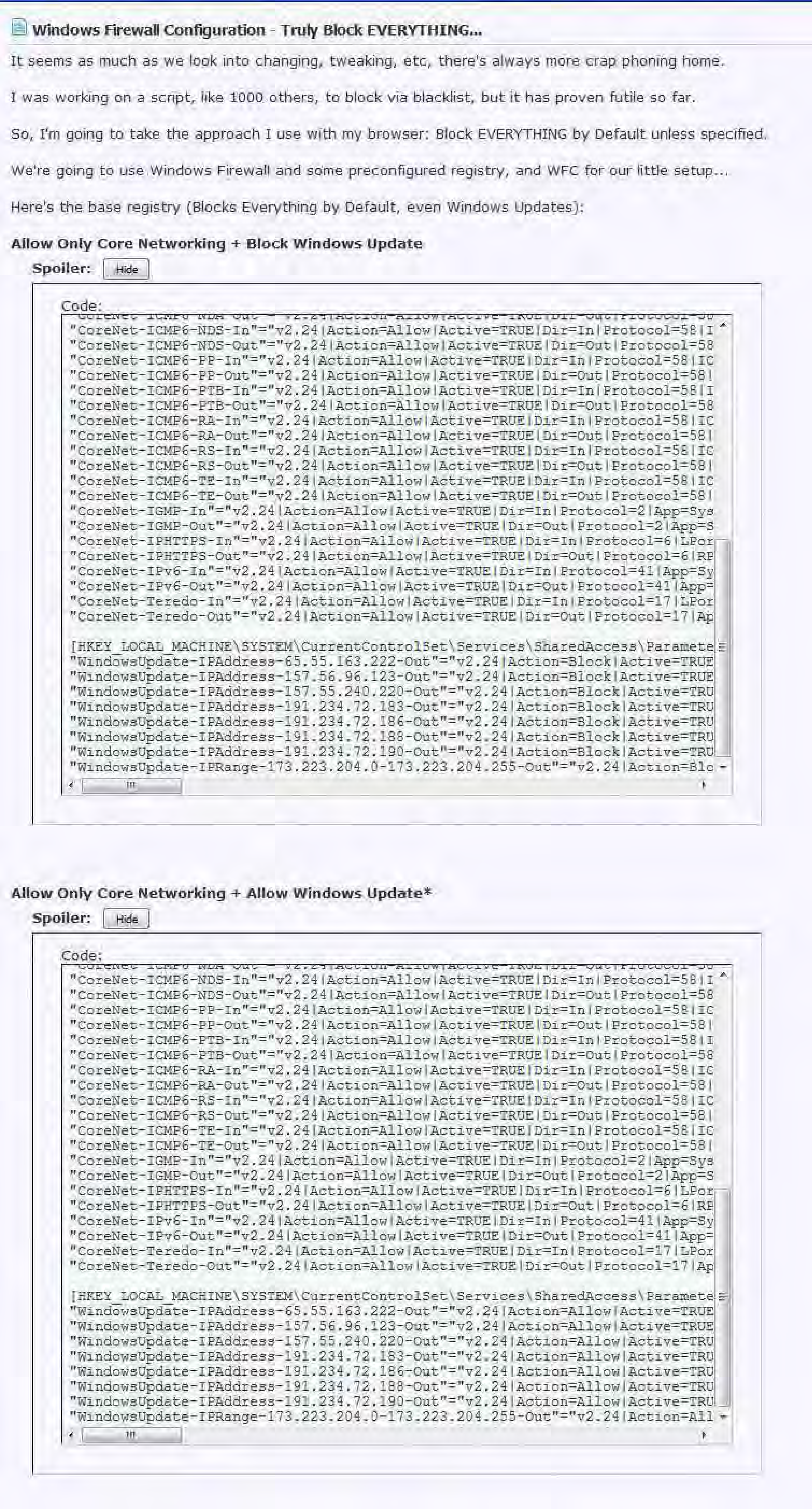


Windows Firewall Configuration - Truly Block EVERYTHING...

It seems as much as we look into changing, tweaking, etc, there's always more crap phoning home.

I was working on a script, like 1000 others, to block via blacklist, but it has proven futile so far.

So, I'm going to take the approach I use with my browser: Block EVERYTHING by Default unless specified.

We're going to use Windows Firewall and some preconfigured registry, and WFC for our little setup...

Here's the base registry (Blocks Everything by Default, even Windows Updates):

Allow Only Core Networking + Block Windows Update

Spoiler: Hide

Code:

```
"CoreNet-ICMP6-NDA-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58
"CoreNet-ICMP6-NDS-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=58|I
"CoreNet-ICMP6-NDS-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58
"CoreNet-ICMP6-PP-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=58|IC
"CoreNet-ICMP6-PP-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58|
"CoreNet-ICMP6-PTB-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=58|I
"CoreNet-ICMP6-PTB-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58
"CoreNet-ICMP6-RA-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=58|IC
"CoreNet-ICMP6-RA-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58|
"CoreNet-ICMP6-RS-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=58|IC
"CoreNet-ICMP6-RS-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58|
"CoreNet-ICMP6-TE-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=58|IC
"CoreNet-ICMP6-TE-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58|
"CoreNet-IGMP-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=2|App=Sys
"CoreNet-IGMP-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=2|App=S
"CoreNet-IPHTTPS-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPor
"CoreNet-IPHTTPS-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=6|RP
"CoreNet-IPv6-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=41|App=Sy
"CoreNet-IPv6-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=41|App=
"CoreNet-Teredo-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=17|LPor
"CoreNet-Teredo-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=17|Ap

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Paramete
"WindowsUpdate-IPAddress-65.55.163.222-Out"="v2.24|Action=Block|Active=TRUE
"WindowsUpdate-IPAddress-157.56.96.123-Out"="v2.24|Action=Block|Active=TRUE
"WindowsUpdate-IPAddress-157.55.240.220-Out"="v2.24|Action=Block|Active=TRU
"WindowsUpdate-IPAddress-191.234.72.183-Out"="v2.24|Action=Block|Active=TRU
"WindowsUpdate-IPAddress-191.234.72.186-Out"="v2.24|Action=Block|Active=TRU
"WindowsUpdate-IPAddress-191.234.72.188-Out"="v2.24|Action=Block|Active=TRU
"WindowsUpdate-IPAddress-191.234.72.190-Out"="v2.24|Action=Block|Active=TRU
"WindowsUpdate-IPRange-173.223.204.0-173.223.204.255-Out"="v2.24|Action=Blo
```

Allow Only Core Networking + Allow Windows Update*

Spoiler: Hide

Code:

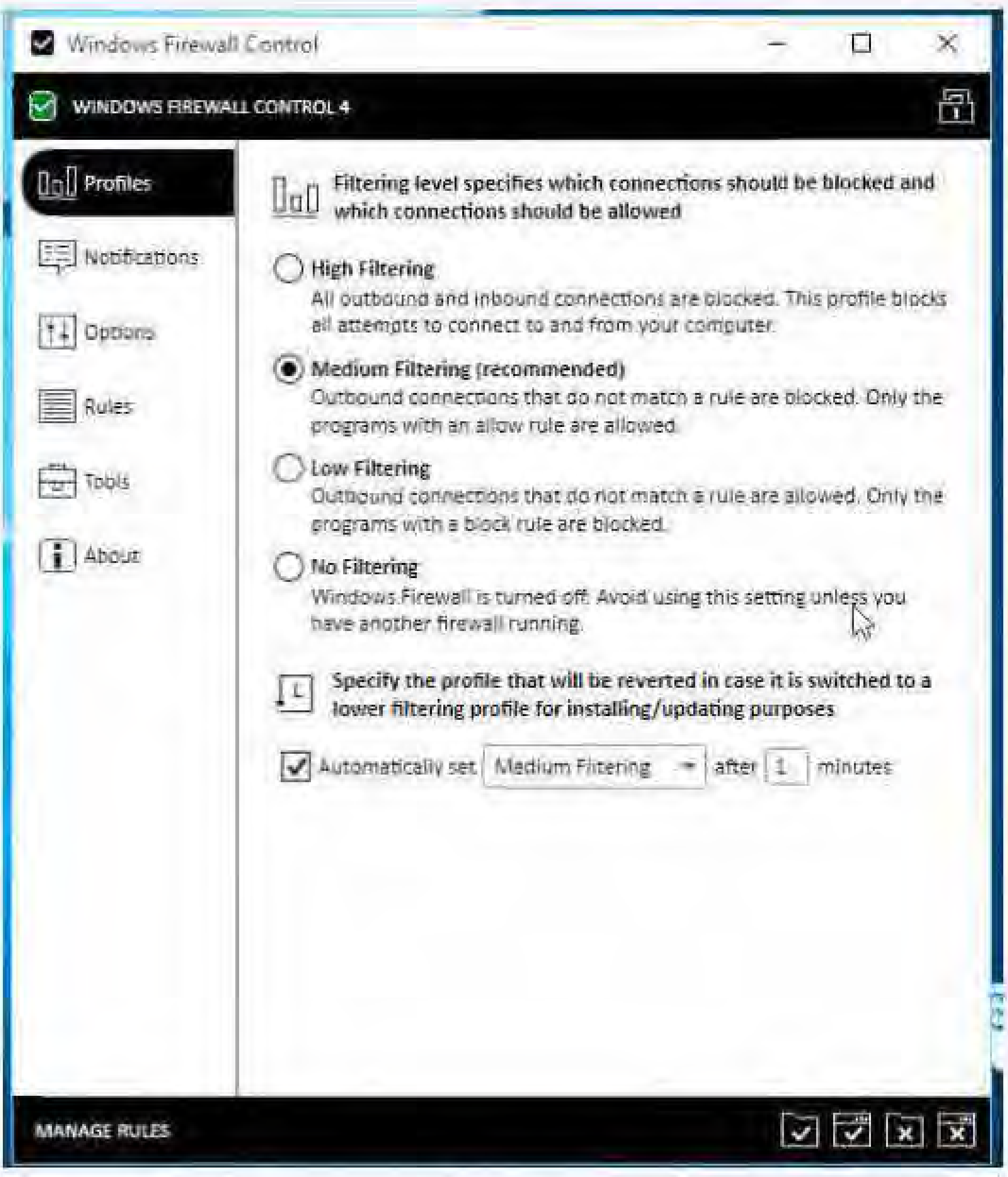
```
"CoreNet-ICMP6-NDA-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58
"CoreNet-ICMP6-NDS-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=58|I
"CoreNet-ICMP6-NDS-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58
"CoreNet-ICMP6-PP-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=58|IC
"CoreNet-ICMP6-PP-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58|
"CoreNet-ICMP6-PTB-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=58|I
"CoreNet-ICMP6-PTB-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58
"CoreNet-ICMP6-RA-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=58|IC
"CoreNet-ICMP6-RA-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58|
"CoreNet-ICMP6-RS-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=58|IC
"CoreNet-ICMP6-RS-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58|
"CoreNet-ICMP6-TE-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=58|IC
"CoreNet-ICMP6-TE-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=58|
"CoreNet-IGMP-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=2|App=Sys
"CoreNet-IGMP-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=2|App=S
"CoreNet-IPHTTPS-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPor
"CoreNet-IPHTTPS-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=6|RP
"CoreNet-IPv6-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=41|App=Sy
"CoreNet-IPv6-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=41|App=
"CoreNet-Teredo-In"="v2.24|Action=Allow|Active=TRUE|Dir=In|Protocol=17|LPor
"CoreNet-Teredo-Out"="v2.24|Action=Allow|Active=TRUE|Dir=Out|Protocol=17|Ap

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Paramete
"WindowsUpdate-IPAddress-65.55.163.222-Out"="v2.24|Action=Allow|Active=TRUE
"WindowsUpdate-IPAddress-157.56.96.123-Out"="v2.24|Action=Allow|Active=TRUE
"WindowsUpdate-IPAddress-157.55.240.220-Out"="v2.24|Action=Allow|Active=TRU
"WindowsUpdate-IPAddress-191.234.72.183-Out"="v2.24|Action=Allow|Active=TRU
"WindowsUpdate-IPAddress-191.234.72.186-Out"="v2.24|Action=Allow|Active=TRU
"WindowsUpdate-IPAddress-191.234.72.188-Out"="v2.24|Action=Allow|Active=TRU
"WindowsUpdate-IPAddress-191.234.72.190-Out"="v2.24|Action=Allow|Active=TRU
"WindowsUpdate-IPRange-173.223.204.0-173.223.204.255-Out"="v2.24|Action=All
```

What we've done here, is removed all preset rules to ensure nothing is pre-whitelisted, except the most core guts of Networking. Blocking those = nothing will work at all, totally broken. You chose whether to accept/block Windows Updates.
***IMPORTANT: Windows Update IPs may vary from person or region. Those were what I needed for it to work.**

Now, we're going to use Windows Firewall Control for easier management. Configure exactly as depicted in the screenshots...

1. Profiles:

Spoiler: Hide



Filtering level specifies which connections should be blocked and which connections should be allowed

○ High Filtering
All outbound and inbound connections are blocked. This profile blocks all attempts to connect to and from your computer.

● Medium Filtering (recommended)
Outbound connections that do not match a rule are blocked. Only the programs with an allow rule are allowed.

○ Low Filtering
Outbound connections that do not match a rule are allowed. Only the programs with a block rule are blocked.

○ No Filtering
Windows Firewall is turned off. Avoid using this setting unless you have another firewall running.

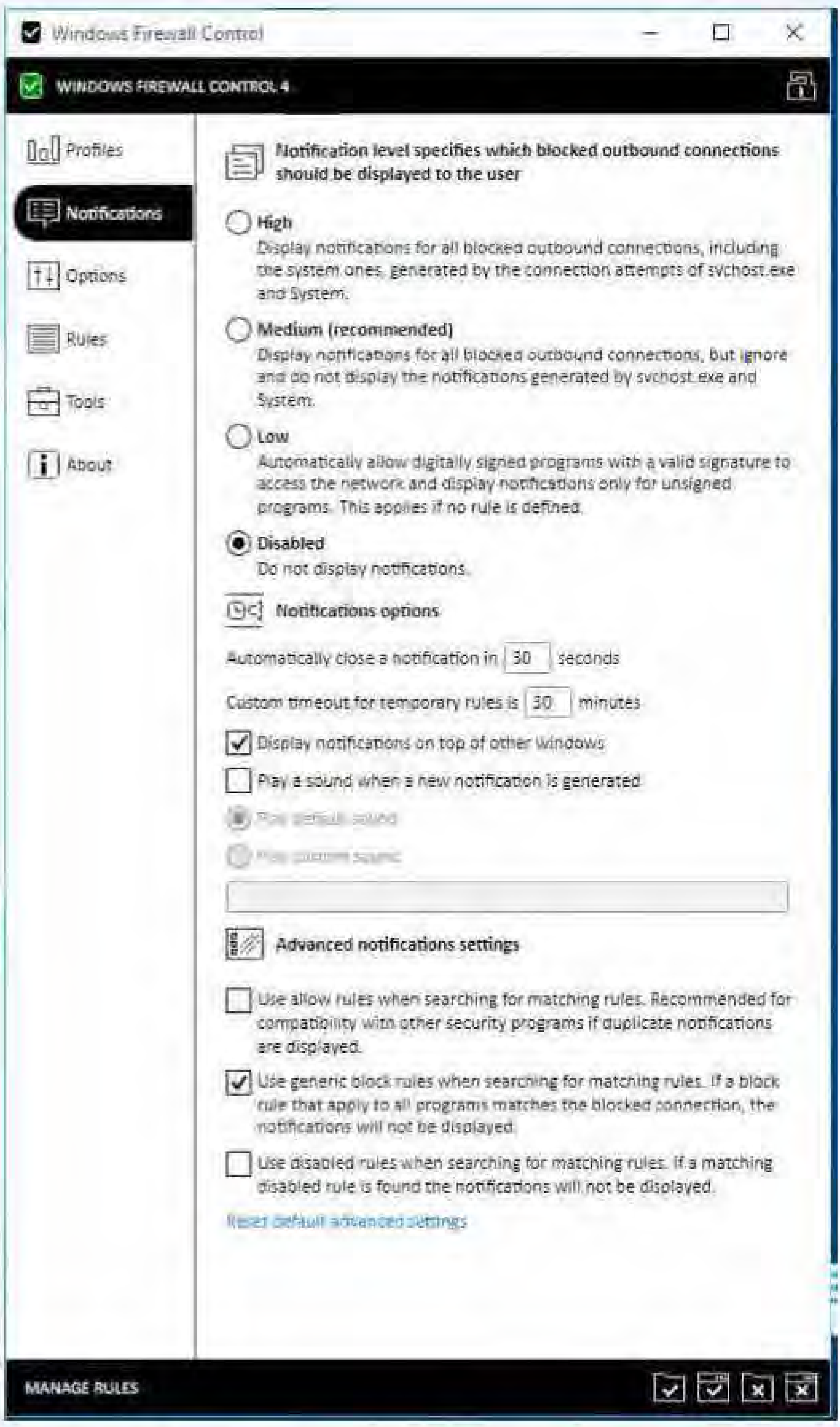
Specify the profile that will be reverted in case it is switched to a lower filtering profile for installing/updating purposes

☑ Automatically set Medium Filtering after 1 minutes

This ensures everything you haven't allowed, will be blocked. High Blocks EVERYTHING, no matter what, as if you disabled your internet. Also, there's a 1 minute option. You could quickly lower/deactivate Firewall, but make sure it comes back up.

2. Notifications

Spoiler: Hide



Notification level specifies which blocked outbound connections should be displayed to the user

○ High
Display notifications for all blocked outbound connections, including the system ones, generated by the connection attempts of svchost.exe and System.

○ Medium (recommended)
Display notifications for all blocked outbound connections, but ignore and do not display the notifications generated by svchost.exe and System.

○ Low
Automatically allow digitally signed programs with a valid signature to access the network and display notifications only for unsigned programs. This applies if no rule is defined.

● Disabled
Do not display notifications.

Notifications options

Automatically close a notification in 30 seconds

Custom timeout for temporary rules is 30 minutes

☑ Display notifications on top of other windows

☐ Play a sound when a new notification is generated

● Play default sound

○ Play custom sound

Advanced notifications settings

☐ Use allow rules when searching for matching rules. Recommended for compatibility with other security programs if duplicate notifications are displayed.

☑ Use generic block rules when searching for matching rules. If a block rule that apply to all programs matches the blocked connection, the notifications will not be displayed.

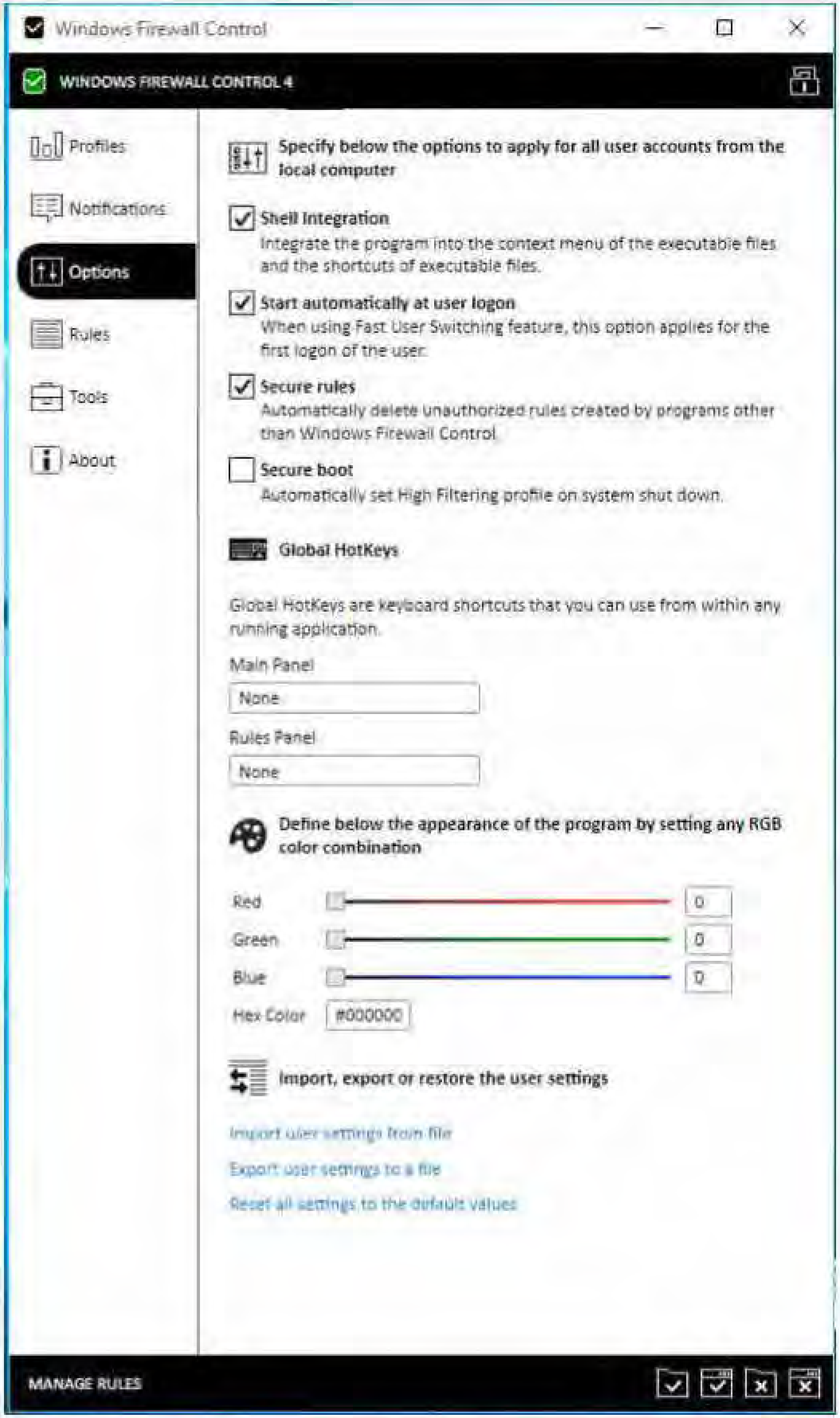
☐ Use disabled rules when searching for matching rules. If a matching disabled rule is found the notifications will not be displayed.

Reset default advanced settings

Altogether, we disable notifications and any leniency. You'll be bombarded otherwise.

3.Options

Spoiler: Hide



Specify below the options to apply for all user accounts from the local computer

☑ **Shell Integration**
Integrate the program into the context menu of the executable files and the shortcuts of executable files.

☑ **Start automatically at user logon**
When using Fast User Switching feature, this option applies for the first logon of the user.

☑ **Secure rules**
Automatically delete unauthorized rules created by programs other than Windows Firewall Control.

☐ **Secure boot**
Automatically set High Filtering profile on system shut down.

Global HotKeys

Global HotKeys are keyboard shortcuts that you can use from within any running application.

Main Panel: None

Rules Panel: None

Define below the appearance of the program by setting any RGB color combination

Red: 0
Green: 0
Blue: 0
Hex Color: #000000

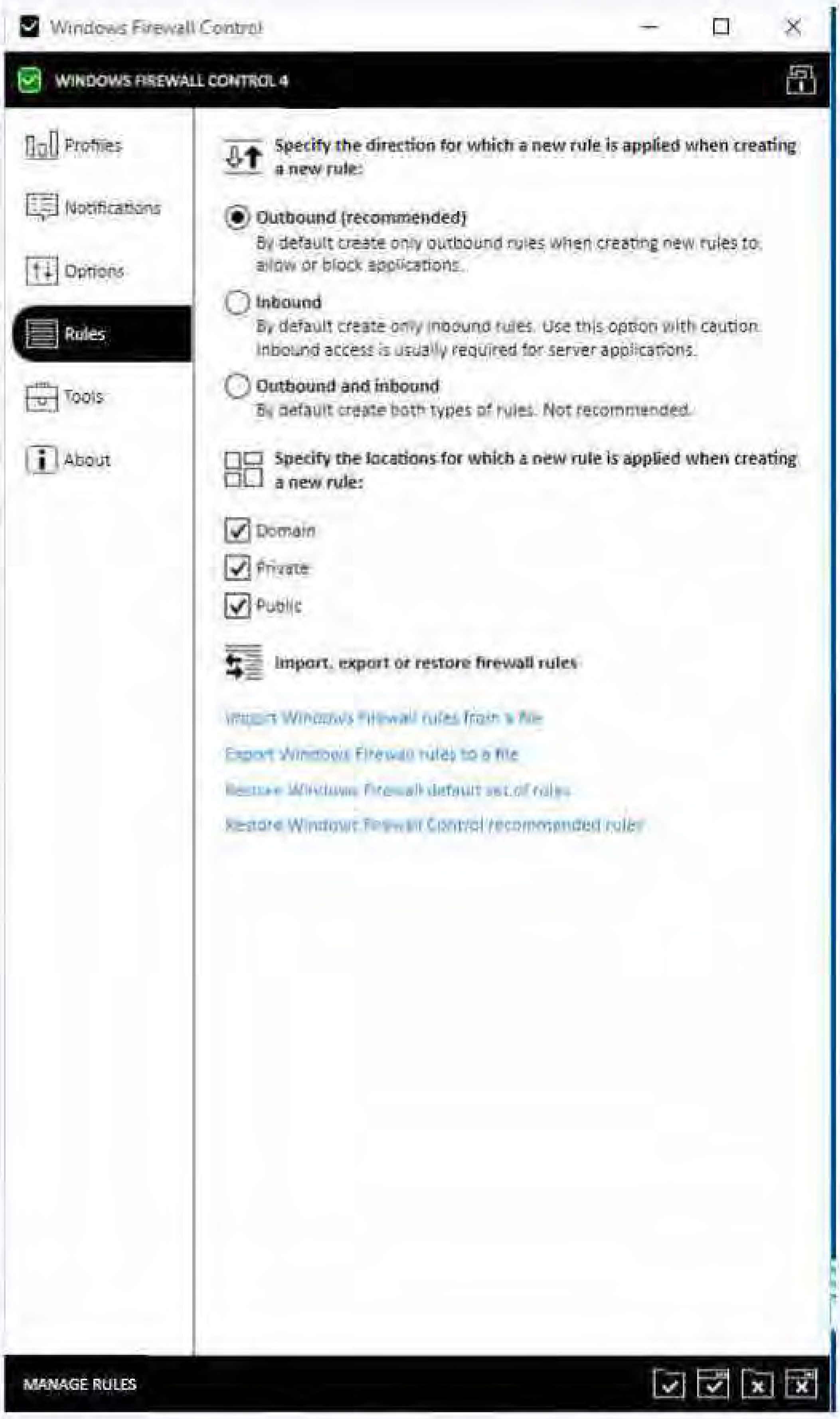
Import, export or restore the user settings

Import user settings from file
Export user settings to a file
Reset all settings to the default values

Easy Right Click to Whitelist, Disable anything else from tampering with rules, and autostart WFC. (I didn't use Secure Boot, as it would kill my TeamViewer on reboot, as you have to manually downgrade to Medium from High every restart if you enable this).

4. Rules

Spoiler: Hide



Specify the direction for which a new rule is applied when creating a new rule:

● Outbound (recommended)
By default create only outbound rules when creating new rules to allow or block applications.

○ Inbound
By default create only inbound rules. Use this option with caution. Inbound access is usually required for server applications.

○ Outbound and inbound
By default create both types of rules. Not recommended.

Specify the locations for which a new rule is applied when creating a new rule:

☑ Domain
☑ Private
☑ Public

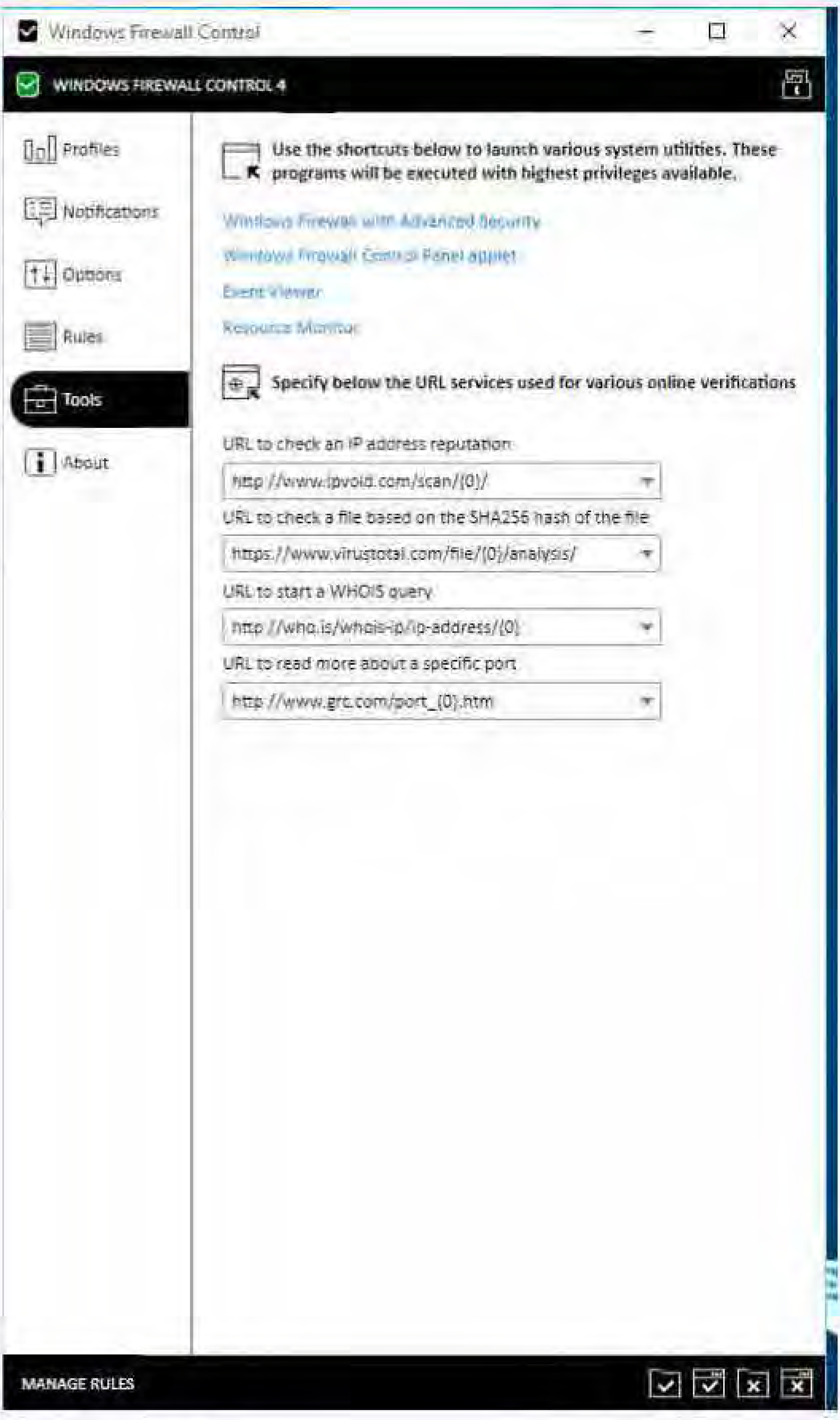
Import, export or restore firewall rules

Import Windows Firewall rules from a file
Export Windows Firewall rules to a file
Restore Windows Firewall default set of rules
Restore Windows Firewall Control recommended rules

Apply for all connection profile types, and let's not blanket allow Incoming Connections. Most apps don't need them.

5. Tools

Spoiler: Hide



Use the shortcuts below to launch various system utilities. These programs will be executed with highest privileges available.

Windows Firewall with Advanced Security
Windows Firewall Control Panel applet
Event Viewer
Resource Monitor

Specify below the URL services used for various online verifications

URL to check an IP address reputation
http://www.ipvoid.com/scan/{0}/

URL to check a file based on the SHA256 hash of the file
https://www.virustotal.com/file/{0}/analysis/

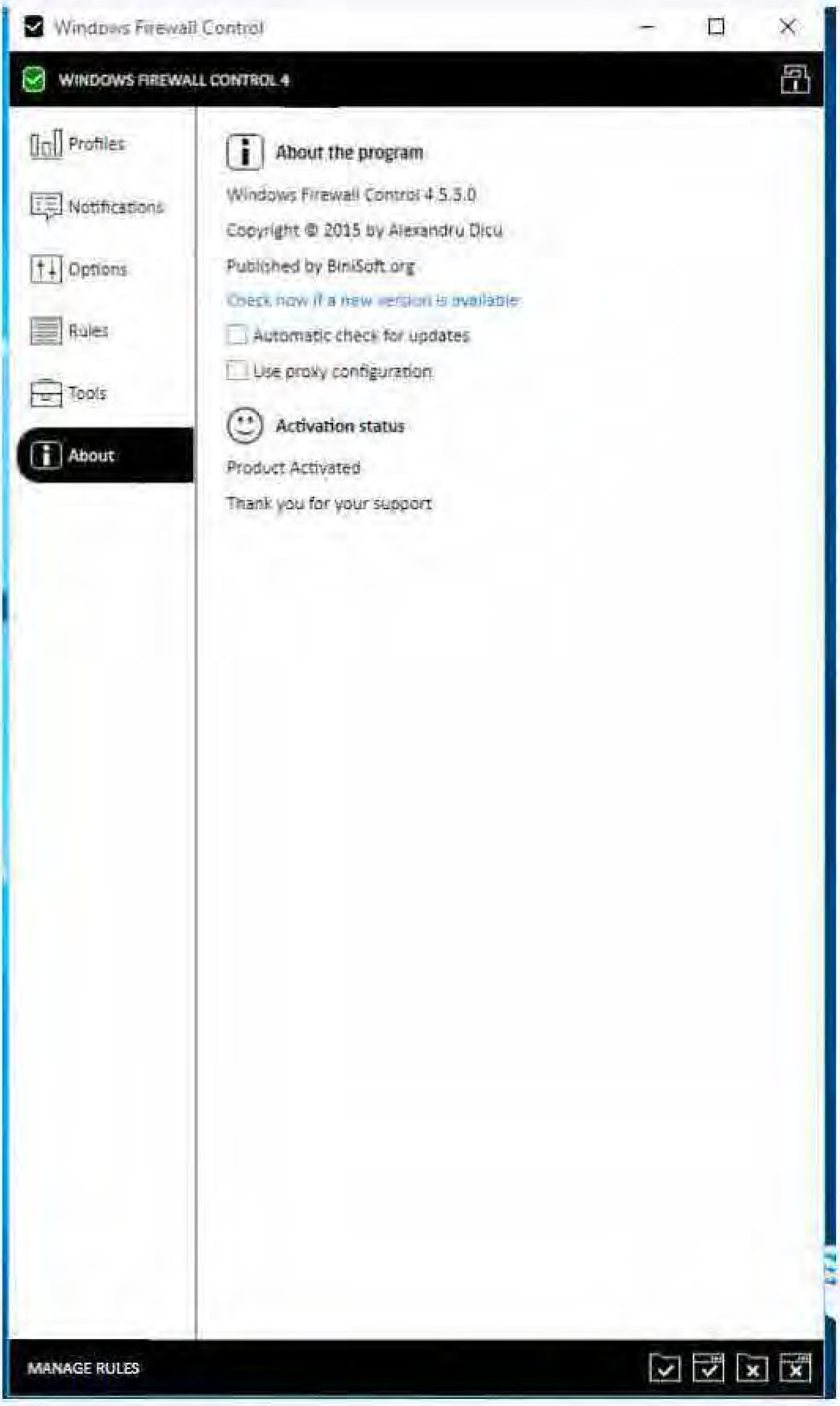
URL to start a WHOIS query
http://who.is/whois-ip/ip-address/{0}

URL to read more about a specific port
http://www.grc.com/port_{0}.htm

Leave this section alone.

6. About

Spoiler: Hide



About the program

Windows Firewall Control 4.5.5.0

Copyright © 2015 by Alexandru Dicu

Published by BiniSoft.org

Check now if a new version is available

☐ Automatic check for updates

☐ Use proxy configuration

Activation status

Product Activated

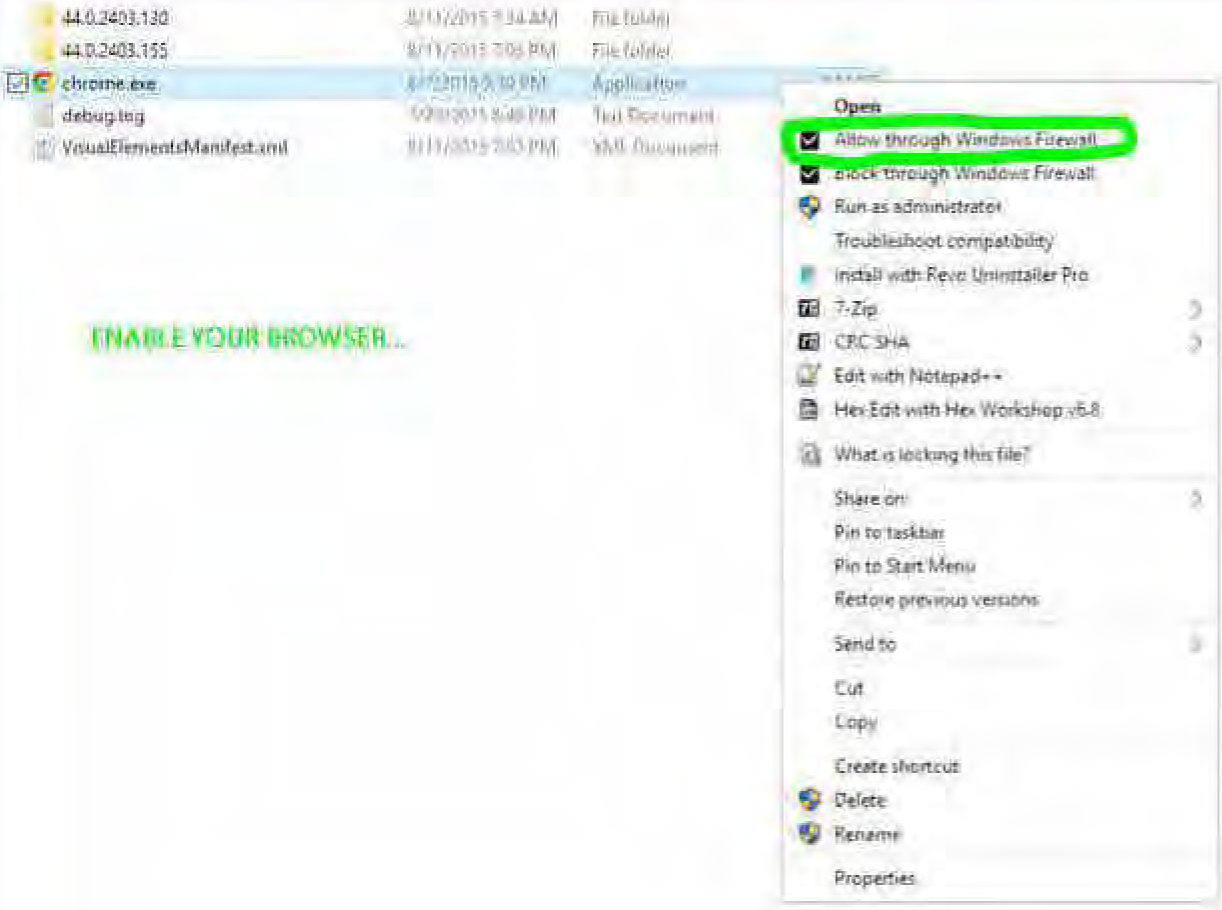
Thank you for your support

I disabled the auto-update.

Whitelisting Programs:

Spoiler: Hide

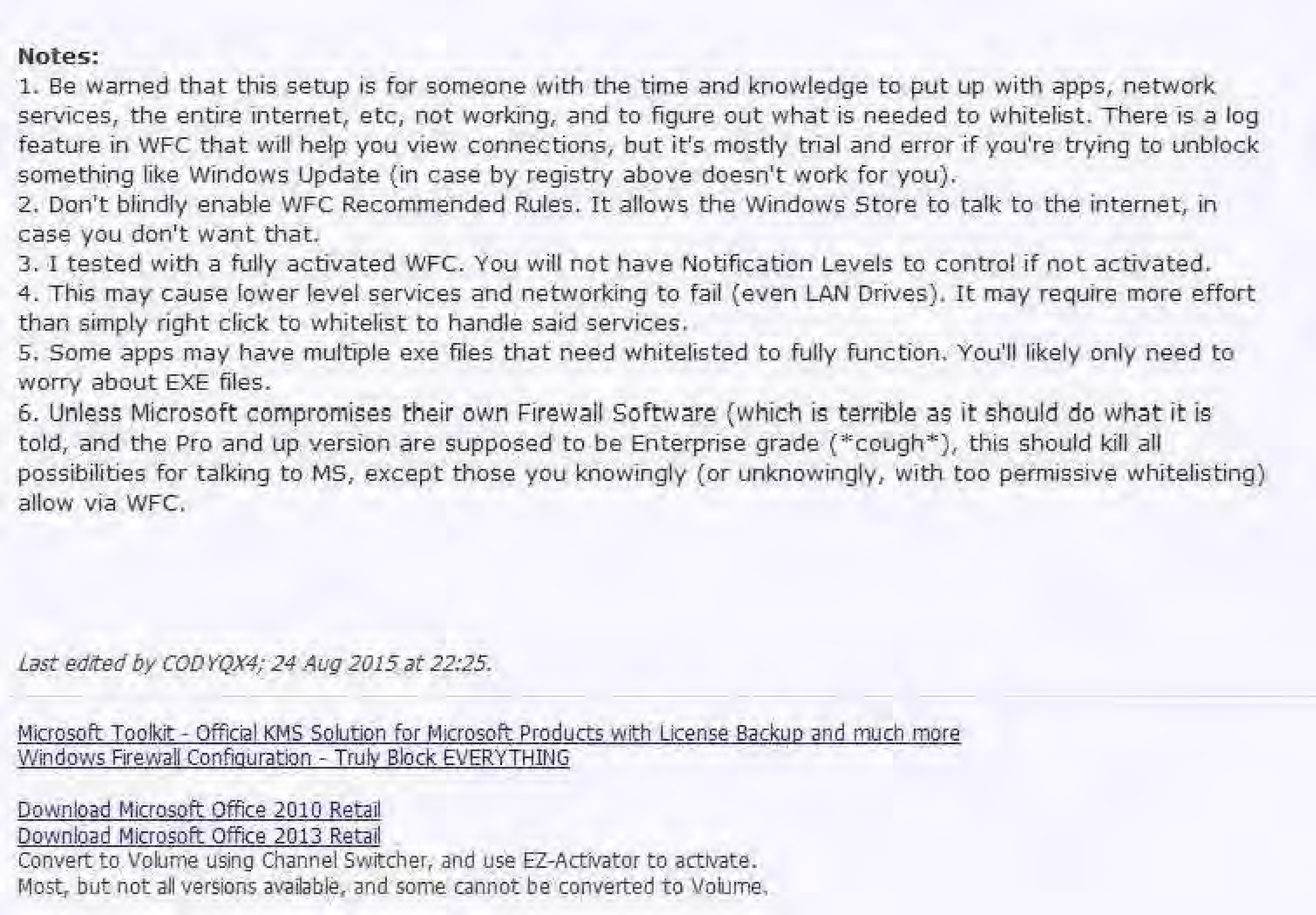
Now, find apps that you want to use the internet, right click them, and whitelist them:



44.0.2403.130	8/11/2015 1:34 AM	File folder
44.0.2403.155	8/11/2015 7:06 PM	File folder
☑ chrome.exe	8/12/2015 5:30 PM	Application
debug.log	10/3/2015 8:48 PM	Text Document
VisualElementsManifest.xml	8/11/2015 7:03 PM	XML Document

Open
Allow through Windows Firewall
Block through Windows Firewall
Run as administrator
Troubleshoot compatibility
Install with Revo Uninstaller Pro
7-Zip
CRC SHA
Edit with Notepad++
Hex Edit with Hex Workshop v6.8
What is locking this file?
Share on
Pin to taskbar
Pin to Start Menu
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties

ENABLE YOUR BROWSER...



Notes:

1. Be warned that this setup is for someone with the time and knowledge to put up with apps, network services, the entire internet, etc, not working, and to figure out what is needed to whitelist. There is a log feature in WFC that will help you view connections, but it's mostly trial and error if you're trying to unblock something like Windows Update (in case by registry above doesn't work for you).
2. Don't blindly enable WFC Recommended Rules. It allows the Windows Store to talk to the internet, in case you don't want that.
3. I tested with a fully activated WFC. You will not have Notification Levels to control if not activated.
4. This may cause lower level services and networking to fail (even LAN Drives). It may require more effort than simply right click to whitelist to handle said services.
5. Some apps may have multiple exe files that need whitelisted to fully function. You'll likely only need to worry about EXE files.
6. Unless Microsoft compromises their own Firewall Software (which is terrible as it should do what it is told, and the Pro and up version are supposed to be Enterprise grade (*cough*), this should kill all possibilities for talking to MS, except those you knowingly (or unknowingly, with too permissive whitelisting) allow via WFC.

Last edited by CODYQX4; 24 Aug 2015 at 22:25.

Microsoft Toolkit - Official KMS Solution for Microsoft Products with License Backup and much more
Windows Firewall Configuration - Truly Block EVERYTHING

Download Microsoft Office 2010 Retail
Download Microsoft Office 2013 Retail
Convert to Volume using Channel Switcher, and use EZ-Activator to activate.
Most, but not all versions available, and some cannot be converted to Volume.