Running an HQIP (Hardware Quick Inspection Package) test

Description

HQIP (Hardware Quick Inspection Package) is a hardware diagnostic firmware image that detects hardware problems on Fortinet products including FortiGate, FortiWifi, FortiAnalyzer, and FortiManager. Running the HQIP test is as straight forward as downloading the HQIP image for your device from the support site, loading the image onto your device, setting up Ethernet cables on the interfaces, letting the package run and recording the results.

If there is an image for your device, you can find it on the Fortinet Service and Support site. If there is no image available for your specific device, you can request one. Turnaround times for new or custom images vary. Share your experience in the comments below.

What an HQIP test does

- Performs tests on a number hardware elements including CPU, Memory, Compact Flash, Hard Disk, and PCI devices (NIC/ASIC)
- Performs actions such as component loop test, factory default restore, and reformat hard drive.

What an HQIP test doesn't do

- Detect ***all*** hardware malfunctions. Tests for the most common hardware problems are performed.
- Diagnose issues that cause a device to reboot or be unstable.
- Detect software configuration errors, OS bugs, or OS Kernel Crash issues (one type of OS bug).
- Diagnose devices with multiple Hard Drives

Determining which image to use

The Device Management section of the Customer Service and Support web portal is integrated with the HQIP Download page. Once you have logged into the site not only does the site know the serial number of your devices, it knows which models and versions of those models the serial numbers refer to. Once you have selected which serial number you need to test, the site can determine the appropriate HQIP image. Because the HQIP images are designed to work with very specific hardware configurations the image will not work on a hardware configuration that it wasn't designed for, so it is crucial to download the correct image.

In the event that the site offers no result, create an RMA ticket, include the serial number(s) of the devices, and request the HQIP Image File.

Scope

Fortinet Devices testable by HQIP

This is a listing to Products and the models that have an available download of the HQIP test for their product and model.

As time goes by and more products are developed the number of images will grow. This list may become out of date so even if you don't see your device listed here check the site for an image just in case.

FortiAuthenticator

- FAC-400C
- FAC-1000C
- FAC-3000B

FortiAP (WiFi Access Point)

- FAP-28C

FortiAnalyzer

- FAZ-100B, FAZ-100C
- FAZ-400B, FAZ-400C
- FAZ-800B
- FAZ-1000B-EMU01, FAZ-1000C
- FAZ-2000, FAZ-2000B
- FAZ-4000A, FAZ-4000B

FortiBridge

- FB-2001, FB-2001F
- FB-2C02
- FB-2F02

FortiCache

- FCH-1000C
- FCH-3000C
- FCH-400C

FortiController

- FTCL-5103B
- FCTRL-5903C

FortiDB

- FD400B
- FDB-400C
- FDB-1000C

FortiDDoS

- FortiDDoS-200B
- FortiDDoS-400B
- FortiDDoS-800B

FortiDNS

- FNS-400C
- FNS-1000C

FortiExtender

- FEX-100B

FortiGate / FortiWiFi

- FG-20C, FWF-20C, FWF-20C-ADSL
- FG-30B, FG-30D, FG-30D-POE, FWF-30B, FWF-30D, FWF-30D-POE
- FG-40C, FWF-40C
- FG-50B, FG-51B, FWF-50B
- FG-60, FG-60B, FG-60C, FG-60C-LENC, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FWF-60B, FWF-60C, FWF-60CA, FWF-60CM, FWF-60CM-3G4G-B, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE
- FG-70D,
- FG-80C, FG-80C-DC-r2, FG-80CM, FG-80D, FG-82C, FWF-80CM, FWF-81CM
- FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FWF-90D, FWF-90D-POE, FWF-92D
- FG-100D, FG-110C, FG-111C
- FG-140D, FG-140D-POE, FG-140D-POE-T1
- FG-200A, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE
- FG-224B
- FG-240D, FG-240D-POE,
- FG-280D-POE
- FG-300C, FG-300D
- FG-310B, FG-311B
- FG-500A, FG-500D
- FG-600C, FG-620B, FG-621B
- FG-800C, FG-800F
- FG-1000A-LENC, FG-1000AFA2, FG-1000C, FG-1000D
- FG-1200D
- FG-1240B, FG-1240B-DC
- FG-1500D
- FG-3016B

- FG-3040B, FG-3040B-LENC
- FG-3140B, FG-3140B-DC
- FG-3240C
- FG-3600, FG-3600A, FG-3600C
- FG-3700D
- FG-3810A-E4, FG-3810D
- FG-3950B, FG-3950B-DC, FG-3951B-DC, FK-3950B, FK-3950B-DC
- FG-5001A-SW, FG-5001B, FG-5001C, FG-5001D, FG-5001SX, FK-5001B
- FG-5101C

FortiGate Rugged

- FGR-60D
- FGR-100C

FortiGate Voice

- FortiGateVoice-70D4
- FGV-80C

FortiMail

- FML-100, FML-100C
- FML-400, FML-400B, FML-400C
- FML-2000A, FML-2000B
- FML-3000C

FortiManager

- FMG-100C
- FMG-400A, FMG-400B, FMG-400C
- FMG-1000C
- FMG-3000, FMG-3000B, FMG-3000C-E02S

FortiScan

- FSC-1000B-EMU01, FSC-1000C
- FSC-3000C

FortiSwitch

- FS-28C
- FS-324B-POE, FS-348B
- FS-448B
- FS-5003A, FS-5003B
- FS-5203B

FortiWeb

- FWB-400B, FWB-400C
- FWB-1000C, FWB-3000C
- FWB-3000CFsx
- FWB-4000C

Modules

Fortinet Rear Transmission Module

- RTM-XB2
- RTM-XD2

Fortinet Security Processing Module

- ADM-FE8
- ADM-XE2

Precautions

- You will want to be local to the firewall to perform this test because of the need to console in and set up the loop-back cabling.
- Plan on installing the HQIP image and running the test on the weekend or evening, as the process of running the test will mean a traffic outage for the duration test until the firmware is back.
- Make sure that you have a good backup of the configuration file and that it is for the firmware version that will be installed on the FortiGate after the test is completed.
- The wiring cannot be set up entirely in advance on most devices because when the loop-backs are set up on the same internal interface that needs to connect to the TFTP server there is a networking conflict and instead of getting a progress bar made up of "#"s you will get a progress bar of "T"s; indicating a transmission error. It will make a number of attempts at connection before timing out. The instructions on Saving the Test indicate the proper time to connect the loop-back cables.
- If there is a chance the configuration file is corrupted, reconfigure the FortiGate device from the default settings.
- For HDD issue with multiple disks device, do not run HQIP because this will destroy the data. Ask for smart test or HDD diagnose command.
- There can be difficulties in loading the image on to a device that is configured to be FIPS compliant. If you suspect that this is the issue, make sure that you have a good copy of the configuration and perform a factory reset before attempting to load the HQIP image.
- There are a number of FortiAnalyzer and FortiMail models with a RAID card (FortiAnalzyer-2000, FortiMail-2000, FortiAnalzyer-2000A, FortiMail-2000A, FortiAnalzyer-4000A, FortiMail-4000A, etc). When conducting the HQIP test on any of the models with a RAID card, set the RAID level to 0 so that HQIP can test each hard disk.

Preparation

The secret to running a smooth HQIP is preparation. Get all of the components in place before you begin and the running of the test will be straight forward.

Downloading the Test

Before going to the Fortinet Service and Support web site there are a few things you will need:

- Valid account credentials on the Fortinet Service and Support site.

The account that you use should be the one that is associated with the FortiGate that you are going to be testing.

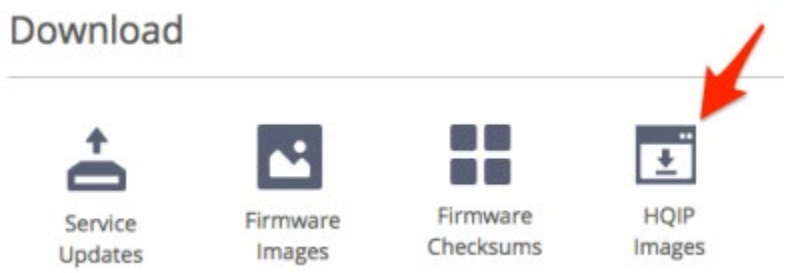
- Serial number of the device that you wish to run the HQIP test on.

Tip: if the device is racked, and you don't have the serial number already written down, rather than crawling around in back with pen and paper, use the camera on your phone to take a picture of the sticker with the serial number.

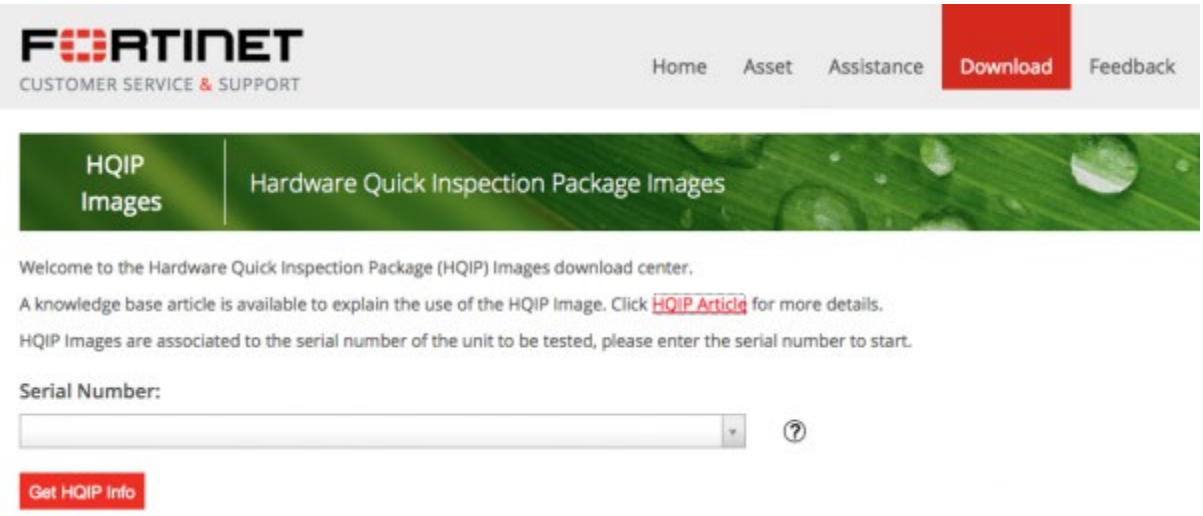
Once you have these pieces of information go to the Fortinet Service and Support web site and log in.

On the opening page, once you are in, you have 2 choices:

1. In the menu bar at the top of the page, hover the cursor over the **Download** text. This will reveal a drop down menu with **HQIP Images** as one of the possible selections.
2. Scroll down the **Downloads** section where you will find a number of icons representing the types of files that you can download.



Select the icon for HQIP firmware images. This should take you to a new web page.



This page has a field for you to enter the serial number of the Fortinet device that you will be testing.

As you enter the characters of the serial number it will begin searching through the serial numbers that are associated with the account that you are logged in as. Once you have entered enough numbers to select the correct serial number select the specific serial number of the device you will be testing.

This is the reason that you need to make sure that you use the account credentials that are associated with the device you will be testing. For most users that will not be an issue but for some organizations where departments will purchase their own equipment but the equipment is managed by a central IT department, this could be an issue. Third party IT service providers could also have problems downloading the correct version of the image if they are not using the customer's account and serial number.

Once you have entered the serial number in the field select the "Get HQIP Info" button.

The site will search the database of serial numbers, compare them to specific models and model version and present a HQIP image for you to download. The file name of the image shown is the link to download the image. Just click on it and use your browser as normal to save the file.

If you cannot get the correct HQIP image

If you have searched for but cannot find the correct HQIP image for your device the alternative approach is to open an RMA ticket at https://support.fortinet.com.

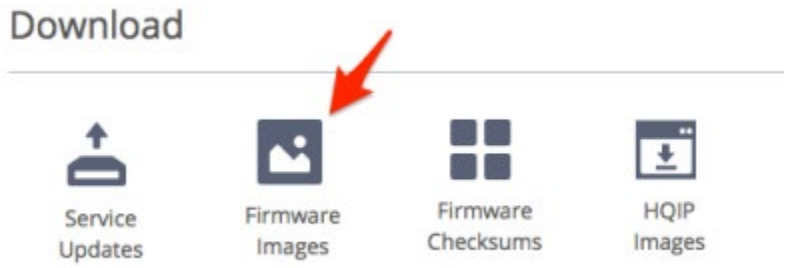
Downloading the Firmware

After the test, if there are no hardware issues you are going to want to load a nice fresh copy of the firmware on the device. I will be convenient if you already have the image on the computer that you have connected to the device being tested. If you don't already have it on your computer take the time to download it before starting the test.

The firmware and the HQIP images are found in almost the same location, so just like the HQIP test image you will need to have your Fortinet Service and Support web site credentials handy. Of course if you download both items at the same time you only have to log in once.

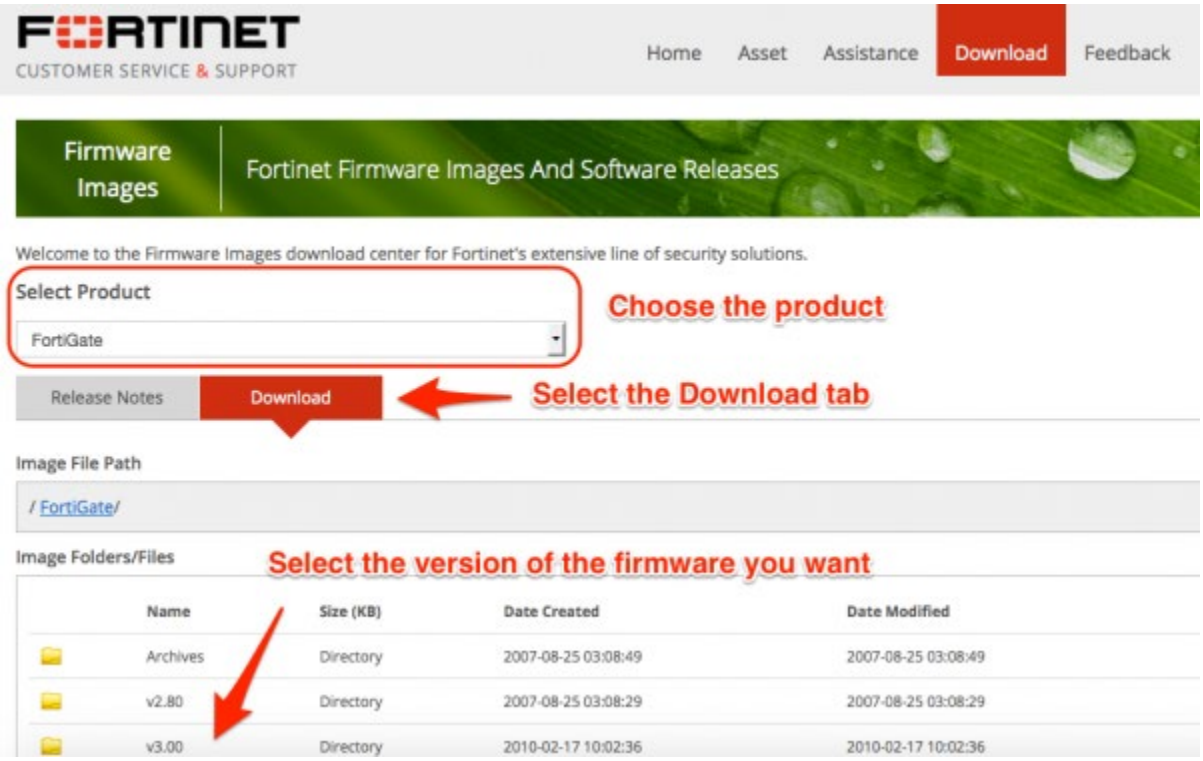
Once you have logged into the site and are on the opening page, once you are in, you have 2 choices:

1. In the menu bar at the top of the page, hover the cursor over the **Download** text. This will reveal a drop down menu with **Firmware Images** as one of the possible selections.
2. Scroll down the **Downloads** section where you will find a number of icons representing the types of files that you can download.



Select the icon for firmware images. This should take you to a new web page.

On this new page you will need to Select the product that you are looking to install the firmware on. Select the Download tab. Select the first number of the version number of the firmware's version.



You will be lead through a few more similar pages while you focus in on the specific version or build of firmware for your device until you arrive at a page that consists of a listing of all of the available firmware images, by model, for a single build/version of the firmware. The listing is alphabetical by file name and not incremental by model number so in the case of the FortiGate product the FortiGate 1000 will appear before the FortiGate 20 and while the FGT60D (FortiGate 60D) will be near the top of the list the FWF60D (FortiWiFi 60D) will be near the bottom.

Once you have found the image file that you are looking for select the HTTP link in the second from the right column to download the file. Select the Checksum link to download the checksum value of you want to verify that the file you downloaded is identical to the one on the server.

While other strategies can be used, a common one is to save the firmware image in a directory that is used by the TFTP server so that there is less to track down when it comes time to install the firmware.

Wiring the Device

The HQIP program will supply a wiring diagram should you want to test the interfaces.

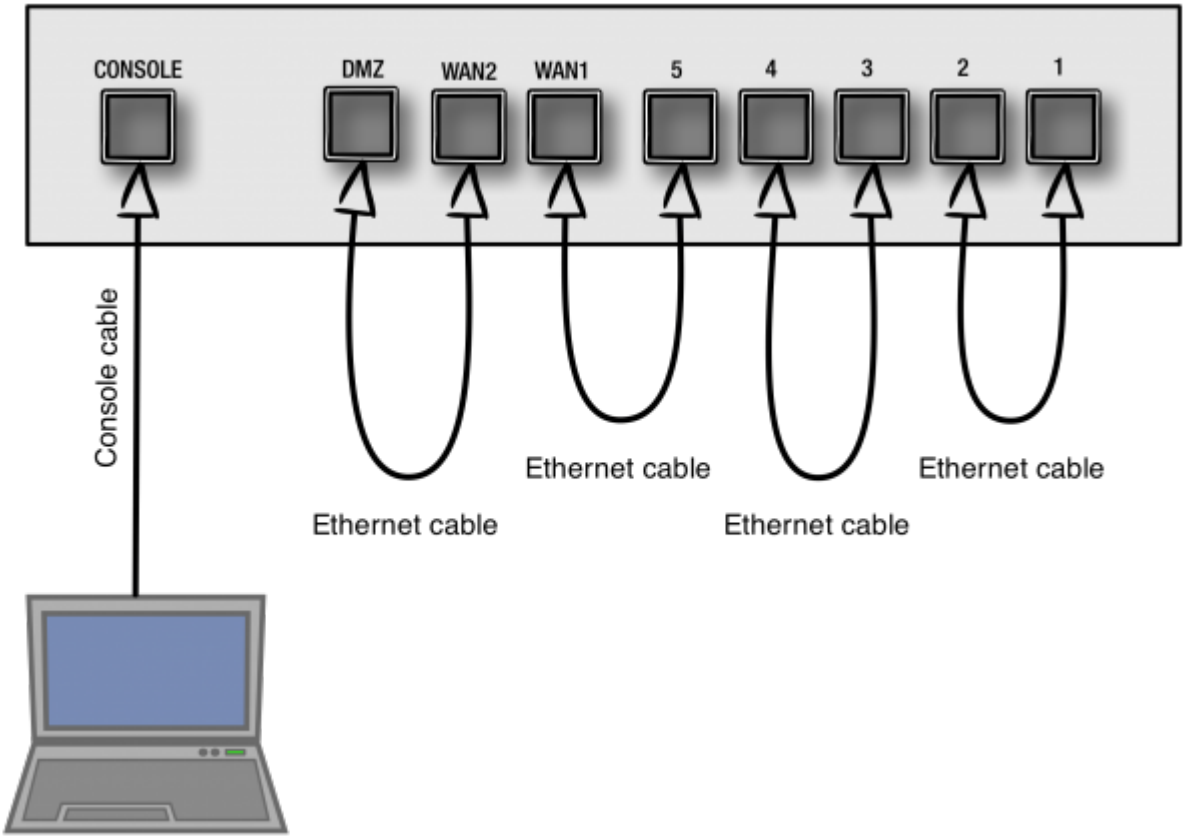
Because the various models have different numbers of physical interfaces, the wiring may in written into the test for each model.

The following is an example from the HQIP test of a FortiGate 60C:

```
Wire the network ports as follow for NIC loopback test.
       Internal
  [1]+-+ [3]+-+ [WAN1]+-+ [DMZ] [WAN2]
  [2]  | [4]  | [5]     |   |       |
   +   |  +   |  +      |   |       |
   +---+  +---+  +------+   +------+
```

If you do not immediately recognize that this is meant to be a wiring diagram, the translation is: Use Ethernet cables to connect

- Port 1 to Port 2
- Port 3 to Port 4
- Port WAN1 to Port 5
- Port DMZ to Port WAN2



Listing of Wiring Diagrams

This section has been set aside for any wiring diagrams that users wish to submit to the site. We encourage people to submit diagrams to this section as they use the HQIP test. These diagrams can be in the form of text-based descriptions or ASCII diagrams. Whenever possible we will take these and create a more easily readable graphical version.

Because:

- product lines and models are constantly being added
- products eventually do go out of support
- the HQIP test provides its own wiring map
- most people, once the test is completed just want to get back to work

this section will not likely contain many maps, but we thought that we would put forth the suggestion and space within the document.

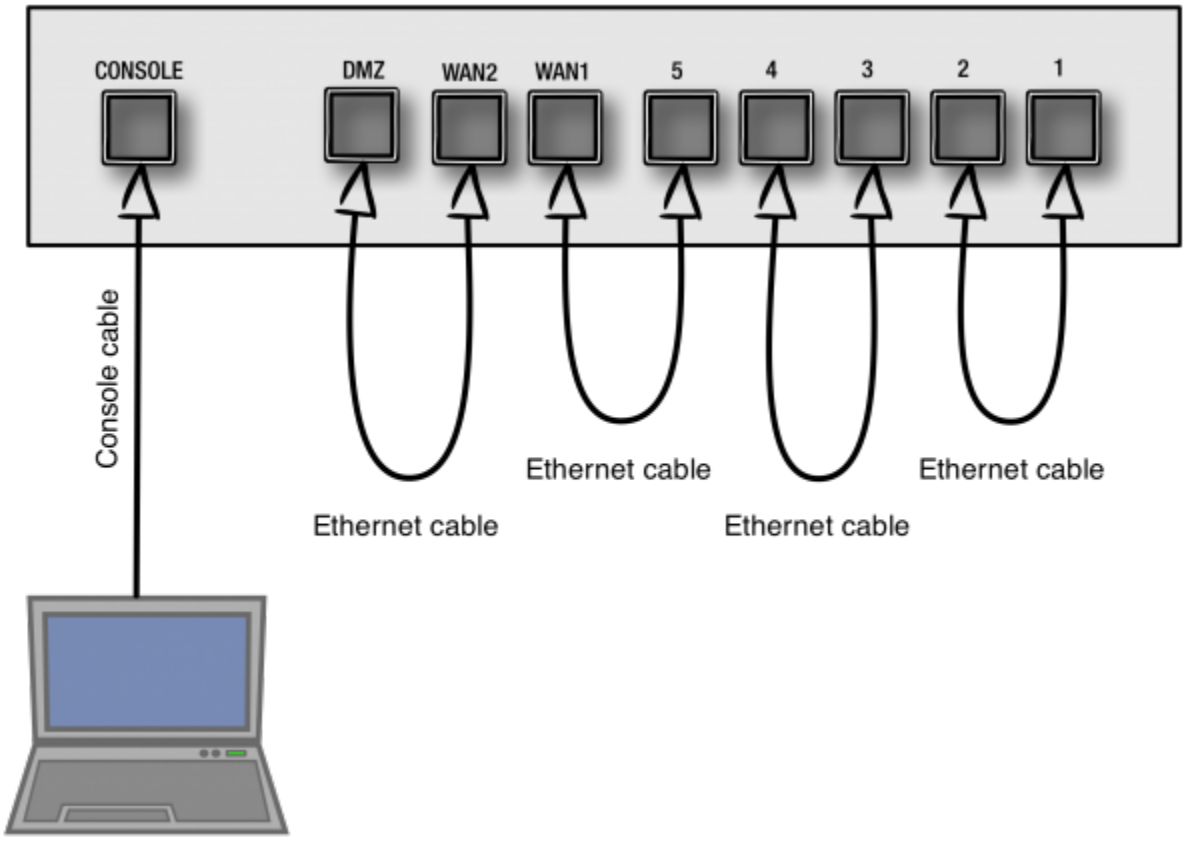
FortiGates

List of the available wiring diagrams for FortiGate devices.

FortiGate 60C
ASCII Diagram

```
      Internal
[1]+-+ [3]+-+ [WAN1]+-+ [DMZ] [WAN2]
[2]  | [4]  | [5]     |   |       |
 +   |  +   |  +      |   |       |
 +---+  +---+  +------+   +------+
```

Graphical Diagram



WiFi (Optional)

To correctly test WIFI from HQIP (for all Fortinet WIFI models), set up a wireless access point with the following parameters

SSID:	fwqc
IP address:	10.80.2.11

Console Connection

While there is a Console widget in the Web Based Manager (GUI) and in FortiExplorer as well, neither of these will work for the purposes of installing the HQIP image. These tools require that the device's firmware be loaded and up and running before they will work. Because the HQIP image needs to be installed from the BIOS, which is only accessible by interrupting the loading of the firmware a tool/application needs to be used that can talk directly to the BIOS. This tool is generally called a terminal emulator and the one that you use will depend on the operating system of the computer you are using. Almost every operating system, such as Windows, Linux and MacOS, will have a built-in version of this software. In the Unix like OSs it is usually referred to as Terminal which is like the Command prompt for Windows but there are commands that can be used to connect to

remoted devices. For Windows users, Hyper-terminal comes with the OS, but the most popular one is a free software application called Putty, downloadable off of the Internet.

Regardless of which application is used, there are some settings you will want use to connect to the Fortinet devices. Some tools will work well enough on the default or automatic settings but you may need to enter the following manually.

Normal Settings

Setting	Value
Bits per second:	9600
Data bits:	8
Parity:	none
Stop bits:	1
ASCII setup:	Append line feeds to incoming lines

Known exception(s)

FortiManager and FortiGate 300

Setting	Value
Bits per second:	115000
Data bits:	8
Parity:	none
Stop bits:	1
ASCII setup:	Append line feeds to incoming lines

Hardware

In devices that have a console port an appropriate cable will comes supplied with the device. It may not say on it, but it will be a null modem serial cable that has an internal pinning appropriate to the device. It is important to keep the cable that comes with the device. It is possible, because of internal pinning patterns within the cable that the cable from one model will not work on another. Most Fortinet devices will use the same standard cable, but there are rare exceptions.

TFTP server

TFTP is the protocol that is used to move the HQIP image, as well as other firmware images from your computer to the Fortinet Device being tested. These devices, like many networking devices, have a basic TFTP client built into the BIOS so that they can be firmware can be updated or upgraded.

There are a number of different TFTP servers, depending on the operating system of the computer that can be installed. A number of them are free. The best TFTP server is likely to be the one that you are most familiar with and comfortable using. If you've never used one before, there are a few listed in the Fortinet's SysAdmin Toolkit document that can be found in the SysAdmin Notebook section of the Fortinet Cookbook website.

While it is often the case that users will put the TFTP server on the computer that they are using to console into the Fortinet device, there is no rule that says this has to be the case. Some environments may have a computer on the network that is set aside as a common or centralized TFTP server so that there aren’t multiple copies of firmware on multiple machines. The only requirement is that the Fortinet device and the TFTP server can be placed on the same physical subnet, even if it is only for the duration of the transfer of the image file.

Connecting to the Device

There are a few configurations of connecting the to the Fortinet device and the basics of these configurations will be based on a combination of the scenarios below. Keep in mind that while the Computer with the terminal emulator and the computer hosting the TFTP server are most commonly the same computer, this is not a requirement. The only requirement for the TFTP server is that it be on the same physical subnet as the Fortinet device for the duration of the data transfer.

Terminal Emulator to the Console interface

Computer with built-in Serial Port			<->	Console Cable	<->	Console Cable
Computer without built-in Serial Port but with USB ports	<->	USB to Serial Adapter	<->	Console Cable	<->	Console Cable

Computer with the TFTP Server to the Enternet interface

TFTP Server				<->	Ethernet cable	<->	Ethernet interface indicated for model
TFTP Server	Ethernet cable	<->	Switch or Hub	<->	Ethernet cable	<->	Ethernet interface indicated for model

Some TFTP servers are more finicky than others when it comes to recognizing the Ethernet connection when there is no live device on the other end of the cable, such as when the device is being rebooted, so there may be confusion on the part of the computer in assigning an interface that is accessible to the TFTP server, so it can be an advantage to go through a network device to connect to the Ethernet interface on the Fortinet device. If you have some familiarity with the TFTP server you are using, you may be aware of whether or not this will be an issue.

* While not much of an issue anymore, some older computer network interfaces cannot automatically detect whether an Ethernet cable is connected to a network device or directly to another computer. If you have a network interface that cannot automatically determine whether to use MDI or MDI-X you may have to use a cross-over Ethernet cable if you are connecting directly to the Fortinet device from the TFTP server.

Running the Test

Make sure that everything you will need is on the computer(s)

Once you have started the test it is not likely that you will be able to connect to the Internet or in some cases even the rest of the network. You will not want to have to stop part way through to load up something you need.

Prepare the TFTP server

- Make sure that the TFTP server is up and running.
- Make sure that the TFTP server is listening on the correct network interface
- Make sure that the TFTP server is pointing at the directory with the HQIP test file image in it.

Prepare the cabling

- Connect the console cable from the computer to the device
- Connect the Ethernet cable to the TFTP server. If you know which interface on the device you will be connecting to in advance, you can make that connection as well. In some cases, you will have to wait until the test is running and tells you which interface to use, but you can always make sure the cable will reach before you start. Often the correct interface will be port 1 of the internal interfaces, but be prepared to change this if this is not the one your model uses.

Set the IP address of the TFTP server

- You don't have to do this first but it is a lot easier if you are not going back and forth between interfaces.
- The TFTP client on the Fortinet device will normally use 192.168.1.168 as a default IP address for the TFTP server so it is easiest to set the IP address of the TFTP server computer to this one. The client will give you the opportunity to inter an address manually so this is not a hard rule but a convenient option.

Initiate a console session

Make sure your computer is successfully connected to the device through a console session. You show be able to see a prompt and get responses to key strokes.

Reboot the device

The method of rebooting the device will depend on the model. Some models do not have power switches. The possible options for rebooting the device are:

- Use the Reboot feature in the GUI (if you have already reconfigured the IP address of your computer this may not be possible)
- Use the reboot command in the CLI (if you have already reconfigured the IP address of your computer this may not be possible)
- Use the power switch to turn the device of and on again (provided the device has such a switch)
- Disconnect and reconnect the power to the device

Interrupt the boot sequence

As the device is powering up you should see output on the console session. As soon as you see the "`Press any key to display configuration menu`" message, do so to interrupt the normal boot sequence. You need to get to the BIOS menu to load the test firmware.

Load the Test

Once the Configuration Menu is display you will have a number of options of what to do next.

```
[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 with default firmware.
[H]:  Display this list of options.

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

- At the selection window, select G.
- At the `Enter TFTP server address [192.168.1.168]:` prompt...

This is for assigning the IP address of the computer with the TFTP server.

- If you have already configured the computer with the default IP address, Pressing the Return key will use the default value of 192.168.1.168.
- If your TFTP server has a different IP address manually enter it here.

- At the `Enter local address [192.168.1.188]:` prompt...

This is for assigning the IP address of the Fortinet device. As long as it is in the same IP address subnet range as the TFTP server and doesn't conflict with any existing nodes on the network, you can use any IP address that you want.

- If you want to use the default IP address of 192.168.1.188, just press the Return key.
- If you want to use another IP address, manually enter it here.

- At the `Enter File Name [image.out]:` prompt...

This is for the name of the file on the TFTP server.

- Manually type in the name of the HQIP test file or cut and paste the name into which every terminal emulator program you are using. An example name is FORTIGATE-60C_HQIP_1900.IMG.
- The TFTP server is case sensitive with file names so make sure that the name used is correct.
- There is a default file name of image.out that can be used if you have renamed the HQIP test file in advance but it can be a bit of an administrative chore to keep renaming files back and forth.

The file transfer should be displayed on the TFTP server (ensure that the image is located in the appropriate folder), along with a series of hash "#" characters.

Saving the Test

After the image has been successfully received, you will be asked how you want the image saved.

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

When prompted with the choice to save as Default, save as Backup, or Run image without saving, Select "D" or "B" to save the image on the device. If the image is run without saving there is a risk of the test failing to run properly.

Once the test begins running, it does not pause to make changes to the setup. If you want to test the Ethernet interfaces and have the map, you might want to verify the loopback wiring is set up at this point before proceeding.

Functional check: The HQIP (Hardware Quick Inspection Package) test image is used to check the device’s system function and its interfaces. A console cable connection is required, and the entire console output must be logged to a file.

HQIP will check almost all components, including CPU, memory, CF, HD and PCI devices (NIC/ASIC). It will also check the critical benchmarks and system configurations. Observe the console output to make sure there is no warning stop or error message(s) from the test. For testing FortiGate 5000 and other models with backbone ports, the inner ports cannot be tested without specific configuration. If any errors or warning stops have occurred during this test, do not continue with the rest of steps 2 and go to Report.

Run the Test

Normally, the act of saving the HQIP image starts the test. However, there are some models, the test does not automatically start running once it is loaded. You will know if you have one of these models when nothing happens after the image file is loaded besides being given a command line prompt.

It will look something like this:

```
Enter firmware image file name [image.out]: FGT_3600C-
HQIP.3.0.0.1019.OUT
MAC:085B0E14D11F8
###################
Total 20491209 bytes data downloaded.
Verifying the integrity of the firmware image..

Total 69632kB unzipped.

Save as Default firmware/Backup firmware/Run image without
saving:[D/B/R]?R
.................................................................
Reading boot image 3956279 bytes.
Initializing firewall...ˇ

System is started.


Please press Enter to activate this console.
FORTITEST/FG3K56C3A1380262 ~#
```

The next step is to enter the command

```
diag hqip start
```

Once the test is started

The test will go through a number of step, most of them will not pause to wait for input.

The different sections of the test will be:

1. System information
2. Memory test
3. CPU test
4. Test Compact Flash and Harddisk.
5. Test USB ports.
6. Test Network interface controller.
7. Test SDHC LED.
8. Test NIC LEDS.
9. Test HA/STATUS LEDS.

There will be output and status indicators through each step of the test but there will also be a summary at the end of the test laid out in the following format:

```
============== Fortinet Hardware Quick Inspection Report
==================


                   BIOS Integrity Check:      PASS
      System Configuration Verification:      PASS
                            Memory Test:      PASS
                               CPU Test:      PASS
                               USB Test:      PASS
                          HD/FLASH Test:      PASS
                 Network Controller Test:      PASS
                            SDHC LED Test:      PASS
                             NIC LED Test:      PASS
                        HA/ALARM LED Test:      PASS


========== Fortinet Hardware Quick Inspection <xxx PASS xxx>
==============
```

Save the Output

The HQIP test can be run at any time you choose for your own information but if the purpose is for use in the RMA process it is best to record the output to a text file to send in to verify the results and make the RMA process smoother.

The method of saving the output to a text file will depend on the terminal emulator. Some of them will have built in features that can transfer the output to a file while with others you might have to do some cutting and pasting.

After the Test

Restore the Firmware

If all the tests passed successfully, then you will want to restore the firmware. For two reasons you will want to install a recently downloaded version of the firmware from the support site. However, the build should be the same as the one that was on the device before the test.

1. At the beginning of the test process, if you chose to save the image as the default image the HQIP test will load any time the device is rebooted. If you chose to save it as a backup firmware image and something goes wrong with the primary there will be no backup so it is best to reestablish a proper configuration of default and backup images during a single planned outage rather than have a second outage at a later point in time.
2. Presumably, if you are running the HQIP test it must be because something is not working as expecting. This would be a good time to reinstall a pristine copy of the firmware. At the very least this would eliminate the firmware installation as a potential source of any issues that you're having. If you do this, it also makes sense to take the opportunity to include formatting the hard drive as part of the process. At the configuration menu, before selecting `[G]`, select the `[F]` option.

Installing a fresh copy of the firmware is the procedure as installing the HQIP test. The only difference is that instead of using the name of the HQIP image file, the name of the firmware image file should be used.

RMA

If the test shows a failure, the next step is to work with the Technical Assistance Center. Verify whether that the device is still under warranty. Depending on the symptoms that initiated that lead the test and the results of the test, they may want to verify that it is not a false positive, but for the most part there should be very little difficulty in requesting a RMA.