



**FortiAnalyzer  
Version 3.0 MR6**

**FORTINET.**

[www.fortinet.com](http://www.fortinet.com)

*FortiAnalyzer Install Guide*  
Version 3.0 MR6  
16 September 2008  
05-30006-0411-20080916

© Copyright 2008 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

#### **Trademarks**

Fortinet, FortiGate and FortiGuard are Registered Trademarks and ABACAS, APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiManager, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

#### **Regulatory compliance**

FCC Class A Part 15 CSA/CUS



**CAUTION:** Risk of Explosion if Battery is replaced by an Incorrect Type.  
Dispose of Used Batteries According to the Instructions.

# Contents

<b>Introduction .....</b>	<b>5</b>
<b>Register your FortiAnalyzer unit .....</b>	<b>5</b>
<b>About this guide .....</b>	<b>5</b>
<b>FortiAnalyzer documentation .....</b>	<b>6</b>
Fortinet Tools and Documentation CD .....	6
Fortinet Knowledge Center .....	6
Comments on Fortinet technical documentation .....	6
<b>Customer service and technical support .....</b>	<b>6</b>
<b>Installing .....</b>	<b>9</b>
<b>Environmental specifications .....</b>	<b>9</b>
Rack mount instructions .....	9
<b>Mounting the FortiAnalyzer-800 and FortiAnalyzer-800B .....</b>	<b>10</b>
<b>Mounting the FortiAnalyzer-1000B .....</b>	<b>10</b>
<b>Mounting the FortiAnalyzer-2000A and FortiAnalyzer-4000A .....</b>	<b>11</b>
Disassembling the slide rail .....	11
Attaching the slide rail to the FortiAnalyzer unit .....	12
Mounting the FortiAnalyzer unit .....	12
<b>Powering on the FortiAnalyzer unit .....</b>	<b>13</b>
Connecting to the network .....	13
<b>Powering off the FortiAnalyzer unit .....</b>	<b>13</b>
Manual shutdown .....	14
<b>Using the FortiAnalyzer-1000B recovery CD .....</b>	<b>14</b>
<b>Configuring .....</b>	<b>15</b>
<b>Connecting to the FortiAnalyzer unit .....</b>	<b>15</b>
Web-based manager .....	15
Command line interface .....	15
Front control buttons and LCD .....	15
<b>Using the web-based manager .....</b>	<b>16</b>
<b>Using the command line interface .....</b>	<b>17</b>
<b>Using the LCD .....</b>	<b>18</b>
<b>Collecting logs .....</b>	<b>19</b>
Adding a FortiGate unit .....	19
Log configuration .....	20
Register the FortiGate unit with FortiAnalyzer .....	20
<b>Further reading .....</b>	<b>21</b>

<b>Advanced FortiAnalyzer applications .....</b>	<b>22</b>
Log Aggregation.....	22
Log forwarding .....	23
<b>Factory defaults.....</b>	<b>24</b>
<b>Firmware .....</b>	<b>27</b>
<b>Backing up the FortiAnalyzer unit .....</b>	<b>27</b>
Backing up the configuration.....	27
Backing up the FortiAnalyzer hard disk .....	27
Restoring the logs .....	28
<b>Using the web-based manager.....</b>	<b>28</b>
Upgrading the firmware.....	28
Downgrading the firmware .....	28
<b>Using the CLI .....</b>	<b>29</b>
Upgrading the firmware.....	29
Downgrading using the CLI.....	30
<b>Installing firmware images from a system reboot using the CLI .....</b>	<b>31</b>
<b>Index.....</b>	<b>35</b>

# Introduction

The FortiAnalyzer is a network appliance that provides reporting, data analysis and integrated log collection tools. Detailed log reports provide historical as well as current analysis of network traffic, such as email, FTP and web browsing activity, to help identify security issues and reduce network misuse and abuse.

The FortiAnalyzer unit provides a selection of reporting tools from detailed reports that can be scheduled or generated on demand, to basic traffic sniffing and real-time network monitoring.

## Register your FortiAnalyzer unit

Before you begin, take the time to register your FortiAnalyzer unit by visiting <http://support.fortinet.com> and select Product Registration.

To register, enter your contact information and the serial numbers of the FortiAnalyzer units that you or your organization have purchased. You can register multiple FortiAnalyzer units in a single session without re-entering your contact information.

By registering your FortiAnalyzer unit will ensure your access to technical support and firmware updates and patches.

## About this guide

This guide describes how to set up, configure and use the FortiAnalyzer unit to collect logs and generate reports on network use.

This guide has the following sections:

- [Installing](#) describes how to set up and install the FortiAnalyzer unit in your network environment.
- [Configuring](#) describes how to configure the FortiAnalyzer system settings, such as system time, and adding FortiGate units.
- [Firmware](#) describes how to upgrade or downgrade the operating system and how to back up the configuration and logs before beginning the procedure.

## FortiAnalyzer documentation

Along with this installation guide, the following documentation is also available.

- *FortiAnalyzer QuickStart Guides*  
Explains how to quickly install and set up the FortiAnalyzer unit.
- *FortiAnalyzer Administration Guide*  
Describes how to configure a FortiAnalyzer unit to collect FortiGate, FortiMail, FortiClient, FortiManager and Syslog log files. It also describes how to view log files, generate and view reports on various network activities, and use the FortiAnalyzer unit in advanced applications including log aggregation.
- *FortiAnalyzer CLI Reference*  
Describes how to use the command line interface of the FortiAnalyzer unit, and describes all the commands available.
- *FortiAnalyzer online help*  
Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.

### Fortinet Tools and Documentation CD

All Fortinet documentation is available from the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

### Fortinet Knowledge Center

The knowledge center contains short how-to articles, FAQs, technical notes, and much more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

### Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

## Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at <http://support.fortinet.com> to learn about the technical support services that Fortinet provides.





# Installing

You can install the FortiAnalyzer unit as a free-standing appliance on any flat, stable surface, providing you adhere to the environmental and air flow specifications outlined below. You can also choose to install the FortiAnalyzer-800 and higher unit in a standard 19-inch rack or cabinet.

The FortiAnalyzer-800, FortiAnalyzer-800B FortiAnalyzer-1000B and requires 1U of vertical space. The FortiAnalyzer-2000/A and FortiAnalyzer-4000/A requires 2U of vertical space.

## Environmental specifications

- Operating temperature: 41 to 95°F (5 to 35°C)  
If you install the FortiAnalyzer unit in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature. Therefore, make sure to install the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature.
- Storage temperature: -4 to 176°F (-20 to 80°C)
- Humidity: 10 to 90% non-condensing
- Air flow - For rack installation, make sure that the amount of air flow required for safe operation of the equipment is not compromised.
- For free-standing installation, make sure that the appliance has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.



**Caution:** Ensure the FortiAnalyzer unit is connected and properly grounded to a lightning and surge protector to a terminal within the building. The equipment is to be connected only without routing to the outside plant.

Do not connect or disconnect cables during lightning activity to avoid damage to the FortiAnalyzer unit or personal injury.

## Rack mount instructions

**Elevated Operating Ambient** - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (T<sub>ma</sub>) specified by the manufacturer.

**Reduced Air Flow** - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

**Mechanical Loading** - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

**Circuit Overloading** - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

**Reliable Earthing** - Reliable earthing of rack-mounted equipment should be maintained.

Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

## Mounting the FortiAnalyzer-800 and FortiAnalyzer-800B

The FortiAnalyzer unit can be placed on any flat surface, or mounted in a standard 19-inch rack unit.

When placing the FortiAnalyzer unit on any flat, stable surface, ensure the unit has adequate clearance on each side to ensure adequate airflow for cooling.

For rack mounting, use the mounting brackets and screws included with the FortiAnalyzer unit.



**Note:** Fortinet recommends purchasing side rail mounts or similar rack mount aids separately to ensure the FortiAnalyzer unit is attached safely to the rack.



**Caution:** To avoid personal injury, you may require two or more people to install the FortiAnalyzer unit in the rack.

### To install the FortiAnalyzer unit into a rack

- 1 Attach the mounting brackets to the side to the unit so that the brackets are on the front portion of the FortiAnalyzer unit if they are not already attached when shipped. Ensure that the screws are tight and not loose.
- 2 Position the FortiAnalyzer unit in the rack to allow for sufficient air flow.
- 3 Line up the mounting bracket holes to the holes on the rack, ensuring the FortiAnalyzer unit is level.
- 4 Finger tighten the screws to attach the FortiAnalyzer unit to the rack.
- 5 Once you verify the spacing of the FortiAnalyzer unit and that it is level, tighten the screws with a screwdriver. Ensure that the screws are tight and not loose.

## Mounting the FortiAnalyzer-1000B

For instructions on mounting the FortiAnalyzer-1000B in a rack mount unit, see the *FortiAnalyzer Rack Install Guide*.

## Mounting the FortiAnalyzer-2000A and FortiAnalyzer-4000A

To mount the FortiAnalyzer unit on a 19 in rack or cabinet, use the slide rails included with the product. The rails enable you to safely pull the FortiAnalyzer units out from the rack to access the back or top of the unit.



**Caution:** To avoid personal injury or damage to the FortiAnalyzer unit, it is highly recommended a minimum of two people perform this procedure.

Mounting requires three steps:

- disassembling the slide rail from the rail housing
- attaching the slide rail to the sides of the FortiAnalyzer unit
- mounting the FortiAnalyzer unit to the rack or cabinet.

### Disassembling the slide rail

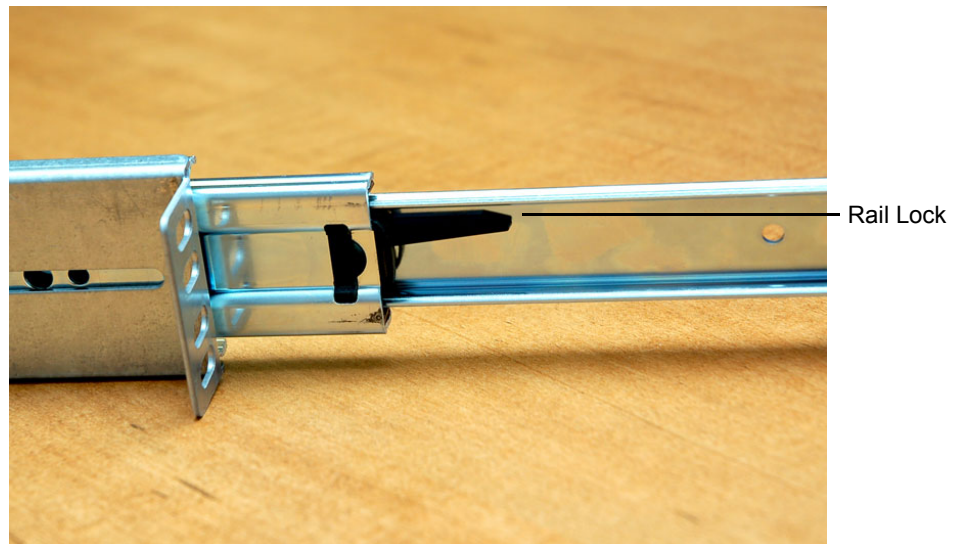
The slide rail assembly has two moving rails within the rail housing. You need to remove the innermost rail. This rail will attach to the sides of the FortiAnalyzer unit.

**Figure 1: FortiAnalyzer side rail**

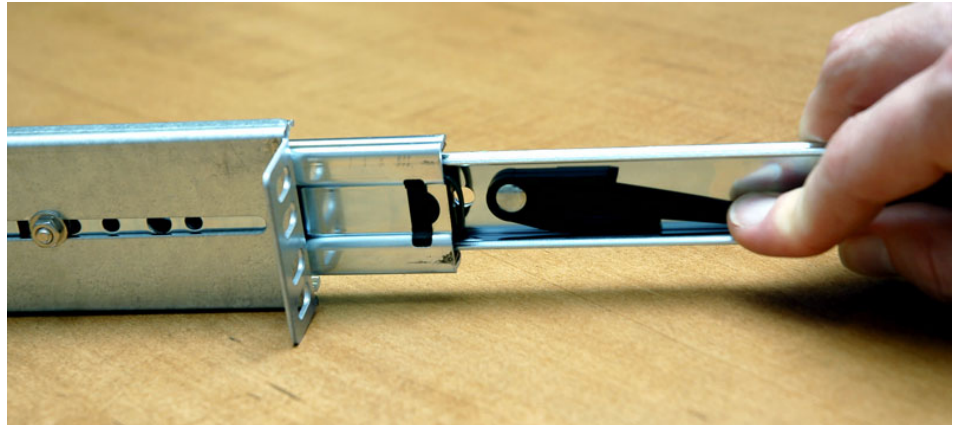


#### To remove the side rail

- 1 Open the slide rails package and remove the rails.
- 2 Extend the slide rail and locate the slide rail lock on the inside of the top sliding rail.



- 3 Pull down on the lock while pulling the rail completely out of the slide rail assembly.



- 4 Repeat these steps for the other slide rail assembly.  
You will attach this part to the side of the FortiAnalyzer unit.

### Attaching the slide rail to the FortiAnalyzer unit

Attach the disconnected slide rails from the previous step to the sides of the FortiAnalyzer unit. Align the holes of the slide rail with the mounting holes on the sides of the FortiAnalyzer unit. Use the screws provided with the slide rail package, being sure to securely fasten the rail to the FortiAnalyzer chassis.



### Mounting the FortiAnalyzer unit

Mounting the FortiAnalyzer-2000A or FortiAnalyzer-4000A is a two step process. First, you must attached the slide rail housing to the rack or cabinet, then insert the FortiAnalyzer unit.

### To mount the FortiAnalyzer unit

- 1 Mount the slide rail housing to the rack or cabinet frame. Adjust the outside L-shaped brackets for a proper fit. Ensure that both housings are level to ensure the FortiAnalyzer unit can easily glide into place and is level.
- 2 Use the screws and additional L-brackets (if required) to securely fasten the housing.
- 3 Position the FortiAnalyzer unit so that the back of the unit is facing the rack or cabinet, and the slide rails affixed in the previous step line up with the slide rail housing.
- 4 Gently push the FortiAnalyzer unit into the rack or cabinet. You will hear a click when the slide rail lock has been engaged.
- 5 Push the FortiAnalyzer unit until it is fully inserted into the rack.

## Powering on the FortiAnalyzer unit

### To power on the FortiAnalyzer unit

- 1 Connect the power cable to the back of the FortiAnalyzer unit.
- 2 Connect the power cable to a power outlet.
- 3 Turn on the power switch on the back of the unit (FortiAnalyzer-400 and FortiAnalyzer-800).

### Connecting to the network

Using the supplied Ethernet cable, connect one end of the cable to your router or switch. Connect the other end to the FortiAnalyzer unit. Connect to port 1.

## Powering off the FortiAnalyzer unit

When powering off the FortiAnalyzer unit, always shut down the unit using the following procedures before disconnecting the power supply. By not following this procedure, you risk damaging the FortiAnalyzer hard disk.

### To power off the FortiAnalyzer unit

- 1 From the web-based manager, go to **System > Dashboard**.
- 2 In the System Operation list, select Shut Down and select Go.  
OR  
from the CLI, enter:  

```
execute shutdown
```
- 3 Disconnect the power supply when the FortiAnalyzer unit indicates it is safe to disconnect the power.

## Manual shutdown

On FortiAnalyzer-400 and FortiAnalyzer-800, units where you must hold the power button for 4 seconds to shut down the unit, you can use the power switch to perform a safe shutdown without using the above steps.

After holding the power button for two seconds, a beep will sound. When you hear the beep, release the power button. The system will perform an orderly shutdown and then power off the system. If you continue to hold the button for four seconds the regular hard power-off will occur, which should be avoided.

## Using the FortiAnalyzer-1000B recovery CD

The CD included with the FortiAnalyzer-1000B is a recovery CD as well as including documentation. Should the FortiAnalyzer become unresponsive, you can use the recovery CD to reset the FortiAnalyzer unit.



**Note:** The FortiAnalyzer unit may take a few minutes to load the CD. There may be a short delay for the following messages to appear on the screen.

### To use the recovery CD

- 1 Connect console cable and power cable to FortiAnalyzer unit.
- 2 Open a terminal window and set the baud rate to 9600.
- 3 Power on the FortiAnalyzer unit.
- 4 Insert the recovery CD into CD-ROM drive of the FortiAnalyzer unit.  
The message “Do you want to recover the FortiBootLoader? (Y/N)” appears.
- 5 Enter `Y` and press enter.

After a few minutes, the message “Please remove the recover CD, press any key to reboot the system” appears.

- 6 Remove recovery CD from CD-ROM and press any key.  
The FortiAnalyzer unit reboots with the recovered system.

# Configuring

The FortiAnalyzer unit ships with a factory default configuration. The default configuration enables you to connect to and use the FortiAnalyzer web-based manager to configure the FortiAnalyzer unit onto the network. To configure the FortiAnalyzer unit onto the network, you add an administrator password, change network interface IP addresses, add DNS server IP addresses, and, if required, configure basic routing.

Once you complete the network configuration, you can perform additional configuration tasks such as setting system time, adding Fortinet devices or user accounts.

## Connecting to the FortiAnalyzer unit

There are three methods of connecting and configuring the basic FortiAnalyzer settings:

- the web-based manager
- the command line interface (CLI)
- the front control buttons and LCD (FortiAnalyzer-400, FortiAnalyzer-800 and FortiAnalyzer-2000)

### Web-based manager

You can configure and manage the FortiAnalyzer unit using HTTP or a secure HTTPS connection from any computer running Microsoft Internet Explorer 6.0 or recent browser.

You can use the web-based manager to configure most FortiAnalyzer settings, and monitor the status of the FortiAnalyzer unit.

### Command line interface

You can access the FortiAnalyzer command line interface (CLI) by connecting a management computer serial port to the FortiAnalyzer serial console connector. You can also use Telnet or an SSH connection to connect to the CLI from any network that is connected to the FortiAnalyzer unit, including the Internet.

### Front control buttons and LCD

You can use the front control buttons and LCD on the FortiAnalyzer-400, FortiAnalyzer-800 and FortiAnalyzer-2000 to configure IP addresses and default gateways and switch operating modes. For more information on the front control buttons and LCD, see [“Front control buttons and LCD” on page 15](#).

## Using the web-based manager

The web-based manager provides a GUI interface to configure and administer the FortiAnalyzer unit.

Use the web-based manager to:

- configure most FortiAnalyzer settings
- monitor the status of the FortiAnalyzer unit
- configure and view reports
- view real-time and historical log messages
- administer users, groups and set access rights.

You can configure and manage the FortiAnalyzer unit using a secure HTTPS connection from any computer running Internet Explorer 6.0 or other current browser.

Configuration changes made using the web-based manager are effective immediately without restarting the FortiAnalyzer unit or interrupting service. For all FortiAnalyzer models, use the following procedure to connect to the web-based manager for the first time.

To connect to the web-based manager, you need:

- an Ethernet connection between the FortiAnalyzer unit and management computer
- Internet Explorer version 6.0 or higher or other current popular web browser on the management computer

### To connect to the web-based manager

- 1 Connect the Port1 interface of the FortiAnalyzer unit to the Ethernet port of the management computer.
- 2 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.
- 3 Configure the management computer to be on the same subnet as the FortiAnalyzer LAN interface.
- 4 To do this, change the IP address of the management computer to 192.168.1.2 and the netmask to 255.255.255.0.
- 5 To access the FortiAnalyzer web-based manager, start your browser and browse to <https://192.168.1.99/> (remember to include the “s” in https://).
- 6 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 the FortiAnalyzer unit using the web-based manager

- 1 In the web-based manager, go to **System > Network > Interface**.
  - 2 Select Edit for Port1.
  - 3 Enter the IP address and netmask and select OK.
- If the FortiAnalyzer unit will be connected to the internet:
- 4 Go to **System > Network > DNS**.

- 5 Enter the, primary DNS server IP address, secondary DNS server IP address (optional).
- 6 Select Apply.
- 7 Got to **System > Network > Routing**.
- 8 Select Create New and add the default gateway IP address and any other routes as required.
- 9 Select OK.

For more configuring options, see the [FortiAnalyzer Administration Guide](#).

## Using the command line interface

You can also use terminal emulation software to connect to the command line interface (CLI) from any network that is connected to the FortiAnalyzer unit, including the Internet. This applies to all FortiAnalyzer models.

For all FortiAnalyzer models except the FortiAnalyzer-400, you can also use the null-modem cable provided to connect to the unit's console port. The FortiAnalyzer-400 does not have a console port.

The CLI supports the same configuration as the web-based manager. You cannot use the CLI to view log data or reports.

### To connect to the FortiAnalyzer unit through the console

- 1 Use a null-modem cable to connect the serial port.
- 2 Start a terminal emulation program (such as HyperTerminal) on the management computer. Use these settings:
  - Baud Rate (bps) 9600
  - Data bits 8
  - Parity None
  - Stop bits 1
  - Flow Control None.
- 3 At the `login:` prompt, type `admin` and press Enter.

After connecting to the CLI, you can configure the 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 LAN interface:

```
config system interface
  edit port1
    set ip <ip_address><netmask>
  end
```

- 2 Confirm that the address is correct:

```
get system interface
```

- 3 Set the primary and optionally the secondary DNS server IP address:

```
config system dns
  set primary <dns-server_ip>
  set secondary <dns-server_ip>
end
```

- 4 Set the default gateway:

```
config system route
  edit 1
  set device port1
  set dst <destination_ip><netmask>
  set gateway <gateway_ip>
end
```

For more configuring options, see the [FortiAnalyzer CLI Reference](#).

## Using the LCD

You can use the front panel buttons on the FortiAnalyzer-400 and FortiAnalyzer-800 to set up the unit's IP address, netmask, and default gateway.



Press the cycle button to cycle through options and select the IP address information.



Press the enter button to select a menu option or number in the IP address.

On the FortiAnalyzer-2000, use the up and down arrow buttons to cycle through the options and enter the IP address information, and select Enter to select a menu option or number in the IP address.

### To change the IP address and netmask of an interface

- 1 Press Enter to display the network settings.
- 2 Use the up and down arrows or the cycle button to highlight the name of the interface to change and press Enter.
- 3 Press Enter for IP address.
- 4 Use the up and down arrow keys or cycle button to increase or decrease the value of each IP address digit. Press Enter to move to the next digit. Press Esc to move to the previous digit.
- 5 After you set the last digit of the IP address, press Enter.
- 6 Use the down arrow to highlight Netmask.
- 7 Press Enter and change the Netmask.
- 8 After you set the last digit of the Netmask, press Enter.
- 9 Press Esc to return to the main menu setting.



**Note:** When you enter an IP address, the LCD always shows three digits for each part of the address. For example, the IP address 192.168.100.1 appears on the LCD as 192.168.100.001. The IP address 192.168.23.45 appears as 192.168.023.045.

**To add a default gateway to an interface**

- 1 Press Enter to display the network settings.
- 2 Use the down arrow or cycle button to select Default Gateway.
- 3 Press Enter and set the default gateway.
- 4 After you set the last digit of the default gateway, press Enter.
- 5 Press Esc to return to the main menu setting.

## Collecting logs

The power of FortiAnalyzer units centers on reporting and network analysis capability collated from log data. The FortiAnalyzer unit can collect log messages from multiple FortiGate, FortiManager, FortiClient and FortiMail devices and Syslog servers, to enable you to generate many different report types from that log data.

This section describes how to configure the FortiAnalyzer unit and a FortiGate unit for log collection. For information on collecting log data from other Fortinet products, see the [FortiAnalyzer Administration Guide](#).

### Adding a FortiGate unit

A FortiGate unit must be configured to send log messages to a FortiAnalyzer unit. This configuration can occur before or after the FortiAnalyzer unit's configuration to receive those logs.

The steps to add a device vary according to the log settings you want, and to a FortiAnalyzer unit's configured response to an initial log connection attempt. For details, see "Unregistered Device Options" in the [FortiAnalyzer Administration Guide](#).

The following procedure uses the default options and configures the FortiGate unit first.



**Note:** Due to the nature of connectivity for certain HA modes, full content archiving and quarantining may not be available for FortiGate units in an HA cluster. For details, see the [FortiGate HA Overview](#).

**To send FortiGate unit logs to a FortiAnalyzer unit**

- 1 On the FortiGate unit, go to **Log&Report > Log Config > Log Setting**.
- 2 Select FortiAnalyzer.
- 3 Select the blue arrow for FortiAnalyzer to expand the options.
- 4 Select a security level to log.
- 5 Select Static IP Address and enter the IP Address of the FortiAnalyzer unit.
- 6 Select Apply.

For more information on the logging options, see the "Log&Report" chapter in the [FortiGate Administration Guide](#).

## Log configuration

You must also configure the FortiGate unit for the kind of data you want the FortiGate to log and send to the FortiAnalyzer unit. There are two main locations for configuring the log types:

- configure the event logs by going to **Log&Report > Log Config > Event Log**.
- enable feature logs by going to **Firewall > Protection Profile**, and editing a profile.

For details on enabling logs, see the [Logging Technical Note](#), available on the Fortinet Knowledge Center (<http://kc.forticare.com>) or the [FortiGate Administration Guide](#).

## Register the FortiGate unit with FortiAnalyzer

Once the FortiGate unit begins sending log data to the FortiAnalyzer unit, the FortiGate unit will appear in the devices list. To complete the connection, configure the device privileges and port assignments for the log data.

### To register a FortiGate unit with a FortiAnalyzer unit

- 1 On the FortiAnalyzer unit, go to **Device > All**.
- 2 If the device is in the device list but is Unregistered, select Unregistered from the Show list, then select Add from the Action column.
- 3 Expand the Devices Privileges settings.
- 4 Set the privileges the FortiGate unit has when sending and viewing log files, archived content and quarantined files.



**Note:** Accessing logs, content logs and quarantined files is available on FortiGate units running firmware version 3.0 or later.

- 5 Expand the Group Membership settings.
- 6 Select the group where you want to include the FortiGate unit, and select the right arrow button to add the FortiGate unit to the group. A FortiGate unit can belong to multiple groups.

You can also add the FortiGate unit to a group later or change the group you assigned.

- 7 Expand the FortiGate Interface Specification settings.
- 8 Define the port interface options using the arrow buttons. For details on port interface settings see [“Defining FortiGate interfaces” on page 20](#).  
If you want to add a VLAN or other interface, type the name of the interface and select Add.
- 9 Select OK.

For more information, see the [FortiAnalyzer Administration Guide](#).

### Defining FortiGate interfaces

FortiAnalyzer network activity reports include information on inbound and outbound traffic flow. Traffic flow information is based on the source and destination interfaces of the device and how they are configured to send and receive information.

To ensure that the traffic information is represented correctly in these reports, you need to assign the FortiGate interfaces to an interface type. The device interface can include an interface name or a defined VLAN on the device.

You can classify the device interfaces as one of None, LAN, WAN or DMZ to match the type of traffic the interface will process. When the FortiAnalyzer unit generates the traffic log report, the FortiAnalyzer unit compares the source and destination interface classifications and determines the directional traffic.

The traffic direction is one of:

- incoming
- outgoing
- unclassified

and the source or destination interface is one of:

- internal
- external

The table below illustrates how the source and destination interface types are represented in the log report as traffic direction.

**Table 1: Log report traffic direction identification**

Source	Destination	Traffic Direction
None	All types	Unclassified
All types	None	Unclassified
WAN	LAN, DMZ	Incoming
WAN	WAN	External
LAN, DMZ	LAN, DMZ	Internal
LAN, DMZ	WAN	Outgoing

## Further reading

The FortiGate unit and FortiAnalyzer unit are now configured to send and receive log information. Using this log collection, you can view traffic, vulnerability statistics and run reports from a selection of over 200 reports in 15 categories.

To help you in further configuration and data analysis, see these other Fortinet documents, available from the Fortinet Knowledge Center (<http://kc.forticare.com>) and the Technical Documentation web site (<http://docs.forticare.com>).

- [FortiAnalyzer Administration Guide](#) includes further configuration and technical information on your FortiAnalyzer unit.
- [FortiGate Administration Guide](#) includes steps for enabling the various logging options and details on the logging levels.
- [FortiGate Logging Technical Note](#) provides details on configuring the logging options for a FortiGate unit and details the various log types.
- [FortiGate Log Message Reference](#), describes what each log messages means and its components.

## Advanced FortiAnalyzer applications

In addition to log collection you can configure the FortiAnalyzer unit for the following advanced configurations. These configurations enable you to use the FortiAnalyzer unit as a log aggregation tool as a centralized log storage repository, or as a means of backing up log data for redundancy.

### Log Aggregation

Log aggregation is a method of collating log data from remote FortiAnalyzer units to a central FortiAnalyzer unit.

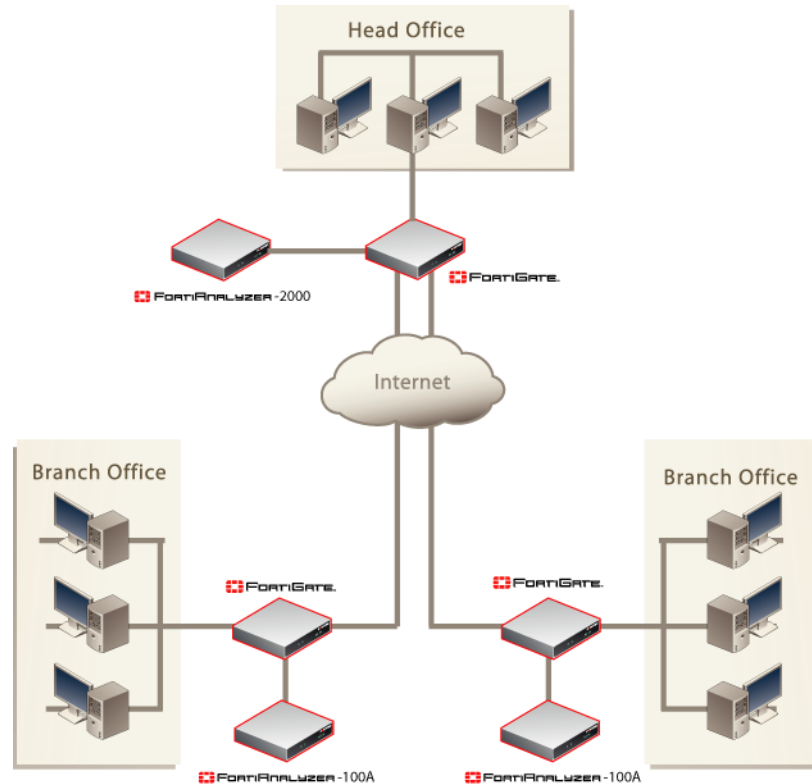
For example, a company may have a headquarters and a number of branch offices. Each branch office has a FortiGate unit and a FortiAnalyzer-100A/100B to collect local log information. The headquarters has a FortiAnalyzer-2000/2000A as the central log aggregator.

You can also use the FortiAnalyzer unit to aggregate logs for third party network devices or server/work stations that supports syslog log messaging.

Log aggregation is supported on selected FortiAnalyzer units due to storage and resource requirements. See the table below to determine what unit supports client and server aggregation:

FortiAnalyzer Model	Aggregation Client	Aggregation Server
FortiAnalyzer-100A/100B	Yes	No
FortiAnalyzer-400	Yes	No
FortiAnalyzer-800	Yes	Yes
FortiAnalyzer-2000/2000A	Yes	Yes
FortiAnalyzer-4000/4000A	Yes	Yes

Figure 2: Log aggregation diagram



Log aggregation enables the branch office FortiAnalyzer units to send or upload their logs at regular intervals to the headquarter FortiAnalyzer unit. This provides a central storage location as well as a method of running reports that include data from all branch offices in a single report.

Log aggregation involves an aggregation client (branch office) and an aggregation server (headquarters). The aggregation client sends all log information for the registered devices using SSH on port 22. This does not include quarantined files. It does include the active log to the point of aggregation (tlog.log for example) and all rolled logs available on the client hard disk (tlog.1.log, tlog.2.log, etc.). Subsequent log uploads will only include the most recent updates. The FortiAnalyzer unit will not re-send all logs again.

For more information and configuring details, see the [FortiAnalyzer Administration Guide](#).

## Log forwarding

Log forwarding replicates log messages in real-time to an external syslog server as they are received by the FortiAnalyzer unit.

This can be useful for additional log storage or processing.

The log forwarding destination (Remote device IP) may receive either a full duplicate or a subset of the FortiAnalyzer's received log messages. Log messages are forwarded only if they meet or exceed the Minimum Severity threshold.

Log forwarding is similar to log uploading or log aggregation, but log forwards are sent as real-time syslog messages, not whole files over FTP, SFTP, or SCP, and not as syslog batches.

For more information and configuring details, see the [FortiAnalyzer Administration Guide](#).

## Factory defaults

The following tables are the default settings for the FortiAnalyzer for your reference.

**Table 2: FortiAnalyzer-100A and FortiAnalyzer-100B factory defaults**

<b>Administrator account</b>	User name:	admin
	Password:	(none)
<b>Port 1</b>	IP:	192.168.1.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 2</b>	IP:	192.168.2.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 3</b>	IP:	192.168.3.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 4</b>	IP:	192.168.4.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH

**Table 3: FortiAnalyzer-400 factory defaults**

<b>Administrator account</b>	User name:	admin
	Password:	(none)
<b>Port 1</b>	IP:	192.168.1.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 2</b>	IP:	192.168.2.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 3</b>	IP:	192.168.3.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH

**Table 4: FortiAnalyzer-800 factory defaults**

<b>Administrator account</b>	User name:	admin
	Password:	(none)
<b>Port 1</b>	IP:	192.168.1.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 2</b>	IP:	192.168.2.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 3</b>	IP:	192.168.3.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 4</b>	IP:	192.168.4.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH

**Table 5: FortiAnalyzer-800B factory defaults**

<b>Administrator account</b>	User name:	admin
	Password:	(none)
<b>Port 1</b>	IP:	192.168.1.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 2</b>	IP:	192.168.2.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 3</b>	IP:	192.168.3.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 4</b>	IP:	192.168.4.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH

**Table 6: FortiAnalyzer-2000/2000A factory defaults**

<b>Administrator account</b>	User name:	admin
	Password:	(none)
<b>Port 1</b>	IP:	192.168.1.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 2</b>	IP:	192.168.2.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 3</b>	IP:	192.168.3.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 4</b>	IP:	192.168.4.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH

**Table 7: FortiAnalyzer-4000/4000A factory defaults**

<b>Administrator account</b>	User name:	admin
	Password:	(none)
<b>Port 1</b>	IP:	192.168.1.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH
<b>Port 2</b>	IP:	192.168.2.99
	Netmask:	255.255.255.0
	Management Access:	HTTP, HTTPS, PING, SSH

# Firmware

Fortinet periodically updates the FortiAnalyzer firmware to include enhancements and address issues. After you have registered your FortiAnalyzer unit, FortiAnalyzer firmware is available for download at [http:// support.fortinet.com](http://support.fortinet.com).

Only the FortiAnalyzer administrators, whose access profiles contain system configuration read and write privileges, and the FortiAnalyzer admin user can change the FortiAnalyzer firmware.

## Backing up the FortiAnalyzer unit

Before upgrading the FortiAnalyzer firmware, it is good practice to backup your configuration information and logs stored on the hard disk in the event something goes wrong during the upgrade.

### Backing up the configuration

Backup the FortiAnalyzer configuration to a local PC using the web-based manager or to a FTP server using the CLI.

#### To back up the configuration using the web-based manager

- 1 Go to **System > Maintenance > Backup & Restore**.
- 2 Select Encrypt if you want a secure configuration file or to save the passwords included in the configuration.
- 3 Select Backup and select a location to store the configuration file.

To back up the configuration using the CLI, enter the following command:

```
execute backup config <filename> <IP_address> <password>
```

where IP address is the FTP server where you are saving the configuration file, and password is optional.

For example:

```
execute backup config faz_config.txt 10.10.10.15
```

### Backing up the FortiAnalyzer hard disk

Before upgrading the FortiAnalyzer firmware, it is extremely important that you back up the log data first. Using the CLI, you can perform a global backup of all log information to an FTP server.

To backup the log information on the FortiAnalyzer hard disk, use the CLI to enter the following command:

```
execute backup logs <device_name> <ftp_ip_address>  
<ftp_username> <ftp_password> <ftp_dir>
```

## Restoring the logs

Once you complete the firmware upgrade, you can restore the log information to the FortiAnalyzer hard disk.



**Note:** Before using the restore CLI command, ensure you add the FortiGate units for the logs first. The command will not function without the devices to associate with the logs. For details on adding a FortiGate unit, see the chapter “Adding a FortiGate unit” on page 19.

```
execute restore logs <device> <ftp_ip_address>
<ftp_username> <ftp_password> <ftp_dir>
```

## Using the web-based manager

The web-based manager provides an easy to use method of upgrading or downgrading the firmware on the FortiAnalyzer unit.

### Upgrading the firmware



**Note:** To use this procedure, you must log in using the admin administrator account, or an administrator account that has system configuration read and write privileges.

#### To upgrade the firmware

- 1 Download the firmware image file to your management computer.
- 2 Log into the web-based manager as the admin administrative user.
- 3 Go to **System > Dashboard**.
- 4 Under **System Information > Firmware Version**, select Update.
- 5 Type the path and file name of the firmware image file, or select Browse and locate the file.
- 6 Select OK.

The FortiAnalyzer unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiAnalyzer login. This process takes a few minutes.

- 7 Log into the web-based manager.
- 8 Go to **System > Dashboard** and verify the Firmware Version to confirm the firmware upgrade was installed successfully.

### Downgrading the firmware

The following procedures install an older version of the firmware and reverts the FortiAnalyzer unit to its factory default configuration.

Before beginning this procedure, it is recommended that you:

- back up the FortiAnalyzer unit configuration
- back up the logs on the hard disk.



**Note:** To use this procedure, you must log in using the admin administrator account, or an administrator account that has system configuration read and write privileges.

**To revert to a previous firmware version**

- 1 Download the firmware image file to the management computer.
- 2 Log into the FortiAnalyzer web-based manager.
- 3 Go to **System > Dashboard**.
- 4 Under **System Information > Firmware Version**, select Update.
- 5 Type the path and file name of the firmware image file, or select Browse and locate the file.
- 6 Select OK.

The FortiAnalyzer unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiAnalyzer login. This process takes a few minutes.

- 7 Log into the web-based manager.
- 8 Go to **System > Dashboard** and check the Firmware Version to confirm that the firmware is successfully installed.
- 9 Restore your configuration and log data.

## Using the CLI

The CLI provides an easy to use method of upgrading or downgrading the firmware on the FortiAnalyzer unit.

### Upgrading the firmware

To use the following procedure, you must have a TFTP server the FortiAnalyzer unit can connect to.



**Note:** To use this procedure, you must log in using the admin administrator account, or an administrator account that has system configuration read and write privileges.

#### To upgrade the firmware using the CLI

- 1 Make sure the TFTP server is running.
- 2 Copy the new firmware image file to the root directory of the TFTP server.
- 3 Log into the CLI.
- 4 Make sure the FortiAnalyzer unit can connect to the TFTP server.

You can use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

```
execute ping 192.168.1.168
```

- 5 Enter the following command to copy the firmware image from the TFTP server to the FortiAnalyzer unit:

```
execute restore image <name_str> <tftp_ip>
```

Where `<name_str>` is the name of the firmware image file and `<tftp_ip>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server is `192.168.1.168`, enter:

```
execute restore image.out 192.168.1.168
```

The FortiAnalyzer unit responds with the message:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

6 Type `y`.

The FortiAnalyzer unit uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.

7 Reconnect to the CLI.

8 To confirm the new firmware image is successfully installed, enter:

```
get system status
```

## Downgrading using the CLI

This procedure reverts the FortiAnalyzer unit to its factory default configuration and deletes IPS custom signatures, web content lists, email filtering lists, and changes to replacement messages.

Before beginning this procedure you should:

- back up the FortiAnalyzer unit system configuration
- back up the logs on the hard disk



**Note:** To use this procedure, you must log in using the admin administrator account, or an administrator account that has system configuration read and write privileges.

To use the following procedure, you must have a TFTP server the FortiAnalyzer unit can connect to.

### To revert to a previous firmware version using the CLI

- 1 Make sure the TFTP server is running.
- 2 Copy the firmware image file to the root directory of the TFTP server.
- 3 Log into the FortiAnalyzer CLI.
- 4 Make sure the FortiAnalyzer unit can connect to the TFTP server.

You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is `192.168.1.168`:

```
execute ping 192.168.1.168
```

- 5 Enter the following command to copy the firmware image from the TFTP server to the FortiAnalyzer unit:

```
execute restore image <name_str> <tftp_ip>
```

Where `<name_str>` is the name of the firmware image file and `<tftp_ip>` is the IP address of the TFTP server. For example, if the firmware image file name is `old_image.com` and the IP address of the TFTP server is `192.168.1.168`, enter:

```
execute restore old_image.out 192.168.1.168
```

The FortiAnalyzer unit responds with the message:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

**6** Type `y`.

The FortiAnalyzer unit uploads the firmware image file. After the file uploads, a message similar to the following is displayed:

```
Get image from tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

**7** Type `y`.

The FortiAnalyzer unit reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.

**8** Reconnect to the CLI.

**9** To confirm the new firmware image has been loaded, enter:

```
get system status
```

**10** To restore your previous configuration use the command:

```
execute restore config <name_str> <tftp_ipv4>
```

## Installing firmware images from a system reboot using the CLI

This procedure installs a specified firmware image and resets the FortiAnalyzer unit to default settings. You can use this procedure to upgrade to a new firmware version, revert to an older firmware version, or re-install the current firmware version.

To use this procedure, you must connect to the CLI using the FortiAnalyzer console port and a RJ-45 to DB-9 or null-modem cable. This procedure reverts the FortiAnalyzer unit to its factory default configuration.



**Note:** This procedure will not work with a FortiAnalyzer-400 because it does not have a console port.

For this procedure you:

- Access the CLI by connecting to the FortiAnalyzer console port using a null-modem cable.
- Install a TFTP server that you can connect to from the FortiAnalyzer interface. The TFTP server should be on the same subnet as the internal interface.

Before beginning this procedure you can:

- back up the FortiAnalyzer unit configuration
- back up the log data on the hard disk

**To install firmware from a system reboot**

- 1 Connect to the CLI using the null-modem or RJ-45 to DB9 cable and FortiAnalyzer console port.
- 2 Make sure the TFTP server is running.
- 3 Copy the new firmware image file to the root directory of the TFTP server.
- 4 Make sure the internal interface is connected to the same network as the TFTP server.
- 5 Enter the following command to restart the FortiGate unit:

```
execute reboot
```

The FortiAnalyzer unit responds with the following message:

```
This operation will reboot the system !
Do you want to continue? (y/n)
```

- 6 Type `y`.

As the FortiAnalyzer units starts, a series of system startup messages is displayed.

When one of the following messages appears:

```
Press any key to display configuration menu.....
```

Immediately press any key to interrupt the system startup.



**Note:** You have only 3 seconds to press any key. If you do not press a key soon enough, the FortiGate unit reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, one of the following messages appears:

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default
[C]: Configuration and information
[Q]: Quit menu and continue to boot with default
firmware.
[H]: Display this list of options.
```

```
Enter G,F,B,C,Q, or H:
```

- 7 Type `G` to get the new firmware image from the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```

- 8 Type the address of the TFTP server and press `Enter`.

The following message appears:

```
Enter Local Address [192.168.1.188]:
```

- 9 Type an IP address that can be used by the FortiAnalyzer unit to connect to the FTP server.

The IP address can be any IP address that is valid for the network the interface is connected to. Make sure you do not enter the IP address of another device on this network.

The following message appears:

```
Enter File Name [image.out]:
```

- 10 Enter the firmware image file name and press Enter.

The TFTP server uploads the firmware image file to the FortiAnalyzer unit and messages similar to the following are displayed:

```
Save as Default firmware/Run image without saving:[D/R]
```

- 11 Type D.

The FortiAnalyzer unit installs the new firmware image and restarts. The installation might take a few minutes to complete.



# Index

## A

- ackup 27
- Adding a FortiGate unit 19
- air flow 9
- ambient temperature 9

## B

- backup 27

## C

- CLI 16
  - connecting 17
- command line interface 16, 17
- configuration backup 27
- configuring
  - LCD 18
- connecting
  - to the CLI 17
  - to the web-based manager 16

## D

- defaults 24
- define device port interfaces 20
- downgrade firmware 28

## E

- environmental specifications 9

## F

- factory defaults 24
- firmware
  - downgrade 28
  - installing 31
  - re-installing current version 31
  - reverting to an older version 31
  - upgrade 28
- firmware updates 27
- FortiAnalyzer
  - specs 9
- FortiGate
  - port interfaces 20
  - registering 19
- FortiGate unit
  - groups 20
  - registering 20
- further reading 21

## G

- groups

- FortiGate unit 20

## H

- humidity 9

## I

- installing slide rails 11

## K

- Knowledge Center 6

## L

- LCD 18
- log
  - aggregation 22
  - forwarding 23
- logs
  - backup 27
  - configuring 20
  - restore 27

## M

- mounting 11

## N

- null modem 17

## O

- operating temperature 9

## P

- port
  - interfaces 20
- powering
  - off 13
  - on 13

## R

- recovery CD 14
- Register a FortiGate unit 20
- registering the FortiAnalyzer unit 5
- restore 27
- reverting, to an older firmware version 31

## S

- shut down 13
- slide rails 11
- specifications

environmental 9  
FortiAnalyzer 9

## T

Technical Support 6  
terminal settings 17  
traffic  
  flow on a FortiGate unit 20  
turning  
  off 13  
  on 13

## U

updating firmware 27  
upgrade  
  firmware 28

## W

web-based manager 16  
  connecting 16

**FORTINET.**

[www.fortinet.com](http://www.fortinet.com)

**FORTINET.**

[www.fortinet.com](http://www.fortinet.com)