Symantec Reporter 10.5.1.1

Command Line Interface Reference

Updated: Friday, February 28, 2020

A Division of Broadcom

Legal Notice

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Friday, February 28, 2020

Table of Contents

Reference: CLI

> **Note:** For Reporter 10.3 and later go to this page.

The Reporter CLI provides a set commands through a serial console that allows you to manage and change networking settings (IP, Mask, Gateway, DNS), configure / change username / password, and generate SSL self-signed certificate.

```
--------------------MENU--------------------
1) Command Line Interface
2) Setup console
--------------------------------------------
Enter option:
```

Option **2** begins the guided setup, as described in Install Reporter on a Virtual Appliance.

Option **1** enters basic CLI mode.

Command	Sub-Commands	Description

CLI Behavior and Command Changes

The following commands have been changed or their behavior has been modified in Reporter 10.3.

New Command	Old Command	Version	Description / Behavior Change
`licensing`	`license`	**10.3** and later	`licensing` replaced the `license` command.
`shutdown`	`shutdown graceful`	**10.3** and later	`shutdown graceful` is no longer available. `shutdown` will perform a graceful shutdown.

Standard Mode Commands

The following commands are available in standard mode, the mode after logging in to the CLI, The > prompt indicates standard mode.

To see a list of commands available in standard mode, type **`help`** or **?** at the > prompt.

enable

Enter the elevated privilege mode, known as *enable mode*. You will be prompted to enter the enable password.

Syntax

```
> enable
```

Notes

- When enable mode is turned on, the prompt changes from **>** to **#**,
- To return to standard mode, use the **`disable`** command.

quit

Exit the management session.

Syntax

```
> quit
```

show

Display information about the system and settings.

> **Note:** These commands are available in standard and enable modes.

Syntax

```
(config)# show ?
```

`appliance-csr`	Show appliance certificate signing requests (CSR).

`banner-message`	Display pre-authentication consent banner message
`banner-status`	Display pre-authentication consent banner status (enabled vs. disabled).
`cli`	Display CLI-related settings, such as complete-on-space, idle-timeout, and history.
`clock`	Display current date and time (local and UTC) and timezone.
`configuration commit changes`	Display committed configuration changes.
`configuration rollback changes`	Display configuration changes that were rolled back.
`full-configuration`	Display current configuration. This displays the same output as the **`show running-configuration`** command in standard/enable mode. **Note:** When in a configuration mode, such as authentication or SSL mode, the **`show full-configuration`** command shows just the settings applicable to the mode.
`hardware-configuration`	Display system hardware configuration details, such as amount of RAM, number of CPUs, and NIC speed.
`history`	Display a list of previously-entered CLI commands.
`licenses`	Show license components, including subscription services. For each component, the activation and expiration dates are listed.
`login-banner message | status`	Show the currently defined login banner message and feature status (enabled vs. disabled). See "login-banner" on page 23.
`password-policy-configuration`	Display current settings for password policy, such as minimum password length. See password-policy.

`reboot_reason`	Show the reason the appliance was last rebooted. Possible reasons include:
	`Reboot_requested`
	`Shutdown_requested`
	`Halt_requested`
	If an unexpected reboot occurs (for example, when the system reboots on its own or the plug is pulled), the reason is listed as **`Unknown`**.

`running-config`	Display current configuration.
`ssl ca-certificate | certificate | keypair | keyring | signing-request`	Display certificate details.
`statistics`	Display system statistics.
`timezone`	List supported timezones.
`version`	List the software version and release ID, appliance serial number, and the MAC address.

show raid

Display RAID configuration information.

Syntax

```
> show raid ?
```

array [*<raid_name>*]	Display the state of the RAID array *<raid_name>*, or state of all RAID arrays if a raid name is not specified.
members [*<raid_name>*]	Display hard disk drives that are part of the RAID *<raid_name>*, or all hard drives in the system if a raid name is not specified.
spares	Display all spare hard disk drives available in the system.

Examples

```
# show raid array
+-------------+-------------+----------------------------+-------------------+
| RAID name   | RAID level  | RAID size(used/total)      | RAID state        |
+-------------+-------------+----------------------------+-------------------+
| casma_raid  | raid10      | (1000.07 GB / 3000.21 GB)  |    active        |
|             |             |                            | 100% completed    |
+-------------+-------------+----------------------------+-------------------+
# show raid members
RAID name: casma_raid
Location    State
slot6       active sync set-A
slot1       active sync set-B
slot2       active sync set-A
slot3       active sync set-B
slot4       active sync set-A
slot5       active sync set-B
```

Enable Mode Commands

The following commands are available in enable mode. Enable is a privileged mode that requires its own password.

To enter enable mode, type **`enable`** at the standard command prompt (>) and enter the password. The prompt will change to #. To see a list of commands available in enable mode, type **`help`** or **`?`** at the # prompt.

access-logs

List or delete access-log files. This command is available in both the `enable` and `config` modes.

Syntax

```
# access-logs
```

`delete`	Delete one or more log files
`list-dirs`	List access-log directories
`list-files`	List access-log files in the specified directory

Example

```
# access-logs list-files <directory>
```

authentication

Enable and disable user lockout. To change passwords or manage security settings use the *config* command "authentication" on page 35.

Syntax

```
# authentication ?
```

`disable-user-lockout`	Disable lockouts for all users
`enable-user-lockout`	Enable lockouts for all users; lockout is for 15 min after five failed login attempts

Example

```
# authentication enable-user-lockout
```

backup-settings

Saves a backup of the Reporter configuration in the `/.settings.backups/` file directory used by FTP and SCP. The system saves the settings to a .zip file.

After executing the `backup-settings` command, you can use FTP or SCP to move backup files to and from the file directory. For example, you can create a settings backup file on one Reporter appliance, copy it to your FTP server, and then move it to the `/.settings.backups/` folder on a different Reporter appliance.

> **Caution:** The backup settings can only be restored onto a Reporter that is running the same version that was running when the backup was created. It is highly recommended that you create a new backup every time you upgrade to a new Reporter version.

Syntax

# **`backup-settings`** *Settings backup name*

The backup-settings command takes a name as the only variable.

Examples

Backup the Reporter configuration to a file called L4_Backup:

```
# backup-settings L4_Backup
Backing up settings to L4_Backup
Backup succeeded.
```

clock

Manually set the time and date of the appliance in Coordinate Universal Time (UTC). This command is available in both the `enable` and `config` modes.

Syntax

```
# clock day <value>|hour <value>|minute <value>|month <value>|second <value>|year <value>
```

Each value must be entered as a separate command.

Examples

To set the date to September 2, 2016:

```
# clock day 2
```

```
# clock month 9
```

```
# clock year 2016
```

> **Note:** If you are using an NTP server, you do not need to manually set the clock.

clone

Copy Reporter 9.x configuration files onto a Reporter 10.x appliance.

See Clone Migration in the *Reporter 10.x Administration Guide* on **support.symantec.com** for instructions.

configuration-management

Manage saved configuration files. This command is available in both the `enable` and `config` modes.

Syntax

```
(config)# configuration-management <argument>
```

`copy`	Copy a saved configuration
`delete`	Delete a saved configuration
`list`	List saved configurations
`load`	Load a saved configuration
`save`	Save a configuration and give it a name
`status`	Show status of loaded configurations

Example

```
(config)# configuration-management save <string>
```

configure

A command to enter a mode in which CLI commands are available for changing the configuration of the software and appliance.

Syntax

```
# configure
```

Notes

- When in configure mode, the command prompt changes to: `(config)#`
- Type **?** to see a list of CLI commands available in configure mode.
- Type **`exit`** to disable configure mode. The command prompt changes to: #

dbbackup

Create database backups; update and delete backups; restore a database from backup.

Syntax

```
# dbbackup [list] [create | delete | restore | update] [<index number>]
```

`create`	Create new database backup
`delete`	Delete database backup
`list`	Show available database backups. Specify the operation for which you want the list.
`restore`	Restore a database from the specified backup. You must run **`stop-reporter`** before this command.
`update`	Update existing database backup. To create a stable backup run **`stop-reporter`** first.

Examples

Create a backup for DB1:

```
# dbbackup list create

   1   "DB1"

   2   "DB2"

# dbbackup create 1
```

Delete one of the DB1 backups.

```
# dbbackup list delete

   1   20181130-205009  done  stable    "DB1"

   2   20181130-213937  done  stable    "DB1"

   3   20181130-215951  done  unstable  "DB1"

# dbbackup delete 3
```

Restore DB1 from one of its backups

```
# dbbackup list restore

   1   20181130-205009  done  stable    "DB1"

   2   20181130-213937  done  stable    "DB1"

# dbbackup restore 2
```

diagnostics

Provide access to the appliance or submit troubleshooting information to Symantec Support to help diagnose hardware or software issues.

Syntax

```
# diagnostics ?
```

`activate-remote-access`	Activate remote diagnostics access so that Symantec Support can help troubleshoot an issue on your appliance.
`heartbeat disable|enable|view|send`	Enable/disable the sending of heartbeat data to Symantec; view current heartbeat report or configuration; send report to Symantec.
`service-info save-core`	Create a snapshot core file, similar to that created when Reporter terminates unexpectedly. The snapshot core file will be included in subsequent `diagnostics service-info export` or `send` operations. The `save-core` operation is useful for times when Reporter seems unresponsive, for example, when you execute the `stop-reporter` command but the Reporter process does not shut down. Notes: ▪ If the CLI is unavailable, run the `save-core` command from another SSH session or from the serial console. ▪ If the Reporter process is not running when this command is issued, the `save-core` operation aborts. ▪ The `save-core` operation might take some time to complete if the appliance has a large database.
`service-info send-sr` ***`<service request number>`***	Generate and upload the service diagnostics information to Symantec using the case number of your support case.
`service-info send-url` ***`url`***	Generate and upload the service diagnostic information to a remote server via URL.

`service-info export`	Copy diagnostic information to a subdirectory called `.diags` at the root of the FTP access logs directory.
	List the exported files using the following command:
	`# access-logs list-files .diags`
	After you have exported the diagnostic information, upload it normally using the following commands:
	`# diagnostics service-info send-sr`
	`# diagnostics service-info send-url`

Examples

```
# diagnostics heartbeat send
# diagnostics service-info send-sr 123456789
```

diagnostic-systems

This command is not present in the virtual appliance deployment of Symantec Reporter.

Manage diagnostic images installed on the system. Up to six images can be installed on the system. If your system already has six images installed and you add another image, the oldest unlocked image will be replaced with the new image, unless you have designated a particular image to be replaced.

Syntax

```
# diagnostic-systems ?
```

cancel	Cancel the download process of an image that is currently downloading
delete ***<image#>***	Delete an image from the system. Use the **diagnostic-systems view** command to identify the image number to delete. Note: You cannot remove a locked image or the current running image.
load ***<URL>***	Download and install a diagnostic image on the system. *<URL>* is the path to an image on a web server that the appliance has access to. Example: http://webserver.mycompany.com/images/diag.bcs
lock ***<image#>***	Lock a diagnostic image to protect it from accidental deletion.
replace ***<image#>***	Designate which image will be replaced next (if the system already has six installed images and you load another image). If you do not specify an image to be replaced, the oldest unlocked image on the system will be replaced.
unlock ***<image#>***	Unlock a diagnostic image that you no longer want to protect from deletion. You have to unlock a locked image before you can remove it.
unset-replace	Unset image to be replaced next. When a replacement image is not designated, the oldest image will be replaced when you load a seventh image.
view	Show a list of installed diagnostic images along with their image numbers, software versions, release IDs, whether the image is locked or unlocked, whether it has ever been booted, creation date/time, and boot date/time. The summary at the bottom of the list indicates which image number is the current running system, the default system to run the next time the appliance is restarted, and the image number that will be replaced next.

Example

```
# diagnostic-systems load http://webserver.mycompany.com/images/diag.bcs
```

disable

Return to standard mode.

Syntax

```
# disable
```

When enable mode is turned off, the prompt changes from **#** to **>**,

display-level

Set the depth of the configuration that is shown by the **`show full-configuration and show running-configuration`** commands. For example, if the display-level is set to 1, only top-level configuration nodes and their values are shown. If it is set to 2, then top-level nodes and their child nodes are shown, and so on. By default, the entire configuration is shown.

Syntax

```
# display-level [level<n>]
```

Examples

```
# display-level 1
```

event-log

Manage syslog settings. The syslog feature gives administrators a way to centrally log and analyze events on the system. This command is available in both the `enable` and `config` modes.

Syntax

```
(config)# event-log
```

> **Note:** You can add multiple syslog servers.

`level` ***`<value>`***	Set the level to specify which messages to suppress to the syslog server. For example, setting the level to 3 allows messages with levels 0 - 3 and suppresses messages with levels 4 - 7. **`<value>`** can be one of the following: **0** Emergency: system is unusable **1** Alert: action must be taken immediately **2** Critical: critical conditions **3** Error: error conditions **4** Warning: warning conditions **5** Notice: normal but significant condition **6** Informational: informational messages **7** Debug: debug-level messages

`syslog add host <host> port <port>`	Configure a syslog server where *`<host>`* is the host name or IP address of the syslog server. Optionally, you can also specify a custom port, where *<port>* is the port number.
`syslog add udp host <host> port <port>`	Configure a syslog server using UDP where *`<host>`* is the host name or IP address of the syslog server. Optionally, you can also specify a custom port, where *<port>* is the port number.
`syslog remove host <host>`	Remove a configured syslog server by specifying the *<host>*.
`syslog clear`	Removes all configured syslog servers.
`view`	View syslog settings

> **Note:** The sub-commands listed above can either be entered in event-log configuration mode (at the `config-event-log` prompt, or in configuration mode (at the `config` prompt).

Examples

```
(config)# event-log
(config-event-log)# syslog add udp host 203.0.113.17
Added syslog server host 203.0.113.17:514.
(config-event-log)# view
Log level: 5 (notice)
Remote syslog servers:
       203.0.113.17:514
```

exit

Exit from current mode.

For example, if you are in configuration mode, **`exit`**returns you to enable mode. If you are in health-monitoring mode, **`exit`** returns you to configure mode.

Syntax

```
exit
```

> **Note:** If you type **`exit`** when you are in standard or enable mode, the management session is closed.

Example

```
(config-authentication)# exit
(config) # exit
#
```

# ftp | ftps

Manage the local FTP and FTPS servers. The FTP(S) server must first be configured in the web UI.

Syntax

# [ftp | ftps] <argument>

`edit`	Modify the FTP(S) daemon configuration file
`pasv-ports`	Set the range of passive ports available for FTP(S)
`restart`	Restart the FTP(S) daemon
`start`	Start the FTP(S) daemon
`stop`	Stop the FTP(S) daemon

Example

```
# ftps edit
#...
# daemon options
listen=YES
session_support=NO
#
# login options and access controls
anonymous_enable=NO
ftpd_banner=Welcome to the Reporter FTP service.
local_enable=YES
pam_service_name=vsftpd
tcp_wrappers=YES
#...valid user must be in the list
"etc/nossl_vsftpd.conf" 103 lines, 2513 characters
#...
# daemon options
listen=YES
session_support=NO
#
# login options and access controls
anonymous_enable=NO
ftpd_banner=Welcome to the Reporter FTP service.
local_enable=YES
pam_service_name=vsftpd
tcp_wrappers=YES
#...valid user must be in the list
userlist_deny=NO
userlist_enable=YES
userlist_file=/etc/vsftpd/nossl_user_list
userlist_log=YES
#
```

```
# anonymous user options
ftp_username=no_anonymous_ftp_user
#...
#
# daemon options
listen=YES
session_support=NO
#
# login options and access controls
anonymous_enable=NO
ftpd_banner=Welcome to the Reporter FTP service.
local_enable=YES
pam_service_name=vsftpd
tcp_wrappers=YES
#...valid user must be in the list
userlist_deny=NO
userlist_enable=YES
userlist_file=/etc/vsftpd/nossl_user_list
userlist_log=YES
#
# anonymous user options
ftp_username=no_anonymous_ftp_user
#
# umask and permission modes
# (restrict to minimal access including few execution bits)
anon_umask=007
local_umask=007
file_open_mode=0660
chown_upload_mode=0660
#
# local user options
chmod_enable=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/nossl_chroot_list
chroot_local_user=NO
guest_enable=YES
guest_username=rpt_data
local_root=/data/bluecoat/accesslogs
#local_umask=022
passwd_chroot_enable=NO
allow_writeable_chroot=YES
#
```

halt

Halts the operating system and stops all CPUs. Once the system is cleanly halted, the user may safely press the SSL Visibility power switch to turn off the appliance.

Syntax

```
# halt
```

> **Note:** The **halt** and **shutdown** commands are similar; the only difference is that **shutdown** disconnects the power via the CLI command.

health-monitoring

View Health Monitoring (HM) events and status, and view and change HM settings. This command is available in both the `enable` and `config` modes.

Syntax

```
(config-health-monitoring)# ?
```

clear-history	Clear the entire event history **product1234-10414124(config-health-monitoring)# clear-history** **Event history has been cleared for all metrics.**
history-duration	Sets the number of days that the HM framework is to store its history of events. ▪ It takes one argument, an integer representing the number of days. ▪ Default value is 30. ▪ Once per day, the HM framework clears the event history of all events older than the specified number of days. **product1234-10414124(config-health-monitoring)# history-duration** **(<int>) (30): 60** This option is available only in config mode.
view	Show health status and metric settings. See "health-monitoring view " on page 39.

history

Specify how far back in the command history previously-entered commands can be retrieved. For example, with a history size of 5, the previous five commands can be retrieved. Each time you press the up arrow, a previously-entered command is displayed.

> **Note:** When using the up arrow to retrieve previously-entered commands that use passwords, password values are obscured with asterisks.

Syntax

```
# history <size>
```

installed-systems

Manage images installed on the system. Up to six images can be installed on the system. If your system already has six images installed and you add another image, the oldest unlocked image will be replaced with the new image, unless you have designated a particular image to be replaced.

> **Caution:** Only customers with a valid support contract can upgrade to major releases. If your support contract has expired, the image installation will fail. Note that you can still upgrade to maintenance releases for the current version.

Syntax

```
# installed-systems ?
```

cancel	Cancel the download process of an image that is currently downloading
default ***<image#>***	Specify the image that will be run the next time the system is restarted. Tip: Use the **installed-systems view** command to identify the image number.
delete ***<image#>***	Delete an image from the system. Use the **installed-systems view** command to identify the image number to delete. Note: You cannot remove a locked image or the current running image.
load ***<URL>***	Download and install an image on the system. *<URL>* is the path to an image on a web server that the appliance has access to. Example: http://webserver.mycompany.com/images/542386.bcs **Note:** Image loading will fail if the appliance does not have a license installed or if your support contract has expired.
lock ***<image#>***	Lock an image to protect it from accidental deletion.
replace ***<image#>***	Designate which image will be replaced next (if the system already has six installed images and you load another image). If you do not specify an image to be replaced, the oldest unlocked image on the system will be replaced.

`unlock <image#>`	Unlock an image that you no longer want to protect from deletion. You have to unlock a locked image before you can remove it.
`unset-replace`	Unset image to be replaced next. When a replacement image is not designated, the oldest image will be replaced when you load a seventh image.
`view`	Show a list of installed images along with their image numbers, software versions, release IDs, whether the image is locked or unlocked, whether it has ever been booted, creation date/time, and boot date/time. The summary at the bottom of the list indicates which image number is the current running system, the default system to run the next time the appliance is restarted, and the image number that will be replaced next.

Examples

```
# installed-systems view
1. Version : 2.0.0.0, Release ID : 218372, Locked : false, Booted : true BuildType : Debug,
CreationTime : 2018-05-07T23:07:05+0000, BootTime : 2018-05-08T14:03:08.153+0000 DisplayName : Blue
Coat Management Center 2.0.0.0, Release ID: 218372
2. Version : 1.11.1.3, Release ID : 211560, Locked : true, Booted : true BuildType : Debug,
CreationTime : 2017-12-18T16:30:01+0000, BootTime : 2018-05-04T14:54:30.888+0000 DisplayName : Blue
Coat Management Center 1.11.1.3, Release ID: 211560
Default system to run on next hardware restart: 1
Current running system: 1
System to replace next: None
# installed-systems load http://webserver.mycompany.com/images/542386.bcs
```

licensing

Configure licensing, including the loading of licenses on to the appliance. This command is available in both the `enable` and `config` modes.

Syntax

```
(config)# licensing
```

```
(config-licensing)#
```

`inline license-key [passphrase <value>]`	Import a license from terminal input (typically by pasting the license content with a right-click). Include the **`passphrase`** to decrypt the private key if the license has birth-cert and birth-key in it. Press Ctrl-D after pasting the certificate content.

`load [username <value>] [password <value>]`	Enter your MySymantec credentials to download the appliance license from the Network Protection Licensing Portal (NPLP). **Note**: MySymantec credentials are required only for Management Center virtual appliances and Reporter appliances.
`load url` ***`<url>`*** **`passphrase`** ***`<value>`***	Download a license from the specified URL.
`view [status|configuration]`	Display the license install status or licensing configuration details.

> **Note:** The sub-commands listed above can either be entered in licensing configuration mode (at the `config-licensing` prompt or in configuration mode (at the `config` prompt).

Examples

To load a license from a URL other than NPLP:

```
(config)# licensing load http://test.server.com/license.txt
```

To view the currently installed license:

```
(config-licensing)# view
Appliance Serial Number : 1000xxxxxx

Licensable component information:
Serial Number       : 0000xxxxxx
Part Number         : 000-00000
Expiration Date     :
Expiration Type     : Perpetual
Product Description : Reporter VA, up to 2TB HDD, Yr Subscription
Activation Date     : 2019-10-23
Component Name      : Reporter
```

login-banner

Configure a banner message to appear before users log in to the appliance. The message will appear before users log in to the CLI (via serial console and SSH) . This feature meets the security technical implementation guideline STIG V-3013. Messages can contain up to 2,047 characters and can be defined using multi-byte UTF-8 characters.

Syntax

```
# login-banner ?
```

`disable`	Disable the login banner message.

enable	Enable the login banner message. (You cannot enable the feature until you define the message.)
inline message	Define the login banner message. You will be prompted to enter the message text and press Ctrl-D when finished.
view message | status	Show the currently defined message and feature status (enabled vs. disabled).

Examples

```
# login-banner inline message
Enter the login banner message below and end it with a Ctrl+D
This is a banner message.
ok
# login-banner enable
# login-banner view message
This is a banner message.
# login-banner view status
Login banner is enabled.
```

logout

Log out the current user. The management session is ended.

Syntax

```
# logout
```

pcap

Capture packets that are sent to and/or from the appliance. The captured data can be imported into a packet analysis tool such as Wireshark. This command is available in both the `enable` and `config` modes.

Syntax

```
# pcap ?
```

start	Start capturing packets.
stop	Stop capturing packets.
transfer *<full-url/filename> <username> <password>*	Copy captured data to an FTP site. While not necessary, Symantec recommends that you use **pcap stop** before using this command.
filter direction [both|in|out]	Filter packets by direction.
filter interface *<nic>*	Filter packets by interface number (0:0, 1:0, 1:1)

Before enabling packet capture, you can optionally restrict the packets that are captured by filtering by direction (in or out) or filtering by interface (for example, just packets sent out of the 1:0 NIC.

After capture is turned on, the system will create a .dmp file in TCPDump format and start capturing packets into this file.

Packets are captured until capturing is disabled with the **pcap stop** command, or after 30 minutes, whichever comes first.

Examples

```
(config)# pcap filter direction in
(config)# pcap start
(config)# pcap stop

(config)# pcap transfer ftp://example.com/john_files/test.dmp john.smith ******
```

ping

Generate pings to test connectivity with another device on the network. If the device answers the pings, a message displays such as *5 packets transmitted, 5 received, 0% packet loss, time 3007ms*. If the appliance is unable to connect with the other device, the system displays a message such as "*5 packets transmitted, 0 received, 100% packet loss, time 13999ms*."

Syntax

```
# ping ipv4|ipv6 source <source ip address>dont-fragment repeat <ping count>size <packet size><ip address>|<hostname> ?
```

ipv4|ipv6	Explicitly force an IPv4 or IPv6 ping. When an IP version isn't specified, the program will try to resolve the name given, and choose the appropriate protocol automatically. If resolving a host name returns both IPv4 and IPv6 addresses, ping will use IPv4.
source *<source ip address>*	The source IP address to put in the ping packet
repeat *<ping count>*	The number of ping packets to send. The default is 5.
size *<packet size>*	The size of the ping packets (in bytes). The default is 100 bytes.
dont-fragment	Set the dont-fragment flag on the ping packets.
<ip address>*|*<hostname>	The destination to ping. This is the only required ping parameter.

Examples

```
# ping repeat 3 size 50 cnn.com
PING cnn.com (198.51.100.122) 50(78) bytes of data.
58 bytes from www.cnn.com (198.51.100.122): icmp_seq=1 ttl=115 time=63.2 ms
58 bytes from www.cnn.com (198.51.100.122): icmp_seq=2 ttl=115 time=62.8 ms
58 bytes from www.cnn.com (198.51.100.122): icmp_seq=3 ttl=115 time=62.9 ms
```

```
--- cnn.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2066ms
rtt min/avg/max/mdev = 62.880/63.022/63.268/0.338 ms
# ping 203.0.113.17
PING 203.0.113.17 (203.0.113.17) 100(128) bytes of data.
--- 203.0.113.17 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 13999ms
```

restart

Reboots the system and restarts services such as image, licensing, subscription, SNMP, and health monitoring. You will need to restart the system after upgrading to a new image or changing the running image on the appliance.

Syntax

```
# restart
```

restore-defaults

Restore system to factory default settings. This process deletes all data on the appliance.

Syntax

```
# restore-defaults factory-defaults [halt|shutdown] [force]
```

halt	After the system is restored to factory defaults, the operating system is halted and CPUs are stopped.
shutdown	After the system is restored to factory defaults, the operating system is halted, CPUs are stopped, and the appliance is powered off.
force	The user is not prompted to confirm the action.

Examples

```
#restore-defaults factory-defaults
```

```
Restoring box to factory state. This will delete all customer data and shutdown the system. Do you
want to proceed (yes/no):
```

If the user responds with y (for yes), the system will be restored to factory defaults and all customer data will be wiped from the drives.

```
#restore-defaults factory-defaults shutdown force
```

The user is not asked to confirm the action; the system is restored to factory defaults and then powered down.

Caution: After restoring factory defaults, verify that RAID is not performing a re-sync before starting Reporter (`start-reporter`).

restore-settings

Restore Reporter from a backed-up state. Before restoring a Reporter configuration, you must stop the reporter service.

> **Caution:** The backup settings can only be restored onto a Reporter that is running the same version that was running when the backup was created. It is highly recommended that you create a new backup every time you upgrade to a new Reporter version.

> **Note:** You can also create and manage the automatic backup sets with "configuration-management" on page 36.

Syntax

```
# restore-settings ?
```

automatic	Allows you to view and restore the available, automatically backed up settings sets.
manual	Allows you to view or restore the available settings .zip files in the `/.settings.backups/` folder. These .zip files are created using the command "backup-settings" on page 10.

Examples

```
# restore-settings manual list
Available backup sets:
primary mainhq

# restore-settings <backup set>
```

security

Specify security options for Reporter.

The Reporter client-authentication option uses SSL mutual authentication. In mutual SSL authentication, an SSL connection between a client and a server is established only if the client and server validate each other’s identity during the SSL handshake. The server and the client must each have their own valid X.509 certificate and the associated private key in order to perform SSL mutual authentication. Refer to Authenticate Users with SSL Mutual Authentication for more information.

> **Caution:** The options and subcommands listed here are applicable when the security command is run from a `(config)#` prompt. You may also run this command from an enable prompt, but the primary focus of using this command in enable mode is to view your existing security configuration.

Syntax

```
(config)# security [subcommands]
```

`client-authentication [disable | set-optional <cr> | set-regex <value>]`	Set restrictions for how Reporter challenges administrative users to use X.509 client certificates to login.

Examples

```
(config)# security client-authentication disable
```

Disable X.509 client authentication.

```
(config)# security client-authentication set-optional
```

If X.509 client authentication fails, users can log in using the standard Reporter login page. Issuing this command requires Reporter to restart.

```
(config)# security client-authentication set-regex
```

Sets the regex command used to extract the certificate's name or data set in the certificate's Subject Alternative Name (`subjAltName`); the default is `CN=(.*?),`.

> **Caution:** Backslashes (\) and single-quotes (`'`) in the regex must be escaped, for example: `\\s` for `\s` and `\'` for `'`

Subcommand:

`default`

Resets the principal regex to the default.

Subject alternative name example:

```
# security client-authentication set-regex "'1\\.3\\.6\.1\\.4\\.1\\.311\\.20\\.2\\.3,\\s\\[0\\]
(.*?)@\'"
```

```
# security client-authentication view
```

View current X.509 client authentication settings.

send

Send one or all users a message to their terminal. The message will be shown in the CLI session of any logged-in user.

Syntax

```
# send <user>|all <message>
```

> **Note:** The user must be logged on to receive the message.

Examples

```
# send all "This is an important message."
#
Message from admin@ at 2016-09-22 15:09:36...
This is an important message.
```

shutdown

Shuts down the operating system, stops all CPUs, and sends a signal to the power supply unit to disconnect the main power. With this command (as compared to the halt command), you don't have to press the power switch to power down the appliance. This command is used to prepare physical appliances for transport.

Syntax

```
# shutdown
```

ssh generate

Generate a 2048-bit RSA host key pair. If you believe the key's security was compromised, you can generate a new SSH key pair. This command is available in both the `enable` and `config` modes.

Syntax

```
(config) # ssh generate host-keypair | view
```

Example

```
(config) # ssh generate host-keypair
Are you sure you want to regenerate the keypair? [yes,no] y
SSH host key successfully regenerated
```

ssl

Configure Secure Socket Layer (SSL) settings. This command is available in both the `enable` and `config` modes.

Syntax

```
(config)# ssl ?
```

`create [keyring | ccl | self-signed-certificate | signing-request |]`	Create SSL objects. See "ssl create" on page 55.
`delete [ca-certificate certificate | keyring | signing-request |]`	Delete SSL objects. See "ssl delete" on page 55.
`edit [ca-certificate certificate | keyring | signing-request |]`	Edit the appliance's current SSL settings. See SSL Edit.
`inline [ca-certificate | ccl | certificate | keyring | signing-request]`	Import SSL keyrings, CA certificate lists, signing requests, and certificates. See "ssl inline" on page 57.
`regenerate certificate <keyring-id> subject <subject> [alternative-names] [force]`	Regenerate an existing CA certificate and provide new subject and alternative name data. **`Force`** is optional, and will overwrite an existing certificate without confirmation.
`trust-package [auto-update | download-now | update-interval | url]`	Manage the list of trusted CA certificates provided by Symantec, how frequently to update it, and from where.

**`view [ca-certificate	ccl	certificate	keypair	keyring	signing-request |]`**	View available SSL objects.

Notes

- The sub-commands listed above can either be entered in SSL configuration mode (at the `config-ssl` prompt or in configuration mode (at the `config` prompt).
- Use the **`show full-configuration ssl`** command in configure mode to display basic SSL settings, and **`(config-ssl-view)# ?`** to view specific keyrings, CA Certificate LIsts, Certificates, and Certificate Signing Requests.

Examples

Add a certificate from a Certificate Authority; the certificate name in this example is *ca1*.

```
(config)# ssl
(config-ssl) inline ca-certificate ca1 content
Enter the certificate below and end it with a Ctrl-D
-----BEGIN CERTIFICATE-----
MIIEDTCCAvWgAwIBAgIJAIk7y/gggzO8MA0GCSqGSIb3DQEBBQUAMIGcMQswCQYD
VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTESMBAGA1UEBwwJU3Vubnl2YWxl
MRIwEAYDVQQKDAlCbHVlIENvYXQxFDASBgNVBAsMC0RldmVsb3BtZW50MRQwEgYD
VQQDDAtjYS5ibHVlY29hdDEkMCIGCSqGSIb3DQEJARYVZXJpYy5jaGlAYmx1ZWNv
YXQuY29tMB4XDTE1MDExMzAxMzI0MFoXDTI1MDExMDAxMzI0MFowgZwxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRIwEAYDVQQHDAlTdW5ueXZhbGUx
EjAQBgNVBAoMCUJsdWUgQ29hdDEUMBIGA1UECwwLRGV2ZWxvcG1lbnQxFDASBgNV
BAMMC2NhLmJsdWVjb2F0MSQwIgYJKoZIhvcNAQkBFhVlcmljLmNoaUBibHVlY29h
dC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCysxBQYApdEvNc
Nv6e7ELUtYRvnixueKceQM1y28Lj17lMPng6Dghs3ZKF/VPXw+lEsc+LG11a75d9
WziSsv7u4nKjt2Y2nPC4jE8jzgI7Fej26B6//bePh91v/+bJRwNSYR9z6wNa0cQt
prx8e6SvUbq7MkuE6vC9paqBqz4TQL0vyVHaWZXxodRLJaKGsZmq1yn1ogxjBT9+
Mj3HdmzVVRPQ5jNNjV6oKppGOrqpFkzOwcjpKWufOgk850kjsB2mOBE4QDHbJhtg
UtLMSGLaj2hmb58v6JdDROn4T3piZEDzAPl/4N9aOfbliF2nrdRNi2n5d8Q2JaXH
hXPGBGrVAgMBAAGjUDBOMB0GA1UdDgQWBBTCph9yrG16afTN6vaZJDTT2iv6xDAf
BgNVHSMEGDAWgBTCph9yrG16afTN6vaZJDTT2iv6xDAMBgNVHRMEBTADAQH/MA0G
CSqGSIb3DQEBBQUAA4IBAQCmI+pLumWXIAiznvq+zU/3/PTHwzcVcwJdK+ngWbHa
-----END CERTIFICATE-----
```

<Ctrl-D>

```
CA certificate ca1 is added successfully.
```

To view the certificate details for the ca1 certificate:

```
(config-ssl)# view ca-certificate ca1
Issuer: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Subject: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Valid From: Jan 13 01:32:40 2015 GMT
Valid Until: Jan 10 01:32:40 2025 GMT
Fingerprint: DB:AF:B1:82:EF:0C:9F:AD:84:F7:D8:35:0A:AA:0B:5D:93:DA:77:A5
```

start-reporter

Bring Reporter on line.

> **Note:** This command does not reboot the appliance.

Syntax

```
# start-reporter
```

stop-reporter

Take Reporter off line.

> **Note:** This command does not reboot the appliance.

Syntax

```
# stop-reporter
```

traceroute

Determines the path that an IP packet takes to travel from the appliance to a destination host.

Syntax

```
# traceroute ipv4|ipv6source <source ip address>size <packet size>timeout <seconds>probe-count <number of times to probe>min-ttl <minimum ttl value>max-ttl <maximum ttl value>dont-fragment <ip address>|<hostname>
```

`ipv4|ipv6`	Explicitly force an IPv4 or IPv6 traceroute. When an IP version isn't specified, the program will try to resolve the name given, and choose the appropriate protocol automatically. If resolving a host name returns both IPv4 and IPv6 addresses, traceroute will use IPv4.
`source <source ip address>`	The source IP address to put in the traceroute packets.
`size <packet size>`	Size of the traceroute packets, in bytes (default=100 bytes)

timeout ***<seconds>***	Number of seconds to wait for a response to a probe packet (default=3)
min-ttl ***<minimum ttl value>***	TTL value for the first probes (default=1)
max-ttl ***<maximum ttl value>***	The largest time to live (TTL) value that can be used (default=30)
dont-fragment	Set the dont-fragment flag on the probe packets.
<ip address>*|*<hostname>	The destination to trace the route of. This is the only required traceroute parameter. The IP address can be IPv4 or IPv6.

Examples

```
# traceroute size 50 timeout 4 cnn.com
1: 10.131.16.1 (10.131.16.1) 4.486ms
2: 172.16.131.66 (172.16.131.66) 0.486ms
3: 199.91.135.130 (199.91.135.130) 7.546ms asymm 4
4: 70.102.68.162 (70.102.68.162) 2.057ms
5: be1.br02.plalca01.integra.net (209.63.100.118) 20.784ms asymm 8
6: te-3-3.car2.SanJose2.Level3.net (4.59.4.29) 20.381ms asymm 7
7: no reply
8: no reply
```

upload

Upload the third-party attributions zip file to an FTP site.

Syntax

```
# upload ATTRIBUTIONS <full-url/filename><username> <password>
```

> **Note:** ATTRIBUTIONS must be in uppercase.

Example

```
upload ATTRIBUTIONS ftp://exampleftp.com/attributions.zip mary ******
```

Configure Mode Commands

The following commands are available in configure mode. This mode offers commands that change the configuration of the appliance.

To enter configure mode, type **configure** at the enable prompt (#). The prompt will change to (config)#. To see a list of commands available in configure mode, type **help** or **?** at the (config) # prompt.

access-logs

List or delete access-log files. This command is available in both the enable and config modes.

Syntax

```
# access-logs
```

delete	Delete one or more log files
list-dirs	List access-log directories
list-files	List access-log files in the specified directory

Example

```
# access-logs list-files <directory>
```

acl

Create firewall rules—access control lists—for accessing services on the appliance.

Syntax

```
(config)# acl ?
```

disable	Disable the user-defined access control list. This command is useful when locked out of the interface with a misconfigured access list.
enable	Enable the user-defined access control list.
rule *<source IP> <service>*	Define the IP addresses (individual, range, or subnet) that are allowed to access an appliance service (such as Management or SNMP).

Notes

- The sub-commands listed above can either be entered in acl configuration mode (at the config-acl prompt or in configuration mode (at the config prompt).
- To see the access control list, use the **show full-configuration acl** command.

- To remove a rule, enter **`no rule`** followed by the rule definition.
- Up to 1000 ACL rules can be entered in the access control list.
- The access control list only apply to incoming connections. Connections originating from the appliance are not subject to the access control list.
- Changes take effect immediately after a new rule is added or removed. It's not necessary to reboot.
- Existing connections that are allowed under a access control list are not affected when the rule is removed.
- The access list is not interface specific; the list applies to all interfaces.

Examples

```
(config)# acl
(config-acl)# rule 10.167.9.0/24 Management
(config-act)# rule 10.167.9.129 255.255.255.0 SNMP
(config-acl)# no rule 10.167.9.0/24 Management
```

appliance-name

Assign a unique name to the appliance. The appliance name is used when alerts are sent out to recipients, plus in other elements such as the command-line prompt and SNMP logs. Consider using a geographic or other location-based name to ensure each appliance in your network can be identified easily.

Syntax

```
(config)# appliance-name <name>
```

Example

```
ManagementCenter(config)# appliance-name
(config)#
```

authentication

Change a password or manage authentication settings. You can also change the *enable* and *console* passwords using the setup console.

Syntax

```
(config)# authentication ?
```

`disable-user-lockout`	Disable all lockouts on all local accounts
`enable-password`	Change the *enable* password

<table>
<tr><td><code>enable-user-lockout</code></td><td>Enable lockouts on all user accounts. The lockout is for 15 minutes after five failed login attempts</td></tr>
<tr><td><code>management</code></td><td>Manage security parameters
<table>
<tr><td><code>inactivity-timeout</code></td><td>Number of seconds a session can be inactive before it is terminated. Valid values: 60–86400</td></tr>
<tr><td><code>max-concurrent-logins</code></td><td>Set the maximum number of concurrent logins allowed per user. Valid values: 1–999</td></tr>
</table></td></tr>
</table>

Examples

```
(config)# authentication management max-concurrent-logins 500
(config)# authentication enable-password
Enter password:
```

clock

Manually set the time and date of the appliance in Coordinate Universal Time (UTC). This command is available in both the `enable` and `config` modes.

Syntax

```
# clock day <value>|hour <value>|minute <value>|month <value>|second <value>|year <value>
```

Each value must be entered as a separate command.

Examples

To set the date to September 2, 2016:

```
# clock day 2
```

```
# clock month 9
```

```
# clock year 2016
```

> **Note:** If you are using an NTP server, you do not need to manually set the clock.

configuration-management

Manage saved configuration files. This command is available in both the `enable` and `config` modes.

Syntax

```
(config)# configuration-management <argument>
```

`copy`	Copy a saved configuration
`delete`	Delete a saved configuration
`list`	List saved configurations
`load`	Load a saved configuration
`save`	Save a configuration and give it a name
`status`	Show status of loaded configurations

Example

```
(config)# configuration-management save <string>
```

dns

Configure servers and domains for the domain name system (DNS).

Syntax

```
(config)# dns ?
```

`name-server` ***`<IP address>`***	IP address of a DNS server. Enter one or more IP addresses, each separated by a space.
`domain-list` ***`<domain> <domain>`*** **`...`**	A list of DNS domain names of which this appliance will consider itself to be a member. DNS queries which use a short name will append these domains, in turn, until a match is found.

Notes

- To clear these settings, use the **no** command. For example, **`no dns name-server`**.
- To view the current settings, type .

Examples

```
(config)# dns name-server 10.2.2.10 10.2.2.11
```

event-log

Manage syslog settings. The syslog feature gives administrators a way to centrally log and analyze events on the system. This command is available in both the `enable` and `config` modes.

Syntax

```
(config)# event-log
```

> **Note:** You can add multiple syslog servers.

`level` ***`<value>`***	Set the level to specify which messages to suppress to the syslog server. For example, setting the level to 3 allows messages with levels 0 - 3 and suppresses messages with levels 4 - 7. **`<value>`** can be one of the following: **`0`** Emergency: system is unusable **`1`** Alert: action must be taken immediately **`2`** Critical: critical conditions **`3`** Error: error conditions **`4`** Warning: warning conditions **`5`** Notice: normal but significant condition **`6`** Informational: informational messages **`7`** Debug: debug-level messages
`syslog add host` ***`<host>`*** **`port`** ***`<port>`***	Configure a syslog server where *`<host>`* is the host name or IP address of the syslog server. Optionally, you can also specify a custom port, where *<port>* is the port number.
`syslog add udp host` ***`<host>`*** **`port`** ***`<port>`***	Configure a syslog server using UDP where *`<host>`* is the host name or IP address of the syslog server. Optionally, you can also specify a custom port, where *<port>* is the port number.
`syslog remove host` ***`<host>`***	Remove a configured syslog server by specifying the *<host>*.
`syslog clear`	Removes all configured syslog servers.
`view`	View syslog settings

> **Note:** The sub-commands listed above can either be entered in event-log configuration mode (at the `config-event-log` prompt, or in configuration mode (at the `config` prompt).

Examples

```
(config)# event-log
(config-event-log)# syslog add udp host 203.0.113.17
Added syslog server host 203.0.113.17:514.
(config-event-log)# view
Log level: 5 (notice)
Remote syslog servers:
       203.0.113.17:514
```

health-monitoring

View Health Monitoring (HM) events and status, and view and change HM settings. This command is available in both the `enable` and `config` modes.

Syntax

```
(config-health-monitoring)# ?
```

`clear-history`	Clear the entire event history
	`product1234-10414124(config-health-monitoring)# clear-history`
	`Event history has been cleared for all metrics.`

`history-duration`	Sets the number of days that the HM framework is to store its history of events. ■ It takes one argument, an integer representing the number of days. ■ Default value is 30. ■ Once per day, the HM framework clears the event history of all events older than the specified number of days. **`product1234-10414124(config-health-monitoring)# history-duration`** **`(<int>) (30): 60`** This option is available only in config mode.
`view`	Show health status and metric settings. See "health-monitoring view " below.

health-monitoring view

The `view` command in the health monitoring system is used for showing the event history and metric settings.

Syntax

```
(config-health-monitoring)# view ?
```

`current`	View the current state of all metrics. The output lists each metric, when the health monitoring system last checked it, the current state (OK, Warning, Critical) and the current value (for example, 28%).

`events [ all] [duration` ***`<value>`*** **`d|h|m]`**	Shows the event history for all metrics or for one metric, for the specified duration. An *event* is an occasion where the metric exceeded a configured threshold and changed state (for example, from OK to Warning, Warning to Critical). ▪ The **`metric`** and **`duration`** parameters are optional. ▪ If the **`metric`** parameter is omitted, 'all' is assumed. ▪ If the **`duration`** parameter is omitted, "24h" is assumed. ▪ The **`d`**, **`h`**, or **`m`** suffix is used to indicate days, hours, or minutes, respectively.

Examples

View the current state (OK, Warning, Critical) and value of all metrics.

interface

Configure the interface settings (such as IP address) on the appliance.

Syntax

```
(config)# interface <interface number> ?
```

where *`<interface number>`* is the interface (0:0, 1:0, 1:1, and so forth) that you want to configure.

`description` ***`<text>`***	Description of the interface; enclose in quotes if the description contains spaces.
`disable`	Disable the interface.
`enable`	Enable the interface.
`ip-address` ***`<ip address>`***	Set the static IP address of the interface.
`mtu-size` ***`<size>`***	Specify Maximum Transmission Unit (MTU) size (default=1500 bytes).
`speed` ***`<speed>`***	Set the speed of the interface (for example, 1gb,10gb,100mb). The default setting is **`auto`**.

Notes

- The sub-commands listed above can either be entered in interface configuration mode (for example, at the `config-interface-1:0` prompt or in configuration mode (at the `config` prompt).
- Use the **`show full-configuration`** command in interface configuration mode to display the interface settings. (See example below.)

Examples

```
(config)# interface 0:0
(config-interface-0:0)# ip-address 203.0.113.17 255.255.248.0
```

ok

```
(config-interface-0:0)# show full-configuration
interface 0:0
 description "management interface"
  enable
 speed auto
 duplex auto
 mtu-size 1500
 ip-address 203.0.113.17 255.255.248.0
```

ip

Configure the gateway, IPv6 neighbors, ARP table entries, and static routes.

Syntax

```
(config)# ip ?
```

arp *<IP address> <MAC address>*	Add a static IPv4 or IPv6 address to the Address Resolution Protocol (ARP) table, correlating the specified MAC address to the IP address.
default-gateway *<IP address>*	Change the IP address of the default gateway.
neighbor *<IPv6 address> <MAC address*	Configure static IPv6 neighbor entries (similar to a static ARP entry for IPv4). The IPv6 address and the hardware MAC address must be provided.
route *<IP address>*[/*<prefix>*] [*<subnet mask>*] [device-name *<interface>*] [metric *<value>]*	Specify the static route. For deployments where the default gateway does not route traffic to all segments of the network, you can define additional routes. A typical use for the route table is when the SMTP or DNS servers are located on an internal network. The route metric is used by routing protocols to determine whether one route should be chosen over another. With all else being equal, lower metrics are given preference when choosing routes. The specific metric values you assign are arbitrary, but they should have values relative to routing priority. For example, a route you want to assign high priority could have a metric value of 5 and a lower priority route could have a metric value of 10 or 20.

Examples

```
(config)# ip arp 1.1.1.1 01:23:45:67:89:ab
(config)# ip route 10.64.0.0/16 10.63.158.213 device-name 0:0 metric 10
(config)# ip route 2001:db8::/32 2001:0db8:0000:0000:0000:ff00:0042:8329 metric 20
(config)# ip route 10.63.0.0 255.255.0.0 10.63.158.213 metric 30
(config)# ip neighbor 2001:db8::ff00:42:8329 01:23:45:67:89:ac
```

licensing

Configure licensing, including the loading of licenses on to the appliance. This command is available in both the `enable` and `config` modes.

Syntax

```
(config)# licensing
```

```
(config-licensing)#
```

`inline license-key [passphrase <value>]`	Import a license from terminal input (typically by pasting the license content with a right-click). Include the **`passphrase`** to decrypt the private key if the license has birth-cert and birth-key in it. Press Ctrl-D after pasting the certificate content.
`load [username <value>] [password <value>]`	Enter your MySymantec credentials to download the appliance license from the Network Protection Licensing Portal (NPLP). **Note**: MySymantec credentials are required only for Management Center virtual appliances and Reporter appliances.
`load url <url> passphrase <value>`	Download a license from the specified URL.
`view [status|configuration]`	Display the license install status or licensing configuration details.

> **Note:** The sub-commands listed above can either be entered in licensing configuration mode (at the `config-licensing` prompt or in configuration mode (at the `config` prompt).

Examples

To load a license from a URL other than NPLP:

```
(config)# licensing load http://test.server.com/license.txt
```

To view the currently installed license:

```
(config-licensing)# view
Appliance Serial Number : 1000xxxxxx

Licensable component information:
Serial Number       : 0000xxxxxx
Part Number         : 000-00000
Expiration Date     :
Expiration Type     : Perpetual
```

```
Product Description : Reporter VA, up to 2TB HDD, Yr Subscription
Activation Date     : 2019-10-23
Component Name      : Reporter
```

ntp

Configure Network Time Protocol (NTP) settings. Use NTP to synchronize the time on the appliance with another server or reference time source. You can configure up to 10 NTP servers.

Syntax

```
(config)# ntp ?
```

`disable`	Stops the NTP service on the appliance. The NTP service is configured to not start when the appliance is rebooted. **`(config)# ntp disable`**
`enable`	Starts the NTP service on the appliance. The NTP service is configured to start automatically when the appliance is rebooted. At least one NTP server must be defined in order to enable the NTP service. **`(config)# ntp enable`**
`server` ***`<hostname or IP address>`***	Domain name or IP address of the NTP server. The default NTP servers are ntp.bluecoat.com and ntp2.bluecoat.com.
`symmetric-key key-id <value 1-65534> algorithm <sha1> [encrypted-secret <value> | secret <string>]`	If your NTP server supports symmetric-key authentication, enter the key with this series of commands. Only SHA1 is supported in this release. Defer to your NTP provider's instructions on whether to use an encrypted secret or unencrypted.

`update-now`	Forces the NTP service to update the appliance's clock.
	`# ntp update-now`
	`System date and time successfully updated.`

Notes

- Type **`ntp`** to enter NTP configuration mode. The prompt will display as `(config-ntp)#`.
- Use the **`no server`** command in the NTP configuration mode to remove a configured server. (See example below.)
- Use the **`show full-configuration`** command in the NTP configuration mode to display the NTP settings. (See example below.)

Examples

```
(config)# ntp server ntp1.net.symantec.com
(config)# ntp enabled
```

```
(config)# ntp
(config-ntp)# show full-configuration
(config-ntp)# show full-configuration
ntp
  enabled
  server ntp.bluecoat.com
  server ntp2.bluecoat.com
(config-ntp)# no server ntp2.net.symantec.com
```

To view the current configuration:

```
# show running-config ntp
ntp
enable
symmetric-key 1 algorithm sha1
symmetric-key 1 encrypted-secret $AES256-
CBC$4dQX+DOtMmVWdhtM4PG/+g==$gFDz7v2vfOM0A1D+qjzLPB5jqfqsEZhdoYx8EslIvkY=$kKZd4y09r3hNnlhziLwArw==$eR4
tJbJSB7309qcDCQ+jmLnCXUhfz7gQAcwvHdwFyEKfZUx5QqyKptrQiGGjjRwveM5UXcmem43v65eZan/WGzBow8YjdwLZNOcoN87xh
dN456EWJ8wsKsmd/60dhzVoMu5k3PQS1nQbCtmAn1BreBsrh2L/9zaJFl8C1HrdV5AYZpNokiakrMjxvw01ZAwxsagCflqqr2udV0K
SQSH0FiSPJbRJr/1rAjFIP/2LBL3EVahfRr+iwXROzUKMoWO4PJj05SF3idHMz2NwecIoXby3nA2e/WY0u/8UhqJauZ/+d1vr5H/8O
9VClASR4PL0Nrx2Vi0wjG25WYwuZNe+hQ==
server ntp.bluecoat.com
server ntp2.bluecoat.com
server symmetric-key
!
```

# pcap

Capture packets that are sent to and/or from the appliance. The captured data can be imported into a packet analysis tool such as Wireshark. This command is available in both the `enable` and `config` modes.

Syntax

# pcap ?

start	Start capturing packets.
stop	Stop capturing packets.
transfer ***<full-url/filename> <username> <password>***	Copy captured data to an FTP site. While not necessary, Symantec recommends that you use **pcap stop** before using this command.
filter direction [both|in|out]	Filter packets by direction.
filter interface ***<nic>***	Filter packets by interface number (0:0, 1:0, 1:1)

Before enabling packet capture, you can optionally restrict the packets that are captured by filtering by direction (in or out) or filtering by interface (for example, just packets sent out of the 1:0 NIC.

After capture is turned on, the system will create a .dmp file in TCPDump format and start capturing packets into this file.

Packets are captured until capturing is disabled with the **pcap stop** command, or after 30 minutes, whichever comes first.

Examples

```
(config)# pcap filter direction in
(config)# pcap start
(config)# pcap stop

(config)# pcap transfer ftp://example.com/john_files/test.dmp john.smith ******
```

proxy-settings

Configure an HTTP proxy server in situations where your network requires all servers to connect through a proxy to access Internet resources.

Syntax

```
(config)# proxy-settings enable|disable host <hostname or IP address> password <string> port <value>
username <string>

(config)# proxy-settings view
```

disable	Turn the proxy settings off.
enable	Turn the proxy settings on.
host *<hostname or IP address>*	Configure the HTTP proxy host name or IPv4/IPv6 address.
password ***<string>***	Enter the password for the HTTP proxy server.
port ***<value>***	Define the port number of the HTTP proxy server (0-65535).
username ***<string>***	Enter the user name for the HTTP proxy server.
view	View the HTTP proxy config settings

You can enter all the subcommands in one line, or enter each command on a separate line.

Examples

```
(config)# proxy-settings enable host 10.10.12.11
(config)# proxy-settings enable
(config)# proxy-settings host 10.10.12.11
(config)# proxy-settings port 8008
```

```
(config)# proxy-settings view
enabled:true
host :10.10.12.11
port no:8008
username:becky
```

snmp

Configure Secure Network Management Protocol (SNMP).

Syntax

```
(config) # snmp ?
```

agent	Configure the SNMP agent. When an SNMP manager polls a device for information, the SNMP agent on the device responds to the queries. See "snmp agent" below.
community	Define the community strings for SNMP v1/v2c. See "snmp community" on the next page.
system	System configuration (contact, location, name). See "snmp system" on page 48.
usm local	Define an SNMP local user entry. See "snmp usm local" on page 49.
usm remote	Define a user or a management system that receives notification of SNMPv3 traps and informs. See "snmp usm remote" on page 49.
vacm	Configure view-based access control model. See "snmp vacm group access" on page 49 and "snmp vacm group member" on page 50.

snmp agent

When an SNMP manager polls a device for information, the SNMP agent on the device responds to the queries.

Syntax

```
(config) snmp agent ?
```

disabled	Disable the agent
enabled	Enable the agent.
max-message-size *<value>*	The maximum length of SNMP message the agent can send or receive. Range: 484-214748364. Default=50000.
version v1 | v2c | v3	SNMP protocol version used by the agent.

Examples

```
(config)# snmp agent enabled
(config)# snmp agent version v3
```

snmp community

Define community strings for SNMP v1/v2. The community string acts as a password for accessing statistics on the device. Equipment usually ships with a read-only community string set to *public* but network managers typically change the community string to a customized value. Each system that polls your appliance could potentially have a different community string.

> **Note:** SNMP community strings are used only by devices that support SNMPv1 and SNMPv2c protocol. SNMPv3 uses username/password authentication, along with an encryption key.

Syntax

```
(config)# snmp community <string>
```

After defining the community string, the command prompt changes, indicating the community string. For example, for a community string `public`, the prompt looks as follows:

```
(config-community-public)#
```

The following sub-commands are available in community string configuration mode.

name ***<string>***	Necessary only when the community string is not the same as the index.
sec-name ***string <value>***	Initially set to the value of 'index.'
target-tag ***<target_name>***	Limit access for this community to the specified target(s). See snmp target for more information.

Examples

```
(config)# snmp community public
(config-community-public)# target-tag v1target
```

snmp reporter-traps

Reporter-specific commands for SNMP traps. These traps are enabled on a per-service basis.

Syntax

```
(config)# snmp reporter-traps ?
```

`community`	Set the community string for Reporter-specific SNMP traps
`disable`	Disable sending of Reporter-specific SNMP traps

`target-server`	Specify the remote SNMP host for Reporter-specific SNMP traps
`v2-enable`	Enable sending of Reporter-specific SNMP version 2c traps after specifying SNMPv2c parameters
`v3-authentication-passcode`	Specify the authentication passcode for Reporter-specific SNMP v3 traps
`v3-authentication-protocol`	Specify the authentication protocol for Reporter-specific SNMP v3 traps such as **`aes`**, **`sha`**, **`md5`**
`v3-enable`	Enable sending of Reporter-specific SNMP version 3 traps after you have specified the other SNMPv3 parameters
`v3-engine`	Specify the engine ID for Reporter-specific SNMP v3 traps
`v3-privacy-passcode`	Specify the privacy passcode for Reporter-specific SNMP v3 traps
`v3-privacy-protocol`	Specify the privacy protocol for Reporter-specific SNMP v3 traps such as **`aes`**, **`sha`**, **`md5`**
`v3-user`	Specify the user ID for Reporter-specific SNMP v3 traps

Example

```
(config)# snmp reporter-traps target-server 203.0.113.22
(config)# snmp reporter-traps v3-engine 0x1234567
(config)# snmp reporter-traps v3-user <username>
(config)# snmp reporter-traps v3-authentication-passcode <passcode>
(config)# snmp reporter-traps v3-authentication-protocol aes
(config)# snmp reporter-traps v3-privacy-passcode <passcode>
(config)# snmp reporter-traps v3-privacy-protocol md5
(config)# snmp reporter-traps v3-enable
```

snmp system

Configure SNMP system settings to identify the contact name, location, and fully-qualified domain name of the appliance.

Syntax

```
(config) snmp system ?
```

`contact <name>`	The name of the person managing the appliance; *<name>* can be up to 256 characters long and must be enclosed in quotation marks if spaces are used.
`location <place>`	The physical location of the appliance (room, floor, building), where *<place>* can be up to 256 characters long and must be enclosed in quotation marks if spaces are used.
`name <fqdn>`	The appliance's fully-qualified domain name for SNMPv1, where *<fqdn>* can be up to 256 characters long and must be enclosed in quotation marks if spaces are used.

Examples

```
(config)# snmp system contact "Gail Jellison"
(config)# snmp system location "building B, 1st floor"
```

snmp usm local

Define an SNMPv3 local user entry.

Syntax

```
(config)# snmp usm local user <user_name>
```

After defining the local user name, the command prompt changes, indicating you are in configuration mode for the local user. You can then define authentication and/or privacy keys that a management system can use to access the appliance.

auth [md5 | sha {key *<key>* | password *<password>*}]	Specify either the MD5 or SHA hash algorithm and enter an authentication key or password for the user (8-32 characters).
priv [aes | des {key *<key>* | password *<password>*}]	Specify either the AES or DES encryption algorithm and enter the privacy key or password (8-32 characters).

Examples

```
(config)# snmp usm local user altman
(config-user-altman)# auth md5 password Gquw4321
(config-user-altman)# priv aes password Gquw4321
```

snmp usm remote

Define the remote engine ID that receives notification of SNMPv3 traps and informs.

Syntax

```
(config)# snmp usm remote
```

snmp vacm group access

Define access for an SNMP group. Each group is defined by a name, a security model (and level), and a set of views that specifies which types of MIB data that access group can read or write.

Syntax

```
(config)# snmp vacm group <group_name> access {usm | v1 | v2c} {auth-no-priv | auth-priv | no-auth-no-priv}
```

auth-no-priv	A connection that is secured with a passphrase and authentication but no encryption.
auth-priv	A connection that is secured with both authentication and encryption.

`no-auth-no-priv`	A connection that uses a simple passphrase (known as a shared secret) to secure the communication.

After defining the access rights for the group, the command prompt changes, indicating the security level. For example: `(config-access-v1/auth-no-priv)#`

You then need to specify the name of the MIB view for each type of access.

`notify-view` ***`<MIB_view>`***	Specify the name of the MIB view of the SNMP context authorizing notify access. For example, in Content Analysis the view is named `cas-view` (and is not user-definable).
`read-view` ***`<MIB_view>`***	Specify the name of the MIB view of the SNMP context authorizing read access. Note that SNMPv1 is not permitted in read-view.
`write-view` ***`<MIB_view>`***	Specify the name of the MIB view of the SNMP context authorizing write access. Note that write-view is not implemented in all products.

Examples

```
(config)# snmp vacm group cas-group-v2c access v2c auth-no-priv
(config-access-v1/auth-no-priv)# read-view cas-view
```

snmp vacm group member

Define an SNMP access group member for a defined set of access rights.

Syntax

```
(config)# snmp vacm group <group_name> member <member_name> {sec-model usm | v1 | v2c}
```

Examples

```
(config)# snmp vacm group cas-group-2vc member member1 sec-model v2c
(config)# snmp vacm group cas-group-2vc member member2 sec-model v2c
```

After defining members, you can define the access rights for the group. See "snmp vacm group access" on the previous page.

ssh generate

Generate a 2048-bit RSA host key pair. If you believe the key's security was compromised, you can generate a new SSH key pair. This command is available in both the `enable` and `config` modes.

Syntax

```
(config) # ssh generate host-keypair | view
```

Example

```
(config) # ssh generate host-keypair
Are you sure you want to regenerate the keypair? [yes,no] y
SSH host key successfully regenerated
```

ssl

Configure Secure Socket Layer (SSL) settings. This command is available in both the `enable` and `config` modes.

Syntax

```
(config)# ssl ?
```

create [keyring | ccl | self-signed-certificate | signing-request |]	Create SSL objects. See "ssl create" on page 55.
delete [ca-certificate certificate | keyring | signing-request |]	Delete SSL objects. See "ssl delete" on page 55.
edit [ca-certificate certificate | keyring | signing-request |]	Edit the appliance's current SSL settings. See SSL Edit.
inline [ca-certificate | ccl | certificate | keyring | signing-request]	Import SSL keyrings, CA certificate lists, signing requests, and certificates. See "ssl inline" on page 57.

`regenerate certificate` ***`<keyring-id>`*** **`subject <subject> [alternative-names] [force]`**	Regenerate an existing CA certificate and provide new subject and alternative name data. **`Force`** is optional, and will overwrite an existing certificate without confirmation.
`trust-package [auto-update | download-now | update-interval | url]`	Manage the list of trusted CA certificates provided by Symantec, how frequently to update it, and from where.
`view [ca-certificate | ccl | certificate | keypair | keyring | signing-request |]`	View available SSL objects.

Notes

- The sub-commands listed above can either be entered in SSL configuration mode (at the `config-ssl` prompt or in configuration mode (at the `config` prompt).
- Use the **`show full-configuration ssl`** command in configure mode to display basic SSL settings, and **`(config-ssl-view)# ?`** to view specific keyrings, CA Certificate LIsts, Certificates, and Certificate Signing Requests.

Examples

Add a certificate from a Certificate Authority; the certificate name in this example is *ca1*.

```
(config)# ssl
(config-ssl) inline ca-certificate ca1 content
Enter the certificate below and end it with a Ctrl-D
-----BEGIN CERTIFICATE-----
MIIEDTCCAvWgAwIBAgIJAIk7y/gggzO8MA0GCSqGSIb3DQEBBQUAMIGcMQswCQYD
VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTESMBAGA1UEBwwJU3Vubnl2YWxl
MRIwEAYDVQQKDAlCbHVlIENvYXQxFDASBgNVBAsMC0RldmVsb3BtZW50MRQwEgYD
VQQDDAtjYS5ibHVlY29hdDEkMCIGCSqGSIb3DQEJARYVZXJpYy5jaGlAYmx1ZWNv
YXQuY29tMB4XDTE1MDExMzAxMzI0MFoXDTI1MDExMDAxMzI0MFowgZwxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRIwEAYDVQQHDAlTdW5ueXZhbGUx
EjAQBgNVBAoMCUJsdWUgQ29hdDEUMBIGA1UECwwLRGV2ZWxvcG1lbnQxFDASBgNV
```

```
BAMMC2NhLmJsdWVjb2F0MSQwIgYJKoZIhvcNAQkBFhVlcmljLmNoaUBibHVlY29h
dC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCysxBQYApdEvNc
Nv6e7ELUtYRvnixueKceQM1y28Lj17lMPng6Dghs3ZKF/VPXw+lEsc+LG11a75d9
WziSsv7u4nKjt2Y2nPC4jE8jzgI7Fej26B6//bePh91v/+bJRwNSYR9z6wNa0cQt
prx8e6SvUbq7MkuE6vC9paqBqz4TQL0vyVHaWZXxodRLJaKGsZmq1yn1ogxjBT9+
Mj3HdmzVVRPQ5jNNjV6oKppGOrqpFkzOwcjpKWufOgk850kjsB2mOBE4QDHbJhtg
UtLMSGLaj2hmb58v6JdDROn4T3piZEDzAPl/4N9aOfbliF2nrdRNi2n5d8Q2JaXH
hXPGBGrVAgMBAAGjUDBOMB0GA1UdDgQWBBTCph9yrG16afTN6vaZJDTT2iv6xDAf
BgNVHSMEGDAWgBTCph9yrG16afTN6vaZJDTT2iv6xDAMBgNVHRMEBTADAQH/MA0G
CSqGSIb3DQEBBQUAA4IBAQCmI+pLumWXIAiznvq+zU/3/PTHwzcVcwJdK+ngWbHa
-----END CERTIFICATE-----
```

<Ctrl-D>

```
CA certificate ca1 is added successfully.
```

To view the certificate details for the ca1 certificate:

```
(config-ssl)# view ca-certificate ca1
Issuer: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Subject: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Valid From: Jan 13 01:32:40 2015 GMT
Valid Until: Jan 10 01:32:40 2025 GMT
Fingerprint: DB:AF:B1:82:EF:0C:9F:AD:84:F7:D8:35:0A:AA:0B:5D:93:DA:77:A5
```

Certificate Signing Request (CSR)

This section provides information concerning Certificate Signing Request (CSR).

Assign an Imported Certificate

This section provides instructions on importing and assigning a certificate.

1. Access the Reporter command line.

2. In the command line, enter **`localhost# ssl create signing-request default`** along with the appropriate subjects. For a list of known subjects, see "CLI Commands to Support Keyring" on the facing page, below. For details on creating a CSR see "ssl create" on page 55 in the *CLI Reference Guide* on **support.symantec.com**.

3. Enter **`localhost# ssl view signing-request default`** to view the certificate. For details see "ssl view" on page 58 in the *CLI Reference Guide* on **support.symantec.com**.

4. Copy the certificate and submit it to a signing authority.

5. Copy the resulting certificate provided by the signing authority.

6. In the command line, enter **`localhost# ssl inline certificate default`**. For details see "ssl inline" on page 57 in the *CLI Reference Guide* on **support.symantec.com**.

7. When prompted to replace the existing certificate, enter **`yes`**.

CLI Commands to Support Keyring

The CLI commands below are under the **`ssl`** sub-mode of **`config`**.

CLI will use the following abbreviations during certificates/signing request creation. The subject field accepted for the certificate will be similar to what OpenSSL will accept, but comma separated. All the below fields are optional, but at least one of the field is required as subject. Each field can have comma separated multiple values except for country code. validation on the values is similar to what is done by OpenSSL during certificate creation.

subject example

```
C=US,ST=CA,L=Sunnyvale,O=BC,OU=BCQA,CN=common,emailAddress=support@symantec.com
```

subject table

This table provides detail on possible attributes for the subject field:

Short Name	Long Name	Description
`C`	`countyName`	Country
`ST`	`stateOrProvinceName`	State or Province Name
`L`	`localityName`	Organization
`OU`	`organizationalUnitName`	Organizational Unit
`CN`	`commonName`	Common Name
	`dnQualifier`	Distinguished Name Qualifier
`DC`	`domainComponent`	Domain Component
	`emailAddress`	Email Address
	`serialNumber`	Serial Number
	`title`	Title
`SN`	`surname`	Surname
`GN`	`givenName`	Given Name
	`initials`	Initials
	`pseudonym`	Pseudonym
	`generationQualifier`	Generation Qualifier

ssl create

Create SSL keyrings, CA Certificate Lists (CCLs), signing requests, self-signed certificates, and ssl-contexts.

Syntax

```
(config)# ssl create ?
```

ccl	Create a CA Certificate List (CCL).
keyring *<keyring id>* algorithm rsa length *<key_length>* showable [yes | no]	Create a keyring. Keyrings are containers for SSL certificates and their associated public and private keys on the appliance, and can be used to manage self-signed or CA-signed certificates. For RSA keys, key length values are 2048, 3072, 4096. Default = 2048.
certificate *<keyring id>*	Create a self-signed certificate associated with the specified keyring. You will be prompted to define values for each of the certificate fields (country, state, and so forth).
(config-ssl)# create ssl-context <context_id> [keyring <keyring_id>] [ccl <ccl_name>] [protocol [<protocol> ...]] [cipher-suite [<cipher-suite> ...]]	Creates an SSL context with the specified name and (optional) keyring, CCL, protocols and cipher suites.
signing-request *<keyring id>*	Create a request for a signed certificate associated with the specified keyring. You will be prompted to define values for each of the certificate fields (country, state, etc).

Examples

```
(config)# ssl create keyring sslkey algorithm rsa length 3072 showable no
(config-ssl)# create signing-request sslkey
Value for '' (<Country Code>): US
Value for '' (<State or Province Name (full name)>): CA
Value for '' (<Locality Name (eg city)>): Mountain View
Value for '' (<Organization Name (eg company)>): Symantec
Value for '' (<Organizational Unit Name (eg section)>): Marketing
Value for '' (<Common Name (eg server FQDN or YOUR name)>): symantec.com
Value for '' (<Email address>): jsmith@test.com
```

ssl delete

Delete SSL certificates, keyrings, and signing requests.

Syntax

```
(config)# ssl delete ?
```

ca-certificate *<certificate name>*	Delete CA certificate.
certificate *<keyring id>*	Delete the certificate that's in the specified keyring.
keyring *<keyring id>*	Delete the specified keyring.
signing-request *<keyring id>*	Delete the certificate request for the specified keyring.
ssl context *<context_id>*	Delete the specified SSL context.

Example

```
(config-ssl)# delete signing-request sslkey
```

ssl edit

Edit CA certificate lists (CCLs) or SSL contexts.

Syntax

```
(config)# ssl edit ccl <ccl_name> [action]  ?
```

`add`	Add a certificate by name to the selected CA certificate list.
`remove`	Remove a certificate from the selected CA certificate list.
`reset`	Empty the CA certificate list for this CA certificate list.
`set`	Set CA certificate list for this CA certificate list.
`view`	View the certificates in the selected CA certificate list.

```
(config)# ssl edit ssl-context <context_id> [action]  ?
```

Examples

```
(config)# ssl
(config-ssl)# edit ccl browser-trusted

(config-ccl-browser-trusted)# add esignit.org

ok

(config-ccl-browser-trusted)# view

Name: browser-trusted
FIPS compliant: no
Certificates:
      1st_Data_Digital
      A-Trust-Qual-02
      A-Trust-Root-05
      A-Trust-nQual-03
      AC1_Raiz_Mtin
      ACA_ROOT
```

```
    ACCV_ACCVRAIZ1
    ACEDICOM_Root
    ..
```

ssl inline

Import SSL keyrings, signing requests, and certificates.

Syntax

```
(config)# ssl inline ?
```

ca-certificate *<certificate name>* content	Import a Certificate Authority (CA) certificate from terminal input (typically by pasting the certificate content with a right-click). Press Ctrl-D after pasting the certificate content.
certificate *<keyring id>*	Import a certificate into the specified keyring. You will be prompted to paste the certificate content and press Ctrl-D when finished.
keyring *<keyring id>*	Install a keyring. Keyrings are containers for SSL certificates on the appliance, and can be used to manage self-signed or CA-signed certificates. You will be prompted to paste the keyring content and press Ctrl-D when finished.
signing-request *<keyring id>*	Install a request for a signed certificate associated with the specified keyring. You will be prompted to paste the signing request content and press Ctrl-D when finished.

Examples

Add a certificate from a Certificate Authority; the certificate name in this example is *ca1*.

```
(config)# ssl
(config-ssl) inline ca-certificate ca1 content
Enter the certificate below and end it with a Ctrl-D
-----BEGIN CERTIFICATE-----
MIIEDTCCAvWgAwIBAgIJAIk7y/gggzO8MA0GCSqGSIb3DQEBBQUAMIGcMQswCQYD
VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTESMBAGA1UEBwwJU3Vubnl2YWxl
MRIwEAYDVQQKDAlCbHVlIENvYXQxFDASBgNVBAsMC0RldmVsb3BtZW50MRQwEgYD
VQQDDAtjYS5ibHVlY29hdDEkMCIGCSqGSIb3DQEJARYVZXJpYy5jaGlAYmx1ZWNv
YXQuY29tMB4XDTE1MDExMzAxMzI0MFoXDTI1MDExMDAxMzI0MFowgZwxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRIwEAYDVQQHDAlTdW5ueXZhbGUx
EjAQBgNVBAoMCUJsdWUgQ29hdDEUMBIGA1UECwwLRGV2ZWxvcG1lbnQxFDASBgNV
BAMMC2NhLmJsdWVjb2F0MSQwIgYJKoZIhvcNAQkBFhVlcmljLmNoaUBibHVlY29h
dC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCysxBQYApdEvNc
Nv6e7ELUtYRvnixueKceQM1y28Lj17lMPng6Dghs3ZKF/VPXw+lEsc+LG11a75d9
```

```
WziSsv7u4nKjt2Y2nPC4jE8jzgI7Fej26B6//bePh91v/+bJRwNSYR9z6wNa0cQt
prx8e6SvUbq7MkuE6vC9paqBqz4TQL0vyVHaWZXxodRLJaKGsZmq1yn1ogxjBT9+
Mj3HdmzVVRPQ5jNNjV6oKppGOrqpFkzOwcjpKWufOgk850kjsB2mOBE4QDHbJhtg
UtLMSGLaj2hmb58v6JdDROn4T3piZEDzAPl/4N9aOfbliF2nrdRNi2n5d8Q2JaXH
hXPGBGrVAgMBAAGjUDBOMB0GA1UdDgQWBBTCph9yrG16afTN6vaZJDTT2iv6xDAf
BgNVHSMEGDAWgBTCph9yrG16afTN6vaZJDTT2iv6xDAMBgNVHRMEBTADAQH/MA0G
CSqGSIb3DQEBBQUAA4IBAQCmI+pLumWXIAiznvq+zU/3/PTHwzcVcwJdK+ngWbHa
GGVAhC+aMe+k3K+tTOO+3zxkSA7zF5X0NSZSRUAovZMrbXRxj+RuK1CMETEVAFzI
70uJv1EQoSt/Fg+Ax0h8M0Jn4lvUGsYPIAbcLjlxCtMNyfcOUG1Ss0yo/A/GXg13
eWINmdtdZHT/+ge01EEssswLxbyw3Pyl4CRMprjxlzg15Rx/PWV+zB+P2yolIrV4
pb5fsCuNrK4lYSdco5XE6P2m0c3P8QL/pB4SiZgWCr1sd0IKIoEphTk0kI++PTYx
d8cuVqPUXEi+UmibOBtfDz2ZffNkmBTdyvLfesINz0ce
-----END CERTIFICATE-----
```

<Ctrl-D>

```
CA certificate ca1 is added successfully.
```

To view the certificate details for the ca1 certificate:

```
(config-ssl)# view ca-certificate ca1
Issuer: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Subject: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Valid From: Jan 13 01:32:40 2015 GMT
Valid Until: Jan 10 01:32:40 2025 GMT
Fingerprint: DB:AF:B1:82:EF:0C:9F:AD:84:F7:D8:35:0A:AA:0B:5D:93:DA:77:A5
```

ssl view

View certificate and keyring details and signing request confirmations.

Syntax

```
(config)# ssl view ?
```

ca-certificate *<certificate name>* [verbose]	Show CA certificate and content.
ccl *<ca certificate list name>*	View the details for a specific CA Certificate List.
certificate *<keyring id>*	Show the certificate that's in the specified keyring.
keypair *<keyring id>*	Show the RSA private key for the specified keyring. If the keyring was created with the "showable no" option, the key will not be displayed.
keyring *<keyring id>*	Show details about the specified keyring, including its certificate and any signing requests.
signing-request *<keyring id>*	View certificate request for the specified keyring.

Examples

To view the certificate details for the ca1 certificate:

```
(config-ssl)# view ca-certificate ca1
Issuer: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Subject: /C=US/ST=California/L=Sunnyvale/O=Blue
Coat/OU=Development/CN=ca.bluecoat/emailAddress=eric.chi@bluecoat.com
Valid From: Jan 13 01:32:40 2015 GMT
Valid Until: Jan 10 01:32:40 2025 GMT
Fingerprint: DB:AF:B1:82:EF:0C:9F:AD:84:F7:D8:35:0A:AA:0B:5D:93:DA:77:A5
```

To show information about a keyring, in this case called **sslkey**:

```
(config-ssl)# view keyring sslkey
Keyring ID: sslkey
Private key showability: no-show
Signing request: absent
Certificate: present
Certificate subject:
/C=us/ST=ca/L=pa/O=symantec/OU=marketing/CN=symantec.com/emailAddress=test@test.com
Certificate issuer:
/C=us/ST=ca/L=pa/O=symantec/OU=marketing/CN=symantec.com/emailAddress=test@test.com
Certificate valid from: Jul 21 05:17:51 2017 GMT
Certificate valid to: Jul 21 05:17:51 2017 GMT
Certificate thumbprint: D7:3A:40:69:1A:D1:C2:77:95:B0:0F:DB:97:55:DE:02:BB:A9:54:00
```

To view the CA certificates contained in the CA certificate list, bluecoat-licensing:

```
(config-ssl)# view ccl bluecoat-licensing
Name: bluecoat-licensing
FIPS compliant: no
Certificates:
      BC_Engineering_CA
```

timezone

Set the time zone where the appliance is located or choose the Coordinated Universal Time (UTC) time standard. The default is UTC. Modify the settings for your time zone if you want to run Reporter jobs in your local time.

Syntax

```
(config)# timezone [<area>/<location> | UTC | GMT]
```

Supporting Commands

show timezone current	Display the currently configured timezone
show timezone	Display the available timezone areas.
show timezone <area>	Display the full list of timezones in a specific area.
show timezone <value>	Display the current time to see the local time in a specific timezone.

Examples

To select UTC as the time standard (instead of setting a time zone):

```
(config)# timezone UTC
```

To set an Antarctica time zone:

```
(config)# show timezone
Africa
America
Antarctica
Arctic
Asia
Atlantic
Australia
Europe
Indian
Pacific
UTC
GMT
all
current
(config)# show timezone Antarctica
Antarctica/McMurdo
Antarctica/Rothera
Antarctica/Palmer
Antarctica/Mawson
Antarctica/Davis
Antarctica/Casey
Antarctica/Vostok
Antarctica/DumontDUrville
Antarctica/Syowa
Antarctica/Troll
Antarctica/Macquarie
(config)# timezone set Antarctica/Davis
```

Reference: Ports and Protocols

Consult these tables when deploying Reporter behind a firewall or proxy.

> **Note:** These are the default ports. Some ports can be changed and others not used, depending on your deployment.

Inbound Connections

Service	Port(s)	Protocol	Configurable	Destination	Description
Web UI/API SSL	8082	TCP	No	Admin	HTTPS UI access (encrypted)
FTP	21	TCP	Yes	Local / accesslogs directory	Non-secure access logs file uploads/downloads/inspection
SCP	2024	TCP	No	Local / accesslogs directory	Secure access log file uploads
SNMP	161	TCP	Yes	Admin	SNMP communication
CLI SSH	22	TCP	No	Admin	CLI management shell access

Outbound Connections

Service	Port(s)	Protocol	Configurable	Destination	Description
LDAP	389	TCP	Yes	LDAP server	User authentication
LDAPS	636	TCP	Yes	LDAP server (encrypted)	User authentication
SMTP	25	TCP	No	SMTP server	Emails, reports, and event notifications
HTTPS	443	TCP	No	Symantec	Licensing and updates for products, subscriptions, ect..

Service	Port(s)	Protocol	Configurable	Destination	Description
DNS	53	UDP/TCP	No	Domain name server	Hostname resolution
FTP	21	TCP	Yes	FTP log file server	Access log file upload
NTP	123	UDP	No	Time server	Network time synching
syslog	514	UDP/TCP	Yes	syslog server(s)	Sending syslog messages to remote host (disabled by default)
Cloud log download	443	TCP	No	Symantec WSS	Request download of archived access logs from the Cloud Reporting service

Required IP Addresses and URLs

URL	Protocol	Description
`support.symantec.com`	`https/TCP 443`	Support links to software, support cases, and documentation.
`upload.bluecoat.com`	`https/TCP 443`	Upload portal logs and other large files.
`download.bluecoat.com`	`http/TCP 80`	Licensing portal; redirects to **`support.symantec.com`**
`esdhttp.flexnetoperations.com`	`https/TCP 443`	Software portal.
`device-services.es.bluecoat.com`	`https/TCP 443`	License related.