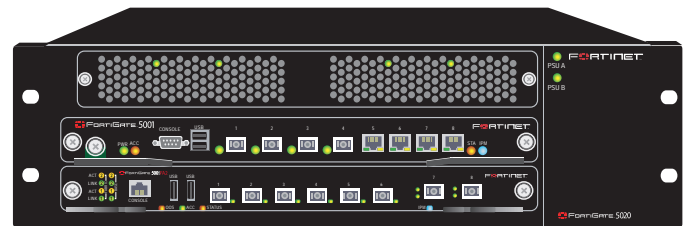
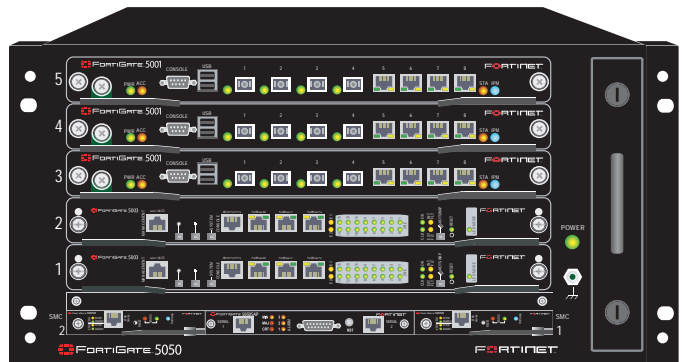


Firmware and FortiUSB Guide

FortiGate-5000 Series



Visit <http://support.fortinet.com> to register your FortiGate-5000 Series product. By registering you can receive product updates, technical support, and FortiGuard services.



www.fortinet.com

FortiGate-5000 Series Firmware and FortiUSB Guide

1 February 2007

01-30004-0383-20070201

© Copyright 2007 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

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, 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

Introduction	5
Revision history	5
Warnings and cautions	5
About this document.....	7
Fortinet documentation.....	7
Fortinet Tools and Documentation CD	7
Fortinet Knowledge Center	7
Comments on Fortinet technical documentation.....	7
Customer service and technical support	7
Register your Fortinet product.....	8
FortiGate firmware	9
Upgrading to a new firmware version.....	9
Reverting to a previous firmware version	10
Installing firmware images from a system reboot using the CLI	12
Testing a new firmware image before installing it.....	15
The FortiUSB key	19
Backup and Restore from the FortiUSB key	19
Using the USB Auto-Install feature	20
Additional CLI commands for the FortiUSB key.....	21

Introduction

This *FortiGate-5000 Series Firmware and FortiUSB Guide* contains the information you need to change the firmware running on your FortiGate-5000 series security system. This document also describes how to use the FortiUSB key with your FortiGate-5000 series security system. The information in this document applies to all currently available FortiGate-5000 modules running FortiOS v3.0 firmware.

This chapter includes the following topics:

- [Revision history](#)
- [Warnings and cautions](#)
- [About this document](#)
- [Fortinet documentation](#)
- [Customer service and technical support](#)

Revision history

Table 1: Revision History

Version	Description of changes
01-30003-0383-20061204	Initial version
01-30004-0383-20070201	Minor graphics fixes. Added "Register your Fortinet product" on page 8 . Minor change to "Upgrading to a new firmware version" on page 9 .

Warnings and cautions

Only trained and qualified personnel should be allowed to install or maintain FortiGate-5000 series equipment. Read and comply with all warnings, cautions and notices in this document.



Caution: You should be aware of the following cautions and warnings before installing FortiGate-5000 series hardware.

- Turning off all power switches may not turn off all power to the FortiGate equipment. Except where noted, disconnect the FortiGate equipment from all power sources, telecommunications links and networks before installing, or removing FortiGate components, or performing other maintenance tasks. Failure to do this can result in personal injury or equipment damage. Some circuitry in the FortiGate equipment may continue to operate even though all power switches are off.

- An easily accessible disconnect device, such as a circuit breaker, should be incorporated into the data center wiring that connects power to the FortiGate equipment.
- Install FortiGate chassis at the lower positions of a rack to avoid making the rack top-heavy and unstable.
- Do not insert metal objects or tools into open chassis slots.
- Electrostatic discharge (ESD) can damage FortiGate equipment. Only perform the procedures described in this document from an ESD workstation. If no such station is available, you can provide some ESD protection by wearing an anti-static wrist or ankle strap and attaching it to an ESD connector or to a metal part of a FortiGate chassis.
- Some FortiGate components may overload your supply circuit and impact your overcurrent protection and supply wiring. Refer to nameplate ratings to address this concern.
- Make sure all FortiGate components have reliable grounding. Fortinet recommends direct connections to the branch circuit.
- If you install a FortiGate component in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Make sure the operating ambient temperature does not exceed the manufacturer's maximum rated ambient temperature.
- Installing FortiGate equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- This equipment is for installation only in a Restricted Access Location (dedicated equipment room, service closet or the like), in accordance with the National Electrical Code.
- Per the National Electrical Code, sizing of a Listed circuit breaker or branch circuit fuse and the supply conductors to the equipment is based on the marked input current rating. A product with a marked input current rating of 25 A is required to be placed on a 40 A branch circuit. The supply conductors will also be sized according to the input current rating and also derated for the maximum rated operating ambient temperature, T_{ma} , of the equipment.
- FortiGate equipment shall be installed and connected to an electrical supply source in accordance with the applicable codes and regulations for the location in which it is installed. Particular attention shall be paid to use of correct wire type and size to comply with the applicable codes and regulations for the installation / location. Connection of the supply wiring to the terminal block on the equipment may be accomplished using Listed wire compression lugs, for example, Pressure Terminal Connector made by Ideal Industries Inc. or equivalent which is suitable for AWG 10. Particular attention shall be given to use of the appropriate compression tool specified by the compression lug manufacturer, if one is specified.

About this document

This document includes the following chapters:

- [FortiGate firmware](#) describes how to use the FortiOS web-based manager and CLI to upgrade to a new firmware version, revert to a previous firmware version, install firmware from a reboot using the CLI, and test a new firmware image before installing it.
- [The FortiUSB key](#) describes how to use the FortiUSB key to backup and restored configurations and firmware images, to use FortiUSB auto-install, and to use additional FortiUSB CLI commands.

Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at <http://docs.forticare.com>. All FortiGate-5000 information is available from the [FortiGate-5000](#) page.

Fortinet Tools and Documentation CD

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at <http://docs.forticare.com>. FortiGate-5000 series documentation is located in its own section of the site at <http://docs.forticare.com/fgt5k.html>.

Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

The [FortiGate Log Message Reference](#) is available exclusively from the [Fortinet Knowledge Center](#), the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.

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.

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.

Register your Fortinet product

Register your Fortinet product to receive Fortinet customer services such as product updates and technical support. You must also register your product for FortiGuard services such as FortiGuard Antivirus and Intrusion Prevention updates and for FortiGuard Web Filtering and AntiSpam.

Register your product by visiting <http://support.fortinet.com> and selecting Product Registration.

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

FortiGate firmware

Fortinet periodically updates the FortiGate firmware to include enhancements and address issues. After you have registered your FortiGate security system (see [“Register your Fortinet product” on page 8](#)), you can download firmware from the support web site <http://support.fortinet.com>.

Only FortiGate administrators with system read and write privileges can change the FortiGate firmware (for example, the admin administrator).

This section includes the following topics:

- [Upgrading to a new firmware version](#)
- [Reverting to a previous firmware version](#)
- [Installing firmware images from a system reboot using the CLI](#)
- [Testing a new firmware image before installing it](#)

Upgrading to a new firmware version

Use the web-based manager or CLI procedure to upgrade to a new FortiGate firmware version or to a more recent build of the same firmware version.



Note: Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date.



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

To upgrade the firmware using the web-based manager

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

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

- 7 Log into the web-based manager.
- 8 Go to **System > Status** and check the Firmware Version to confirm the firmware upgrade is successfully installed.
- 9 Update the FortiGate antivirus and attack definitions. See the FortiGate online help for details.

To upgrade the firmware using the CLI

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

- 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 FortiGate CLI.
- 4 Make sure the FortiGate module 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 FortiGate module:

```
execute restore image <name_str> <tftp_ipv4>
```

Where `<name_str>` is the name of the firmware image file and `<tftp_ipv4>` 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 image.out 192.168.1.168
```

The FortiGate module responds with the message:

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

- 6 Type `y`.
The FortiGate module 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 firmware image is successfully installed, enter:

```
get system status
```
- 9 Update antivirus and attack definitions. You can use the command

```
execute update-now
```

Reverting to a previous firmware version

Use the web-based manager or CLI procedure to revert to a previous firmware version. Reverting to a previous firmware version reverts the FortiGate module to its factory default configuration.

Before beginning this procedure, it is recommended that you:

- back up the FortiGate system configuration (from the CLI, use the command `execute backup config`)
- back up the IPS custom signatures (from the CLI, use the command `execute backup ipsuserdefsig`)
- back up web content and email filtering lists

If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.



Note: Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date.



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 using the web-based manager

- 1 Copy the firmware image file to the management computer.
- 2 Log into the FortiGate web-based manager.
- 3 Go to **System > Status**.
- 4 Under **System Information > Firmware Version**, select Update.
- 5 Type the path and filename of the firmware image file, or select Browse and locate the file.
- 6 Select OK.
The FortiGate module uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiGate login. This process takes a few minutes.
- 7 Log into the web-based manager.
- 8 Go to **System > Status** and check the Firmware Version to confirm the firmware is successfully installed.
- 9 Restore your configuration. See the FortiGate online help for details.
- 10 Update the FortiGate antivirus and attack definitions. See the FortiGate online help for details.

To revert to a previous firmware version using the CLI

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

- 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 FortiGate CLI.
- 4 Make sure the FortiGate module 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 FortiGate module:

```
execute restore image <name_str> <tftp_ipv4>
```

Where <name_str> is the name of the firmware image file and <tftp_ipv4> 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 image.out 192.168.1.168
```

The FortiGate module responds with this message:

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

- 6 Type `y`.

The FortiGate module 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 FortiGate module 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, if needed, use the command:

```
execute restore config <name_str> <tftp_ip4>
```

- 11 Update antivirus and attack definitions. You can use the command

```
execute update-now
```

Installing firmware images from a system reboot using the CLI

This procedure installs a specified firmware image and resets the FortiGate module 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 FortiGate console cable. This procedure reverts the FortiGate module to its factory default configuration.

For this procedure you:

- Access the CLI by connecting to the FortiGate console port using the console cable.
- Connect a FortiGate interface to your network.
- Have a TFTP server that you can connect to from the FortiGate interface.

Before beginning this procedure, it is recommended that you:

- back up the FortiGate system configuration (from the CLI, use the command `execute backup config`)
- back up the IPS custom signatures (from the CLI, use the command `execute backup ipsuserdefsig`)
- back up web content and email filtering lists

If you are reverting to a previous FortiOS version, you might not be able to restore the previous configuration from the backup configuration file.



Note: Installing firmware replaces your current antivirus and attack definitions, along with the definitions included with the firmware release you are installing. After you install new firmware, make sure that antivirus and attack definitions are up to date.

To install firmware from a system reboot

- 1 Connect a management computer to the FortiGate CLI using the FortiGate console port.
- 2 Connect a FortiGate interface to your network.
- 3 Make sure the TFTP server is running and connected to the same network as the FortiGate interface.
- 4 Copy the new firmware image file to the root directory of the TFTP server.
- 5 Enter the following command to restart the FortiGate module.

```
execute reboot
```

The FortiGate module responds with the following message:

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

- 6 Type `y`.

As the FortiGate module starts, a series of system startup messages is displayed. When the following messages appears:

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

- 7 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 module reboots and you must log into the CLI again and repeat the `execute reboot` command.

If you successfully interrupt the startup process, a menu similar to the following appears:

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

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

- 8** Type **I** and the Configuration and information menu is displayed:
- ```
[S]: Set serial port baudrate(will take effect on next boot).
[T]: Set image download port.
[C]: Set DHCP enable (will take effect on next boot).
[D]: Set bootup debug message display (will take effect on next boot).
[I]: Display hardware information.
[Q]: Quit this menu.
[H]: Display this list of options.
```

Enter S,T,C,D,I,Q, or H:

- 9** Type **T** to set the image download interface. The following message is displayed:

Enter image download port number [1]:

- 10** Enter the number of the FortiGate interface that you connected to the same network as the TFTP server and press Enter.

For example, if you have connected interface 6 (port6) to the network, enter 6 and press Enter.

- 11** Type **Q** to return to the previous menu.  
**12** Type **G** to get to the new firmware image form the TFTP server.

The following message appears:

Enter TFTP server address [192.168.1.168]:

- 13** Type the address of the TFTP server and press Enter:

The following message appears:

Enter Local Address [192.168.1.188]:

- 14** Type an IP address that the FortiGate image download interface (see step 10) can use to connect to the TFTP server.

This IP address is a temporary IP address only assigned to this interface for uploading the firmware image from the TFTP server. The IP address can be any IP address that is valid for the network that the image download 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]:

- 15** Type the new firmware image filename and press Enter.

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

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

- 16** Type **D**.

The FortiGate module installs the new firmware image and restarts. The installation might take a few minutes to complete. The FortiGate starts up in the factory default configuration.

- 17 To confirm the new firmware image has been loaded, connect to the FortiGate CLI and enter:

```
get system status
```

### To restore the previous configuration

After installing firmware from a system reboot, you can use the following procedure to restore your previous configuration from the CLI console connection.

- 1 Make sure a FortiGate interface is connected to the same network as TFTP server containing the saved configuration file for the FortiGate module.
- 2 If required, Change the IP address of the interface connected to the same network as the TFTP server.

You can do this from the CLI using the following commands (shown for the port6 interface):

```
config system interface
 edit port6
 set ip <address_ip4mask>
 set allowaccess {ping https ssh telnet http}
 end
```

- 3 To restore your previous configuration, if needed, use the command:
 

```
execute restore config <name_str> <tftp_ip4>
```
- 4 Update antivirus and attack definitions. You can use the command
 

```
execute update-now
```

## Testing a new firmware image before installing it

You can test a new firmware image by installing the firmware image from a system reboot and saving it to system memory. After completing this procedure, the FortiGate module operates using the new firmware image with the current configuration. This new firmware image is not permanently installed. The next time the FortiGate module restarts, it operates with the originally installed firmware image using the current configuration. If the new firmware image operates successfully, you can install it permanently using the procedure [“Upgrading to a new firmware version” on page 9](#).

Use this procedure to test a new firmware image before installing it. To use this procedure, you must connect to the CLI using the FortiGate console port and a RJ-45 to DB-9 serial cable. This procedure temporarily installs a new firmware image using your current configuration.

For this procedure you:

- Access the CLI by connecting to the FortiGate console port using the console cable.
- Connect a FortiGate interface to your network.
- Have a TFTP server that you can connect to from the FortiGate interface.

**To test the new firmware image**

- 1 Connect a management computer to the FortiGate CLI using the FortiGate console port.
- 2 Connect a FortiGate interface to your network.
- 3 Make sure the TFTP server is running and connected to the same network as the FortiGate interface.
- 4 Copy the new firmware image file to the root directory of the TFTP server.
- 5 Enter the following command to restart the FortiGate module.

```
execute reboot
```

The FortiGate module responds with the following message:

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

- 6 Type `y`.  
As the FortiGate module starts, a series of system startup messages is displayed. When the following messages appears:

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

- 7 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 module reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following menu appears:

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

Enter G,F,B,I,Q,or H:

- 8 Type `I` and the Configuration and information menu is displayed:
 

```
[S]: Set serial port baudrate(will take effect on next
boot).
[T]: Set image download port.
[C]: Set DHCP enable (will take effect on next boot).
[D]: Set bootup debug message display (will take effect
on next boot).
[I]: Display hardware information.
[Q]: Quit this menu.
[H]: Display this list of options.
```

Enter S,T,C,D,I,Q,or H:
- 9 Type `T` to set the image download interface. The following message is displayed:
 

```
Enter image download port number [1]:
```

- 10** Enter the number of the FortiGate interface that you connected to the same network as the TFTP server and press Enter.

For example, if you have connected interface 6 (port6) to the network, enter 6 and press Enter.
- 11** Type Q to return to the boot menu.
- 12** Type G to get to the new firmware image from the TFTP server.

The following message appears:

```
Enter TFTP server address [192.168.1.168]:
```
- 13** Type the address of the TFTP server and press Enter:

The following message appears:

```
Enter Local Address [192.168.1.188]:
```
- 14** Type an IP address that the FortiGate image download interface (see step 10) can use to connect to the TFTP server.

This IP address is a temporary IP address only assigned to this interface for uploading the firmware image from the TFTP server. The IP address can be any IP address that is valid for the network that the image download 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]:
```
- 15** Type the firmware image filename and press Enter.

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

```
Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
```
- 16** Type R.

The FortiGate image is installed to system memory and the FortiGate module starts up and operates using the new firmware image, but with its current configuration.
- 17** You can log into the CLI or the web-based manager using any administrative account.
- 18** To confirm the new firmware image has been loaded from the CLI, enter:

```
get system status
```

You can test the new firmware image as required. When you reboot the FortiGate module it restarts running the previous firmware image.



# The FortiUSB key

The FortiUSB key provides flexibility and control when backing up and restoring configuration files. The FortiUSB key also enables you to have a single, secure location for storing configuration files.

The FortiUSB key is used with the USB Auto-Install feature, automatically installing a configuration file and a firmware image file on a system reboot. The USB Auto-Install feature uses a configuration file and a firmware image file that is on the FortiUSB key, and on a system reboot, checks if these files need to be installed. If they do, the FortiGate module installs the configuration file and firmware image file directly from the key to the module.



**Note:** The FortiUSB key is purchased separately. The FortiGate module only supports the FortiUSB key available from Fortinet.

This section includes the following topics:

- [Backup and Restore from the FortiUSB key](#)
- [Using the USB Auto-Install feature](#)
- [Additional CLI commands for the FortiUSB key](#)

## Backup and Restore from the FortiUSB key

You can use the FortiUSB key to either backup a configuration file or restore a configuration file.

You should always make sure the FortiUSB key is properly inserted before proceeding since the FortiGate module must recognize that the key is inserted in its USB port.



**Note:** You can only save VPN certificates if you encrypt the file. Make sure the configuration encryption is enabled so you can save the VPN certificates with the configuration file.

### To backup a FortiGate configuration using the web-based manager

- 1 Insert the FortiUSB key you want to use to store the configuration file into one of the USB sockets on the FortiGate front panel.
- 2 Go to **System > Maintenance > Backup and Restore**.
- 3 Select USB Disk from the Backup configuration to list.
- 4 Select Backup.

### To restore configuration using the web-based manager

- 1 Insert the FortiUSB key containing the configuration file you want to restore into one of the USB sockets on the FortiGate front panel.
- 2 Go to **System > Maintenance > Backup and Restore**.

- 3 Select USB Disk from the Restore configuration from list.
- 4 Select the configuration file you want restored in the Filename list.
- 5 Select Restore.

#### To backup configuration using the CLI

- 1 Insert the FortiUSB key you want to use to store the configuration file into one of the USB sockets on the FortiGate front panel.
- 2 Log into the CLI.
- 3 Enter the following command to backup the configuration files:  
`exec backup config usb <filename>`
- 4 Enter the following command to check the configuration files are on the key:  
`exec usb-disk list`

#### To restore configuration using the CLI

- 1 Insert the FortiUSB key containing the configuration file you want to restore into one of the USB sockets on the FortiGate front panel.
- 2 Log into the CLI.
- 3 Enter the following command to restore the configuration files:  
`exec restore image usb <filename>`  
The FortiGate module responds with the following message:  
This operation will replace the current firmware version!  
Do you want to continue? (y/n)
- 4 Type `y`.

## Using the USB Auto-Install feature

The USB Auto-Install feature automatically updates the FortiGate configuration file and image file on a system reboot. Also, this feature provides you with an additional backup if you are unable to save your system settings before shutting down or rebooting your FortiGate module.

The following procedures use both the web-based manager and the CLI. However, it is recommended you use the CLI since the login screen may appear before the installation is complete. The FortiGate module may reboot twice if installing the firmware image and configuration file.



**Note:** You need an unencrypted configuration file for this feature. Also the default files, `image.out` and `fgt_system.conf`, must be in the root directory.

#### To configure the USB Auto-Install using the web-based manager

- 1 Go to **System > Maintenance > Backup and Restore**.
- 2 Select the blue arrow to expand the Advanced options.

- 3 Select the following:
  - On system restart, automatically update FortiGate configuration file if default filename is available on the USB disk.
  - On system restart, automatically update FortiGate firmware image if default image is available on the USB disk.
- 4 Enter the configuration and image filenames or use the default configuration filename (fgt\_system.conf) and default image name (image.out).
- 5 Select Apply.

#### To configure the USB Auto-Install using the CLI

- 1 Log into the CLI.
- 2 Enter the following command:

```
config system auto-install
 set default-config-file <filename>
 set auto-intall-config <enable/disable>
 set default-image-file <filename>
 set auto-install-image <enable/disable>
end
```

## Additional CLI commands for the FortiUSB key

Use the following CLI commands when you want to delete a file from the FortiUSB key, list what files are on the key, including formatting the key or renaming a file:

- `exec usb-disk list`
- `exec usb-disk delete <filename>`
- `exec usb-disk format`
- `exec usb-disk rename <old_filename1> <old_filename2>`



**Note:** If you are trying to delete a configuration file from the CLI command interface, and the filename contains spaces, you will need quotations around the file name before you can delete the file from the FortiUSB key.



**FORTINET™**

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