

REDLINE NETWORKS WEB I/O ACCELERATOR

Command Reference



Copyright ©2003 Redline Networks, Inc.

The Redline Symbol is a registered trademark of Redline Networks, Inc. Redline Networks, Deploy and Enjoy, and TIX are trademarks of Redline Networks, Inc. All rights reserved. All other products and services mentioned in this publication are the trademarks, service marks, registered trademarks, or registered servicemarks of their respective owners.

Document Vers. 2.0.3

Redline Networks
675 Campbell Technology Parkway #150
Campbell, CA 95008

+1 408.369.3800

www.RedlineNetworks.com

Table of Contents

Table of Contents.....	i
Introduction.....	5
add.....	6
add route.....	7
arp.....	8
capture.....	9
clear admin.....	11
clear cluster N.....	12
clear cluster [N all] stats.....	13
clear cluster N listen ssl clientauth.....	14
clear dns server.....	15
clear forwarder N.....	16
clear forwarder [N all] stats.....	17
clear log.....	18
clear ntp server.....	19
clear redirector N.....	20
clear server.....	21
cls.....	22
configure.....	23
copy.....	24
delete.....	26
display.....	28
exit.....	29
export.....	30
gen.....	31
help.....	32
history.....	34
import.....	35
install.....	36
list.....	38
netstat.....	39
ping.....	40
quit.....	41
reboot.....	42
reload.....	43
reset config.....	44
rollback.....	45
set admin email.....	46
set admin interface.....	47
set admin log.....	48
set admin netmask.....	50
set admin snmp.....	51
set admin ssh.....	52
set admin syslog.....	53

set admin tcpdump	54
set admin telnet.....	55
set admin tftp	56
set admin tsdump	57
set admin upgrade.....	58
set admin vip	59
set admin webui.....	60
set boot.....	61
set clock.....	62
set cluster N busyredirect	63
set cluster N connbind.....	64
set cluster N convert302protocol.....	65
set cluster N dsr.....	66
set cluster N health	67
set cluster N listen.....	69
set cluster N listen ssl.....	70
set cluster N listen ssl clientauth.....	72
set cluster N sticky	74
set cluster N target	75
set cluster N target ssl.....	76
set cluster N weblog	78
set dns	79
set ether N	80
set forwarder N.....	81
set hostname.....	82
set ntp.....	83
set password.....	84
set redirector N	85
set redirector N listen.....	86
set redirector N listen ssl.....	87
set route	89
set server.....	90
set server customiplogheader.....	91
set server failover.....	92
set timezone	94
show admin	95
show admin email.....	97
show admin log	98
show admin snmp	99
show admin ssh.....	100
show admin syslog.....	101
show admin tcpdump	102
show admin telnet.....	103
show admin tftp.....	104
show admin tsdump	105
show admin upgrade.....	106
show admin webui.....	107
show arp	108

show audit	109
show boot	110
show clock.....	111
show cluster.....	112
show cluster N.....	113
show cluster N health status.....	116
show cluster N listen ssl.....	118
show cluster N listen ssl clientauth.....	120
show cluster [N all] stats	121
show cluster N target host [M all] stats.....	122
show cluster N target ssl.....	123
show commands.....	125
show config	126
show dashboard	129
show dns	131
show ether N	132
show file	133
show flash.....	134
show forwarder N	135
show forwarder [N all] stats.....	136
show forwarder N target host [M all] stats	137
show hostname	138
show log	139
show netstat.....	140
show ntp.....	141
show ntpq	142
show redirector N.....	143
show redirector N listen ssl.....	145
show route.....	147
show server.....	148
show server stats	149
show support.....	150
show tcpdump	151
show timezone.....	152
show ua.....	153
show version.....	154
show vmstat.....	155
tcpdump	156
tsdump	157
upgrade	158
vmstat.....	159
wall.....	160
who.....	161
write.....	162
Appendix A: Glossary.....	163
Appendix B: List of Events.....	166
Index.....	168

Introduction

This manual provides a complete command reference for the Web I/O Accelerator command set.

Commands are provided alphabetically in man page format, and each man page has the following sections:

- Purpose: reason for using the command
- Options: all options under this command
- Notes: Context for using this command and references to other commands that may be related.
- Examples: A couple of annotated examples

At the back of the manual are two appendices:

Appendix A: Glossary

Appendix B: List of Events

For more information on the context and usage of the command set, see the *Web I/O Accelerator Installation and Administration Guide*. The Web I/O Accelerator is also referred to as the “appliance” in this manual.

Tips for Help on Commands

The **help** command can be used to find syntax and a brief explanation of each command. See the description of help in this manual.

The **show commands** command provides a hierarchical list of all commands.

Typing a command with incomplete argument followed by the “tab” key provides a list of valid options for the command.

Additional Notes on Set Commands

Set commands are divided into two broad groups in general.

- ✓ One group of set commands only take effect after the explicit write operation.
- ✓ The other group of set commands will take effect immediately after the set command is entered. These are the commands that change the state of the appliance. Examples of these commands are:
 - Setting the appliance up or down
 - Setting the telnet service up or down
 - Setting the ssh service up or down
 - Setting the web user interface service up or down
 - Setting the SNMP service up or down
 - Setting the administrative password of the appliance

The command reference will indicate if the set command will take effect immediately.

Web Interface for Web I/O Accelerator

In addition to the command line interface, Redline Networks supports a web interface to the Web I/O Accelerator known as the Web User Interface (WebUI).

For more information on the WebUI, see the *Web I/O Accelerator Installation and Administration Guide*.

add

Purpose

Use **add** to create a new cluster, forwarder, redirector or a route.

Options

The following options may be entered after **add**.

cluster	Add a new cluster.
forwarder	Add a new forwarder.
redirector	Add a new redirector. This feature is only available on the E X Web I/O Accelerator product line.
route	To add a static route. See next page for details.

Notes

You need to add a cluster, forwarder or redirector to the Web I/O Accelerator configuration before configuring it.

Examples

add cluster

Add a new cluster.
 Response will be
 tx2% add cluster
 Created cluster 3
 (*) tx2%
 You can then set the attributes of the cluster.

add forwarder

Add a new forwarder.
 Response will be
 tx2% add forwarder
 Created forwarder 1
 (*) tx2%
 You can then set the attributes of the forwarder.

add redirector

Add a new redirector.
 Response will be
 tx2% add redirector
 Created redirector 1
 (*) tx2%
 You can then set the attributes of the redirector.

add route

Purpose

Use **add route** to add a static route.

Options

The format of the **add route** command is:

add route <destination> <gateway> <netmask>

<destination> is the IP network that you want to route to.

<gateway> is the IP address of the router you want to use.

<netmask> is an optional parameter. The default is set to 255.255.255.255, which represents a host route.

Notes

None.

Examples

```
add route 66.12.13.5 192.168.0.10
```

Add a static route to the host 66.12.13.5 through the gateway 192.168.0.10.

```
add route 66.12.13.0 192.168.0.10  
255.255.255.0
```

Add a static route to the network 66.12.13.0 through the gateway 192.168.0.10.

arp

Purpose

Use **arp** to display the ARP table.

Options

None.

Notes

None.

Examples

arp

Display the current ARP table.

E.g. of output:

```
gateway.company.com (192.168.0.1) at  
0:f0:e7:85:ac:d0 [ethernet]  
mail.company.com (192.168.0.2) at 0:e0:a7:ee:e0:2e  
[ethernet]  
brown.company.com (192.168.0.20) at  
0:f0:e7:85:a8:2c [ethernet]  
? (192.168.33.2) at 0:f0:e7:25:d6:26 [ethernet]
```

capture

Purpose

Use **capture** to capture data entered on the screen into a file on the Web I/O Accelerator.

Options

The following options may be entered after **capture**

file	<filename>	To capture a SSL key or certificate from the terminal into the Web I/O Accelerator.
------	------------	---

Notes

This operation is currently used for capturing SSL keys and certificates only. The content entered on the screen will be captured into the file specified. To finish copying the file, it must end with a "." on a blank line.

Examples

capture file my_key Start capturing a SSL Key from the terminal and name it "my_key".

You will paste the content of the file and end the file with a "." on a blank line. Example output is:

```
2200% capture file my_key
Enter file. End with . on a blank line.
-----BEGIN CERTIFICATE-----
MIIDejCCAuOgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBizELMAkGA
EjAQBgNVBAGTCURFTU8gT05MWTESMBAGA1UEBxMJREVNTyBPT
EwIERU1PIE9OTFkxEjAQBgNVBAsTCURFTU8gT05MWTESMBAGA1
TkxZMRgwFgYJKoZIhvcNAQkBFglERU1PIE9OTFkwHhcNMDIwMzA1
MDIwMzA2MjM1MzAxWjCBizELMAkGA1UEBhMCWFgxEjAQBgNVBA
WTESMBAGA1UEBxMJREVNTyBPTkxZMRlWEAYDVQQKEwIERU1P
BAsTCURFTU8gT05MWTESMBAGA1UEAxMJREVNTyBPTkxZMRgw
FglERU1PIE9OTFkwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoG
HkubHFrpC1tub2CEANVBJSXfk/n8rle/JIXCm2Gv1Q85Fk6pW8P597r
gQE/1xBaSEwJv4GuVPtfcGyG8PJmAKoO0d/OkYsYHIZJG7aIMmJB1
mFlgT9EJ7nZAYE/Rb1p6dmJBNZYtOMaXAgMBAAGjgeswgegWHQY
MnFJOsgvF3B4HuaX9fBBDk9xMIG4BgNVHSMGgbAwga2AFCCeMn
9fBBDk9xoYGRpIGOMIGLMQswCQYDVQQGEwJYWDESMBAGA1U
MRlWEAYDVQQHEwIERU1PIE9OTFkxEjAQBgNVBAoTCURFTU8gT
CxMJREVNTyBPTkxZMRlWEAYDVQQDEwIERU1PIE9OTFkxGDAW
CURFTU8gT05MWYIBADAMBgNVHRMEBTADAQH/MA0GCSqGSIsb
L8dbydfkNbydH3wHcF5uUuLG5rajGzput7GrQEjKUmKEB+bl/VIRbPQ
W0FOiR7MsY64y5cbpMoGrfZ2qNgNKF+i6WLimTfh4+1tKiCMnhTRP
```

hivbsYqWBdOFwrkqAUapuUDwctaAxV2pwJos47IO

2200% list file
democert
demokey
my_key

clear admin

Purpose

Use **clear admin** to clear settings of tftp, syslog, email, interface, tsdump, tcpdump and logging.

Options

The following options may be entered after **clear admin**.

email	defaulmailto	Clear default mail to address setting.
interface	ether	Clear admin interface setting.
log	email	Clear log level setting for logging via email.
	mailto1	Clear mailto1 setting.
	mailto2	Clear mailto2 setting.
	memory	Clear log level setting for memory logging.
syslog	syslog	Clear log level setting for logging to syslog.
	host1	Clear syslog host1 setting.
	host2	Clear syslog host2 setting.
	facility	Clear syslog facility setting.
tcpdump	mailto1 or mailto2	Clear mailto1 or mail2 settings.
tftp	server	Clear tftp server setting.
tsdump	mailto1 or mailto2	Clear mailto1 or mail2 settings.

Notes

Clearing the admin interface also clears the admin VIP.

Examples

clear admin tftp server	Clear tftp server setting.
clear admin syslog host1	Clear host1 in syslog setting.
clear admin tcpdump mailto1	Clear mailto1in TCP dump setting.
clear admin syslog facility	Clear syslog facility setting.

clear cluster N

Purpose

Use **clear cluster N** to clear cluster options, or the certfiles, passwords, keyfiles associated with SSL traffic of a listener or target.

Options

The following options may be entered after **clear cluster N**.

health	string		Clear the health check string.
	size		Clear the size of return page.
listen	ssl	certfile	Clear cluster listener SSL certfile.
		keyfile	Clear cluster listener SSL keyfile.
		keypass	Clear cluster listener SSL keypass (password).
		clientauth	Clear SSL client authentication parameters. See clear cluster N listen ssl clientauth section for details. This feature is only available on the E X Web I/O Accelerator product line.
target	host	<ip address:port>	Clear the specific target host.
		all	Clear all the target hosts.
	ssl	certfile	Clear cluster target SSL certfile.
		keyfile	Clear cluster target SSL keyfile.
		keypass	Clear cluster target SSL keypass (password).

Notes

None.

Examples

clear cluster 1 listen ssl certfile

Clear the certfile for listen traffic on the cluster.

clear cluster 1 health string

Clears the string to check for the content health checking.

clear cluster [N | all] stats

Purpose

Use **clear cluster [N | all] stats** to clear all statistics for a specific cluster or all clusters.

Options

None.

Notes

When cluster stats are cleared, all physical target stats are also cleared.

Examples

clear cluster 1 stats

Clear all statistics for cluster 1.

clear cluster all stats

Clear all statistics for all clusters.

clear cluster N listen ssl clientauth

Purpose

Use **clear cluster N listen ssl clientauth** to clear out CA cert file, CA CRL file and CA trusted certificate. This feature is only available on the E|X Web I/O Accelerator product line.

Options

The following options may be entered after **clear cluster N**.

cacertfile	Clear the value of the CA certificate file making this field empty.
cacrflfile	Clear the value of the CA CRL file making this field empty.
catrustfile	Clear the value of the CA trusted file making this field empty.

Notes

None.

Examples

clear cluster 1 listen ssl certfile Clear the certfile for listen traffic on the cluster.

clear dns server

Purpose

Use **clear dns server** to clear a specific DNS server or all DNS server settings.

Options

N	Clears a specific DNS server, N.
all	Clears all DNS servers.

Notes

None.

Examples

clear dns server 1
clear dns server all

Clear DNS server 1.
Clear all DNS servers.

clear forwarder N

Purpose

Use **clear forwarder N** to clear entire forwarder or cluster options.

Options

The following options may be entered after **clear forwarder N**.

target host <ipaddress:port>	Clear target server settings for a host.
target host all	Clear all target server settings in the forwarder

Notes

None.

Examples

clear forwarder 1 target host 10.10.10.10:80 Clear all target settings for host 10.10.10.10.

clear forwarder 1 target host all Clear all target all servers' settings.

clear forwarder [N | all] stats

Purpose

Use **clear forwarder [N | all] stats** to clear all statistics for a specific forwarder or all forwarders.

Options

None.

Notes

When forwarder stats are cleared, all physical target stats are also cleared.

Examples

clear forwarder 1 stats

Clear all statistics for forwarder 1.

clear forwarder all stats

Clear all statistics for all forwarders.

clear log

Purpose

Use **clear log** to clear all memory log entries on the Web I/O Accelerator.

Options

None.

Notes

This command clears log entries in memory.

Examples

clear log	Clear all log entries
-----------	-----------------------

clear ntp server

Purpose

Use **clear ntp server** to clear a specific NTP server or all NTP servers.

Options

N	Clears a specific NTP server, N.
all	Clears all NTP servers.

Notes

None.

Examples

clear ntp server 1

Clear NTP server 1.

clear ntp server all

Clear all NTP servers.

clear redirector N

Purpose

Use **clear redirector N** to clear out redirector options, or the certfiles, passwords, keyfiles associated with SSL traffic of a redirector. This feature is only available on the E|X Web I/O Accelerator product line.

Options

The following options may be entered after **clear cluster N**.

customURL			Clear the URL for redirecting.
listen	<blank>		Clear redirector listen settings
	ssl	certfile	Clear redirector listen SSL certfile.
		keyfile	Clear redirector listen SSL keyfile.
		keypass	Clear redirector listen SSL keypass (password).

Notes

None.

Examples

clear redirector 1 listen ssl certfile Clear the certfile for listen traffic on the redirector.

clear redirector 1 customURL Clears the custom URL string for the redirector.

clear server

Purpose

Use **clear server** to clear server statistics or a custom IP log header.

Options

The following options may be entered after **clear server**.

customiplogheader	Clear custom IP log header.
stats	Clear all server statistics.

Notes

None.

Examples

clear server stats	Clear all server statistics, including I/O, HTTP and SSL statistics of the server.
clear server customiplogheader	Clear a servers custom IP log header

copy

Purpose

Use **copy** to copy configurations, files and captured tcpdump information.

Options

The following options may be entered after **copy**

config	<src> <dst>	<p>Use copy config to perform the following operations:</p> <ol style="list-style-type: none"> 1. To copy configurations from the Web I/O Accelerator to a remote location or from a remote location to the Web I/O Accelerator via TFTP. 2. To display the CLI commands needed to re-create the configurations on the screen 3. To reset the configurations to factory defaults <p>Format of <src> and <dst> is:</p> <ol style="list-style-type: none"> 1. Remote location: tftp://tftp_server/filename 2. Local location: <ul style="list-style-type: none"> memory: configurations currently on the memory active: configurations currently on flash terminal: the CLI screen factory: the factory default configuration block local filename: to create a named configuration locally. <p>Either <src> or <dst> must be memory</p>
file	<src> <dst>	<p>User copy file to perform the following operations:</p> <ol style="list-style-type: none"> 1. To display the content of the file on the terminal 2. To capture a SSL key or certificate as a file onto the Web I/O Accelerator <p>Format of <src> and <dst> is:</p> <ol style="list-style-type: none"> 1. Local filename 2. terminal: the CLI screen <p>Either <src> or <dst> must be terminal.</p>
tcpdump		<p>To send the tcpdump information via email or tftp as configured in the tcpdump destination using the command:</p> <pre>set admin tcpdump [tftp smtp]</pre>

Notes

- 1) Copying configurations from a remote location is equivalent to importing a configuration. This can also be performed by the following command:

- import config (see import config)
- 2) Copying configurations to a remote location is equivalent to exporting a configuration. This can also be performed by the following command:
export config (see export command)
 - 3) To display the CLI commands to re-create the configurations can also be performed by the following command:
display config (see display command)
 - 4) To reset all configurations back to factory default can also be performed by the following command:
reset config (see reset config command)
 - 5) To display the content of a file can also be performed by the following command:
display file (see display command)
 - 6) Capturing a SSL key or certificate onto a file on the Web I/O Accelerator can also be performed by the following command:
capture file (see capture file command)

Examples

copy tcpdump	Copy previously captured tcpdump information to a remote location via configured destinations, e.g. tftp or email.
copy config memory tftp://mytftpserver.domain.com/tx_config	To export TX configuration to an external host named mytftpserver.domain.com using the filename tx_config.
copy config tftp://mytftpserver.domain.com/tx_config memory	To import a TX configuration from an external host named mytftpserver.domain.com using the filename tx_config.
copy config memory terminal	Dump all commands needed to re-create the configurations onto the screen
copy config factory memory	Reset the Web I/O Accelerator to factory settings.
copy file terminal mycert	Capture information that you provide on the screen to a file called "mycert". Example is to import the SSL certificate or key into the Web I/O Accelerator.
copy file democert terminal	Display the content of the file "democert" on the screen.

delete

Purpose

Use **delete** to delete clusters, forwarders, redirectors, routes, configurations and files.

Options

The following options may be entered after **delete**.

cluster	<cluster number>	To delete a specific cluster
	all	To delete all clusters
config	<saved_config>	Delete a configuration saved previously.
file	<filename>	To delete a file. To show the list of files that can be removed, use "list file".
forwarder	<forwarder number>	To delete a specific forwarder
	all	To delete all forwarders
redirector	<redirector number>	To delete a specific redirector. This feature is only available on the E X Web I/O Accelerator product line.
route	<route number>	Delete a route. Show route provides the route number.

Notes

None.

Examples

delete cluster all	Delete all clusters from the Web I/O Accelerator configuration.
delete cluster 2	Delete cluster 2
delete forwarder all	Delete all forwarders from the Web I/O Accelerator configuration.
delete file my_cert	Delete the file called "my_cert"
delete redirector 1	Delete redirector 1
delete route 1	Output of show route is: se2200% show route Default route: 192.168.0.1 [1] 66.12.13.5 192.168.0.10

[2] 66.12.14.0 192.168.0.11 255.255.255.0

The result of this command will delete the route to the host 66.12.13.5.

delete config my_config

Delete a previously stored named configuration that has the name "my_config" on the Web I/O Accelerator.

display

Purpose

Use **display** to display the CLI commands to create the configuration and the content of a file.

Options

The following options may be entered after **display**

config		Display the CLI commands to re-create the configuration.
file	<filename>	To display the content of a file.

Notes

None.

Examples

display config

To display the list of CLI commands needed to re-create the configurations on the terminal.

display file my_ssl_key

To display the content of the SSL key name "my_ssl_key".

export

Purpose

Use **export**, to export configurations from the Web I/O Accelerator to a remote server via TFTP.

Options

The following options may be entered after **export**

config	<dest>	To export a configuration from the Web I/O Accelerator to a remote location via TFTP. Format of <dst> is: tftp://tftp_server/filename Double quotes must be used if the filename has spaces. E.g. "tftp://tftp_server/tx config"
--------	--------	--

Notes

The export command exports the actual set commands from the CLI to recreate the configuration. The export operation does not export the following information:

1. "set" commands that take effect immediately. These include the state of the various services:
 - a. Server
 - b. SSH service
 - c. Telnet service
 - d. SNMP service
 - e. Web User Interface service
2. Administrative password.
3. All SSL private keys, certificates and self-signed certificates.

Examples

```
export config tftp://192.168.40.228/tx_config
```

To export the configuration from the Web I/O Accelerator to the tftp server with an IP address 192.168.40.228 and name the configuration file "tx_config".

gen

Purpose

Use **gen** to generate an SSL private key, an SSL certificate signing request or an SSL self-signed certificate.

Options

The following options may be entered after **gen**.

csr	<key file> <csr file>	Generate a SSL certificate signing request. Input to the command is a 1024-bit RSA private key file and out is a CSR file. <key_file> and <csr_file> are optional parameters and will be prompted, if not provided.
key	<key file>	Generate a 1024-bit RSA SSL private key.
ssc	<key file> <ssc file>	Generate a SSL self-signed certificate. Input to the command is a 1024-bit RSA private key file and out is a CSR file.;

Notes

You will be prompted for such information as country, state, department etc. for the certificate.

See the *Setting up T[X] (or E[X]) for SSL Traffic* chapter of the *Installation and Administration Guide*.

Examples

```
gen ssc my_key my_ssc
```

Generate an SSL self-signed certificate.

The input is the SSL private key, "my_key" and the output is an SSL self-signed certificate, "my_ssc".

```
gen csr my_key my_csr
```

Generate an SSL certificate signing request.

The input is the SSL private key, "my_key" and the output is an SSL certificate signing request, "my_csr".

```
gen key
```

Generate an SSL private key

help

Purpose

Use **help** to display a help message.

Options

None.

Notes

If you just type help you get a list of the top level commands high level commands:

add	Consult your Administration Guide.
capture	Consult your Administration Guide.
clear	show the Address Resolution Protocol tables
cls	clear the screen
configure	re-run the configuration walkthrough
copy	show network statistics
delete	show memory statistics
display	show a traceroute to a host
exit	exit
export	Consult your Administration Guide.
gen	Consult your Administration Guide.
help	display a help message
history	display the command history
import	Consult your Administration Guide.
list	Consult your Administration Guide.
ping	ping another network node
quit	exit
reboot	reboot
reload	generate a Self-Signed Cert
reset	Consult your Administration Guide.
rollback	roll back to a previous firmware edition
set	Consult your Administration Guide.
show	generate a Certificate Signing Request
tcpdump	generate a tcpdump
tsdump	generate a Technical Service dump
upgrade	upgrade the firmware
who	display a list of other people logged in
write	make the configuration in memory the active
one	

If you then type `help` in conjunction with a command that has a subcommand, you get a list of all subcommands; for instance,

```
help set
```

gives the following output:

```
admin          Consult your Administration Guide.
clock          set the system date and time
cluster        Consult your Administration Guide.
dns            Consult your Administration Guide.
ether          Consult your Administration Guide.
forwarder      Consult your Administration Guide.
hostname       set the hostname
ntp            Consult your Administration Guide.
password       change the login password
route          Consult your Administration Guide.
server         Consult your Administration Guide.
timezone       set the timezone
```

Examples

```
help set
```

Displays a list of all the `set` subcommands.

history

Purpose

Use **history** to display the command history.

Options

None.

Notes

None.

Examples

history	Gives command history.
---------	------------------------

import

Purpose

Use **import** to import configurations to the Web I/O Accelerator via TFTP.

Options

The following options may be entered after **import**

config	<src>	<p>To import a configuration to the Web I/O Accelerator from a remote location via TFTP. Format of <src> is:</p> <p style="text-align: center;">tftp://tftp_server/filename</p> <p>Double quotes must be used if the filename has spaces. E.g.</p> <p style="text-align: center;">"tftp://tftp_server/tx config"</p>
--------	-------	--

Notes

You must perform the write operation to have the changes take effect. It is important to note that the SSL keys and certificates are not exported during an export operation. When importing a configuration, you must make sure that the required SSL keys and certificates are already installed on the Web I/O Accelerator.

Examples

```
import config tftp://192.168.40.228/tx_config
write
```

To import a configuration named "tx_config" from the tftp server with an IP address 192.168.40.228.

install

Purpose

Use **install** to download new firmware to a non-active partition.

Options

None.

Notes

Another method to download pac file is to use the “upgrade” procedure. Use the “install” procedure only if you would like to preserve the current version of the firmware. The “install” procedure will download the firmware to a non-active partition. Make sure that the correct pac file is used as the pac file for “install” is different from the one for “upgrade”. Note that the pac file for “install” operation is approximately 10M bytes where the pac file for “upgrade” is approximately 3M bytes.

The tftp server and the filename to install from must be set

- set admin tftp server <tftp server>
- set admin upgrade <pac file filename>.

If your active partition is currently partition 1, you would probably want to **install** the new firmware into partition 2. This lets you test the new firmware and reload the original firmware stored in partition 1, if needed. The *rollback* operation will only be applicable for the existing **upgrade** operation and not the **install** operation.

The **install** operation will preserve the following information:

- a) SSH keys
- b) User names and passwords for the administrative users
- c) Network settings, including static routes

The **install** operation will also allow an option to preserve the following configuration settings. On first boot to a new partition, you can choose to import these configuration settings.

- a) User names and passwords for all users.
- b) Network settings, including static routes, including admin interface bindings.
- c) SSL keys and certificates.
- d) Current (active) server configuration.
- e) State of the services, which includes:
 - Server status
 - Telnet
 - SSH
 - SNMP
 - Web UI

After the **import** operation, you will be prompted to save the configurations using the **write** operation. Admin services (e.g. server, WebUI, SSH, ...etc.) will also be prompted to start accordingly, based on the state before the **install** operation was done.

Examples

install

To install new firmware to a non-active partition.

list

Purpose

Use **list** to display a list of user files on the Web I/O Accelerator.

Options

The following options may be entered after **list**.

config	To display the list of saved configurations on the Web I/O Accelerator
file	To display the list of user files stored on the Web I/O Accelerator.

Notes

Examples

list file

Sample output is:
2200% list file

democert
demokey

list config

Sample output is:
2200% list config
Factory
my_config
abc

netstat

Purpose

Use **netstat** to show network statistics. These statistics include active internet connection information: send and receive queues, local and foreign addresses, and states.

Options

The following options may be entered after **netstat**

blank	Show network statistics. Default is with the <code>-a</code> option.
N	Where N is an integer. Show network statistics every N seconds.
-a	Show active connections
-s	Show network statistics
-r	Show the routing tables
-l	Show the state of all network interfaces. This has the same effect as the option <code>-a</code> .

Notes

This command is the same as “show netstat”. Sample **netstat** output is in the following format

```
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         (state)
tcp4      0      20 10.0.22.50.22          192.168.0.234.1094     ESTABLISHED
tcp4      0      0 *.8090                 *.*                     LISTEN
tcp4      0      0 *.23                    *.*                     LISTEN
tcp4      0      0 *.22                    *.*                     LISTEN
```

Examples

```
netstat          Show network statistics
netstat 1        Show network statistics every second. Use ^C (control C) to stop.
netstat -r      Show the routing table. Sample out:
```

```
tx2200% show netstat -r
Routing tables
```

```
Internet:
Destination      Gateway           Flags    Refs    Use Netif    Expire
default          192.168.0.1      UGSc    4        0 ether0
12.12.1.23       12.12.12.12     UGHS    0        0 ether0
192.168.0/16     link#1           UC       2        0 ether0
192.168.0.1      0:d0:b7:85:bc:a0 UHLW    3        0 ether0    812
192.168.40.169/32 link#1           UC       0        0 ether0
192.168.40.188/32 link#1           UC       0        0 ether0
192.168.40.228  8:0:46:4d:60:40 UHLW    1       310 ether0   1125
```

ping

Purpose

Use **ping** to ping another network node.

Options

The following options may be entered after **ping**.

<IP Address> | <DNS name>

Notes

This is typically used in troubleshooting and in installation. Common tasks are to ping the target host or the default gateway to verify installation.

Examples

ping 191.68.44.32

Ping another network node.

ping foobar.com

Ping via DNS name. Make sure that DNS resolution is set up on the Web I/O Accelerator.

reset config

Purpose

Use **reset config** to reset the Web I/O Accelerator to factory settings.

Options

None.

Notes

You must perform the write operation to have the changes take effect.

This command will bring the Web I/O Accelerator back to the default settings from the factory. Connectivity will be lost, if you are connected to the appliance remotely. You will need to set the appropriate network settings before the write operation, if you want to have remote access after the **reset config** and **write** operations.

A warning message as shown below will be displayed. You must confirm to perform the reset config operation.

Executing this command will reset all configurations, including network settings. If you continue, you will need to connect to the console (serial) port to access the box again.

Are you sure you want to continue (y/n)? [n]

Examples

```
reset config          Reset all settings to factory defaults
write
```


set admin email

Purpose

Use **set admin email** to set parameters for the email operation.

Options

The following options may be entered after **set admin email**.

defaultmailto	<default address>	Default address to be used when the other email addresses are not set. Specific email address for log, tcpdump and tsdump, if set will overwrite the default email address.
from	<from address>	The sender address
server	<smtp server>	IP address or hostname for the SMTP server.

Notes

The settings made by this command will take effect after a write operation.

Examples

set admin email from admin@company.com	Set the from email address to be admin@company.com
set admin email defaultmailto support@company.com	Set the default email address to be support@company.com.
set admin email server 192.168.1.2	Set the email server to be 192.168.1.2.

set admin interface

Purpose

Use **set admin interface** to set parameters for the admin interface.

Options

The following options may be entered after **set admin interface**.

all		Use all interfaces, ether 1 and ether 0 for administration traffic.
ether	<0 1>	Set which ethernet interface to use for administration traffic.

Notes

The settings made by this command will take effect after a write operation.

Examples

set admin interface ether 1

Set ether 1 to be the administration interface.

set admin log

Purpose

Use **set admin log** to set parameters for logging to various destinations, including the memory of the Web I/O Accelerator, email and syslog.

Options

The following options may be entered after **set admin log**.

email	< EMERG ALERT >	Set logging via email at one of the log levels. Send a log message to the configured email address(s) when an event greater than or equal to the selected level occurs. The severity levels are in the following order: EMERG – highest level ALERT
enabled		Enable logging function
disabled		Disable logging function
mailto1	<first email address>	First email address that the log should be sent to.
mailto2	<second email address>	Second email address that the log should be sent to.
memory	< EMERG ALERT >	Set logging to memory on the Web I/O Accelerator at one of the log levels. Default is set to ALERT. Send a log message to the Web I/O Accelerator memory when an event greater than or equal to the selected level occurs. The severity levels are in the following order: EMERG – highest level ALERT
syslog	< EMERG ALERT >	Set logging to a syslog host at one of the log levels. Send a log message to the configured syslog host(s) when an event greater than or equal to the selected level occurs. The severity levels are in the following order: EMERG – highest level ALERT

Notes

The settings made by this command will take effect after a write operation.

Examples

set admin log email ALERT

Only send events of ALERT or higher level via email.

set admin log syslog EMERG

Send all events to the syslog host configured.

set admin log memory EMERG

Send all events to the to the screen.

set admin netmask

Purpose

Use **set admin netmask** to set the netmask for the administrative IP address.

Options

None.

Notes

The settings made by this command will take effect after a write operation. The netmask value is an optional parameter. The default value is 255.255.255.255.

Examples

```
set admin netmask 255.255.255.255      Set netmask for the administrative address
```

set admin snmp

Purpose

Use **set admin snmp** to set options relating to SNMP connections.

Options

The following options may be entered after **set admin snmp**.

community	name	<name>	Set the SNMP read-only community name.
	ip	<IP address>	Set the IP to allow SNMP connections from.
	netmask	<IP netmask>	Set the netmask to allow SNMP connections from.
contact		<contact>	Set the SNMP system contact (MIB II).
down			Turn off SNMP
location		<location>	Set the SNMP system location (MIB II).
up			Turn on SNMP

Notes

Setting the SNMP service up or down will take effect immediately after the command is executed. The rest of the settings in this section will only take effect after a write operation. Only supports Read for SNMP operations.

Examples

```
set admin snmp location snmp-rack1      Set SNMP system location
set admin snmp community ip 19.9.9.2   Set IP to allow SNMP connections from the specified
                                         IP address.
```

set admin ssh

Purpose

Use **set admin ssh** to turn SSH (secure shell) access on and off.

Options

The following options may be entered after **set admin ssh**.

down	Turn off SSH access
up	Turn on SSH access

Notes

This command will take effect immediately after it is executed.

Examples

set admin ssh up	Allow SSH access
set admin ssh down	Disallow SSH access

set admin syslog

Purpose

Use **set admin syslog** to set up one or two syslog hosts for logging.

Options

The following options may be entered after **set admin syslog**.

facility	<LOG_USER LOG_LOCAL0 LOG_LOCAL1 LOG_LOCAL2 LOG_LOCAL3 LOG_LOCAL4 LOG_LOCAL5 LOG_LOCAL6 LOG_LOCAL7>	syslog facility. Default is LOG_USER.
host1	<ip address or hostname>	First syslog host
host2	<ip address or hostname>	Second syslog host

Notes

The settings made by this command will take effect after a write operation.

Examples

- | | |
|--------------------------------------|--|
| set admin syslog host1 192168.0.1 | Set the first syslog host to be 192.168.0.1. |
| set admin syslog host2 192168.0.2 | Set the second syslog host to be 192.168.0.1. |
| set admin syslog facility LOG_LOCAL0 | Set the syslog facility to be LOG_LOCAL0 that the Web I/O Accelerator will log to the syslog host. |

set admin tcpdump

Purpose

Use **set admin tcpdump** to set options relating to tcpdump.

Options

The following options may be entered after **set admin tcpdump**.

disabled	Disable tcpdump function	
filename	<tcpdump filename>	Set the remote filename for the tcpdump.
mailto1	<first email address>	First email address that the tcpdump should be sent to.
mailto2	<second email address>	Second email address that the tcpdump should be sent to.
smtp	Send tcpdump information via pre-configured email addresses. Either smtp or tftp can be set but not both at the same time.	
tftp	Send tcpdump information via the pre-configured tftp host. Either smtp or tftp can be set but not both at the same time.	

Notes

The settings made by this command will take effect after a write operation.

Before running the **tcpdump** command, the following parameters must be set:

- ✓ Filename for storing the tcpdump, if you are using tftp
- ✓ Either an email address or a tftp server

Examples

set admin tcpdump disabled	Disable the tcpdump function
set admin tcpdump smtp	Use the pre-configured email addresses to send the tcpdump information
set admin tcpdump tftp	Use the pre-configured tftp host to upload the tcpdump information
set admin tcpdump filename tx_tcpdump	Set the filename to capture the TCP dump to be tx_tcpdump.

set admin telnet

Purpose

Use **set admin telnet** to turn telnet access on and off.

Options

The following options may be entered after **set admin telnet**

down	Turn off telnet access.
up	Turn on telnet access.

Notes

This command will take effect immediately after it is executed.

Examples

set admin telnet up Allow telnet access

set admin telnet down Disallow telnet access

set admin tftp

Purpose

Use **set admin tftp** to set the tftp server information.

Options

The following options may be entered after **set admin tftp**.

server	<hostname or IP address>	Set the TFTP server.
--------	--------------------------	----------------------

Notes

The settings made by this command will take effect after a write operation.

TFTP server is used for the following operations:

- ✓ Upgrading of firmware
- ✓ Importing and exporting of configurations
- ✓ Storing of TCP dump data captured.
- ✓ Storing of Technical Service Dump (TSDump) captured data for sending to Redline Networks Support organization.

Examples

```
set admin tftp server 19.8.7.4
```

Set TFTP server by IP address

set admin tsdump

Purpose

Use **set admin tsdump** to set options relating to technical service dump.

Options

The following options may be entered after **set admin tsdump**.

disabled	Disable tsdump function	
filename	<tspdmp filename>	Set the remote filename for the tsdump.
mailto1	<first email address>	First email address that the tsdump should be sent to.
mailto2	<second email address>	Second email address that the tsdump should be sent to.
smtp	Send tsdump information via pre-configured email addresses. Either smtp or tftp can be set but not both at the same time.	
tftp	Send tsdump information via the pre-configured tftp host. Either smtp or tftp can be set but not both at the same time.	

Notes

The settings made by this command will take effect after a write operation.

Technical service dump are information useful for troubleshooting the Web I/O Accelerator by Redline Networks authorized personnel. These parameters must be set before running the **tsdump** command:

- ✓ Filename for storing the tsdump, if you are using tftp
- ✓ Either an email address or a tftp server

Examples

set admin tsdump disabled	Disable the tsdump function
set admin tsdump smtp	Use the pre-configured email address to send the tsdump information
set admin tsdump tftp	Use the pre-configured tftp host to upload the tsdump information

set admin upgrade

Purpose

Use **set admin upgrade** to configure the filename of the Web I/O Accelerator pac file (the firmware) to upgrade from.

Options

The following options may be entered after **set admin upgrade**.

filename	<filename for the firmware>	Set the filename of the firmware to upgrade from.
----------	-----------------------------	---

Notes

The settings made by this command will take effect after a write operation.

The tftp server must be configured before the upgrade. “set admin tftp server <tftp server>”.

Examples

```
set admin upgrade filename tx.pac
```

Set the filename of the Web I/O Accelerator pac file to be tx.pac.

set admin vip

Purpose

Use **set admin vip** to set the administrative IP address.

Options

None.

Notes

The settings made by this command will take effect after a write operation.

Examples

set admin vip 10.0.11.10 Set the administrative IP address.

set admin webui

Purpose

Use **set admin webui** to set web administration manager characteristics.

Options

The following options may be entered after **set admin webui**.

down		Turn the web user interface off.
port	<port number>	Set the administrative port
sessionExpireTime	<seconds>	Set an administrative session timeout.
ssl	cert	SSL certificate for the administration manager via SSL
	disabled	Disable the administration manager via SSL.
	enabled	Enable the administration manager via SSL.
up		Turn the web user interface on.

Notes

Setting the Web user interface service up or down will take effect immediately after the command is executed. The rest of the settings in this section will only take effect after a write operation.

Examples

set admin webui port 8090 Set in-band administrative port to 8090.

set admin webui up Turn the web administration manager on

set admin webui ssl enabled Enable access of the Web UI via SSL

set boot

Purpose

Use **set boot** to set the boot partition for the next reboot.

Options

The following options may be entered after **set boot**.

1	Set partition 1 to be the active partition for the next reboot.
2	Set partition 2 to be the active partition for the next reboot.

Notes

None

Examples

set boot 1

Set partition 1 to be the boot partition for next reboot.

set clock

Purpose

Use **set clock** to set the server's date and time.

Options

The following options may be entered after **set clock**

```
set clock <YYYY.MM.DD HH:MM:SS>
```

- YYYY: Year
- MM: Month
- DD: Day
- HH: Hour
- MM: Minute
- SS: Second

Notes

The settings made by this command will take effect after a write operation.

If date and time are controlled by NTP, you must

```
set ntp down
```

before using this command.

Examples

```
set clock 2002.08.13. 14:00:00    Set the date and time in <YYYY.MM.DD HH:MM:SS> format.
```

set cluster N busyredirect

Purpose

Use **set cluster N busyredirect** to redirect client to an alternate URL when a target server sends a “server busy” message.

Options

The following options may be entered after **set cluster N busyredirect**.

url	The URL that the client should be redirected to when the target server sends a “server busy” message.
-----	---

Notes

The settings made by this command will take effect after a write operation.

Examples

set cluster 1 busyredirect www.alternate.com Redirects client to the page www.alternate.com when the target servers sends a “server busy” message.

set cluster N connbind

Purpose

Use **set cluster N connbind** to enable or disable connection binding. This feature is only available on the E|X Web I/O Accelerator product line.

Options

The following options may be entered after **set cluster N connbind**.

disabled	Disable connection binding.
enabled	Enable connection binding.

Notes

The settings made by this command will take effect after a write operation.

Examples

set cluster 1 connbind enabled Enables connection binding.
set cluster 1 connbind disabled Disables connection binding.

set cluster N convert302protocol

Purpose

Use **set cluster N convert302protocol** to enable or disable the convert302protocol.

Options

The following options may be entered after **set cluster N convert302protocol**.

disabled	Disable convert302protocol.
enabled	Enable convert302protocol.

Notes

The settings made by this command will take effect after a write operation. Enabling this option will convert the HTTP 302 responses from the target server from http to https or https to http. For example, if the HTTP 302 responses from the target server is using http, enabling this option will cause the Web I/O Accelerator to convert the 302 responses back to the client to use https protocol. A scenario that this is useful is when SSL acceleration is enabled on the listen side and the target side remains as clear traffic. When the target server sends a HTTP 302 response, the Web I/O Accelerator will automatically convert the HTTP 302 response back to the client using https protocol.

Examples

set cluster 1 convert302protocol enabled Enables the convert302 protocol.

set cluster N dsr

Purpose

Use **set cluster N dsr** to enable or disable Direct Server Response (DSR), which reduces traffic by allowing web servers to send HTTP responses directly back to the requesting client, thus bypassing the load balancer in the response path.

Options

The following options may be entered after **set cluster N dsr**

enabled	Enable cluster N dsr.
disabled	Disable cluster N dsr.

Notes

The settings made by this command will take effect after a write operation.

See the *Installation and Administration Guide* for more information.

Examples

set cluster 1 dsr enabled Enable dsr on cluster 1.

set cluster 2 dsr disabled Disable dsr on cluster 2.

set cluster N health

Purpose

Use **set cluster N health** to set the content health check parameters for target servers.

Options

The following options may be entered after **set cluster N health**

enabled		Enable content health check.
disabled		Disable content health check.
returncode	<return code>	The expected return code. Default is 200.
size (optional)	<size of response>	Expected size of the response. This is the number of bytes in the body of the response as would be reflected in an HTTP Content-Length header. Default is -1.
string (optional)	<string>	Search for the string in the non-header portion of the HTTP response. The string is case-sensitive and must be enclosed in double quotes if there is white space in the string. The maximum length of the string is 64 bytes. This option only applies to the following MIME type: <ul style="list-style-type: none"> ✓ text/html ✓ text/css ✓ text/plain ✓ text/xml
interval	<interval>	Interval for health check requests in seconds. Default is 2 seconds. Can be ranged from 1-60 seconds.
retry	<retry number>	Number of health check retries with no response before declaring the Target Server as "down". Default is 2. Can be ranged from 1-20.
resume	<resume number>	Number of health checks with good responses before declaring the Target Server as "operational". Default is 4. Can be ranged from 1-20.
urlpath	<url path>	The URL path that the Web I/O Accelerator wills end to target servers fir health check. The URL path must begin with a "/".

Notes

The settings made by this command will take effect after a write operation.

The Web I/O Accelerator verifies the health of the Target Server by sending a HTTP "GET" request to all the Target Servers in the cluster at a pre-configured interval.

Examples

set cluster 1 health urlpath /index.html	Set the URL for health check to be index.html.
set cluster 1 health returncode 200	Set expected return code to be 200.
set cluster 1 health enabled	Enable health check for cluster 1

set cluster N listen

Purpose

Use **set cluster N listen** to set properties for the cluster's listen traffic (between the Web I/O Accelerator and the client browser). This establishes a virtual IP address, netmask, port, or SSL for a server cluster's listen traffic.

Options

The following options may be entered after **set cluster N listen**.

netmask	<IP netmask>	Set the cluster's listen virtual IP netmask. The default is 255.255.255.255.
port	<port number>	Set cluster listen port. The default is set to 80.
ssl	SSL configuration: see the set cluster N listen ssl page (next).	
vip	<IP address>	Set the cluster's listen virtual IP address

Notes

The settings made by this command will take effect after a write operation.

If the Virtual IP subnet is the same as the subnet(s) entered for the network interfaces Ethernet 0, the Virtual IP Netmask must be set to 255.255.255.255.

Examples

set cluster 1 listen vip 10.0.22.51 Set cluster 1's listen virtual IP address to 10.0.22.51

set cluster 1 listen port 80 Set cluster 1's listen port to 80.

set cluster N listen ssl

Purpose

Use **set cluster N listen ssl** to establish properties of a cluster's SSL listen traffic.

Options

The following options may be entered after **set cluster N listen ssl**.

enabled		Enable SSL for cluster's listen traffic
disabled		Disable SSL for cluster's listen traffic
certfile		Specify the SSL certfile for cluster's listen traffic
keyfile		Specify the SSL keyfile for cluster's listen traffic
keypass		Specify the SSL key password for cluster's listen traffic
ciphersuite	all	Allow all supported SSL cipher suites for cluster's listen traffic.
	common	Allow only the most commonly used cipher suites from both the strong and export groups
	export	Allow only the lower-security cipher suites that have been traditionally available for export
	strong	Allow only the highest security cipher suites that have traditionally only been available in the USA.
protocol	sslv2 sslv23 sslv3 tlsv1	Specify the SSL protocol type for cluster's listen traffic. <ul style="list-style-type: none"> - sslv2: SSL Version 2 only - sslv23: SSL Version 2, SSL Version 3 and TLS Version 1 - sslv3: SSL Version 3 only - tlsv1: TLS Version 1 only
clientauth		SSL client certificate authentication. see the set cluster N listen ssl clientauth page (next). This feature is only available on the E X Web I/O Accelerator product line.

Notes

The settings made by this command will take effect after a write operation.

The details on cipher suites are listed below. This can also be found in the *Setting up the T|X or E|X for SSL Traffic* chapter of the *Installation and Administration Guide*.

All SSL Ciphers

```

RC4_MD5
RC4_SHA
DES_CBC_MD5
DES_CBC_SHA
DES_CBC3_MD5
DES_CBC3_SHA
EXP_RC4_MD5
EXP_RC2_CBC_MD5
EXP1024_RC4_MD5

```

EXP1024_RC2_CBC_MD5

Common SSL Ciphers

RC4_MD5
 RC4_SHA
 EXP_RC4_MD5
 EXP_RC2_CBC_MD5
 EXP1024_RC4_MD5
 EXP1024_RC4_SHA
 EXP1024_RC2_CBC_MD5

Export SSL Ciphers

EXP_RC4_MD5
 EXP_RC2_CBC_MD5
 EXP1024_RC4_MD5
 EXP1024_RC2_CBC_MD5

Strong SSL Ciphers

RC4_MD5
 RC4_SHA
 DES_CBC_MD5
 DES_CBC_SHA
 DES_CBC3_MD5
 DES_CBC3_SHA

Examples

set cluster 1 listen ssl certfile certfile.dat	Set cluster 1's listen SSL certfile to certfile.dat
set cluster 1 listen ssl keypass	Set cluster 1's listen SSL password (prompted)
set cluster 1 listen ssl ciphersuite export	Set cluster 1's listen SSL ciphersuite to export

set cluster N listen ssl clientauth

Purpose

Use **set cluster N listen ssl clientauth** to establish properties of a cluster's SSL listen traffic with client certificate authentication. This feature is only available on the E|X Web I/O Accelerator product line.

Options

The following options may be entered after **set cluster N listen ssl clientauth**.

disabled		Disable SSL client certificate authentication
enabled		Enable SSL client certificate authentication
cacertfile	<filename>	Sets the advertised Certificate Authority (CA) file as <filename> for the cluster. The <filename> must contain a list of one or more valid CA certificates that are self-signed or signed by: <ol style="list-style-type: none"> (1) a well-known trusted CA (2) a CA listed in the trusted CA certificate file. <p>All certificate entries in this file must be in base64-encoded format.</p>
caclfile	<filename>	Sets the CA Certificate Revocation List (CRL) as <filename> for the cluster. The <filename> must be a list of one or more valid CRLs containing certificates signed by one of the CAs listed in the trusted CA certificate file. All CRL entries not corresponding to an entry in the trusted CA certificate file are ignored. <p>All CRLs listed in the file must be in base64-encoded format.</p>
catrustfile	<filename>	Sets the CA trusted certificate file as <filename> for the cluster. The <filename> must be a file containing a valid list of one or more either root or intermediate CA certificates; each certificate is encoded in base64 format. <p>If the certificate is an intermediate certificate, it's root CA certificate must also be present in either the catrustfile or the cacertfile.</p>

Notes

The settings made by this command will take effect after a write operation.

Examples

set cluster 1 listen ssl clientauth enabled	Enable client authentication for cluster 1.
set cluster 1 listen ssl clientauth cacertfile ca_cert_list	Sets the advertised CA file to be "ca_cert_list" for cluster 1.
set cluster 1 listen ssl clientauth cacertfile ca_crl_list	Set the CA CRL to be "ca_crl_list" for cluster 1.
set cluster 1 listen ssl clientauth catrustfile ca_trusted_list	Set the CA trusted certificate file to

be "ca_trusted_list" for cluster 1.

set cluster N sticky

Purpose

Use **set cluster N sticky** to set client to target sever bindings.

Options

The following options may be entered after **set cluster N sticky**.

clientip	timeout	Set the time (in minutes) to keep the clientip bound to a target host.
cookie	expire	Set the time (in minutes) to keep the cookie valid.
mask	iponly	Use only IP address to identify a target server.
	ipport	Use both IP address and port for identifying a target server.
		Mask only applicable to the cookie method.
method	clientip	Use clientip for binding clients to a target host.
	cookie	Use cookies for binding clients to a target host.
	none	No sticky bindings.

Notes

The settings made by this command will take effect after a write operation.

Examples

set cluster 1 sticky clientip timeout 1000	Set sticky (via clientip) timeout to 1000 minutes
set cluster 1 sticky cookie expire 1000	Set sticky (via cookie) timeout to 1000 minutes
set cluster 1 sticky method cookie	Use cookies for binding clients to a target host.
set cluster 1 sticky method none	Disable client IP-based stickiness
set cluster 1 sticky mask ipport	Use IP address and port to identify a target server.

set cluster N target

Purpose

Use **set cluster N target** set a target name, target host, or enable/disable the target host.

Options

The following options may be entered after **set cluster N target**

host	<IP and port>	<blank>	Set cluster target host.
		enabled	Enable cluster target host.
		disabled	Disable cluster target host.
name	<DNS Name>		Set the cluster target name.
ssl	SSL configuration: see the set cluster N target ssl page.		

Notes

The settings made by this command will take effect after a write operation.

Examples

set cluster 1 target host 10.0.22.3:80	Establish a target host for cluster1 at the specified IP address and port number.
set cluster 1 target host 66.218.71.87:80 enabled	Enable target server 66.218.71.87 in cluster 1.
set cluster 1 target host all enabled	Enable all target servers in cluster 1
set cluster 1 target name foobar.com	Set domain name of the of target host for cluster 1.

set cluster N target ssl

Purpose

Use **set cluster N target ssl**

Options

The following options may be entered after **set cluster N target ssl**.

enabled		Enable ssl for cluster's target traffic
disabled		Disable ssl for cluster's target traffic
certfile		Specify the ssl certfile for cluster's target traffic
keyfile		Specify the ssl keyfile for cluster's target traffic
keypass		Specify the ssl key password for cluster's target traffic
timeout <minutes>		Timeout in number of minutes. Default is 1440 minutes
ciphersuite	all common export strong	Allow all supported SSL cipher suites for cluster's target traffic. Allow only the fastest cipher suites from both the strong and export groups Allow only the lower-security cipher suites that are suitable for export Allow only the highest security cipher suites that are suitable for use in USA
protocol	sslv2 sslv3 sslv23 tlsv1	Specify SSL protocol type for cluster's target traffic: - sslv2: SSL Version 2 only - sslv3: SSL Version 3 only - sslv23: SSL Version 2, SSL Version 3 and TLS Version1 - tlsv1: TLS Version 1 only

Notes

The settings made by this command will take effect after a write operation.

The details on cipher suites are listed below. This can also be found in the *Setting up the T|X or E|X for SSL Traffic* chapter of the *Installation and Administration Guide*.

All SSL Ciphers

RC4_MD5
RC4_SHA
DES_CBC_MD5
DES_CBC_SHA
DES_CBC3_MD5
DES_CBC3_SHA
EXP_RC4_MD5
EXP_RC2_CBC_MD5
EXP1024_RC4_MD5
EXP1024_RC2_CBC_MD5

Common SSL Ciphers

RC4_MD5
RC4_SHA
EXP_RC4_MD5

EXP_RC2_CBC_MD5
EXP1024_RC4_MD5
EXP1024_RC4_SHA
EXP1024_RC2_CBC_MD5

Export SSL Ciphers

EXP_RC4_MD5
EXP_RC2_CBC_MD5
EXP1024_RC4_MD5
EXP1024_RC2_CBC_MD5

Strong SSL Ciphers

RC4_MD5
RC4_SHA
DES_CBC_MD5
DES_CBC_SHA
DES_CBC3_MD5
DES_CBC3_SHA

Examples

set cluster 1 target ssl enabled

Enable ssl encryption for cluster 1

Set cluster 1 target ssl ciphersuite all

Use "all" SSL cipher suites type for cluster's target traffic.

set cluster N weblog

Purpose

Use **set cluster N weblog** to enable or disable cluster logging,

Options

The following options may be entered after **set cluster N weblog**

enabled		Enable cluster logging.
disabled		Disable cluster logging.
combinedlogformat	enabled disabled	Enable or disable combined log format.
host	<host IP address>	Set cluster log host address.

Notes

The settings made by this command will take effect after a write operation.

Examples

set cluster 1 weblog enabled	Enable logging on cluster 1.
set cluster 2 weblog disabled	Disable logging on cluster 2.
set cluster 1 weblog host <10.4.5.4>	Set cluster 1's log host address.

set dns

Purpose

Use **set dns** to set the nameservice domain and the name server.

Options

The following options may be entered after **set dns**

domain <DNS name>	Set the nameservice domain.
server N <IP address>	Set the name server. Where N = 1, 2 or 3.

Notes

The settings made by this command will take effect after a write operation.

Examples

set dns domain www.foo.bar Set DNS domain to a domain name

set dns server 1 192.177.45.13 Set name server to an IP address

set ether N

Purpose

Use **set ether N** to set the IP address, media, mtu and the netmask.

Options

The following options may be entered after **set ether N**.

ip	<IP address>	Set the IP address.
media	<media description or #>	Set the media parameters.
mtu	<MTU #>	Set the interface MTU.
netmask	<IP mask>	Set the netmask

Notes

The settings made by this command will take effect after a write operation.

Ether N may be ether 0 or ether 1.

Ether 0 is for user traffic and in-band administration.

Ether 1 is for “heartbeat” traffic ensuring that the Web I/O Accelerator is active and there is no need to cut over to the standby Web I/O Accelerator.

Admin interface can be all interfaces or specified by the **set admin interface** command. The setting for media must exactly match the switch to which the Web I/O Accelerator is attached. If the switch is managed and has explicit settings, choose the exact speed and setting. If the switch is unmanaged, choose auto negotiate.

Examples

set ether 0 ip 10.44.5.5	Set ether 0 IP address
set ether 1 media 100baseTX full-duplex	Set ether 1's media type to 100 BaseT with hardware loop back.
set ether 1 media 6	Change media for ether0 to autoselect. (See show etherN for more information.)

set forwarder N

Purpose

A forwarder is used to forward non-HTTP traffic (for instance, SMTP traffic).

Use **set forwarder N listen** to set the address, netmask or port for forwarder listening.

Use **set forwarder N weblog** to set the host or logging for a forwarder.

Use **set forwarder N target** to establish a target host, or enable/disable that host.

Options

The following options may be entered after **set forwarder N**.

listen	vip	<IP address>	Set the forwarder's virtual IP address.
	netmask	<IP netmask>	Set the forwarder's virtual IP netmask. Default is 255.255.255.255.
	port	<Port number>	Set the forwarder's listen port. This should usually be set to 80. Default is port 80.
target	host	<ipaddress:port>	Set the IP address and the port for forwarder target.
	host	<enabled disabled>	Set forwarder target host status: enabled or disabled.
	all	<enabled disabled>	Set all forwarder target host status: enabled or disabled.

Notes

The settings made by this command will take effect after a write operation.

Examples

set forwarder 1 listen port 80

Set forwarder 1's listen port to 80

set forwarder 1 target host enabled

Enable the target host for forwarder 1.

set hostname

Purpose

Use **set hostname** to set the hostname.

Options

The following options may be entered after **set hostname**.

<host name>	Name of the host.
-------------	-------------------

Notes

The settings made by this command will take effect after a write operation. The hostname must be a fully qualified name.

Examples

set hostname www.foobar.com Set the hostname.

set ntp

Purpose

Use **set ntp** to set the NTP server or daemon.

Options

The following options may be entered after **set ntp**.

server N <hostname/IP Address>	Set NTP server N. Where = 1, 2 or 3.
up	Turn on the NTP daemon.
down	Turn off the NTP daemon.

Notes

The settings made by this command will take effect after a write operation.

Examples

set ntp server 1 www.foobar.com	Set NTP server
set ntp up	Turn on the NTP daemon

set password

Purpose

Use **set password** to set the login password.

Options

The following options may be entered after **set password**.

None	You are prompted for the password.
------	------------------------------------

Notes

This command takes effect immediately.

You are prompted for the old password before you are allowed to set the new password.

Examples

```
tx2% set password                To change the password.
Old password: *****
New password: *****
Retype new password: *****
tx2%
```

set redirector N

Purpose

Use **set redirector N** to set properties for the redirector. This feature is only available on the E|X Web I/O Accelerator product line.

Options

The following options may be entered after **set redirector N**.

customurl	<URL string>	Set the URL for redirecting. Only used when urlmethod is set to "custom".
enabled		Enable the redirector
disabled		Disable the redirector
dsr	enabled	Enable use of DSR
	disabled	Disable use of DSR
host	<hostname or IP address>	Set the hostname or IP address to redirect requests to.
port	<port number>	Set the port to redirect requests to. Default is port 443.
protocol	http	To redirect requests to use HTTP protocol.
	https	To redirect requests to use HTTPS protocol. Default is set to https.
urlmethod	custom	To redirect request to a custom page defined in customurl.
	request	To redirect to the same page as the original request. The default is set to "request".
listen	Redirector listen configuration: see the set redirector N listen page (next).	

Notes

The settings made by this command will take effect after a write operation. The redirector must be enabled before requests will be redirected.

Examples

set redirector 1 host 205.178.13.100 Set redirector 1's host to be 205.178.13.100.

set redirector 1 port 443 Redirect requests to port 443.

set redirector N listen

Purpose

Use **set redirector N listen** to set properties for the redirector. This establishes a virtual IP address, netmask, port, or SSL for a server redirector's traffic. This feature is only available on the E|X Web I/O Accelerator product line.

Options

The following options may be entered after **set redirector N listen**.

netmask	<IP netmask>	Set the redirector's listen virtual IP netmask. The default is 255.255.255.255.
port	<port number>	Set redirector listen port. Default is port 80.
ssl	SSL configuration: see the set cluster N listen ssl page (next).	
vip	<IP address>	Set the redirector's listen virtual IP address

Notes

The settings made by this command will take effect after a write operation.

If the Virtual IP subnet is the same as the subnet(s) entered for the network interfaces Ethernet 0, the Virtual IP Netmask must be set to 255.255.255.255.

Examples

set redirector 1 listen vip 205.178.13.100 Set redirector 1's listen virtual IP address to 205.178.13.100

set redirector 1 listen port 80 Set redirector 1's listen port to 80.

set redirector N listen ssl

Purpose

Use **set redirector N listen ssl** to establish properties of a redirector's SSL listen traffic. This feature is only available on the E|X Web I/O Accelerator product line.

Options

The following options may be entered after **set redirector N listen ssl**.

ssl	enabled	Enable SSL for redirector's listen traffic
	disabled	Disable SSL for redirector's listen traffic
	certfile	Specify the SSL certfile for redirector's listen traffic
	keyfile	Specify the SSL keyfile for redirector's listen traffic
	keypass	Specify the SSL key password for redirector's listen traffic
ciphersuite	all	Allow all supported SSL cipher suites for redirector's listen traffic.
	common	Allow only the fastest cipher suites from both the strong and export groups
	export	Allow only the lower-security cipher suites that are suitable for export
	strong	Allow only the highest security cipher suites that are suitable for use in USA
protocol	ssl2	Specify the SSL protocol type for redirector's listen traffic.
	ssl3	- ssl2: SSL Version 2 only
	ssl23	- ssl3: SSL Version 3 only
	tlsv1	- ssl23: SSL Version 2, SSL Version 3 and TLS Version 1
		- tlsv1: TLS Version 1 only

Notes

The settings made by this command will take effect after a write operation.

The details on cipher suites are listed below. This can also be found in the *Setting up the T|X or E|X for SSL Traffic* chapter of the *Installation and Administration Guide*.

All SSL Ciphers

```
RC4_MD5
RC4_SHA
DES_CBC_MD5
DES_CBC_SHA
DES_CBC3_MD5
DES_CBC3_SHA
EXP_RC4_MD5
EXP_RC2_CBC_MD5
EXP1024_RC4_MD5
EXP1024_RC2_CBC_MD5
```

Common SSL Ciphers

```
RC4_MD5
RC4_SHA
```

EXP_RC4_MD5
 EXP_RC2_CBC_MD5
 EXP1024_RC4_MD5
 EXP1024_RC4_SHA
 EXP1024_RC2_CBC_MD5

Export SSL Ciphers

EXP_RC4_MD5
 EXP_RC2_CBC_MD5
 EXP1024_RC4_MD5
 EXP1024_RC2_CBC_MD5

Strong SSL Ciphers

RC4_MD5
 RC4_SHA
 DES_CBC_MD5
 DES_CBC_SHA
 DES_CBC3_MD5
 DES_CBC3_SHA

Examples

set redirector 1 listen ssl certfile certfile.dat	Set redirector 1's listen SSL certfile to certfile.dat
set redirector 1 listen ssl keypass	Set redirector 1's listen SSL password (prompted)
set redirector 1 listen ssl ciphersuite export	Set redirector 1's listen SSL ciphersuite to export

set route

Purpose

Use **set route** to set the default route.

Options

The following options may be entered after **set route**.

default	Set the default route.
---------	------------------------

Notes

This command takes effect immediately. To add a route, see **add route** command

Examples

set route default 10.8.8.8

Set the default route to the device at the specified address.

set server customiplogheader

Purpose

Use **set server customiplogheader** to set the custom HTTP header to which will be added with the client's origin IP to the client's request.

Options

The following options may be entered after **set server customiplogheader**.

<header>

Header can be either a literal or a custom field in which the Web I/O Accelerator will insert the origin client's IP address. For more information, see the *Logging* chapter of the *Installation and Administration Guide*.

Notes

The settings made by this command will take effect after a write operation.

Examples

```
set server customiplogheader rlnclientipaddr
```

Use the rlnclientipaddr argument as a field to insert the IP address.

set server failover

Purpose

Use **set server failover** to enable or disable Redline server failover.

The first server established as failover is the active server; the second is the standby server.

Options

The following options may be entered after **set server failover**

disabled		Disable Redline Server fail-over.
enabled		Enable Redline Server fail-over.
linkfail	count	Fail-over link failure count. Default is 4.
	pollinterval	Fail-over link failure poll interval in milliseconds. Default is 500.
vmac	disabled	Disable fail-over with Virtual MAC (vmac) option.
	enabled	Enable fail-over with Virtual MAC (vmac) option
	id	Fail-over Virtual MAC (vmac) ID. Default is 0.

Notes

The settings made by this command will take effect after a write operation.

Both the active and the stand-by Web I/O Accelerators should have this option enabled, and both units should have the same clusters and forwarders settings.

Examples

set server failover enabled Enable Redline server failover.

set server failover disabled Disable Redline server failover.

set timezone

Purpose

Use **set timezone** to set the server's time zone.

Options

The following options may be entered after **set timezone**.

<time zone>

Notes

The settings made by this command will take effect after a write operation.

Use **show timezone list** to get a list of all time zones, and see what your local one is called.

Examples

```
set timezone America/Los_Angeles
```

show admin

Purpose

Use **show admin** to show the administrative services configuration.

Options

The following options may be entered after **show admin**.

<blank>	Show all admin settings, e.g. telnet, SNMP, SSH. Web UI information
email	Show email server and email address information.
interface	Show admin interface setting.
log	Show all logging settings.
netmask	Show the netmask setting for the admin interface.
snmp	Show SNMP information.
ssh	Show whether ssh is enable.
syslog	Show syslog setting
tcpdump	Show TCPdump settings.
telnet	Show whether telnet is enable.
tftp	Show TFTP server setting.
tsdump	Show TSDump settings.
upgrade	Show upgrade filename.
vip	Show admin VIP setting.
webui	Show admin server information.

Notes

For a simple **show admin**, the following output is obtained:

```

----- Admin Interface -----
Admin Interface: ether0
VIP Address:
VIP Netmask: 255.255.255.255

----- Web UI -----
Port: 8090
SSL Status: disabled
Session Expire Time: 900
Admin: up

----- SNMP -----
System contact: Tom
System location: Unknown
SNMP community name: public
SNMP community IP: 192.168.0.0
SNMP community netmask: 255.255.0.0
SNMP: up

```

----- Terminal Services -----

SSH: up
Telnet: up

----- Logging -----

Logging: enabled
Logging to:
 email: EMERG
 memory: ALERT
 syslog: ALERT
Email 'mailto' addresses:
 mailto1: jim@company.com
 mailto2: tom@company.com

----- Upgrade -----

Upgrade Filename: 2_2.pac

Examples

show admin ssh	Show if ssh is enabled.
show admin snmp	Show SNMP information.

show admin email

Purpose

Use **show admin email** to show the email configuration.

Options

None.

Notes

None.

Examples

show admin email

Show the email information configured. This includes:

- SMTP server
- From email address
- Default to email address

show admin log

Purpose

Use **show admin log** to show the logging configurations.

Options

None.

Notes

None.

Examples

show admin log

Show the logging configurations. This include:

- Where it will log to: memory, syslog or email
- Level of logging for each destination
- Email addresses that the log will be sent to
- If logging is enabled.

show admin snmp

Purpose

Use **show admin snmp** to show SNMP configuration information.

Options

The following options may be entered after **show admin snmp**.

<blank>		Show SNMP configuration
status		Show whether SNMP is up or down
community	<blank>	Show SNMP community configuration
	ip	Show SNMP community IP address.
	name	Show SNMP community name.
	netmask	Show SNMP community netmask.
contact		Show SNMP system contact
location		Show SNMP system location.

Notes

The output of a simple **show snmp** command is as follows:

```
System contact: Unknown
System location: Unknown
SNMP community name: public
SNMP community IP: 194.166.0.0
SNMP community netmask: 255.255.0.0
SNMP: down
```

Examples

show snmp status

Show whether SNMP is up or down

show admin telnet

Purpose

Use **show admin telnet** to show whether telnet is up or down.

Options

The following options may be entered after **show telnet**.

<blank>	Show telnet configuration
status	Show whether telnet is up or down

Notes

None

Examples

show admin telnet

Show telnet configuration: up or down.

show admin upgrade

Purpose

Use **show admin upgrade** to show the filename of the Web I/O Accelerator pac file (the firmware) to upgrade from.

Options

The following options may be entered after **show admin tftp**.

<blank>	Show the upgrade information.
filename	Show the filename to upgrade from. This is currently the same information as show admin upgrade .

Notes

None.

Examples

show admin upgrade

Show the filename of the Web I/O Accelerator pac file.

show admin webui

Purpose

Use **show admin webui** to show the server configuration.

Options

The following options may be entered after **show admin webui**.

<blank>	Show Web Administration Server configuration.
port	Show admin server listen port.
ssl	Show whether Admin server is using SSL.
sessionexpiretime	Show timeout for admin sessions.
status	Show whether admin server is up or down.

Notes

For a simple **show admin webui**, the following output is obtained:

```
Port: 8090
SSL Status: disabled
Session Expire Time: 900
Admin: up
```

Examples

show admin webui port	Show the administrative server's listen port.
show admin webui status	Show whether the admin server is up or down.

show arp

Purpose

Use **show arp** to display the ARP table.

Options

None.

Notes

This command is the same as the “arp” command.

Examples

show arp Display the current ARP table.

E.g. of output:

```
gateway.company.com (192.168.0.1) at 0:f0:e7:85:ac:d0 [ethernet]  
mail.company.com (192.168.0.2) at 0:e0:a7:ee:e0:2e [ethernet]  
brown.company.com (192.168.0.20) at 0:f0:e7:85:a8:2c [ethernet]  
? (192.168.33.2) at 0:f0:e7:25:d6:26 [ethernet]
```

show audit

Purpose

Use **show audit** to show recent administrative actions.

Options

None.

Notes

Sample **show audit** output is in the following format; it summarizes recent administrative actions.

```
Aug 14 14:13:04 192.168.0.234 rlshell busy_redirect: [empty]->www.foobar.com
Aug 14 14:13:04 192.168.0.234 rlshell server_listenprotocol_status: Off->On
Aug 13 17:13:20 192.168.0.234 rlshell server_status: Off->On
Aug 13 17:13:20 192.168.0.234 rlshell server_status: On->Off
```

Examples

```
show audit
```

Show a list of recent administrative actions.

show boot

Purpose

Use **show boot** to show boot partition information.

Options

None.

Notes

Sample **show boot** output:

```
% show boot
Boot 1 (Current): Redline Networks Accelerator 2.2 Thu Nov  7
20:25:47 GMT
Boot 2 (Active) : Redline Networks Accelerator 2.3 Fri Nov  8
20:25:47 GMT
```

Current partition indicates the partition that is currently running. Active partition is the one that will be used after the next reboot. Current and active partitions can be the same one. An example is shown below:

```
% show boot
Boot 1 (Current, Active): Redline Networks Accelerator 2.2 Thu Nov  7
20:25:47 GMT
Boot 2                   : Empty partition.
```

Examples

show boot

Show boot partition information.

show clock

Purpose

Use **show clock** to show the time and date.

Options

None

Notes

The output is in the following format:

<YYYY.MM.DD HH:MM:SS TZ>

Where YYYY = year

MM = month

DD = day

HH = hour

MM = minute

SS = second

TZ = timezone

Examples

show clock

Show date and time. Example output is:
2002.08.14 14:22:06 PDT

show cluster

Purpose

Use **show cluster** to show information for all clusters.

Options

<blank>	Show all cluster configurations.
all	Show all cluster configurations.
N	Show specific cluster configurations. See next section for more details.

Notes

None.

Examples

show cluster	Show all cluster information
show cluster all	Show all cluster information

show cluster N

Purpose

Use **show cluster N** to show the configuration for a specific cluster.

Options

The following options may be entered after **show cluster N**.

<blank>		Show cluster configuration.
busyredirect		Show cluster busy-redirect page.
connbind		Show connection binding settings. This feature is only available on the E X Web I/O Accelerator product line.
convert302protocol		Show cluster's HTTP 302 protocol conversion configuration
dsr		Show cluster's DSR status
health	<blank>	Show the content health check settings.
	urlpath	Show the urlpath to check.
listen	<blank>	Show cluster's listener configuration
	netmask	Show the cluster's virtual IP netmask
	port	Show cluster listen port
	ssl	Show cluster listen SSL. See the following command for more detail: show cluster N listen ssl
	vip	Show the cluster's virtual IP address.
sticky	<blank>	Show sticky configuration for the cluster.
	method	Show sticky method configuration
	mask	Show sticky mask configuration
	cookie	Show cookie-based sticky configuration
	cookie expire	Show cookie expire time configuration
	clientip	Show client IP base sticky configuration
	clientip timeout	Show client IP timeout configuration
target	<blank>	Show cluster target configuration
	host	Show all target hosts in the cluster
	host all	Show all target hosts in the cluster
	host N	Show cluster target hosts
	name	Show cluster target name
	ssl	Show cluster target SSL. See the following command for more detail: show cluster N target ssl
	status	Show the health of the target server based on layer 7 health check. See the command show cluster N health status for more details.

	returncode	Show the expected returncode.
	size	Show the expected size of the response
	string	Show the expected string in the response.
	interval	Show the health check interval
	retry	Show the number retries.
	resume	Show the number of times health check fail before the Web I/O Accelerator declares the target server down.
	status	Show the health of the target server. See next section for details.
weblog	combinelogformat host status	Show combined log format setting Show cluster log host address Show if cluster logging is enabled or disabled.

Notes

For a simple **show cluster 1**, the following output is obtained:

```
Cluster [1]
Listen Port: 80
Virtual IP Address: 192.168.4.145
Virtual IP Netmask: 255.255.255.255
Busy redirect URL: www.foobar.com
Listen SSL Status: Disabled
Listen Protocol: sslv23
Listen Certfile:
Listen Keyfile:
Listen Keypass: none
Listen Ciphersuite: all
Targetname: mywebservers.redlinenetworks.com
Target SSL Status: Disabled
Target Protocol: tlsv1
Target Certfile:
Target Keyfile:
Target Keypass: none
Target Ciphersuite: common
Target Timeout: 1440
Health Check Status: enabled
Health Check Interval: 2
Health Check Retry: 4
Health Check Resume: 2
Health Check Url Path: /index.html
Health Check Return Code: 200
Health Check Size: -1
Health Check String:
Sticky Method: None
Sticky Mask: IP-Port
Sticky Cookie Expire: 0
Sticky Client IP Timeout: 120
DSR Status: Disabled
Convert 302 Protocol Status: Disabled
Combined Log Format Status: Disabled
Log host:
```

Log status: Disabled
TargetHosts:
[1] 166.218.71.87:80 (enabled)

Examples

show cluster 1 listen ssl

Show cluster1's listen SSL status

show cluster 1 target

Show cluster1's target configuration

show cluster 1 health

Show the content health check settings for cluster 1

Show cluster 1 health status

Show the health of the target servers in cluster 1

show cluster N health status

Purpose

Use **show cluster N health status** to show the health of the target servers based on content health check.

Options

None.

Notes

Sample output of the command:

```
se2200% show cluster 1 health status
Health Check Status: enabled
TargetHosts:
  [1] 66.218.71.87:80    Up
      Total:003 In Use:000 Hot:003 Cold:000 Discards:000
  [2] 66.218.71.88:80    Layer 7 Down; Pending Change to Up
      Total:003 In Use:001 Hot:002 Cold:000 Discards:000
  [3] 66.218.71.89:80    Layer 7 Down; Return Code Mismatch
      Total:003 In Use:000 Hot:002 Cold:001 Discards:000
  [4] 66.218.71.90:80    TCP Layer Down; Unknown Reason
      Total:003 In Use:000 Hot:003 Cold:000 Discards:000
```

Notes on number of connections:

1. Total
Total Number of connections created.
2. In Use
Number of successful connections made to the target server.
3. Hot
Number of successful connections available for use by incoming client requests.
4. Cold
Number of connections available to clients, that are not currently connected to target servers.
5. Discards
Number of connections discarded by the Web I/O Accelerator.

The Web I/O Accelerator will indicate the result of health checking the target servers giving the status at TCP layer and Layer 7, with reasons for failure, if available. Examples are:

1. Up
2. TCP Layer Down
3. Layer 7 Down: Return Code Mismatch
4. Layer 7 Down: Pending Change to Up – In the process of going through the health checking.
5. Layer 7 Down: Reason Unknown.
6. Layer 7 Down:

Examples

show cluster 1 health status

Show the health of all the target servers in the cluster.

show cluster N listen ssl

Purpose

Use **show cluster N listen ssl** to show the configuration of cluster's SSL listen parameters for a specific cluster.

Options

The following options may be entered after **show cluster N listen ssl**.

<blank>	Show the cluster listen SSL configurations.
certfile	Show the cluster's listen SSL certfile
ciphersuite	Show cluster's listen SSL ciphersuite
keyfile	Show the cluster's listen SSL keyfile
protocol	Show the cluster's listen SSL protocol
status	Show the cluster's listen SSL status
clientauth	Show the SSL client certification.. See the following command for more detail: <pre>set cluster N listen ssl clientauth</pre> This feature is only available on the E X Web I/O Accelerator product line.

Notes

The details on cipher suites are listed below. This can also be found in the *Setting up the T|X or E|X for SSL Traffic* chapter of the *Installation and Administration Guide*.

All SSL Ciphers

```
RC4_MD5
RC4_SHA
DES_CBC_MD5
DES_CBC_SHA
DES_CBC3_MD5
DES_CBC3_SHA
EXP_RC4_MD5
EXP_RC2_CBC_MD5
EXP1024_RC4_MD5
EXP1024_RC2_CBC_MD5
```

Common SSL Ciphers

```
RC4_MD5
RC4_SHA
EXP_RC4_MD5
EXP_RC2_CBC_MD5
EXP1024_RC4_MD5
EXP1024_RC4_SHA
EXP1024_RC2_CBC_MD5
```

Export SSL Ciphers

EXP_RC4_MD5
EXP_RC2_CBC_MD5
EXP1024_RC4_MD5
EXP1024_RC2_CBC_MD5

Strong SSL Ciphers

RC4_MD5
RC4_SHA
DES_CBC_MD5
DES_CBC_SHA
DES_CBC3_MD5
DES_CBC3_SHA

Examples

show cluster 1 listen ssl

Show cluster 1 listen SSL information.

show cluster 1 listen ssl ciphersuite

Show cluster 1 listen SSL ciphersuite settings

show cluster N listen ssl clientauth

Purpose

Use **show cluster N listen ssl clientauth** to show the configuration of cluster's SSL client authentication parameters for a specific cluster. This feature is only available on the E|X Web I/O Accelerator product line.

Options

The following options may be entered after **show cluster N listen ssl**.

<blank>	Show the SSL client authentication configurations.
status	Show the SSL client authentication status
cacertfile	Show the setting for the CA certfile.
cafile	Show the setting for the CA CRL file.
catrustfile	Show the setting for the CA trusted certificate file.

Notes

None.

Examples

show cluster 1 listen ssl clientauth Show SSL client authentication settings for cluster 1.

Sample output:

```
tx% show cluster 1 listen ssl clientauth
Client Authentication: enabled
CA Certfile: ca_cert_list.cert
CA CRL File: ca_crl_list.crl
CA Trust File: ca_trusted_list.cert
```

show cluster 1 listen ssl clientauth status Show if client authentication is enabled or not.

Sample output:

```
tx% show cluster 1 listen ssl clientauth status
Client Authentication: enabled
```

show cluster [N | all] stats

Purpose

Use **show cluster [N | all] stats** to display the I/O, HTTP or SSL statistics for a specific cluster or for all clusters.

Options

The following options may be entered after **show cluster [N | all] stats**.

<blank>	Display the I/O, HTTP and SSL statistics for a cluster or all clusters.
http	Display the HTTP statistics for a cluster or all clusters.
io	Display the I/O, HTTP and SSL statistics for a cluster or all clusters.
ssl	Display the SSL statistics for a cluster or all clusters.

Notes

None.

Examples

show cluster 1 stats	Display the I/O, HTTP and SSL statistics for cluster 1.
show cluster all stats	Display the I/O, HTTP and SSL statistics for all clusters.
show cluster all stats io	Display the I/O statistics for all clusters.
show cluster 1 stats ssl	Display the SSL statistics for cluster 1.

show cluster N target host [M | all] stats

Purpose

Use **show cluster N target host [M | all] stats** to display the I/O, HTTP or SSL statistics for a specific target host or for all target hosts in a cluster.

Options

The following options may be entered after **show cluster N target host [M | all] stats**.

<blank>	Display the I/O, HTTP and SSL statistics for a target host or all target hosts in a cluster.
http	Display the HTTP statistics for a target host or all target hosts in a cluster.
io	Display the I/O statistics for a target host or all target hosts in a cluster.
ssl	Display the SSL statistics for a target host or all target hosts in a cluster.

Notes

None.

Examples

show cluster 1 target host all stats	Display the I/O, HTTP and SSL statistics for all target hosts in cluster 1.
show cluster 1 target host all stats io	Display the I/O statistics for all target hosts in cluster 1.
show cluster 1 target host 1 stats http	Display the HTTP statistics for target host 1 in cluster 1.

show cluster N target ssl

Purpose

Use **show cluster N target ssl** to show the configuration of cluster's SSL parameters of target servers for a specific cluster.

Options

The following options may be entered after **show cluster N target ssl**.

<blank>	Show the target server SSL configurations.
certfile	Show the target server SSL certfile
ciphersuite	Show the target server SSL ciphersuite
keyfile	Show the target server SSL keyfile
protocol	Show the target server SSL protocol
status	Show the target server SSL status
timeout	Show the target server SSL timeout

Notes

The details on cipher suites are listed below. This can also be found in the *Setting up the T|X or E|X for SSL Traffic* chapter of the *Installation and Administration Guide*.

All SSL Ciphers

- RC4_MD5
- RC4_SHA
- DES_CBC_MD5
- DES_CBC_SHA
- DES_CBC3_MD5
- DES_CBC3_SHA
- EXP_RC4_MD5
- EXP_RC2_CBC_MD5
- EXP1024_RC4_MD5
- EXP1024_RC2_CBC_MD5

Common SSL Ciphers

- RC4_MD5
- RC4_SHA
- EXP_RC4_MD5
- EXP_RC2_CBC_MD5
- EXP1024_RC4_MD5
- EXP1024_RC4_SHA
- EXP1024_RC2_CBC_MD5

Export SSL Ciphers

- EXP_RC4_MD5
- EXP_RC2_CBC_MD5
- EXP1024_RC4_MD5

EXP1024_RC2_CBC_MD5

Strong SSL Ciphers

RC4_MD5
RC4_SHA
DES_CBC_MD5
DES_CBC_SHA
DES_CBC3_MD5
DES_CBC3_SHA

Examples

show cluster 1 target ssl

Show cluster target server SSL information.

show cluster 1 target ssl ciphersuite

Show cluster 1 target server SSL ciphersuite settings

show commands

Purpose

Use **show commands** to show the command list.

Options

None.

Notes

None.

Examples

show commands

Show a command list.

show config

Purpose

Use **show config** to show the configuration in memory.

Options

None.

Notes

The output of show config is as follows:

```

----- Hostname, Date, & Time -----
Hostname: tx2.redlinenetworks.com
2002.08.14 14:19:12 PDT
Timezone: America/Los_Angeles
NTP server1: www.foobar.com
NTP: down

----- Network -----
Domain: redlinenetworks.com
Nameserver1: 192.168.0.2
ether0: IP address = 10.0.22.50 netmask = 255.255.255.0
ether0: MAC = 00:e0:81:04:a0:06 MTU = 1500
ether0 media: 100baseTX full-duplex (100baseTX full-duplex) Status: active
ether0 supported media options:
  [1] 10baseT/UTP
  [2] 10baseT/UTP full-duplex
  [3] 100baseTX
  [4] 100baseTX full-duplex
  [5] autoselect
ether1: IP address = 10.10.1.2 netmask = 255.255.0.0
ether1: MAC = 00:e0:81:04:a0:07 MTU = 1500
ether1 media: autoselect (none) Status: no carrier
ether1 supported media options:
  [1] 10baseT/UTP
  [2] 10baseT/UTP full-duplex
  [3] 100baseTX
  [4] 100baseTX full-duplex
  [5] autoselect
Default route: 10.0.22.1

----- Clusters -----
Cluster [1]
Listen Port: 80
Listen VIP: 192.168.4.145
Virtual IP Netmask: 255.255.255.255
Busy redirect URL: www.foobar.com
Listen SSL Status: Disabled

```

```

Listen Protocol: sslv23
Listen Certfile:
Listen Keyfile:
Listen Keypass: none
Listen Ciphersuite: all
Targetname: mywebserver.redlinenetworks.com
Target SSL Status: Disabled
Target Protocol: tlsv1
Target Certfile:
Target Keyfile:
Target Keypass: none
Target Ciphersuite: common
Target Timeout: 1440
Sticky Method: None
Sticky Mask: IP-Port
Sticky Cookie Expire: 0
Sticky Client IP Timeout: 120
DSR Status: Disabled
Convert 302 Protocol Status: Disabled
Combined Log Format Status: Disabled
Log host:
Log status: Disabled
TargetHosts:

```

```
----- Forwarders -----
```

```
----- Server -----
```

```
Failover Status: Disabled
Server: up
```

```
----- Web Administration Server -----
```

```
Port: 8090
SSL Status: Disabled
Admin: up
Session Expire Time: 900
Admin Interface:
VIP Address:
VIP Broadcast: 0.0.0.0
VIP Netmask: 255.255.255.255
```

```
----- SNMP -----
```

```
System contact: Unknown
System location: Unknown
SNMP community name: public
SNMP community IP: 192.168.0.0
SNMP community netmask: 255.255.0.0
SNMP: down
```

```
----- Terminal Services -----
```

```
SSH: up
Telnet: up
```

Examples

show config

Shows the current configuration

show dashboard

Purpose

Use **show dashboard** to display a summary view of the overall health of the Web I/O Accelerator's memory, CPU status, VIP and Target server health status, connections count and bytes savings with TX

Options

None.

Notes

The sample output of show dashboard is as follows:

```
% show dashboard

Start Time:    July 27, 12:04
Current Time:  July 31, 14:26
Uptime:        4 days 2 hours, 22 minutes

T|X Health:
-----
Memory   - OK.
CPU      - OK.
Network  - OK.

VIP and Target Server Heath:
-----
Cluster 1 - 216.136.145.168 - (up)
  Target 1 192.168.0.5  (up)
  Target 2 192.168.0.6  (up)
  Target 3 192.168.0.7  (up)

Cluster 2 - 216.136.145.169 - (up)
  Target 1 192.168.0.8  (**TCP Layer Down; Connection Timed Out**)
  Target 3 192.168.0.9  (up)
  Target 3 192.168.0.10 (disabled)

Performance (Last 4 days 2 hours, 22 minutes)
-----
Connections Accepted:      6,725,256 (6.7M)
Connections Refused:      0 (0)
Requests Processed:      11,215,369 (11.2M)
Bytes Saved:              25,365,256,263 (25 GB)

Avg. Connections/Day      156,263 (156K)
Avg. Requests/Day        257,896 (257K)
```

Avg. Bytes Saved/Day 238,005,365 (238M)

Byte Savings:

Since clearing the stats on July 27, 12:04 this Redline appliance has saved a total of 25,365,256,263 bytes.

How long would it take to transfer that much data over various links?

- A T-1 user would need: 1 year, 4 months, 3 days
- A DSL user would need: 3 years, 6 months, 12 days
- A 56K user would need: 12 years, 2 months, 0 days

Examples

show dashboard

Shows the status of the Web I/O Accelerator, VIP and Target Servers.

show dns

Purpose

Use **show dns** to show the Domain name service options.

Options

The following options may be entered after **show dns**.

<blank>		Show DNS options
domain		Show the name service domain
server	N	Show the specified nameserver. N is optional.

Notes

None

Examples

show dns	Displays both the nameserver and the domain
show dns domain	Displays just the domain (i.e., foobar.com)
show dns server 1	Displays the IP address of the domain name server.

show ether N

Purpose

Use **show ether N** to show the settings for Ethernet interfaces.

Options

The following options may be entered after **show ether N**.

blank	Show settings for ethernet interfaces
ip	Show the IP address
mac	Show the MAC for an interface
media	Show media configuration for an interface
mtu	Show the MTU for an interface
netmask	Show the netmask

Notes

Ether N may be ether 0 or ether 1.

Ether 0 is for user traffic and in band administration.

Ether 1 is for “heartbeat” traffic ensuring that the Web I/O Accelerator is active and there is no need to cut over to the standby Web I/O Accelerator.

A simple show ether0 provides the following output:

```
ether0: IP address = 10.0.22.50 netmask = 255.255.255.0
ether0: broadcast 10.0.255.255
ether0: MAC = 00:e0:81:04:a0:06 MTU = 1500
ether0 media: 100baseTX full-duplex (100baseTX full-duplex) Status: active
ether0 supported media options:
  [1] 100baseTX hw-loopback
  [2] 10baseT/UTP
  [3] 10baseT/UTP full-duplex
  [4] 100baseTX
  [5] 100baseTX full-duplex
  [6] autoselect
```

The MTU (Maximum Transmission Unit) should be set to 1500 for ethernet. DO NOT change this value unless your switch and network are configured to work with a different MTU.

Examples

show ether 1 mac Show ether 1's MAC address

show ether 1 Show ether 1's settings.

show file

Purpose

Use **show file** to display content of a file.

Options

The command takes a filename as an input.

<filename>	To display the content of the file with the name <filename>.
------------	--

Notes

This command has the same effect as the command **display file**.

Examples

show file my_ssl_key To display the content of the SSL key name "my_ssl_key".

show flash

Purpose

Use **show flash** to show flash disk usage: kilobytes used, kilobytes available, and total kilobytes.

Options

None.

Notes

Output of show flash is as follows:

```
42120 Kb used, 20272 Kb avail, 62392 Kb total
```

Examples

```
show flash                               Show flash disk usage.
```

show forwarder N

Purpose

Use **show forwarder N** to show the forwarder configuration.

A forwarder is used to forward TCP traffic only (for instance, SMTP traffic).

Options

The following options may be entered after **show forwarder N**

blank	Show information for all forwarders
N	Show information for a specific forwarder
all	Show information for all forwarders

Notes

None

Examples

show forwarder	Show all forwarder configurations. See set forwarder N for more information.
show forwarder 1	Show information for forwarder 1
show forwarder all	Show all forwarder information

show forwarder [N | all] stats

Purpose

Use **show forwarder [N | all] stats** to display the I/O statistics for a specific forwarder or for all forwarders.

Options

None,

Notes

None.

Examples

show forwarder 1 stats

Display the I/O statistics for forwarder 1.

show forwarder all stats

Display the I/O statistics for all forwarder.

show forwarder N target host [M | all] stats

Purpose

Use **show forwarder N target host [M | all] stats** to display the I/O statistics for a specific target host or for all target hosts in a forwarder.

Options

None.

Notes

None.

Examples

show forwarder 1 target host 1 stats	Display the I/O statistics for target host 1 in forwarder 1.
show forwarder 1 target host all stats	Display the I/O statistics for all target hosts in forwarder 1.

show hostname

Purpose

Use **show hostname** to show the hostname.

Options

None.

Notes

None

Examples

show hostname

Show domain name for host; for instance,
tx2.foobar.com

show log

Purpose

Use **show log** to show events logged on the Web I/O Accelerator memory log.

Options

None.

Notes

Examples

show log

Show a list of events logged on the Web I/O Accelerator.

show netstat

Purpose

Use **show netstat** to show network statistics. These statistics include active internet connection information: send and receive queues, local and foreign addresses, and states.

Options

The following options may be entered after **show netstat**

blank	Show network statistics
N	Where N is an integer. Show network statistics every N seconds.
-a	Show active connections
-s	Show network statistics
-r	Show the routing tables

Notes

This is the same as the “netstat” command. Sample **show netstat** output is in the following format

```
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4    0      20  10.0.22.50.22         192.168.0.234.1094    ESTABLISHED
tcp4    0      0  *.8090                *.*                    LISTEN
tcp4    0      0  *.23                  *.*                    LISTEN
tcp4    0      0  *.22                  *.*                    LISTEN
```

Examples

```
show netstat          Show network statistics
show netstat 1       Show network statistics every second. Use ^C (control C) to stop.
Show netstat -r      Show the routing table. Sample out:
```

```
tx2200% show netstat -r
Routing tables
```

```
Internet:
Destination          Gateway             Flags    Refs    Use Netif
Expire
default              192.168.0.1        UGSc     4       0 ether0
12.12.1.23           12.12.12.12       UGHS     0       0 ether0
192.168.0/16         link#1             UC       2       0 ether0
192.168.0.1         0:d0:b7:85:bc:a0  UHLW     3       0 ether0  812
192.168.40.169/32   link#1             UC       0       0 ether0
192.168.40.188/32   link#1             UC       0       0 ether0
192.168.40.228      8:0:46:4d:60:40   UHLW     1      310 ether0  1125
```

show ntp

Purpose

Use **show ntp** to show the NTP configuration.

Options

The following options may be entered after **show ntp**.

blank	Show NTP configuration.
server N	Show NTP server. Where N = 1, 2 or 3.
server all	Show all NTP servers
status	Show whether the NTP daemon is up or down.

Notes

None.

Examples

show ntp

Show the NTP configuration, including the server and whether the NTP daemon is up or down.

show redirector N

Purpose

Use **show redirector N** to show the configuration for a specific redirector. This feature is only available on the E|X Web I/O Accelerator product line.

Options

The following options may be entered after **show redirector N**.

<blank>		Show the complete redirector configuration.
customURL		Show the customURL setting for the redirector.
dsr		Show the DSR status, i.e. if DSR is enabled or disabled.
host		Show the redirect hostname or IP address for the redirector.
listen	<blank>	Show redirector's listen configuration
	netmask	Show redirector's virtual IP netmask
	port	Show redirector's listen port
	ssl	Show redirector's listen SSL. See the following command for more detail: show redirector N listen ssl
	vip	Show redirector's virtual IP address
port		Show the port that requests will be redirected to.
protocol		Show the protocol that requests will be redirected to.
status		Show the status of redirector, i.e. if redirector is enabled or disabled.
URLmethod		Show the URLmethod setting of the redirector.

Notes

For a simple **show redirector 1**, the following output is obtained:

```
tx% show redirector 1
Redirector [1]
Listen Port: 80
Listen VIP: 192.168.113.114
Listen Netmask: 255.255.255.255
Listen SSL Status: disabled
Listen Protocol: sslv23
Listen Certfile:
Listen Keyfile:
Listen Keypass: none
Listen Ciphersuite: all
Listen Client Authentication: disabled
Listen CA Certfile:
```

```
Listen CA CRL File:  
Listen CA Trustfile:  
DSR Status: disabled  
Status: enabled  
Protocol: https  
Host: 192.168.113.114  
Port: 443  
URL Method: request  
Custom URL:
```

Examples

```
show redirector 1 listen ssl
```

Show redirector 1's listen SSL status

```
show redirector 1 customURL
```

Show redirector's custom URL string configured.

show redirector N listen ssl

Purpose

Use **show redirector N listen ssl** to show the configuration of redirector's SSL listen parameters for a specific redirector. This feature is only available on the E|X Web I/O Accelerator product line.

Options

The following options may be entered after **show redirector N listen ssl**.

<blank>	Show the redirector listen SSL configurations.
certfile	Show the redirector's listen SSL certfile
ciphersuite	Show redirector's listen SSL ciphersuite
keyfile	Show the redirector's listen SSL keyfile
protocol	Show the redirector's listen SSL protocol
status	Show the redirector's listen SSL status

Notes

The details on cipher suites are listed below. This can also be found in the *Setting up the T|X or E|X for SSL Traffic* chapter of the *Installation and Administration Guide*.

All SSL Ciphers

- RC4_MD5
- RC4_SHA
- DES_CBC_MD5
- DES_CBC_SHA
- DES_CBC3_MD5
- DES_CBC3_SHA
- EXP_RC4_MD5
- EXP_RC2_CBC_MD5
- EXP1024_RC4_MD5
- EXP1024_RC2_CBC_MD5

Common SSL Ciphers

- RC4_MD5
- RC4_SHA
- EXP_RC4_MD5
- EXP_RC2_CBC_MD5
- EXP1024_RC4_MD5
- EXP1024_RC4_SHA
- EXP1024_RC2_CBC_MD5

Export SSL Ciphers

- EXP_RC4_MD5
- EXP_RC2_CBC_MD5
- EXP1024_RC4_MD5

EXP1024_RC2_CBC_MD5

Strong SSL Ciphers

RC4_MD5

RC4_SHA

DES_CBC_MD5

DES_CBC_SHA

DES_CBC3_MD5

DES_CBC3_SHA

Examples

show redirector 1 listen ssl

Show redirector 1's listen SSL information.

show redirector 1 listen ssl ciphersuite

Show redirector 1's listen SSL ciphersuite settings

show route

Purpose

Use **show route** to show the routing table.

Options

None.

Notes

None.

Examples

show route

Show the route. Sample output:

```
se2200% show route
Default route: 192.168.0.1
[1] 66.12.13.5 192.168.0.10
[2] 66.12.14.0 192.168.0.11 255.255.255.0
```

[1] and [2] above represent the route number. This is used when deleting a route. The example above shows that the destination with IP address 66.12.13.5 can be reached via the gateway 192.168.0.10.

show server

Purpose

Use **show server** to show the server configuration.

Options

The following options may be entered after **show server**.

<blank>	Show server configuration.
customiplogheader	show custom header name that will be added to client's request with client's origin IP
failover	
maxconns	Show the maximum number of simultaneous connections that the TjX 2600 or 2650 can support. The maximum value is 500,000. Note that this option is only applicable for TjX 2600 or 2650.
status	Show if the server is up or down
stats	Show the stats of the server with the following information: <ul style="list-style-type: none"> ✓ Active and total number of sessions ✓ Active and total number of requests ✓ Total bytes in and bytes out See the command "show server stats" for more detail

Notes

Examples

```
show server stats
show server status
```

Display the statistics of the server
Display the status of the server, up or down.

show server stats

Purpose

Use **show server stats** to display the server statistics.

Options

The following options may be entered after **show server**.

<blank>	Display all server statistics, including I/O, HTTP and SSL statistics of the server.
io	Display all I/O statistics of the server.
http	Display all HTTP statistics of the server.
ssl	Display all SSL statistics of the server.

Notes

None.

Examples

show server stats	Display all statistics of the server
show server stats io	Display all I/O statistics of the server.
show server stats http	Display all HTTP statistics of the server.
show server stats ssl	Display all SSL statistics of the server.

show support

Purpose

Use **show support** to display the support contact information at Redline Networks, Inc.

Options

None.

Notes

Examples

show support	Display the phone number, email and web site address for Redline Networks, Inc support.
--------------	---

show timezone

Purpose

Use **show timezone** to show the time zone.

Options

The following options may be entered after **show timezone**.

<blank>	Show current time zone.
list	Show list of all time zones

Notes

The settings made by his command will take effect after a write operation.

Examples

show timezone	Show the current time zone.
show timezone list	Show a list of all time zones.

show vmstat

Purpose

Use **show vmstat** to show memory and CPU statistics.

Options

blank	Show memory and CPU statistics
N	Where N is an integer. Show CPU and memory statistics every N seconds.

Notes

This is the same as the “vmstat” command. Sample output is as follows:

```
procs      memory      page      disks      faults      cpu
r b w      avm      fre flt re pi po fr sr ad0 adl  in  sy  cs us sy id
0 0 0 362072 1678068 3100 0 0 0 2823 0 0 0 229 125 8 0 3 97
0 0 0 362072 1678068 5 0 0 0 0 0 0 0 233 48 9 0 0 100
0 0 0 362072 1678068 3 0 0 0 0 0 0 0 231 48 9 0 0 100
0 0 0 362072 1678068 3 0 0 0 0 0 0 0 232 48 9 0 0 100
0 0 0 362072 1678068 3 0 0 0 0 0 0 0 232 48 10 0 0 100
0 0 0 21644 2012164 68 0 0 0 83579 0 0 0 231 80 16 0 11 89
1 0 0 185964 1945584 16708 0 0 0 28 0 0 0 231 393 23 2 31 67
2 0 0 359016 1678308 67218 0 0 0 12 0 0 0 233 2169 19 7 43 50
```

Examples

show vmstat

Show memory and CPU statistics

show vmstat 1

Show memory and CPU statistics every 1 second.

tcpdump

Purpose

Use **tcpdump** to collect the TCP dump information to a file.

Options

None.

Notes

TCP dump consist of information useful for troubleshooting. You must configure the mechanism to deliver the dump and the filename for storing the TCP dump, if you are using tftp before executing this command.

```
set admin tcpdump filename <filename> (only needed for tftp)
set admin tcpdump (tftp | smtp)
```

Prior to Release 2.3, the TCP dump collected by the Web I/O Accelerator is encoded in base64. Starting from Release 2.3, the TCP dump collected is in binary format. The command for viewing the TCP dump content online is:

```
show tcpdump
```

TCP dump collected prior to Release 2.3 can be viewed offline after you decoded from the base64 format using a standard utility such as uudecode. Once decoded, it can be viewed with a standard TCPdump utility with the `-r` option. TCP dump collected with Release 2.3 or later can be viewed directly with a standard TCPdump utility.

Examples

tcpdump

Execute the `tcpdump` command and collect the dump information into a file.

tsdump

Purpose

Use **tsdump** to send the technical service dump to a tftp server or via email configured.

Options

None.

Notes

Technical Service dump consist of information useful for remote troubleshooting. You must configure the mechanism to deliver the dump and the filename for storing the technical service dump, if you are using tftp before executing this command.

set admin tsdump filename <filename> (only needed for tftp)

set admin tsdump (tftp | smtp)

Examples

tsdump

Execute the tsdump and send the information to the configured destination.

upgrade

Purpose

Use **upgrade** to download new firmware from a tftp server.

Options

None.

Notes

Another method to download pac file is to use the “install” procedure. Use the “install” procedure only if you would like to preserve the current version of the firmware. Use the “upgrade” procedure if you would like to download the firmware over the current version of the firmware. Make sure that the correct pac file is used as the pac file for “upgrade” is different from the one for “install”. Note that the pac file for “upgrade” operation is approximately 3M bytes where the pac file for “install” is approximately 10M bytes.

The tftp server and the filename to upgrade from must be set

- set admin tftp server <tftp server>
- set admin upgrade <pac file filename>.

Examples

upgrade Upgrade from a TFTP server.

vmstat

Purpose

Use **vmstat** to show memory and cpu statistics.

Options

blank	Show memory and CPU statistics
N	Where N is an integer. Show CPU and memory statistics every N seconds.

Notes

This is the same as the “show vmstat” command. Sample output is as follows:

```
procs      memory      page      disks      faults      cpu
r  b  w      avm      fre flt re  pi  po  fr  sr  ad0  ad1  in  sy  cs  us  sy  id
0  0  0    362072  1678068 3100  0  0  0 2823  0  0  0  229 125  8  0  3  97
0  0  0    362072  1678068   5  0  0  0  0  0  0  0  233  48  9  0  0 100
0  0  0    362072  1678068   3  0  0  0  0  0  0  0  231  48  9  0  0 100
0  0  0    362072  1678068   3  0  0  0  0  0  0  0  232  48  9  0  0 100
0  0  0    362072  1678068   3  0  0  0  0  0  0  0  232  48 10  0  0 100
0  0  0     21644  2012164  68  0  0  0 83579  0  0  0  231  80 16  0 11  89
1  0  0    185964  1945584 16708  0  0  0  28  0  0  0  231 393 23  2 31  67
2  0  0    359016  1678308 67218  0  0  0  12  0  0  0  233 2169 19  7 43  50
```

Examples

vmstat

Show memory and cpu statistics

vmstat 1

Show memory and CPU statistics every 1 second.

wall

Purpose

Use **wall** to write a message to all users who are currently logged in to the Web I/O Accelerator.

Options

None.

Notes

None.

Examples

wall please log off now rebooting in 2 mins...

Write the message “please log off now, rebooting in 2 minutes...” on the console to all users who are logged in.

who

Purpose

Use **who** to display a list of other people logged in.

Options

None.

Notes

None

Examples

who

Display a list of who is logged on. Example of output:

```
tx2200% who
rlshell          tty0    Nov  5 13:35  (dhcp-228)
```


Appendix A: Glossary

"Busy" Redirect	If the Target web server responds with a "Busy" error, the Web I/O Accelerator will serve the page specified by this URL instead.
Certfile	Certification file for SSL traffic.
Cipher	Cryptographic algorithm for a server and client to authenticate each other, transmit certificates, and establish session keys.
Ciphersuite	A set of ciphers.
Cluster	A set of web servers
Convert302protocol	Convert the 302 responses from http to https or from https to http.
Customiplogheader	A special header to annotate the log; showing the session that is being logged in an easily identifiable way.
DNS Domain	Also known as the Domain Suffix, this will be used to resolve unqualified hostnames
DNS Nameserver	IP address of the primary name server for the Web I/O Accelerator. This is the machine the Web I/O Accelerator queries to resolve hostnames into IP addresses
DSR	Reduces traffic by allowing web servers to send HTTP responses directly back to the requesting client, thus bypassing the load balancer in the response path.
Ethernet 0 (ether0)	This is the primary ethernet port of the Web I/O Accelerator and the interface through which web traffic travels.
Ethernet 1 (ether1)	Also known as the "Heartbeat" port, Ethernet 1 is used to communicate with a second Web I/O Accelerator configured as a cold-standby fail-over unit.
Farm	A set of web clusters, typically with each cluster serving a different purpose.
Fail-over	This specifies whether or not the Web I/O Accelerator should act as a cold-standby fail-over unit for another Web I/O Accelerator on the network.
Forwarder	A host for forwarding traffic. This is for non-HTTP traffic; the forwarder simply sends the traffic on without examining it.
Hostname	The fully qualified DNS name for the Web I/O Accelerator.
Keyfile	Key file for SSL traffic.
Keypass	Password for SSL key.

Listen Port	The port on which the Web I/O Accelerator listens for incoming web traffic. This should usually be set to 80.
Log Host	The IP address of the server to which the Web I/O Accelerator will be sending logging data.
Logging	Turns logging on or off. Remember that logging always exacts a performance penalty.
Media	Media is the mode in which an ethernet interface (ether0 and ether1) operates.
Netmask	A mask to filter out addresses that should not access the device.
NTP	Network Time Protocol. Specifies whether or not the Web I/O Accelerator should listen for your NTP server.
Rendex	
Route (Default)	Also known as the "Gateway," this is the IP address of the machine the Web I/O Accelerator talks with in order to access the outside world
Server	Web I/O Accelerator service.
Sticky	Ties a client to a server via cookie or the client's IP address.
Target Host:Port	This is the IP address and accompanying port of the web server that the Web I/O Accelerator will accelerate. Depending on the Web I/O Accelerator model, you may be able to enter IP addresses and ports for up to 8 Target Hosts.
Target Name	This is the fully-qualified hostname which clients use to reach your website/the servers you are accelerating.
Web I/O Accelerator Statistics	The following Web I/O Accelerator Statistics are available: <ul style="list-style-type: none"> • <i>Uptime</i>: The elapsed time since the Web I/O Accelerator was turned on. • <i>Sessions (active/total)</i>: The number of TCP sessions that the Web I/O Accelerator has handled • <i>Requests (active/total)</i>: The number of HTTP requests the Web I/O Accelerator has received • <i>Bytes (in/out)</i>: The total amount, in bytes, of data the Web I/O Accelerator has received from target hosts and the total amount of data that the Web I/O Accelerator has sent out to clients.
Virtual IP Address	This is the IP address to which all incoming web traffic should be routed. It should be different from the IP address(es) you specified on the Network Settings page.
Virtual IP Netmask	The proper subnet mask for a device with the given Virtual IP Address.

Web Administration
Manager (WAM)

The Web interface for administering the Web I/O Accelerator. See the *Installation and Administration Guide* for more information.

Appendix B: List of Events

EMERG Events

"T|X Server was started"
 "Not licensed for this device"

ALERT Messages

"the admin password has been changed by pressing the reset button."
 "T|X rebooted from CLI."
 "Target Server <target_server> disabled through configuration."
 "admin password changed."
 "Cannot contact Default Gateway <gateway>."
 "Cannot contact DNS server <dns_server>."
 "Cannot contact NTP server <ntp_server>"
 "Cannot contact TFTP server <tftp_server>"
 "Cannot contact syslog host <syslog_host>"
 "Target Server <target_server> failed layer 7 health check."
 "Illegal Content-Length header of <length> sent from "target_server" for request <url_requested>"
 "Illegal reply from <target server> (HTTP <http version>) for request <url_requested> (no Content-length/chunking/Connection: Close)."
 "Illegal reply from <target server> (HTTP <http version>) for request <url_requested> (no Content-Length/Keep-Alive set)."
 "Bad HTTP request: HEAD/0.9"
 "Bad HTTP request: POST request did not contain content length. Request line: <POST request_line>"
 "Bad HTTP request: POST has length less than 0. Request line: <POST request_line>"
 "Bad HTTP request: POST request specified content length of zero and not configured to allow this."
 "TX received excessive bytes from target <target_server> for request <url_requested>"
 "Bad HTTP request: Header line longer than allowed or poorly formed"
 "Bad HTTP request: Client sent an invalid Header line: <http_header_line>"

"VIP <vip> Down"

"VIP <vip> Up"

"Can't upgrade: archive is <number_of_bytes> Kb. flash has <number of bytes> avail."

"bad or missing private key file. <keypath> password not set."

Index

"Busy" Redirect		Log Host	
definition	163	definition	164
add	6, 7	Logging	
Certfile		definition	164
definition	163	Media	
Cipher		definition	164
definition	163	Netmask	
Ciphersuite		definition	164
definition	163	NTP	
clear clusterN	12, 13, 14, 17, 20	definition	164
clear dns	15, 18	ping	40
clear forwarderN	11, 16	reboot	42
clear ntp serverN	19	reload	43
clear server	21	Rendex	
cls	22	definition	164
Cluster		rollback	45
definition	163	Route (Default)	
configure	23	definition	164
Convert302protocol		Server	
definition	163	definition	164
Customiplogheader		set admin	46, 47, 48, 53, 60
definition	163	set clusterN convert302protocol	63, 64, 65
DNS Domain		set clusterN dsr	66
definition	163	set clusterN listen	69, 85, 86
DNS Nameserver		set clusterN listen SSL	70, 72, 87, 118, 120,
definition	163	121, 122, 123, 136, 137, 145	
DSR		set clusterN log	9, 24, 26, 28, 30, 35, 36, 44,
definition	163	78, 133	
Ethernet 0 (ether0)		set clusterN sticky	74
definition	163	set clusterN target	67, 75
Ethernet 1 (ether1)		set clusterN target SSL	76
definition	163	set date	62
exit	29, 41	set dns	79
Failover		set etherN	80
definition	163	set forwarderN	81
Farm		set hostname	82
definition	163	set ntp	83
Forwarder		set password	84
definition	163	set route	89
gen	31, 38	set server	90
Glossary	163, 167	set server customiplogheader	91
help	32	set server failover	92
Help on Commands	5	set snmp	51
history	34	set ssh	52
Hostname		set telnet	55
definition	163	set tftp	50, 56, 59
Keyfile		set timezone	94
definition	163	show admin	95, 107
Keypass		show clusterN	113, 143
definition	163	show commands	116, 125
Listen Port		show config	126, 129
definition	164	show dns	131

show etherN.....	132	definition	164
show flash.....	134	TjX Statistics	
show forwarderN	135	definition	164
show hostname	138	Target Host:Port	
show log ...109, 110, 139, 150, 151, 156, 157		definition	164
show netstat.....	39, 140	Target Name	
show ntp	141, 142	definition	164
show route	147	upgrade	158
show server.....	148, 149	Virtual IP Address	
show snmp	99	definition	164
show ssh.....	100	Virtual IP Netmask	
show telnet	103	definition	164
show tftp .58, 97, 98, 101, 102, 104, 105, 106		Web Administration Manager (WAM)	
show timezone	152	definition	165
show ua	153	Web Interface for TjX Web I/O Accelerator .5	
show vmstat	154, 155, 159	who.....	161
Sticky		write.....	162