

Command Line Interface

This topic contains the following sections:

- Overview of the Command Line Interface , on page 1
- Accessing the Command Line Interface, on page 1
- General Purpose CLI Commands, on page 4
- Secure Web Appliance CLI Commands, on page 5

Overview of the Command Line Interface

The AsyncOS Command Line Interface (CLI) allows you to configure and monitor the Secure Web Appliance. The Command Line Interface is accessible using SSH on IP interfaces that have been configured with these services enabled, or using terminal emulation software on the serial port. By default, SSH is configured on the Management port.

The commands are invoked by entering the command name with or without any arguments. If you enter a command without arguments, the command prompts you for the required information.

Accessing the Command Line Interface

You can connect using one of the following methods:

- **Ethernet.** Start an SSH session with the IP address of the Secure Web Appliance. The factory default IP address is 192.168.42.42. SSH is configured to use port 22.
- **Serial connection.** Start a terminal session with the communication port on your personal computer that the serial cable is connected to.

First Access

You can add other users with differing levels of permissions after you have accessed the CLI the first time using the **admin** account—log in to the appliance by entering the default **admin** user name and passphrase:

- User name: **admin**
- Passphrase: **ironport**

The System Setup Wizard prompts you to change the passphrase for the **admin** account the first time you log in with the default passphrase.

You can also reset the **admin** account passphrase at any time using the `passwd` command.

Subsequent Access

You can connect and log into the appliance at any time, using a valid user name and passphrase. Note that a listing of recent appliance access attempts, both successes and failures, for the current user name is displayed automatically upon log-in.

See the following `userconfig` command description, or Administering User Accounts for information about configuring additional users.

Working with the Command Prompt

The top-level command prompt consists of the fully qualified hostname, followed by the greater than (>) symbol, followed by a space. For example:

```
example.com>
```

When running commands, the CLI requires input from you. When the CLI is expecting input, the prompt displays the default values enclosed in square brackets (`[]`) followed by the greater than (>) symbol. When there is no default value, the brackets are empty.

For example:

```
example.com> routeconfig

Choose a routing table:
- MANAGEMENT - Routes for Management Traffic
- DATA - Routes for Data Traffic
[]>
```

When there is a default setting, the setting is displayed within the command-prompt brackets. For example:

```
example.com> setgateway

Warning: setting an incorrect default gateway may cause the current connection
to be interrupted when the changes are committed.
Enter new default gateway:
[172.xx.xx.xx]>
```

When a default setting is shown, typing Return is equivalent to accepting the default.

Command Syntax

When operating in the interactive mode, the CLI command syntax consists of single commands with no white space and no arguments or parameters. For example:

```
example.com> logconfig
```

Select Lists

When you are presented with multiple choices for input, some commands use numbered lists. Enter the number of the selection at the prompt.

For example:

```
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 3
```

Yes/No Queries

When given a yes or no option, the question is posed with a default in brackets. You may answer **Y**, **N**, **Yes**, or **No**. Case is not significant.

For example:

```
Do you want to enable the proxy? [Y]> Y
```

Subcommands

Some commands give you the opportunity to use subcommand directives such as `NEW, EDIT, and DELETE`. The `EDIT` and `DELETE` functions provide a list of previously configured values.

For example:

```
example.com> interfaceconfig
Currently configured interfaces:
1. Management (172.xxx.xx.xx/xx: example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- DELETE - Remove an interface.
[]>
```

Within subcommands, pressing Enter or Return at an empty prompt returns you to the main command.

Escaping Subcommands

You can use the Ctrl+C keyboard shortcut at any time within a subcommand to immediately exit return to the top level of the CLI.

Command History

The CLI keeps a history of all commands entered during a session. Use the Up and Down arrow keys on your keyboard, or the Ctrl+P and Ctrl+N key combinations to scroll through a running list of the recently-used commands.

Completing Commands

The AsyncOS CLI supports command completion. You can enter the first few letters of some commands followed by the Tab key and the CLI completes the string. If the letters you entered are not unique among commands, the CLI "narrows" the set. For example:

```
example.com> set (press the Tab key)
setgateway, setgoodtable, sethostname, settime, settz
example.com> seth (pressing the Tab again completes the entry with sethostname)
example.com> sethostname
```

Committing Configuration Changes Using the CLI

- Many configuration changes do not take effect until you commit them.
- The `commit` command allows you to change configuration settings while other operations proceed normally.
- To successfully commit changes, you must be at the top-level command prompt. Type **Return** at an empty prompt to move up one level in the command line hierarchy.
- Changes to configuration that have not been committed are recorded, but do not go into effect until you run the `commit` command. However, not all commands require the `commit` command to be run. Exiting the CLI session, system shutdown, reboot, failure, or issuing the `clear` command clears changes that have not yet been committed.
- Changes are not actually committed until you receive confirmation and a timestamp.

General Purpose CLI Commands

This section describes some basic commands you might use in a typical CLI session, such as committing and clearing changes.

CLI Example: Committing Configuration Changes

Entering comments after the commit command is optional.

```
example.com> commit

Please enter some comments describing your changes:
[]> Changed "psinet" IP Interface to a different IP address
Changes committed: Wed Jan 01 12:00:01 2007
```

CLI Example: Clearing Configuration Changes

The clear command clears any changes made to the appliance configuration since the last commit or clear command was issued.

```
example.com> clear

Are you sure you want to clear all changes since the last commit? [Y]> y
Changes cleared: Wed Jan 01 12:00:01 2007
example.com>
```

CLI Example: Exiting the Command Line Interface Session

The exit command logs you out of the CLI application. Configuration changes that have not been committed are cleared.

```
example.com> exit

Configuration changes entered but not committed. Exiting will lose changes.
Type 'commit' at the command prompt to commit changes.

Are you sure you wish to exit?  [N]> y
```

CLI Example: Seeking Help on the Command Line Interface

The `help` command lists all available CLI commands and gives a brief description of each command. The `help` command can be invoked by typing either help or a single question mark (?) at the command prompt.

```
example.com> help
```

Further, you can access help for a specific command by entering **`help`** `commandname`.

Related Topics

- Secure Web Appliance CLI Commands, on page 5

Secure Web Appliance CLI Commands

The Secure Web Appliance CLI supports a set of proxy and UNIX commands to access, upgrade, and administer the system.



Note Not all CLI commands are applicable/available in all operating modes (Standard and Cloud Web Security Connector).

adminaccessconfig

You can configure the Secure Web Appliance to have stricter access requirements for administrators logging into the appliance, and you can specify an inactivity time-out value. See Additional Security Settings for Accessing the Appliance and User Network Access for more information.

advancedproxyconfig

Configure advanced Web Proxy options; subcommands are:

`AUTHENTICATION` – Authentication configuration options:

- `When would you like to forward authorization request headers to a parent proxy`
- `Enter the Proxy Authorization Realm to be displayed in the end user authentication dialog`
- `Would you like to log the username that appears in the request URI`

- Should the Group Membership attribute be used for directory lookups in the Web UI (when it is not used, empty groups and groups with different membership attributes will be displayed)
- Would you like to use advanced Active Directory connectivity checks
- Would you like to allow case insensitive username matching in policies
- Would you like to allow wild card matching with the character * for LDAP group names
- Enter the charset used by the clients for basic authentication [ISO-8859-1/UTF-8]
- Would you like to enable referrals for LDAP
- Would you like to enable secure authentication
- Enter the hostname to redirect clients for authentication
- Enter the surrogate timeout for user credentials
- Enter the surrogate timeout for machine credentials
- Enter the surrogate timeout in the case traffic permitted due to authentication service unavailability
- Enter re-auth on request denied option [disabled / embedlinkinblockpage]
- Would you like to send Negotiate header along with NTLM header for NTLMSSP authentication
- Configure username and IP address masking in logs and reports
- Timeout to enable/disable local Auth cache.

  You can use this CLI option to enable or disable the proxy process immediate authentication cache. The time set is in seconds. By default this option is enabled and set for 30 seconds. It must be shorter than IP surrogate time.

CACHING – Proxy Caching mode; choose one:

- Safe Mode
- Optimized Mode
- Aggressive Mode
- Customized Mode

  See also Choosing The Web Proxy Cache Mode.

DNS – DNS configuration options:

- Enter the URL format for the HTTP 307 redirection on DNS lookup failure
- Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure
- Would you like proxy not to automatically failover to DNS results when upstream proxy (peer) is unresponsive
- Do you want to disable IP address in Host Header
- Find web server by:

```
0 = Always use DNS answers in order

1 = Use client-supplied address then DNS

2 = Limited DNS usage

3 = Very limited DNS usage
```

The default value is 0. For options 1 and 2, DNS will be used if Web Reputation is enabled. For options 2 and 3, DNS will be used for explicit proxy requests, if there is no upstream proxy or in the event the configured upstream proxy fails. For all options, DNS will be used when Destination IP Addresses are used in policy membership.

EUN – End-user notification parameters:

- `Choose:`

  ```
  1. Refresh EUN pages

  2. Use Custom EUN pages

  3. Use Standard EUN pages
  ```

- `Would you like to turn on presentation of the User Acknowledgement page?`

See also Web Proxy Usage Agreement and End-User Notifications Overview.

NATIVEFTP – Native FTP configuration:

- `Would you like to enable FTP proxy`
- `Enter the ports that FTP proxy listens on`
- `Enter the range of port numbers for the proxy to listen on for passive FTP connections`
- `Enter the range of port numbers for the proxy to listen on for active FTP connections`
- `Enter the authentication format:`

  ```
  1. Check Point

  2. No Proxy Authentication

  3. Raptor
  ```

- `Would you like to enable caching`
- `Would you like to enable server IP spoofing`
- `Would you like to enable client IP spoofing`
- `Would you like to pass FTP server welcome message to the clients`
- `Enter the max path size for the ftp server directory`

See alsoOverview of FTP Proxy Services.

FTPOVERHTTP – FTP Over HTTP options:

- `Enter the login name to be used for anonymous FTP access`
- `Enter the password to be used for anonymous FTP access`

See also Overview of FTP Proxy Services.

Highperformance- enable and disable the high performance mode.

HTTPS – HTTPS-related options:

- `HTTPS URI Logging Style - fulluri or stripquery`
- `Would you like to decrypt unauthenticated transparent HTTPS requests for authentication purpose`
- `Would you like to decrypt HTTPS requests for End User Notification purpose`
- `Action to be taken when HTTPS servers ask for client certificate during handshake:`

  `1. Pass through the transaction`

  `2. Reply with certificate unavailable`
- `Do you want to enable server name indication (SNI) extension?`
- `Do you want to enable automatic discovery and download of missing Intermediate Certificates?`
- `Do you want to enable session resumption?`

See also Overview of Create Decryption Policies to Control HTTPS Traffic.

SCANNING – Scanning options:

- `Would you like the proxy to do malware scanning all content regardless of content type`
- `Enter the time to wait for a response from an anti-malware scanning engine (Sophos, McAfee, or Webroot), in seconds`
- `Do you want to disable Webroot body scanning`

See also Overview of Anti-Malware Scanning and Overview of Scanning Outbound Traffic.

SCANNERS- You can use the scanners subcommand to configure the settings for scanner engines. To use the scanners subcommand, you must disable the 'Adaptive Scanning' feature.

- Choose the operation you want to perform:

  `AMP - Secure Endpoint related option`

  `SOPHOS - Sophos Memory related option`

- **AMP** – Using this command, you can add the MIME types that need not be scanned by the AMP engine to increase the scanning performance. Default MIME type options are 'image/ALL and text/ALL'.

  To add the MIME types, you must append them after the default options. For example, if you want to add the video and audio MIME types, the format must be:

  'image/ALL and text/ALL video/ALL audio/ALL'

- **SOPHOS** – Sophos engine scan may get timed out and run out of memory when there is a huge traffic running through the engine. This is due to malloc memory issue, you can use the sophos subcommand and then choose `MALLOC_SETTING` to resolve this issue. When you select `MALLOC_SETTING`, you will be prompted with following message:

```
Changing Sophos Malloc Settings will lead to stoppage of coredumps.
Do you want to change the sophos malloc settings ? [Y]>
```

If you select yes, malloc settings will be changed and sophos will get restarted. To revert to default settings, you can use the same command.

Note Before using the command, we recommend you to take a note of the following:

- Make sure no traffic is running while changing the sophos malloc settings.
- When you change the settings from the CLI, the changes may take some time to update since sophos requires a restart.
- Do not change the malloc settings frequently.

Note For TAC use only.

- If sophos is coring due to any windows/linux update traffic, you must only change the malloc settings after the coring is completed.
- After the sophos restart, you might see the coring once because the changes will take some time to update.

PROXYCONN – Manage the list of user agents that cannot accept the proxy connection header. The list entries are interpreted as regular expressions in Flex (Fast Lexical Analyzer) dialect. A user agent will be matched if any substring of it matches any regular expression in the list.

- Choose the operation you want to perform:

```
NEW - Add an entry to the list of user agents

DELETE - Remove an entry from the list
```

CUSTOMHEADERS – Manage custom request headers for specific domains.

- Choose the operation you want to perform:

```
DELETE - Delete entries

NEW - Add new entries

EDIT - Edit entries
```

See also Adding Custom Headers To Web Requests.

MISCELLANEOUS – Miscellaneous proxy-related parameters:

- `Would you like proxy to respond to health checks from L4 switches (always enabled if WSA is in L4 transparent mode)`
- `Would you like proxy to perform dynamic adjustment of TCP receive window size`
- `Would you like proxy to perform dynamic adjustment of TCP send window size`

- Do you want to filter non-HTTP responses?

  (Non-HTTP responses are filtered by default.Enter **N** if you want to allow non-HTTP responses via proxy)
- Enable caching of HTTPS responses
- Enter minimum idle timeout for checking unresponsive upstream proxy (in seconds)
- Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)
- Mode of the proxy:

  1. Explicit forward mode only
  2. Transparent mode with L4 Switch or no device for redirection
  3. Transparent mode with WCCP v2 Router for redirection
- Spoofing of the client IP by the proxy:

  1. Enable for all requests
  2. Enable for transparent requests only
- Do you want to pass HTTP X-Forwarded-For headers?
- Do you want to enable server connection sharing?
- Would you like to permit tunneling of non-HTTP requests on HTTP ports?
- Would you like to block tunneling of non-SSL transactions on SSL Ports?
- Would you like proxy to log values from X-Forwarded-For headers in place of incoming connection IP addresses?
- Do you want proxy to throttle content served from cache?
- Would you like the proxy to use client IP addresses from X-Forwarded-For headers
- Do you want to forward TCP RST sent by server to client?
- Do you want to enable WCCP proxy health check?
- Do you want to enable URL lower case conversion for velocity regex?

See also Using the P2 Data Interface for Web Proxy Data and Configuring Web Proxy Settings.

SOCKS – SOCKS Proxy options:

- Would you like to enable SOCKS proxy
- Proxy Negotiation Timeout
- UDP Tunnel Timeout
- SOCKS Control Ports
- UDP Request Ports

See also Using the P2 Data Interface for Web Proxy Data and SOCKS Proxy Services.

CONTENT-ENCODING – Allow and block content-encoding types.

Currently allowed content-encoding type(s): compress, deflate, gzip

Currently blocked content-encoding type(s): N/A

To change the setting for a specific content-encoding type, select an option:

1. compress

2. deflate

3. gzip

[1]>

The encoding type "compress" is currently allowed

Do you want to block it? [N]>



Note The **centralauthcache** command is applicable for high performance enabled devices and to improve authentication cache performance.

adminaccessconfig

You can configure the Secure Web Appliance to have stricter access requirements for administrators logging into the appliance.

alertconfig

Specify alert recipients, and set parameters for sending system alerts.

authcache

Allows you to delete one or all entries (users) from the authentication cache. You can also list all users currently included in the authentication cache.



Note When *centralauthcache* is enabled, the *authcache* command does not display ISE authenticated user name. To obtain the ISE user information, use the *isedata* command.

bwcontrol

Debugs the bandwidth control feature.

- **bwcontrol listpipes**—Displays list of all bandwidth control pipes active on the Secure Web Appliance.
- **bwcontrol monitor <pipe number>**—Displays bandwidth measured for the given pipe, once every five seconds.

Starting from AsyncOS 14.5, the proxy logs in trace mode are displayed by default.

Terminologies

- `URLBW`—Bandwidth control applied by Access Policy URL Category.
- `OverallBW`—Bandwidth control applied by Access Policy Overall Web Activity Quota.

- `OverallMediaBW`—Bandwidth control applied by Overall Bandwidth Limit.
- `AVCPerUserBW`—Bandwidth control applied by AVC Bandwidth Limit.

certconfig

`SETUP` – Configure security certificates and keys.

`OCSPVALIDATION` – Enable/disable OCSP validation of certificate during upload.

`OCSPVALIDATION_FOR_SERVER_CERT` - Enable OCSP validation for server certificates

clear

Clears pending configuration changes since last commit.

clientconnections

Displays the connection details when the maximum connections per client is enabled. The details include the client IP address and the number of connections.

Choose the operation you want to perform:

- `LIST`—List all entries from cstat DB
- `SEARCH`—Search an entry from cstat DB

commit

Commits pending changes to the system configuration.

configbackup

Saves backup configuration file and sends the file to a remotely located backup server through FTP or SCP

csidconfig

You can configure different parameters of the Cisco Success Network feature on the appliance related to the publishing of telemetry data to the security services exchange portal.

Subcommands are:

- `CISCO_SUCCESS_NETWORK` – To enable/disable sending your appliance details and feature usage to Cisco.
- `CSIDATAPUSHINTERVAL` – Configure time interval of telemetry data push.

createcomputerobject

Creates a computer object at the location you specify.

curl

Send a cURL request directly to a Web server, or to a Web server via proxy, with the request and response HTTP headers returned to let you determine why a Web page is failing to load.

Note This command is for Administrator or Operator use only, under TAC supervision.

Subcommands are:

- `DIRECT` – URL access going direct
- `APPLIANCE` – URL access through the Appliance

datasecurityconfig

Defines a minimum request body size, below which upload requests are not scanned by the Cisco Data Security Filters.

date

Displays the current date. Example:

```
Thu Jan 10 23:13:40 2013 GMT
```

diagnostic

Proxy- and reporting-related subcommands:

`NET` – Network Diagnostic Utility

This command has been deprecated; use packetcapture to capture network traffic on the appliance.

`PROXY` – Proxy Debugging Utility

Choose the operation you want to perform:

- `SNAP` – Take a snapshot of the proxy
- `OFFLINE` – Take the proxy off-line (via WCCP)
- `RESUME` – Resume proxy traffic (via WCCP)
- `CACHE` – Clear proxy cache

`proxyscannermap-` This command displays PID mapping between each proxy and corresponding scanner process.

`REPORTING` – Reporting Utilities

The reporting system is currently enabled.

Choose the operation you want to perform:

- `DELETEDB` – Re-initialize the reporting database
- `DISABLE` – Disable the reporting system
- `DBSTATS` – List DB and Export Files (Displays the list of unprocessed files and folders under export_files and always_onbox folders.)
- `DELETEEXPORTDB` – Delete Export Files (Deletes all unprocessed files and folders under export_files and always_onbox folders.)

- DELETEJOURNAL – Delete Journal Files(Deletes all aclog_journal_files.)

dnsconfig

Configure DNS server parameters.

Choose the operation you want to perform:

- NEW—Add a new server.
- EDIT—Edit a server.
- DELETE—Remove a server .
- SETUP—Configure general settings.
- SEARCH —Configure DNS domain search list.

```
[]> setup

Do you want to enable Secure DNS? [N]> Yes
```

dnsflush

Flush DNS entries on the appliance.

etherconfig

Configure Ethernet port connections.

Choose the operation you want to perform:

- MEDIA – View and edit ethernet media settings.
- PAIRING – View and configure NIC Pairing.
- VLAN – View and configure VLANs.
- MTU – View and configure MTU.



Note M2, Data 1, and Data 2 interfaces are not supported. Hence, these interface options will not be available in the CLI.

externaldlpconfig

Defines a minimum request body size, below which upload requests are not scanned by the external DLP server.

externaldlpconfig

Defines a minimum request body size, below which upload requests are not scanned by the external DLP server.

fipsconfig

SETUP – Enable/disable FIPS 140-2 compliance, and encryption of Critical Sensitive Parameters (CSP). Note that an immediate reboot will be necessary.

FIPSCHECK – Check FIPS mode compliance. Indicates whether various certificates and services are FIPS compliant.

See FIPS Compliance for additional information.

grep

Searches named input files for lines containing a match to the given pattern.

gathererdconfig

Configure the polling functionality between the appliance and the authentication server.

help

Returns a list of commands.

httppatchconfig

Enables or disables outgoing HTTP PATCH requests. The default value is enable.

http2

Enables or disables HTTP 2 configurations.

iccm_message

Clears the message in the web interface and CLI that indicates when this Secure Web Appliance is managed by a Security Management appliance (M-Series).

ifconfig or interfaceconfig

Configure and manage network interfaces including M1, P1, and P2. Displays currently configured interfaces, and provides an operations menu to create, edit, or delete interfaces.

iseconfig

Displays current ISE configuration parameters; specify an ISE configuration operation to perform:

`ISE RECONCILIATION TIME SETUP`—Configure ISE reconciliation time setup. To restart the ised process automatically, set the time in the HH::MM format within 24 hours of ISE configuration. After a restart, the bulk download takes place.

`REMOVEISENODEDETAILS`—Remove secondary ISE pxGrid Node . The Security Web Appliance will communicate with the ISE pxGrid node to support Web Appliance data subscription (ongoing updates). Specifying a secondary ISE pxGrid node (server) is optional. You can remove the secondary ISE pxGrid Node by choosing the `REMOVEISENODEDETAILS` operation.

```
Choose the operation you want to perform:
-ISE RECONCILIATION TIME SETUP - Configure ISE reconciliation time setup.
```

```
-REMOVEISENODEDETAILS - remove seconadry ise config details
```

By default, the value for option 1 is 00:00 mid-night.

isedata

Specify an ISE data-related operation:

`statistics` – Show ISE server status and ISE statistics.

`cache` – Show the ISE cache, or check an IP address:

`sgts` – Show the ISE Secure Group Tag (SGT) table.

`groups` – Show the ISE Groups table.

If VDI is implemented, the sub commands `show` and `checkip` under the main command `cache` displays more details. The `show` subcommand displays details about port range and `checkip` subcommand displays details about the VDI user such as IP address, name, port range etc.

```
[]> cache

Choose the operation you want to perform:
- SHOW - Show the ISE ID cache.
- CHECKIP - Query the local ISE cache for an IP address
```

last

Lists user-specific user information that includes ttys and hosts, in reverse time order or lists the users that are logged in at a specified date and time.

loadconfig

Load a system configuration file.

logconfig

Configure access to log files.

mailconfig

Mail the current configuration file to the address specified.

maxhttpheadersize

Set the maximum HTTP header size or URL size for proxy requests; enter the value in bytes, or append a K to the number to indicate kilobytes.

Policy Trace can fail for a user that belongs to a large number of authentication groups. It can also fail if the HTTP response header size or URL size is greater than the current “max header size.” Increasing this value can alleviate such failures. Minimum value is 32 KB; default value is 32 KB; maximum value is 1024 KB.

modifyauthhelpers

Use this command to configure the number of Kerberos authentication helpers within a range of 5 to 21 for BASIC, NTLMSSP, and NEGO.

musconfig

Use this command to enable Secure Mobility and configure how to identify remote users, either by IP address or by integrating with one or more Cisco adaptive security appliances.



Note Changes made using this command cause the Web Proxy to restart.

musstatus

Use this command to display information related to Secure Mobility when the Secure Web Appliance is integrated with an adaptive security appliance.

This command displays the following information:

- The status of the Secure Web Appliance connection with each adaptive security appliance.
- The duration of the Secure Web Appliance connection with each adaptive security appliance in minutes.
- The number of remote clients from each adaptive security appliance.
- The number of remote clients being serviced, which is defined as the number of remote clients that have passed traffic through the Secure Web Appliance.
- The total number of remote clients.

networktuning

The Secure Web Appliance utilizes several buffers and optimization algorithms to handle hundreds of TCP connections simultaneously, providing high performance for typical Web traffic—that is, short-lived HTTP connections.

In certain situations, such as frequent downloading of large files (100+ MB), larger buffers can provide better per-connection performance. However, overall memory usage will increase, and thus any buffer increases should be in line with the memory available on the system.

The send- and receive-space variables represent the buffers used for storing data for communications over any given TCP socket. The send- and receive-auto variables are used to enable and disable the FreeBSD auto-tuning algorithm for dynamically controlling window size. These two parameters are applied directly in the FreeBSD kernel.

When `SEND_AUTO` and `RECV_AUTO` are enabled, the system tunes the window size dynamically based on system load and available resources. On a lightly loaded Secure Web Appliance, the system attempts to keep window sizes large to reduce per transaction latency. The maximum value of the dynamically tuned window size is dependent on the configured number of mbuf clusters, which in turn is dependent on the total RAM available on the system. As the total number of client connections increases, or when the available network buffer resources become scarce, the system tunes down the window sizes to protect itself from losing all network buffer resources to proxied traffic.

See Upload/Download Speed Issues for additional information about using this command.

The `networktuning` subcommands are:

`SENDSPACE` – TCP send-space buffer size; range is from 8192 to 131072 bytes; the default is 16000 bytes.

`RECVSPACE` – TCP receive-space buffer size; range is from 8192 to 131072 bytes; the default is 32768 bytes.

SEND-AUTO – Enable/disable TCP send auto-tuning; 1 = On, 0 = Off; default is Off. If you enable TCP send auto-tuning, be sure to use `advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP send window size?` to disable send buffer auto-tuning.

RECV-AUTO – Enable/disable TCP receive auto-tuning; 1 = On, 0 = Off; default is Off. If you enable TCP receive auto-tuning, be sure to use `advancedproxyconfig > miscellaneous > Would you like proxy to perform dynamic adjustment of TCP receive window size? Yes` to disable receive buffer auto-tuning.

MBUF CLUSTER COUNT – Change the number of available mbuf clusters; acceptable range is from 98304 to 1572864. The value should vary according to installed system memory, using this calculation: 98304 * (X/Y) where is X is gigabytes of RAM on the system and Y is 4 GB. For example, with 4 GB RAM, the recommended value is 98304 * (4/4) = 98304. Linear scaling is recommended as RAM increases.

SENDBUF-MAX – Specify the maximum send buffer size; range is from 131072 bytes to 2097152 bytes; the default is 1 MB.

RECVBUF-MAX – Specify the maximum receive buffer size; range is from 131072 bytes to 2097152 bytes; the default is 1 MB.

CLEAN-FIB-1 – Remove all M1/M2 entries from the data-routing table—essentially, enable control-plane/data-plane separation. That is, disable any data-plane process from sending data over the M1 interface when “Separate Routing” is enabled. Data-plane processes are those for which “Use data routing table” is enabled, or which carry strictly non-management traffic. Control-plane processes can still send data of over either the M1 or P1 interfaces.

Following any changes to these parameters, be sure to commit your changes and the restart the appliance.



Caution Use this command only if you understand the ramifications. We recommend using only with TAC guidance.

nslookup

Queries Internet domain name servers for information about specified hosts and domains or to print a list of hosts in a domain.

ntpconfig

Configure NTP servers. Displays currently configured interfaces, and provides an operations menu to add, remove, or set the interface from whose IP address NTP queries should originate.

packetcapture

Intercepts and displays TCP/IP and other packets being transmitted or received over the network to which the appliance is attached.

passwd

Set the passphrase.

pathmtudiscovery

Enables or disables Path MTU Discovery.

You might want to disable Path MTU Discovery if you need to packet fragmentation.

ping

Sends an ICMP ECHO REQUEST to the specified host or gateway.

process_status

Display the list of active processes of the appliance.



Note This command is available only in admin mode

proxyconfig <enable | disable>

Enables or disables the Web Proxy.

proxystat

Display web proxy statistics.

quit, q, exit

Terminates an active process or session.

quotaquery

To check or reset the volume and time used by a category.

Choose the operation you want to perform:

- `RESET`—Reset quota for specific entry in proxy quota cache.
- `SEARCH`—Search list of user entries in proxy quota cache.
- `RESETALL`—Reset all entries in proxy quota cache.



Note In a multi-proxy mode, when you want to reset the appliance while accessing *quotoquery* from the CLI, if the quota username consists of a "\" character, append another "\", and then reset the appliance. For example, if you find a quota username "vol:W2012-01\administrator@AD1", before performing a reset, edit the quota username (add additional "\") as "W2012-01\\administrator@AD1". The prefix "vol:" is not required when you perform a reset.

reboot

Flushes the file system cache to disk, halts all running processes, and restarts the system.

reportingconfig

Configure a reporting system.

resetconfig

Restores the configuration to factory defaults.

revert

Revert the AsyncOS for Web operating system to a previous qualified build. This is a very destructive action, destroying all configuration logs and databases. Refer to Reverting to a Previous Version of AsyncOS for Web for information about using this command.

rollbackconfig

Allows you to rollback to one of the previously committed 10 configurations. By default, the rollback configuration feature is enabled.

rollovernow

Roll over a log file.

routeconfig

Configure destination IP addresses and gateways for traffic. Displays currently configured routes, and provides an operations menu to create, edit, or delete, or clear entries.

saveconfig

Saves a copy of the current configuration settings to a file. This file can be used to restore defaults, if necessary.

If FIPS mode is enable, provide a passphrase-handling option: `Mask passphrases` or `Encrypt passphrases`.

setgateway

Configure the default gateway for the machine.

sethostname

Set the hostname parameter.

setntlmsecuritymode

Changes the security setting for the NTLM authentication realm to either “ads” or “domain”.

- `domain` — AsyncOS joins the Active Directory domain with a domain security trust account. AsyncOS requires Active Directory to use only nested Active Directory groups in this mode.
- `ads` — AsyncOS joins the domain as a native Active Directory member.

Default is `ads` .

settime

Set system time.

settz

Displays the current time zone and the time zone version. Provides an operations menu to set a local time zone.

showconfig

Display all configuration values.



Note User passphrases are encrypted.

shutdown

Terminates connections and shuts down the system.

smbprotoconfig

Enables or disables SMB1 Protocol support for Samba version 4.11.15.

Choose the operation you want to perform:

- Enable—Enable SMB1 protocol
- Disable—Disable SMB1 protocol

smtprelay

Configure SMTP relay hosts for internally generated email. An SMTP relay host is required to receive system generated email and alerts.

smtpconfig

Configure the local host to listen for SNMP queries and allow SNMP requests.

sshconfig

Configure hostname and host key options for trusted servers.



Note When you upgrade from AsyncOS 14.x to AsyncOS 15.x, the default sshconfig values can be observed. After the upgrade, you must re-configure the sshconfig values to supported values immediately before proceeding any operations in SWA.

sslconfig

The default cipher for AsyncOS versions 9.0 and earlier is `DEFAULT:+kEDH`.

The default cipher for AsyncOS versions 9.1 - 11.8 is:

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
!AES256-SHA:DHE-RSA-AES128-SHA
```

In this case, the default cipher may change based on your ECDHE cipher selections.

The default cipher for AsyncOS versions 12.0 and later is:

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```

Note Update the default cipher suite while upgrading to a newer AsyncOS version. The ciphers suites are not automatically updated. When you upgrade from an earlier version to AsyncOS 12.0 and later, Cisco recommends updating the cipher suite to:

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384
```

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:
TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```

FALLBACK – Enable/disable the SSL/TLS fall-back option. If enabled, communications with remote servers will fall back to the lowest configured protocol following a handshake failure.

After a protocol version is negotiated between client and server, handshake failure is possible because of implementation issues. If this option is enabled, the proxy attempts to connect using the lowest version of the currently configured TLS/SSL protocols.

Note On new AsyncOS 9.x installations, fall-back is disabled by default. For upgrades from earlier versions on which the fall-back option exists, the current setting is retained; otherwise, when upgrading from a version on which the option did not exist, fall-back is enabled by default.

ECDHE – Enable/disable use of ECDHE ciphers for LDAP.

Additional ECDH ciphers are supported in successive releases; however, certain named curves provided with some of the additional ciphers cause the appliance to close a connection during secure LDAP authentication and HTTPS traffic decryption. See SSL Configurationfor more information about specifying additional ciphers.

If you experience these issues, use this option to disable or enable ECDHE cipher use for either or both features.

ssltool

Executes different OPENSSL commands from appliance's CLI to troubleshoot SSL connections. The `ssltool` command has the following subcommands:

- **sclient** -This is CLI version of openssl s_client command. It will connect to a remote host using SSL/TLS directly without using the appliance.
  - `COMMAND` - Executes an openssl s_client command. The following openssl s_client commands are supported:

```
-connect, -servername, -verify, -cipher, -verify_return_error, -reconnect, -pause,
 -showcerts, -prexit, -state, -debug, -msg, -tls1, -tls1_1, -tls1_2, -no_ssl2,
-no_ssl3, -no_tls1, -no_tls1_1, -no_tls1_2, -tlsextdebug, -no_ticket, -status,
-save, -noout
```

See the inline help for more information about the supported openssl s_client commands .



Note After you execute the `command`, you can save the output to a file using the `-save` option. You cannot access the saved log files. These log files are used by Cisco support team for debugging.

- `HELP -` Provides help information.

- **`CLEARLOGS`** -Deletes all logs generated by `ssltool`.

status

Displays system status.

supportrequest

Send the support request email to Cisco Customer Support. This includes system information and a copy of the primary configuration.

(Optional) If you provide the service request number, a larger set of system and configuration information is added to the service request automatically. This information is zipped and uploaded to the service request using FTP.

tail

Displays the end of a log file. Command accepts log file name as parameter.

Example 1

```
example.com> tail
Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll
…
…
Enter the number of the log you wish to tail.
[]> 9
Press Ctrl-C to stop scrolling, then `q` to quit.
~
~
Thu Dec 14 10:03:07 2017 Info: Begin Logfile
~
~
…
…
"CTRL-C" + "q"
```

Example 2

```
example.com> tail system_logs
Press Ctrl-C to stop scrolling, then `q` to quit.
~
```

```
~
Thu Dec 14 09:59:10 2017 Info: Begin Logfile
…
…
"CTRL-C" + "q"
```

tcpservices

Displays information about open TCP/IP services.

techsupport

Provides a temporary connection to allow Cisco Customer Support to access the system and assist in troubleshooting.

testauthconfig

Tests the authentication settings for a given authentication realm against the authentication servers defined in the realm.

testauthconfig [-d level] [realm name]

Running the command without any option causes the appliance to list the configured authentication realms from which you can make a selection.

The debug flag (`-d`) controls the level of debug information. The levels can range between 0-10. If unspecified, the appliance uses a level of 0. With level 0, the command will return success or failure. If the test settings fail, the command will list the cause of the failure.



Note Cisco recommends you use level 0. Only use a different debug level when you need more detailed information to troubleshoot.

tuiconfig tuistatus

These two commands are documented in Using the CLI to Configure Advanced Transparent User Identification Settings.

traceroute

Traces IP packets through gateways and along the path to a destination host.

trailblazerconfig

You can use the `trailblazerconfig` command to route your incoming and outgoing connections through HTTP and HTTPS ports on the new web interface.



Note By default, `trailblazerconfig` CLI command is enabled on your appliance. You can see the inline help by typing the command: `help trailblazerconfig`.

The syntax is as follows:

```
trailblazerconfig enable <https_port> <http_port>

trailblazerconfig disable

trailblazerconfig status
```

Where:

`'enable'` runs the trailblazer on the default ports (HTTPS: 4431 or HTTP: 801).

`'disable'` terminates the trailblazer

`'status'` checks the status of the trailblazer.



Note If you have enabled `trailblazerconfig` command on the appliance, the request URL will contain the HTTP/HTTPS port number appended to the hostname.

You can try any one of the following steps to make the navigation in your browser seamless:

- Accept the certificate used by the web interface and use the following URL syntax: `https://hostname:<https_api_port> (for example, https://some.example.com:6443)` in a new browser window and accept the certificate. Here `<https_api_port>` is the AsyncOS API HTTPS port configured in **Network > IP Interfaces**. Also, ensure that the API ports (HTTP/HTTPS) are opened on the firewall.
- By default, `trailblazerconfig` CLI command is enabled on your appliance. Make sure that the HTTP/HTTPS ports are opened on the firewall. Also ensure that your DNS server can resolve the hostname that you specified for accessing the appliance.

  If the `trailblazerconfig` CLI command is disabled, you can run the **trailblazerconfig** > **enable** command using the CLI to avoid the following issues:

  - Requiring to add multiple certificates for API ports in certain browsers.
  - Redirecting to the legacy web interface when you refresh the Spam quarantine, Safelist or Blocklist page.
  - Metrics bar on the Advanced Malware Protection report page does not contain any data.

updateconfig

Configure update and upgrade settings.

updatenow

Update all components.

upgrade

Install the Async OS software upgrade.

`downloadinstall` – Download and immediately install an upgrade package.

`download` – Download and save upgrade package for installation later.

After you enter either of these commands, a list of upgrade packages applicable for this Secure Web Appliance is displayed. Select the desired package by entering its entry number and then pressing Enter; download begins in the background. During download, additional subcommands are available: `downloadstatus` and `canceldownload`.

When download is complete, if you initially entered `downloadinstall`, installation begins immediately. If you entered `download`, two additional commands are available when download is complete: `install` and `delete`. Enter `install` to begin installing a previously downloaded package. Use `delete` to remove the previously downloaded package from the Secure Web Appliance.

userconfig

Configure system administrators.

version

Displays general system information, installed versions of system software, and rule definitions.

wccpstat

`all` - Displays details of all WCCP (Web Cache Communication Protocol) service groups.

`servicegroup` - Displays details of a specific WCCP service group.

webcache

Examine or modify the contents of the proxy cache, or configure domains and URLs that the appliance never caches. Allows an administrator to remove a particular URL from the proxy cache or specify which domains or URLs to never store in the proxy cache.

who

Displays users logged into the system, for both CLI and Web interface sessions.



Note Individual users can have a maximum of 10 concurrent sessions.

whoami

Displays user information.