

bt-WebFilter for MS ISA Server Quick Start Guide

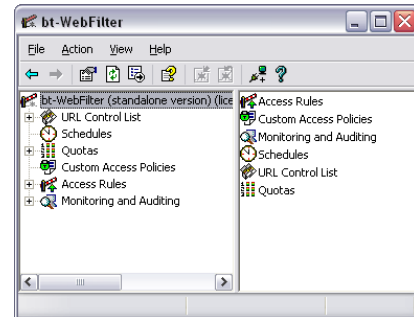
System Requirements

Windows 2000, 2003, 2008

MS Forefront TMG, MS ISA Server 2000, 2004, 2006

NOTE: After installation, 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/categories.htm>

Quick Setup Procedure

1. To start the installation wizard, unzip and double-click on the **setup.exe** for bt-WebFilter and **reboot** your server.
2. If you are NOT authenticating users, the default filtering policy should be blocking access to "questionable" categories (i.e. XXX Sexual Content, Gambling, Malicious Code, and more).

Setting Up bt-WebFilter with ISA 2004 and 2006

1. Install ISA 2004 or 2006 Server.
2. Turn authentication on:
 - a. Open up the ISA Management console.
 - b. Click the "+" next to Configuration.
 - c. Click on Networks.
 - d. On the Right pane, right click on the Internal, and select Properties.
 - e. Click on the Web Proxy tab.
 - f. Click on the Authentication button.
 - g. Integrated should already be checked. Check the box next to require all users to authenticate.
 - h. Check the box labeled "**Require all users to authenticate.**"
 - i. Apply the changes.
3. Create an Access Rule:
 - a. Open up the ISA Management Console.

- b. Right-click on Firewall Policy, select **New > Access Rule**.
 - c. Type in the Access Rule Name.
 - d. Select "**Allow**" for the Rule Action, and click "**Next.**"
 - e. Select "**All Outbound Traffic**" for Protocols, and click the next button.
 - f. Click the "Add" button for the Access Rule Sources.
 - g. Click the "+" next to "**Network Sets**" and select "**All Networks (and Local Host)**", and click the "Add" button, and then the "**Close**" button, then click the next button.
 - h. Repeat steps f and g for "**Access Rules Destinations.**"
 - i. In the **User Sets** screen, make sure "**All Users is selected**" then click the next button.
 - j. Click the "**Finish**" button.
 - k. Apply the settings.
4. Install the bt-WebFilter ISA Server version
 - a. Download the latest version of bt-WebFilter ISA Server version
 - b. Unzip the file
 - c. Double click on Setup.exe
 - d. Follow the default installation instructions
 - e. Once the install is complete, reboot the machine
 5. Configure the bt-WebFilter (By default the bt-WebFilter is set to a *Restrictive* policy):
 - a. Open up the bt-WebFilter Console.
 - b. Right click on **Access Rules**, and select **Register Domain**.
 - c. Select the Drop down box and click on your domain name and click the "**OK**" button.
 - d. Click on the **Custom Access Policies**.
 - e. On the right hand pane, right click on the **Default Custom Policy** and select **Properties**.
 - f. Click on the "**Apply to**" tab, and check the box next to the user groups (Domain Users) you want to apply this policy to.

Setting Up bt-WebFilter with ISA 2000

1. Install ISA 2000 Server.
2. Turn authentication on:
 - a. Right-click your ISA server and then click Properties.
 - b. Click on **Outgoing Web Requests**.
 - c. Check the box labeled "**Ask unauthenticated users for identification.**"
 - d. Select your server in the identification box and then please click "**Edit.**"
 - e. Integrated should already be checked. Click in the appropriate boxes to enable any desired additional authentication features.
 - f. Apply the changes.
3. Create an Access Rule:

- a. Open up the ISA Management Console.
 - b. Click to expand **Access Policy**.
 - c. Right-click **Protocol Rules** and then click "**New.**"
 - d. Create an Allow protocol rule and then click "**Next.**"
 - e. Enable the rule to apply to all IP traffic and/or Users and then click "**Next.**"
 - f. Click to select the schedule and then click "**Next.**"
 - g. Click **Any Request**, click "**Next**" and then click "**Finish.**"
4. Install the bt-WebFilter ISA Server version
 - a. Download the latest version of bt-WebFilter ISA Server version
 - b. Unzip the file
 - c. Double click on **Setup.exe**.
 - d. Follow the default installation instructions
 - e. Once the install is complete, reboot the machine
 5. Configure the bt-WebFilter (By default the bt-WebFilter is set to a *Restrictive* policy):
 - a. Open up the bt-WebFilter Console.
 - b. Right click on **Access Rules**, and select **Register Domain**.
 - c. Select the Drop down box and click on your domain name and click the "**OK**" button.
 - d. Click on the **Custom Access Policies**.
 - e. On the right hand pane, right click on the **Default Custom Policy** and select **Properties**.
 - f. Click on the "**Apply to**" tab, and check the box next to the user groups (Domain Users) you want to apply this policy to.

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/btWebFilter/bestPractices.htm>

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

1. Click on **Start> All Programs > Administrative Tools > Active Directory Users and Computers**.
2. Right click on your Domain and select "**Properties.**"
3. Click on the "**Group Policy**" tab.

4. Click on the Default Domain Policy, and click on the **"Edit"** button.
5. 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.
6. Click on the **Internet Control Panel** folder.
7. In the right hand pane, double click on **"Disable the Connections Page."**
8. Select the Radio button next to **Enable**.
9. Click the **"Apply"** button, then the **"OK"** button.
10. Close out of Group Policy.
11. Click the **"OK"** button on the **"Group Policy"** tab.
12. Close out of Active Directory for Users and Computers.

Technical Support Contacts

Phone: 239.495.5900

E-mail: support@burstek.com

Web: <http://www.burstek.com/support/btWebFilter/faq.htm>