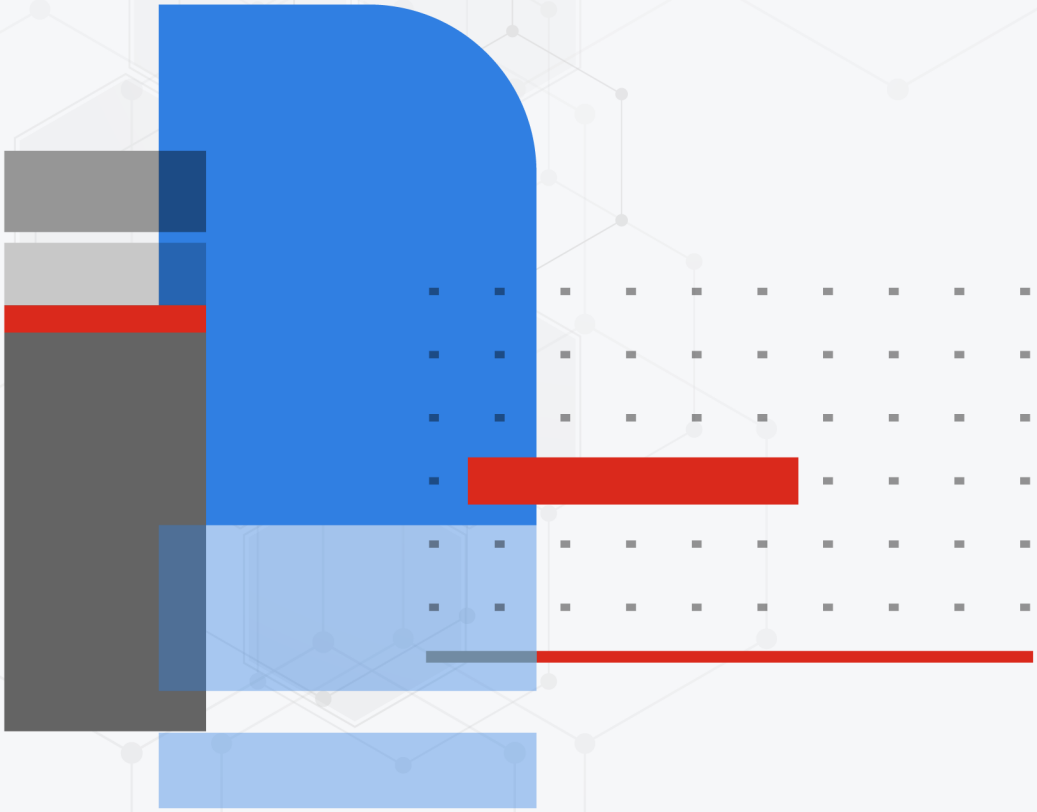
CLI Reference

FortiAnalyzer-BigData 7.4.5



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 04, 2026
FortiAnalyzer-BigData 7.4.5 CLI Reference
58-745-1225369-20260204

TABLE OF CONTENTS

Introduction

FortiAnalyzer-BigData improves upon base FortiAnalyzer appliances and offers analytics-powered security and event log management to process large volumes of data. Redesigned with a new distributed architecture and high-end hardware, the Security Event Manager of FortiAnalyzer-BigData is a horizontally scalable, high availability (HA) system that supports the needs of large enterprise organizations. The Security Event Manager of FortiAnalyzer-BigData comprises multiple server blades working together as a cluster, so you can add new blades to expand and scale the Security Event Manager as your organization grows.

FortiAnalyzer-BigData documentation

The following FortiAnalyzer-BigData product documentation is available:

- *FortiAnalyzer-BigData Getting Started Guides*
  These documents describe how to set up the FortiAnalyzer-BigData system according to your appliance.
- *FortiAnalyzer-BigData Administration Guide*
  This document describes how to use the FortiAnalyzer-BigData system with supported Fortinet units.
- *FortiAnalyzer-BigData CLI Reference*
  This document describes how to use the FortiAnalyzer-BigData Command Line Interface (CLI) to manage the cluster hosts.
- *FortiAnalyzer CLI Reference*
  This document describes how to use the FortiAnalyzer Command Line Interface (CLI) and contains references for FortiAnalyzer CLI commands.
- *FortiAnalyzer-BigData Release Notes*
  This document describes new features and enhancements in the FortiAnalyzer-BigData system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.

Using the Command Line Interface

This section explains how to connect to the CLI and describes the basics of using the CLI. You can use CLI commands to view all system information and to change all system configuration settings.

CLI command syntax

This guide uses the following conventions to describe command syntax.

- Angle brackets < > indicate variables.
- Vertical bar and curly brackets { | } separate alternative, mutually exclusive required keywords.
  For example:
  ```
  set protocol {ftp | sftp}
  ```
  You can enter `set protocol ftp` or `set protocol sftp`.
- Square brackets [ ] indicate that a variable is optional.
  For example:
  ```
  show system interface [<name_str>]
  ```
  To show the settings for all interfaces, you can enter `show system interface`. To show the settings for the Port1 interface, you can enter `show system interface port1`.
- A space separates options that can be entered in any combination and must be separated by spaces.
  For example:
  ```
  set allowaccess {https ping}
  ```
  You can enter any of the following:
  ```
  set allowaccess ping
  set allowaccess https ping
  set allowaccess http https ping snmp ssh telnet webservice
  ```
  In most cases to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.
- Special characters:
  - The \ is supported to escape spaces or as a line continuation character.
  - The single quotation mark ' and the double quotation mark " are supported, but must be used in pairs.
  - If there are spaces in a string, you must precede the spaces with the \ escape character or put the string in a pair of quotation marks.

Setting administrative access on an interface

To perform administrative functions through a FortiAnalyzer-BigData network interface, you must enable the required types of administrative access on the interface to which your management computer connects. Access to the CLI requires Secure Shell (SSH) access. If you want to use the GUI, you need HTTPS access.

To use the CLI to configure SSH access:

1. Connect and log into the CLI using the FortiAnalyzer-BigData console port and your terminal emulation software.
2. Use the following command to configure an interface to accept SSH connections:
   ```
   config system interface
      edit <interface_name>
         set allowaccess <access_types>
      end
   ```
   Where `<interface_name>` is the name of the FortiAnalyzer-BigData interface to be configured to allow administrative access, and `<access_types>` is a whitespace-separated list of access types to enable.
   For example, to configure port1 to accept HTTPS and SSH connections, enter:
   ```
   config system interface
      edit port1
         set allowaccess https ssh
      end
   ```

   Remember to press `Enter` at the end of each line in the command example. Also, type `end` and press `Enter` to commit the changes to the FortiAnalyzer-BigData configuration.

3. To confirm that you have configured SSH access correctly, enter the following command to view the access settings for the interface:
   ```
   get system interface <interface_name>
   ```
   The CLI displays the settings, including the management access settings, for the named interface.

Connect to the FortiAnalyzer-BigData CLI

Once you configure the FortiAnalyzer-BigData network, you can use the IP addresses to access the FortiAnalyzer-BigData Main CLI or the cluster controller and manage the system.

To connect to the FortiAnalyzer-BigData Main CLI:

1. Establish an SSH connection to the Main host IP you configured during initial setup.
2. Log in using the administrator credentials you created previously.
   If you did not create a new administrator credential during initial setup, use the default credentials of username `admin` with no password.

To connect to the cluster controller CLI:

1. Establish an SSH connection to the management IP you configured during initial setup.
2. Log in using the default username `root` and password `fortinet@123`.
3. Once you establish a connection, you can use the `fazbdctl` CLI commands to manage the cluster. For more information, see FortiAnalyzer-BigData cluster controller CLI on page 8.

Fortinet strongly recommends that you update the password with the `passwd` command.

FortiAnalyzer-BigData cluster controller CLI

This section describes how to use `fazbdctl`, the FortiAnalyzer-BigData Command Line Interface (CLI), and contains references for all `fazbdctl` commands.

`fazbdctl` is available on the cluster controller (see Connect to the FortiAnalyzer-BigData CLI on page 6) and is the main command used to manage the hosts of FortiAnalyzer-BigData.

Syntax

```
fazbdctl <command>
```

Commands

Command	Description
`enable`	Enable/disable cluster-wide features.
`help`	Help about any command.
`init`	Initialize the FAZ-BD cluster.
`reset`	Factory-reset or re-install the OS of a single node or the whole cluster.
`set`	Set system parameters.
`show`	Display system or cluster information.
`upgrade`	Upgrade system components.
`decommission`	Decommission a defect blade after it is powered off to get ready for new blade.
`disk-encryption`	Operations related to disk-encryption.

Option	Description
`-h, --help`	Help information.

Show version

```
fazbdctl show version
```

Shows the FortiAnalyzer-BigData version of the host.

Show members

```
fazbdctl show members
```

Lists all the cluster hosts' information managed by the cluster controller.

Option	Description
`{-o | --option} wide`	Display additional columns such as MAC address and version information in wide format.

Example response

In this example:

- `Management IP/Mask` is `10.106.2.168/24`

Field name	Chassis	Blade	Role	Address	Ext Address	Host Name
Value example	1	2	Controller	198.18.1.2	10.106.2.170	blade-198.18.1.2
	1	32	Member	198.18.1.32	10.106.2.174	blade-198.18.1.32

Field name	State	Status	Tips
Value example	Joined	Alive	
	Upgrading	Alive	Need upgrade

Field descriptions

Field name	Description
Management IP/Mask	This is the management IP address that is configured.
Chassis	By default, the Chassis ID is 1. If you want to designate an appliance as an extender appliance, change the Chassis ID to a range between 2-254.
Blade	Represents which the slot the blade is located in. The order of the blade slots starts from the left side of the FortiAnalyzer-BigData appliance, starting from 1 to 14.
Role	Role is either controller or member.
Address	The internal IP address is immutable and is generated from the blade's Chassis ID and Blade ID. 198.18.{chass ID}.{blade ID}
Ext Address	The external IP address is set by users through `fazbdctl set` command.

Field name	Description
Host Name	The host name.
State	The current status of the host. • **joined**: The host has joined the cluster. • **upgrading**: The host has joined this cluster and is running the upgrade process.
Status	The current status of the host. • **alive**: The host is up and running. • **failed**: The host fails to run.
Tips	Tips and notes about the host. • **Need upgrade**: The host's version does not match the controller's version.

Example response in wide format

In this example:

- `Management IP/Mask` is `10.106.2.168/24`
- `Gateway` is `10.106.2.254`

Field name	Chassis	Blade	Role	Address	Ext Address	Ext Gateway	Host Name
Value example	1	2	Controller	198.18.1.2	10.106.2.170	10.106.2.254	blade-10-0-1-2
	1	32	Member	198.18.1.32	10.106.2.174	10.106.2.254	blade-10-0-1-32

Field name	MAC	Version	State	Status	Tips
Value example	00:50:56:b2:7d:77	FortiAnalyzer-BigData-VM64 1.2.0	Joined	Alive	
	00:50:56:b2:e2:7b	FortiAnalyzer-BigData-VM64 1.1.0	Upgrading	Alive	Need upgrade

Additional field descriptions for wide format

Field name	Description
Gateway	This is the gateway for the management IP address that is configured.
Ext Gateway	The gateway for the external IP address.
MAC	The MAC address of the internal interface.
Version	The FortiAnalyzer-BigData version number running on the host.

Upgrade

```
fazbdctl upgrade {bootloader | fazbd | cluster} [-U <URL>][-o <option>][-p <password>][-u
      <username>][-n][-s]
```

Use this command to upgrade bootloader with argument "bootloader" and upgrade FortiAnalyzer-BigData OS with argument "fazbd" or "cluster" for the whole cluster. For more information, see the FortiAnalyzer-BigData Administration Guide in the Fortinet Doc Library.

- This command should be executed only on the cluster controller. It has no effect if run on other hosts.
- This command is only allowed when all the FortiAnalyzer-BigData services are healthy, but you can use `-f` to force the upgrade to run.

Extra options	Description
`{-U | --image-url} <URL>`	URL with protocol for the image to be downloaded and installed. Supported protocols are FTP, SFTP, HTTP and HTTPS. Example: `http://10.160.74.123/FAZBD.out`
`{-o | --option} <Option>`	Re-run options when failed: `skip | retry | restart`.
`{-p | --password} [<password>]`	Password for the download server if there is one.
`{-u | --username} [<username>]`	Username for the download server if there is one.
`{-n | --no-swap}`	Disable RAM swap creation during the upgrade process.
`{-s | --skip-pre-upgrade}`	Skip the pre-upgrade.

Examples

Command	Description
`fazbdctl upgrade cluster`	Interactively upgrade FortiAnalyzer-BigData.
`fazbdctl upgrade cluster -o retry`	If last upgrade fails, retry from the state where the upgrade fails.

Reset

```
fazbdctl reset [<worker-ip> | cluster] [-A | -I] [-o <option>][-n]
```

Reset the entire OS and optionally format all the disks for a single host or the whole cluster. When there is no argument specified, the reset applies to local host.

These are the available options in this command:

Extra options	Description
{-A | --all-settings}	Resets all settings.
{-I | --all-except-ip}	Keeps the public IP constant.
{-o | --option} <Option>	Re-run options when failed in soft reset: skip, retry, restart
{-x | --exclude-faz}	Excludes the Main host when resetting the cluster.
{-n | --retain-internal-subnet}	Keeps current subnet after hard-resetting cluster.

If no option is set, a soft reset will be performed. Otherwise, a hard reset will be performed to additionally format all the disks.

Examples

Command	Description
fazbdctl reset	Re-install the OS of this node (local).
fazbdctl reset 198.18.1.32	Re-install the OS of node 198.18.1.32, from a controller.
fazbdctl reset 198.18.1.32 -A	Factory-reset and clears all settings and data from the specified node, from a controller.
fazbdctl reset cluster	Re-install the OS of the whole cluster, from the controller.
fazbdctl reset cluster -I	Factory-reset the whole cluster from the controller, keeping external management IP address.
fazbdctl reset cluster -A	Factory-reset the whole cluster from the controller, clearing all settings and data.
fazbdctl reset cluster -A -n	Factory-reset the whole cluster from the controller, clearing all settings and data but retaining the original subnet after reset.

For instructions on how to reset your device, see the FortiAnalyzer-BigData Administration Guide in the Fortinet Doc Library.

Init

```
fazbdctl init cluster [-o <option>][-n][-F][-l]
```

Initialize the FortiAnalyzer-BigData cluster. This command initializes and configures the FortiAnalyzer-BigData cluster hosts. The process takes approximately 30 to 40 minutes. For more information, see the FortiAnalyzer-BigData Administration Guide in the Fortinet Doc Library.

- This command should be executed only on the cluster controller. It has no effect if run on other hosts.

Extra options	Description
{-o | --option} <Option>	Re-run options when failed: skip | retry |restart
{-n | --no-swap}	Disable RAM swap creation during the initialization process.
{-F | --force}	Force to run, even if the cluster is already initialized.
{-l | --encrypt-data-disks}	Enable data-at-rest encryption on the data disks.

If you run this command on an existing cluster, it will reinitialize and cause you to lose all log data and configurations.

Decommission

```
fazbdctl decommission <member IP/host name>[-Y]
```

After a defective blade is powered off, run this command to make the cluster ready for a replacement blade.

Extra options	Description
{-Y | --auto-confirm}	Skip interactive prompt and confirmation.

Disk Encryption

```
fazbdctl disk-encryption {init | change-phrase | status | open} [-f]
```

For instructions to enable data-at-reset encryption and related operations, see the FortiAnalyzer-BigData Administration Guide in the Fortinet Doc Library.

Command	Description
init	Initialize disk encryption on target host(s) when they are newly added or added as replacement. Pass a list of space-separated hosts with quotes if needed. For example, `fazbdctl disk-encryption init "blade-198-18-1-3 blade-198-18-1-5"`
change-passphrase	Change the data disk encryption passphrase for all cluster hosts.

Command	Description
`status <IP(s)/Host(s)>`	Get the status of data disk encryption for the cluster or target host(s).
`open all|members|<IP (s)/Host(s)`	Open the encrypted disk on all, members, or target host(s) will operate on local host if no argument is passed.

Extra options	Description
`[-f]`	Filter the status output by the attribute name.

Set management and external addresses

```
fazbdctl {set | unset} addr {<external ip/mask>} [<gateway>] [--management | --external | --mainhost
      | --mainhost-outbound] [-H] [-A] [-Y] [-v]
```

Set management IP address on the cluster controller and external IP addresses (used for Hyperscale logging) on cluster hosts to allow them to communicate with the outside world.

`external ip/mask` is an IP CIDR address to be set.

Optional flags	Description
`[management]`	Indicates the data carried in the `external ip/mask` and `gateway` fields is used to set the main management IP address. This flag is not compatible with `-H` and `-A` and is only available on the cluster controller.
`[external]`	Indicates the data carried in the `external ip/mask` and `gateway` fields is used to set the external IP address for cluster host(s).
`[mainhost]`	Indicates the data carried in the `ip address/mask` and `gateway` fields is used to set the Main host IP address and gateway. This flag is not compatible with `-H` and `-A` and is only available on the cluster controller. This flag is only available in the 4500G appliance.
`[mainhost-outbound]`	indicates the data carried in the `ip address/mask` and `gateway` fields is used to set the Main host secondary IP address and gateway for outbound traffic. This flag is not compatible with `-H` and `-A` and is only available on the cluster controller. This flag is only available in the 4500G appliance.
`[-H]`	Specifies the internal IP address of a host where the external IP will be assigned. Without this flag, the external IP address is assigned to the local host.

Optional flags	Description
[-A]	Sets external IP addresses on all hosts from the controller. In this case, the external ip/mask field specifies the starting external IP address to be assigned to the first host. The remaining hosts are assigned external IP addresses incrementally from the starting external IP address within the network subnet, wrapping around when reaching the boundary of the network subnet.
[-Y]	Lets you skip interactive confirmation when the command is issued.
[-v]	Indicates the `external ip/mask` will be set through dedicated network interface, separated from regular network interface. In most cases, the dedicated network interface resides in a different network subnet from the regular network interface. Not compatible with `management` flag. This flag is only available in the 4500G appliance.

Examples

`fazbdctl set addr 10.160.74.174/24 10.160.74.1 --external`	Set external IP CIDR address and gateway on local host.
`fazbdctl set addr -H 198.18.1.3 10.160.74.174/24 10.160.74.1 --external`	Set external IP CIDR address and gateway for host 198.18.1.3 from controller.
`fazbdctl set addr 10.160.74.174/24 --external`	Set external IP CIDR address on local host.
`fazbdctl set addr 10.160.74.174/24 10.160.74.1 --management`	Set management IP CIDR address with gateway on controller host.
`fazbdctl unset addr -H 198.18.1.3 --external`	Unset external IP CIDR address on host 198.18.1.3.
`fazbdctl set addr -H 198.18.1.3 10.106.49.63/24 10.106.49.254 --external -v`	Set external IP CIDR address and gateway for host 198.18.1.3 through dedicated network interface from controller. This example applies to the 4500G appliance.
`fazbdctl set addr 10.160.74.175/24 10.160.74.1 --mainhost`	Set primary IP CIDR address with gateway on Main host. This example applies to the 4500G appliance.
`fazbdctl set addr 10.106.49.61/24 10.106.49.254 --mainhost-outbound -v`	Set secondary IP CIDR address with gateway for outbound traffic through dedicated network interface on Main host. This example applies to the 4500G appliance.
`fazbdctl unset addr --management`	Unset the management IP CIDR address.
`fazbdctl set addr 10.160.74.174/24 10.160.74.1 --external -A`	Set external IP CIDR address on all members, starting from 10.160.74.174.
`fazbdctl unset addr --external -A`	Unset external IP CIDR address on all members.

Set appliance role

```
fazbdctl set appliance {extender-chassis-id}
```

Designate an appliance as an extender appliance so you can add it as an extender to the main appliance. For instructions on assigning a new chassis ID to the extender appliance, see the FortiAnalyzer-BigData Administration Guide in the Fortinet Doc Library.

- This command should be executed only on the cluster controller. It has no effect if run on other hosts.

Set Security Event Manager hosts OS password

```
fazbdctl set password
```

By default, the OS password for the Security Event Manager hosts is `fortinet@123`. Use this command to set a new password for them. This password is used to SSH to Security Event Manager hosts and enters the secure shell by using `fazbdctl execute shell` in a remote CLI console.

Enable Secure Shell

```
fazbdctl execute shell
```

Enter the secure shell by using in a remote CLI console session from the Cluster Manager web GUI. The Security Event Manager host OS password will be prompted.

Enable/Disable IP-Forward

```
fazbdctl [ enable | disable ] ip-forward
```

By default, all the cluster hosts except the cluster controller have no external network access. In some cases, you might want to allow external network access for all hosts, for example, to backup and restore data to external HDFS, to support Hyperscale log ingestion, etc.. This command allows you to forward packets from your internal network by enabling or disabling the NAT setup on the cluster controller.

- This command should be executed only on the cluster controller. It has no effect if run on other hosts.

Unstack chassis

```
fazbdctl unstack-chassis
```

Use this command in the cluster controller to unstack the chassis so that they can be separated safely. For more information see *How to remove a chassis from a stacked setup* in the *FortiAnalyzer-BigData Administration Guide*.

FortiAnalyzer-BigData log export CLI

This section describes how to use `fazbd-log-export`, the FortiAnalyzer-BigData log export Command Line Interface (CLI) tool, and contains references for all `fazbd-log-export` commands.

`fazbd-log-export` is available on the cluster controller (see Connect to the FortiAnalyzer-BigData CLI on page 6) and is the command used to export logs from the FortiAnalyzer-BigData log database. It allows you to perform various operations related to log export sessions.

Syntax

```
fazbd-log-export <command>
```

Commands

Command	Description
`init`	Initialize a log export session with specified parameters such as ADOM, log type, device type, device IDs, start and end dates, and log file format (CSV or Parquet).
`start <session_id>`	Start or resume a log export session with the given session ID.
`pause <session_id>`	Pause a log export session with the given session ID.
`force-stop`	Force stop the running session and release the lock.
`status <session_id>`	List all log export sessions or retrieves the status of a specific session.
`push <session_id>`	Transfer the exported log files to an external target server using SCP or FTP. Requires a session ID.
`close <session_id>`	Close a log export session with the given session ID and clear all the resources.

Initialize a log export session

```
fazbd-log-export init
```

Initialize the log export session with parameters. This command estimates the size and prepares the metadata for the export, and returns a session ID.

Extra options	Description
`{-Y | --auto-complete}`	Auto-completes the confirmations.
`{-f | --config}`	The path of the config file which contains the request in json format.

Examples

Interactive mode:

```
fazbd-log-export init
```

Pass the config inline:

```
fazbd-log-export init '{
   "adom": "root",
   "start_date": "2023-08-10",
   "end_date": "2023-08-13",
   "device_ids": ["FG100FTK20016262"],
   "format": "parquet"
}'
```

Pass the config file path:

```
fazbd-log-export init -f /path/to/config/init.json
cat /path/to/config/init.json
{
   "adom": "root",
   "start_date": "2023-08-10",
   "end_date": "2023-08-13",
   "device_ids": ["FG100FTK20016262"],
   "format": "csv"
}
```

Supported parameters:

Parameter	Description	Example
"adom"	The ADOM name.	"root"
"log_type"	The log type.	"traffic", "event", etc.
"device_type"	The device type.	"fgt", "fmg", etc.
"device_ids"	The device IDs.	["FG100FTK20016262"]
"start_date"	The start date of the log export session.	"2023-08-10"
"end_date"	The end date of the log export session.	"2023-08-13"
"filter"	The filter string.	"vd='root'"
"format"	The format of the log files. Supports "csv" or "parquet".	"csv"

Start a log export session

```
fazbd-log-export start <session_id>
```

Start or resume a log export session with the given session ID. This command starts the background (by default) tasks to extract, load, and transfer the logs of an initialized log export session to a desired format (CSV or Parquet) and stores them in a staging workspace located in the HDFS of the cluster.

Extra options	Description
{-Y | --auto-complete}	Auto-completes the confirmations.
{-F | --foreground}	Run the upgrade process at the foreground.

Pause a log export session

```
fazbd-log-export pause <session_id>
```

Pauses a log export session with the given session ID. This command pauses the background (by default) log export tasks. The task may not be paused immediately but will be paused on the next slice of the sub-tasks. The paused task can be resumed with the `fazbd-log-export start` command.

Extra options	Description
{-Y | --auto-complete}	Auto-completes the confirmations.

Force-stop a log export session

```
fazbd-log-export force-stop <session_id>
```

Force-stop a log export session with the given session ID. This command immediately force kills the running log export session tasks and releases the lock. In some situations, the log export session may be ungracefully killed by accident, but the lock may still be on hold. This command can be used to force unlock the session.

Extra options	Description
{-Y | --auto-complete}	Auto-completes the confirmations.

List log export sessions

```
fazbd-log-export status
```

List all open log export sessions.

Get log export session details

```
fazbd-log-export status <session_id>
```

Print the status and details of a log export session.

Extra options	Description
{-o | --option}	Display format option: "wide" or "narrow" for formatted display, or "json" for json format display (default = "wide").

Push a log export session

```
fazbd-log-export push <session_id>
```

Push the logs in a completed log export session to a remote server.

Extra options	Description
{-Y | --auto-complete}	Auto-completes the confirmations.
{-f | --config}	The path of the config file which contains the request in json format.

Examples:

Interactive mode:

```
fazbd-log-export push
```

Pass the config inline:

```
fazbd-log-export push [session_id] '{
   "protocol": "scp",
   "host_port": "10.160.74.123",
   "user": "fazbd",
   "password": "fortinet"
   "directory": "/home/fortinet",
}'
```

Pass the config file path:

```
fazbd-log-export push [session_id] -f /path/to/config/push.json
cat /path/to/config/push.json
{
   "protocol": "scp",
   "host_port": "10.160.74.123",
   "user": "fazbd",
   "password": "fortinet"
   "directory": "/home/fortinet",
}
```

Supported fields:

Parameter	Description	Example
"protocol"	The protocol to use to transfer the log files.	"scp", "ftp", "sftp"

Parameter	Description	Example
"directory"	The directory path to store the log files on the target server.	
"ip"	The IP address of the target server.	
"user"	The username to login to the target server.	
"password"	The password to login to the target server.	
"ssh_cert_path"	The path to the SSH certificate file (only available for SCP).	

Close a log export session

```
fazbd-log-export close <session_id>
```

Close the log export session and releases all the resources.

Extra options	Description
{-Y | --auto-complete}	Auto-completes the confirmations.

FortiAnalyzer-BigData Main CLI

The FortiAnalyzer-BigData Main CLI consists of the following command branches:

config system	**config fmupdate**	**get**
show	**diagnose**	**execute**

system

Use `system` to configure options related to the overall operation of the FortiAnalyzer-BigData unit.

The following commands are unique to FortiAnalyzer-BigData.
For all other `system` commands, see the FortiAnalyzer CLI Reference.

global

```
config system global
   set bd-management-gateway <string>
   set bd-management-ip <string>
end
```

Variable	Description
bd-management-gateway <string>	Set the Gateway for the FortiAnalyzer-BigData management GUI.
bd-management-ip <string>	Set the IP of the FortiAnalyzer-BigData management GUI.

fmupdate

Use `fmupdate` to configure settings related to FortiGuard service updates and the FortiAnalyzer-BigData's built-in FortiGuard Distribution Server (FDS).

For information on `fmupdate` commands, see the FortiAnalyzer CLI Reference.

execute

The `execute` commands perform immediate operations on the FortiAnalyzer-BigData unit. You can:

- Back up and restore the system settings, or reset the unit to factory settings.
- Set the unit date and time.
- Use ping to diagnose network problems.
- View the processes running on the FortiAnalyzer-BigData unit.
- Start and stop the FortiAnalyzer-BigData unit.
- Reset or shut down the FortiAnalyzer-BigData unit.

For information on `execute` commands, see the FortiAnalyzer CLI Reference.

diagnose

The `diagnose` commands display diagnostic information that help you to troubleshoot problems.

For information on `diagnose` commands, see the FortiAnalyzer CLI Reference.

get

The `get` commands display a part of your FortiAnalyzer-BigData unit's configuration in the form of a list of settings and their values.

The `get` command displays all settings, including settings that are in their default state.

Unlike the `show` command, `get` requires that the object or table whose settings you want to display are specified, unless the command is being used from within an object or table.

For example, at the root prompt, this command would be valid:

```
get system status
```

and this command would not:

```
get
```

For information on `get` commands, see the FortiAnalyzer CLI Reference.

show

The `show` commands display a part of your unit's configuration in the form of the commands that are required to achieve that configuration from the firmware's default state.

Unlike the `get` command, `show` does not display settings that are in their default state.

For information on `show` commands, see the FortiAnalyzer CLI Reference.

Change Log

Date	Change Description
2026-02-04	Initial release.

www.fortinet.com