Server
```

```
# The address of an NTP Time Server  
Enter blank value for none
```

```
> 192.5.41.41 <enter>
```

```
[Enter the IP address for your NTP time server, and then press <enter>]
```

```
NTP server has been set
```

```
ForumOS#
```

## system config ports

Command Availability		
Restricted	Command	Enable
		X

This command sets the system management ports.

```
ForumOS# system config ports <enter>
```

```
# Please enter: Management port
# Select the port to configure
  1 for the Web Admin port
  2 for the GDM port
> 1 <enter>
```

```
[Enter 1 to set the Web Admin port, or enter 2 to set the GDM port, and then
press <enter>]
```

```
# Please enter: Port value
# The new value of the selected port
```

```
> 5050 <enter>
[Enter the new port number, and then press <enter>]
```

```
Port has been set
```

```
ForumOS#
```

## system config session-timeout

Command Availability		
Restricted	Command	Enable
		X

This command is used to configure the inactive timeout for sessions.

```
ForumOS# system config session-timeout <enter>
```

```

# Please enter: Session timeout
# The maximum inactive interval for a session

> 120
[Press <enter> to select the default [120] or enter number of seconds for
session-timeout, and then press <enter>.]

Session timeout updated

ForumOS#

```

## system config smtp

Command Availability		
Restricted	Command	Enable
		X

This command configures an SMTP mail server.

```

ForumOS# system config smtp <enter>

# Please enter: SMTP Server
# The address of an SMTP Server
  Enter blank value for none

> 192.5.48.48 <enter>
[Enter the IP address for your SMTP mail server, and then press <enter>]

SMTP server has been set
ForumOS#

```

## system config tibrv multicast

Command Availability		
Restricted	Command	Enable
		X

This command configures IP multicast for a specific service.

```

ForumOS# system config tibrv multicast <enter>

```

```
# Please enter: Service
# The service to configure multicast for
>
[Enter the Service name to configure Tibco multicast for, and then press
<enter>]
> 7500 <enter>
```

```
# Please enter: Receive Address
# The address to listen for IP multicast traffic on
[Enter an IP address to listen for IP multicast traffic on, and then press
<enter>]
> 224.0.1.78 <enter>
```

ForumOS#

## system config time

Command Availability		
Restricted	Command	Enable
		X

This command sets the system time. NTP syncs only take place on change/setting of NTP server

```
ForumOS# system config time <enter>
```

```
# Please enter: Time
# The time in the format HH:MM, in 24-hour time.
  e.g. 12 for 12PM, 00 for 12AM, 13 for 1PM, etc
```

```
> 14:31 <enter>
[Enter hours, a colon, minutes, and then press <enter>]
```

```
# Please enter: Date
# The system date in the format MM/DD/YYYY, with leading zeros.
  e.g. 01 for January, etc.
```

```
> 12/15/2003 <enter>
[Enter the month, date and year, and then press <enter>]
```

```
Date and time successfully set
ForumOS#
```

## system config time-zone

Command Availability		
Restricted	Command	Enable
		X

This command sets the system time zone.

ForumOS# *system config time-zone* <enter>

# Please enter: Country

#

1)Africa	11)Cuba	21)Jamaica	31)Singapore
2)America	12)Egypt	22)Japan	32)Turkey
3)Antarctica	13)Eire	23)Kwajalein	
4)Arctic	14)Europe	24)Libya	
5)Asia	15)Greenwich	25)Mexico	
6)Atlantic	16)Hongkong	26)Mideast	
7)Australia	17)Iceland	27)Navajo	
8)Brazil	18)Indian	28)Pacific	
9)Canada	19)Iran	29)Poland	
10)Chile	20)Israel	30)Portugal	

> 2 <enter>

*[Enter number for designated country, and then press <enter>]*

# Please enter: Time zone

1)Adak	31)Managua	61)Louisville	91)Montserrat	121)Sao_Paulo
2)Atka	32)Menominee	62)Montreal	92)Port_of_Spain	122)Noronha
3)Anchorage	33)Merida	63)Nassau	93)Porto_Velho	123)Scoresbysund
4)Juneau	34)Mexico_City	64)New_York	94)Puerto_Rico	
5)Nome	35)Monterrey	65)Nipigon	95)Santiago	
6)Yakutat	36)Rainy_River	66)Panama	96)Santo_Domingo	
7)Dawson	37)Rankin_Inlet	67)Pangnirtung	97)St_Kitts	
8)Ensenada	38)Regina	68)Port-au-Prince	98)St_Lucia	
9)Los_Angeles	39)Swift_Current	69)Porto_Acre	99)St_Thomas	
10)Tijuana	40)Tegucigalpa	70)Rio_Branco	100)St_Vincent	
11)Vancouver	41)Winnipeg	71)Thunder_Bay	101)Thule	
12)Whitehorse	42)Bogota	72)Anguilla	102)Tortola	
13)Boise	43)Cayman	73)Antigua	103)Virgin	
14)Cambridge_Bay	44)Detroit	74)Aruba	104)St_Johns	
15)Chihuahua	45)Eirunepe	75)Asuncion	105)Araguaina	
16)Dawson_Creek	46)Fort_Wayne	76)Barbados	106)Belem	
17)Denver	47)Grand_Turk	77)Boa_Vista	107)Buenos_Aires	
18)Edmonton	48)Guayaquil	78)Caracas	108)Catamarca	
19)Hermosillo	49)Havana	79)Cuiaba	109)Cayenne	

```

20) Inuvik          50) Indiana/Indiana 80) Curacao        110) Cordoba
21) Mazatlan       51) Indiana/Knox    81) Dominica       111) Fortaleza
22) Phoenix        52) Indiana/Marengo 82) Glace_Bay     112) Godthab
23) Shiprock       53) Indiana/Vevay  83) Goose_Bay     113) Jujuy
24) Yellowknife    54) Indianapolis    84) Grenada        114) Maceio
25) Belize         55) Iqaluit         85) Guadeloupe    115) Mendoza
26) Cancun         56) Jamaica         86) Guyana         116) Miquelon
27) Chicago        57) Kentucky/Louisv 87) Halifax       117) Montevideo
28) Costa_Rica     58) Kentucky/Montic 88) La_Paz        118) Paramaribo
29) El_Salvador    59) Knox_IN         89) Manaus         119) Recife
30) Guatemala      60) Lima            90) Martinique    120) Rosario

```

```
> 64 <enter>
```

```
[Enter number for designated area, and then press <enter>]
```

```
Time zone set successfully
```

```
ForumOS#
```

## system failover config

Command Availability		
Restricted	Command	Enable
		X

This command is used to configure failover mode. This example displays configuring a gateway in Master mode.

```
ForumOS# system failover config <enter>
```

```
# Please enter: Configuration mode
```

```
# Failover configuration mode
```

```
 1 for Standalone
```

```
 2 for Master
```

```
 3 for Standby
```

```
> 1
```

```
[Press <enter> to accept the default 1 for a Standalone configuration, or use the <backspace> key to overwrite option 1 to option 2 for Master, and then press <enter>]
```

```
> 2 <enter>
```

Failover configuration updated

ForumOS#

**Note:** For an overview of Failover, refer to the Failover section of the *Forum Systems Sentry™ System Management Guide*. Failover is unavailable with the Type-PCI card product.

## system failover synchronize

Command Availability		
Restricted	Command	Enable
		X

This command schedules a policy synchronization for server running in Standby mode. This command is enabled only on the system running in Master mode. Synchronization will occur at the next Standby heartbeat interval (10 seconds).

```
ForumOS# system failover synchronize <enter>
```

Synchronization scheduled

ForumOS#

**Note:** For an overview of Failover, refer to Failover section of the *Forum Systems Sentry™ System Management Guide*. Failover is unavailable with the Type-PCI card product.

## traceroute

Command Availability		
Restricted	Command	Enable
X		

This command is used to run a traceroute to a host. The returned text of this command is truncated for brevity.

```
ForumOS# traceroute <enter>
```

```
# Please enter: Host Name
```

```
# The destination to traceroute
```

```
> 12.11.11.11
```

```
1 10.5.9.1 (10.5.9.1) 0.862 ms 0.721 ms 0.679 ms
2 67.9.11.3 (67.9.11.3) 1.626 ms 1.610 ms 1.669 ms
3 65.9.26.49 (65.9.26.49) 8.289 ms 7.942 ms 7.902 ms
5 .....
.....
29 12.11.9.24 (12.11.9.24) 40.454 ms 39.656 ms 40.985 ms
30 * 12.11.9.25 (12.11.9.25) 58.689 ms 57.788 ms

# ForumOS#
```

**Note:** The CLI will timeout any request after two minutes. If traceroute is taking a long time, users can open a new CLI connection.

## APPENDIX

### Appendix A - CLI Key Bindings

The following table displays a list of CLI functions and their respective key bindings for EMACS mode and VI mode. These functions do not interact with the system; rather, they interact with user input values only.

KEY BINDING FUNCTION	DESCRIPTION
user-interrupt	Send a SIGINT signal to the parent process.
abort	Send a SIGABRT signal to the parent process.
suspend	Suspend the parent process.
stop-output	Pause terminal output.
start-output	Resume paused terminal output.
literal-next character	Arrange for the next character to be treated as a normal This allows control characters to be entered.
cursor-right	Move the cursor one character right.
cursor-left	Move the cursor one character left.
insert-mode	Toggle between insert mode and overwrite mode.
beginning-of-line	Move the cursor to the beginning of the line.
end-of-line	Move the cursor to the end of the line.
delete-line	Delete the contents of the current line.
kill-line	Delete everything that follows the cursor.
backward-kill-line	Delete all characters between the cursor and the start of the line.
forward-word	Move to the end of the word which follows the cursor.
forward-to-word	Move the cursor to the start of the word that follows the cursor.
backward-word	Move to the start of the word which precedes the cursor.
goto-column	Move the cursor to the 1-relative column in the line specified by any preceding digit-argument sequences. For details, see the section Entering Repeat Counts in this document.
find-parenthesis	If the cursor is currently over a parenthesis character, move it to the matching parenthesis character. If not over a parenthesis character, move right to the next close parenthesis.
forward-delete-char	Delete the character under the cursor.
backward-delete-char	Delete the character which precedes the cursor.

KEY BINDING FUNCTION	DESCRIPTION
list-or-eof	This is intended for binding to ^D. When invoked when the cursor is within the line, it displays all possible completions then redisplay the line unchanged. When invoked on an empty line, it signals end-of-input (EOF) to the CLI.
del-char-or-list-or-eof	This is intended for binding to ^D. When invoked when the cursor is within the line, it invokes forward-delete-char. When invoked at the end of the line, it displays all possible completions then redisplay the line unchanged. When invoked on an empty line, it signals end-of-input (EOF) to the CLI.
forward-delete-word	Delete the word which follows the cursor.
backward-delete-word	Delete the word which precedes the cursor.
upcase-word	Convert all of the characters of the word which follows the cursor, to upper case.
downcase-word	Convert all of the characters of the word which follows the cursor, to lower case.
capitalize-word	Capitalize the word which follows the cursor.
change-case	If the next character is upper case, toggle it to lower case and vice versa.
redisplay	Redisplay the line.
clear-screen	Clear the terminal, then redisplay the current line.
transpose-chars	Swap the character under the cursor with the character just before the cursor.
set-mark	Set a mark at the position of the cursor.
exchange-point-and-mark	Move the cursor to the last mark that was set, and move the mark to where the cursor used to be.
kill-region	Delete the characters that lie between the last mark that was set, and the cursor.
copy-region-as-kill	Copy the text between the mark and the cursor to the cut abort - buffer, without deleting the original text.
yank	Insert the text that was last deleted, just before the current position of the cursor.
append-yank	Paste the current contents of the cut buffer, after the cursor.
up-history	Recall the next oldest line that was entered. Note that in VI mode you are left in command mode.
down-history	Recall the next most recent line that was entered. If no history recall session is currently active, the next line from a previous recall session is recalled. Note that in VI mode you are left in command mode.

KEY BINDING FUNCTION	DESCRIPTION
history-search-backward	Recall the next oldest line whose prefix matches the string which currently precedes the cursor (in VI command mode, the character under the cursor is also included in the search string). Note that in VI mode you are left in command mode.
history-search-forward	Recall the next newest line whose prefix matches the string which currently precedes the cursor (in VI command mode, the character under the cursor is also included in the search string). Note that in VI mode you are left in command mode.
history-re-search-backward	Recall the next oldest line whose prefix matches that established by the last invocation of either history-search-forward or history-search-backward.
history-re-search-forward	Recall the next newest line whose prefix matches that established by the last invocation of either history-search-forward or history-search-backward.
complete-word	Attempt to complete the incomplete word which precedes the cursor. Unless the host program has customized word completion, filename completion is attempted. In vi command mode the character under the cursor is also included in the word being completed, and you are left in vi insert mode.
expand-filename	Within the command line, expand wild cards, tilde expressions and dollar expressions in the filename which immediately precedes the cursor. In VI command mode, the character under the cursor is also included in the filename being expanded, and you are left in insert mode.
list-glob	List any filenames which match the wild-card, tilde and dollar expressions in the filename which immediately precedes the cursor, and then redraw the input line unchanged.
list-history	Display the contents of the history list for the current history group. If a repeat count of > 1 is specified, only that many of the most recent lines are displayed. For details, see the section Entering Repeat Counts in this document.
read-from-file	Temporarily switch to reading input from the file whose name precedes the cursor.
read-init-files	Re-read CLI configuration files.
beginning-of-history	Move to the oldest line in the history list. Note that in VI mode you are left in command mode.
end-of-history	Move to the newest line in the history list (ie. the current line). Note that in VI mode this leaves you in command mode.
digit-argument	Enter a repeat count for the next key-binding function. For details, see the section Entering Repeat Counts in this document.
newline	Terminate and return the current contents of the line, after appending a newline character. The newline character is normally '\n', but will be the first character of the key-sequence that invoked the newline action, if this happens to be a printable character. If the action was invoked by the '\n' newline character or the '\r' carriage return character, the line is appended to the history buffer.



KEY BINDING FUNCTION	DESCRIPTION
repeat-history	Return the line that is being edited, then arrange for the next most recent entry in the history buffer to be recalled. Repeatedly invoking this action causes successive historical input lines to be re-executed. Note that this action is equivalent to the 'Operate' action in ksh.
ring-bell	Ring the terminal bell, unless the bell has been silenced via the nobeep configuration option.
forward-copy-char	Copy the next character into the cut buffer (NB. use repeat counts to copy more than one).
backward-copy-char	Copy the previous character into the cut buffer.
forward-copy-word	Copy the next word into the cut buffer.
backward-copy-word	Copy the previous word into the cut buffer.
forward-find-char	Move the cursor to the next occurrence of the next character that you type.
backward-find-char	Move the cursor to the last occurrence of the next character that you type.
forward-to-char	Move the cursor to the character just before the next occurrence of the next character that the user types.
backward-to-char	Move the cursor to the character just after the last occurrence before the cursor of the next character that the user types.
repeat-find-char	Repeat the last backward-find-char, forward-find-char, backward-to-char or forward-to-char.
invert-refind-char	Repeat the last backward-find-char, forward-find-char, backward-to-char, or forward-to-char in the opposite direction.
delete-to-column	Delete the characters from the cursor up to the column that is specified by the repeat count.
delete-to-parenthesis	Delete the characters from the cursor up to and including the matching parenthesis, or next close parenthesis.
forward-delete-find	Delete the characters from the cursor up to and including the following occurrence of the next character typed.
backward-delete-find	Delete the characters from the cursor up to and including the preceding occurrence of the next character typed.
forward-delete-to	Delete the characters from the cursor up to, but not including, the following occurrence of the next character typed.
backward-delete-to	Delete the characters from the cursor up to, but not including, the preceding occurrence of the next character typed.
delete-refind	Repeat the last *-delete-find or *-delete-to action.
delete-invert-refind	Repeat the last *-delete-find or *-delete-to action, in the opposite direction.
copy-to-column	Copy the characters from the cursor up to the column that is specified by the repeat count, into the cut buffer.
copy-to-parenthesis	Copy the characters from the cursor up to and including the matching parenthesis, or next close parenthesis, into the cut buffer.
forward-copy-find	Copy the characters from the cursor up to and including the following occurrence of the next character typed, into the cut buffer.

KEY BINDING FUNCTION	DESCRIPTION
backward-copy-find	Copy the characters from the cursor up to and including the preceding occurrence of the next character typed, into the cut buffer.
forward-copy-to	Copy the characters from the cursor up to, but not including, the following occurrence of the next character types, into the cut buffer.
backward-copy-to	Copy the characters from the cursor up to, but not including, the preceding occurrence of the next character typed, into the cut buffer.
copy-refind	Repeat the last *-copy-find or *-copy-to action.
copy-invert-refind	Repeat the last *-copy-find or *-copy-to action, in the opposite direction.
vi-mode	Switch to VI mode from EMACS mode.
emacs-mode	Switch to EMACS mode from VI mode.
vi-insert	From VI command mode, switch to insert mode.
vi-overwrite	From VI command mode, switch to overwrite mode.
vi-insert-at-bol	From VI command mode, move the cursor to the start of the line and switch to insert mode.
vi-append-at-eol	From VI command mode, move the cursor to the end of the line and switch to append mode.
vi-append	From VI command mode, move the cursor one position right, and switch to insert mode.
vi-replace-char	From VI command mode, replace the character under the cursor with the next character entered.
vi-forward-change-char	From VI command mode, delete the next character then enter insert mode.
vi-backward-change-char	From VI command mode, delete the preceding character then enter insert mode.
vi-forward-change-word	From VI command mode, delete the next word then enter insert mode.
vi-backward-change-word	From VI command mode, delete the preceding word then enter insert mode.
vi-change-rest-of-line	From VI command mode, delete from the cursor to the end of the line, then enter insert mode.
vi-change-line	From VI command mode, delete the current line, then enter insert mode.
vi-change-to-bol	From VI command mode, delete all characters between the cursor and the beginning of the line, then enter insert mode.
vi-change-to-column	From VI command mode, delete the characters from the cursor up to the column that is specified by the repeat count, then enter insert mode.
vi-change-to-parenthesis	Delete the characters from the cursor up to and including the matching parenthesis, or next close parenthesis, then enter insert mode.
vi-forward-change-find	From VI command mode, delete the characters from the cursor up to and including the following occurrence of the next character typed, then enter insert mode.
vi-backward-change-find	From VI command mode, delete the characters from the cursor up to and including the preceding occurrence of the next character typed, then enter insert mode.

KEY BINDING FUNCTION	DESCRIPTION
vi-forward-change-to	From VI command mode, delete the characters from the cursor up to, but not including, the following occurrence of the next character typed, then enter insert mode.
vi-backward-change-to	From VI command mode, delete the characters from the cursor up to, but not including, the preceding occurrence of the next character typed, then enter insert mode.
vi-change-refind	Repeat the last vi-*-change-find or vi-*-change-to action.
vi-change-invert-refind	Repeat the last vi-*-change-find or vi-*-change-to action, in the opposite direction.
vi-undo-	In VI mode, undo the last editing operation.
vi-repeat-change	In VI command mode, repeat the last command that modified the line.

## Appendix B - Default Key Bindings in EMACS Mode

The following default key bindings are designed to mimic most of the bindings of the unix tcsh shell when in EMACS Send editing mode. This is the default editing mode of the CLI shell.

Note that a key sequence like ^A or C-a means hold the control-key down while pressing the letter A, and that where you see \E or M- in a binding, this represents the escape key or the Meta modifier key.

Also note that to the CLI, pressing the escape key before a key is equivalent to pressing the meta key at the same time as that key. Thus, the key sequence M-p can be typed in two ways, by pressing the escape key, followed by pressing p, or by pressing the Meta key at the same time as p.

Under UNIX, the terminal driver sets a number of special keys for certain functions. The CLI attempts to use the same key bindings to maintain consistency. If you have used the sty command to change these keys, then the default bindings should match.

SPECIAL KEY	FUNCTION
Ctrl-C	user-interrupt
Ctrl-\	abort
Ctrl-Z	suspend
Ctrl-Q	start-output
Ctrl-S	stop-output
Ctrl-V	literal-next

The cursor keys are referred to by name, as follows. This is necessary because different types of terminals generate different key sequences when their cursor keys are pressed.

CURSOR KEY	KEY SEQUENCE
right	cursor-right
left	cursor-left
up	up-history
down	down-history

The remaining bindings do not depend on the terminal settings.

KEY BINDING	DESCRIPTION
Crl-F	cursor-right
Crl-B	cursor-left
M-i	insert-mode
Crl-A	beginning-of-line
Crl-E	end-of-line
Crl-U	delete-line
Crl-K	kill-line
M-f	forward-word
M-b	backward-word
Crl-D	del-char-or-list-or-eof
Crl-H	backward-delete-char
Crl-?	backward-delete-char
M-d	forward-delete-word
M-^H	backward-delete-word
M-^?	backward-delete-word
M-u	upcase-word
M-l	downcase-word
M-c	capitalize-word
Crl-R	redisplay
Crl-L	clear-screen
Crl-T	transpose-chars
Crl-@	set-mark
Crl-X Crl-X	exchange-point-and-mark
Crl-W	kill-region
M-w	copy-region-as-kill
Crl-Y	yank
Crl-P	up-history
Crl-N	down-history
M-p	history-search-backward
M-n	history-search-forward
Crl-l	complete-word
Crl-X*	expand-filename
Crl-X Crl-F	read-from-file
Crl-X Crl-R	read-init-files
Crl-Xg	list-glob
Crl-Xh	list-history

KEY BINDING	DESCRIPTION
M-<	beginning-of-history
M->	end-of-history
\n	newline
\r	newline
M-o	repeat-history
M-Ctrl-V	vi-mode

M-0, M-1, ... M-9 -> digit-argument (see below)

Note that ^I is what the TAB key generates, and that ^@ can be generated not only by pressing the control key and the @ key simultaneously, but also by pressing the control key and the space bar at the same time.

## Appendix C - Default Key Bindings in VI Mode

The following default key bindings are designed to mimic the VI style of editing as closely as possible. This means that very few editing functions are provided in the initial character input mode; editing functions are provided by the VI command mode instead. VI command mode is entered whenever the escape character is pressed, or whenever a key-sequence that starts with a meta character is entered. In addition to mimicking VI, the CLI provides bindings for tab completion, wild-card expansion of file names, and historical line recall.

As previously mentioned in the EMACS section, note that a key sequence like ^A or C-a means hold the control-key down while pressing the letter A, and that where you see \E or M- in a binding, this represents the escape key or the Meta modifier key. Also note that to the CLI, pressing the escape key before a key is equivalent to pressing the meta key at the same time as that key. Thus, the key sequence M-p can be typed in two ways:

- by pressing the escape key, followed by pressing p.
- by pressing the Meta key at the same time as p.

Under UNIX, the terminal driver sets a number of special keys for certain functions. The CLI attempts to use the same key bindings to maintain consistency, binding them both in input mode and in command mode. If you have used the sty command to change these keys, then the default bindings should match.

KEY BINDING	DESCRIPTION
Ctrl-C	user-interrupt
Ctrl-\	abort
Ctrl-Z	suspend
Ctrl-Q	start-output
Ctrl-S	stop-output
Ctrl-V	literal-next
M- Ctrl-C	user-interrupt
M- Ctrl-\	abort
M- Ctrl-Z	suspend
M- Ctrl-Q	start-output
M- Ctrl-S	stop-output

Note that above, most of the bindings are defined twice; once as a raw control code like ^C, and then a second time as a meta character like M-^C. The former is the binding for VI input mode; whereas the latter is the binding for VI command mode.

Once in command mode, all key-sequences that the user types that does not explicitly start with an escape or a meta key, have their first key secretly converted to a meta character before the key sequence is looked up in the key binding table. Thus, once in command mode, when you type the letter i, for example, the CLI actually looks up the binding for M-i.

The cursor keys are referred to by name, as follows. This is necessary because different types of terminals generate different key sequences when their cursor keys are pressed.

CURSOR KEY	FUNCTION
right	cursor right
left	cursor left
up	up-history
down	down-history

The cursor keys normally generate a key sequence that starts with an escape character, so beware that using the arrow keys will put you into command mode (if you aren't already in command mode).

## Appendix D - Terminal-independent Key Bindings in VI Mode

The following are the terminal-independent key bindings for VI input mode:

KEY BINDING	FUNCTION
Ctrl-D	list-or-eof
Ctrl-G	list-glob
Ctrl-H	backward-delete-char
Ctrl-I	complete-word
\r	newline
\n	newline
Ctrl-L	clear-screen
Ctrl-N	down-history
Ctrl-P	up-history
Ctrl-R	redisplay
Ctrl-U	backward-kill-line
Ctrl-W	backward-delete-word
Ctrl-X*	expand-filename
Ctrl-X Ctrl-F	read-from-file
Ctrl-X Ctrl-R	read-init-files
Ctrl-?	backward-delete-char

## Appendix E - Key Bindings for VI Command Mode

The following are the key bindings that are defined in VI command mode, this being specified by all key bindings starting with a meta character. As mentioned above, once in command mode, the initial meta character is optional. For example, you might enter command mode by typing Esc, and then press h twice to move the cursor two positions to the left. Both h characters get quietly converted to M-h before being compared to the key-binding table; the first one because Escape followed by a character is always converted to the equivalent meta character, and the second, because command mode was already active.

KEY BINDING	FUNCTION
M-\	cursor-right (Meta-space)
M-\$	end-of-line
M-*	expand-filename
M+	down-history
M-	up-history
M-<	beginning-of-history
M->	end-of-history
M-Ctrl	beginning-of-line
M-;	repeat-find-char
M-,	invert-refind-char
M-	goto-column
M~	change-case
M.	vi-repeat-change
M-%	find-parenthesis
M-a	vi-append
M-A	vi-append-at-eol
M-b	backward-word
M-B	backward-word
M-C	vi-change-rest-of-line
M-cb	vi-backward-change-word
M-cB	vi-backward-change-word
M-cc	vi-change-line
M-ce	vi-forward-change-word
M-cE	vi-forward-change-word
M-cw	vi-forward-change-word
M-cW	vi-forward-change-word
M-cF	vi-backward-change-find
M-cf	vi-forward-change-find
M-cT	vi-backward-change-to
M-ct	vi-forward-change-to
M-c;	vi-change-refind

KEY BINDING	FUNCTION
M-c,	vi-change-invert-refind
M-ch	vi-backward-change-char
M-c Ctrl-H	vi-backward-change-char
M-c Ctrl-?	vi-backward-change-char
M-cl	vi-forward-change-char
M-c\	vi-forward-change-char (Meta-c-space)
M-c Ctrl	vi-change-to-bol
M-c0	vi-change-to-bol
M-c\$	vi-change-rest-of-line
M-c	vi-change-to-column
M-c%	vi-change-to-parenthesis
M-dh	backward-delete-char
M-d Ctrl-H	backward-delete-char
M-d Ctrl-?	backward-delete-char
M-dl	forward-delete-char
M-d	forward-delete-char (Meta-d-space)
M-dd	delete-line
M-db	backward-delete-word
M-dB	backward-delete-word
M-de	forward-delete-word
M-dE	forward-delete-word
M-dw	forward-delete-word
M-dW	forward-delete-word
M-dF	backward-delete-find
M-df	forward-delete-find
M-dT	backward-delete-to
M-dt	forward-delete-to
M-d;	delete-refind
M-d,	delete-invert-refind
M-d^	backward-kill-line
M-d0	backward-kill-line
M-d\$	kill-line
M-D	kill-line
M-d	delete-to-column
M-d%	delete-to-parenthesis
M-e	forward-word
M-E	forward-word
M-f	forward-find-char
M-F	backward-find-char

KEY BINDING	FUNCTION
M--	up-history
M-h	cursor-left
M-H	beginning-of-history
M-i	vi-insert
M-I	vi-insert-at-bol
M-j	down-history
M-J	history-search-forward
M-k	up-history
M-K	history-search-backward
M-l	cursor-right
M-L	end-of-history
M-n	history-re-search-forward
M-N	history-re-search-backward
M-p	append-yank
M-P	yank
M-r-	vi-replace-char
M-R	vi-overwrite
M-s	vi-forward-change-char
M-S	vi-change-line
M-t	forward-to-char
M-T	backward-to-char
M-u	vi-undo
M-w	forward-to-word
M-W	forward-to-word
M-x	forward-delete-char
M-X	backward-delete-char
M-yh	backward-copy-char
M-y Crl-H	backward-copy-char
M-y Crl-?	backward-copy-char
M-yl	forward-copy-char
M-y\	forward-copy-char (Meta-y-space)
M-ye	forward-copy-word
M-yE	forward-copy-word
M-yw	forward-copy-word
M-yW	forward-copy-word
M-yb	backward-copy-word
M-yB	backward-copy-word
M-yf	forward-copy-find
M-yF	backward-copy-find

KEY BINDING	FUNCTION
M-yt	forward-copy-to
M-yT	backward-copy-to
M-y;	copy-refind
M-y,	copy-invert-refind
M-y Crl	copy-to-bol
M-y0	copy-to-bol
M-y\$	copy-rest-of-line
M-yy	copy-line
M-Y	copy-line
M-y	copy-to-column
M-y%	copy-to-parenthesis
M-Crl-E	emacs-mode
M- Crl-H	cursor-left
M- Crl-?	cursor-left
M- Crl-L	clear-screen
M- Crl-N	down-history
M- Crl-P	up-history
M- Crl-R	redisplay
M- Crl-D	list-or-eof
M- Crl-I	complete-word
M-\r	newline
M-\n	newline
M- Crl-X Crl-R	read-init-files
M- Crl-Xh	list-history

M-0, M-1, ... M-9 -> digit-argument (see below)

Note that ^I is what the TAB key generates.

## Appendix F - Entering Repeat Counts

Many of the key binding functions described previously, take an optional count, typed in before the target key sequence. This is interpreted as a repeat count by most bindings. A notable exception is the goto-column binding, which interprets the count as a column number.

By default, you can specify this count argument by pressing the meta key while typing in the numeric count. This relies on the digit-argument action being bound to Meta-0, Meta-1, etc. Once any one of these bindings has been activated, you can optionally take your finger off the meta key to type in the rest of the number, since every numeric digit thereafter is treated as part of the number, unless it is preceded by the literal-next binding. As soon as a non-digit, or literal digit key is pressed, the repeat count is terminated and either causes the just typed character to be added to the line that many times, or causes the next key-binding function to be given that argument.

For example, in EMACS mode, typing:

M-12a

causes the letter 'a' to be added to the line 12 times, whereas typing

M-4M-c

capitalizes the next 4 words.

In VI command mode, the Meta modifier is automatically added to all characters typed in, so entering a count in VI command-mode just involves typing in the number, just as it does in the VI editor itself.

For example, in VI command mode, typing:

4w2x

moves the cursor four words to the right, then deletes two characters.

You can also bind digit-argument to other key sequences. If these end in a numeric digit, that digit gets appended to the current repeat count.

If these do not end in a numeric digit, a new repeat count is started with a value of zero, and can be completed by typing in the number, after releasing the key which triggered the digit-argument action.

## Appendix G - CLI Routing Commands and Equivalent UNIX Commands

The following table displays a list of CLI routing commands for and their equivalent UNIX command:

CLI COMMAND	EQUIVALENT UNIX COMMAND
route host add	route add -host <host address> gw <gateway>
route host remove	route del -host <host address> gw <gateway>
route network add	route add -net <net address> netmask <netmask> gw <gateway>
route network remove	route del <net address> netmask <netmask> gw <gateway>
show routes	route -n

## Appendix H - Output of show hsm stattree Command

The stattree utility returns the statistics gathered by the HSM module. Running the stattree utility displays a snapshot of all statistics currently available on the system.

**Note:** Many of the statistics relate to the internal communication between the system software and the HSM module and will hold little meaning for the product's Administrator.

Statistics are displayed in the form of a tree. At each node in the tree, either a set of statistics or a list of sub-categories is displayed. Each node has a label which consists of one of the following:

- a tag that identifies its contents.
- a number that corresponds to an instance in the category, for example, a module identifier or an internal client connection identifier. Times are listed in seconds. Other numbers are integers, which are either real number or counters. For example, a result –CmdCount 74897 means that there have been 74,897 commands submitted.

## Appendix I - Terms and Definitions for Output of show hsm stattree Command

The following table presents terms and their definitions for the returned output of running the command *show hsm stattree* on the CLI.

**Note:** The "hardserver" mentioned in some of the definitions below refers to an internal server process which relays information from the system software to the HSM module. The "clients" refer to system software which open connections to talk to the hardserver.

TERM	DEFINITION
ServerGlobals	Aggregate statistics for all commands processed by the hardserver since it started. The standard statistics (as described below) apply to the commands sent from the hardserver to modules. Commands processed internally by the server are not included here. The Uptime statistic gives the total running time of the server so far.
Connections	Statistics for connections between clients and the hardserver. There is one node for each currently active connection. Each node has an instance number that matches the log message generated by the server when that client connected. For example, when the hardserver message is "Information: New client #24 connected", the client's statistics appear under node #24 in the stattree output.
PerModule	Statistics kept by the modules. There is one instance node for each module, numbered using the standard module numbering. The statistics provided by each module depend on the module type and firmware version.
ModuleJobStats	Statistics for the commands (jobs) processed by a module. Appears under the Permodule category.
ModuleSCSIStats	Statistics from the module's SCSI interface. Appears only on SCSI-interfaced modules.
ModulePCISStats	Statistics from the module's PCI host interface. Appears only on PCIinterfaced modules.

TERM	DEFINITION
ModuleObjStats	Statistics for the module's Object Store, which contains keys and other resources. These statistics may be useful in debugging applications that 'leak' key handles, for example.
ModuleEnvStats	General statistics for the module's operating environment.
Uptime	The length of time (in seconds) since a module was last reset, the hardserver was started, or a client connection was made.
CmdCount	The total number of commands sent for processing from a client to the server, or from the server to a module. Contains the number of commands currently being processed.
ReplyCount	The total number of replies returned from server to client, or from module to server.
CmdBytes	The total length of all the command blocks sent for processing.
ReplyBytes	The total length of all the reply block received after completion.
CmdMarshalErrors	The number of times a command block was not understood when it was received. A non-zero value indicates either that the parties at each end of a connection have mismatched version numbers (for example, a more recent hardserver has sent a command to a less recent module that the module does not understand), or that the data transfer mechanism is faulty.
ReplyMarshalErrors	The number of times a reply was not understood when it was received. A non-zero value indicates either that the parties at each end of a connection have mismatched version numbers (for example, a more recent hardserver has sent a command to a less recent module that the module does not understand), or that the data transfer mechanism is faulty.
ClientCount	The number of client connections currently made to the server. This appears in the hardserver statistics.
MaxClients	The maximum number of client connections ever in use simultaneously to the hardserver. This gives an indication of the peak load experienced so far by the server.
DeviceFails	The number of times the hardserver has declared a device to have failed. The hardserver provides a diagnostic message when this occurs.
DeviceRestarts	The number of times the hardserver has attempted to restart a module after it has failed. The hardserver provides a "Notice" message when this occurs. The message does not indicate that the attempt was successful.
QOutstanding	The number of commands waiting for a module to become available on the specified client connection. When a module accepts a command from a client, this number decreases by 1 and DevOutstanding increases by 1. Commands that are processed purely by the server are never included in this count.
DevOutstanding	The number of commands sent by the specified client that are currently executing on one or more modules. When a module accepts a command from

TERM	DEFINITION
	a client, QOutstanding decreases by 1 and this number increases by 1. Commands that are processed purely by the server are never included in this count.
HostWriteCount	The number of write operations (used to submit new commands) that have been received by the module from the host machine. One write operation may contain more than one command block. The operation is most efficient when this is the case.
HostWriteErrors	The number of times write data from the host was rejected by the module. A non-zero value may indicate that data is being corrupted in transfer, or that the hardserver/device driver has got out of sync with the module's interface.
HostWriteBadData	Not currently reported by the module. Attempts to write bad data to the module are reflected in HostWriteErrors.
HostWriteOverruns	Not currently reported by the module. Write overruns are reflected in HostWriteErrors.
HostWriteNoMemory	Not currently reported by the module. Write failures due to lack of memory are reflected in HostWriteErrors.
HostReadCount	The number of times a read operation to the module was attempted. The module can defer a read if it has no replies at the time, but expects some to be available later. Typically the module reports HostReadCount in two places: the number under ModuleJobStats counts a deferred read twice, once when it is initially deferred, and once when it finally returns some data. The number under ModuleSCSIStats or ModulePCISStats counts this as one operation.
HostReadErrors	The number of times a read to a module failed because the parameters supplied with the read were incorrect. A non-zero value here typically indicates some problem with the host interface or device driver.
HostReadEmpty	The number of times a read from the module returned no data because there were no commands waiting for completion. In general, this only happens a small number of times during module startup or reset. It can also happen if PauseForNotifications is disabled.
HostReadUnderruns	Not currently reported by the module.
HostReadDeferred	The number of times a read operation to the module was suspended because it was waiting for more replies to become available. When the module is working at full capacity, a sizeable proportion of the total reads are likely to be deferred.
HostReadTerminated	The number of times a module had to cancel a read operation which has been deferred. This normally happens only if the clear key is pressed while the module is executing commands. Otherwise it might indicate a device driver, interface, or firmware problem.
PFNIssued	The number of PauseForNotifications commands accepted by the module from the hardserver. This normally increases at a rate of roughly one every two seconds. If the hardserver has this facility disabled (or a very early version), this will not occur.

TERM	DEFINITION
PFNRejected	The number of PauseForNotifications commands rejected by the module when received from the hardserver. This can happen during module startup or reset, but not in normal use. It indicates a hardserver bug or configuration problem.
PFNCompleted	The number of PauseForNotifications commands that have been completed by the module. Normally, this is one less than the PFNIssued figure, since there is normally one such command outstanding.
ANIssued	The number of Asynchronous Notification messages issued by the module to the hardserver. These messages indicate such things as the clear key being pressed and the module being reset. In later firmware revisions inserting or removing the smartcard or changing the non-volatile memory also generate asynchronous notifications.
ChanJobsIssued	The number of fast channel jobs issued to the module. The fast channel facility is unsupported on current modules. This number should always be zero.
ChanJobsCompleted	The number of fast channel jobs completed by the module. The fast channel facility is unsupported on current modules. This number should always be zero.
CPULoadPercent	The current processing load on the module, represented as a number between 0 and 100. Because a module typically contains a number of different types of processing resources (for example, main CPU, and RSA acceleration), this figure is hard to interpret precisely. In general, modules report 100% CPU load when all RSA processing capacity is occupied; when performing non-RSA tasks the main CPU or another resource (such as the random number generator) can be saturated without this statistic reaching 100%.
HostIRQs	On PCI modules, the total number of interrupts received from the host. On current modules, approximately equal to the total of HostReadCount and HostWriteCount.
ChanJobErrors	The number of low-level (principally data transport) errors encountered while processing 'fast channel' jobs. Should always be zero on current modules.
HostDebugIRQs	On PCI modules, the number of 'debug' interrupts received. This is used only for driver testing, and should be zero in any systemion environment.
HostUnhandledIRQs	On PCI modules, the number of unidentified interrupts from the host. If this is non-zero, a driver or PCI bus problem is likely.
HostReadReconnect	On PCI modules, the number of deferred reads that have now completed. This should be the same as HostReadDeferred, or one less if a read is currently deferred.
SCSIConnections	The number of times a SCSI module has been successfully selected as a target.
SCSICommands	The total number of SCSI commands (including Read, Write, and Inquiry) that have been issued to the module.
SCSIInquiries	The number of SCSI Inquiry commands that have been sent to the module. A host typically sends a SCSI Inquiry command searching the SCSI bus for

TERM	DEFINITION
	devices, for example, at startup.
SCSIDisconnects	The number of SCSI bus disconnects issued to the host by the module. A SCSI disconnect is issued whenever a read is deferred.
SCSIReconnects	The number of reconnections attempted by the module after a SCSI disconnect. This should be the same as SCSIDisconnects, or one less if the bus is currently disconnected.
SCSILUN0Use	The number of times SCSI LUN 0 was specified when the host connected to the module. A host is normally configured to use LUN 0 for Write commands.
SCSILUN1Use	The number of times SCSI LUN 1 was specified when the host connected to the module. Normally a host will be configured to use LUN 1 for Read commands, in order to allow writes to take place (on LUN 0) when a read is in operation. If this is zero, it is possible that the host has a SCSI interface which does not support multiple LUNs correctly. This will give performance problems - see the nFast troubleshooting guide.
SCSICmdErrors	The number of times an error was sent in response to a SCSI command by the module.
SCSIBusResets	The number of SCSI bus reset conditions issued by the host. If this occurs other than at start-up, it may indicate a serious error condition has been detected by the SCSI driver.
SCSICtrlErrors	The number of times the SCSI controller in the module reported various sorts of error. If non-zero, indicates either a SCSI cabling and termination problem, or a faulty module.
SCSITagQUse	The number of times SCSI Tagged Queueing was used when the host selected the module as target. If the host supports tagged queueing correctly, it does not need to use multiple LUNs for reads and writes. (The module offers both tagged queuing and multiple LUN support; it is up to the host to choose either or both of these as options when giving SCSI commands).
SCSIReconFailures	The number of times a SCSIReconnect operation ended in failure. If this is non-zero, SCSI bus cabling and termination could be at fault, or possibly the host's SCSI adapter or driver.
SCSIWideNeg	The number of times the SCSI 'Wide' option was negotiated between host and module. This is non-zero if both sides are Wide SCSI devices and are configured to allow wide data transfers.
SCSISyncNeg	The number of times Synchronous SCSI data transfer was negotiated between host and module. This is non-zero if both sides are Synchronous SCSI devices and are configured to allow synchronous data transfers.
ObjectsCreated	The number of times a new object has been put into the object store. This appears under the module's ModuleObjStats node.
ObjectsDestroyed	The number of items in the module's object store that have been deleted and their corresponding memory released.

TERM	DEFINITION
ObjectCount	The current number of objects (keys, logical tokens, buffers) in the object store. This is equal to ObjectsCreated minus ObjectsDestroyed. An 'empty' module contains a small number of objects that are always present.
CurrentTempC	The current temperature (in degrees Celsius) of the module main circuit board. First-generation modules do not have a temperature sensor and do not return temperature statistics.
MaxTempC	The maximum temperature recorded by the module's temperature sensor. This is stored in non-volatile memory, which is cleared only when the unit is initialized. First-generation modules do not have a temperature sensor and do not return temperature statistics.
MinTempC	The minimum temperature recorded by the module's temperature sensor. This is stored in non-volatile memory, which is cleared only when the unit is initialized. First-generation modules do not have a temperature sensor and do not return temperature statistics.
MemTotal	The total amount of RAM (both allocated and free) available to the module. This is the installed RAM size, minus various fixed overheads.
MemAllocKernel	The total amount of RAM allocated for kernel use in a module. This is principally used for the object store (keys, logical tokens, and similar) and for big-number buffers.
MemAllocUser	The total amount of RAM allocated for user-mode processes in the module.

## Appendix J - Constraints in CLI Reference

The following table displays constraints for the CLI:

ELEMENT	CONSTRAINT	CHAR COUNT
Enable Mode Password	Unique & case sensitive. No spaces allowed.	6-32
HSM Administrator Card Passphrase	Unique & case sensitive. Accepts all printable characters (i.e. #, \$, %, &, etc. are valid). Spaces are allowed, but leading and trailing white space is ignored.	6-128
Bootstrap export file name	Unique & case sensitive. May be from 2 to 32 alphanumeric characters, may include underscores, dashes but no spaces. Will accept one period ( . ) character.	2-32

## INDEX

- \$ character, 1
- % character, 1
- ACL Name, 12
- add a Group, 13
- add a host route, 52
- add a network route, 53
- add an ACL, 12
- add remote Syslog destination, 83
- allow User access to a Group, 16
- allows for initial system configuration, 28
- associate IP address to a host name, 46
- associate User with a Group, 13
- available key binding functions, 102
- capacity of routes supported, 53
- change Admin Card set for a Security World, 25
- change passphrase on an Admin Card, 23
- CLI commands, summary of, 7
- CLI key bindings, 102
- CLI modes, 3
- CLI start up screen, 2
- Command hierarchy, 6
- Command mode
  - prompt, 3
- configure all system logs, 34
- configure all system net interface settings, 43
- configure an NTP time server, 94
- configure an SMTP mail server, 96
- configure default gateway, 38
- configure DNS entries, 37
- configure Failover, 99
- configure inactive timeout for sessions, 95
- configure IP multicast for a specific service, 96
- configure management / device port traffic filtering, 39
- configure management network IP address, 40
- configure the system's name, 40
- configure WAN and LAN device interfaces, 41
- configures management / device port traffic filtering, 38
- configures the WAN IP address, 43
- default key binding in EMACS mode, 108
- default key binding in VI Command mode, 112
- default key binding in VI mode, 110
- determine route that packets take to network host, 50
- disable a remote Syslog destination, 85
- disable cryptographic HW acceleration, 21
- disable User, 16
- disassociate IP address from a host name, 46
- disassociate User from a Group, 14
- disassociate User from Group, 20
- display current log configuration, 73
- display current maximum number of listener threads allowed, 73
- display default AV log, 70
- display default AV updated log, 71
- display internal audit logs, 68, 69
- display internal system logs, 72
- display Security World id for this system, 63
- display the current failover configuration, 59
- EMACS mode
  - key bindings for, 102
- enable a remote Syslog destination, 86
- enable automatic backup of the config file, 87
- enable cryptographic HW acceleration, 22
- Enable mode
  - exiting from, 22
  - prompt, 4
- enable User, 18
- entering repeat counts for key bindings, 116
- erase an Admin Card, 24
- exit Enable mode, 22
- exit from any command prompt, 22
- export a bootstrap configuration file, 35
- flush DNS cache, 47
- host route
  - showing all, 74
- HSM
  - Admin Card passphrase, 23, 24, 25
- import a bootstrap configuration file, 36
- Initiates a configuration file backup immediately, 87
- interface where management listeners bind to, 39
- key pair to sign archived logs, 32
- listeners
  - showing all, 66
- look up IP address if a host via DNS, 48
- max amount of day to keep archived logs, 32
- modify User password, 18, 19
- network and host routes
  - showing all, 74
- ping network destination from system, 48, 51
- reboot system, 51
- remove a Group, 14
- remove a host route, 53
- remove a network route, 54
- remove a remote Syslog destination, 86
- remove an ACL, 12
- remove User, 19
- Rescue mode
  - prompt, 3

- reset SSL Certificate in product, 90
- reset system settings, 91
- resets system log for today, 35
- return to Command mode, 22
- routes
  - capacity supported, 53
- run a traceroute to a host, 100
- schedule policy synchronization for server
  - running in Standby mode, 100
- set a signing key for User, 20
- set dn alias for User, 17
- set email alias for User, 17
- set Enable mode password, 90
- set maximum number of seconds to wait for next
  - request from same client on same connection, 93
- set maximum size of listener pool, 94
- set the log level of internal logs, 33
- set the system management ports, 95
- set the system time, 97
- set the system time zone, 98
- set WAN and WAN physical characteristics, 41
- sets ftp parameters for backup of the config file, 88
- show advanced options for a specific User, 81
- show all ACLs, 56
- show all Groups, 62
- show all host routes, 74
- show all network and host routes, 74
- show all remote Syslog destinations, 78
- show all Tibco/Rendezvous registered services, 79
- show all Tibco/Rendezvous statistics for a
  - service, 79
- show all Users, 82
- show arp, 56
- show backup settings, 57
- show commands in Command mode, 4
- show commands in Enable mode, 4
- show commands in Rescue mode, 3
- show cryptographic acceleration settings, 58
- show cryptographic statistics, 58
- show email-config, 59
- show general system stats, 60
- show Groups associated with ACL, 55
- show Groups associated with User, 81
- show hsm enquiry, 62
- show hsm stattree, 64
- show network connections, 21, 57
- show network interface settings, 66
- show Network Policy listeners, 66
- show statistics and configuration on all
  - interfaces, 64
- show system date and time, 80
- show system IP tables, 74
- show system statistics, 77
- show system-wide configuration, 78
- show Users associated with Group, 61
- shutdown system, 83
- SNMP system name, location and contact
  - showing, 75
- static table lookup for host names
  - showing, 75
- synchronize system time via NTP, 48
- system
  - rebooting, 51
- system name, 40
- tab completion, 6
- terminal-independent key binding in VI mode, 111
- toggle FIPS mode, 60
- toggles FIPS mode, 92
- UNIX equivalent commands for CLI routing
  - commands, 116
- update Security World information on an system, 26
- upgrade system software, 36
- user name, 82
- user password, 15, 82
- verify passphrase on an Admin Card, 24
- VI mode
  - key bindings for, 102