

## Support Guide: Managing the Subject machine's Firewall.

*Note: This guide assumes you have successfully deployed F-Response to the subject/target machine. If not, then we recommend you look at one of the many Mission Guides for your version of F-Response. All F-Response Mission Guides are available at [www.f-response.com](http://www.f-response.com) under Mission Guides and Documentation.*

### Contents

It may be the Firewall if.....	2
Firewall Exceptions .....	2
Windows Firewalls .....	4
Windows 2000.....	4
Windows 2003.....	4
XP and Vista.....	5
Windows 7.....	7
Apple Firewalls.....	9
OSX version .....	9
OSX 10.4 and 10.5 .....	10
OSX 10.6 .....	11
OSX 10.7 and 10.8 .....	12
Linux Firewalls.....	13

## It may be the Firewall if...

If there are problems starting or deploying F-Response, the first place to investigate is the F-Response Messages tab. The following message panel errors point to potential firewall interference:

### **Error - <COMPUTER> could not send TCP data to License Manager.**

This is most often a firewall on the examiner machine. Disable the firewall on the examiner machine and try starting F-Response on the subject machine.

### **Error - Could not receive TCP data from License Manager, could this be a firewall issue for <COMPUTER>.**

This indicates information from the F-Response License Manager was not received by the subject machine. Check to make sure the Firewall on the subject machine is disabled.

### **iSCSI operation failed for <COMPUTER>. Connection Failure. Cannot establish network connectivity with target, please check the Firewall on target machine.**

F-Response uses port 3260 to communicate with the target machine's resources. As stated in this message, this port is being blocked, check the subject machine's firewall is disabled to allow access to the machine.

### **Error - Could not connect to License Manager, is the License Manager IP and Port correct for <COMPUTER>.**

This common error message indicates the subject machine is unable to locate the license manager running on the examiner machine. It is not necessarily firewall related.

Often an Examiner is using a laptop with the wireless interface enabled while plugged into the network thereby having two network connections. Ideally, the Examiner will be connected to the Subject machine over the wired interface. Check to make sure F-Response was configured and deployed with the correct IP (the wired network) and port number for the License Manager on the Examiner machine.

## Firewall Exceptions

While the simplest solution is to disable the local firewall on the Examiner and Subject machines, in a large corporate environment there may be an enterprise level firewall in place. In this case the Network Administrator for the site will need to make the necessary port exceptions to allow for F-Response to run on the network.

F-Response uses the following ports to communicate on the network:

3260 – This is the main port F-Response uses to communicate with the target machine’s resources (iSCSI TCP).

\*3261—This is the port the F-Response FlexDisk option uses to communicate with the target machine should you choose to enable it (HTTPS).

5681 – This port is used to communicate with the F-Response Licensing Manager. (TCP is used for most editions of F-Response, UDP is used for F-Response Tactical Edition).

\*Optional port. Not needed if FlexDisk is not enabled.

\*\*Note all of these ports have the option of being changed to utilize a different port if necessary.

## Windows Firewalls

Windows Operating System's firewall settings windows generally contain the following tabs:

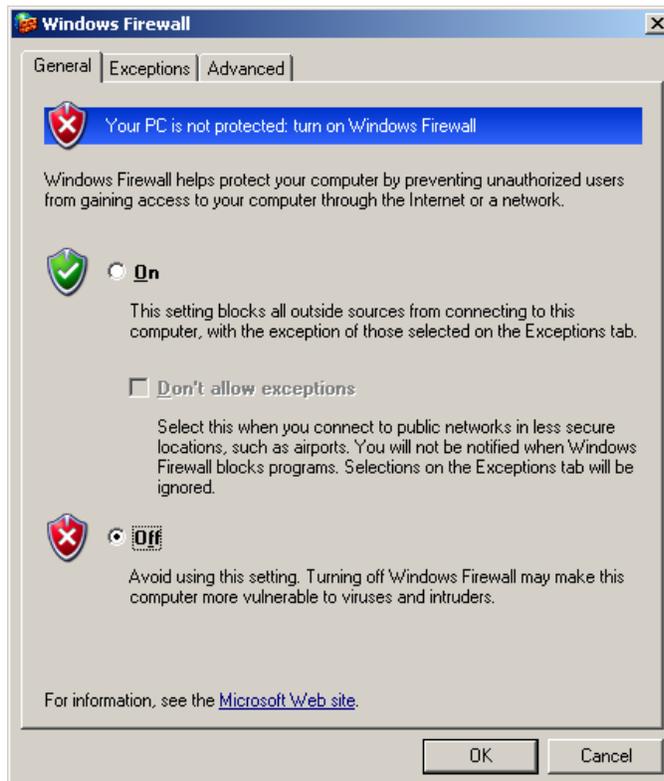
- The "General" tab: The main switch, allows you to turn the firewall on and off. There is also a check box to disable all exceptions that may have been made to the firewall.
- The "Exceptions" tab: Here you can add programs, services, and ports that will be allowed to communicate through the firewall.
- The "Advanced" tab: Contains additional configuration options for logging and enabling or disabling the firewall for different interfaces (network connections).

The steps to access the Windows Firewall vary slightly according to which operating system you are running:

### Windows 2000

Windows 2000 does not have a built in firewall.

### Windows 2003



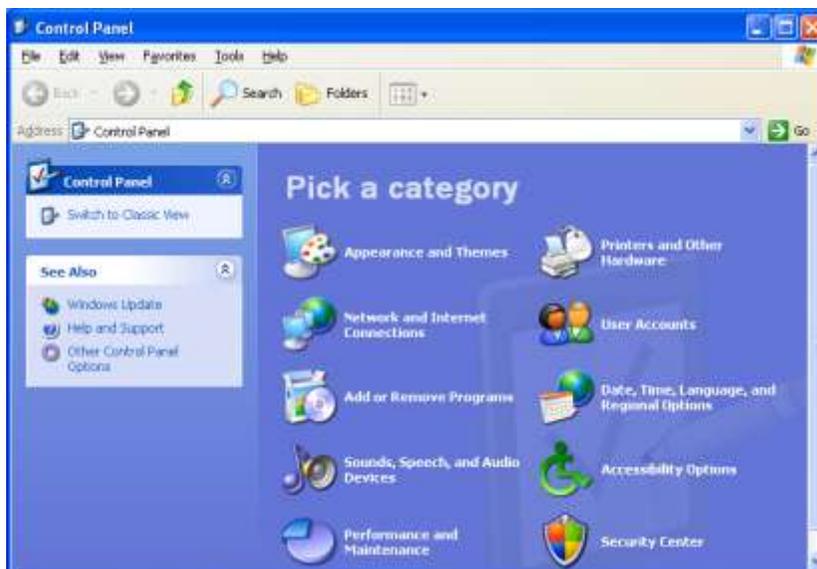
The firewall on a Windows 2003 server can be found by clicking the Start button and going to: Settings|Control Panel|Windows Firewall. Here under the General Tab the firewall can be disabled by choosing the **Off** option button.

## XP and Vista

Locating the firewall on the XP or Vista OS will depend up the view enabled for the desktop. Begin by clicking the Start button. Go to Control Panel and look for the Windows Firewall among the options listed:



This is the list of options if you have the “Classic View” enabled (notice the option to switch to Category view in the upper left).



If the Windows firewall is not listed among the options here, Windows is most likely in Category view as seen here:

In Category View, click on “Security Center”, then choose the Windows Firewall option in the next window that appears.

## Manage security settings for:

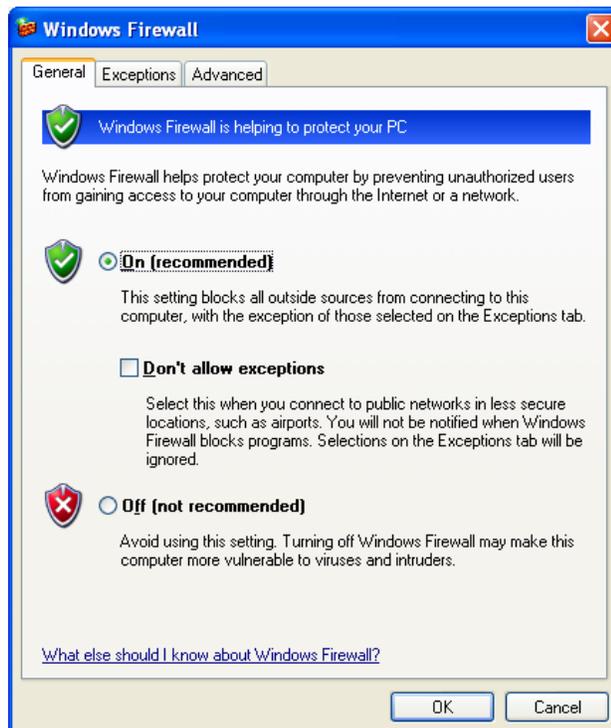


Internet Options



Windows Firewall

Regardless, either view will ultimately lead to the same settings window for the built in firewall. Here the firewall can be disabled by choosing the option button to turn off the firewall.



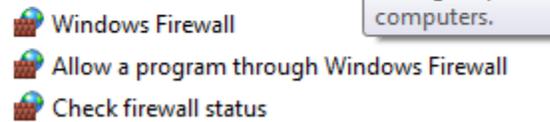
## Windows 7

To locate the Windows firewall on a Windows 7 OS, click the Start button and open Control Panel, then Windows Firewall, then choose Advanced Settings.

### Programs (1)



### Control Panel (4)



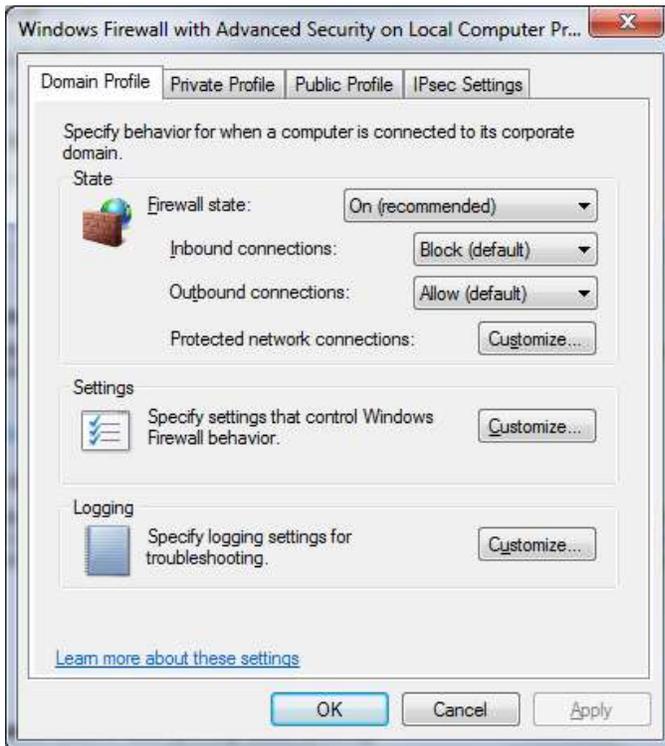
Or, simply click the Start button and type “firewall” into the search field. An option for “Windows Firewall with Advanced Security” will appear in the results list—choose this option.

The Windows Firewall with Advanced Security window will appear:



In the Windows 7 OS, there are three different default policies for the firewall that apply depending on the network you are connected to: Public, Private, and Domain. The easiest solution is to temporarily disable each firewall profile. Click on the blue “Windows Firewall Properties” hyperlink.

The Windows Firewall configuration window will open. This window will allow access to each Firewall Profile State.



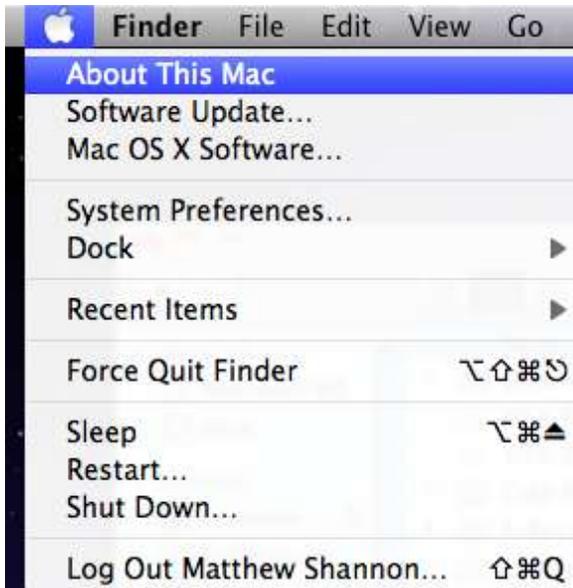
The firewall state can be changed to "Off" under the Domain, Private, and Public tabs. Change each Profile state to off and click the Apply button.

(If the Domain Profile is grayed out, you most likely do not have permissions to make the change and will need to work with the Network Administrator to make an exception for you.)

## Apple Firewalls

### OSX version

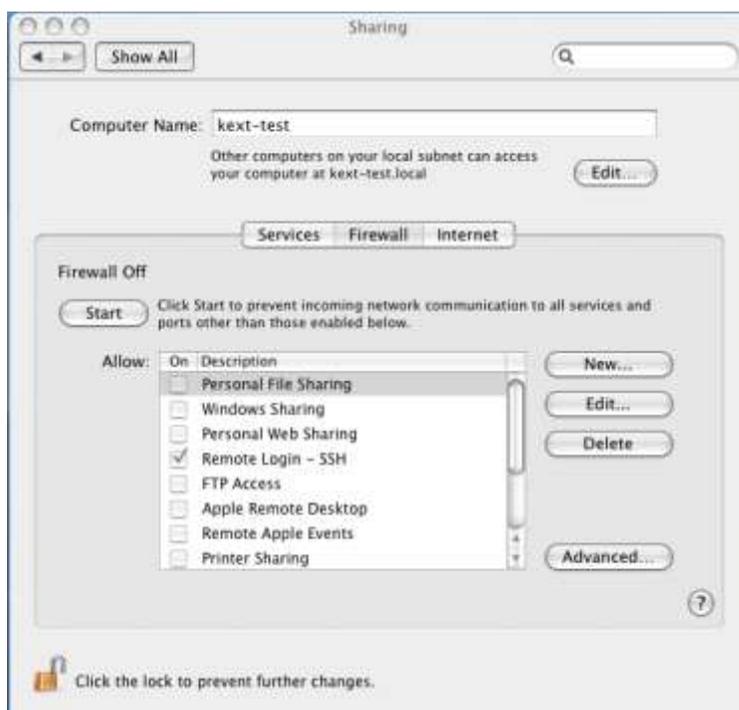
In order to locate the firewall on an Apple machine, the version of OSX running must be determined. The OSX version can be found by clicking the Apple icon and choosing “About this Mac” from the menu.



The OSX version number can be seen here in the “About This Mac” window.

## OSX 10.4 and 10.5

To locate the firewall on OSX version 10.4 or 10.5, click the apple icon and choose “System Preferences” from the menu. When the “System Preferences” window opens, from the “View” menu, select “Security.”



Or, simply click on the “Sharing” icon under the Internet & Network section.

Select the firewall button to access the firewall. Click the Stop button to disable the firewall. Note, if the padlock icon in the lower left side corner is closed, click on it and input the Administrator credentials to change the firewall state.

## OSX 10.6

To locate the firewall on OSX version 10.6, click the apple icon and choose “System Preferences” from the menu. When the “System Preferences” window opens, from the “View” menu, select “Security.”



Select the firewall tab to access the firewall. Click the Stop button to disable the firewall. Note, if the padlock icon in the lower left side corner is closed, click on it and input the Administrator credentials to change the firewall state.



## OSX 10.7 and 10.8

To locate the firewall on OSX version 10.7 or 10.8, click the apple icon and choose “System Preferences” from the menu. When the “System Preferences” window opens, select “Security & Privacy.”



The Security & Privacy window will open.



Select the firewall tab to locate the option to turn the firewall on or off. Note, if the padlock icon in the lower left side corner is closed, click on it and input the Administrator credentials to change the firewall state.

## Linux Firewalls

Linux firewalls vary heavily by distribution and release, in addition they can often be challenging for a casual Linux user to control and navigate. We recommend you defer to the Linux administrator in this instance and provide them with the [aforementioned ports and protocols](#).