



FortiAnalyzer-BigData - CLI Reference

Version 6.4.5

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



June 03, 2021

FortiAnalyzer-BigData 6.4.5 CLI Reference

58-645-698016-20210603

TABLE OF CONTENTS

Introduction	4
FortiAnalyzer-BigData documentation	4
Using the Command Line Interface	5
CLI command syntax	5
Setting administrative access on an interface	5
Connect to the FortiAnalyzer-BigData CLI	6
FortiAnalyzer-BigData cluster controller CLI	7
Show version	7
Show members	8
Upgrade	10
Reset	10
Init	11
Set management and external addresses	11
Set appliance role	12
Enable/Disable IP-Forward	12
Delete host	12
FortiAnalyzer-BigData Main CLI	13
system	13
fmupdate	13
execute	14
diagnose	14
get	14
show	15
Change Log	16

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 Administration Guide*
This document describes how to set up the FortiAnalyzer-BigData system and use it with supported Fortinet units.
- *FortiAnalyzer-BigData CLI Reference*
This document describes how to use the FortiAnalyzer-BigData Command Line Interface (CLI) to manage the Security Event Manager 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 BigData Cluster controller and manage the system.

To connect to the FortiAnalyzer-BigData Main CLI:

1. Establish an SSH connection to the Cluster Management 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 BigData Cluster controller:

1. Establish an SSH connection to the Cluster 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 7](#).



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 BigData Cluster controller (see [Connect to the FortiAnalyzer-BigData CLI on page 6](#)) and is the main command used to manage the Security Event Manager hosts of FortiAnalyzer-BigData.

Syntax

```
fazbdctl [command]
```

Commands

Command	Description
<code>delete</code>	Remove a worker node from the cluster.
<code>enable</code>	Enable/disable cluster-wide features.
<code>help</code>	Help about any command.
<code>init</code>	Initialize k8s cluster.
<code>reset</code>	Factory-reset or re-install the OS of a single node or the whole cluster.
<code>set</code>	Set system parameters.
<code>show</code>	Display system or cluster information.
<code>upgrade</code>	Upgrade system components.

Option	Description
<code>-h, --help</code>	Help information.

Show version

```
fazbdctl show version
```

Shows the FortiAnalyzer-BigData version of the host.

Show members

```
fazbdctl show members
```

Lists all the Security Event Manager member hosts' information managed by the BigData Cluster controller.

Option	Description
-o 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	10.0.1.2	10.106.2.168	blade-10-0-1-2
	1	32	Member	10.0.1.32	10.106.2.174	blade-10-0-1-32

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

Field descriptions

Field name	Description
Management IP/Mask	This is the main 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 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 blade's Chassis ID and Blade ID. 10.0.{chass ID}.{blade ID}
Ext Address	The external IP address is set by users through <code>fazbdctl set</code> command.
Host Name	The host name.
MAC	The MAC address of the internal interface.
Version	The FortiAnalyzer-BigData version number running on the host.

Field name	Description
State	The current status of the host. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> alive: The host is up and running. failed: The host fails to run.
Tips	Tips and notes about the host. <ul style="list-style-type: none"> 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	10.0.1.2	10.106.2.168	10.106.2.254	blade-10-0-1-2
	1	32	Member	10.0.1.32	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 main management gateway that is configured.
Ext Gateway	The gateway for each external IP address.
MAC	The MAC address of the internal interface.
Version	The FortiAnalyzer-BigData version number running on the host.

Upgrade

```
fazbdctl upgrade fazbd
```

Use this command to upgrade the system or components. For more information, see the FortiAnalyzer-BigData Administration Guide in the [Fortinet Doc Library](#).

- This command should be executed only on the BigData 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.

For more details and example command usage, use `fazbdctl upgrade -h`

<code>fazbdctl upgrade fazbd</code>	Upgrade both FortiAnalyzer (FAZ) OS and FortiAnalyzer-BigData OS interactively.
<code>fazbdctl upgrade fazbd -U ftp://1.2.3.4/path/fazbd.zip -u <user> -p <password></code>	Upgrade both FortiAnalyzer (FAZ) OS and FortiAnalyzer-BigData OS.

Reset

```
fazbdctl reset [{worker-ip} | cluster | members] [-A | -I | -S | -B]
```

Reset the entire OS of the blades and optionally format all the disks. There are four available options in this command:

Extra options	Description
<code>-A, all-settings</code>	Resets all settings.
<code>-I, all-except-ip</code>	Keeps the public IP constant.
<code>-S, all-except-ssh</code>	Keeps the ssh public key constant.
<code>-B, all-except-ip-ssh</code>	Keeps the ssh public key and public IP constant.

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
<code>fazbdctl reset</code>	Re-install the BigData (BD) OS of this node (local).
<code>fazbdctl reset 10.0.1.32</code>	Re-install the BigData (BD) OS of node 10.0.1.32, from a controller.
<code>fazbdctl reset 10.0.1.32 -A</code>	Factory-reset and clears all settings and data from the specified node, from a controller.
<code>fazbdctl reset cluster</code>	Re-install the BigData (BD) OS of the whole cluster, from the controller.

Command	Description
<code>fazbdctl reset cluster -I</code>	Factory-reset the whole cluster from the controller, keeping external management IP address.
<code>fazbdctl reset cluster -A</code>	Factory-reset the whole cluster from the controller, clearing all settings and data.
<code>fazbdctl reset members -A</code>	Factory-reset all members except the controller, clearing all settings and data.

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

Init

```
fazbdctl init cluster
```

Initialize the Security Event Manager after a hard reset. This command initializes and configures the Security Event Manager. 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 BigData Cluster controller. It has no effect if run on other hosts.



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

Set management and external addresses

```
fazbdctl [ set | unset ] addr {external ip/mask} {gateway} --management -H {internal ip} -A -Y
```

Set management IP address on Security Event Manager controller and external IP addresses on Security Event Manager hosts to allow them to communicate with the outside world.

`external ip/mask` can be IP CIDR address or simply `dhcp`.

- The optional `management` flag 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 Security Event Manager controller.
- The optional `-H` flag specifies the internal IP address of a Security Event Manager host where the external IP will be assigned. Without this flag, the external IP address is assigned to the local host.
- The optional `-A` flag sets external IP addresses on all Security Event Manager hosts from the Security Event Manager controller. In this case, the `external ip/mask` field specifies the starting external IP address to be assigned to the first Security Event Manager host. The remaining Security Event Manager 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. This flag is not compatible if `external ip/mask` is `dhcp`.
- The optional `-Y` flag lets you skip interactive confirmation when the command is issued.

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 BigData Cluster controller. It has no effect if run on other hosts.

Enable/Disable IP-Forward

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

By default, all the BigData Cluster hosts except the BigData 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. This command allows you to forward packets from your internal network by enabling or disabling the NAT setup on the BigData Cluster controller.

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

Delete host

```
fazbdctl delete {member_ip_addr}
```

Decommission a host in the BigData Cluster members. For more information, see the FortiAnalyzer-BigData Administration Guide in the [Fortinet Doc Library](#).

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

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

fmupdate

Use `fmupdate` to configure settings related to FortiGuard service updates and the FortiAnalyzer-BigData unit'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
2021-06-03	Initial release.



FORTINET[®]



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.