




FortiAnalyzer Unit LED Indicators

Light Icon	Description
	The light flashes orange when packets are sent and received on the Ethernet port.
	Power indicator is blue when the FortiAnalyzer system is on.
	The light flashes blue when reading the boot device.
Hard Disk Upper LED	Blue when the hard disk is properly inserted into the drive bay and the FortiAnalyzer is plugged in to a power source.
Hard Disk Lower LED	Flashes blue when reading and writing to the hard disk.



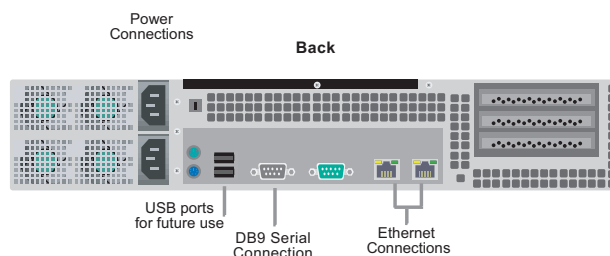
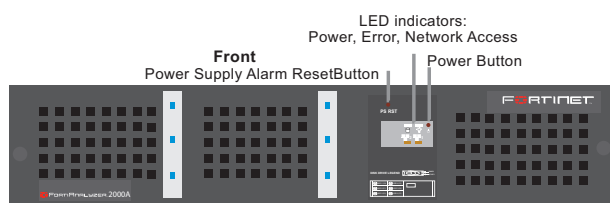
FortiAnalyzer-2000A



© Copyright 2008 Fortinet Incorporated. All rights reserved.
 Products mentioned in this document are trademarks or registered trademarks of their respective holders.
 Regulatory Compliance
 FCC Class A Part 15 CSA/CUS
 18 March 2008

05-30006-0352-20080318

1 Checking the Package Contents



Ethernet Cables:
 Orange - Crossover
 Grey - Straight-through



Null-Modem Cable
 (RS-232)



Power Cable

Connector	Type	Speed	Protocol	Description
Ports 1 and 2	RJ-45	10/100/1000 Base-T	Ethernet	Connection to the network
CONSOLE	DB-9	9600 bps	RS-232	Connection to the management computer. Provides access to the command line interface (CLI).

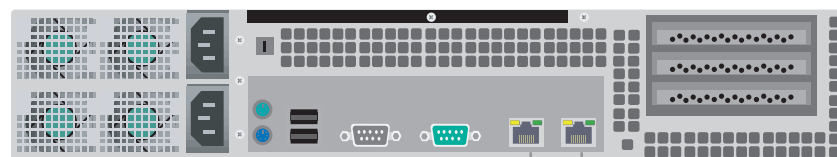
2 Connecting

Connect the FortiAnalyzer unit to a power outlet and to the network hub or switch.

- Insert the hard disks included in the FortiAnalyzer package into the bays of the FortiAnalyzer unit, starting in bay 1. **Use the diagram on the front panel as a guide.**
- Place the FortiAnalyzer unit on a stable surface. It requires 1.5 inches (3.75 cm) clearance on each side to allow for cooling.
- Insert a network cable to port 1. Insert the other end to the router or switch connected to the network.
- Connect one power chord to a power supply. Connect the other power cord to an alternate power source if available.
- Connect the Power Cord to a surge protected power bar or power supply.
- Press the Power button to turn on the FortiAnalyzer unit.
- The power LED appears blue and the hard disk icon LED flashes blue while the system boots.
- For more information, see the *FortiAnalyzer Install Guide*.



Power connections



Null modem cable connects to serial port on management computer.

Straight-through Ethernet cable connects to hub or switch on the network.

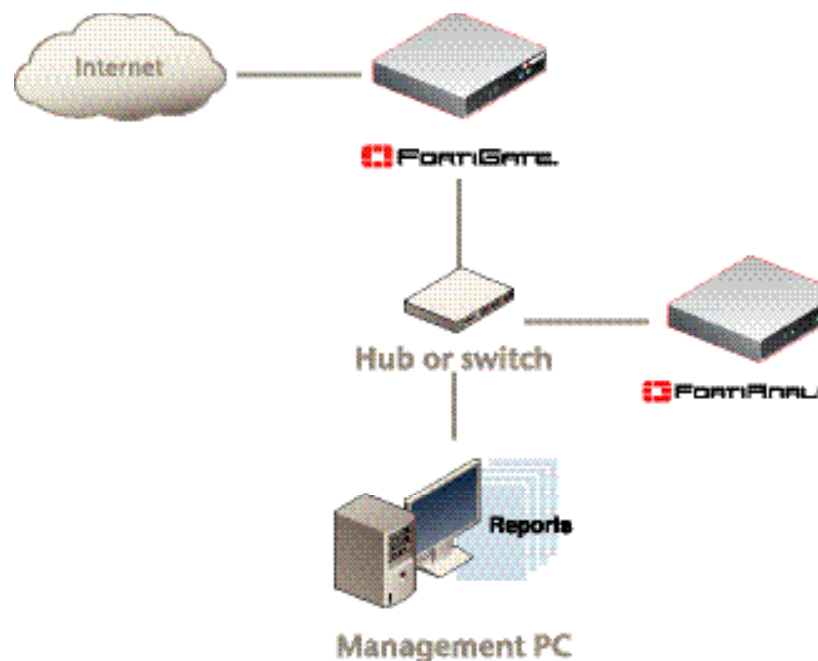
3 Planning the Configuration

You can add the FortiAnalyzer unit to your local FortiGate network to receive log messages from your local FortiGate units, or connect the FortiAnalyzer unit to the FortiGate units remotely using FortiManager. To connect the FortiAnalyzer unit to the FortiGate units remotely, you must configure the DNS server and the default gateway.

To manage the FortiAnalyzer unit, you can use a computer within the local network or over the Internet.

Factory Defaults

Administrator Account	User name:	admin
	Password:	(none)
Port 1	IP:	192.168.1.99
	Netmask:	255.255.255.0
	Management Access:	ping, https, http, ssh
Port 2	IP:	192.168.2.99
	Netmask:	255.255.255.0
	Management Access:	ping, https, http, ssh



4 Choosing a Configuration Tool

Web-based manager

The FortiAnalyzer web-based manager is an easy to use management tool. Use it to configure the administrator password, the interface and default gateway addresses, and the DNS server addresses.

Requirements:

- An Ethernet connection between the FortiAnalyzer unit and management computer.
- Internet Explorer 6.0 or higher on the management computer.

Command Line Interface (CLI)

The CLI is a full-featured management tool. Use it to configure the administrator password, the interface addresses, the default gateway address, and the DNS server addresses. To configure advanced settings, see the Tools and Documentation CD-ROM.

Requirements:

- An DB-9 serial connection between the FortiAnalyzer unit and management computer.
- A terminal emulation application (HyperTerminal for Windows) on the management computer.

5 Configuring the FortiAnalyzer Unit

Web-based Manager

Use the following procedure to connect to the web-based manager for the first time. Configuration changes made with the web-based manager are effective immediately without resetting the FortiAnalyzer unit or interrupting service.

To connect to the web-based manager

1. Connect the Port 1 interface of the FortiAnalyzer unit to Ethernet port of the management computer.
Use a cross-over Ethernet cable to connect the devices directly. Use straight-through Ethernet cables to connect the devices through a hub or switch.
2. Configure the management computer to be on the same subnet as the FortiAnalyzer LAN interface.
To do this, change the IP address of the management computer to 192.168.1.2 and the netmask to 255.255.255.0.
3. To access the FortiAnalyzer web-based manager, in your browser, go to <https://192.168.1.99> (remember to include the "s" in https://).
4. Type `admin` in the Name field and select Login.

After connecting to the Web-based manager, you can configure the FortiAnalyzer unit IP address, DNS server IP address, and default gateway to connect the FortiAnalyzer unit to the network.

To configure interfaces

1. Go to **System > Network > Interface**.
2. Select the edit icon for each interface to configure.
3. Set the IP address and netmask for the interface.
4. Select OK.

To configure the Primary and Secondary DNS server IP addresses

1. Go to **System > Network > DNS**, enter the Primary and Secondary DNS IP addresses select Apply.

To configure a Default Gateway

1. Go to **System > Network > Routing** and select Create New.
2. Set Gateway to the Default Gateway IP address and select OK.

Command Line Interface

The FortiAnalyzer-2000A has an DB-9 console port. Use the DB-9 cable to connect it to your management computer.

To connect to the FortiAnalyzer unit

1. Use a DB-9 cable to connect the FortiAnalyzer serial port to the management computer serial port.
2. Start a terminal emulation program (such as HyperTerminal) on the management computer. Use these settings: Baud Rate 9600, Data bits 8, Parity None, Stop bits 1, Flow Control None.
3. At the login: prompt, type `admin` and press Enter twice.
(The login prompt is preceded by the server default host name.)

After connecting to the CLI, you can configure the FortiAnalyzer unit IP address, DNS server IP address, and default gateway to connect the FortiAnalyzer unit to the network.

To configure the FortiAnalyzer unit using the CLI

1. Set the IP address and netmask of the Port1 interface.

```
config system interface
    edit port1
        set ip <intf_ip>/<netmask_ip>
    end
```
3. Configure the primary and secondary DNS server IP addresses.

```
config system dns
    set primary <dns-server_ip>
    set secondary <dns-server_ip>
end
```
4. Configure the default gateway.

```
config system route
    edit 1
        set device <interface>
        set dst <destination_ip>
        set gateway <gateway_ip>
    end
```

Adding an administration password

By default, the admin user does not have a password. To restrict access to the FortiAnalyzer unit management account, add password for the admin user account.

To add the admin user account password

1. Go to **System > Admin**.
2. For the admin user, select the Change Password icon.
3. Enter a new password in the New Password box.
4. Reenter the password to Confirm Password box.
5. Select OK.

Adding an administration password using the CLI

To add an administration password in the CLI enter the following commands:

```
config system settings
    edit admin
        set password <password>
    end
```

Shutting down the FortiAnalyzer unit

When powering off the FortiAnalyzer unit, always shut down the unit using the following procedures before disconnecting the power supply. Not following this procedure can increase the risk of damaging the FortiAnalyzer hard disk.

To power off the FortiAnalyzer unit

1. Go to **System > Dashboard**.
2. In the System Operation list, select Shut Down.
3. Select Go.
4. Once the indicates the shut down procedure has completed, disconnect the FortiAnalyzer unit from the power source.

Shutting down the FortiAnalyzer unit using the CLI

Enter the following command at the prompt:

```
execute shutdown
```

6 Completing the Configuration

Congratulations!

You have finished configuring the basic settings. You are ready to add FortiGate devices and collect log information. To explore the full range of configuration options, see the online help or the Tools and Documentation CD-ROM.

Visit these links for more information and documentation for your Fortinet product.

- Technical Documentation - <http://docs.forticare.com>
- Fortinet Knowledge Center - <http://kc.forticare.com>
- Fortinet Technical Support - <http://support.fortinet.com>