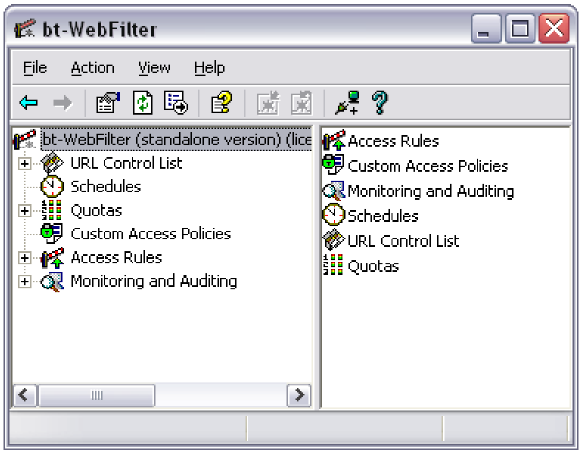
BURSTEK™
The World's Choice for Internet Security.

# bt-WebFilter Standalone Version
# Quick Start Guide



## System Requirements

Microsoft Windows Server (All Microsoft Supported Version)

**NOTE:** After installation and selecting default access policy, WebFilter immediately blocks the following categories:
Anonymizers, Criminal Skills, Extreme & Violence, Gambling, Hacking, Hate Speech, Malicious Code, Mature, Spyware/Adware and XXX-Sexual Content.

Examples of other categories you may wish to block include Chat, File Sharing, Remote Access, and Social Networking.

A complete list of categories with definitions and examples can be viewed on our Web site at: http://www.burstek.com/products/web-filtering/control-list/control-list-categories/

**NOTE:** For testing purposes, the bt-WebFilter Standalone Version may be installed on a Windows 2000 or XP Pro workstation or Server 2003+

## Quick Setup Procedure

1. Temporarily disable anti-virus software.
2. To start the installation wizard, extract the ZIP file to a directory on your system.
3. Navigate to the extracted directory and double-click on the setup.exe for bt-WebFilter. Click ‘Run’ if you receive an ‘Open File – Security Warning’ dialog box
4. Click ‘Next’ at the bt-WebFilter Welcome screen.
5. Accept the terms and click ‘Next’
6. Accept the default installation directory and click ‘Next’
7. Ensure the ‘Complete’ option is select and click ‘Next’
8. Accept the defaults for the URL Control List Update and select ‘Next’
9. Click ‘Install’. The program will now begin copying files.
10. Click ‘Finish’ when prompted
11. **Reboot** your server.

## Starting bt-WebFilter

1. Click on ‘Start > Programs > Burst Technology > bt-WebFilter Management’
2. Click ‘OK’ at the license warning
3. Determine how you will be filtering connections (Anonymous, IP Based, Domain Based) and go to that section:

## Domain User Filtering

1. Right click on the ‘Access Rules’ object on the left side of the screen and select ‘Register Domain’
2. Select your domain from the drop down box and select ‘OK’
3. Select ‘OK’ at the domain properties dialog box
4. Select the ‘Custom Access Policies’ object in the left window
5. Double-Click the ‘Default Custom Access Policy’ in the right window
6. Click the ‘Apply To’ tab
7. Select the ‘Add Groups’ option at the bottom of the properties page.
8. Enter the domain group that you wish to perform Content Filtering on and select ‘Check Names’
9. Click ‘OK’ when complete.
10. Verify that the group you added is listed in the box with a check mark next to it and click ‘Apply’ and ‘OK’.
11. Right click the ‘bt-WebFilter (standalone version) at the top of the left window and select properties

12. Click on the ‘Proxy Options’ tab
13. Under ‘Authentication’, Select ‘Ask unauthorized users for identification’ and select your domain. Ensure the options ‘Basic with this domain:’ and ‘Integrated’ are also selected.
14. Click ‘Apply’ and ‘OK’
15. Proceed to ‘Testing the Software’

## IP Range Filtering

1. Under ‘Access Rules’ in the left window, right click ‘IP Ranges’ and select ‘Register IP Range’
2. Enter the IP range of the address you wish to filter and click ‘OK’. You can enter multiple IP ranges by adding them individually.
3. The properties for the range that you specified will appear. Select the ‘Custom Access Policies’ tab and put a checkmark in the ‘Default Custom Access Policy’
4. Click ‘Apply’ then ‘OK’

## Unauthenticated Access

1. To block unauthenticated access to the web, right click on the ‘Unauthenticated Access’ object on the left side of the screen and select ‘Properties’
2. Click on the ‘Individual Access Policy Type’ and select the ‘Permissions policy’ option.
3. Click ‘OK’ then ‘Apply’ then ‘OK’

## Testing the Software

1. Launch Internet Explorer.
2. Click Tools> Internet Options> Connections> LAN Settings.
3. Check the box marked ‘Use a proxy server for your LAN’.
4. Enter the IP of the computer with bt-WebFilter in the ‘Address’ field.
5. Set the ‘Port’ to port 8080.
6. Click ‘OK’ to save, and then close the browser.
7. Re-launch Internet Explorer and try going to www.casino.com

## Recommended Filtering Settings

Please visit: **http://www.burstek.com/support/webfilter-support/webfilter-best-practices/**

## How do I prevent users from bypassing the bt-WebFilter?

1. Open the ‘Group Policy Object Editor’ for your ‘Default Domain Controllers Policy’
2. In the ‘User Configuration’ section, click the ‘+’ sign next to ‘Administrative Templates’, click the ‘+’ sign next to ‘Windows Components’, click the ’+’ sign next to Internet Explorer.
3. Click on the ‘Internet Control Panel’ folder.
4. In the right hand pane, double click on ‘Disable the Connections Page’
5. Select the Radio button next to ‘Enable’
6. Click the ‘Apply’ button, then the ‘OK’ button.
7. Click the ‘+’ next to the ‘Windows Settings’ then ‘Internet Explorer Maintenance’
8. Click on the ‘Connection’ option.
9. In the left pane, open up the ‘Proxy Settings’ object.
10. Put a checkmark in the ‘Enable proxy settings’ option and enter the IP and port number for ‘HTTP’ and “Secure’ for the bt-WebFilter server. Default port number for WebFilter Standalone is 8080.
11. Click ‘Apply’ then ‘OK’
12. Close out of Group Policy.
13. Allow up to 15 minutes for Active Directory to replicate the Group Policy then log on to a workstation
14. Open Internet Explorer and select ‘Tools’ from the ‘Menu Bar’ and choose ‘Internet Options’
15. Click on the ‘Connections Tab’ and verify that the options are unavailable.

## Technical Support Contacts

Phone: 239.495.5900
E-mail: support@burstek.com
Web: http://www.burstek.com/support-2/webfilter-support/webfilter-faqs