websense®

Using the X-Series Command Line Interface (CLI)

CLI Guide | Websense X-Series Appliances | v7.8.x

Starting in version 7.8.x, Websense X-Series appliances are configured and maintained through a command line interface (CLI). The CLI is a text-based user interface for configuring, troubleshooting, and monitoring the appliance.

The CLI replaces the web-based graphical user interface (GUI) provided in older X-Series appliance versions.

- The CLI allows you to write scripts to execute configuration changes and perform updates across multiple blades more efficiently.
- The CLI allows you to view and configure many of the features implemented in prior versions of X-Series appliances.

This guide describes the syntax and usage of each CLI command, including:

- *Conventions*, page 1
- *System configuration*, page 8
- *Maintenance and support*, page 22

Conventions

CLI Guide | Websense X-Series Appliances | v7.8.x

Administrators who are new to the Websense appliance CLI may benefit from these quick summaries:

- *Logon and authentication*, page 1
- *CLI modes (context) and account privileges*, page 3
- *Command syntax*, page 7
- *Help for CLI commands*, page 7

Logon and authentication

After the X10G hardware is set up, you will execute the **firstboot** wizard through the CMC to boot each blade appliance into the correct security mode (Web or Email) and policy mode (for Web appliances), and to give each blade a name and IP address.

See the X10G Getting Started Guide on the Websense eSupport site for full setup details.

Important

Make sure that Microsoft SQL Server is installed and running, and that you have database credentials ready.

To support Web Security Gateway, the network needs one—and only one—policy source machine to manage policy and configuration data for your deployment. That server must be set up first. This can be a server that is off-chassis (recommended) or the blade in SLOT-1.

The Getting Started Guide (linked above) provides important assistance with off-chassis policy source setup.

When you are ready to start booting the blades:

1. Power on a blade.
2. Log on to the CMC.
   a. Enter the IP address of the CMC into a browser that has connectivity to the network the chassis is on.

      ```
      http://<CMC_IP_address>
      ```

      Replace <*CMC_IP_address*> with the address assigned to the CMC during initial configuration of the chassis.

   b. If there is a security warning, continue to the address and enter the CMC logon credentials.
3. On the home screen, select SLOT-*N* from the list on the left, where “N” is the slot of the blade being configured. If the policy source machine will be a blade server, configure it first in SLOT-1.
4. Select **Launch Remote Console** on the upper right. A new command-line window opens.

   If it fails to open, look in the blade iDRAC window (launched when you attempted to open the console), and:

   a. Go to **Overview > Server > Virtual Console**.
   b. Change the **Plug-in Type** from **Native** to **Java** or **Java** to **Native**.
   c. Click **Apply** and then **Launch Virtual Console** (upper left).
5. In the console, accept the subscription agreement if prompted. You are now entering the firstboot wizard.

Choose initialization settings such as the appliance name, IP address, time and date, and, for a Web module, the policy mode.

You have an opportunity to change these settings before you exit firstboot. All except one setting can be changed later, through the CLI.

Important

After firstboot has been run to completion, you cannot change the security mode or policy mode without re-imaging the blade.

In addition, if you assign a default VLAN ID during firstboot, then later want to configure the blade to be VLAN-unaware, you must re-image.

At the conclusion of firstboot, you are logged on as **admin** automatically. Your logon session is timed out after 15 minutes, unless you log out prior to that.

From that point forward, the account name and password are required for logging on.

CLI modes (context) and account privileges

Tip

Be sure to enable CLI remote access if you plan to use PuTTY or other remote tool to access the CLI.

(*v7.8.3 and later*)

```
set access ssh --status on
```

(*v7.8.2*)

```
set account remote-cli --status on
```

By default, only the **admin** account is enabled on each blade. This is the account whose password you set during the firstboot process.

Two working **contexts** are supported by the Command Line Interface (CLI) and are available to every person logged on as **admin**:

- The **view** context (default) is for displaying status and settings.
- The **config** context is for changing settings and enabling/disabling options.

Immediately after logon, an admin is always working in the view context.

To move from **view** context to the **config** context, an admin simply enters the **config** command. The admin password is required for this context switch.

- Only one person logged in as **admin** can be working in **config** context at a time.

- If needed, a person logged in as **admin** who is working in the **view** context can use the following command to immediately bump the admin who is working in the **config** context:

  ```
  clear session --config
  ```

  This moves the administrator who had been working in **config** context back into the **view** context.

A person logged in as **admin** can optionally enable two accounts: an **audit** account for colleagues who need to view settings, and a technical support account for use by a Websense technician (**websense-ts**).

To summarize the differences between the admin and audit accounts:

- The **admin** account has full privileges, in both **view** and **config** contexts.
- The **audit** account can work only in the **view** context and can use only **show** and **exit** commands.

Basic account management

A person who is logged in as **admin** can view, enable, and disable the **audit** account status and can change the password for the **admin** and **audit** accounts.

Configure accounts

Action and Syntax	Details
Change the password for the admin account. `set account admin --password <password>`	You must know the current admin password to make this change. The admin password is first set when you run the firstboot script. The password must be at least 8 characters but less than 15 characters. The password must contain at least one letter and one number.
See if the audit account is enabled or disabled. `show account audit --status`	The audit account is disabled by default.

Enable or disable the audit account.
`set account audit --status <on|off>`
Set or change the audit account password.
`set account audit --password <password>`
	The --status and --password parameters cannot be used at the same time.
	The password must be at least 8 characters but less than 15 characters. The password must contain at least one letter and one number.

(*v7.8.3 and later*) Enable or disable remote CLI access via SSH. `set access ssh --status <on|off>`	SSH status is enabled or disabled for all active accounts.

Action and Syntax	Details
(*v7.8.3 and later*) Display whether remote CLI access via SSH is enabled or disabled. `show access ssh --status`	
Define an email address to use for admin account password recovery. `set account email --address <address>`	A temporary password is sent to this email address when you request automated password recovery help. You must also define an SMTP server. (See next command.) Websense Technical Support can also manually issue a temporary password if you provide the security code you see in the appliance iDRAC console.
Define an SMTP server for use during admin account password recovery. `set account smtp --host <location> --port <port> --user <name>`	Password recovery requires you to define: 1. An SMTP server 2. A valid email address to receive a temporary password The host location can be either the SMTP server's IPv4 address or its hostname. The SMTP port is optional (set to 25, by default). The user is the account to use to connect to the SMTP server
For admin account password recovery, enter **Ctrl+P**.	If you have lost or forgotten your admin password, you can either: • Have a temporary password sent to the email address configured on the blade. • Contact Websense Technical Support to receive a temporary password by providing the security code displayed on the appliance iDRAC console. Use the temporary password to log on to the blade and enter a new password within 1 hour. If you are not able to set a new password within the hour, you'll need to start the password recovery process over, by obtaining a new temporary password. The password must be at least 8 characters but less than 15 characters. The password must contain at least one letter and one number.
Delete the password recovery email address. `delete account email`	
Delete SMTP settings. `delete account smtp`	

Action and Syntax	Details

Show Websense Technical Support account access or activity history.
`show account websense-ts --status`
`show account websense-ts --history`
	The --status and --history parameters cannot be used at the same time.
	The activity history includes both local and remote access via the websense-ts account.

Enable or disable access for Websense Technical Support. `set account websense-ts --status <on|off>`	A temporary passcode is generated when you enable this access. Websense Technical Support retrieves the passcode from a special URL. ◆ (*v7.8.3 and later*) To allow Technical Support remote access, SSH access must also be enabled via the “set access ssh --status on” command. ◆ (*v7.8.2*) Remote SSH access on this account is enabled automatically when you grant access to Websense Technical Support. When a technician uses the websense-ts account, the session ends automatically after 15 minutes of inactivity. View the logon history of the websense-ts account with: `show account websense-ts --history`
(*v7.8.2*) Show whether SSH access to the CLI is enabled or disabled. `show account remote-cli --status`	Remote access to the CLI is disabled by default.
(*v7.8.2*) Enable or disable remote CLI access for accounts. `set account remote-cli --status <on|off>`	Remote access lets you use PuTTY or other remote tool to access the CLI. For readers who also use V-Series appliances, this is equivalent to the V-Series command: `ssh enable|disable` The status of the remote-cli account does not affect the status of the websense-ts account, and vice versa. The two accounts do not interact. When you enable either the websense-ts account or remote-cli, the ssh service is started. The ssh service is not stopped until both of these accounts are disabled.

Session management

Action and Syntax	Details
Enter the appliance CLI config context. `config`	Audit accounts do not have access to this context. The admin password is required.
Show connection information for active CLI sessions. `show session`	
End a config mode session immediately. `clear session --config`	Ends the session for whichever admin is in config mode, and allows another admin to enter config mode.
Exit the current config context. `exit`	If you are working in the config context, you return to the view context. If you are in the view context, your session ends and you exit the appliance CLI.

Command syntax

The CLI syntax follows this format:

```
Command + Option + Parameter
```

Typically, verbs such as **show, set,** and **save** are used to view status or statistics, to change the configuration, and to initiate actions.

For example:

```
# set system clock --date <yyyy/mm/dd>
```

In this example:

- **set system** is the command.
- **clock** is the option.
- **--date** is the parameter, which takes a value in the format yyyy/mm/dd.

Some commands have options and parameters, while others do not. Please refer to *Help for CLI commands*, page 7, for more details.

Help for CLI commands

Assistance is built into the CLI.

Use the **help** command to access information at any level.

```
# help
# help show
# help show log
```

Use the special character (**?** the question mark) to display help for the current command path without pressing **Enter** and without losing the current input.

```
# ?
# show ?
# show system ?
```

System configuration

CLI Guide | Websense X-Series Appliances | v7.8.x

Use the System Configuration commands of the security blade CLI to view, set, or change:

- *Time and date*, page 8
- *Host name and description*, page 10
- *Filestore definition and file save commands*, page 11
- *Appliance interface configuration*, page 12
- *Static routes*, page 14.
- *SNMP monitoring (polling)*, page 17
- *SNMP traps and queries*, page 19

Time and date

Action and Syntax	Details
View the system date and time. `show system clock`	The time and date format is: yyyy/mm/dd hh:mm:ss
Set system time and date manually. `set system clock --date <yyyy/mm/dd> --time <hh:mm:ss>`	Stop all Websense services before changing the time. Then, set the time **and** make certain that the time is consistent across all servers running Websense services. Finally, start Websense services. If you do not stop the services first, client updates and policy changes entered after the time reset are not saved. Note that instead of setting the time manually, you can synchronize with a Network Time Protocol (NTP) server. See “set system ntp” below.
View the configured time zone. `show system timezone`	

Action and Syntax	Details
View supported timezone formats. `show system timezone-list`	
Set the timezone for this security blade. `set system timezone --zone <zone_string>`	GMT (Greenwich Mean Time), the default, is also known as UTC (Universal Time, Coordinated). Other time zones are calculated by adding or subtracting from GMT. GMT is sometimes chosen to provide a common time stamp for geographically distributed systems.
View the configured NTP servers. `show system ntp`	
Configure timezone synchronization with up to 3 NTP servers. `set system ntp {--status <on|off> | --server <server1>, <server2>,<server3>}`	To synchronize with a Network Time Protocol (NTP) server (www.ntp.org.), set the status to “on” and enter the address of a primary NTP server. The secondary and tertiary servers are optional. If you synchronize the system clock with an NTP server, NTP protocol packets and their response packets must be allowed on any firewall or NAT device between a security blade and the NTP server. Ensure that you have outbound connectivity to the NTP servers. Add a firewall rule that allows outbound traffic to UDP port 123 for the NTP server. If interface P1 on a security blade is not connected to the Internet, then you must provide a way for interface P1 to reach an NTP server. One solution is to install an NTP server on the local network where interface P1 can reach it.

Host name and description

Action and Syntax	Details
View the security blade hostname and description. `show system host`	These values are set initially during the firstboot wizard.

Change the hostname and description for the security blade.
`set system host`
`--name <name>`
`--description`
`"<description>"`
	Name: The hostname may be 1 - 60 characters long.
	◆ The first character must be a letter.
	◆ Other characters can be letters, numbers, dashes, or periods.
	◆ The name cannot end with a period.
	◆ The name cannot have 2 periods in a row.
	For Web mode blades where Content Gateway will be configured to perform Integrated Windows Authentication (IWA), the hostname cannot exceed 11 characters, excluding the domain name.
	In addition, if the hostname is changed after the blade has been joined to a domain, IWA will immediately stop working and will not work again until the domain is unjoined and then re-joined with the new hostname.
	For more information, see Integrated Windows Authentication in Content Gateway Manager Help.
	Description (*optional*): A unique appliance description to help you identify and manage the system.
	◆ Must be in quotation marks
	◆ May contain up to 100 characters

Filestore definition and file save commands

Action and Syntax	Details
Display all filestore aliases. `show filestore`	A filestore is a remote storage location that you define for storing backup and configuration files.

Define a remote location to host backup and configuration files.
`set filestore`
`--alias <name>`
`--type <ftp|samba|tftp>`
`--host <ip_address>`
`--path <share_directory>`
`[--user <user_name>]`
`[--port <port>]`
	◆ --alias: Provide a unique name for the remote storage location.
	The alias must be between 1 and 60 characters and begin with a letter. It may contain letters, numbers, periods, and hyphens, but may not contain 2 consecutive periods, nor end with a period.
	◆ --type: Specify the protocol to use to connect to the filestore (FTP, Samba, or TFTP).
	◆ -- host: Provide the IP address of the machine hosting the filestore.
	◆ --path: Give the directory path to the shared location on the remote server.
	◆ --user (*optional*): Provide a user account with full permissions to the filestore.
	◆ --port (*optional*): Specify a port to use to connect to the filestore.

Delete one or more filestore aliases.
`delete filestore`
`--alias <filestore_alias>`
	You can specify a comma-separated list of filestore aliases:
	`delete filestore`
	`--alias ftp-fs1,samba-fs5`

Save the appliance MIB file to the specified location.
`save mibfile`
`--location <filestore_alias>`
	Saves the MIB file to a remote storage location defined by the “set filestore” command.

Summarize configuration data and save it to a specified location.
`save configsummary`
`--location <filestore_alias>`
	Saves your configuration data to a remote storage location defined by the “set filestore” command.
	May be requested by Websense Technical Support for analyzing unexpected behavior.

Save SNMP trap events settings for editing or later use.
`save trap`
`--location <filestore_alias>`
`[--default]`
	Saves default trap settings for editing. If “--default” is not specified, saves current trap settings.

Zip a log file and save it to a remote filestore.
`save log --module <all|app>`
`--type <file_type>`
`--location <filestore_alias>`
	Specify which module logs to save, which type of logs to save, and where to save the file.
	The module options are **all** or **app**, both of which currently save logs for all modules.
	The log types are **all**, **system**, or **audit**.

Appliance interface configuration

Action and Syntax	Details
Display the current network interface configuration. `show interface`	

Configure appliance interface in IPv4 settings.
(*v7.8.3 and later*)
`set interface ipv4`
`--interface <p1|p2>`
`--ip <ipv4_address>`
`--mask <ipv4_netmask>`
`--gateway <ipv4_address>`
(*v7.8.2*)
`set interface ipv4`
`--name <p1|p2>`
`--ip <ipv4_address>`
`--mask <ipv4_netmask>`
`--gateway <ipv4_address>`
	The interface name must be p1 or p2.
	IP address, netmask, and gateway definitions must use IPv4 format.

(*v7.8.4 and later; Email only*) Configure appliance virtual IP address settings.
`set interface ipv4`
`--interface <p1|p2>`
`--vip <virtual_ip_address>`
	Specify a single virtual IPv4 address.
	You can assign up to 10 virtual IP addresses to an interface, entered one at a time.

(*v7.8.3 and later; Web only*) Enable or disable IPv6 support on an appliance.
`set interface ipv6`
`--status <on|off>`	

(*v7.8.3 and later; Web only*) Configure appliance interface in IPv6 settings.
`set interface ipv6`
`--interface <p1|p2>`
`--ip <ipv6_address>`
`--prefixlen <integer>`
`--gateway <ipv6_address>`
	The interface name must be p1 or p2.
	IP address and gateway definitions must use IPv6 format.
	The **prefixlen** parameter sets the prefix length of the IPv6 address. It must be an integer between 1 and 128.

Configure appliance DNS settings.
`set interface dns`
`--dns1 <ip_address>`
`[--dns2 <ip_address>]`
`[--dns3 <ip_address>]`
	Enter the IP address of the primary domain name server.
	You can optionally also specify a second and third DNS server.
	For Email appliances, IP addresses must be entered in IPv4 format only.
	Web appliances support IPv4 or (*v7.8.3 and later*) IPv6 format.

Action and Syntax	Details
Enable or disable optional interface P2. `set interface p2 --status <on|off>`	Determines whether the interface is enabled (on) or disabled (off).
(*v7.8.4 and later*) Configure appliance VLAN settings. `set interface vlan --interface <p1|p2> --vid <integer>`	Assign a VLAN ID to an interface. The VLAN ID must be an integer in the range 2 - 4094. In order for blades to receive VLAN traffic, the A1 and A2 switches must be configured for VLAN support. See the Switch Configuration Guide for details.

Static routes

Action and Syntax	Details
Display the list of configured static IPv4 routes. `show route`	
(*v7.8.3 and later*, *Web only*) Display the list of configured static IPv6 routes. `show route6`	

Add a static route in IPv4 format.
(*v7.8.3 and later*)
`set route`
`--dest <ipv4_address>`
`--interface <p1|p2>`
`--mask <ipv4_netmask>`
`--gateway <ipv4_address>`
(*v7.8.2*)
`set route`
`--dest <ipv4_address>`
`--nic <p1|p2>`
`--mask <ipv4_netmask>`
`--gateway <ipv4_address>`
	Destination IP address must be in IPv4 format (okay to specify subnet instead).
	The interface name must be p1 or p2.
	Netmask must be in IPv4 format and must be the subnet mask of the IP address.
	Gateway (next hop) must be in IPv4 format.

(*v7.8.3 and later*, *Web only*) Add a static route in IPv6 format.
`set route6`
`--dest <ipv6_address>`
`--interface <p1|p2>`
`--prefixlen <integer>`
`--gateway <ipv6_address>`
	The interface name must be p1 or p2.
	IP address and gateway definitions must use IPv6 format.
	The **prefixlen** parameter sets the prefix length of the IPv6 address. It must be an integer between 1 and 128.

Delete a single IPv4 static route.
(*v7.8.3 and later*)
`delete route`
`--dest <ip_address>`
`--mask <ipv4_netmask>`
`[--interface <p1|p2>]`
`[--gateway <ip_address>]`
(*v7.8.2*)
`delete route`
`--nic <p1|p2>`
`--dest <ipv4_address>`
`--mask <ipv4_netmask>`
`--gateway <ipv4_address>`
	(*v7.8.3 and later*) To delete multiple IPv4 routes in a batch, use the “load route” command (described later in this table).

Action and Syntax	Details

(*v7.8.3 and later, Web only*) Delete a single IPv6 static route.
`delete route6`
`--dest <ipv6_address>`
`--prefixlen <integer>`
`[--interface <p1|p2>]`
`[--gateway <ipv6_address>]`
	To delete multiple IPv6 routes in a batch, use the “load route6” command (described later in this table).

Export IPv4 static routes.
`save route`
`--location <filestore_alias>`
	Saves IPv4 static routes to a remote storage location defined by the “set filestore” command.

(*v7.8.3 and later, Web only*) Export IPv6 static routes.
`save route6`
`--location <filestore_alias>`
	Saves IPv6 static routes to a remote storage location defined by the “set filestore” command.

Add or delete one or more IPv4 static route definitions via a text file.
`load route`
`--file <file_name>`
`--location <filestore_alias>`
`--action <add|del>`
Note: The **--action** parameter is available in versions 7.8.3 and later. Previous versions can add routes in batches, but not delete them.
	The system can handle a maximum of 5000 routes. Each line in the file defines one route.
	The line format is:
	`<destination_address> <netmask> <gateway> <p1|p2>`
	A blank space separates parameters on a single line.
	The following characters serve as separators between lines (individual routes):
	`\r\n`
	(*v7.8.3 and later*) Use the **--action** parameter to specify whether to add or delete the routes in the file.

(*v7.8.3 and later, Web only*) Add or delete one or more IPv6 static route definitions via a text file.
`load route6`
`--file <file_name>`
`--location <filestore_alias>`
`--action <add|del>`
	The system can handle a maximum of 5000 routes. Each line in the file defines one route.
	The line format is:
	`<destination_address> <prefix_length> <gateway> <p1|p2>`
	A blank space separates parameters on a single line.
	The following characters serve as separators between lines (individual routes):
	`\r\n`
	Use the **--action** parameter to specify whether to add or delete the routes in the file.

Appliance status

Action and Syntax	Details
Show current CPU usage, refreshed every 4 seconds. `show cpu`	Press Ctrl+C to quit.
Show system memory usage, refreshed every 4 seconds. `show mem`	Press Ctrl+C to quit.
View disk IO activity for a selected module, refreshed every 4 seconds. `show diskio`	You will be given a choice of modules after you enter the command. (*v7.8.4 and later*) The modules vary depending on whether the appliance security mode is Web or Email. Press Ctrl+C to quit.
Display disk statistics for all partitions. `show diskspace`	Results are shown in these areas: - disk position - total space - used space - free space - rate (*v7.8.4 and later*) The partitions vary depending on whether the appliance security mode is Web or Email.
Show network traffic statistics. `show bandwidth`	Displays bandwidth statistics for each enabled interface. Includes: - Data (byte) - Packets - Packets dropped - Error - Rate (Mbps) - Status Data is refreshed every 5 seconds. Press Ctrl+C to quit.

SNMP monitoring (polling)

Action and Syntax	Details
Show SNMP monitor server information. `show snmp config`	

Enable or disable SNMP monitoring (polling).
`set snmp service`
`--status <on|off>`
	SNMP monitor service and SNMP trap settings are independent, but SNMP monitor service must be enabled before you activate the SNMP trap configuration.

Configure SNMP v1 monitoring.
`set snmp v1`
`--community <name>`
	Community name for the appliance. From 5 to 64 characters long with no spaces. All other ASCII characters can be used.

Configure SNMP v2c monitoring.
`set snmp v2c`
`--community <name>`
	Community name for the appliance. From 5 to 64 characters long with no spaces. All other ASCII characters can be used.

Configure SNMP v3 monitoring.
`set snmp v3`
`--securitylevel <level>`
`...`
	There are 3 levels of security available for SNMP v3 monitoring:
	No authentication or encryption:
	`noAuthNoPriv`
	Authentication only:
	`authNoPriv`
	Authentication and encryption:
	`authPriv`
	See full syntax for each level, immediately below.

Configure SNMP v3 monitoring with no authentication or encryption.
`set snmp v3`
`--securitylevel`
`noAuthNoPriv`
`--user <username>`
	User specifies the account name to use for SNMP monitoring. Enter a user name between 1 and 15 characters long, with no spaces. Only alphanumeric characters can be used.

<table>
<tr><th>Action and Syntax</th><th>Details</th></tr>
<tr><td>Configure SNMP v3 monitoring with authentication only.
set snmp v3
--securitylevel authNoPriv
--user <username>
--authentication <md5|sha></td><td>User is the account name to use for SNMP communication. Enter a user name between 1 and 15 characters long, with no spaces. Only alphanumeric characters can be used.
SNMP authentication protocol (md5 or sha) specifies an interactive mode for entering the authentication password.
Enter an authentication password between 8 and 64 characters long, with no spaces. All other ASCII characters can be used.
Sample password dialog is shown here:
(config)# set snmp v3
--securitylevel authNoPriv
--user test
--authentication md5
Password: ********
Confirm password: ********</td></tr>
<tr><td>Configure SNMP v3 monitoring with authentication and encryption.
set snmp v3
--securitylevel authPriv
--user <username>
--authentication <md5|sha>
--encrypt <des|aes></td><td>User is the account name to use for SNMP communication. Enter a name between 1 and 15 characters, with no spaces. Only alphanumeric characters can be used.
SNMP authentication protocol (md5 or sha) specifies interactive mode for entering password.
You are prompted for a password and encryption key. The password must be 1-64 characters, and the key 8-64 characters long, with no spaces. All other ASCII characters can be used.
Example:
(config)# set snmp v3
--securitylevel authPriv
--authentication sha
--encrypt des --user test
Password: ********
Confirm password: ********
Encrypt key: ********
Confirm encrypt key: ********</td></tr>
</table>

SNMP traps and queries

Action and Syntax	Details
Display SNMP trap server on/off status and version information. `show trap config`	SNMP monitor service and SNMP trap settings are independent, but SNMP monitor service must be enabled before you activate the SNMP trap configuration.
Display a table of SNMP trap events and settings. `show trap events`	
Save SNMP trap events settings for editing or later use. `save trap --location <alias> [--default]`	Saves default trap settings for editing. If "--default" is not specified, saves current trap settings.
Enable or disable SNMP traps. `set trap service --status <on|off>`	SNMP monitor service and SNMP trap settings are independent, but SNMP monitor service must be enabled to activate the SNMP trap configuration.
Load SNMP trap events configuration from a file. `load trap --location <filestore_alias> --file <name>`	Enter the name of a predefined remote filestore alias.
Send a test trap to verify SNMP communication. `test trap event`	

Configure SNMP v1 traps for alerting.
`set trap v1`
`--community <name>`
`--ip <ip_address>`
`--port <port>`
	Enter a community name, trap server IP address, and port for traps sent by the appliance.
	The community name must be 5 to 64 characters long, with no spaces. All other ASCII characters can be used.

Configure SNMP v2c traps for alerting. `set trap v2c --community <name> --ip <ip_address> --port <port>`	Enter a community name, trap server IP address, and port for traps sent by the appliance. The community name must be 5 to 64 characters long, with no spaces. All other ASCII characters can be used.

Action and Syntax	Details

Configure SNMP v3 traps for alerting.
`set trap v3`
` --engineid <id>`
` --ip <ip_address>`
` --port <port>`
` --securitylevel <level>`
`...`
	There are 3 levels of security available for SNMP v3 traps:
	No authentication or encryption:
	`noAuthNoPriv`
	Authentication only:
	`authNoPriv`
	Authentication and encryption:
	`authPriv`
	See full syntax for each security level, immediately below.

Configure SNMP v3 traps with no authentication or encryption.
`set trap v3 --engineid <id>`
` --ip <ip_address>`
` --port <port>`
` --securitylevel`
`  noAuthNoPriv`
` --user <username>`
	Specify the engine ID, IP address, port, and user name to use for communication with your SNMP manager.
	The engine ID is a hexadecimal number between 10 and 64 characters long. The number cannot be all 0 or F characters, and the length of the string must be an even number.
	User is the account name to use for SNMP communication. Enter a name between 1 and 15 characters, with no spaces. Only alphanumeric characters can be used.

Action and Syntax	Details

Configure SNMP v3 traps with authentication only.
`set trap v3 --engineid <id>`
`--ip <ip_address>`
`--port <port>`
`--securitylevel`
`authNoPriv`
`--user <username>`
`--authentication <md5|sha>`
	Specify the engine ID, IP address, port, and user name to use for communication with your SNMP manager.
	The engine ID is a hexadecimal number between 10 and 64 characters long. The number cannot be all 0 or F characters, and the length of the string must be an even number.
	User is the account name to use for SNMP communication. Enter a name with 1-15 alphanumeric characters, with no spaces.
	Specify the authentication protocol used on the trap server (md5 or sha).
	You are prompted for a password. Enter a password between 1 and 64 characters, with no spaces. All other ASCII characters are okay.
	Example:
	`(config)# set trap v3`
	`--engineid 0x802a0581`
	`--ip 10.17.32.5 --port 162`
	`--securitylevel authNoPriv`
	`--authentication sha`
	`--user test`
	`Password: ********`

Configure SNMP v3 traps with authentication and encryption.
`set trap v3 --engineid <id>`
`--ip <ip_address>`
`--port <port>`
`--securitylevel authPriv`
`--user <username>`
`--authentication <md5|sha>`
`--encrypt <des|aes>`
	Specify the engine ID, IP address, port, and user name to use for communication with your SNMP manager.
	The engine ID is a hexadecimal number between 10 and 64 characters long. The number cannot be all 0 or F characters, and the length of the string must be an even number.
	User is the account name to use for SNMP communication. Enter a name with 1-15 alphanumeric characters, with no spaces.
	Specify the authentication protocol used on the trap server (md5 or sha), and the SNMP encryption protocol (des or aes).
	You are prompted for a password and encryption key. The password must be 1-64 characters, and the key 8-64 characters long, with no spaces. All other ASCII characters can be used.
	Example:
	`(config)# set trap v3`
	`--engineid 0x00b62000`
	`--ip 10.17.10.8 --port 162`
	`--securitylevel authPriv`
	`--authentication sha`
	`--encrypt des`
	`--user test`
	`Password: ********`
	`Encrypt key: ********`

Maintenance and support

CLI Guide | Websense X-Series Appliances | v7.8.x

Access the following groups of commands below:

Starting and stopping services

Action and Syntax	Details
(*Web only*) Start Web Security or Content Gateway services. `start <wse|wcg>`	The **start wse** command starts all Websense Web Security services. The **start wcg** command starts all Websense Content Gateway services.
(*v7.8.4 and later; Email only*) Start Email Security Gateway services. `start email`	
(*Web only*) Stop Web Security or Content Gateway services. `stop <wse|wcg>`	The **stop wse** command stops all Websense Web Security services. The **stop wcg** command stops all Websense Content Gateway services.
(*v7.8.4 and later*) Stop Email Security Gateway services. `stop email`	
Shut down the appliance. `shutdown appliance`	
Restart the appliance. `restart appliance`	
(*Web only*) Restart a Web appliance module. `restart <wse|wcg>`	
(*v7.8.4 and later; Email only*) Restart an Email module. `restart email`	

Module status and version details

Action and Syntax	Details
(*Web only*) Review status information for the Web Security module. `show wse --status`	Lists whether each component in the module is running or stopped.
(*Web only*) Find Web Security version information. `show wse --version`	Shows the current Web Security version and build number.
(*Web only*) Review status information for the Content Gateway module. `show wcg --status`	Shows whether Content Gateway and the Content Gateway manager are running or stopped.
(*Web only*) Find Content Gateway version information. `show wcg --version`	Shows the current Content Gateway version and build number.
(*Web only*) Get a link to the Content Gateway manager. `show wcg --manager`	
(*v7.8.4 and later; Email only*) Review status information for the Email module. `show email --status`	Lists whether each component in the module is running or stopped.
(*v7.8.4 and later; Email only*) Find Email Security Gateway version information. `show email --version`	Shows the current Email Security Gateway version and build number.

Appliance patches and hotfixes

All patches and hotfixes available for X10G blades can be listed from the CLI. There are 2 ways to retrieve patch and hotfix files:

- Download the patch or (*v7.8.3 and later*) hotfix file from the mywebsense.com Downloads page to a filestore, then upload the file from the filestore to each blade.
- (*v7.8.3 and later*) Download the patch or hotfix file directly from Websense download servers to each blade.

The speed of your Internet connection and the size of the patch will influence which method is more efficient for your environment.

Action and Syntax	Details

View a list of available upgrade patches.
(*v7.8.3 and later*)
`show patch list`
(*v7.8.2*)
`show patch`
	Shows both patches available on Websense download servers and patch files currently residing on the appliance.

(*v7.8.3 and later*) View a list of available appliance hotfixes. `show hotfix list [--id <hotfix_id>] [--location local] [--module <module>]`	The simple command, with no parameters, shows all hotfixes available for download from Websense servers or residing on the appliance. Note the name and ID of the hotfix file you want to install. - If you want to download a hotfix to a remote filestore, you will need the hotfix file name. Download hotfixes from the **Downloads** page at MyWebsense.com. Select a hotfix to see a detailed description. - If you want to download a hotfix directly to each security blade, you will need the hotfix ID. Parameters can narrow the scope of hotfixes displayed: - Use **--id** to see information about a specific hotfix. - Use **--module** and specify a module type to see hotfixes for the appliance module (**app**), Web Security module (**wse**), Content Gateway module (**wcg**), or (*v7.8.4 and later*) Email Security module (**email**). - Specify **--location local** to see hotfixes residing on the appliance.
(*v7.8.3 and later*) Display the status of the patch download process. `show patch load --status`	The load process is asynchronous, allowing the administrator to perform other CLI tasks while the download occurs. This command lets the administrator check to see if the download is complete.
(*v7.8.3 and later*) Display the status of the hotfix download process. `show hotfix load --status`	The load process is asynchronous, allowing the administrator to perform other CLI tasks while the download occurs. This command lets the administrator check to see if the download is complete.
(*v7.8.3 and later*) Display the status of the patch installation process. `show patch install --status`	

Action and Syntax	Details

(*v7.8.3 and later*) Display the status of the hotfix installation or removal process.
`show hotfix install --status`
`show hotfix uninstall --status`	

Display information about applied patches.
(*v7.8.3 and later*)
`show patch history`
(*v7.8.2*)
`show patch --history`
	The list shows all patches installed on the appliance.

Download or upload a patch to the appliance. `load patch [--file <name> --location <alias>]`	You can specify a patch name without a location to download a patch from Websense servers, or specify both the patch name and a location to upload the patch from a remote filestore. ◆ The filestore alias is created with the "set filestore" command. ◆ <*name*> is the exact name of the patch file. Enter the "load patch" command with no parameters to select the patch file from a list of patches available on Websense servers. Enter "load patch --location <alias>" with no file name to select the patch file from a list of files in the filestore. Note that if you change the name of a patch file in a remote filestore, this option can no longer be used.

(*v7.8.3 and later*) Download or upload a hotfix to the appliance.
`load hotfix [--id <hotfix_id>]`
`[--file <name> --location <alias>]`
	Specify the hotfix ID to download a hotfix from Websense servers, or specify a hotfix file name and location to upload the hotfix from a remote filestore.
	◆ Use the "show hotfix list" command to find the hotfix ID.
	◆ The filestore alias is created with the "set filestore" command.
	Enter the "load hotfix" command with no parameters to select the hotfix file from a list of hotfixes available on Websense servers.
	Enter the "load hotfix --location <alias>" command with no file name to select the hotfix from a list of files on the remote filestore. Note that if you change the name of a hotfix file in a remote filestore, this option can no longer be used.

Action and Syntax	Details

Install a patch file on the appliance.
(*v7.8.3 and later*)
`install patch [--file <patch_name>]`
(*v7.8.2*)
`apply patch --file <patch>`
	(*v7.8.2 only*) This command must be run from the blade's iDRAC console.
	<patch_name> is the exact name of the patch file.
	Enter "install patch" without the "--file" parameter to select the patch file from a list of patch files residing on the appliance.

(*v7.8.3 and later*) Install a hotfix file on the appliance. `install hotfix [--id <hotfix_id>]`	If no hotfix ID is specified, you can choose from a list of available hotfix files.
(*v7.8.3 and later*) Remove a patch file from the appliance. `delete patch --file <patch_name>`	This removes patch files that have been transferred to the appliance, but not installed. *<patch_name>* is the exact name of the patch file.
Remove a hotfix file from the appliance. `delete hotfix [--id <hotfix_id>]`	This removes hotfix files that have been transferred to the appliance, but not installed. If no hotfix ID is specified, you can choose from a list of available hotfix files.
(*v7.8.3 and later*) Uninstall a hotfix from the appliance. `uninstall hotfix [--id <hotfix_id>]`	If no hotfix ID is specified, you can choose from a list of installed hotfixes.

Backup and restore

Action and Syntax	Details

Show all available backups in a specified location.
`show backup list`
`--location <local|alias>`
	Displays the file name, date, and description of each patch file found in the specified location.
	- **local** is the current security blade.
	- **alias** is the filestore alias of a remote storage location.

Display the configured backup schedule. `show backup schedule`	Includes the schedule frequency, the last scheduled backup, the next scheduled backup, and the backup location.

Create a full appliance backup now.
`create backup now`
`--location <local|alias>`
`[--desc "<description>"]`
	You can back up files onto the appliance (local) or onto a remote filestore. You can restore from either location.
	The optional description of the backup is limited to 18 characters and must be enclosed in single or double quotes (' or ").
	Each appliance can store up to 20 backup files.

Restore the appliance configuration settings saved in the specified backup file.
`restore backup`
`--location <local|alias>`
`[--file <file_name>]`
	For location, specify a filestore alias or “local” for a local file.
	Optionally specify the name of the backup file to restore. If you do not specify a name, you can choose a file from a list.

Define a schedule of automatic backups.
`create backup schedule`
`--location <local|alias>`
`--freq <interval>`
`--day <day_name>`
`--date <month_day>`
`--time <hh:mm>`
	Backups are full appliance backups, including all installed modules.
	You can schedule a backup to occur daily, weekly, or monthly, to the appliance (“local”) or to a remote filestore.
	For the frequency interval, specify daily, weekly, or monthly (required).
	For all interval options, specify the time of day in 24-hour format (hh:mm). Do **not** specify seconds.
	If the interval is weekly, also specify the day of the week: Mon, Tue, Wed, Thu, Fri, Sat, or Sun (case matters).
	If the interval is monthly, also specify the day of the month (integer from 1-28).

Cancel all scheduled backups. `cancel backup schedule`	

Delete all backup files in a location or a named backup file.
`delete backup`
`--files <name|all|inter>`
	Takes one of the following values:
	- **name**: the name of a specific file
	- **all**: every backup file on the appliance
	- **inter**: interactive mode, which can be used to select files to delete

Collecting a configuration summary for analysis

Action and Syntax	Details
Create a configuration summary file for Technical Support analysis. `save configsummary --location <filestore_alias>`	Collects both the appliance configuration and all configurations for the modules running on the appliance. You must choose a remote location that can be shared with Technical Support.

Log files

Action and Syntax	Details
Display a list of log file types. `show log typelist --module <all|app>`	Specify a specific module whose log file types should be shown. **all** (default) includes all modules. **app** includes the entire appliance.
Display the last *n* lines of the appliance log file. `show log lastline --module app --type <system|audit> --line <integer>`	
Display data as it is appended to the appliance log file. `show log realtime --filter <string> --type <system|audit> --module app`	
(*v7.8.3 and later*) Configure how log files are archived. `set log archive --type <system|audit> --size <integer|string>] --freq <weekly|monthly| yearly>]`	When a log file reaches the specified maximum size (between 10 MB and 200 MB), or at the specified frequency interval, the file is archived and a new log file is started. **Note:** If both size and frequency values are entered, only the size value is used. The default unit of measurement for **--size** is bytes. To instead use kilobytes or megabytes, append “k” or “m” to the size. For example: `set log archive --size 50m` Use **freq** to specify a frequency interval: weekly, monthly, or yearly.

Action and Syntax	Details

(*v7.8.3 and later*) Display log file archiving settings.
`show log archive`
` --type <system|audit>`
	Determine whether log files are being archived, and if so, what criteria are used to determine when older log data is archived and a new log file is started.

Zip the log file and save it to a remote filestore.
`save log --module <all|app>`
` --type <all|system|audit>`
` --location <filestore_alias>`
	The filestore alias of a remote storage location is defined by the “set filestore” command