



FortiExplorer User Guide

for FortiOS 4.0 MR3



FortiExplorer User Guide

v3

16 November 2011

01-430-147724-20111116

© Copyright 2011 Fortinet, Inc. All rights reserved. Contents and terms are subject to change by Fortinet without prior notice. Reproduction or transmission of this publication is encouraged.

Trademarks

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Visit these links for more information and documentation for your Fortinet products:

Fortinet Knowledge Base - <http://kb.fortinet.com>

Technical Documentation - <http://docs.fortinet.com>

Training Services - <http://campus.training.fortinet.com>

Technical Support - <http://support.fortinet.com>

You can report errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.



Contents

Introduction	5
Before you begin	5
How this guide is organized	5
Installing FortiExplorer	7
Overview	7
Installing FortiExplorer	8
Configuring basic device settings and registering your device	9
Configuring a device’s basic settings using Setup Wizard.	9
Registering your device from FortiExplorer	10
Connecting to the device’s web-based manager and CLI	11
Connecting to the web-based manager	11
Connecting to the CLI	12
Configuring additional settings using FortiExplorer	15
Adding and removing devices	15
Checking for firmware updates.	15
Checking for FortiExplorer updates	15
Upgrading or downgrading device firmware	17
Backing up the configuration file on the device	17
Upgrading firmware on the device	18
Downgrading firmware on the device	18
Appendix	19
Document conventions.	19
IP addresses	19
Example Network configuration	21
Cautions, Notes and Tips	22
Typographical conventions	22
CLI command syntax conventions.	22
Entering FortiOS configuration data	24
Entering text strings (names).	24
Entering numeric values	25
Selecting options from a list	25
Enabling or disabling options	25

Registering your Fortinet product 25

Fortinet products End User License Agreement 25

Training 26

Documentation 26

 Fortinet Tools and Documentation CD. 26

 Fortinet Knowledge Base 26

 Comments on Fortinet technical documentation 26

Customer service and technical support. 26

Index **27**



Introduction

Welcome and thank you for selecting Fortinet products for your network protection. This document explains what is FortiExplorer and what it can do for you when you are first setting up your FortiGate-60C or FortiWiFi-60C series product or after they are up and running as a means of managing them. FortiExplorer is software, similar to the Setup Wizard in the web-based manager, that allows you to configure basic settings so that you can quickly get the FortiGate unit or FortiWiFi-60C series product up and running on the network.

This chapter contains the following topics:

- [Before you begin](#)



In latest FortiExplorer release, which was release with the FortiOS 4.0 MR3 patch release 3, FortiExplorer is available for FortiGate-20C, 40C, 1000C, and 600C models and on the FortiWiFi-40C model.

Before you begin

Before you begin using this guide, please ensure that:

- Your PC or Mac meets the required OS version for running FortiExplorer:
 - Mac OS X 10.6 or later
 - Windows XP, Vista or 7
- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.
- FortiGuard Analysis & Management Service is properly configured.

While using the instructions in this guide, note that administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

How this guide is organized

This document contains the following sections:

- [Installing FortiExplorer](#) explains how to install FortiExplorer on your computer and provides procedures for installing on either Windows or Mac OS.
- [Configuring basic device settings and registering your device](#) explains how to configure the basic settings using FortiExplorer's Setup Wizard, as well as how to register the device from within FortiExplorer.
- [Connecting to the device's web-based manager and CLI](#) explains how you can connect to either the device's web-based manager or CLI.

- [Configuring additional settings using FortiExplorer](#) explains how to check for firmware updates for your device, check for firmware updates for FortiExplorer, and how to remove or add a device in the Saved Devices list.
- [Upgrading or downgrading device firmware](#) explains how to properly back up your current configuration and then upgrade or downgrade the device's firmware from within FortiExplorer.




Installing FortiExplorer

This section explains what FortiExplorer is and how FortiExplorer can help you install the FortiGate-60C or FortiWiFi-60C series products into your network. FortiExplorer is software, similar to the Setup Wizard in the web-based manager, that allows you to configure basic settings so that you can quickly get the FortiGate-60C or FortiWiFi-60C series product up and running on the network.

The following topics are included in this section:

- [Overview](#)
- [Installing FortiExplorer](#)

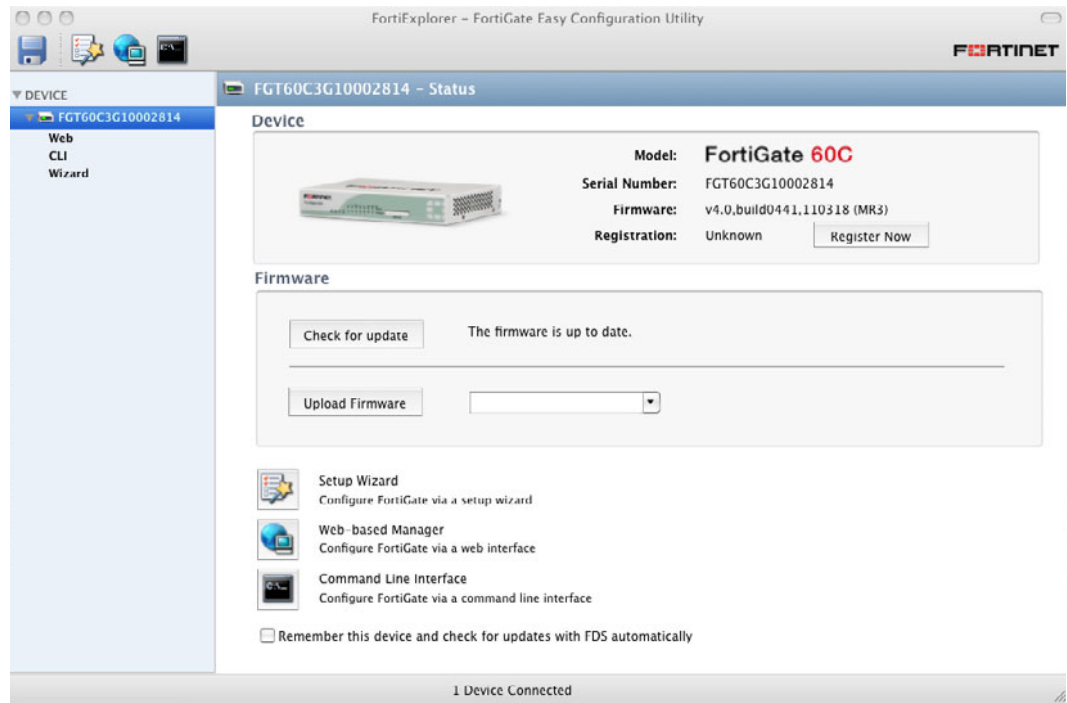


In latest FortiExplorer release, which was released with the FortiOS 4.0 MR3 patch release 3, FortiExplorer is available for FortiGate-20C, 40C, 1000C, and 600C models and on the FortiWiFi-40C model.

Overview

FortiExplorer is a user-friendly connection and configuration tool that helps you to quickly and easily set up your device regardless of your level of network experience.

Figure 1: FortiExplorer’s Status page and icons



You can easily download and install FortiExplorer from the [FortiExplorer Download](#) page from your computer. FortiExplorer also comes on the CD that is shipped with the FortiGate-60C or FortiWiFi-60C series products. FortiExplorer is available for both Windows and Mac OS.

FortiExplorer not only helps you to set up basic configurations, but can also help you:

- register your device
- check for updates for your device and FortiExplorer
- upgrade or downgrade the firmware on your device
- configure settings for your device using either the CLI or web-based manager

Installing FortiExplorer

When using FortiExplorer for the first time, ensure that the device is in its default settings. If the unit needs to be reverted to default settings, insert a pin or paper clip into the Reset button for a few seconds. The device may take a few minutes to reboot.

To install FortiExplorer on Windows using the software CD

- 1 Insert the software CD included in to your computer.
- 2 Select one of the following to install:
 - For Microsoft Windows XP, select FortiExplorer for Microsoft Windows XP.
 - For Microsoft Windows Vista and 7, select FortiExplorer for Microsoft Windows Vista and Windows 7.
- 3 After the installation finishes, connect the USB A cable end to your computer and connect the other end of the cable (USB B) to the USB MGMT port of the unit.
- 4 The New Hardware Wizard opens first, once the unit is connected to your computer and the USB cable. Do the following:
 - Select the option, “No not at this time” and then select *Next*.
 - Select “Install the hardware automatically” and then select *Next*. The New Hardware Wizard installs the hardware and then FortiExplorer opens.

To install FortiExplorer on Mac OS

- 1 Go to the [FortiExplorer Download](#) page on the support web site.
- 2 On the FortiExplorer Download page, select *Mac Download* and save the file to your computer.
- 3 Locate the file on your computer and open it.
- 4 Select the FortiExplorer disk icon on your desktop, and when it opens, drag the FortiExplorer.app file to the Applications folder.

You can install FortiExplorer on a PC running Windows using the above procedure. Instead of selecting *Mac Download*, select *Windows Download*.



Configuring basic device settings and registering your device

This section explains how to configure basic device settings using FortiExplorer's Setup Wizard. The Setup Wizard is similar to the Setup Wizard that is available on all FortiGate products. This section also explains how to register your FortiGate unit after you have configured basic settings on your device.

The following topics are included in this section:

- [Configuring a device's basic settings using Setup Wizard](#)
- [Registering your device from FortiExplorer](#)

Configuring a device's basic settings using Setup Wizard

The FortiExplorer Setup Wizard helps you to set up basic FortiGate or FortiWiFi configuration settings. When you select *Setup Wizard*, each basic configuration step is clearly laid out and if you need to go back to a previous step, you can with the *Back* option. The Setup Wizard helps you to configure:

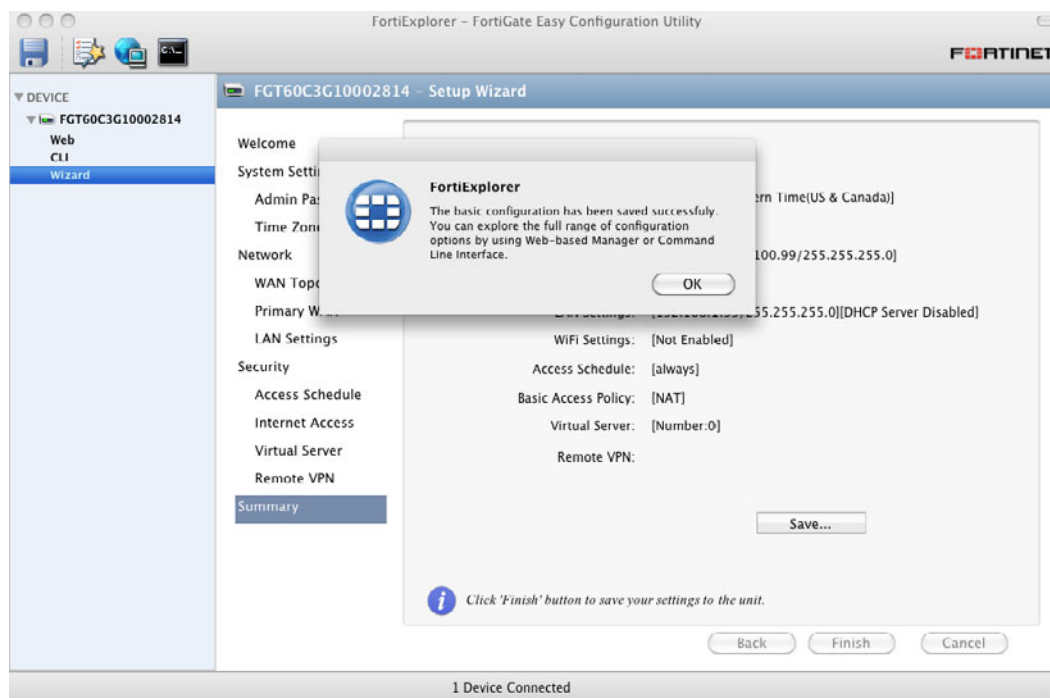
- an administrator password
- time zone
- WAN and LAN settings
- Internet access
- an access schedule
- a virtual server or remote VPN

After completing all of the steps, you can review your device's new settings from the Summary page. The summary page helps you to verify the settings to make sure that everything is correct before updating your device with the new configuration.

To configure basic settings on your FortiGate unit using the Setup Wizard

- 1 Select *Wizard* in the *DEVICE* list.
The login page of the Setup Wizard appears.
- 2 Log in to the wizard using the default admin settings.
The default admin settings are admin and there is no password. After entering the default admin settings, the Welcome to the FortiGate Setup Wizard page appears. You must select *Next* to continue.
- 3 In the *Admin Password* step, enter the new password and then select *Next*.
- 4 To continue on, select *Next* to go to each step.
- 5 When you are at the last step, *Summary*, select *Save* to save the configuration settings to your computer.
The new configuration is saved to the device.

Figure 1: The Summary page within the Setup Wizard, after saving the basic configuration file



Registering your device from FortiExplorer

You can use FortiExplorer to quickly register your device. By registering the device, you can receive updates to threat detection and prevention databases (including Antivirus and Intrusion Detection) and you have access to Fortinet technical support.

There are two ways to register the device: by selecting *Register Now* on the Status page in the FortiExplorer window, or by logging in to your device’s web-based manager, where a window appears and asks if you want to register your device. Follow the steps that appear within the window to complete the registration process.



Connecting to the device's web-based manager and CLI

After installing and setting up the basic settings for your device, you can connect to the device's web-based manager and CLI.

The following topics are included in this section:

- [Connecting to the web-based manager](#)
- [Connecting to the CLI](#)

Connecting to the web-based manager

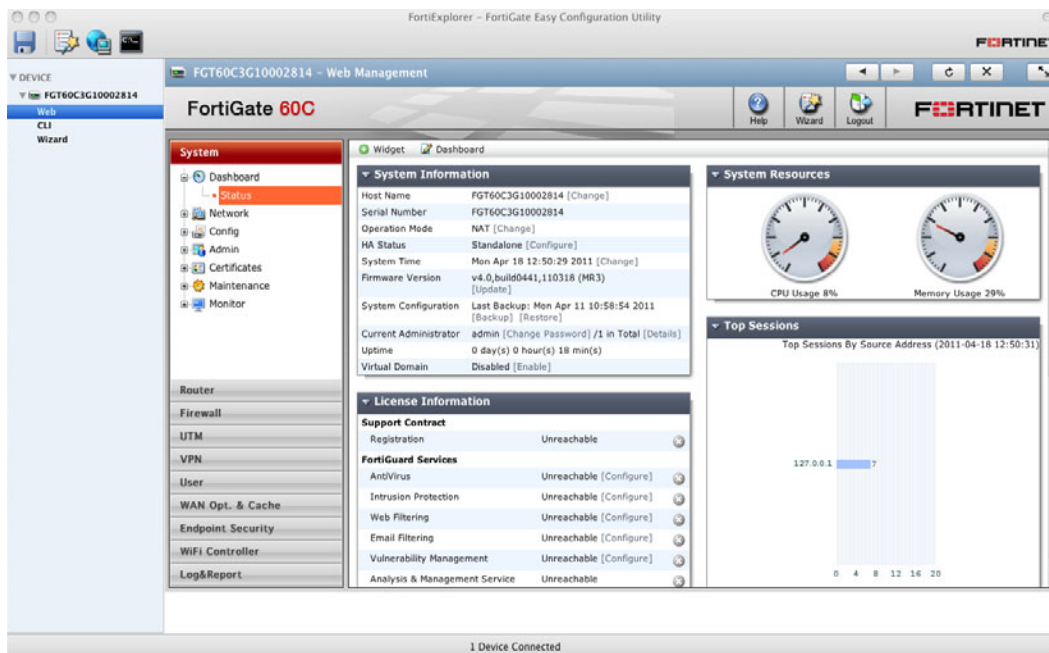
The web-based manager is a user-friendly interface for configuring settings as well as managing your device. Accessing the web-based manager is easy; to use the web-based manager interface, select *Web*, and then log in using your administrator user name and password. After logging in to the web-based manager, you can use the menus, lists and pages to configure most settings.

Configuration changes made within the web-based manager take effect immediately, without resetting the device or interrupting service.

When accessing the web-based manager from within FortiExplorer, you can also access detailed context-sensitive online help that displays for the current web-based manager page.

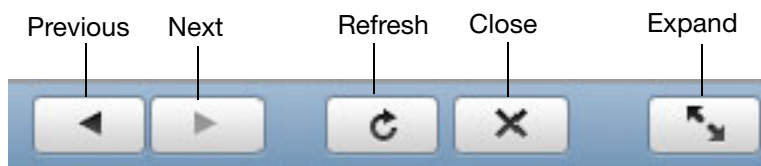
To use the web-based manager from FortiExplorer, select *Web*. Log in to the web-based manager to start configuring settings.

Figure 1: The web-based manager as it appears when accessed in FortiExplorer



When using the web-based manager in the FortiExplorer window, you can see five icons at the top of the page. These icons help you to navigate through the web-based manager. You can also use *Expand* to open the web-based manager in a web browser on your computer.

Figure 2: The five icons that appear above the web-based manager in the FortiExplorer window



Connecting to the CLI

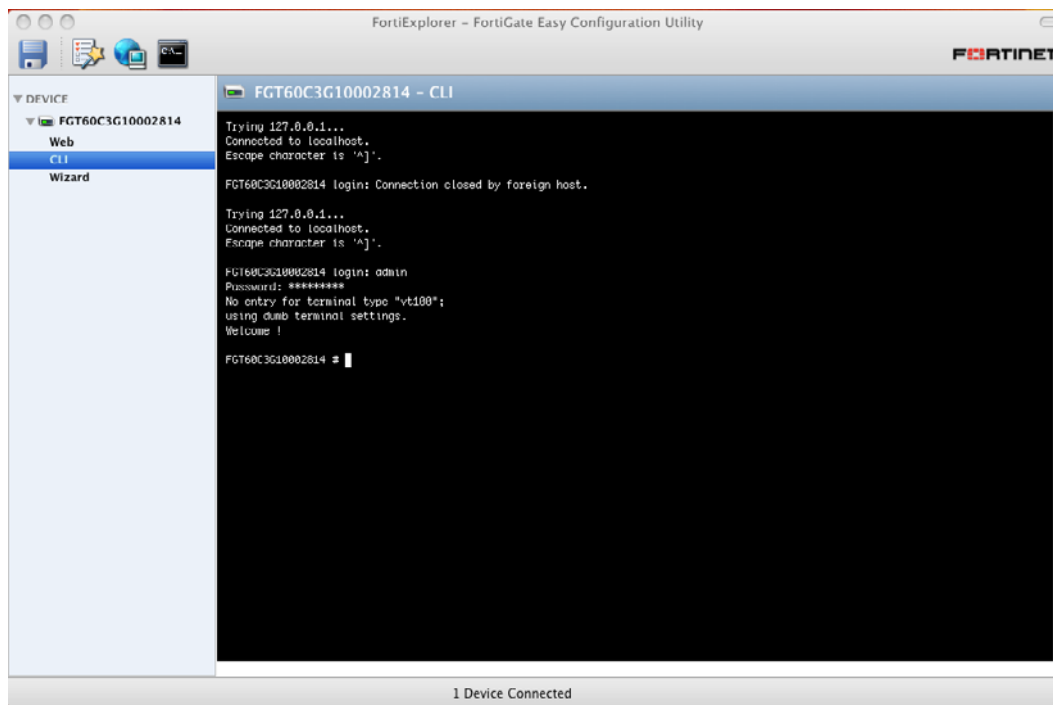
The command line interface (CLI) is an alternative method of configuring the FortiGate unit. The CLI complements the web-based manager in that it not only has the same configuration options, but additional settings not available through the web-based manager.

The CLI contains commands and sub-commands that are used to configure a feature's settings, and you can upload batches of commands from a text file. For example, a configuration script to help you configure a setting or settings.

You should review the [FortiGate CLI Reference](#) before connecting to the CLI so that you are familiar with the command tree structure in the CLI.

To use the CLI from FortiExplorer, select CLI. Log in to the CLI to start configuring settings.

Figure 3: The CLI as it appears when accessed in FortiExplorer





Configuring additional settings using FortiExplorer

There are other settings that you can configure within FortiExplorer that are not web-based manager or CLI-specific. These settings can help you to add or remove devices, check for firmware updates for devices, or check for firmware updates for FortiExplorer.

The following topics are included in this section:

- [Adding and removing devices](#)
- [Checking for firmware updates](#)
- [Checking for FortiExplorer updates](#)

Adding and removing devices

You can add or remove devices from the Saved Devices list, located on the Saved Devices page. If you delete a device in the Saved Devices list, the device is permanently removed.

To add a device to the Saved Devices list

- 1 On the device's Status page, select the check box beside *Remember this device and check for updates with FDS automatically*.
- 2 In the Firmware section of the page, select *Check for update*.
FortiExplorer checks for firmware updates for the device and then automatically adds the devices to the Saved Devices list.

Checking for firmware updates

You can easily and quickly check to see if any device within the Saved Devices list needs its firmware updated. The update results appear in the Saved Devices list only when you select the check box beside *Remember this device and check for updates with FDS automatically*.

To check for firmware updates

- 1 In the Saved Devices list, select the row that contains the unit that you want to check for new firmware.
- 2 Select *Check for update*.
- 3 In the *Check Result* column, the result appears.

Checking for FortiExplorer updates

In a similar way to checking a device for firmware updates, you can check to see if FortiExplorer requires an update to its software.

To check for FortiExplorer updates

- 1** Select *FortiExplorer > Check for Updates*.
FortiExplorer checks for updates. This may take a few minutes.
- 2** If the check finds that FortiExplorer's software needs to be updated, go ahead and update the software.



Upgrading or downgrading device firmware

This section explains how to properly upgrade or downgrade your device using FortiExplorer.

The following topics are included in this section:

- [Backing up the configuration file on the device](#)
- [Upgrading firmware on the device](#)
- [Downgrading firmware on the device](#)

Backing up the configuration file on the device

Whenever a device is about to be upgraded or downgraded, you must back up the current configuration file. A current, backed up configuration file provides a way to easily restore settings if you have issues during the upgrade process that changes the current configuration or if you have to revert your device to factory defaults.

The following procedure assumes that you are using FortiExplorer to back up the configuration file. However, you can go to the device's web-based manager using your web browser and back up the configuration file.

To back up the configuration file

- 1 Within FortiExplorer, select *Web-based Manager* and when the login screen appears, log in.
- 2 In the web-based manager, go to *System > Dashboard > Status*.
- 3 In *System Information* widget, select *Backup* in the *System Configuration* row.
- 4 Select either *Local PC*, *FortiManager* or *USB Disk*.
The *USB Disk* option is grayed out if no USB drive is inserted into the USB port. The *FortiManager* option is not available if the device is not managed by a FortiManager system.
- 5 If VDOMs are enabled, select to back up the entire configuration (*Full Config*), or a specific VDOM's configuration (*VDOM Config*).
- 6 If you are backing up a VDOM configuration, select the VDOM from the list.
- 7 To encrypt the configuration file, select *Encrypt configuration file*.
Encryption must be enabled on the backup file to back up VPN certificates.
- 8 Enter a password and enter it again to confirm it.
The password is needed to restore the file.
- 9 Select *Backup*.
- 10 The web browser will prompt you for a location to save the configuration file. The configuration file will have a .conf extension.

Upgrading firmware on the device

In the FortiExplorer window, you can select *Upload Firmware* and upgrade the firmware on your device. When upgrading a device, the network will be disrupted, so it is best to upgrade the firmware during low-traffic times.

To upgrade a new firmware image on a device

- 1 Back up the configuration file using the procedure, [“To back up the configuration file” on page 17](#).
- 2 In the device’s Status page, select a new firmware image from the list in *Upload Firmware*.
If the firmware image that you want to install is not in the list, select *Choose an Upgrade File* from the list to choose the new firmware image from your computer.
- 3 With the firmware image to install selected in the list, select *Upload Firmware*.
The firmware image uploads to the device. This may take a few minutes.

Downgrading firmware on the device

In the FortiExplorer window, you select *Upload Firmware* to downgrade the firmware on the device. When downgrading firmware on a device, the network will be disrupted, so it is best to downgrade during low-traffic times.

To downgrade firmware on a device

- 1 Back up the configuration file using the procedure, [“To back up the configuration file” on page 17](#).
- 2 In the device’s Status page, select an older firmware image from the list in *Upload Firmware*.
If the firmware image that you want to install is not in the list, select *Choose an Upgrade File* from the list to choose the new firmware image from your computer.
- 3 With the firmware image to install selected in the list, select *Upload Firmware*.
The firmware image uploads to the device. This may take a few minutes.



Appendix

Document conventions

Fortinet technical documentation uses the conventions described below.

IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at <http://ietf.org/rfc/rfc1918.txt?number-1918>.

Most of the examples in this document use the following IP addressing:

- IP addresses are made up of A.B.C.D
- A - can be one of 192, 172, or 10 - the non-public addresses covered in RFC 1918.
- B - 168, or the branch / device / virtual device number.
 - Branch number can be 0xx, 1xx, 2xx - 0 is Head office, 1 is remote, 2 is other.
 - Device or virtual device - allows multiple FortiGate units in this address space (VDMs).
 - Devices can be from x01 to x99.
- C - interface - FortiGate units can have up to 40 interfaces, potentially more than one on the same subnet
 - 001 - 099- physical address ports, and non -virtual interfaces
 - 100-255 - VLANs, tunnels, aggregate links, redundant links, vdom-links, etc.

- D - usage based addresses, this part is determined by what device is doing
 - The following gives 16 reserved, 140 users, and 100 servers in the subnet.
 - 001 - 009 - reserved for networking hardware, like routers, gateways, etc.
 - 010 - 099 - DHCP range - users
 - 100 - 109 - FortiGate devices - typically only use 100
 - 110 - 199 - servers in general (see later for details)
 - 200 - 249 - static range - users
 - 250 - 255 - reserved (255 is broadcast, 000 not used)
 - The D segment servers can be farther broken down into:
 - 110 - 119 - Email servers
 - 120 - 129 - Web servers
 - 130 - 139 - Syslog servers
 - 140 - 149 - Authentication (RADIUS, LDAP, TACACS+, FSAE, etc)
 - 150 - 159 - VoIP / SIP servers / managers
 - 160 - 169 - FortiAnalyzers
 - 170 - 179 - FortiManagers
 - 180 - 189 - Other Fortinet products (FortiScan, FortiDB, etc.)
 - 190 - 199 - Other non-Fortinet servers (NAS, SQL, DNS, DDNS, etc.)
 - Fortinet products, non-FortiGate, are found from 160 - 189.

The following table shows some examples of how to choose an IP number for a device based on the information given. For internal and dmz, it is assumed in this case there is only one interface being used.

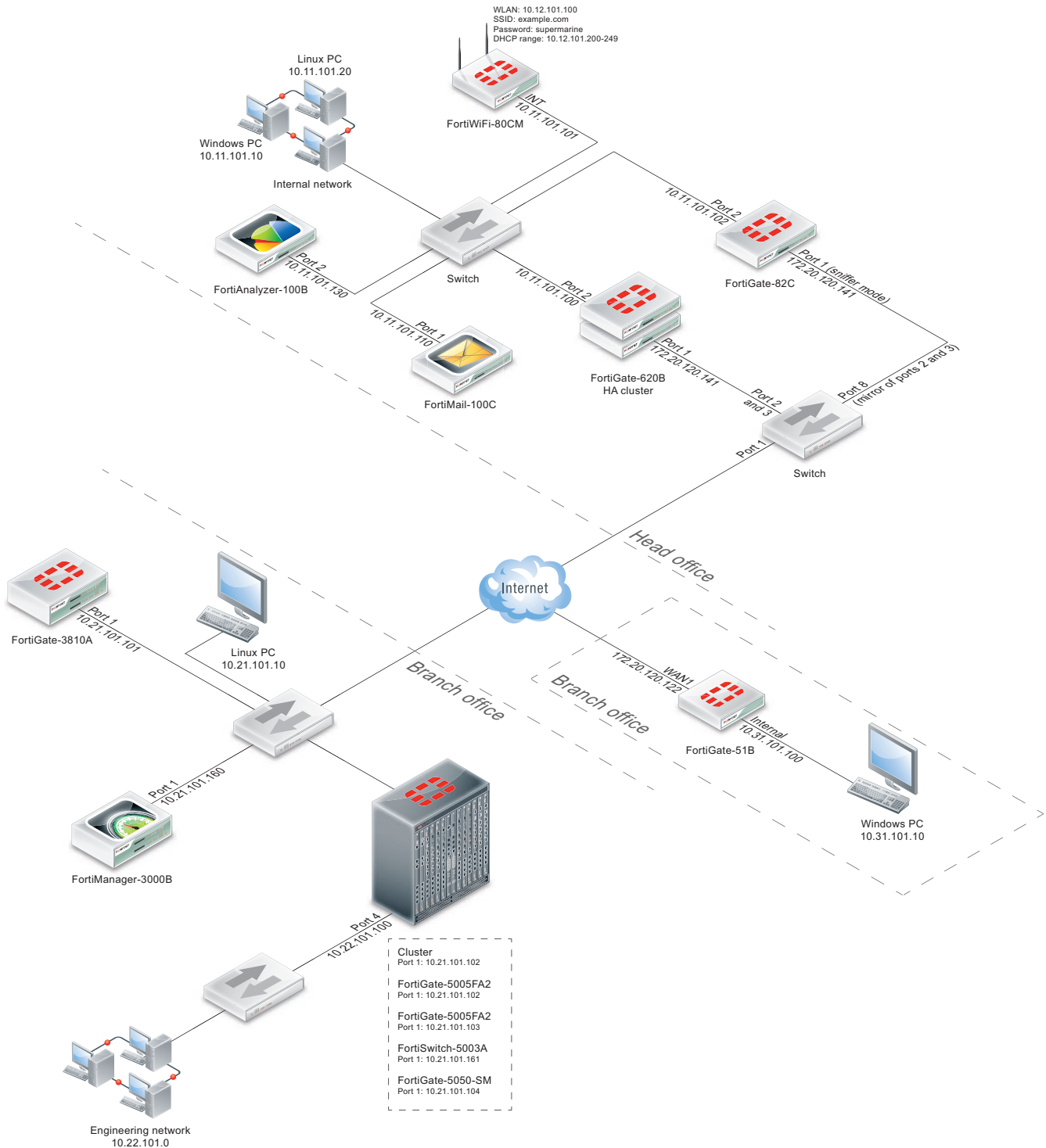
Table 1: Examples of the IP numbering

Location and device	Internal	Dmz	External
Head Office, one FortiGate	10.011.101.100	10.011.201.100	172.20.120.191
Head Office, second FortiGate	10.012.101.100	10.012.201.100	172.20.120.192
Branch Office, one FortiGate	10.021.101.100	10.021.201.100	172.20.120.193
Office 7, one FortiGate with 9 VDOMs	10.079.101.100	10.079.101.100	172.20.120.194
Office 3, one FortiGate, web server	n/a	10.031.201.110	n/a
Bob in accounting on the corporate user network (dhcp) at Head Office, one FortiGate	10.0.11.101.200	n/a	n/a
Router outside the FortiGate	n/a	n/a	172.20.120.195

Example Network configuration

The network configuration shown in [Figure 6](#) or variations on it is used for many of the examples in this document. In this example, the 172.20.120.0 network is equivalent to the Internet. The network consists of a head office and two branch offices.

Figure 1: Example network configuration



Cautions, Notes and Tips

Fortinet technical documentation uses the following guidance and styles for cautions, notes and tips.



A Must Read table details information that is easily missed: configuration changes that only apply to the current session, or services that need restarting before an update will apply.



A Tip provides shortcuts or alternative approaches to the task at hand.



A Troubleshooting tip provides information to help you track down why your configuration is not working.

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 2: Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From <i>Minimum log level</i> , select <i>Notification</i> .
CLI input	<pre>config system dns set primary <address_ipv4> end</pre>
CLI output	<pre>FGT-602803030703 # get system settings comments : (null) opmode : nat</pre>
Emphasis	HTTP connections are <i>not</i> secure and can be intercepted by a third party.
File content	<pre><HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4></pre>
Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com .
Keyboard entry	Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .
Navigation	Go to <code>VPN > IPSEC > Auto Key (IKE)</code> .
Publication	For details, see the FortiOS Handbook .

CLI command syntax conventions

This guide uses the following conventions to describe the syntax to use when entering commands in the Command Line Interface (CLI).

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as `<address_ipv4>`, indicate which data types or string patterns are acceptable value input.

Table 3: Command syntax notation

Convention	Description
Square brackets []	A non-required word or series of words. For example: [verbose {1 2 3}] indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as: verbose 3
Angle brackets < >	A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (<code>_</code>) and suffix that indicates the valid data type. For example: <code><retries_int></code> indicates that you should enter a number of retries, such as 5. Data types include: <ul style="list-style-type: none"> <code><xxx_name></code>: A name referring to another part of the configuration, such as <code>policy_A</code>. <code><xxx_index></code>: An index number referring to another part of the configuration, such as 0 for the first static route. <code><xxx_pattern></code>: A regular expression or word with wild cards that matches possible variations, such as <code>*@example.com</code> to match all email addresses ending in <code>@example.com</code>. <code><xxx_fqdn></code>: A fully qualified domain name (FQDN), such as <code>mail.example.com</code>. <code><xxx_email></code>: An email address, such as <code>admin@mail.example.com</code>. <code><xxx_url></code>: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as <code>http://www.fortinet./com/</code>. <code><xxx_ipv4></code>: An IPv4 address, such as <code>192.168.1.99</code>. <code><xxx_v4mask></code>: A dotted decimal IPv4 netmask, such as <code>255.255.255.0</code>. <code><xxx_ipv4mask></code>: A dotted decimal IPv4 address and netmask separated by a space, such as <code>192.168.1.99 255.255.255.0</code>. <code><xxx_ipv4/mask></code>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as <code>192.168.1.99/24</code>. <code><xxx_ipv6></code>: A colon (<code>:</code>)-delimited hexadecimal IPv6 address, such as <code>3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234</code>. <code><xxx_v6mask></code>: An IPv6 netmask, such as <code>/96</code>. <code><xxx_ipv6mask></code>: An IPv6 address and netmask separated by a space. <code><xxx_str></code>: A string of characters that is not another data type, such as <code>P@sswOrd</code>. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. <code><xxx_int></code>: An integer number that is not another data type, such as <code>15</code> for the number of minutes.

Table 3: Command syntax notation (Continued)

Convention	Description
Curly braces { }	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [].
	Options delimited by vertical bars Mutually exclusive options. For example: {enable disable} indicates that you must enter either <code>enable</code> or <code>disable</code> , but must not enter both.
Options delimited by spaces	Non-mutually exclusive options. For example: {http https ping snmp ssh telnet} indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: <code>ping https ssh</code> Note: To change the options, you must re-type the entire list. For example, to add <code>snmp</code> to the previous example, you would type: <code>ping https snmp ssh</code> If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

Entering FortiOS configuration data

The configuration of a FortiGate unit is stored as a series of configuration settings in the FortiOS configuration database. To change the configuration you can use the web-based manager or CLI to add, delete or change configuration settings. These configuration changes are stored in the configuration database as they are made.

Individual settings in the configuration database can be text strings, numeric values, selections from a list of allowed options, or on/off (enable/disable).

Entering text strings (names)

Text strings are used to name entities in the configuration. For example, the name of a firewall address, administrative user, and so on. You can enter any character in a FortiGate configuration text string except, to prevent Cross-Site Scripting (XSS) vulnerabilities, text strings in FortiGate configuration names cannot include the following characters:

" (double quote), & (ampersand), ' (single quote), < (less than) and > (greater than)

You can determine the limit to the number of characters that are allowed in a text string by determining how many characters the web-based manager or CLI allows for a given name field. From the CLI, you can also use the `tree` command to view the number of characters that are allowed. For example, firewall address names can contain up to 64 characters. When you add a firewall address to the web-based manager you are limited to entering 64 characters in the firewall address name field. From the CLI you can do the following to confirm that the firewall address name field allows 64 characters.

```
config firewall address
tree
-- [address] --*name (64)
    |- subnet
    |- type
    |- start-ip
    |- end-ip
```



```
|- fqdn (256)
|- cache-ttl (0,86400)
|- wildcard
|- comment (64 xss)
|- associated-interface (16)
+- color (0,32)
```

Note that the tree command output also shows the number of characters allowed for other firewall address name settings. For example, the fully-qualified domain name (`fqdn`) field can contain up to 256 characters.

Entering numeric values

Numeric values are used to configure various sizes, rates, numeric addresses, or other numeric values. For example, a static routing priority of 10, a port number of 8080, or an IP address of 10.10.10.1. Numeric values can be entered as a series of digits without spaces or commas (for example, 10 or 64400), in dotted decimal format (for example the IP address 10.10.10.1) or as in the case of MAC or IPv6 addresses separated by colons (for example, the MAC address 00:09:0F:B7:37:00). Most numeric values are standard base-10 numbers, but some fields (again such as MAC addresses) require hexadecimal numbers.

Most web-based manager numeric value configuration fields limit the number of numeric digits that you can add or contain extra information to make it easier to add the acceptable number of digits and to add numbers in the allowed range. CLI help includes information about allowed numeric value ranges. Both the web-based manager and the CLI prevent you from entering invalid numbers.

Selecting options from a list

If a configuration field can only contain one of a number of selected options, the web-based manager and CLI present you a list of acceptable options and you can select one from the list. No other input is allowed. From the CLI you must spell the selection name correctly.

Enabling or disabling options

If a configuration field can only be on or off (enabled or disabled) the web-based manager presents a check box or other control that can only be enabled or disabled. From the CLI you can set the option to enable or disable.

Registering your Fortinet product

Before you begin configuring and customizing features, take a moment to register your Fortinet product at the Fortinet Technical Support web site, <https://support.fortinet.com>.

Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Center article [Registration Frequently Asked Questions](#).

Fortinet products End User License Agreement

See the [Fortinet products End User License Agreement](#).

Training

Fortinet Training Services provides courses that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at <http://campus.training.fortinet.com>, or email training@fortinet.com.

Documentation

The Fortinet Technical Documentation web site, <http://docs.fortinet.com>, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD.

Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, <http://docs.fortinet.com>.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at <http://kb.fortinet.com>.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.

Customer service and technical support

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

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at <https://support.fortinet.com>.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Base article [FortiGate Troubleshooting Guide - Technical Support Requirements](#).



Index

B

backing up config file, 17

C

certification, 26
CLI syntax conventions, 22
comments, documentation, 26
connecting to CLI, 12
connecting to web-based manager, 11
conventions, 19
Cross-Site Scripting
 protection from, 24
customer service, 26

D

default
 password, 5
device
 registering from FortiExplorer, 10
 upgrading firmware, 18
document conventions
 CLI syntax, 22
documentation, 26
 commenting on, 26
 conventions, 19
 Fortinet, 26
downgrading firmware on device
 device
 downgrading firmware, 18

F

FAQ, 26
FortiGate documentation
 commenting on, 26
FortiGuard
 Antispam, 5
 Antivirus, 5, 25
 services, 25
Fortinet
 Knowledge Center, 26
 Technical Documentation, 26
 Technical Documentation, conventions, 19
 Technical Support, 26
 Technical Support, registering with, 25
 Technical Support, web site, 25
 Training Services, 26
Fortinet customer service, 26
Fortinet documentation, 26
Fortinet Knowledge Center, 26

G

glossary, 26

H

how-to, 26

I

installing FortiExplorer
 on Mac OS, 8
 using CD, 8
introduction
 Fortinet documentation, 26
IP address
 private network, 19

K

Knowledge Center, 26

M

mode
 operation, 5

O

operation mode, 5

P

password
 administrator, 5
product registration, 25

R

registering
 with Fortinet Technical Support, 25
registering device, 10
RFC
 1918, 19

S

setting up basic settings, 9
Setup Wizard, 9

T

technical
 documentation, 26
 documentation conventions, 19
 notes, 26
 support, 26

technical support, 26
Training Services, 26

U

upgrading firmware on device, 18

V

vulnerability
 Cross-Site Scripting, 24
 XSS, 24

W

web-based manager
 connecting, 11
wizard
 setting up basic settings, 9

X

XSS vulnerability
 protection from, 24

FORTINET®

www.fortinet.com

FORTINET®

www.fortinet.com