

Trusted Sites & Proxy Exceptions

Internet Explorer Trusted Sites

Some computers are set up to only allow access to sites that are in the Trusted Sites for their security zone. If the HFS web sites are not in this zone, our web services may not be able to connect to the HFS web sites. In addition to adding the HFS web sites to the Trusted Sites, the client may need to also make changes to their firewall settings to allow our software to access the Internet outside of the Internet Explorer application.

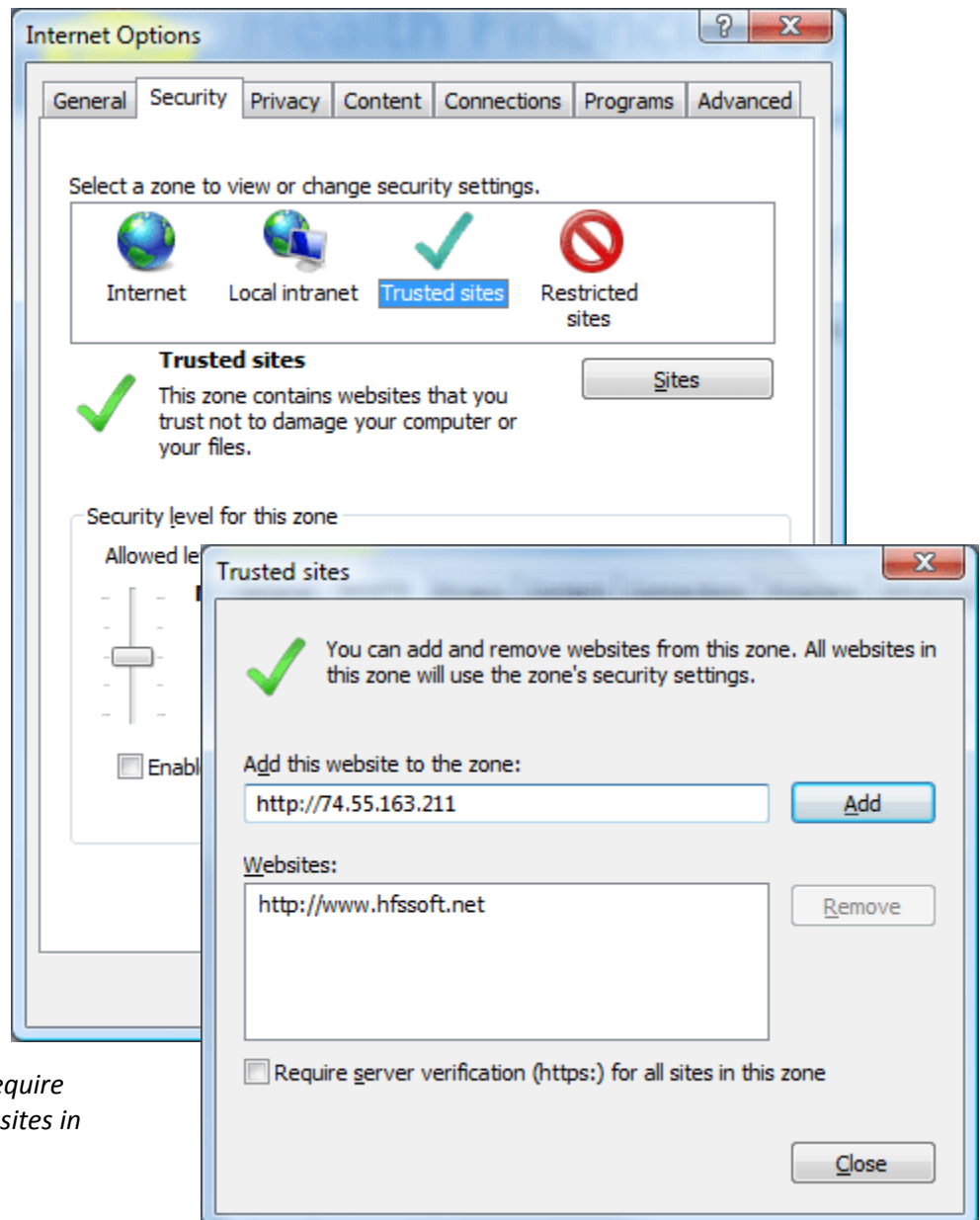
To add HFS web sites to the list of Trusted Sites, open Internet Explorer and select Internet Options from the Tools menu. On the Internet Options screen, select the Security tab. (Note: If you do not have a Security tab, contact your IT department to have them update your Trusted Sites.) On the Security tab, select Trusted sites and then press the Sites button.

On the Trusted sites screen, add the following web sites:

<http://www.hfssoft.com>
<http://www.hfssoft.net>
<http://74.55.163.211>

You will need to uncheck the “Require server verification (https:) for all sites in this zone” option.

After entering the web site addresses, click the Close button and then click the Ok button on the Internet Options screen.

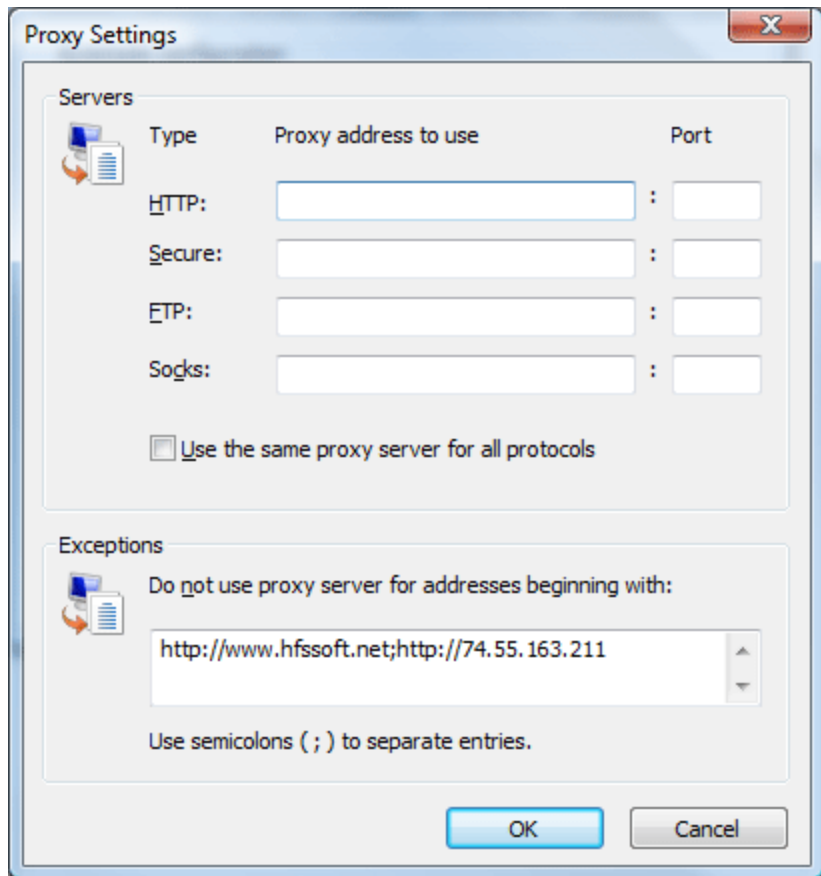


Proxy Exceptions

When using a proxy server to access the Internet it is sometimes necessary to add the HFS web sites to the list of web sites that do not require the proxy server.

It is recommended that only clients experienced with proxy servers change these settings.

To add the proxy server exceptions, open the Proxy settings screen from the Internet Options LAN Advanced Settings screen. In the Exceptions box add the HFS web sites as shown in the image at right. Note: You can also add the hfssoft.com site but this is generally not required.



Adding proxy exceptions

assumes that the computer has Internet access without the proxy server. If the computer only has Internet access through the proxy server then setting these exceptions will have no effect.

Important Note: In most proxy cases the user cannot manually configure their computer to allow access to a server that has not been identified by their company as a trusted site. If they could, the company would not be using the proxy server configuration. In this case, the user must contact their IT department and request that the HFS web sites be added to the list of allowed domains that can be accessed by the proxy server. These domains are:

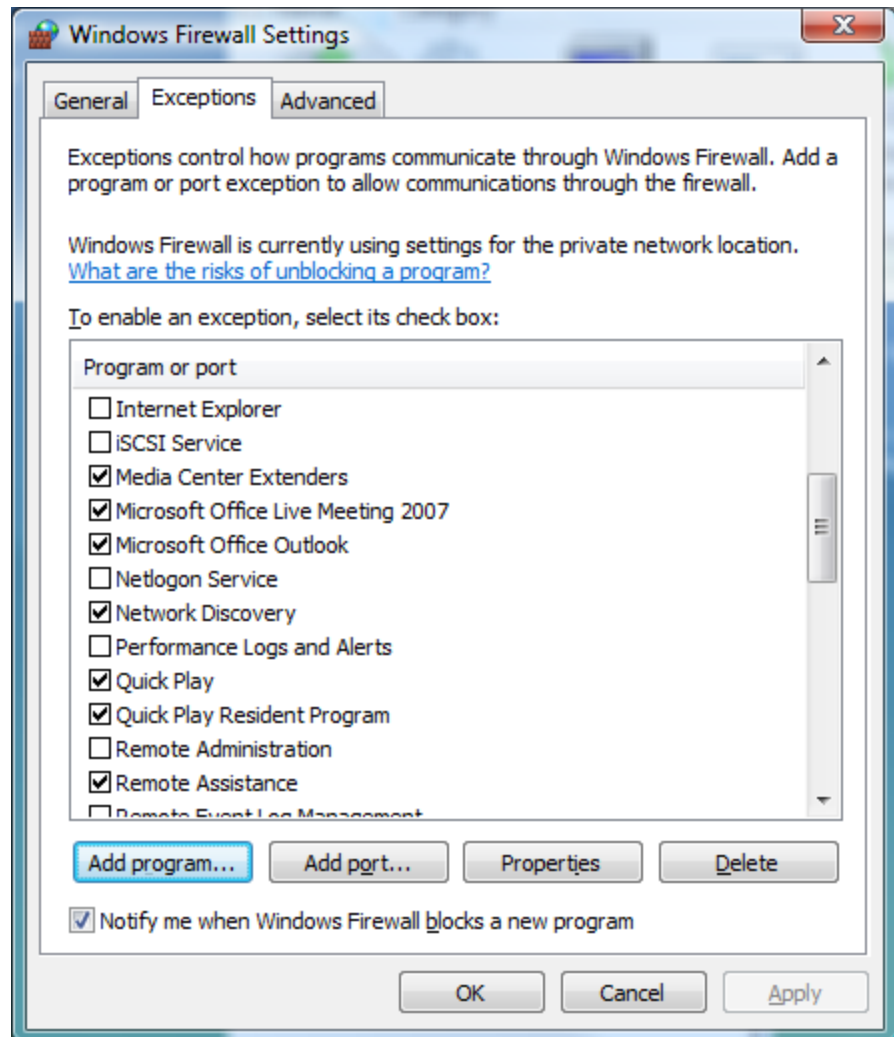
http://www.hfssoft.com
http://www.hfssoft.net
http://74.55.163.211

The above domains need to be added to your proxy server exception list (“white list”) if such a list is used by your company. Contact your IT department to request these domains be added to that list. If your computer uses this white list, any changes you make locally will have no affect on your proxy authorization.

Windows Firewall

Most computers have a firewall installed that helps prevent unwanted Internet access by rogue programs. Windows Firewall can be told to allow a program through the firewall when it is attempting to access the Internet. The MCRIF32 program itself uses the Internet Explorer security settings so has an easier time getting through the firewall. However, the HFS update program cannot use Internet Explorer and as a result, might be blocked by the firewall.

Please note that most computers do not need their firewall changed as this is the least common problem that causes it to not have Internet access.



To allow the HFS update program through Windows Firewall, open the Windows Firewall Settings dialog and press the Add program button.

In the Add a Program dialog, press the Browse button and look for the HFS update program called W32MUPDI.EXE. This program is located in the same folder where your MCRIF32 software is located (usually C:\MCRIF32). Select the W32MUPDI.EXE program and press the OK button.

Press the OK button on the Add a Program dialog, then press the OK button on the Windows Firewall Settings dialog.

Many companies restrict access to the firewall settings so contact your IT department if you do not have access to these settings.