McAfee™
Together is power.

McAfee Advanced Threat Defense 4.6.0 Command Line Interface Reference Guide

CLI commands

The Advanced Threat Defense Appliance supports command-line interface (CLI) commands for tasks such as network configuration, restarting the appliance, and resetting the appliance to factory defaults.

Issuing CLI commands

You can issue CLI commands locally, from the Advanced Threat Defense Appliance console, or remotely through SSH.

Issuing commands

To perform an operation on the Advanced Threat Defense Appliance, you must perform the operation from the command line of the console host that connects to the Advanced Threat Defense Appliance. For example, when you first configure the network details for the Advanced Threat Defense Appliance, you must do so from the console.

Issuing a command through SSH

You can administer a Advanced Threat Defense Appliance remotely from a command prompt over `ssh`.

Log on to the Advanced Threat Defense Appliance

Use the SSH client to log on to the Advanced Threat Defense Appliance.

Task

1. Open an SSH client session.
2. Enter the Advanced Threat Defense Appliance IPv4 address.
3. Enter 2222 as the SSH port number.

4 Enter the log on credentials.

- User name — cliadmin
- Password — atdadmin

If you are logging on for the first time, you are prompted to changed the user name and password.

You can change the CLI password by logging on to Advanced Threat Defense web interface.

1 Go to **Manage** | **Security** | **Advanced Security Settings** | **Password Control**.

2 Click **Click here to reset CLI user password**.

Depending on your SSH client, the number of logon attempts differ. For example, Putty 0.54 and 0.56 allow you three log on attempts, and Putty 0.58 and Linux SSH clients allow you four attempts.

Auto-complete

The CLI allows you to auto-complete commands.

To auto-complete a command, press **Tab** after typing a few characters of a valid command and then press **Enter**. For example, typing `pas` and pressing **Tab** would result in the CLI auto-completing the entry with the command `passwd`.

If the partially entered text matches multiple options, the CLI displays all available matching commands.

CLI syntax

You issue commands at the command prompt as shown.

```
<command> <value>
```

- Values that you must enter are enclosed in angle brackets (< >).
- Optional keywords or values are enclosed in square brackets ([ ]).
- Options are shown separated by a line (|).
- Variables are indicated by *italics*.

Do not type the < or [ ] symbols.

Mandatory commands

There are certain commands that must be executed on the Advanced Threat Defense Appliance before it is fully operational. The remaining commands in this chapter are optional and will assume default values for their parameters unless they are executed with other specific parameter values.

These are the required commands:

- `set appliance name`
- `set appliance ip`
- `set appliance gateway` is also required if any of the following are true:
  - If the Advanced Threat Defense Appliance is on a different network than the McAfee products you plan to integrate
  - If you plan to access Advanced Threat Defense from a different network either using an SSH client or a browser for accessing the Advanced Threat Defense web interface

Log on to the CLI

Before you can enter CLI commands, you must first log on to the Advanced Threat Defense Appliance with a valid user name (default user name is `cliadmin`) and password (default is `atdadmin`).
To log off, type `exit`.

Change the password using the `passwd` command within your first interaction with the Advanced Threat Defense Appliance.

Meaning of "?"

`?` displays the possible command strings that you can enter.
Syntax

```
?
```

If you use `?` in conjunction with another command, it shows the next word you can type. If you execute the ? command in conjunction with the `set` command, for example, a list of all options available with the `set` command is displayed.

List of CLI commands

This section lists Advanced Threat Defense CLI commands in the alphabetical order.

activeResponseStats

Displays the statistics on McAfee Active Response and McAfee Advanced Threat Defense integration.
Syntax:

```
activeResponseStats
```

This command has no parameters.

Example:

```
activeResponseStats
[ Active Response Statistics ]
Status                      : DISABLED
Request Files Received      : 0
Search in Pending state     : 0
Search in Completed state   : 0
ERROR COUNT                 : 0
```

amas

Use this command to restart/start/stop the amas services.

`amas restart` is no longer available.

Syntax: `amas <word>`

Parameter	Description
<WORD>	The amas service you want to stop.

Example: `amas start/stop`

archive-submission-status

Displays status of the archive samples submitted to Advanced Threat Defense system.

Syntax: `archive-submission-status`

This command has no parameters.

Sample output:

```
[ Zip adapter stats]
Status

      : UP
Archive samples
received
                  : 0
Invalid archive
received
                  : 0
Archive successfully
processed                                                                    : 0
Samples found by extracting archives                                           :
0
Samples (extracted from zip) submitted to amas    : 0
```

atdcounter

Displays the engine specific counter e.g. files sent and processed by McAfee GTI, Anti-Virus Engine, Gateway Anti-Virus Engine, and amas.

Syntax: `atdcounter`

This command has no parameters.

backup reports

Use this command to create a backup of the McAfee Advanced Threat Defense reports on an external FTP/SFTP server configured for a user under the FTP results output setting interface ports.

Syntax

`backup reports`

This command has no parameters.

backup reports date

This command creates a backup of the McAfee Advanced Threat Defense reports for a particular date range on an external FTP/SFTP server configured for a user under the FTP results output setting.

Syntax: `backup reports date <yyyy-mm-dd>`

Parameter	Description
yyyy-mm-dd yyyy-mm-dd	The date range for which you want to create a backup for reports.

Example: `2014-07-10 2014-07-12`

Blacklist

Use the following commands to manage the McAfee Advanced Threat Defense blacklist.

Syntax:

- To add an MD5 to the blacklist, use `blacklist add <md5> <score> <file_name> <malware_name> <Eng-ID> <OS-ID>`

Parameter	Description
<md5>	The MD5 hash value of a malware that you want to add to the blacklist.
<score>	The malware severity score. A valid value is from 3 to 5.
<file_name>	The file name for the MD5.
<malware_name>	The malware name for the MD5.
<Eng-ID>	The numerical ID for the engine that detected the malware. Following is the numerical coding. Sandbox — 0, GTI — 1, GAM — 2, Anti-Malware — 4.
<OS-ID>	The numerical ID of the operating system that was used to dynamically analyze the malware.

  Example: `blacklist add 254A40A56A6E28636E1465AF7C42B71F 3 ExampleFileName ExampleMalwareName 4 2`

- To delete an MD5 from the blacklist, use `blacklist delete <md5>`

Parameter	Description
<md5>	The MD5 hash value of a malware that you want to delete from the blacklist.

  Example: `blacklist delete 254A40A56A6E28636E1465AF7C42B71F`

- To check if an MD5 is present in the blacklist, use `blacklist query <md5>`

Parameter	Description
<md5>	The MD5 hash value of a malware that you want to query if it is present in the blacklist.

  Example: `blacklist query 254A40A56A6E28636E1465AF7C42B71F`

  If the MD5 is present, the details such as the engine ID, malware severity score, and so on, are displayed.

- To update the details for an entry in the blacklist, use `blacklist update <md5> <score> <file_name> <malware_name> <Eng-ID> <OS-ID>`

Parameter	Description
<md5>	The MD5 hash value of a malware that you want to update. This value must exist in the blacklist for you to update the record.
<score>	The new malware severity score that you want to change to. A valid value is from 3 to 5.
<file_name>	The new file name for the MD5.
<malware_name>	The new malware name for the MD5.
<Eng-ID>	The new engine ID that you want to change to.
<OS-ID>	The new value for the operating system that was used to dynamically analyze the malware.

  Example: `blacklist update 254A40A56A6E28636E1465AF7C42B71F 4 ExampleFileName ExampleMalwareName 2 4`

clearstats all

Use this command to reset all the McAfee Advanced Threat Defense statistics to zero.

Syntax: `clearstats all`

This command has no parameters.

The following information is displayed using this command:

```
<=== DXL STATUS ===>
Status                                  : DISABLED
DXL Channel Status                      : DOWN
Sample Files Received Count             : 0
Sample Files Published Count            : 0
Sample Files Queued Count               : 0
```

clearstats ActiveResponse

Clears all previous statistics from McAfee Active Response and McAfee Advanced Threat Defense integration.

Syntax:

```
clearstats ActiveResponse
```

This command has no parameters.

Example:

```
clearstats ActiveResponse
All Active Response stats are reset to zero
Request Files Received          : 0
Search in Pending state         : 0
Search in Completed state       : 0
Response from MAR               : 0
```

clearstats dxl

Resets the DXL file counter to zero.

Syntax: `clearstats dxl`

This command has no parameters.

The following information is displayed using this command.

```
All DXL stats are reset to zero
Sample Files Received Count             : 0
Sample Files Published Count            : 0
```

clearstats tepublisher

Clear the count of events sent to McAfee ePO.

Syntax: `clearstats tepublisher`

This command has no parameters.

The following information is displayed using this command:

```
All TEP stats are reset to zero
Sample Files Received Count             : 0
Sample Files Published Count            : 0
```

clearstats taxii

Use this command to reset all TAXII stats to zero.

Syntax: `clearstats taxii`

clearlbconfig

This command is used to destroy cluster using CLI command prompt. It is permitted to run at all nodes (Primary/Backup/Secondary). It wipes out all cluster related configurations from that node and makes it as a standalone box.

This command can be used in scenarios where normal means of removing a node (Remove Node/Withdraw From Cluster) does not remove that node from cluster.

When you execute the clearlbconfig command on a Primary or Active node, you must execute the command on all other nodes in the cluster.

Syntax: `clearlbconfig`

This command has no parameters.

createDefaultVms

Delete all of the existing analyzer VMs and create default analyzer VMs.

Syntax: `createDefaultVms`

This command has no parameters.

This command will not work on the non-active nodes in the cluster.

db_repair

Repairs the Advanced Threat Defense database when the database is corrupt.

Syntax: `db_repair`

This command has no parameters.

deleteblacklist

Remove all the entries from the Advanced Threat Defense blacklist.

Syntax: `deleteblacklist`

This command has no parameters.

deletesamplescore <0-5>

Deletes all sample reports with the specified severity score.

Syntax:

`deletesamplescore <0-5>`

Parameter	Description
<0-5>	Enter a severity score between 0 to 5.

Example:

```
deletesamplescore 0
Deleting all sample results with score=0
delete 0 sample entries with 0
```

deletesamplereport

Deletes all of the analysis reports for a file.

Syntax: `deletesamplereport <md5>`

Parameter	Description
<md5>	The file MD5 value that you want to use to delete all the reports in Advanced Threat Defense.

Example: `deletesamplereport c0850299723819570b793f6e81ce0495`

diskcleanup

Delete old analysis reports when the Advanced Threat Defense disk space is low.

Syntax: `diskcleanup`

This command has no parameters.

To prevent Advanced Threat Defense from losing your results and reports, enable set resultbackup.

dxlstatus

View the DXL status.

Syntax: `dxlstatus`

This command has no parameter.

The following information is displayed using this command:

```
<=== DXL STATUS ===>
Status                                  : DISABLED
DXL Channel Status                      : DOWN
Sample Files Received Count             : 0
Sample Files Published Count            : 0
Sample Files Queued Count               : 0
```

Exit

Exits the CLI.

This command has no parameters.

Syntax:

`exit`

factorydefaults

Deletes all samples, results, logs, and analyzer VM images, then resets the IP addresses before rebooting the device. This command does not appear when you type `?` nor does the auto-complete function applies to this command. You must type the command in full to execute it.

This command has no parameters.

- You are warned that the operation will clear Advanced Threat Defense Appliance and you must confirm the action. The warning occurs since the Advanced Threat Defense Appliance returns to its clean, pre-configured state, thus losing all current configuration settings in both the active and backup disks. Once you confirm, this command immediately clears all your configuration settings, including samples, results, logs, and analyzer VM images, in both the active and backup disks.
- The current software version in the backup disk is applied on the active disk.

Syntax:

```
factorydefaults
```

filetypefilter

Enables Advanced Threat Defense to use the file extension that the file carries before sending it for dynamic analysis.

Syntax:`filetypefilter<enable><disable><status>`

Parameter	Description
status	Displays whether the filetypefilter feature is enabled or disabled. By default, it is disabled.
enable	Enables sample filtering. When enabled, Advanced Threat Defense uses the following supported file types for analysis: *.7z, .ace, .apk, .arj, .bat, .cab, .cgi, .chm, .class, .cmd, .com,* *.dll, .doc, .docm, .docx, .dotm, .dotx, .eml, .exe, .htm,* *.html, .inf, .ins,. js, .lnk, .lzh, l.zma, .mof, .msg,* *.ocx, .pdf, .potm, .potx, .ppam, .pps, .ppsm, .ppsx*
disable	Disables sample filtering. When disabled, Advanced Threat Defense uses the default file types that dynamic analysis supports.

ftptest

Tests the FTP settings.

Syntax: `ftptest USER_NAME`

Parameter	Description
USER_NAME	The user name that you want to test the FTP settings.

Example: `NSPuser`

gti-restart

Restarts the McAfee GTI engine.

Syntax: `gti-restart`

This command has no parameters.

help

Provides a description of the interactive help system.

This command has no parameters.

Syntax:

```
help
```

http_redirect

Enables or disables the redirection of http browser requests to https. When http_redirect is disabled, secure access to the Advanced Threat Defense Appliance is ignored.

Syntax:

```
set http_redirect
```

When port 80 is disabled, then the HTTP port is used to access the Advanced Threat Defense Appliance interface in a browser.

Any sample that you submit during the command execution is rejected as lighttpd is restarted.

Parameter	Description
enable Advanced Threat Defense Appliance	When http_redirect is enabled, the http url is redirected to https. RestAPI calls with only the https protocol are accepted.
disable	When http_redirect is disabled, http is not redirected to https. RestAPI calls with the http or https protocol are accepted.

Make sure http_redirect is always enabled. Disable http_redirect only when there are issues with certificate validation.

To view if http to https redirection is enabled or disabled on the Advanced Threat Defense Appliance, use the show http_redirect command. By default, the redirect feature is enabled.

Syntax: `show http_redirect`

install msu

Installs system-x.x.x.x.x.msu.

Syntax:

```
install msu
```

Parameter	Description
<SWNAME>	The msu filename that you want to install.
<RESET_DB>	Accepts the following values: • 0 — msu file installs without resetting the database • 1 — msu file install and the database is reset

Example: `install msu system-x.x.x.x.x.msu 1`

install package <package path>

Installs the detection or application package in the background.

Before you run this command, SFTP the install package to your Advanced Threat Defense Appliance with atdadmin user account.

Syntax:

```
install package <package path>
```

Parameter	Description
<package path>	Enter the package path and name.

lbservice restart/status

Use this command to restart the LB services or to check the status of LB services.

Syntax:

```
lbservice <restart>/<status>
```

Example:

```
ATD-3000> lbservice status

lbservice is running

ATD-3000> lbservice restart

lbservice restarted

ATD-3000>
```

lbstats

Shows the statistics for Primary node, Back up node and Secondary node in a load-balancing cluster.

This command has no parameters. No output is displayed if the Advanced Threat Defense is not part of a cluster.

Syntax:

```
lbstats
```

list

Lists all of the available CLI commands.

Syntax: `list`

This command has no parameters.

lowseveritystatus

Advanced Threat Defense treats severity 1 and 2 samples as low-severity, and severity 3, 4, and 5 as malicious. By default, when you configure dynamic analysis, the dynamic analysis score is displayed in the summary report for all samples. The score also affects the final score for the sample. You can use the lowseveritystatus command to alter the behavior. For example, for low-severity samples that are dynamically analyzed, Advanced

Threat Defense does not display the dynamic analysis score in the summary report, or consider the score to compute the final score.

The lowseveritystatus command applies only to non-PE samples, such as Microsoft Word documents and PDF files.

Syntax: `lowseveritystatus <show><hide>`

Example: `lowseveritystatus hide`

Parameter	Description
`show`	The default behavior. If a sample is dynamically analyzed, Advanced Threat Defense displays the dynamic analysis score in the report. It also considers the score to compute the final score.
`hide`	Assume that the sample is a non-PE file, which has undergone dynamic analysis. If Advanced Threat Defense detects the file to be low-severity, it does not display the dynamic analysis score in the report (under **Sandbox** in the **Down Selector's Analysis** section). Advanced Threat Defense also does not consider the dynamic analysis score for computing the final score. However, the details of the dynamic analysis such as files opened and files created are included in the report.  The lowseveritystatus hide command affects only the score displayed in the report and does not affect how the results are displayed in the **Analysis Reports** page.

no malware-dns

Use this command to configure the malware dns to the default 127.0.0.1.

Syntax:

no malware-dns

no timeout

Removes timeout for SSH sessions.

Syntax:

`no timeout`

This command has no parameters.

nslookup

Queries the results for domain names. You can use nslookup to verify if Advanced Threat Defense can perform nslookup queries correctly.

Syntax: `nslookup <WORD>`

Parameter	Description
<WORD>	The domain name that you want to query for nslookup.

Example: `nslookup mcafee.com`

passwd

Changes the password of the CLI cliadmin user.

A password must be between 8 and 25 characters in length and can consist of any alphanumeric character or symbol.

You are asked to enter the current password before changing to a new password.

Syntax:

```
passwd
```

ping

Pings a network host or domain name. You can specify an IPv4 address to ping network host and domain name to ping domain names.

Syntax:

```
ping <A.B.C.D>
```

Parameter	Description
<A.B.C.D>	Denotes the 32-bit network host IP address written as four eight-bit numbers separated by periods. Each number (A, B, C or D) is an eight-bit number between 0–255.
<WORD>	The domain name that you want to ping.

quit

Exits the CLI.

This command has no parameters.

Syntax:

```
quit
```

reboot

Reboots the Advanced Threat Defense Appliance with the image in the current disk. You must confirm that you want to reboot.

Syntax:

`reboot` or `reboot <parameter>`

Parameter	Description
`vmcreator`	Recreates the analyzer VMs configured in the Advanced Threat Defense web interface, while rebooting the appliance.
`force`	Force reboots your Advanced Threat Defense.

remove

This command removes all original samples from ATD for which analysis is complete.

The remove command has these parameters:

- `now`: When executed, immediately removes the *original samples* for all the completed samples present on ATD. Even if you enable **Sample Download Access**, you cannot download the sample.
- `enable`: When executed, immediately removes the *original samples* for all the completed samples present on ATD. It also enables you to set a daily task to automatically remove *original samples* from newly completed samples at a configured time.
- `disable`: When executed, disables the daily task to remove *original samples* from newly completed sample files at the configured time.

Syntax: `remove samples all <now><enable><disable>`

Example 1: `ATD-6000> remove samples all now`

```
Removing all sample files now...

10 sample files removed
```

Example 2:
```
ATD-6000> remove samples all enable 11:37:14

Removing all sample files now...

14 sample files removed

Setting up daily task to remove newly completed sample files at 11:37:14
```

Example 3:
```
ATD-6000> remove samples all disable

Disabling daily task
```

removeAndroid

Remove the Android VM from the VM profile list.

Ensure that Android is not the default VM profile and the Vmcreator process is not running

Syntax: removeAndroid

This command has no parameters.

Sample Output:

```
ATD_1U_21> removeAndroid

Started deleting the android VM

Successfully deleted the android VM
```

This command will not work on the non-active nodes in the cluster.

removenetworkaddress

Removes the IP, subnet mask, and gateway addresses from the Advanced Threat Defense Appliance.

The changes are reflected after the box is rebooted. This is a hidden command, but is useful for Support.

Syntax: `removenetworkaddress`

This command has no parameters.

Example:
```
ATD-6000> removenetworkaddress

Remove the appliance network addresses ?

Please enter Y to confirm:
```

removeSampleInWaiting

Remove all of the samples to be analyzed by Advanced Threat Defense.

Syntax: `removeSampleInWaiting`

This command has no parameters.

The following information is displayed using this command:

```
Starting the sample queue cleaning...
The cleaning is done
```

removevmImage

To delete the VM Image from all nodes in the LB cluster when option is specified as **all**, execute this command from Primary[Active] or Backup[Active] Advanced Threat Defense.

If option is specified as A.B.C.D, it deletes the Image only from Secondary with IP A.B.C.D.

Reduce the License count for ImageName to zero before executing this command, or the command execution fails. This command does not delete the ImageName from Active (Primary/Backup) Advanced Threat Defense.

To obtain ImageName, use the show vmImage command.

Syntax:

```
removevmImage <ImageName> <all | A.B.C.D>
```

Example:

```
removevmImage winxpsp3 all
```

```
removevmImage winxpsp3 10.34.2.1
```

resetuiadminpasswd

Resets the Advanced Threat Defense web interface administrator password. When you use the command, the password is reset to the default value, which is admin. The currently logged on sessions are unaffected. A change in password affects only new logon attempts.

Syntax: `resetuiadminpasswd`

Press Y to confirm, or N to cancel.

resetusertimeout

Enables you to log on to Advanced Threat Defense web interface without waiting for the timer to expire.

Syntax: `resetusertimeout <WORD>`

Parameter	Description
<WORD>	The Advanced Threat Defense web interface user name that you want to remove the logon timer. When the action is successful, the **Reset done!** message displays.

Example: `resetusertimeout admin`

revert package application

Revert the current application software package and install the backup application software as current.

Syntax: `revert package application`

This command has no parameters.

Use this command when you cannot revert the application software from the Advanced Threat Defense interface.

revert package detection

Revert the current detection software package and install the backup detection package as current.

Syntax: `revert package detection`

Use this command when you cannot revert the application software from the Advanced Threat Defense interface.

revertwebcertificate

Revert the uploaded web certificate to the default certificate.

Syntax: `revertwebcertificate`

This command has no parameters.

The following information is displayed using this command:

```
revertwebcertificate
Successfully reverted back web certificate to default!
Restarting lighttpd service!
```

route add/delete network

CLI commands are available for adding and deleting static routes to Advanced Threat Defense.

To add a port

`route add network <network ip> netmask <netmask> gateway <gateway ip> intfport <port number 1><port number 2><port number 3>`

Example: `route add network 1.1.1.0 netmask 255.255.255.0 gateway 1.1.1.1 intfport 1`

To delete a port

`route delete network <network ip> netmask <netmask> gateway <gateway ip> intfport <port number 1><port number 2><port number 3>`

Example: `route delete network 1.1.1.0 netmask 255.255.255.0 gateway 1.1.1.1 intfport 1`

run ldt

This command allows you to collect ldt logs, abort the collection, and check the status of a running collection task.

Syntax: `run ldt <parameter>`

Parameter	Description
tool	Collects LDT logs.
status	Displays the status of LDT log collection
abort	Stops the log collection task.

```
run ldt tool
NOTICE: running the log collection tool may impact system performance.
Running LDT log collection. Please stand by.
LDT log collection has been started
```

samplefilter

This command is specific to Network Security Platform Sensors and all REST channel submissions. Use this command to prevent Sensors from sending unsupported file types to McAfee Advanced Threat Defense for analysis.

Syntax:

```
samplefilter <status><enable><disable>
```

Parameter	Description
status	displays whether the sample filtering feature is enabled or disabled currently. By default, it is enabled.
enable	sets the sample filtering on. When it is enabled, McAfee Advanced Threat Defense considers only the supported file types from Network Security Platform for analysis. McAfee Advanced Threat Defense ignores all other file types and also informs Network Security Platform that a sample is of an unsupported file type . This prevents resources being spent on unsupported file types on both McAfee Advanced Threat Defense and Network Security Platform.
disable	sets the sample filtering to off. When disabled, McAfee Advanced Threat Defense considers all the files submitted by Network Security Platform for analysis but only the supported file types are analyzed. The remaining are reported as unsupported in the **Analysis Status** and **Analysis Reports** pages.

Example:

```
samplefilter status
```

service

Use this command to perform service-related tasks such as starting, stopping, restarting, or getting the status of services.

Syntax: `service <parameter> <argument>`

Parameter	Description
start	Starts a service.
stop	Stops a service.
status	Displays the status of one or more services. If you need to see the status of all ATD services, enter `service status all`
restart	Restarts a service.

```
service status all

VM creation in progress, amas service is down until completed.

amas service [ STOPPED ]

dxl service [ RUNNING ]

MA service [ RUNNING ]

LB service [ RUNNING ]

nginx service [ RUNNING ]

mysql service [ RUNNING ]

system networking [ RUNNING ]
```

set appliance dns A.B.C.D E.F.G.H WORD

Configures the Advanced Threat Defense Appliance preferred and alternate DNS address.

Syntax:

```
set appliance dns A.B.C.D E.F.G.H WORD
```

Parameter	Description
<A.B.C.D>	DNS preferred address
<E.F.G.H>	DNS alternate address
<WORD>	Appliance domain name

Example: `ATD-6000> set appliance dns 1.1.1.2 10.11.10.4 nai.com`

```
DNS setting had been configured
```

set port80

Allows you to access Advanced Threat Defense interface from a web browser through HTTP port 80.

Syntax

```
set port80 <enable/disable>
```

Parameter	Description
<enable>	The Advanced Threat Defense interface can be accessed using the *https://<Advanced Threat Defense IP address>* link from a browser. (Replace Advanced Threat Defense IP address with the actual IP address)
<disable>	The Advanced Threat Defense interface can't be accessed from a browser.

Delete the browser cache before you access the Advanced Threat Defense interface.

If you disable port 80, the http redirect will also not work.

Example

```
set port80 enable
Enabling HTTP port 80
Http port 80 enabled
```

set appliance gateway

Specifies the IPv4 address of the gateway for the Advanced Threat Defense Appliance.

Syntax:

```
set appliance gateway <A.B.C.D>
```

Parameter	Description
<A.B.C.D>	A 32-bit address written as four eight-bit numbers separated by periods. A, B, C or D represents an eight-bit number between 0–255.

Example:

```
set appliance gateway 192.34.2.8
```

set appliance ip

Specifies the Advanced Threat Defense Appliance IPv4 address and subnet mask. Changing the IP address requires a restart for the changes to take effect. See the `reboot` command for instructions on how to reboot the Advanced Threat Defense Appliance.

Syntax:

```
set appliance ip <A.B.C.D E.F.G.H>
```

Parameter	Description
<A.B.C.D E.F.G.H>	Indicates an IPv4 address followed by a netmask. The netmask strips the host ID from the IP address, leaving only the network ID. Each netmask consists of binary ones (decimal 255) to mask the network ID and binary zeroes (decimal 0) to retain the host ID of the IP address(For example, the default netmask setting for a Class C address is 255.255.255.0).
dhcp	Allows Advanced Threat Defense Appliance to receive its IP configuration from a DHCP server.

Example:

```
set appliance ip 192.34.2.8 255.255.0.0
```

set appliance name

Sets the name of the Advanced Threat Defense Appliance. This name is used to identify the Advanced Threat Defense Appliance if you integrate it with Network Security Platform.

Syntax:

```
set appliance name <WORD>
```

Parameter	Description
<WORD>	Indicates a case-sensitive character string up to 25 characters. The string can include hyphens, underscores, and periods, and must begin with a letter.

Example:

```
set appliance name SanJose_MATD1
```

set gti dns check

This command requires DNS to be set for McAfee GTI to work. By default this command is set to disabled, which means that if there is no internet access, McAfee GTI works fine. If this command is enabled, McAfee GTI will not work unless Advanced Threat Defense is connected to the Internet and resolves McAfee GTI lookup URLs. You need to restart amas for these changes to reflect in Advanced Threat Defense.

Syntax: `set gti dns check <enable><disable>`

Example: `ATD-6000> set gti dns check enable`

```
DNS access check is now enabled

ATD-6000> set gti dns check disable

DNS access check is now disabled
```

set gti server ip <Private Cloud IP>

Sets to a valid GTI Private Cloud using its IP address.

Syntax:

```
set gti server ip <Private Cloud IP>
```

Parameter	Description
<Private Cloud IP>	Enter the IP address for the GTI Private Cloud.

set gti server url <Domain Name>

Sets to a valid GTI Private Cloud using its URL.

Syntax:

```
set gti server url <Domain Name>
```

Parameter	Description
<Domain name>	Enter the URL for the GTI Private Cloud.

set gti server ip 0.0.0.0

Resets GTI to Public Cloud.

Syntax:

```
set gti server ip 0.0.0.0
```

set gti server url 0.0.0.0

Resets GTI to Public Cloud.

Syntax:

```
set gti server url 0.0.0.0
```

set intfport

Enable or disable the Advanced Threat Defense interface ports.

Syntax:

```
set intfport <1><2><3> <enable><disable>
```

Example: `set intfport 1 enable`

set intfport <1-3> ipdelete <ip address>

Removes IP addresses assigned to an interface.

Syntax:

```
set intfport <1-3> ipdelete <ip address>
```

Parameter	Description
<1-3>	Enter one of the three available ports.
<ip address>	Enter the IP address that you want to remove.

Example:

```
set intfport 1 ipdelete 0.0.0.0
Interfaceport 1 IP deleted successfully
```

set intfport auto

Sets an interface port to auto-negotiate the connection with the immediate network device.

Syntax:

```
set intfport <1><2><3> auto
```

Example:

```
set intfport 1 auto
```

set intfport ip

Sets an IP address to an interface port.

Syntax:

```
set intfport <1><2><3> ip A.B.C.D E.F.G.H
```

Example:

```
set intfport 1 10.10.10.10 255.255.255.0
```

set intfport speed duplex

Configures the speed and duplex setting on the specified interface port.

Syntax:

```
set intfport <1><2><3> speed <10 | 100> duplex <half | full>
```

Parameter	Description
<1> <2> <3>	Specifies the interface port ID that you want to use to configure the speed and duplex.
<10 | 100>	Configures the speed on the interface port. The speed value can be either 10 or 100.
<half | full>	Configures the duplex setting on the interface port. Set the value "half' for half duplex, and full for 'full' duplex.

Example:

```
set intfport 1 speed 100 duplex full
```

set ipAddressSwap

When you submit samples for analysis through Network Security Platform, the source and destination IP information is swapped for the submitted samples.

To reverse the aberration caused by Network Security Platform, Advanced Threat Defense enables `set IPAddressSwap` command. This command nullifies the swap effect of Network Security Platform and displays the correct the source and destination IP information for samples submitted through Network Security Platform. When samples are submitted from McAfee NGFW to Advanced Threat Defense, the source and destination IP information are displayed correctly. Based on the preference, you can use the following command to enable or disable IPAddressSwap.

Syntax: `set ipAddressSwap <enable><disable>`

By default, set ipAddressSwap is enabled.

Example: `set ipAddressSwap enable`

set ldap enable|disable

Enables or disables LDAP authentication. Make sure that all LDAP parameters are configured correctly in the web interface to use this command LDAP.

Syntax:

```
set ldap enable|disable
```

Parameter	Description
enable	Enables LDAP authentication.
disable	Disable LDAP authentication.

Example:

```
set ldap disable
Disabling ldap support...

Note:
Authentication method got changed!
Terminating matdcli session in 10 seconds!
Please login again!
```

set malware-dns

Use this command to configure the malware DNS IP that Advanced Threat Defense uses to route the malware DNS queries.

Syntax: set malware-dns

Example:`set malware-dns 192.168.200.110`

set malware-intfport

Configure the required port to route Internet traffic from an analyzer VM.

Before you run this command, make sure that the required port is enabled and configured with an IP address.

Syntax: `set malware-intfport <1><2><3> gateway A.B.C.D`

Example: `set malware-intfport 1 10.10.10.252`

Run the `show intfport 1` and verify the `Malware Interface Port` and `Malware Gateway` entries.

Advanced Threat Defense uses the configured port to provide Internet access to analyzer VMs.

set mgmtport auto

Configures the network port to auto-negotiate the connection between the Advanced Threat Defense Appliance and the immediate network device.

This command has no parameters.

Syntax:

```
set mgmtport auto
```

Default Value:

By default, the network port is set to **auto** (auto-negotiate).

set malware-intfport mgmt

By default, Internet access to analyzer VMs is through the McAfee Advanced Threat Defense's management port (eth-0). Use this command, if you had configured a different port for routing Internet traffic and want to revert to the management port.

Syntax: `set malware-intfport mgmt`

Run the `show intfport mgmt` and verify the `Malware Interface Port` and `Malware Gateway` entries.

McAfee Advanced Threat Defense uses the management port to provide Internet access to analyzer VMs.

set mgmtport speed and duplex

Configures the network port to match the speed of the network device connecting to the Advanced Threat Defense Appliance, then runs in full- or half-duplex mode.

Syntax:

```
set mgmtport <speed <10 | 100> duplex <full | half>>
```

Parameter	Description
<10|100>	Specifies the speed on the Ethernet network port. The speed value can be either 10 or 100 Mbps. To set the speed to 1000 Mbps, use the set mgmtport auto command.
<half|full>	Specifies the duplex setting on the Ethernet network port. • half — Half duplex • full — Full duplex

Default Value:

By default, the network port is set to **auto** (auto-negotiate).

set pdflinks

Enable or disable validation operation performed by McAfee GTI on links embedded inside PDFs during dynamic analysis.

Syntax: `set pdflinks<enable><disable>`

Sample Output: `set pdflinks enable Enable pdflinks operation`

set filesizes

Enables you to change the minimum and maximum file sizes.

Syntax:

```
set filesizes <type number> <minimum size> <maximum size> <restart engine>
```

Parameter	Description
type number	Type of file submitted for analysis.
minimum size	Minimum file size.

Parameter	Description
maximum size	Maximum file size.
restart engine	Uses a value of 1 or 0. 1 — Restart AMAS service; this is required for NSP and NGFW integration. 0 — Keeps AMAS service running; use this when submission is through GUI/RestAPI.

Type number	File description	Minimum size	Maximum size
1	Windows portable executable (PE) exe, dll or sys file	1024 bytes	10 MB
2	PDF document file with .pdf extension	2048 bytes	25 MB
3	Java class data file with .class extension	1024 bytes	5 MB
4	Microsoft Office older files with .doc, .ppt or .xls extension	5120 bytes	10 MB
5	Microsfot rich text format file with .rtf extension	1024 bytes	10 MB
6	Zip file, APK file, or newer Microsoft Office file with .docx, .pptx or .xlsx extension	200 bytes	20 MB
7	JPEG image file	5120 bytes	1 MB
8	PNG image file	5120 bytes	1 MB
9	GIF image/bitmap file	5120 bytes	1 MB
10	Microsoft DOS executable file with .com extension	1024 bytes	5 MB
11	Flash file with .swf extension	1024 bytes	5 MB
12	7-zip compressed archive file with .7z extension	200 bytes	10 MB
13	RAR compress archive file with .rar extension	200 bytes	10 MB
14	Microsoft cabinet compressed archive file with .cab and .msi extension	200 bytes	10 MB
15	Miscellaneous text or script files, for example .js, .bat, .vbs, .xml, .url, .htm etc	100 bytes	1 MB

For example, if you want to change the minimum file size of a JPEG image file to 300 bytes, then run the command: `set filesizes 7 300 1000000 0`.

If the file size specified is beyond the minimum or maximum value listed in the above table, the following error message is displayed:

The <max><min> file size value=<numeric value specified> is invalid

Set FTP

When you upload files for analysis using an FTP client or when you import a VMDK file into Advanced Threat Defense to create an analyzer VM, you use SFTP since FTP is not supported by default. However, if you prefer to use FTP for these tasks, you can enable FTP.

In Common Criteria (CC) mode, FTP is not supported.

Syntax: `set ftp <enable><disable>`

By default, FTP is disabled.

Example: `set ftp enable`

set internal net sandbox <ip address>

Sets new IP network for the sandbox VMs.

Syntax:

`set internal net sandbox <ip address>`

Parameter	Description
<ip address>	Type the IP address that you want to set for the sandbox VMs. Use one of the following IP addresses: • 192.168.122.0 • 192.168.50.0 • 192.168.112.0

logconfig

Set the debugging mode to be applied for logs.

Syntax: `logconfig <module> <enable> | <disable>`

The following information is displayed using this command:

```
AMAS          Enable logconfig support
  Summary       Disable logconfig support
  IPS
  AvDat
  CLI
  EPO
  Monitor
  Amaslib
  GTI
  GAM
  MAV
  Scanners
  LB
  DXL
  INI
  SNMP
  YARA
  TELEMETRY
  LDAP
  CONFIG
  TEP
  RestAdapter
  WrapperTool
```

set mar-timeout

Configure a timeout period after which Advanced Threat Defense stops querying MAR server for results. The supported timeout range is 1 to 3600 seconds.

Syntax: `set mar-timeout <seconds>`

Example:

```
>set mar-timeout 60
Updated the MAR timeout value to 60 seconds
```

set nsp-ssl-channel-encryption

Use this command to configure an encrypted channel for communication between Advanced Threat Defense and Network Security Platform.

Syntax: `set nsp-ssl-channel-encryption <enable><disable>`

Example: `ATD-6000> set nsp-ssl-channel-encryption enable`

Encrypted data transfer from Network Security Platform

Use these steps for secure communication between Advanced Threat Defense and Network Security Platform.

- If encryption is enabled on Advanced Threat Defense and Network Security Platform, the data sent from Network Security Platform to Advanced Threat Defense is encrypted and uses an AES128-SHA cipher.
  - Log on to the Sensor CLI and enter into debug mode.
  - Execute `set amchannelencryption on`.
  - Log on to the Advanced Threat Defense CLI and execute `set nsp-ssl-channel-encryption enable`.
- If encryption is disabled on Advanced Threat Defense and Network Security Platform, the data sent from Network Security Platform to Advanced Threat Defense is not encrypted and uses a NULL-SHA cipher.
  - Log on to the Sensor CLI and enter into debug mode.
  - Execute `set amchannelencryption off`.
  - Log on to the Advanced Threat Defense CLI and execute `set nsp-ssl-channel-encryption disable`.

set nsp-tcp-channel enable | disable

Enables or disables communicate between Network Security Platform and Advanced Threat Defense over TCP.

Syntax:

```
set nsp-tcp-channel enable | disable
```

Parameter	Description
enable	Enable TCP channel support
disable	Disable TCP channel support

Example:

```
set nsp-tcp-channel enable
NSP TCP Channel Support Enabled and restarted service
```

set resultbackup <enable> <disable>

Use this command to back up old reports and results to the FTP server during disk cleanup. When enabled, Advanced Threat Defense backs up old reports and results before disk cleanup.

Syntax:

```
set resultbackup <enable> <disable>
```

set stixreportstatus

Use this command to enable or disable the STIX report generation.

This command has no parameters.

Syntax: `set stixreportstatus <enable><disable>`

By default, stixreportstatus is disabled.

Example: `set stixreportstatus <enable>`

set timeout <0-35791>

Sets timeout for the CLI session.

Syntax:

```
set timeout <0-35791>
```

Parameter	Description
<0-35791>	The command accepts the input value in **minutes**. The session timeout value is then displayed in seconds.

Example:

```
set timeout 600
CLI session timeout value set to 36000 seconds
```

set uilog

Sets the amount of web interface access information to be logged. Level ranges from 0 to 7.

Syntax:

```
set uilog <debuglevel>
```

Parameter	Description
<debuglevel>	Sets the amount of UI access information to be logged.

Example:

```
ATD-6000> set uilog 5

 new log level is 5
```

set ui-timeout

Specifies the number of minutes the Advanced Threat Defense web interface is inactive before the connection times out.

Syntax:

```
set ui-timeout <60 - 86400>
```

Parameter	Description
<60 - 86400>	You can set a timeout period from 60 to 86,400 seconds.

Example: `set ui-timeout 600`

Default Value: 15 minutes

show

Shows all the current configuration settings on the Advanced Threat Defense Appliance.

This command has no parameters.

Syntax: `show`

```
ATD-3000-62> show
[Appliance Info]
System Name                        : ATD-3000-62

Date                               : Tue Sep 25 11:27:34 2018
TZ Name                            : America/Los_Angeles
System Uptime                 : 20 hrs 28 min 25 secs
System Type                   : ATD-3000
Serial Number                 : A0A3308010
Software Version    : 4.6.0.2
license Status             : Valid License
Expires in                              : Never expires

MGMT Ethernet port: auto negotiated to 1000 mbps, full duplex, link up

[Appliance Network Config]
IP Address (dhcp)                 : 10.71.119.62
Netmask                                                    : 255.255.255.0
Default Gateway                         : 10.71.119.252
DNS domain                                          : nai.org
primary nameserver             : 161.69.96.5
secondary nameserver    : 161.69.5.201
```

show dat version

View the current DAT version of analyzing options.

Syntax: `show dat version`

Sample Output:

```
AV  DAT    version=7868
AV  Engine version=5700
GAM DAT    version=3811
GAM Engine version=7001.1302.1842
```

show ds status

View the status of all analyzing options.

Syntax: `show ds status`

This command has no parameters.

Sample Ouptut:

```
GTI is alive

MAV is alive

GAM is alive

Yara is alive
```

show epo-stats nsp

Displays the number of requests sent to McAfee ePO, the count of responses received from McAfee ePO, and the count of requests that failed.

Syntax: `show epo-stats nsp`

This command has no parameters.

show filequeue

Displays the file queue statistics, such as the estimated average processing time, analyzing time, and files that are pending.

This command has no parameter.

Syntax:`show filequeue`

Following is the information displayed by the `show filequeue` command:

```
Processing  Time:    58.00
Analyzing   Time:    58.00
Files in waiting: 0
files in SandBox: 0
Estimated average processing time for all samples:    58.00 seconds
```

show filesizes

Displays all the filetypes supported by Advanced Threat Defense with details such as type number, minimum and maximum file size, and short description.

This command has no parameters.

Syntax:

`show filesizes`

Following is the information displayed by the `show filesizes` command:

Type number	File description	Minimum size	Maximum size
1	Windows portable executable (PE) file, PE+ file, dll and sys file	1024 bytes	10 MB
2	PDF document file with .pdf extension	2048 bytes	25 MB
3	Java class data file with .class extension	1024 bytes	5 MB
4	Microsoft Office older files with .doc, .ppt or .xls extension	5120 bytes	10 MB
5	Microsfot rich text format file with .rtf extension	1024 bytes	10 MB
6	Zip file, APK file, or newer Microsoft Office file with .docx, .pptx or .xlsx extension	200 bytes	20 MB
7	JPEG image file	5120 bytes	1 MB
8	PNG image file	5120 bytes	1 MB
9	GIF image/bitmap file	5120 bytes	1 MB
10	Microsoft DOS executable file with .com extension	1024 bytes	5 MB
11	Flash file with .swf extension	1024 bytes	5 MB
12	7-zip compressed archive file with .7z extension	200 bytes	10 MB
13	RAR compress archive file with .rar extension	200 bytes	10 MB

Type number	File description	Minimum size	Maximum size
14	Microsoft cabinet compressed archive file with .cab and .msi extension	200 bytes	10 MB
15	Miscellaneous text or script files, for example .js, .bat, .vbs, .xml, .py, .url, .htm etc	100 bytes	10 MB

show ftp

Use this command to know if FTP is enabled or disabled currently. By default, FTP is disabled.

Syntax: `show ftp`

show gti dns

Checks the status of DNS lookup for GTI queries. If the status is enabled, then ensure that Advanced Threat Defense has access to the DNS for the GTI queries to be generated.

Syntax:

```
show gti dns
```

This command has no parameters.

Example:

```
show gti dns
DNS access check is disabled
```

show gti server

Displays the current configuration of your McAfeeMcAfee GTI integration.

Syntax:

```
show gti server
```

This command has no parameters.

Example:

```
show gti server
GTI Server configured to Private Cloud
Private Cloud address: example.com
```

show hardware

Displays variouse hardware information based on the command parameter.

Syntax: `show hardware <parameter> <keyword>`

This command is not available for Virtual Advanced Threat Defense.

Parameter	Description
<no parameter>	Displays the list of parameters for this command.
<keyword>	Replace with **save**. This optional keyword allows you to save the output to a file instead of displaying it. The file is saved in the `~atdadmin` directory where it can be access using SFTP by logging on as atdadmin. The filenames are shown in the following table.
diskinfo	Display the RAID, HDD, and SSD diagnostic information.
ldtlog	Displays the LDT summary log. Ensure that the run the ldt tool before you run this command. For more information, see *run ldt topic*.
rmm	Displays the RMM hardware and system firmware information.
sdr	Displays the repository entries and readings of the sensor data.

show history

Displays the list of CLI commands issued in the session.

Syntax: `show history`

This command has no parameters.

show internal net

Displays the list of all configured network.

Syntax:

`show internal net`

Example:

```
ATD-6000>show internal net
Name                                                Network                 Status
-------------------------------------
sandbox                                 192.168.122.0     Active
emailconnector 192.168.55.0         Active
```

show intfport

Shows the status of the specified interface port or the management port of McAfee Advanced Threat Defense.

Syntax: `show intfport <mgmt><1><2><3>`

Information displayed by the `show intfport` command includes:

- Whether the port's administrative status is enabled or disabled.
- The port's link status.
- The speed of the port.
- Whether the port is set to half or full duplex.
- Total packets received.
- Total packets sent.

- Total CRC errors received.
- Total other errors received.
- Total CRC errors sent.
- Total other errors sent.
- IP address of the port.
- MAC address of the port.
- Whether the port is used to provide Internet access to analyzer VMs.
- If configured to provide Internet access to analzyer VMs, then the corresponding gateway for this traffic.

show ipAddressSwap

Use this command to know if ipAddressSwap is enabled or disabled currently. By default, FTP is enabled.

Syntax: `show IPAddressSwap`

See also: set ipAddressSwap on page 21.

show ldap

Displays the configured parameters for LDAP authentication.

Syntax:

```
show ldap
```

This command has no parameters.

Example:

```
show ldap
+++++ LDAP Configuration +++++
LDAP username           : (null)
Base DN                 : (null)
LDAP Login Attribute    : (null)
LDAP Search scope       : subtree
LDAP Auth Method        : Simple
LDAP Server             : IP:[(null)] Port:[0]
LDAP Service status     : DOWN
LDAP Fallback status    : DISABLE
```

show license info

Displays the license information of the appliance.

Syntax:

```
show license info
```

This command has no parameters.

Example:

```
show license info
ATD License Manager, on non-license-restricted platform
Authorized to SystemId  : NA
Valid before date       : Infinity
```

show license status

Displays the license status of the appliance.

Syntax:

```
show license status
```

This command has no parameters.

Example:

```
show license status
ATD License Manager, on non-license-restricted platform
Valid License
```

show logconfig

Lists the current debug mode employed for debugging.

Syntax: `show logconfig`

This command has no parameters.

Sample Output: `Logging is ON, mode: send to syslog`

show mar-timeout

Displays a configured timeout period after which Advanced Threat Defense stops querying MAR server for results.

Syntax: `show mar-timeout`

This command has no parameters.

Default value: 60 Seconds.

Sample Output: `MAR Timeout is currently set to 90 seconds`

show pdflinks

view whether or not validation operation is performed by McAfee GTI on links embedded inside PDFs during dynamic analysis.

Syntax: `show pdflinks`

This command has no parameters.

Sample Output: `GTI validation of PDF URLs is OFF`

show msu

Displays all the msu files copied to Advanced Threat Defense via SFTP.

Syntax: `show msu`

show nsp scandetails

Shows the file scan details regarding the integrated IPS Sensors.

Syntax: `show nsp scandetails <Sensor IP address>`

If you do not specify the Sensor IP address, the details are displayed for all the Sensors integrated with the Advanced Threat Defense Appliance.

Information displayed by the `show nsp scandetails` command includes:

- The IP address of the IPS Sensor.
- Total number of packets received from the Sensor.
- Total number of packets sent to the Sensor.
- The timestamp of when the last packet was sent to and received from the Sensor.
- The encryption method used for the communication with the Sensor.
- Session handle null counts.
- Count of internal errors.
- Count of unknown commands received from the Sensor.
- File string null.
- File data null.
- Count of unknown files.
- Count of out of order packets.
- Count of MD5 mismatches between what was sent by the Sensor and what was calculated by Advanced Threat Defense.
- Count of memory allocation failures.
- File transfer timeout.
- New file count.
- Count of shared memory allocation failures.
- Count of the number of static analysis responses sent.
- Count of the number of dynamic analysis responses sent.
- Count of scan request received.
- MD5 of the last file that was streamed by the Sensor.

show nsp-ssl-channel-encryption status

Displays the SSL channel encryption status for Network Security Platform.

Syntax:

```
show nsp-ssl-channel-encryption status
```

Parameter	Description
status	Displays the SSL channel encryption status for Network Security Platform.

Example:

```
show nsp-ssl-channel-encryption status
NSP SSL Channel Encryption is Enabled.
```

show port80

Displays the status of HTTP port 80.

Syntax:

```
show port80
```

This command has no parameters.

Example:

```
show port80
HTTP port 80 is closed or blocked
```

show resultbackup

This command displays the resultbackup status.

Syntax:

```
show resultbackup
```

show route

Displays the routes that you configured using the `route add` command as well as the system IP routing table.

Syntax:

```
show route
```

The details from a sample output of the command in the following table.

Table 1 System IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
10.10.10.0	0.0.0.0	255.255.255.0	U	0	0	0	mgmt
11.11.11.0	0.0.0.0	255.255.255.0	U	0	0	0	mgmt
12.12.0.0	0.0.0.0	255.255.0.0	U	0	0	0	mgmt
13.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	mgmt
0.0.0.0	10.10.10.253	0.0.0.0	UG	0	0	0	mgmt

show stixreportstatus

Displays the current status of the stixreportstatus.

This command has no parameter.

Syntax: `show stixreportstatus`

Sample Output: `STIX reporting is OFF`

show system id

Displays the system ID.

Syntax:

```
show system id
```

This command has no parameters.

Example: `show system id`

```
71xxxxxxxx-xxxxxxx-xxxxx-xxxxxx-xxxxxxxxxxxx
```

show taxii status

View the TAXII status of the STIX file published by Advanced Threat Defense.

Syntax: show taxii status

This command has no parameters.

Example:

```
[ TAXII Status for STIX file publish ]
Configuration                          : enable
Channel Status                         : UNKNOWN
Stix Files Received Count              : 0
Stix Files Published Count             : 0
Stix Files Queued Count                : 0
```

show tepublisherstatus

Displays the status of McAfee ePO Threat Event Publisher.

Syntax:

`show tepublisherstatus`

This command has no parameters.

Example: `show tepublisherstatus`

```
********ePO Threat Event Publisher Status********

        tepublisher is not running
```

show timeout

Displays the CLI timeout.

Syntax: `show timeout`

This command has no parameters.

Example:

`show timeout`

```
CLI session timeout is 360000 seconds.
```

show ui-timeout

Displays the Advanced Threat Defense web interface client timeout in seconds.

Syntax: `show ui-timeout`

Sample output: `Current timeout value: 600`

show uilog

Check the current level of uilog.

This command has no parameters.

Syntax:

```
show uilog
```

Following is the information displayed by the `show uilog` command:

```
ATD-6000> show uilog
Current log level is 7
```

show version application

Displays the current and backup versions of the application software.

Syntax:

```
show version application
```

This command has no parameters.

Example:

```
ATD-3000-37> show version application
Current VERSION=3.8.0.21.58782
Current LastModifiedTime=2016-12-04 17:23:29

Backup  VERSION=3.8.0.19.58759
Backup  LastModifiedTime=2016-12-02 02:01:23
```

show version detection

Displays the current and backup versions of the detection software.

Syntax:

```
show version detection
```

This command has no parameters.

Example:

```
ATD-3000-37> show version detection
Current VERSION=3.8.0.161202.58782
Current LastModifiedTime=2016-12-04 17:23:40
```

show vmImage

This command displays the list of the VM Images in Advanced Threat Defense.

Synatx:

```
show vmImage
```

Example:

```
ATD-3000> show vmImage

android

winxpSp3
```

```
win7sp1

ATD-3000>
```

show waittime

Displays the wait time threshold set for Email Gateway.

Syntax: `show waittime`

Sample output: `Current MEG wait time threshold=780 seconds`

shutdown

Stops the Advanced Threat Defense Appliance so you can power it down.

Then, after about a minute, you can power down the Advanced Threat Defense Appliance manually and unplug both the power supplies. Advanced Threat Defense Appliance does not power off automatically. You must confirm that you want to shut it down.

This command has no parameters.

Syntax:

```
shutdown
```

status

Shows Advanced Threat Defense system status, such as the health and the number of files submitted to various engines.

This command has no parameters.

In the output, `Sample files received count: #` shows the count of number of samples submitted to Advanced Threat Defense for analysis. When archive samples are submitted, this count increases based on the number of files extracted.

Syntax: `status`

Sample output:

```
System Health Status : good

Sample files received count: 300

Sample files submitted count: 300

GTI Scanner files submitted count: 50

GAM Scanner files submitted count: 100

MAV Scanner files submitted count: 200

Sandbox files submitted count: 25

Sandbox files finished count: 25

Sample files finished count: 300

Sample files error count: 0
```

terminal

Sets the number of lines to display on the Advanced Threat Defense web interface.

Syntax:

```
terminal <length>¦no
```

Parameter	Description
<length>	Sets the number of lines to display. The value ranges from 0 - 512.
no	Negates the previous command or sets the default value.

tcpdump

Capture tcpdump on any physical interface of Advanced Threat Defense.

Syntax: `tcpdump <parameter>`

- Post tcpump capture, the binary pcap files can be downloaded from Advanced Threat Defence Web UI. Filename: `atd_netdata.zip`.
- The maximum pcap file size is limited to 10 MB. The maximum pcap file count is limited to 25 files.

  Maximum file size: Once the maximum size is reached tcpdump automatically begins recording to a new file.

  Maximum file count: Once the maximum count is reached tcpdump automatically overwrites the first and subsequent log file until the capture is stopped by the user.

Parameter	Description
start	Starts the packet capture operation on the specified tcp dump. You can set custom port option using the following syntax: `tcpdump start <interface> <port options sepearted by underscore>`  `<interface>` is a required parameter. Interface value should be eth0, eth1, eth2, or eth3. **Example**: `tcpdump start eth0_-v_ ip_host_8.8.8.8`
stop	Stops the packet capture operation.
clean	Removes tcpdump results and .zip files.
listfiles	Displays tcpdump output files.
ls	Displays tcpdump output files.
save	Saves .zip archive of tcpdump results to atdadmin account.
status	Displays tcpdump progress status.
view	Displays tcpdump results.

unlockuser <username>

Unlock a locked account.

Syntax

```
unlockuser <username>
```

Parameter	Description
<username>	Enter the username of the locked user account.

Example

```
 unlockuser admin
Unlock user: admin
User unlocked!
```

update_avdat

By default, Advanced Threat Defense updates the DAT files for the McAfee Gateway Anti-Malware Engine and McAfee Anti-Malware Engine every 90 minutes. To update these files immediately, use the `update_avdat` command.

This command has no parameters.

Syntax: `update_avdat`

uploadSupportBundle

This command allows you to upload the support bundle to a specific FTP site.

The bundle includes the following logs:

- Configuration
- Diagnostic
- Debug
- System
- VM
- Install
- UI
- Integration
- Email connector
- Hardware
- Network capture pcap files
- LDT

Follow these steps to upload the support bundle.

1 In the console type `uploadSupportBundle`.

2 Type the relevant values and press **Enter** for each prompt.

The command automatically creates the bundle, then uploads it to `<username>@<host IP>/<remote path>`.

vmlist

Displays a list of all the VMs configured in Advanced Threat Defense.

Syntax: `vmlist`

watchdog

The watchdog process reboots the Advanced Threat Defense Appliance when an unrecoverable failure is detected.

Syntax:

```
watchdog <on | off | status>
```

Parameter	Description
<on>	Enables the watchdog.
<off>	Disables the watchdog. Use it if the appliance reboots continuously due to repeated system failure.
<status>	Displays the status of the watchdog process.

web

Restart, start, stop, and check the web service.

Syntax:

```
web <parameters>
```

Parameter	Description
restart	Restart the web service.
start	Start the web service.
stop	Stop the web service.
check	Check the web service.

Example:

```
web restart
Service: restart
Web restarted
Web request done
```

whitelistMerge

Manually copy the Global Whitelist database of the Active node onto the Secondary or Backup nodes.

This is only a one-time activity, after which the Whitelist database of Secondary/Backup nodes is automatically overwritten by that of Active node at 0000 hours on a daily basis.

Syntax: whitelistMerge <cluster><standalone>

- `whitelistMerge <cluster>` executed on Active node of a cluster: In this scenario, the Global Whitelist database of the Active node is copied onto Secondary/Backup nodes and following sample output is displayed.

  Sample Output:

  ```
  Performing merge of whitelist dB from LB cluster nodes
  ```

- `whitelistMerge <cluster>` executed on Secondary node or Backup node of a cluster: In this scenario, the following sample output is displayed.

  Sample Output:

  ```
  Not an active LB cluster node

  Execute this command from active node in LB mode
  ```

- `whitelistMerge <standalone>` executed on a standalone Advanced Threat Defense: In this scenario, the following sample output is displayed.

  Sample Output:

  ```
  Performing Whitelist Merge for standalone
  ```