

SysAdmin's Notebook

Using the USB MGMT Console port

Some FortiGate models are shipped without the standard RJ-45 or RS-232 serial console port that a lot of users are familiar with. In its place is a USB port that is designed to work with FortiExplorer and a USB cable instead of the Terminal session and console cable.



FortiGate 60D with USB MGMT port

There are other models that work with FortiExplorer, but those models use a USB port that is part of the FortiGate *in addition to* the console port. In those units, accessing the FortiGate through FortiExplorer at the BIOS level is not possible. The firmware has to be up and running before a CLI interface is available.



FortiGate 60C with RJ-45 Console port

Because of the limitation in those models there has been some concern about how to manage certain scenarios with the USB MGMT Console port only models:

1. Formatting and installing a fresh copy of the firmware on a unit.
2. Accessing the unit in the case of firmware corruption.
3. Resetting the Admin password.

There are some FortiGate models with only the USB MGMT Console port, that have a BIOS that allows access through the USB connection to the BIOS.

USB connection requirements

Connecting to a FortiGate unit that does not have an RJ-45 or serial console port requires the following:

1. USB cable (USB-A to Mini-USB).
2. Ethernet cable if you are going to be setting up a TFTP session.
3. FortiExplorer software, installed.

Initial setup

1. Use the USB cable to connect the computer to the USB MGMT Console port.
2. Open FortiExplorer.
3. Connect the FortiGate to a power supply.

Getting to the BIOS

Once the physical connection between the computer and the FortiGate is set up, use one of the following methods to start the login process. Each method involves having FortiExplorer up and running, and the CLI console open.

1. If the firmware is operational, log in to the unit and run the `execute reboot` command through the CLI.
2. If the firmware is not functioning properly, leave FortiExplorer running in the CLI mode and power cycle the FortiGate unit. Unplug the unit and wait approximately 10 seconds, then plug the unit back in.

Example: Using the USB MGMT port and TFTP to install fresh firmware on a FortiGate 60D

In this example, the following assumptions are made:

1. The firmware is functional.
2. TFTP server software is installed on the computer.
3. The firmware that you wish to install has been downloaded from the support site and is located in a directory accessible by the TFTP server software.

Step #1

Statically assign an address to your computer. Common practice is to use something in the 192.168.1.x subnet. To make it simple, use the default address that the FortiGate will suggest in Step #4 (192.168.1.145) and set the subnet mask to 255.255.255.0.

Step #2

In the CLI Console of FortiExplorer, type `execute reboot`.

After a minute or two the CLI displays the following message:

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

Step #3

As soon as this message appears, follow the instructions. After a few seconds, the boot process continues and you will have to start over to get the option again. The configuration menu lists the following options:

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

Type **G** (this is case insensitive).

Step #4

The CLI displays the following:

```
Please connect TFTP server to Ethernet port 'WAN1'.  
Enter TFTP server address [192.168.1.145]:
```

Use an Ethernet cable to connect from the Ethernet port of the computer to the Ethernet port listed in the instruction. For the 60D model it is WAN1, but other models might list different ports.

The TFTP server address is the one statically assigned to your computer, which is serving as the TFTP server. Press the **Enter** key to use the default address shown or

enter the IP address of the computer. You do not need to enter the subnet mask, as it is assumed to be 255.255.255.0.

Once you have entered the TFTP server's address the CLI displays the following:

```
Enter local address [192.168.1.188]:
```

This IP address refers to the FortiGate unit. It is a temporary address only and will not be held past the next reboot. Ensure that it is on the same subnet as the TFTP server. The subnet mask is automatically set to 255.255.255.0. Press the **Enter** key to use the default address displayed.

Step #5

The CLI displays the following:

```
Enter firmware image file name [image.out]:
```

The firmware image should have an ".out" extension.

Example: FGT_60D-v500-build0208-FORTINET.out

The CLI displays the following:

```
MAC: 00:09:0f:b5:55:28
Connect to tftp server 192.168.1.145 ...
#####
```

A series of #s is a good sign that the file is transferring.

The CLI displays the following once the image file is finished transferring:

```
Image Received.
Checking image... OK
```

Step #6

The CLI displays the following:

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

You will need to choose one of the following:

- **D = Default firmware**
Firmware that is loaded by default when the system is booted
- **B = Backup firmware**
A backup copy of firmware to be used incase there are issues with the default firmware
- **R = Run image without saving**
Unit will use this firmware once but revert to default after the first reboot after using the installed firmware.

To make the new firmware image the default, choose D

The CLI displays the following:

```
Programming the boot device now.
.....
Initializing
```

The FortiGate unit will then boot with the freshly installed firmware.

FortiExplorer

The FortiExplorer software is available from two locations:

- The Service and Support site:

<https://support.fortinet.com/>

- The Product site:

http://www.fortinet.com/resource_center/fortiexplorer_product_download.html

If you download the software from the Service and Support site, choose the FortiExplorer_OnlineInstaller file, either the '.exe' for Windows or the '.dmg' file for Mac. These are the files that download from the Product site. These files, once installed, will connect to a Fortinet server and download the latest version of the software.

The TFTP example described, will work with the 2.2.x versions of FortiExplorer for Windows, but not with the Mac software of the same version. To install via TFTP using a Mac make sure that you have a current copy of the software. It has been tested successfully with version 2.3.1052.

When working with FortiExplorer, there may be some points where the CLI window will disappear from the interface, such as during a reboot. When the CLI is available again the widget will either reappear on its own or the menu options to start the CLI will appear.

Resetting the Admin password

Normally, when you use a console session to reset the admin password, there is a point where the CLI session displays the message:

```
Initializing firewall...
System is started.
Login:
```

As soon as the system starts, you have approximately 15 seconds to enter the **maintainer** account credentials.

A small sampling of tests indicates that the use of the Admin reset feature is not available through FortiExplorer and the USB MGMT connection. It has been tested with version 2.3.1052 of both Windows and Mac software and was unsuccessful.

When using FortiExplorer, as soon as the unit starts reading the boot image file and initializing the firewall the terminal window disappears. When it is available again, approximately one minute later, the CLI displays the message:

```
Login:
```

The 15 second window to enter the credentials runs out before access to the CLI returns. I made several attempts to enter the credentials, but all resulted in the message:

```
Login incorrect
```

If the password is lost, a fresh install of the firmware will reset the password to the default setting where the password is <null>. The configuration will be lost so this could be considered extra motivation to create and store frequent backups of the configuration.

Systems Tested

Model Tested	Result
FortiWiFi 20C	Unable to connect at BIOS level
FortiGate 60D	Success

The BIOS of models, especially the newer models, changes periodically, so even if the model has been previously tested unsuccessfully it makes sense to attempt connecting in case you are dealing with a newer BIOS that does allow connection.