



## Quick Start Guide

### Prerequisites

1. If you are installing OfficeShield in a domain/active directory environment, the OfficeShield administrator account must be either a domain administrator (member of the domain administrators group) or a domain user with local administrator rights (i.e. a member of the domain users and local administrators group).
2. Review the OfficeShield technical support page via the link below for step by step instructions on how to configure OfficeShield with the most popular Internet Security/Firewall packages.  
<http://office-shield.com/Tech-Support.php>
3. If you have not already done so, install the OfficeShield client/agent software on each of the PC's you would like to control and manage. **Do not** install the OfficeShield client software on the same PC that will have the OfficeShield Control Panel software.

#### **OfficeShield client agent installation...**

Copy the client installation package (OfficeShieldClient.exe) from the \Program Files\Computer Business Solutions\OfficeShield folder onto a flash drive, CD or network drive and install on each client PC.

OR

Download the client installation package from the following URL  
<http://www.office-shield.com/download/OfficeShieldClient.exe> onto a flash drive, CD or network drive and install on each client PC.



## Getting Started

4. Start the OfficeShield Control Panel from the Windows® start menu by selecting the OfficeShield program group and then the **OfficeShield Control** program. *This assumes that you have installed the OfficeShield Control Panel software on the managers PC or the PC that will be used to manage all of the restriction profiles. If you have not yet installed the control panel software you can download via the following link.*  
<http://www.office-shield.com/download/OfficeShieldControl.exe>
5. Activate the software via the Licenses screen using the serial number you received during the purchase process. If you are trialing the product you will have 15 days to evaluate. If you need more time please contact OfficeShield sales at [sales@office-shield.com](mailto:sales@office-shield.com).
6. Refresh your network via the network panel; *if you encounter any problems seeing all of the PC's on your network or the PC's appear offline, users do not appear, etc. review the firewall setup information on the last page of this document.*
7. Select Profiles from the left navigation bar to create and manage restriction profiles.
8. Create as many restriction profiles as may fit your organization. As a quick start, select and edit the Business Standard profile.
9. Drag PC/domain users into each profile.
10. Click the Update button to propagate the restriction profiles to each of the PC's. This may take a few minutes so please be patient.
11. Once each PC user logs off and back on to the PC, their restrictions and filtering will be enforced.
12. Setup Real Time Alerts under reporting and your SMTP settings under Options to have real time alerts emailed to you.

Questions can be directed to [support@office-shield.com](mailto:support@office-shield.com)



## Firewall Setup

The OfficeShield client was tested with the most popular firewall/Internet security packages. Instructions on how to configure these Internet security packages with OfficeShield has been posted on the OfficeShield technical support page. Please visit <http://www.office-shield.com/Tech-Support.php> for step by step instruction on how to configure your personal firewall/Internet security software with OfficeShield.

If your firewall/Internet security package is not on our list you can manually implement the firewall rules listed below or contact support and request that they test with your package.

Keep in mind that depending how secure or rigid your firewall is some of the rules listed below may not be necessary.

### Firewall Rules

- ✓ Allow incoming TCP/IP WMI communications over any port via the C:\Windows\system32\wbem\unsecapp.exe program.
- ✓ Allow incoming and outgoing TCP/IP WMI communications over any port via the C:\Windows\system32\svchost.exe program, (WINMGMT service).
- ✓ Allow incoming TCP/IP communications over port 135 via the C:\Windows\system32\svchost.exe program, (RPCSS service).
- ✓ Enable File and Printer Sharing via TCP/IP ports 139 & 445 and UDP ports 137 & 138
- ✓ Allow incoming TCP/IP communications over any port via the C:\Windows\System32\kwcaptur.exe program.
- ✓ Allow inbound and outbound communications via the ICMP (ping) protocol.
- ✓ Allow all outgoing TCP/IP communications for KWMMain.exe (Vista/Win 7) or winlogon.exe (XP only) on port 80 (HTTP).
- ✓ Allow all incoming and outgoing UDP communications for KWMMain.exe (Vista/Win 7) or winlogon.exe (XP only) on port 53 (DNS).
- ✓ Allow all incoming TCP/IP communications on port 4566.
- ✓ Allow all outgoing TCP/IP communications on port 25 (SMTP).
- ✓ Allow all UDP communications on port 123.