4500G Getting Started Guide

FortiAnalyzer-BigData 7.6.0

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

FORTINET®

May 30, 2025
FortiAnalyzer-BigData 7.6.0 4500G Getting Started Guide
58-760-1155477-20250530

TABLE OF CONTENTS

Introduction

The set up process in this guide consists of setting up the FortiAnalyzer-BigData unit and the Chassis Management Module (CMM).

To set up the FortiAnalyzer-BigData unit, you must perform the following steps:

1. Initial set up on page 5
2. Set up the FortiAnalyzer-BigData network on page 9
3. Set up Administrator accounts on page 12

Once the unit and network is set up and connected, you can connect to the Main CLI or Security Event Manager Controller. See Connect to the FortiAnalyzer-BigData CLI on page 28.

In addition to setting up FortiAnalyzer-BigData, you also need to set up the CMM. The CMM is used to remotely manage and monitor server hosts, power supplies, cooling fans, and networking switches for the FortiAnalyzer-BigData unit. The CMM comes with a web management utility that consolidates and simplifies system management for the FortiAnalyzer-BigData chassis.

Prerequisites

You must have the following before beginning to set up your FortiAnalyzer-BigData:

- Ethernet cable
- SPF RJ45 transceiver module
- Management computer

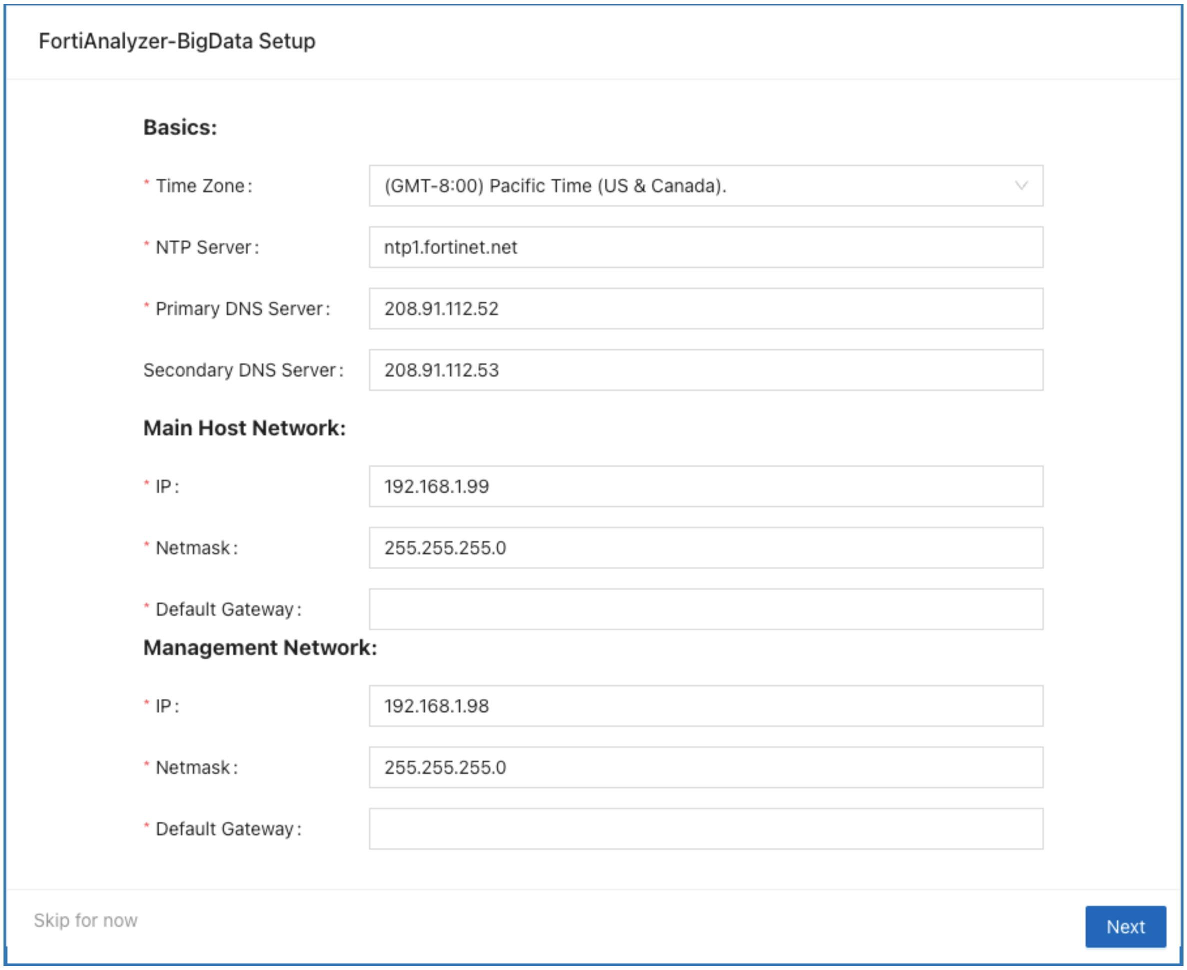
Initial set up

To connect to the FortiAnalyzer-BigData GUI:

1. Install the SFP RJ45 transceiver module into one of the SFP interfaces on the FortiAnalyzer-BigData Switch Module #2.
2. Connect the RJ45 port on the transceiver module to the management computer using the supplied Ethernet cable.
3. Enable DHCP or set the management computer's IP address to be on the same subnet as FortiAnalyzer-BigData.
   For example:
   - **IP address:** 192.168.1.10
   - **Netmask:** 255.255.255.0
4. On the management computer, open a supported web browser and visit https://192.168.1.98.
5. Log in with the username `admin` and no password.
   The FortiAnalyzer-BigData GUI loads.

To set up the system via the FortiAnalyzer-BigData Setup wizard:

1. Configure basic and network settings.
   - Modify the time zone, or use the default value.
   - Modify the NTP server, or use default value.
   - Modify the primary and secondary DNS server, or use default value.
   - Modify or add the IP, netmask, and default gateway for main host network.
   - Modify or add the IP, netmask, and default gateway for management network.



FortiAnalyzer-BigData Setup

Basics:

* Time Zone:	(GMT-8:00) Pacific Time (US & Canada).
* NTP Server:	ntp1.fortinet.net
* Primary DNS Server:	208.91.112.52
Secondary DNS Server:	208.91.112.53

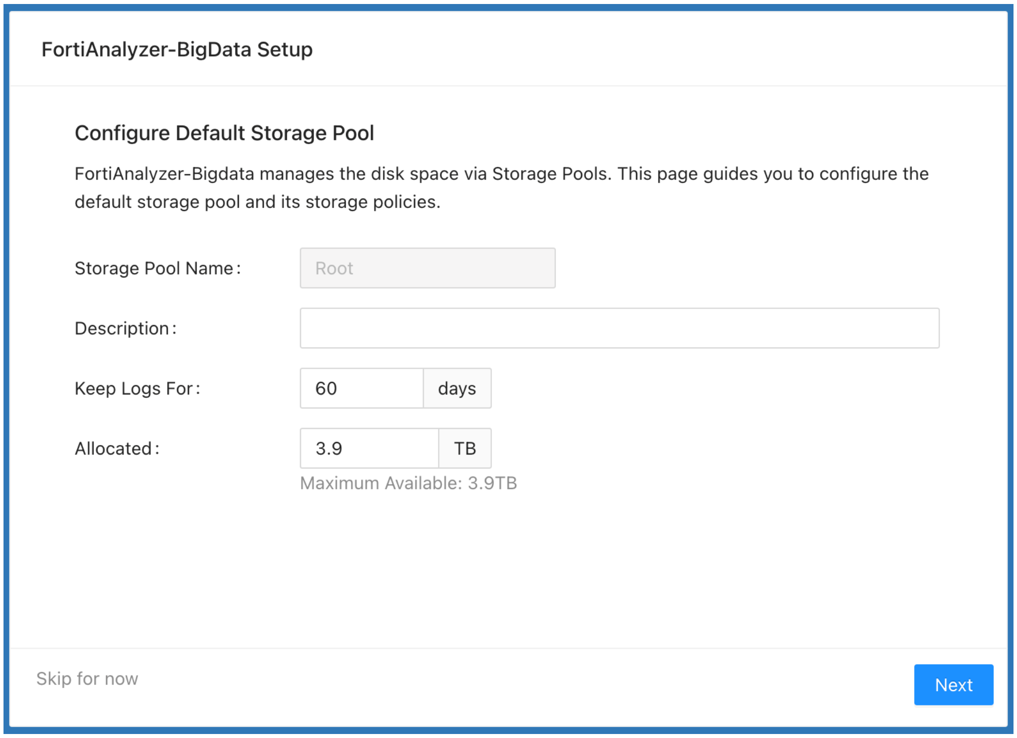
Main Host Network:

* IP:	192.168.1.99
* Netmask:	255.255.255.0
* Default Gateway:	

Management Network:

* IP:	192.168.1.98
* Netmask:	255.255.255.0
* Default Gateway:	

2. Configure the default (Root) Storage Pool.
   - Modify the *Keep Logs For days*, or use the default value.
   - Modify the *Allocated* space, or use the default value to use the entire disk space.
   - You are able to create more Storage Pools later, if needed. You can create up to 5 Storage Pools.



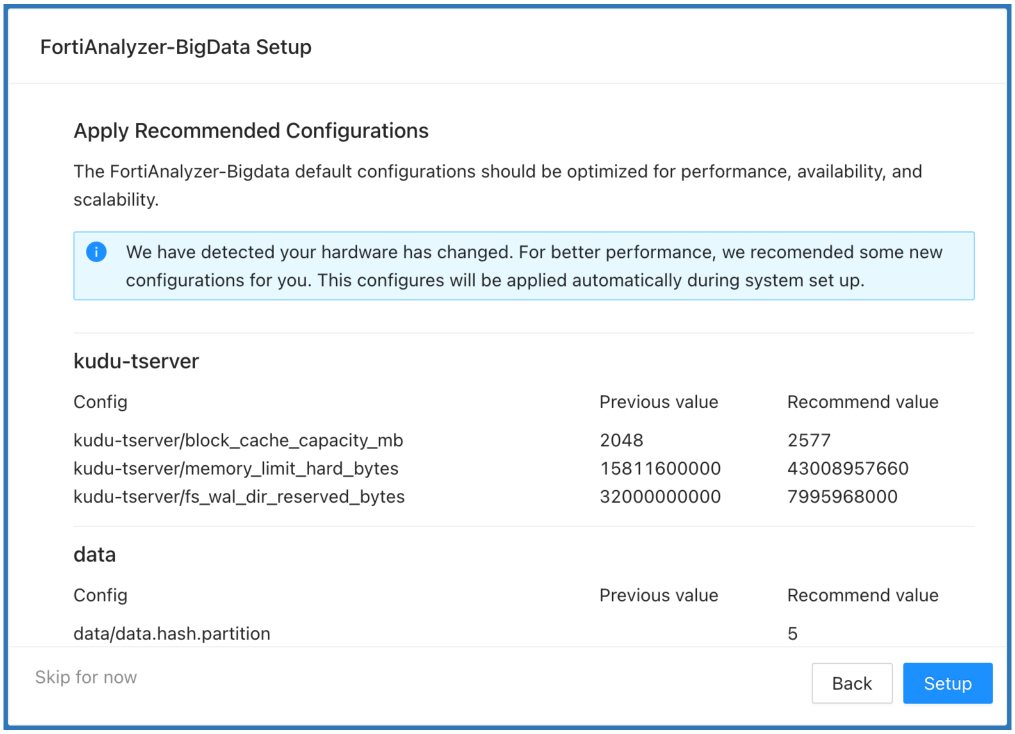
FortiAnalyzer-BigData Setup

Configure Default Storage Pool

FortiAnalyzer-Bigdata manages the disk space via Storage Pools. This page guides you to configure the default storage pool and its storage policies.

Storage Pool Name :	Root
Description :	
Keep Logs For :	60 days
Allocated :	3.9 TB Maximum Available: 3.9TB

3. Click *Next*.
4. Apply the recommended configurations.
   - In this step, the system automatically adjusts the optimized configurations to adapt to the underlying hardware spec.



FortiAnalyzer-BigData Setup

Apply Recommended Configurations

The FortiAnalyzer-Bigdata default configurations should be optimized for performance, availability, and scalability.

We have detected your hardware has changed. For better performance, we recomended some new configurations for you. This configures will be applied automatically during system set up.

kudu-tserver

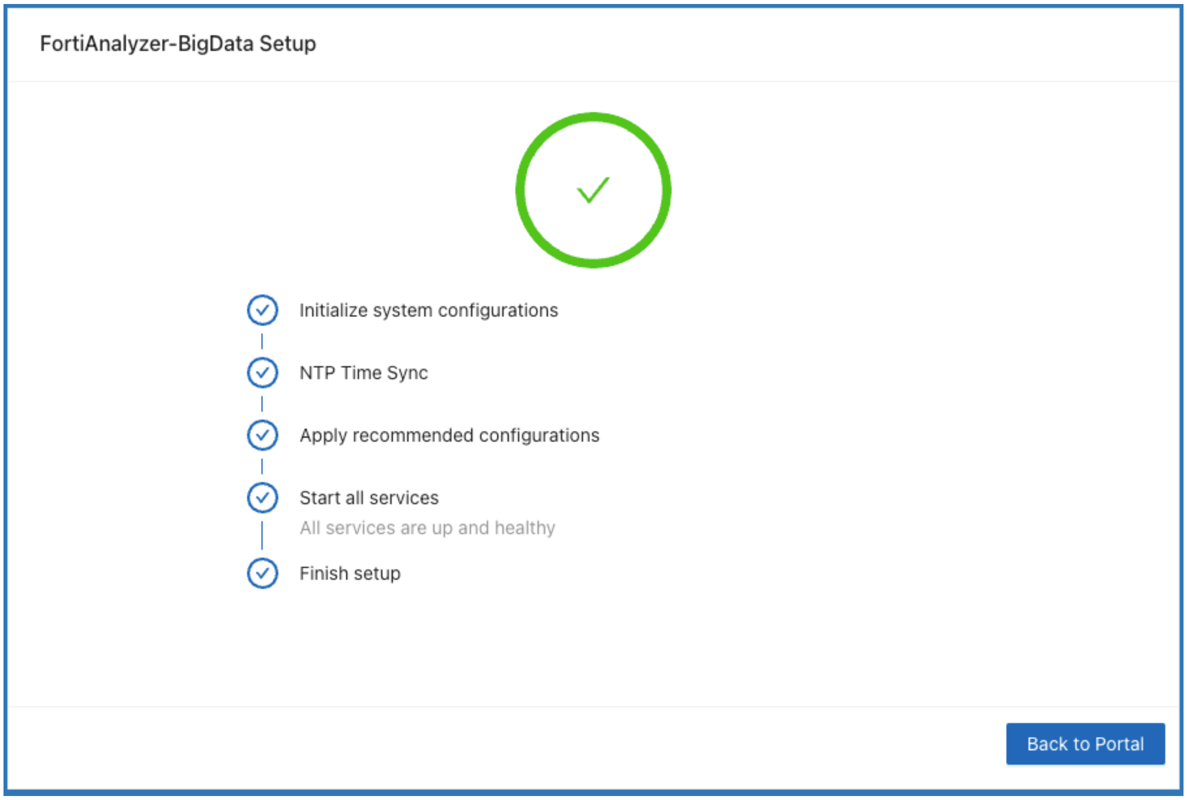
Config	Previous value	Recommend value
kudu-tserver/block_cache_capacity_mb	2048	2577
kudu-tserver/memory_limit_hard_bytes	15811600000	43008957660
kudu-tserver/fs_wal_dir_reserved_bytes	32000000000	7995968000

data

Config	Previous value	Recommend value
data/data.hash.partition		5

5. Click *Setup* to begin the initial setup process.

- The system will perform the necessary setup steps and start all services. After it is complete, you can log into the portal. See below.
- During initial setup, if the management IP setting changed, the browser will try to automatically redirect to new IP address when detected.



FortiAnalyzer-BigData Setup

✓ Initialize system configurations

✓ NTP Time Sync

✓ Apply recommended configurations

✓ Start all services

All services are up and healthy

✓ Finish setup

Set up the FortiAnalyzer-BigData network

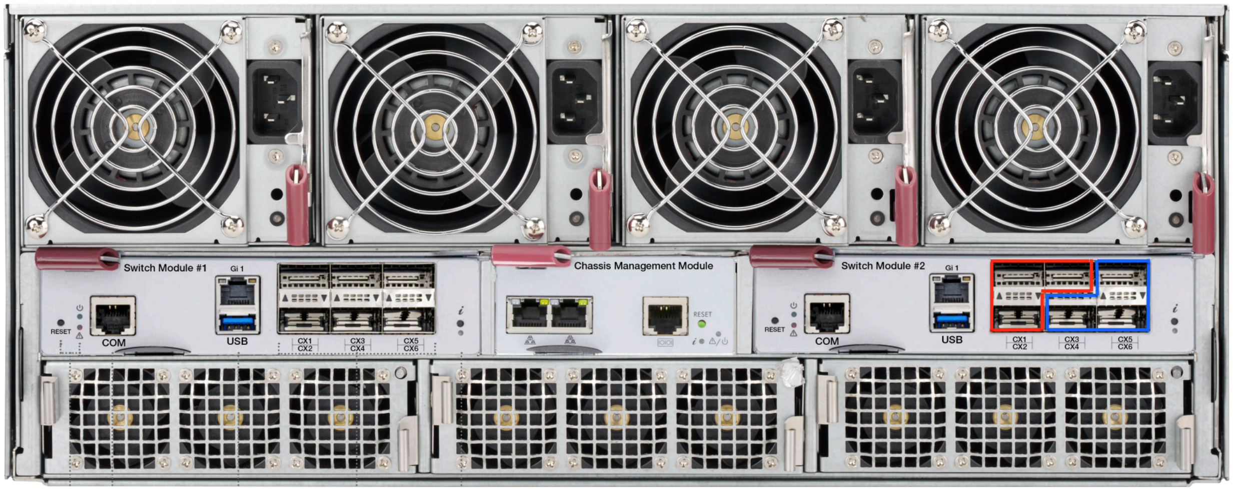
To set up the network for FortiAnalyzer-BigData 4500G, connect a 10GE link with SFP, a 40GE link with QSFP, or a 100GE link with QSFP28 from Switch Module #2 to your public access switch, and then set up the external IP address via the FortiAnalyzer-BigData GUI or CLI. This setup requires two IPs from the same subnet for logging (Main Host) and management (Security Event Manager) access.

If *Dedicated* Main Host or Blade External IP is not enabled (by default), connect the QSFP28 link to one of the CX1 - CX3 ports on Switch Module #2 (highlighted in red below) for all external traffic.

Enable *Dedicated* on Main Host or Blade External to bind the IP to a separate subnet from the Management IP, segregating the log traffic from the Management. See How to segregate the log traffic from the management traffic on page 10.

If *Dedicated* Main Host or Blade External IP is enabled,

- For management traffic network, connect the QSFP28 link to one of the CX1 - CX3 ports on Switch Module #2 (see red highlight in the image below).
- For log traffic network, connect the QSFP28 link to one of the CX4 - CX6 on Switch Module #2 (see blue highlight in the image below).



To set up the network via the GUI for FortiAnalyzer-BigData 4500G:

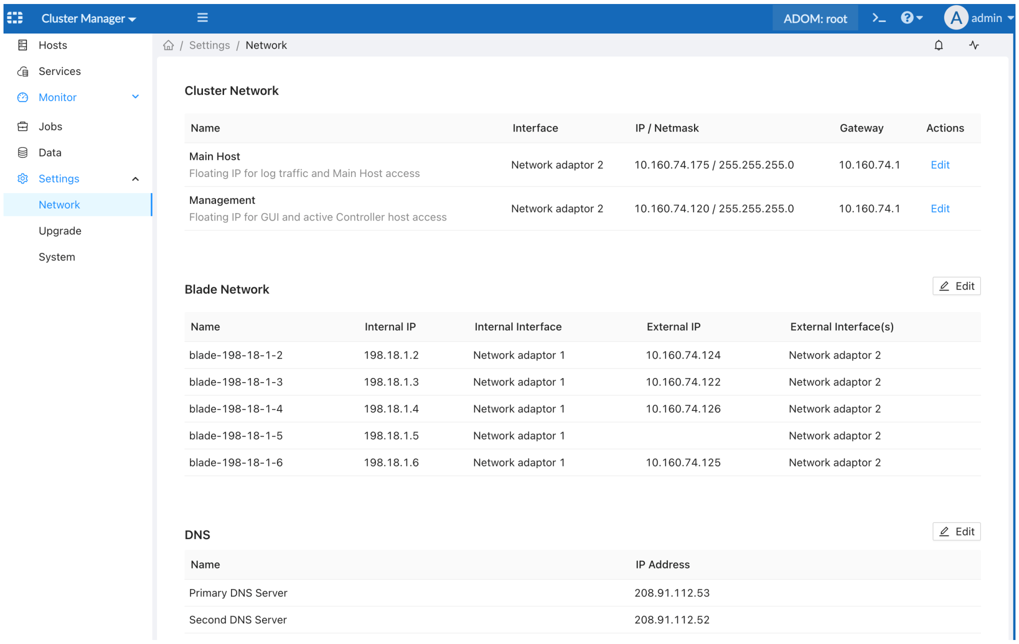
1. From the FortiAnalyzer-BigData web GUI, go to *System Settings* > *Network*.
2. In *Cluster Network* section, edit the Main Host IP Address/Netmask and Gateway fields to your internal network.

   This is the address of the FortiAnalyzer-BigData Main host, which is responsible for collecting the log and serving the services for FortiView, LogView, Reports, and so on.

3. In *Cluster Network* section, edit the Management IP Address/Netmask and Gateway fields to your internal network.

   This is the address of the FortiAnalyzer-BigData Security Event Manager, which is responsible for serving the web GUI and performs various data processing and management workload.

4. Click *Save* to save your changes.



Cluster Network

Name	Interface	IP / Netmask	Gateway	Actions
Main Host Floating IP for log traffic and Main Host access	Network adaptor 2	10.160.74.175 / 255.255.255.0	10.160.74.1	Edit
Management Floating IP for GUI and active Controller host access	Network adaptor 2	10.160.74.120 / 255.255.255.0	10.160.74.1	Edit

Blade Network

Edit

Name	Internal IP	Internal Interface	External IP	External Interface(s)
blade-198-18-1-2	198.18.1.2	Network adaptor 1	10.160.74.124	Network adaptor 2
blade-198-18-1-3	198.18.1.3	Network adaptor 1	10.160.74.122	Network adaptor 2
blade-198-18-1-4	198.18.1.4	Network adaptor 1	10.160.74.126	Network adaptor 2
blade-198-18-1-5	198.18.1.5	Network adaptor 1		Network adaptor 2
blade-198-18-1-6	198.18.1.6	Network adaptor 1	10.160.74.125	Network adaptor 2

DNS

Edit

Name	IP Address
Primary DNS Server	208.91.112.53
Second DNS Server	208.91.112.52

To set up the network via the CLI for FortiAnalyzer-BigData 4500G:

1. Access the Controller. See Connect to the FortiAnalyzer-BigData CLI on page 28.

2. To configure the Management IP Address, use the following command:

   ```
   fazbdctl set addr {ip/mask} {gateway} --management
   ```

   For example, enter `fazbdctl set addr 10.160.74.175/24 10.160.74.1 --management`

   This is the address of the FortiAnalyzer-BigData Security Event Manager, which is responsible for serving the web GUI and performs various data processing and management workload.

3. To configure the main host IP address, use the following command:

   ```
   fazbdctl set addr {ip/mask} {gateway} --mainhost
   ```

   For example, enter `fazbdctl set addr 10.160.74.174/24 10.160.74.1 --mainhost`

   This is the address of the FortiAnalyzer-BigData Main host, which is responsible for collecting the log and serving the services for FortiView, LogView, Reports, and so on.

How to segregate the log traffic from the management traffic

Enable *Dedicated* on Main Host or Blade External to bind the IP to a separate subnet from the Management IP, segregating the log traffic from the Management. The Switch and OS reserve a VLAN with ID 999 and have the ports pre-configured with the VLAN to allow *Dedicated* to be enabled for network segregation purposes. By default, *Dedicated* is disabled on Main Host and Blade External IPs.

To enable *Dedicated* on Main Host for log traffic via the GUI:

1. Make sure the QSFP28 link from the log traffic source to one of the CX4 - CX6 on Switch Module #2 is connected.
2. Go to *System Settings* > *Network*, click *Edit "Main Host" in Cluster Network*.
3. Enable *Dedicated* and update the network settings for log traffic in your segregated subnet.
4. Click *Save* to apply the settings.

To enable *Dedicated* on Main Host for log traffic via the CLI:

1. Make sure the QSFP28 link from the log traffic source to one of the CX4 - CX6 on Switch Module #2 is connected.
2. Access the Controller. See Connect to the FortiAnalyzer-BigData CLI on page 28.
3. To configure the main host IP address through dedicated interface, use the following command:
   ```
   fazbdctl set addr {ip/mask} {gateway} --mainhost -v
   ```

To enable *Dedicated* on Main Host for Hyperscale log traffic via the GUI:

1. Make sure the QSFP28 link from the log traffic source to one of the CX4 - CX6 on Switch Module #2 is connected.
2. Go to *System Settings* > *Network*, click *Edit "Blade Network" in Cluster Network*.
3. Enable *Dedicated* and update the network settings for Hyperscale log traffic in your segregated subnet.
4. Click *Save* to apply the settings.

   For the Management traffic, CX1 - CX3 ports on Switch Module #2 should remain connected.

To enable *Dedicated* on Main Host for Hyperscale log traffic via the CLI:

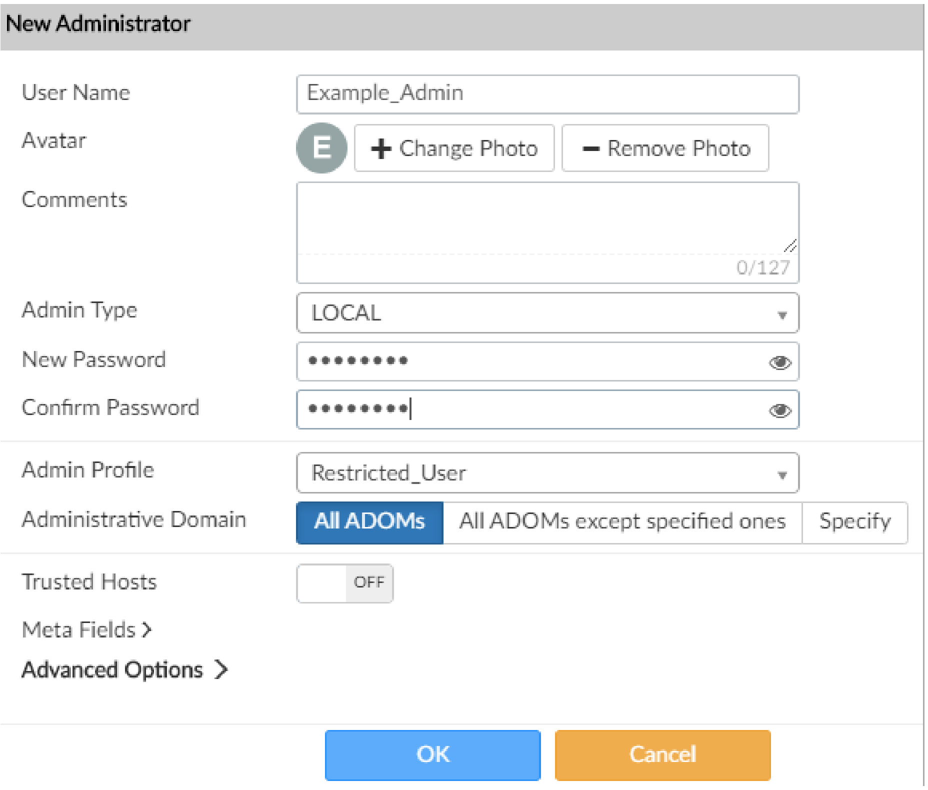
1. Make sure the QSFP28 link from the log traffic source to one of the CX4 - CX6 on Switch Module #2 is connected.
2. Access the Controller. See Connect to the FortiAnalyzer-BigData CLI on page 28.
3. To configure the blade IP address through dedicated interface, use the following command:
   ```
   fazbdctl set addr {ip/mask} {gateway} -v
   ```
   For the Management traffic, CX1 - CX3 ports on Switch Module #2 should remain connected.

Set up Administrator accounts

Set up an administrator account so you can configure your FortiAnalyzer-BigData.

To set up an Administrator account:

1. Go to *System Settings* > *Admin* > *Administrators*, and click *Create New* in the toolbar.
2. In the *User Name* field, enter a new name for your administrator.
3. In the *New Password* and *Confirm Password* fields, enter the password for the administrator account.



New Administrator

User Name	Example_Admin
Avatar	E + Change Photo − Remove Photo
Comments	0/127
Admin Type	LOCAL
New Password	••••••••
Confirm Password	••••••••
Admin Profile	Restricted_User
Administrative Domain	[✓ All ADOMs] All ADOMs except specified ones Specify
Trusted Hosts	OFF

4. Click *OK* to save.

Connect to the Chassis Management Module

The Chassis Management Module (CMM) is used to remotely manage and monitor server hosts, power supplies, cooling fans, and networking switches. The CMM comes with a web management utility that consolidates and simplifies system management for the FortiAnalyzer-BigData chassis. This setup requires 15 IPs from the same subnet: 1 CMM IP and 14 Blade IPMI IPs, and addition two IPs for two switch modules' management GUI if needed.

> The CMM is the module in the middle of the back panel for both the 4500F and 4500G unit; however, there are some differences in the CMM GUI between the two appliances. Proceed with instructions according to your appliance. See the appropriate FortiAnalyzer-BigData Getting Started Guide on the Fortinet Document Library.

Set up the CMM network

To set up CMM network via 4500G CMM GUI:

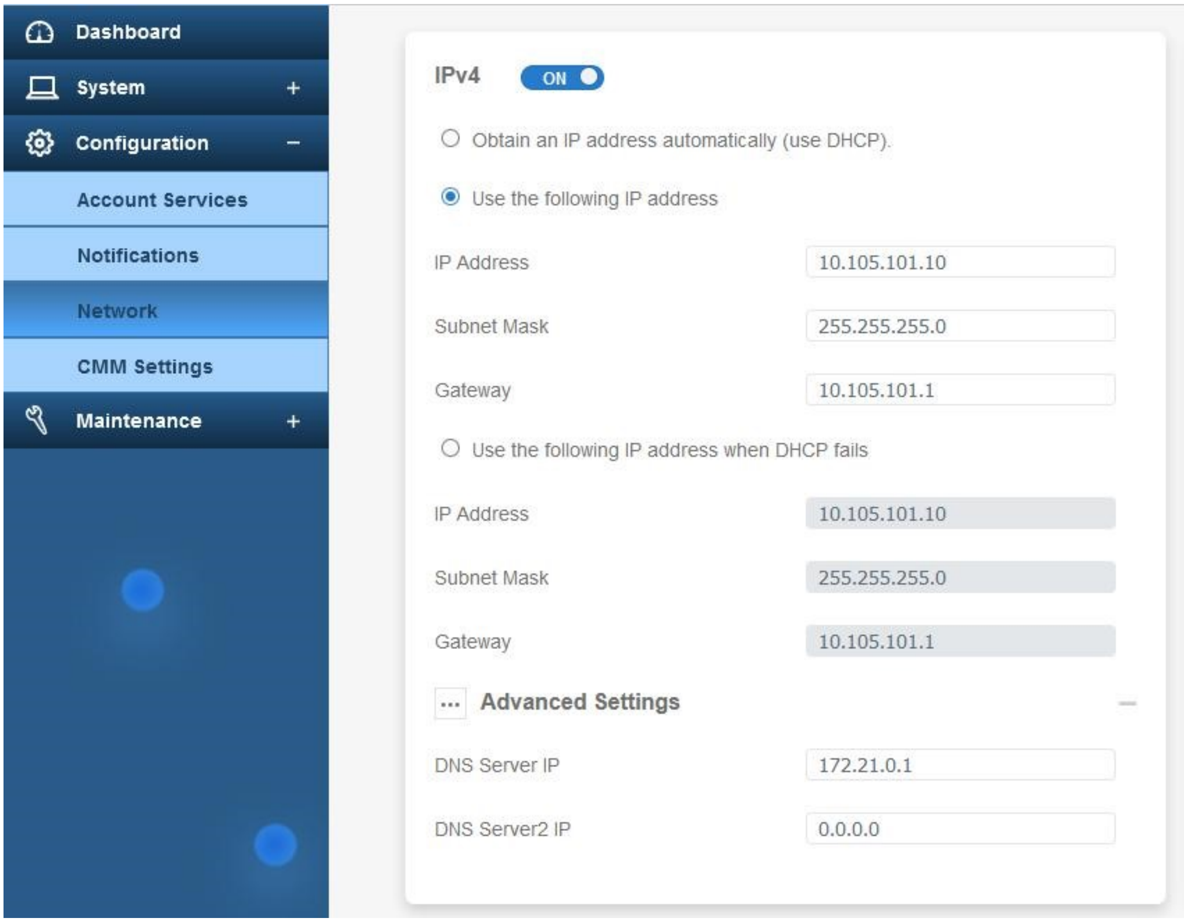
1. Connect a 10GE link from the CMM module (the module in the middle of the back panel) to your public access switch, and set up the external IP address via the CMM web management utility.
2. Connect the port on the CMM Module to a management computer using the supplied Ethernet cable
3. Set the management computer’s IP and subnet to be on the same subnet as FortiAnalyzer-BigData:

   For example:

   - **Static IP Address**: 192.168.100.101
   - **Subnet Mask:** 255.255.255.0
4. On the management computer, open a supported web browser and visit https://192.168.100.100 (the default CMM IP).
5. Log in with the default username and password on the Fortinet Product Credentials card.

   > Changing the default password is strongly recommended. See Configure the CMM password on page 17.
6. Go to *Configuration* > *CMM Network* to configure the CMM network.
7. Select a radio button option for how you want to obtain at IPv4 address.
   - **Obtain an IP address automatically:** Uses DHCP to automatically obtain the IP address.
   - **Use the following IP address:** Set up the IP address by manually entering the IP information into the fields below.

- **Use the following IP address when DHCP fails:** If CMM is unable to obtain the dynamic IP from the DHCP server, it will use the static IP instead. This is the default setting.
- **DNS Server IP**: If DNS server is available, set its IP.



IPv4 ON

○ Obtain an IP address automatically (use DHCP).

● Use the following IP address

IP Address	10.105.101.10
Subnet Mask	255.255.255.0
Gateway	10.105.101.1

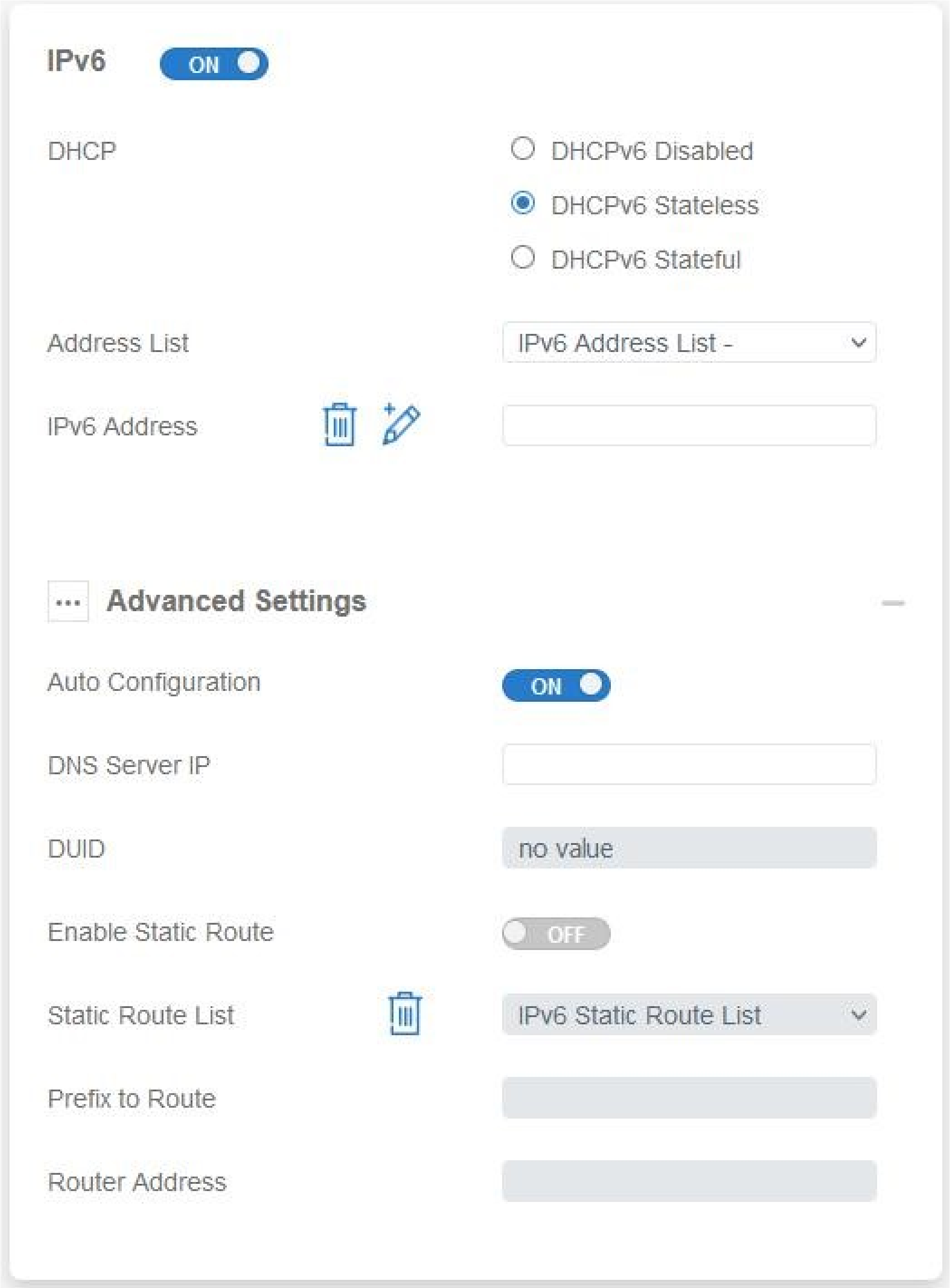
○ Use the following IP address when DHCP fails

IP Address	10.105.101.10
Subnet Mask	255.255.255.0
Gateway	10.105.101.1

... Advanced Settings —

DNS Server IP	172.21.0.1
DNS Server2 IP	0.0.0.0

8. You can also enter your IPv6 information when IPv6 is preferable and available.



IPv6 ON

DHCP
○ DHCPv6 Disabled
● DHCPv6 Stateless
○ DHCPv6 Stateful

Address List: IPv6 Address List -

IPv6 Address:

Advanced Settings

Auto Configuration: ON

DNS Server IP:

DUID: no value

Enable Static Route: OFF

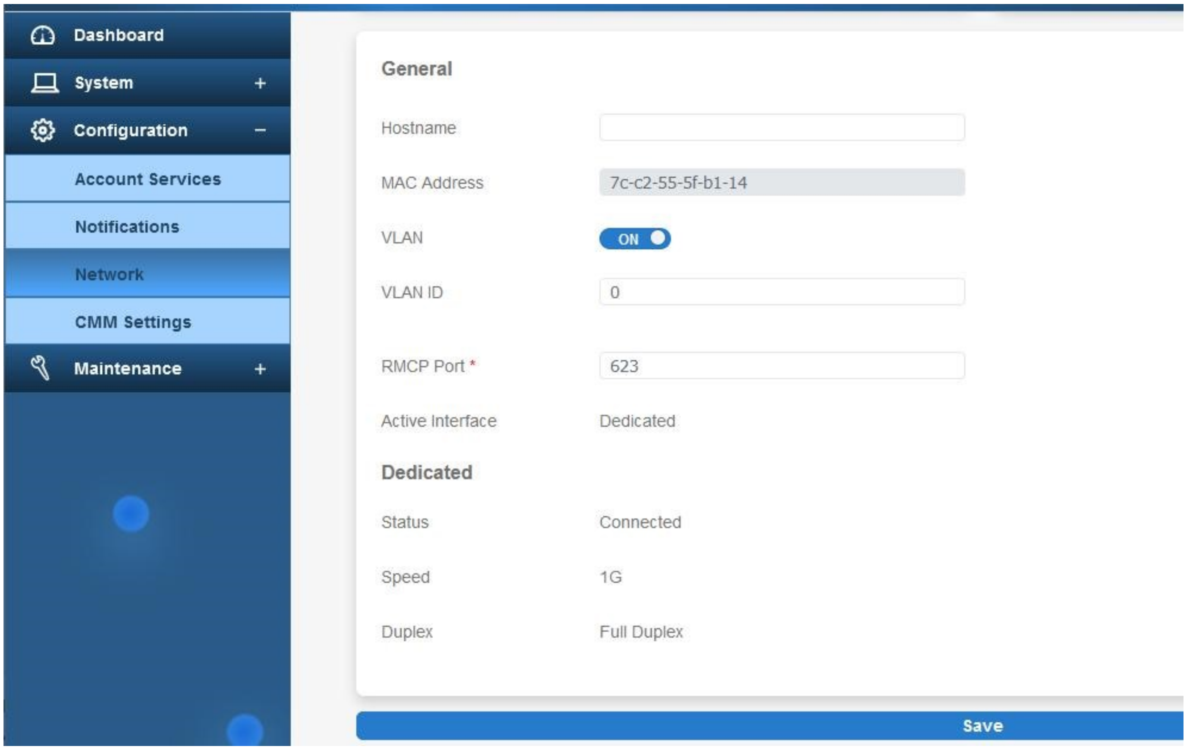
Static Route List: IPv6 Static Route List

Prefix to Route:

Router Address:

9. If you need Virtual LAN support, select **enable** to enable VLAN and enter the VLAN ID in the field.
10. In the RMCP Port field, enter the desired Remote Mail Checking Protocol (RMCP) port based on your configuration.

    The default port is 623.



General

Hostname

MAC Address: 7c-c2-55-5f-b1-14

VLAN: ON

VLAN ID: 0

RMCP Port *: 623

Active Interface: Dedicated

Dedicated

Status: Connected

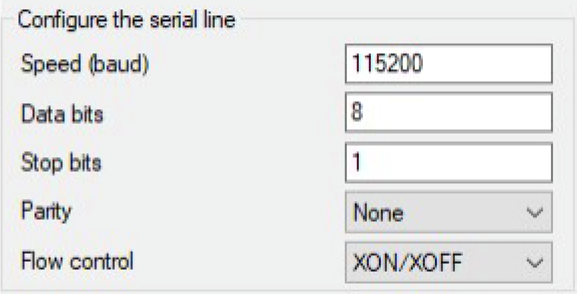
Speed: 1G

Duplex: Full Duplex

11. Once you are done completing the fields, click *Save* to save the CMM Network settings.

To set up CMM network via CLI:

1. Using a USB-to-RJ45 serial adapter, connect a management computer to the serial port on the CMM module.
2. Establish a serial connection to the CMM from the management computer using a serial terminal such as Putty or Hyper Terminal, and enter the following configuration.



Configure the serial line

Speed (baud)	115200
Data bits	8
Stop bits	1
Parity	None
Flow control	XON/XOFF

3. Using the CMM CLI commands, set up IP addresses on the management port.
   Example settings:

```
SET IP 10.100.100.099
SET NETMASK 255.255.255.0
SET GATEWAY 10.100.100.1
SET DHCP DISABLE
APPLY SETTING
```

CMM CLI Commands	Description
`HELP`	Print help.
`RESET`	Reset CMM.
`DEFAULTRESET`	Reset CMM to default.
`VER`	Show CMM FW VER.
`PASSWORDRESET`	Reset password.
`GET LAN INFO`	Get network info.
`SET IP xxx.xxx.xxx.xxx`	Set IP address.
`SET NETMASK xxx.xxx.xxx.xxx`	Set netmask address.
`SET GATEWAY xxx.xxx.xxx.xxx`	Set gateway address.
`SET MAC xx:xx:xx:xx:xx:xx`	Set MAC address.
`SET DHCP ENABLE`	Set DHCP enable.
`SET DHCP DISABLE`	Set DHCP disable.
`SET DHCP FAILOVER`	Set DHCP fails, then use manual configuration.
`APPLY SETTING`	Apply network setting.

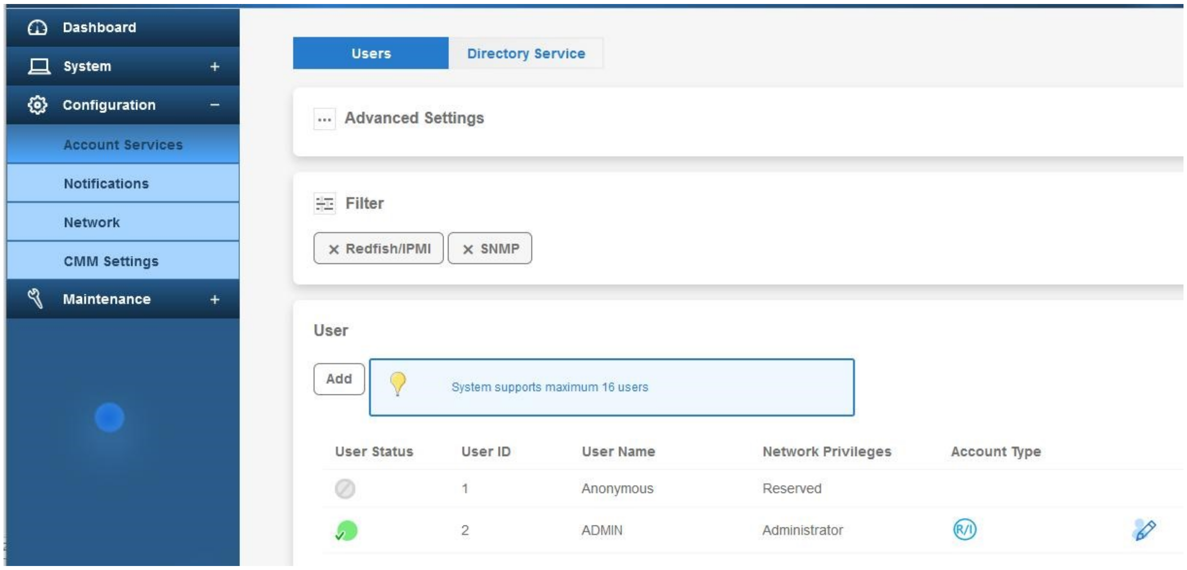
4. Verify the network setup with the `GET LAN INFO` command.
5. Verify that the web management utility can be accessed from a web browser.

Configure the CMM password

You can configure the CMM password via the GUI or CLI.

To change the CMM password via GUI:

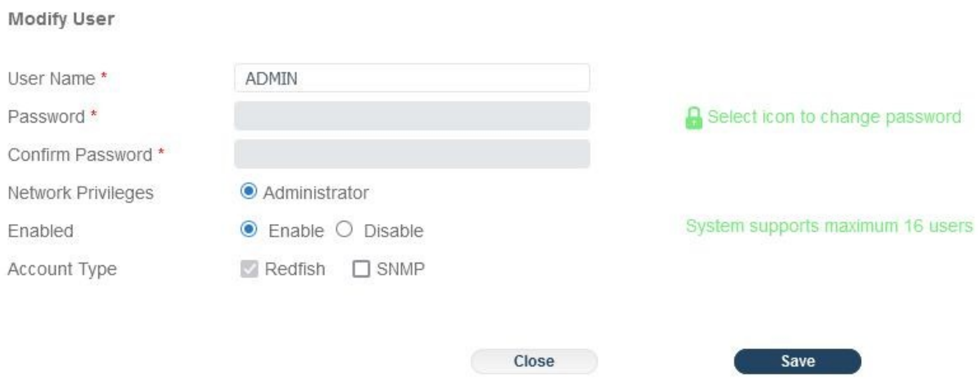
1. From a web browser, access the web management utility using the CMM IP address.
2. Log in with the admin username and password.
3. Go to *Configuration* > *Account Services*.
4. Select the *ADMIN* row and click *Modify User*.



System supports maximum 16 users

User Status	User ID	User Name	Network Privileges	Account Type
⊘	1	Anonymous	Reserved	
✓	2	ADMIN	Administrator	R/I

5. In the *Modify User* dialog, click *Select icon to change password* to change the password.



Modify User

User Name *	ADMIN
Password *	
Confirm Password *	
Network Privileges	● Administrator
Enabled	● Enable ○ Disable
Account Type	☑ Redfish □ SNMP

Select icon to change password

System supports maximum 16 users

6. Click *Save* when done.

To reset the CMM password via CLI:

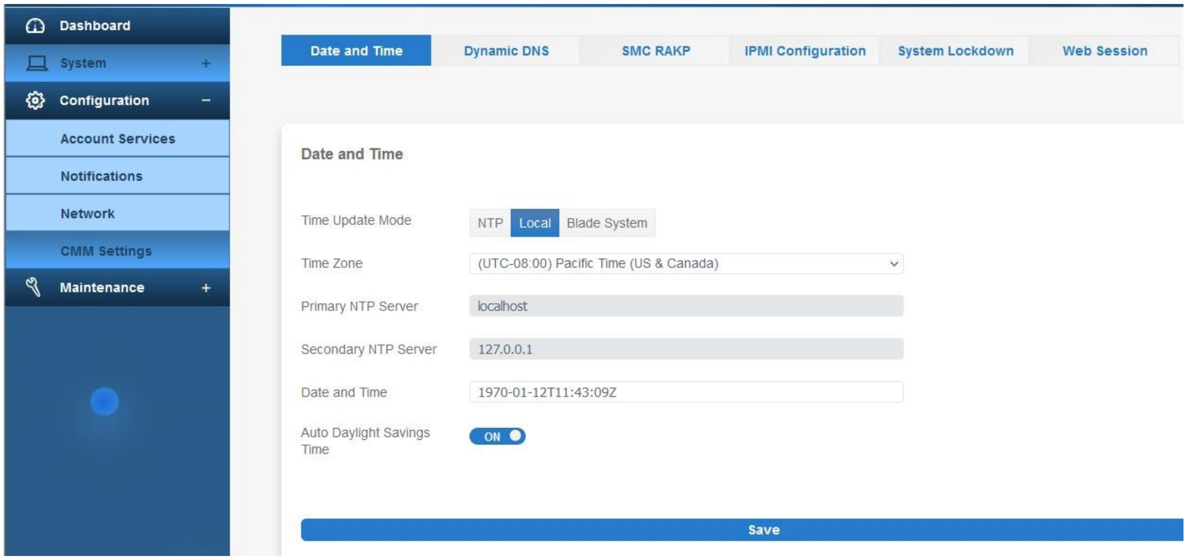
1. Using a USB-to-RJ45 serial adapter, connect a management computer to the serial port on the CMM module.
2. Establish a serial connection to the CMM from the management computer using a serial terminal such as Putty or Hyper Terminal.
3. Use the `PASSWORDRESET` command to reset the password to the default password.

Configure the CMM date and time

You can configure the CMM date and time via the GUI.

To change the CMM date and time via GUI:

1. From a web browser, access the web management utility using the CMM IP address.
2. Log in with the admin username and password.
3. Go to *Configuration* > *CMM Setting* > *Date and Time*.
4. Modify the settings and click *Save* to apply.



Date and Time

Time Update Mode: NTP | [✓ Local] | Blade System

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Primary NTP Server: localhost

Secondary NTP Server: 127.0.0.1

Date and Time: 1970-01-12T11:43:09Z

Auto Daylight Savings Time: ON

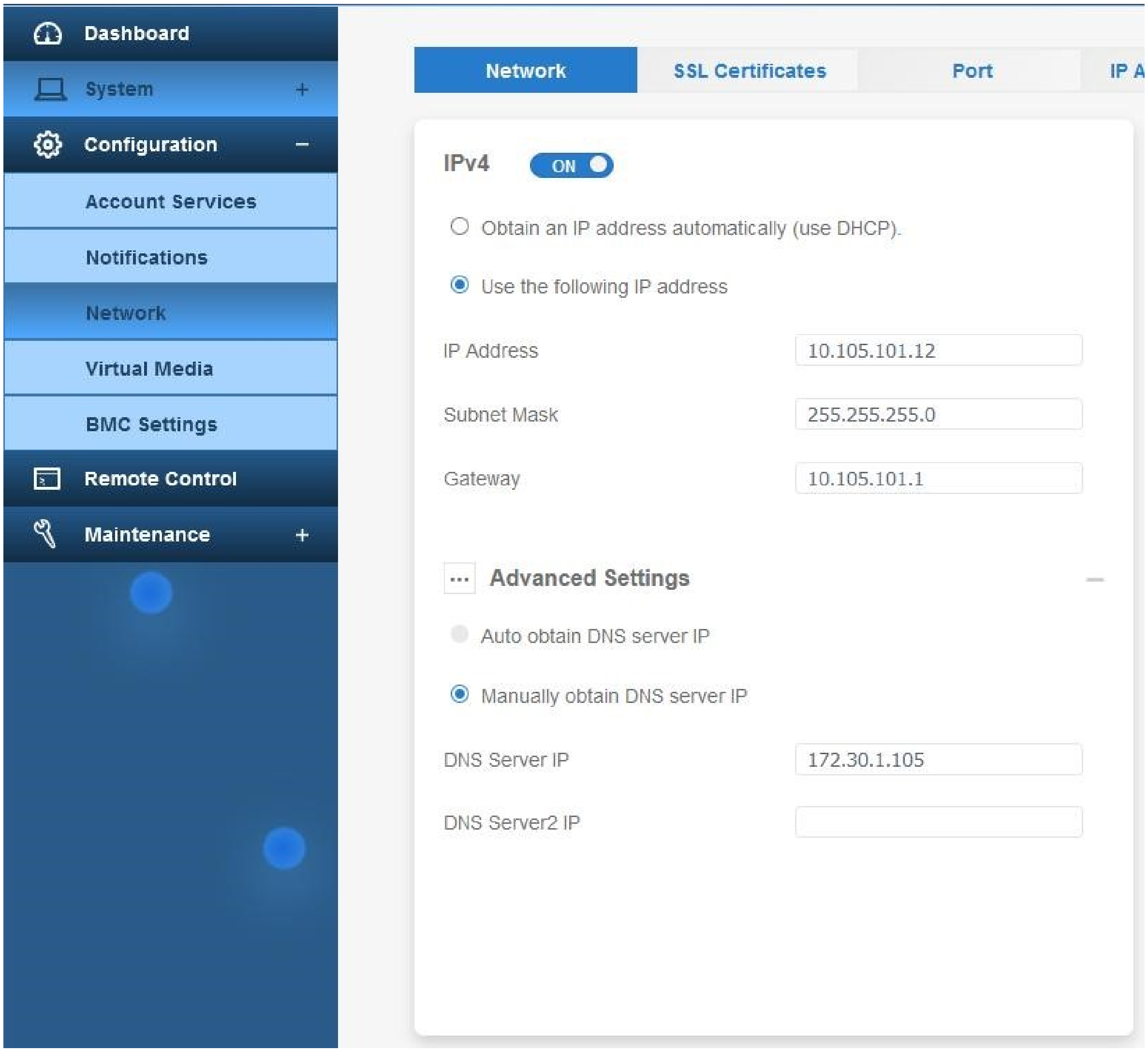
Configure the Blade Management Network

The Blade Management Network should be in the same subnet as Chassis Management Network. See Set up the CMM network on page 13.

To configure the Blade Management Network for a single blade:

1. From a web browser, access the web management utility using the CMM IP address.
2. Go to *Blade System* > *Blade Status*, and click any blade you would like to set up the Blade Management network.
3. In the *Blade Configuration* view, click *Network*.
4. Configure the IPv4 Setting:
   a. Enter the *IP Address*, *Subnet Mask*, *Gateway* and *DNS Service IP*.

b. Click *Save*.



IPv4 ON

○ Obtain an IP address automatically (use DHCP).

● Use the following IP address

IP Address: 10.105.101.12

Subnet Mask: 255.255.255.0

Gateway: 10.105.101.1

Advanced Settings

○ Auto obtain DNS server IP

● Manually obtain DNS server IP

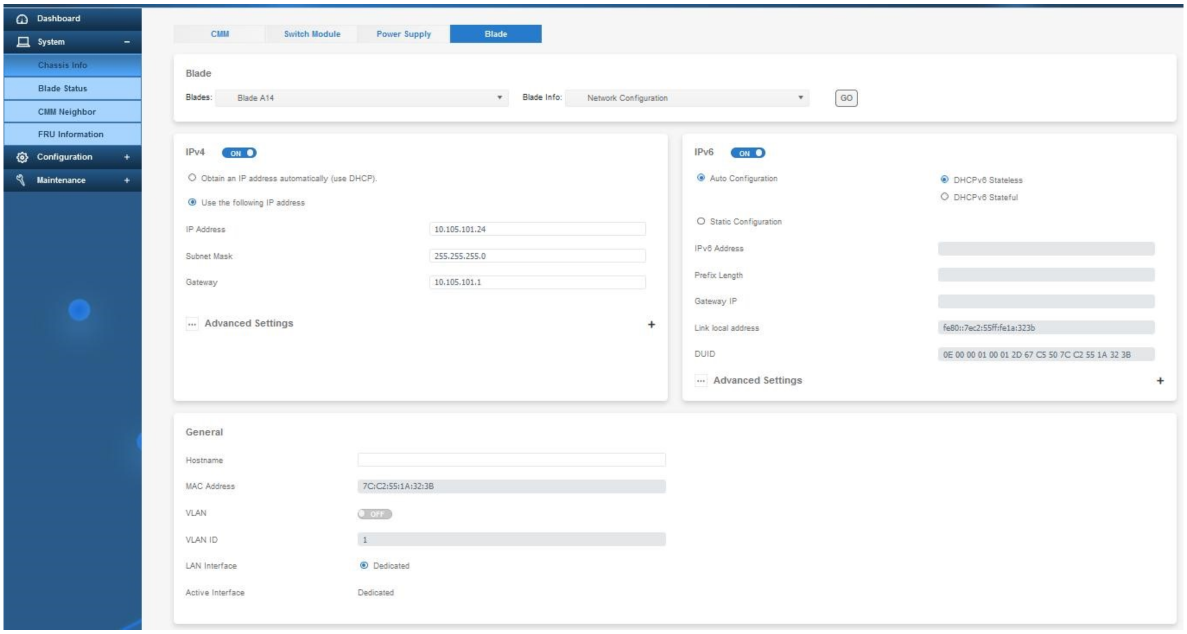
DNS Server IP: 172.30.1.105

DNS Server2 IP:

To configure the Blade Management Network for all blades at once:

1. From a web browser, access the web management utility using the CMM IP address.
2. Go to *System* > *Chassis Info* > *Blade*.
3. Select individual *Blade* and *Network Configuration*.
4. Click *GO*. This enables you to modify the Blade Management Controller (BMC) networks.

5. Click *Save*.



Blade

Blades: Blade A14

Blade Info: Network Configuration

IPv4 ON

○ Obtain an IP address automatically (use DHCP).

● Use the following IP address

IP Address	10.105.101.24
Subnet Mask	255.255.255.0
Gateway	10.105.101.1

Advanced Settings

IPv6 ON

● Auto Configuration

● DHCPv6 Stateless

○ DHCPv6 Stateful

○ Static Configuration

IPv6 Address	
Prefix Length	
Gateway IP	
Link local address	fe80::7ec2:55ff:fe1a:323b
DUID	0E 00 00 01 00 01 2D 67 C5 50 7C C2 55 1A 32 3B

Advanced Settings

General

Hostname	
MAC Address	7C:C2:55:1A:32:3B
VLAN	OFF
VLAN ID	1
LAN Interface	● Dedicated
Active Interface	Dedicated

Remotely control blades via CMM

The CMM web management utility can perform various remote operations on the chassis, such as remote console and power control. This can be used for running diagnostic tasks on individual blades. It also allows the administrator to remotely control the FortiAnalyzer-BigData via CLIs if the management IP resets after a software hard reset. For more information, see the FortiAnalyzer-BigData Administration Guide on the Fortient Document Library.

To access the Security Event Manager Controller:

1. Go to *Blade System* > *Summary* and select *Blade A2*.
2. To enter the BMC for the Security Event Manager Controller, click the *BMC IPV4* link.

   The default login credentials are on the Fortinet Product Credentials card.
3. Go to *Remote Control* > *Console Redirection or iKVM/HTML5*.
4. Log in with username `root` and password `fortinet@123`.

   You can now access the Security Event Manager Controller and use `fazbdctl` CLI commands to manage the cluster.

You can use the CMM web management utility to remotely access and control the other blades by following the general steps.

You can also use the utility to remotely access the FortiAnalyzer-BigData Bootloader. For more information, see the FortiAnalyzer-BigData Administration Guide on the Fortinet Document Library.

Configure the BMC password

You can configure the BMC password via the CMM.

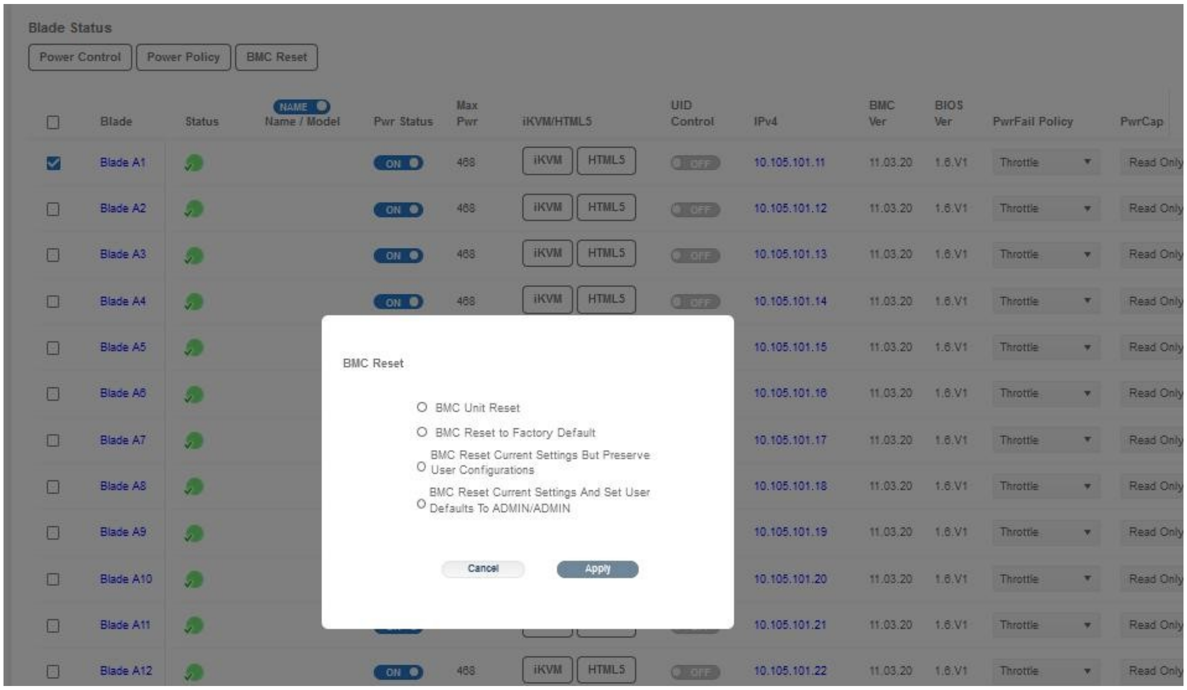
To change the BMC password via the CMM:

1. From a web browser, access the web management utility using the CMM IP address.
2. Log in with the admin username and password.
3. Go to *System* > *Blade Status*.
4. Select the blade you want to change, for example, Blade A1.
5. To enter the BMC for the FortiAnalyzer-BigData main host, click the *BMC IPV4* link.

   The default login credentials are on the Fortinet Product Credentials card.
6. Go to *Configuration* > *Account Services*.
7. Select the *ADMIN* row and click *Modify User*.
8. Click the *Change Password* checkbox, change the password, and click *Modify*.

To reset the BMC password via CMM:

1. From a web browser, access the web management utility using the CMM IP address.
2. Log in with the admin username and password.
3. Go to *Blade Status* and select the blade you want to change, for example, Blade A1.
4. Click *BMC Reset*.
5. Select the appropriate option and click *Apply*.



Blade Status

□	Blade	Status	NAME Name / Model	Pwr Status	Max Pwr	iKVM/HTML5	UID Control	IPv4	BMC Ver	BIOS Ver	PwrFail Policy	PwrCap
☑	Blade A1	●		ON	468	iKVM HTML5	OFF	10.105.101.11	11.03.20	1.6.V1	Throttle ▾	Read Only
□	Blade A2	●		ON	468	iKVM HTML5	OFF	10.105.101.12	11.03.20	1.6.V1	Throttle ▾	Read Only
□	Blade A3	●		ON	468	iKVM HTML5	OFF	10.105.101.13	11.03.20	1.6.V1	Throttle ▾	Read Only
□	Blade A4	●		ON	468	iKVM HTML5	OFF	10.105.101.14	11.03.20	1.6.V1	Throttle ▾	Read Only
□	Blade A5	●						10.105.101.15	11.03.20	1.6.V1	Throttle ▾	Read Only
□	Blade A6	●						10.105.101.16	11.03.20	1.6.V1	Throttle ▾	Read Only
□	Blade A7	●						10.105.101.17	11.03.20	1.6.V1	Throttle ▾	Read Only
□	Blade A8	●						10.105.101.18	11.03.20	1.6.V1	Throttle ▾	Read Only
□	Blade A9	●						10.105.101.19	11.03.20	1.6.V1	Throttle ▾	Read Only
□	Blade A10	●						10.105.101.20	11.03.20	1.6.V1	Throttle ▾	Read Only
□	Blade A11	●						10.105.101.21	11.03.20	1.6.V1	Throttle ▾	Read Only
□	Blade A12	●		ON	468	iKVM HTML5	OFF	10.105.101.22	11.03.20	1.6.V1	Throttle ▾	Read Only

BMC Reset

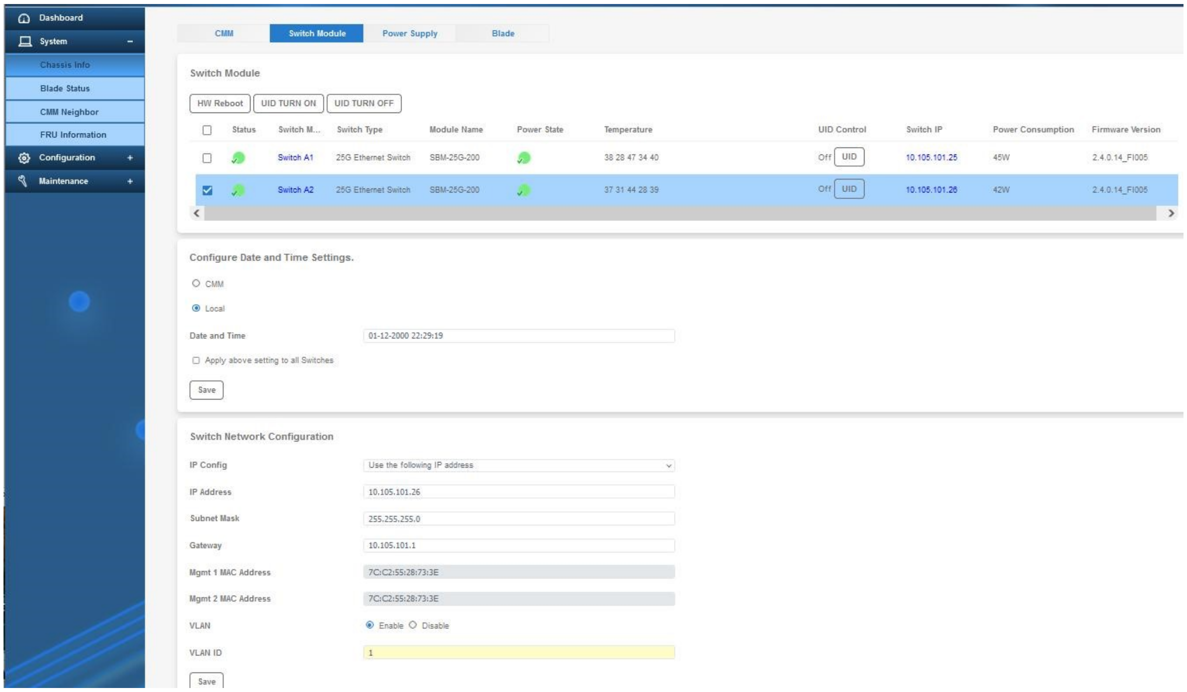
○ BMC Unit Reset
○ BMC Reset to Factory Default
○ BMC Reset Current Settings But Preserve User Configurations
○ BMC Reset Current Settings And Set User Defaults To ADMIN/ADMIN

Turn off STP BPDU

The following configuration is optional.

To turn off STP BPDU:

1. Connect to the Chassis Management Module.
2. Go to *Blade System* > *Switch Module*, and click *Switch A2*. The *Switch Module* pane opens.



Switch Module

☐	Status	Switch M...	Switch Type	Module Name	Power State	Temperature	UID Control	Switch IP	Power Consumption	Firmware Version
☐	●	Switch A1	25G Ethernet Switch	SBM-25G-200	●	38 28 47 34 40	Off UID	10.105.101.25	45W	2.4.0.14_FI005
☑	●	Switch A2	25G Ethernet Switch	SBM-25G-200	●	37 31 44 28 39	Off UID	10.105.101.26	42W	2.4.0.14_FI005

Configure Date and Time Settings.

○ CMM

● Local

Date and Time: 01-12-2000 22:29:19

☐ Apply above setting to all Switches

Save

Switch Network Configuration

IP Config	Use the following IP address
IP Address	10.105.101.26
Subnet Mask	255.255.255.0
Gateway	10.105.101.1
Mgmt 1 MAC Address	7C:C2:55:28:73:3E
Mgmt 2 MAC Address	7C:C2:55:28:73:3E
VLAN	● Enable ○ Disable
VLAN ID	1

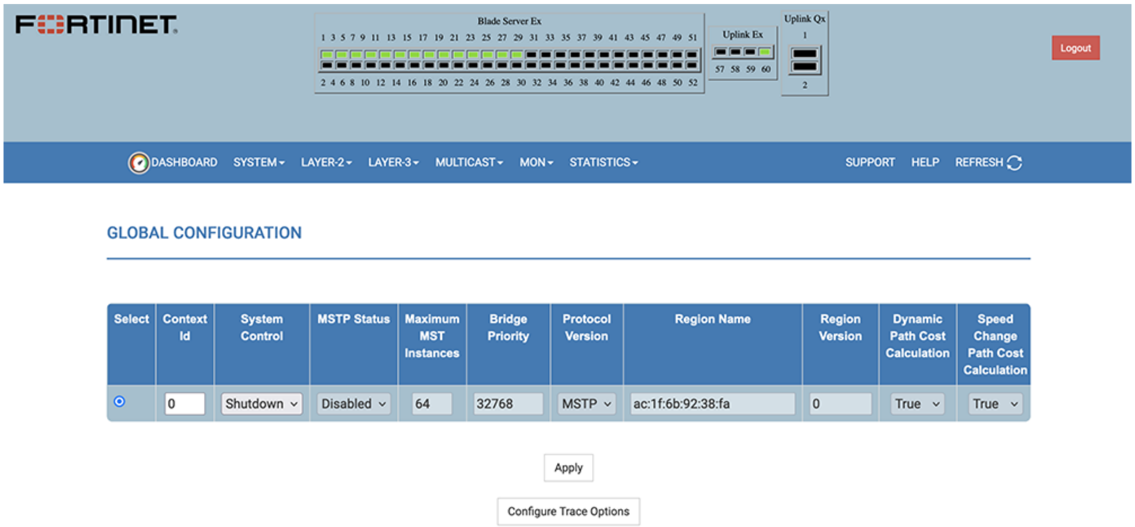
Save

The default *Username* and *Password* are both ADMIN.

For security purposes, we recommend changing the *Username* and *Password*.

3. Under *Switch Network Configuration*, in the *IP Addess* field, enter the IP address, and click *Save*.
4. Under *Switch Information*, click the *Management IP* column, and enter the management web GUI for *Switch A2*.
5. Go to *Layer-2* > *MSTP* > *Basic Settings*.
    a. Set *MSTP Status* to *Disabled*.
    b. Set *System Control* to *Shutdown*.

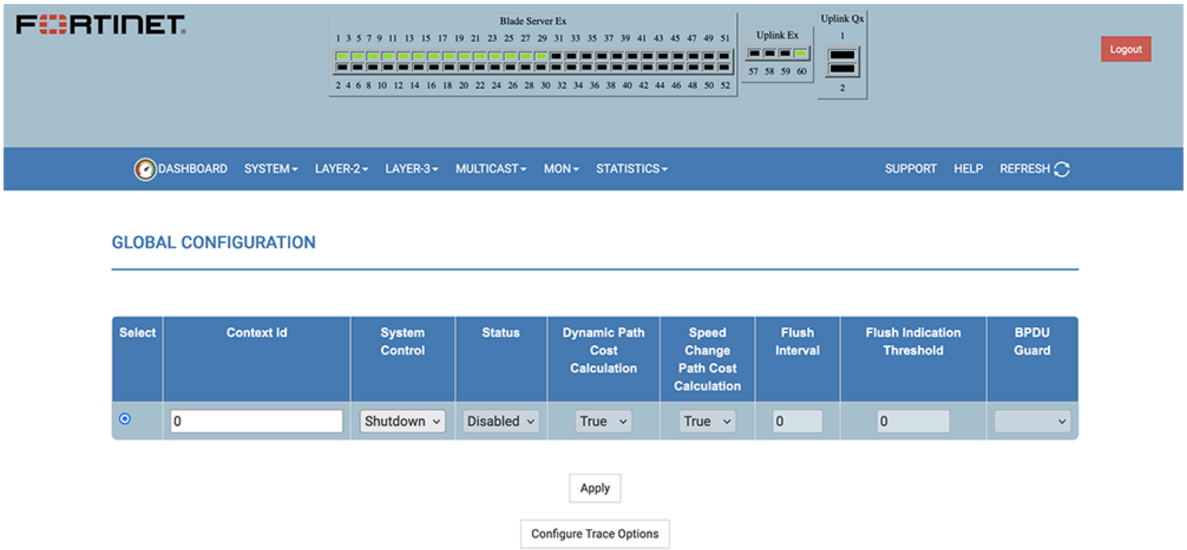
c. Click *Apply*.



GLOBAL CONFIGURATION

Select	Context Id	System Control	MSTP Status	Maximum MST Instances	Bridge Priority	Protocol Version	Region Name	Region Version	Dynamic Path Cost Calculation	Speed Change Path Cost Calculation
●	0	Shutdown	Disabled	64	32768	MSTP	ac:1f:6b:92:38:fa	0	True	True

6. Go to *Layer-2* > *RSTP* > *Global Settings*, and confirm:
   - *Status* is *Disabled*
   - *System Control* is *Shutdown* (default)



GLOBAL CONFIGURATION

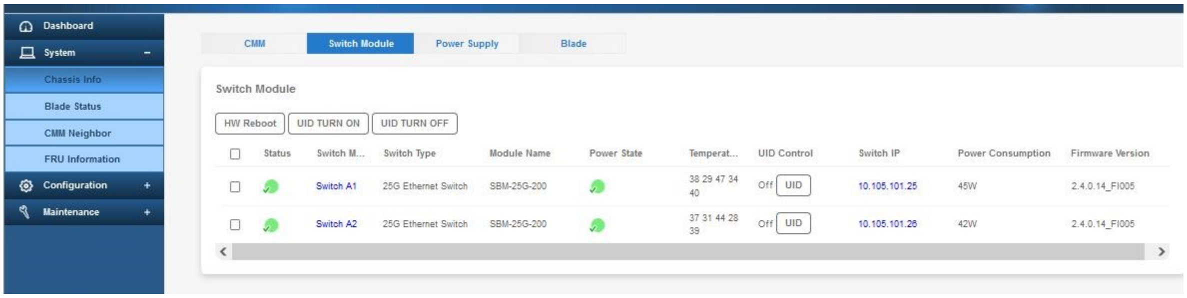
Select	Context Id	System Control	Status	Dynamic Path Cost Calculation	Speed Change Path Cost Calculation	Flush Interval	Flush Indication Threshold	BPDU Guard
●	0	Shutdown	Disabled	True	True	0	0	

Configure LACP

The following configuration is optional.

To configure port channel on the FortiAnalyzer-BigData switch module:

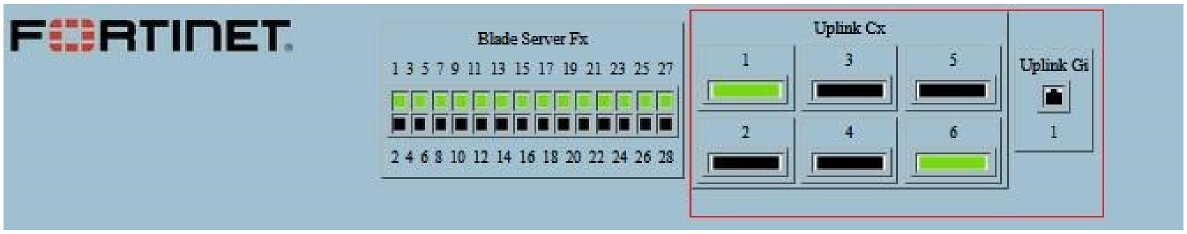
1. In CMM, go to *Switch Module* and click the Management IP of Switch A2 to log into the switch web-based management utility.



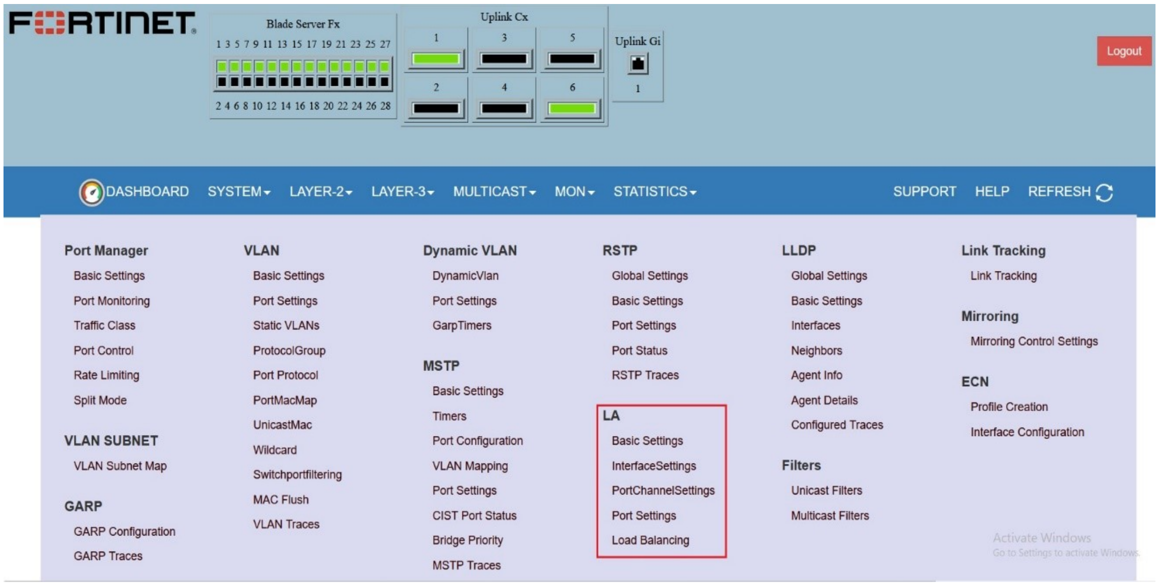
Switch Module

□	Status	Switch M...	Switch Type	Module Name	Power State	Temperat...	UID Control	Switch IP	Power Consumption	Firmware Version
□	●	Switch A1	25G Ethernet Switch	SBM-25G-200	●	38 29 47 34 40	Off UID	10.105.101.25	45W	2.4.0.14_FI005
□	●	Switch A2	25G Ethernet Switch	SBM-25G-200	●	37 31 44 28 39	Off UID	10.105.101.26	42W	2.4.0.14_FI005

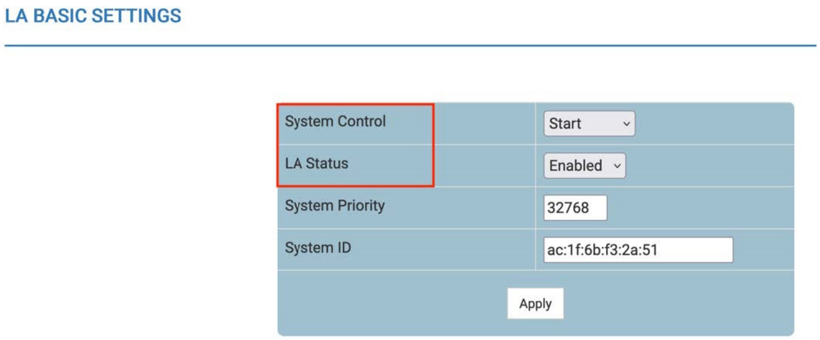
2. In the switch web-based management utility, the switch ports are displayed in home page. The switch external ports are Cx0/1 to Cx0/6, and Gi0/1. Mouse over the port to get the port name.



3. To complete the next steps, you will use the pages for port channel configurations under *LAYER-2 > LA*.



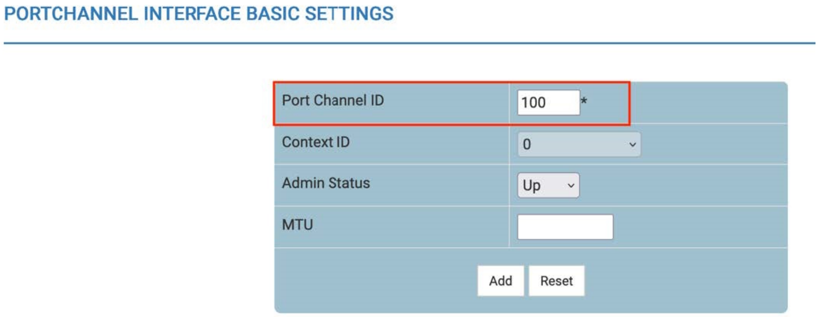
4. In *LA Basic Settings*, verify the following:
   - *System Control* is *Start*
   - *LA Status* is *Enabled*



LA BASIC SETTINGS

System Control	Start
LA Status	Enabled
System Priority	32768
System ID	ac:1f:6b:f3:2a:51

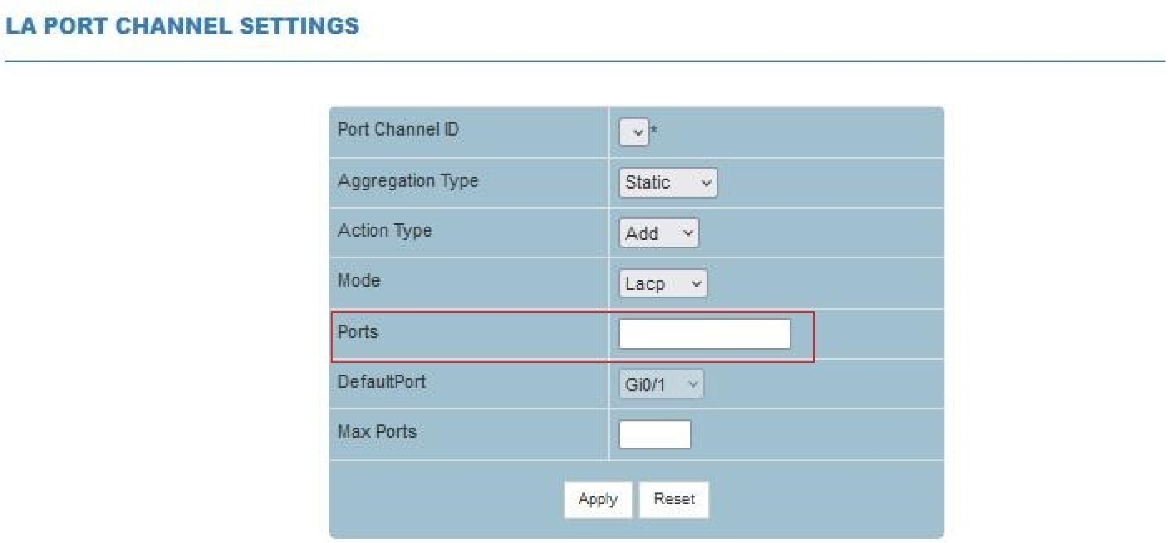
5. In *LA Interface Settings*, input *Port Channel ID*, and click *Add*.



PORTCHANNEL INTERFACE BASIC SETTINGS

Port Channel ID	100 *
Context ID	0
Admin Status	Up
MTU	

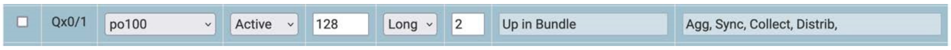
6. In *LA Port Channel Settings*, input member ports in *Ports*, and click *Apply*.



LA PORT CHANNEL SETTINGS

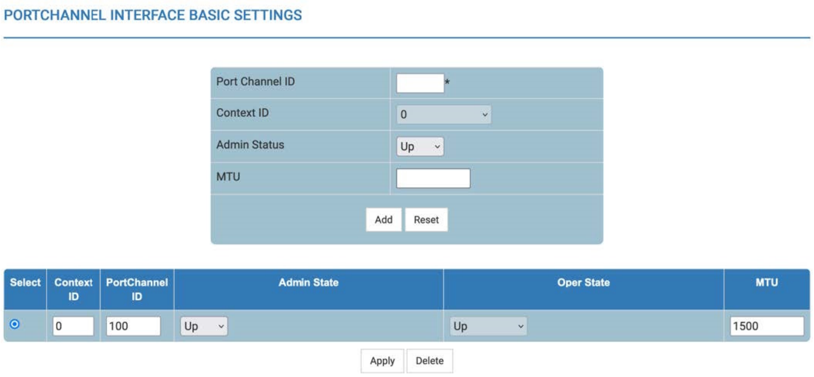
Port Channel ID	*
Aggregation Type	Static
Action Type	Add
Mode	Lacp
Ports	
DefaultPort	Gi0/1
Max Ports	

7. In *LA Port Settings*, verify that the member port is assigned to the port channel and the *Mode* is *Active*. *Port State* should be changed to *Up in Bundle* after the port link comes up.



☐	Qx0/1	po100	Active	128	Long	2	Up in Bundle	Agg, Sync, Collect, Distrib,

8. In *LA Interface Settings*, the port channel *Oper State* will become *Up* after at least one member port link comes up.

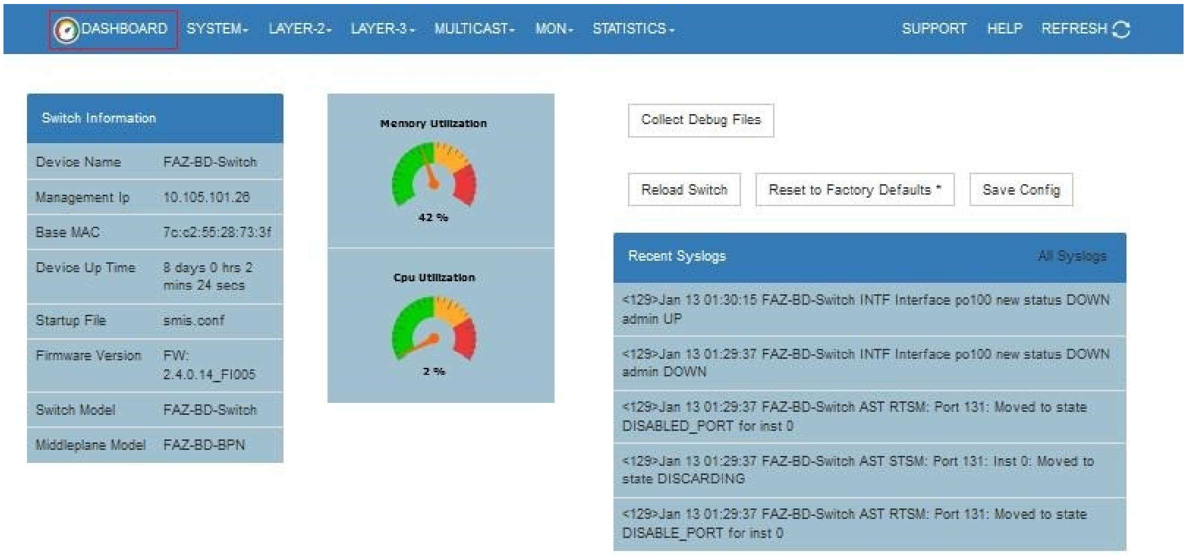


PORTCHANNEL INTERFACE BASIC SETTINGS

Port Channel ID	*
Context ID	0
Admin Status	Up
MTU	

Select	Context ID	PortChannel ID	Admin State	Oper State	MTU
●	0	100	Up	Up	1500

9. Go to *Dashboard*, and then click *Save Config* to save the configuration.



Switch Information	
Device Name	FAZ-BD-Switch
Management Ip	10.105.101.26
Base MAC	7c:c2:55:28:73:3f
Device Up Time	8 days 0 hrs 2 mins 24 secs
Startup File	smis.conf
Firmware Version	FW: 2.4.0.14_FI005
Switch Model	FAZ-BD-Switch
Middleplane Model	FAZ-BD-BPN

Recent Syslogs All Syslogs

```
<129>Jan 13 01:30:15 FAZ-BD-Switch INTF Interface po100 new status DOWN admin UP
<129>Jan 13 01:29:37 FAZ-BD-Switch INTF Interface po100 new status DOWN admin DOWN
<129>Jan 13 01:29:37 FAZ-BD-Switch AST RTSM: Port 131: Moved to state DISABLED_PORT for inst 0
<129>Jan 13 01:29:37 FAZ-BD-Switch AST STSM: Port 131: Inst 0: Moved to state DISCARDING
<129>Jan 13 01:29:37 FAZ-BD-Switch AST RTSM: Port 131: Moved to state DISABLE_PORT for inst 0
```

Connect to the FortiAnalyzer-BigData CLI

After configuring the FortiAnalyzer-BigData network, you can use the IP addresses to access the FortiAnalyzer-BigData Main CLI or the Security Event Manager 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 in the set up process. See Initial set up on page 5.
2. Log in using the administrator credentials you created in Set up Administrator accounts on page 12.

   If you did not create a new administrator credential, use the default credentials of username `admin` with no password.

To connect to the Security Event Manager Controller:

1. Establish an SSH connection to the Cluster Management IP you configured in Initial set up on page 5.

   > If the Cluster Management IP is not reachable, you can SSH to the Main CLI first (see To connect to the FortiAnalyzer-BigData Main CLI: on page 28) and then SSH to the Controller host or any of the cluster hosts using its internal IP. For example, to SSH to the Controller host, use `exec ssh root@198.18.1.2`.
   >
   > The IP it is in can be determined by this format: `198.18.{chassis_id}.{blade_id}` where 198.18* is the default internal subnet.

2. Log in using the default username `root` and password `fortinet@123`.
3. After establishing a connection, you can use the `fazbdctl` CLI commands to manage the cluster.

   For more information, see the FortiAnalyzer-BigData CLI Reference on the Fortinet Doc Library.

   > Fortinet strongly recommends that you update the password with the `fazbdctl set password` command.

Change Log

Date	Change Description
2025-05-30	Initial release.

www.fortinet.com

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 Chief Legal Officer, 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. 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.