Burst Technology

presents

bt-WebFilter

User Guide

Burstek™

9240 Bonita Beach Road

Bonita Springs, FL 34135

Telephone: (239) 495-5900 or toll free (800) 709-2551

Visit the Burstek Website at http://www.burstek.com

Contents

Before you Begin

Requirements

In order to use the bt-WebFilter program you must have the following software:

Remote Client Components

Microsoft Windows 2000 (Windows 2000 Professional, Server or Advanced Server) with SP 4 or higher or Windows 2003 Server Internet Explorer 6.0 or higher

MS ISA Server & TMG

Microsoft Windows 2000 Server (or Advanced Server) with SP 4 or higher or Windows 2003 server Microsoft's ISA Server 2000 or 2004

Standalone Server

Microsoft Windows 2000 Professional or Server, 2003 Server or XP Professional Operating System Internet Explorer 6.0 or higher

Chapter 1 bt-WebFilter Overview

Companies have invested heavily in network-related manpower, hardware, software, and bandwidth. Effective management requires that these resources are:

(a) Being used productively

(b) Not being misused or abused

(c) Generating a positive "return on investment"

bt-WebFilter is an Internet filter and blocking solution that can be customized to ensure that your employees are adhering to your company's Internet Use Policies.

Use bt-WebFilter To:

- Block access to Websites with Malicious Code, Streaming Media, Gambling, and Pornographic URLs.
- Optimize your network resources by limiting online shopping and sports updates by time-of-day or bandwidth or establishing quotas for both.
- Increase productivity by effectively allowing business use of the Internet while reducing recreational surfing.

The bt-WebFilter program can be used as a plug-in to the Microsoft ISA servers, a stand-alone Internet filter and blocking solution or it can be used in combination with the bt-LogAnalyzer program to control and evaluate employee Web and Email use.

The solution allows corporate administrators to:

- Allow or deny access to Web Categories or Website URLs for all members of Windows NT/200x groups or specified IP ranges.
- Define wildcards to place restrictions on users' access to Websites by URLs or IP Addresses.
- View existing Windows NT/200x groups in the application console, and change Internet access restrictions and permissions for these groups.
- View log files containing information about users' attempts to access prohibited URLs.
- Create schedule or activity intervals to further define restrictions and permissions policies for single domain groups.
- Block "https" sites.
- Filter on multiple domains.
- Update the URL Control List automatically.
- Administrate the system remotely.

Features

- Time-of-Day - filter based on time of day/day of the week (i.e. deny access to sports during business hours, but allow access at other times).
- Categories - deny or allow access based on over 60+ categories (i.e. Sexual Content, Criminal Skills, Weapons, etc.). See Burstek's Website for a complete description of all the Categories.
- Group/User Support - customize policies based on NT4 or Windows 200x Active Directory.
- IP Range Support – customize policies based on specified IP ranges.
- Remote Administration Auditing - Log and view denied URLs by User in real-time.
- Performance - bt-WebFilter is multi-threaded and can be dispatched for parallel processing on more than one processor.
- File Type - filtering image file extensions, WebFilter allows users to read the text content on a Website but can prohibit downloading or viewing images and blocking MP3 file trading.
- Yes Lists - allow access only to specific Websites and/or categories (i.e. Shipping Department can only go to UPS, FedEx, USPS, etc.). Multiple 'Yes Lists' supported.
- Manage all Protocols - The bt-WebFilter plug-in for ISA Server allows you to Manage Protocols setup in Microsoft ISA Server. You can set permissions and restrictions to control traffic.
- Customizable - easily create your own categories; add to or exempt what bt-WebFilter blocks by default.
- Replication
- Quotas
- Real-Time Monitoring
- Exempt users from policies

Chapter 2 Installation

Installing bt-WebFilter - ISA Server Version

The bt-WebFilter executable utilizes an InstallShield Wizard. The bt-WebFilter (ISA Server version) can be installed on any Microsoft Windows 2x Operating System with Internet Security and Acceleration Server version 2000, 2004, 2006, including Microsoft Threat Management Gateway (TMG).

NOTE:

If installing bt-LogAnalyzer 6 on the same server, bt-WebFilter must be installed first. If uninstalling the Burstek Software, bt-LogAnalyzer must be uninstalled prior to uninstalling bt-WebFilter.

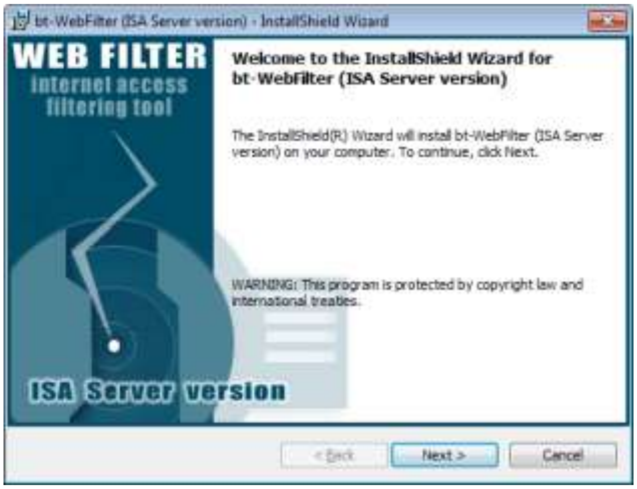
NOTE:

Be sure you are installing the correct version of bt-WebFilter. When you launch the Setup program, the version will be displayed at the top of the InstallShield Wizard as well as in the right side of the window.

NOTE:

If you are installing WebFilter on a Microsoft Server 2008 Operating System, you must run the 'Setup.exe' as an administrator by right clicking on the file and selecting it from the menu. If this step is not followed, you may receive an error message during the installation.

1. To start the installation, locate the zip file that you downloaded from Burstek's website and extract the contents to a directory on your computer.
2. Once the files are extracted, locate the 'Setup.exe' file and double click. The bt-WebFlter (ISA Server version) 'Welcome' screen will appear. Click 'Next' to continue.



bt-WebFilter (ISA Server version) - InstallShield Wizard
WEB FILTER
internet access filtering tool
ISA Server version
< Back
Next >
Cancel

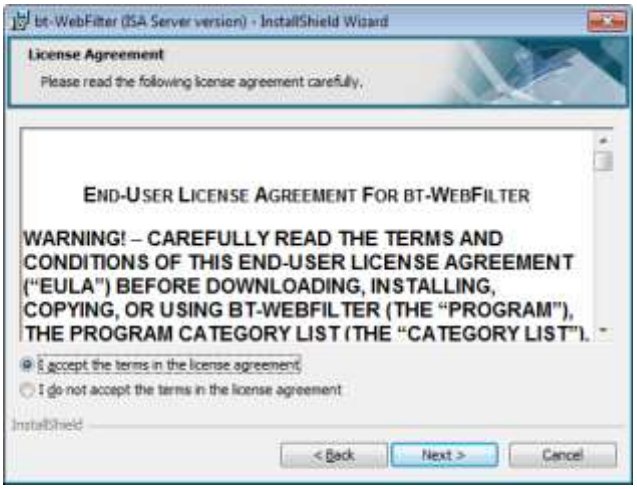
Welcome to the InstallShield Wizard for bt-WebFilter (ISA Server version)

The InstallShield(R) Wizard will install bt-WebFilter (ISA Server version) on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

bt-WebFilter ISA Installation 2-1: Welcome Screen

3. The ‘License Agreement’ screen will be displayed. After reading the ‘**E**nd-**U**ser **L**icense **A**greement For bt-WebFilter’ and you agree, click **“I accept the terms in the license agreement”** and click “Next” to continue.



bt-WebFilter (ISA Server version) - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

END-USER LICENSE AGREEMENT FOR BT-WEBFILTER

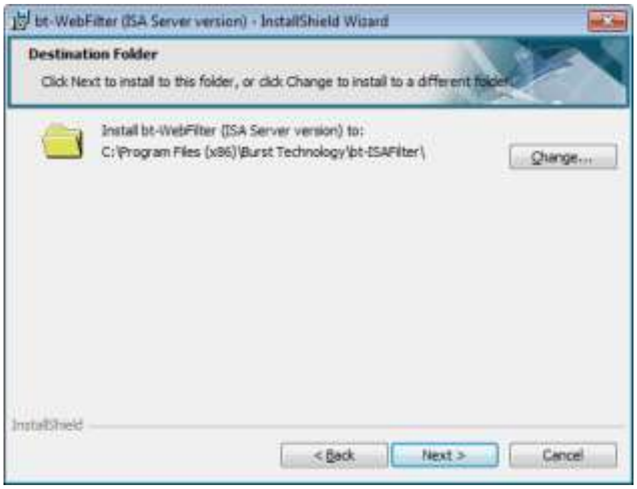
WARNING! – CAREFULLY READ THE TERMS AND CONDITIONS OF THIS END-USER LICENSE AGREEMENT (“EULA”) BEFORE DOWNLOADING, INSTALLING, COPYING, OR USING BT-WEBFILTER (THE “PROGRAM”), THE PROGRAM CATEGORY LIST (THE “CATEGORY LIST”),

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

bt-WebFilter ISA Installation 2-2: EULA

4. The ‘Destination Folder’ screen will appear. Accept the default location or select the “Change” button if you would like to install to a different directory. When completed, click “Next”



bt-WebFilter (ISA Server version) - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

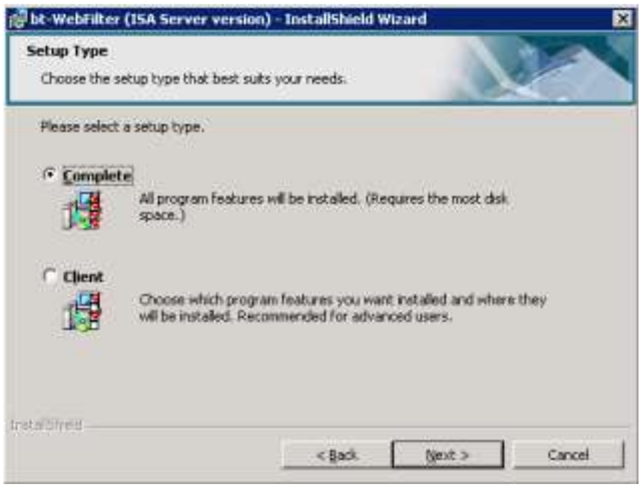
Install bt-WebFilter (ISA Server version) to:
C:\Program Files (x86)\Burst Technology\bt-ISAFilter\

bt-WebFilter ISA Installation 2-3: Destination Folder

5. The ‘Setup Type’ window appears. Since this is a new installation, select the “Complete” installation option and click “Next”

TIP!

You can re-run the installation wizard on another computer and select the “Client” option. This will install the remote management console that will allow you to manage multiple bt-WebFilter for ISA Server installs from a remote computer



Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● Complete

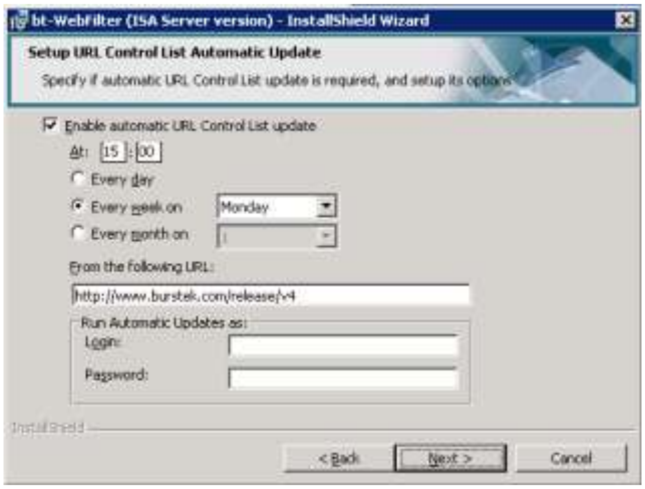
All program features will be installed. (Requires the most disk space.)

○ Client

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

bt-WebFilter ISA Installation 2-4: Setup Type

6. In the "Setup URL Control List Automatic Update" page, make your selections regarding how often you want the server to check for updates to the Control List and select 'Next'



Setup URL Control List Automatic Update

Specify if automatic URL Control List update is required, and setup its options

☑ Enable automatic URL Control List update

At: 15 : 00

○ Every day

● Every week on Monday

○ Every month on 1

From the following URL:

http://www.burstek.com/release/v4

Run Automatic Updates as:

Login:

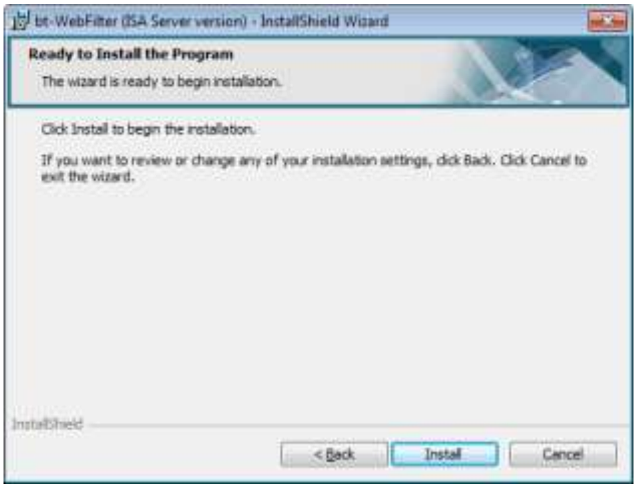
Password:

bt-WebFilter ISA Installation 2-5: URL Control List Udpate

NOTE:

The 'Run Automatic Updates as:' credentials only need to be used if you are required to supply login information to gain access to the Internet. Typically this is not needed.

7. You are now ready to install the application and the next screen will confirm that option. Press 'Install' to continue. The installer will begin copying files and you will see the "InstallShield Wizard Completed" dialog box once it completes successfully.



bt-WebFilter (ISA Server version) - InstallShield Wizard

Ready to Install the Program

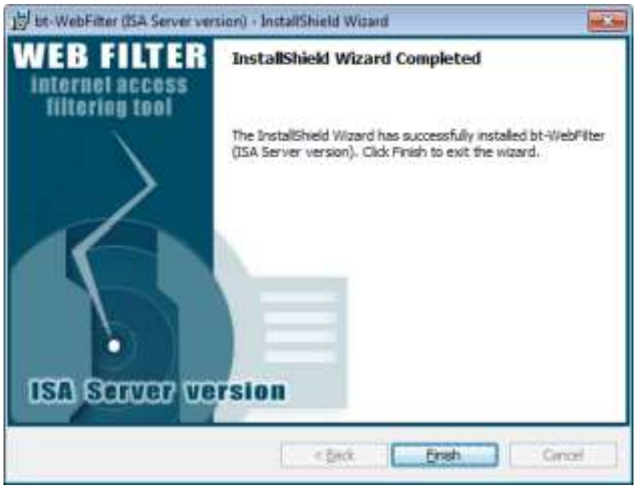
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

bt-WebFilter ISA Installation 2-6: Ready to Install

8. Click 'Finish'. You will be prompted to restart your system. Click 'Yes' if you want to restart now or 'No' to restart manually at a later time.



bt-WebFilter (ISA Server version) - InstallShield Wizard

InstallShield Wizard Completed

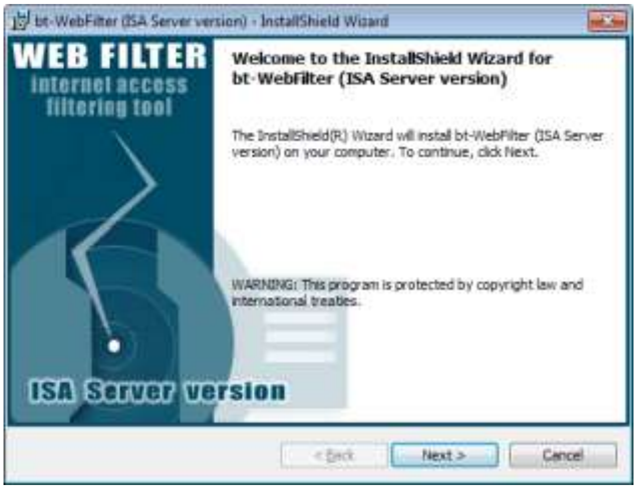
The InstallShield Wizard has successfully installed bt-WebFilter (ISA Server version). Click Finish to exit the wizard.

bt-WebFilter ISA Installation 2-7: Install Complete

Installing bt-WebFilter – Remote Management Console

1. To start the installation, locate the zip file that you downloaded from Burstek's website and extract the contents to a directory on your computer.
2. Once the files are extracted, locate the 'Setup.exe' file and double click. The bt-WebFilter 'Welcome' screen will appear. Click 'Next' to continue.

> **NOTE:**
> Ensure that you are installing the management console for the version of the application you are using.



bt-WebFilter (ISA Server version) - InstallShield Wizard

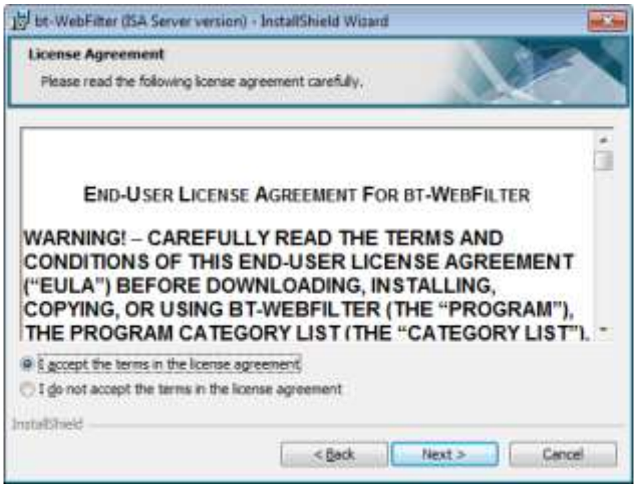
Welcome to the InstallShield Wizard for bt-WebFilter (ISA Server version)

The InstallShield(R) Wizard will install bt-WebFilter (ISA Server version) on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

bt-WebFilter RMC 2-1: Welcome Screen

3. The 'License Agreement' screen will be displayed. After reading the '**E**nd-**U**ser **L**icense **A**greement For bt-WebFilter' and you agree, click **"I accept the terms in the license agreement"** and click "Next" to continue.



License Agreement

Please read the following license agreement carefully.

END-USER LICENSE AGREEMENT FOR BT-WEBFILTER

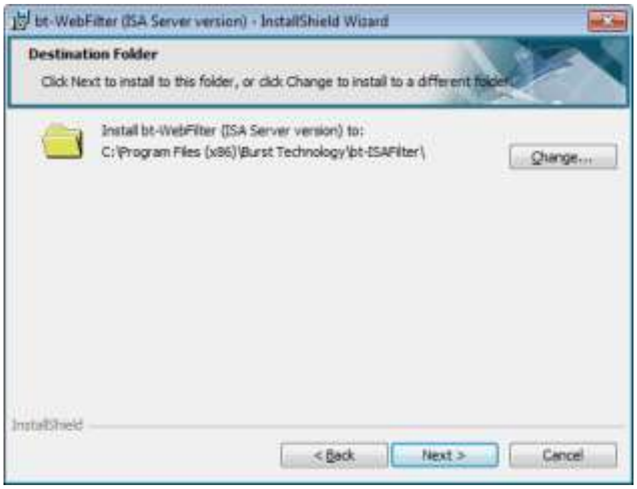
WARNING! – CAREFULLY READ THE TERMS AND CONDITIONS OF THIS END-USER LICENSE AGREEMENT ("EULA") BEFORE DOWNLOADING, INSTALLING, COPYING, OR USING BT-WEBFILTER (THE "PROGRAM"), THE PROGRAM CATEGORY LIST (THE "CATEGORY LIST").

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

bt-WebFilter RMC 2-2: EULA

4. Accept the default installation directory or click 'Change' to install to a different location. When completed click 'Next'.



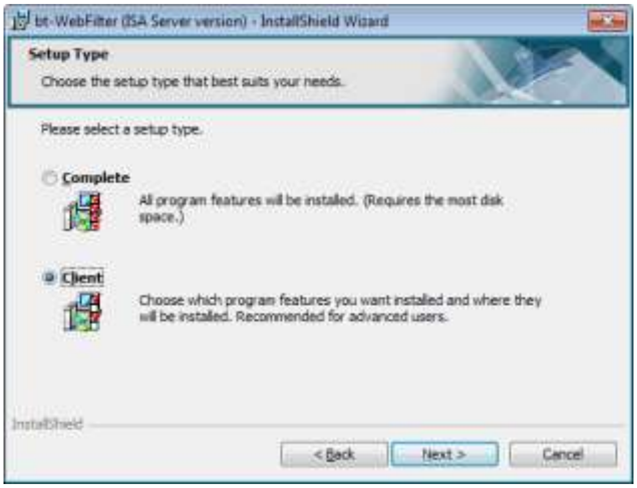
Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

Install bt-WebFilter (ISA Server version) to:
C:\Program Files (x86)\Burst Technology\bt-ISAFilter\

bt-WebFilter RMC 2-3: Destination Folder

5. Select the 'Client' option and click 'Next' to continue.



bt-WebFilter (ISA Server version) - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

○ **Complete**

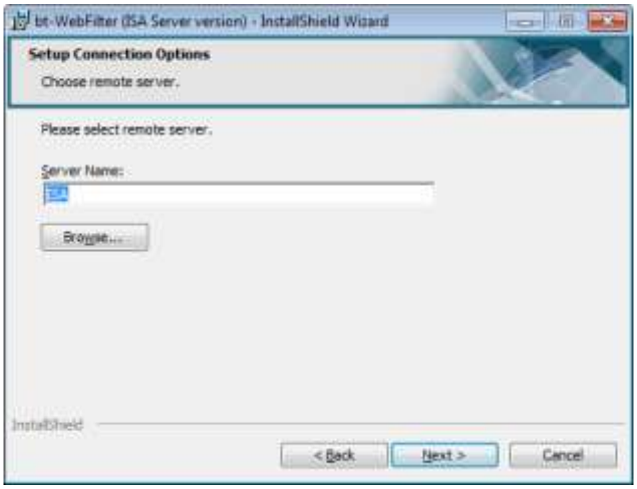
All program features will be installed. (Requires the most disk space.)

● **Client**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

bt-WebFilter RMC 2-4: Setup Type

6. Enter the name of the WebFilter server you are trying to connect to or click 'Browse' and select the system from the list of computers. Once completed click 'Next' to continue.



bt-WebFilter (ISA Server version) - InstallShield Wizard

Setup Connection Options

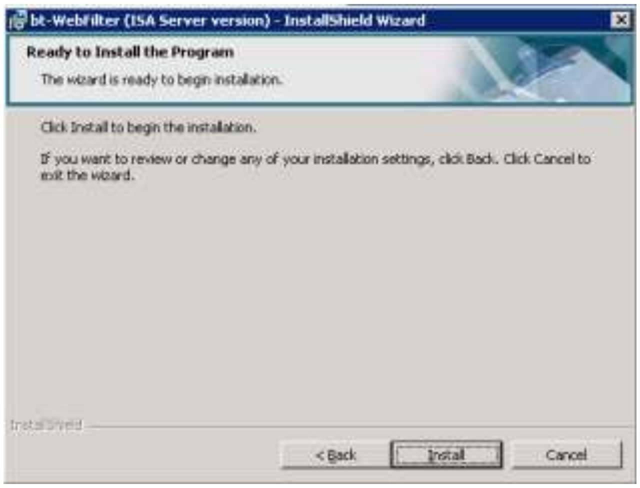
Choose remote server.

Please select remote server.

Server Name:

bt-WebFilter RMC 2-5: Remote Server Selection

7. You are now ready to install the application and the next screen will confirm that option. Press 'Install' to continue and begin copying files.


bt-WebFilter (ISA Server version) - InstallShield Wizard

Ready to Install the Program

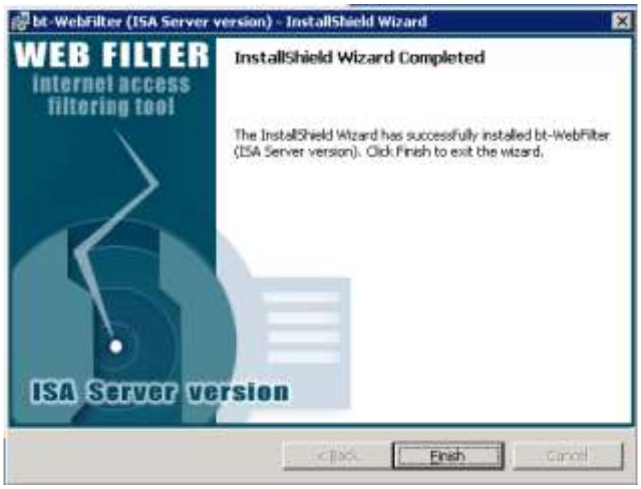
The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

bt-WebFilter RMC 2-6: Ready to Install

8. Once the install finishes copying files you will see the 'InstallShield Wizard Completed' window. Click 'Finish' to exit the installer. You will be prompted to restart your system. Click 'Yes' if you want to restart now or 'No' to restart manually at a later time.


bt-WebFilter (ISA Server version) - InstallShield Wizard

InstallShield Wizard Completed

The InstallShield Wizard has successfully installed bt-WebFilter (ISA Server version). Click Finish to exit the wizard.

bt-WebFilter RMC 2-7: Install Complete

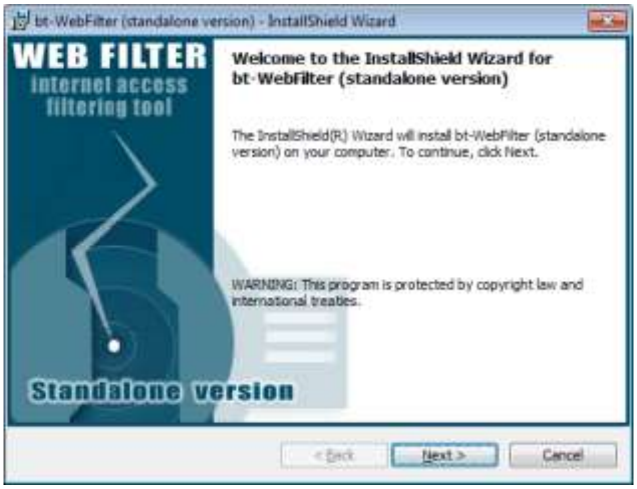
Installing bt-WebFilter – Standalone Version

1. To start the installation, locate the zip file that you downloaded from Burstek's website and extract the contents to a directory on your computer.
2. Once the files are extracted, locate the 'Setup.exe' file and double click. The bt-WebFlter (standalone version) 'Welcome' screen will appear. Click 'Next' to continue.

NOTE:
If installing bt-LogAnalyzer 6 on the same server, bt-WebFilter must be installed first. If uninstalling the Burstek Software, bt-LogAnalyzer must be uninstalled prior to uninstalling bt-WebFilter.

NOTE:
Be sure you are installing the correct version of bt-WebFilter. When you launch the Setup program, the version will be displayed at the top of the InstallShield Wizard as well as in the right side of the window.

NOTE:
If you are installing WebFilter on a Microsoft Server 2008 Operating System, you must run the 'Setup.exe' as an administrator by right clicking on the file and selecting it from the menu. If this step is not followed, you may receive an error message during the installation.



bt-WebFilter (standalone version) - InstallShield Wizard

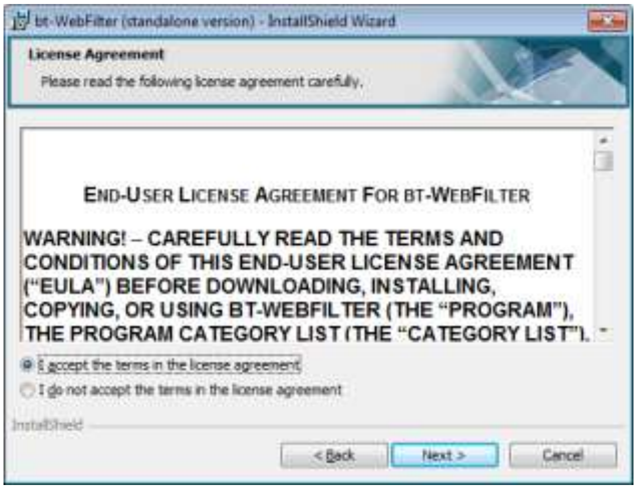
Welcome to the InstallShield Wizard for bt-WebFilter (standalone version)

The InstallShield(R) Wizard will install bt-WebFilter (standalone version) on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

bt-WebFilter Standalone Install 2-1: Welcome Screen

3. The 'License Agreement' screen will be displayed. After reading the '**E**nd-**U**ser **L**icense **A**greement For bt-WebFilter' and if you agree, click **"I accept the terms in the license agreement"** and click "Next" to continue.



bt-WebFilter (standalone version) - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

END-USER LICENSE AGREEMENT FOR BT-WEBFILTER

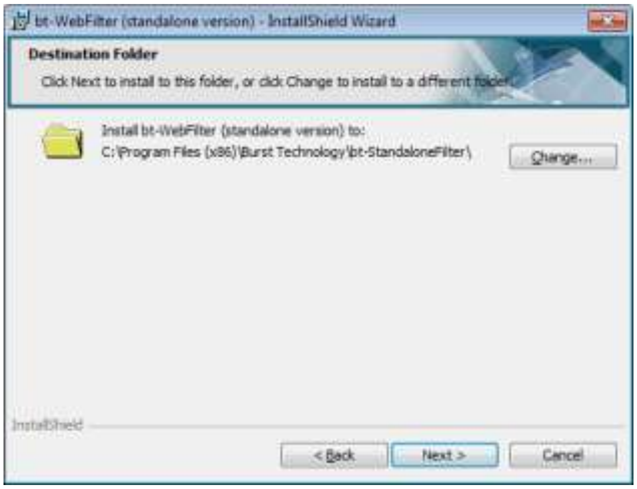
WARNING! – CAREFULLY READ THE TERMS AND CONDITIONS OF THIS END-USER LICENSE AGREEMENT ("EULA") BEFORE DOWNLOADING, INSTALLING, COPYING, OR USING BT-WEBFILTER (THE "PROGRAM"), THE PROGRAM CATEGORY LIST (THE "CATEGORY LIST").

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

bt-WebFilter Standalone Install 2-2: EULA

4. Accept the default installation directory or click 'Change' to install to a different location. When completed click 'Next'.



bt-WebFilter (standalone version) - InstallShield Wizard

Destination Folder

Click Next to install to this folder, or click Change to install to a different folder.

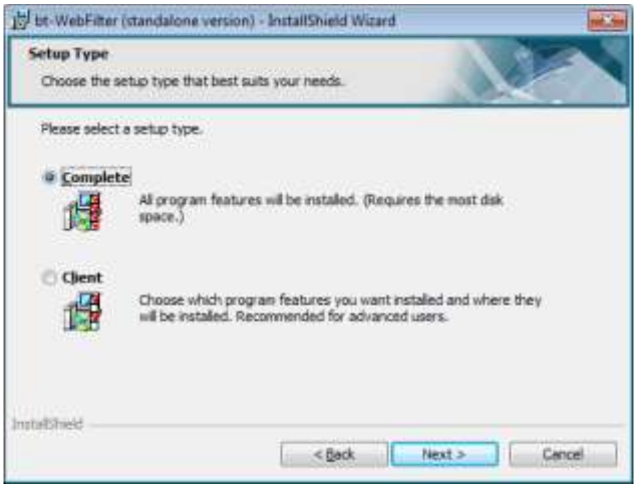
Install bt-WebFilter (standalone version) to:
C:\Program Files (x86)\Burst Technology\bt-StandaloneFilter\

bt-WebFilter Standalone Install 2-3: Destination Folder

5. The ‛Setup Type’ window appears. Since this is a new installation, select the “Complete” installation option and click “Next”

TIP!

You can re-run the installation wizard on another computer and select the “Client” option. This will install the remote management console that will allow you to manage multiple bt-WebFilter installs from a remote computer


bt-WebFilter (standalone version) - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● Complete

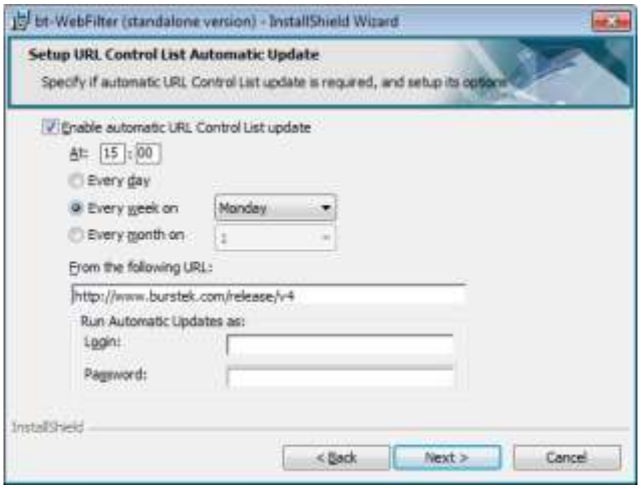
All program features will be installed. (Requires the most disk space.)

○ Client

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

bt-WebFilter Standalone Install 2-4: Setup Type

6. In the “Setup URL Control List Automatic Update” page, make your selections regarding how often you want the server to check for updates to the Control List and select ‛Next’


bt-WebFilter (standalone version) - InstallShield Wizard

Setup URL Control List Automatic Update

Specify if automatic URL Control List update is required, and setup its options

☑ Enable automatic URL Control List update

At: 15 : 00

○ Every day

● Every week on Monday

○ Every month on 1

From the following URL:

http://www.burstek.com/release/v4

Run Automatic Updates as:

Login:

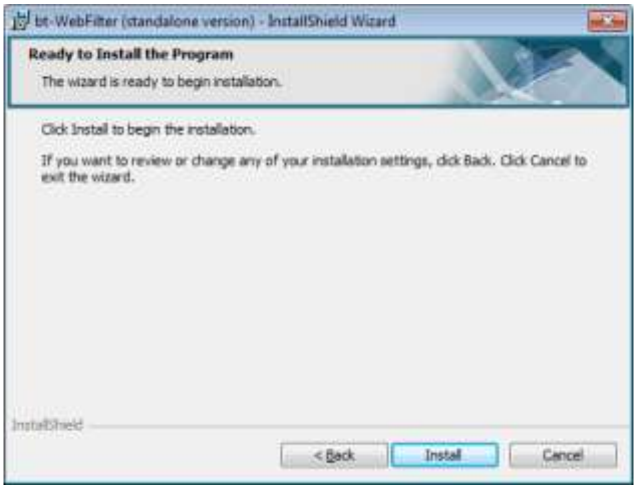
Password:

bt-WebFilter Standalone Install 2-5: Automatic Updates

NOTE:

The ‘Run Automatic Updates as:’ credentials only need to be used if you are required to supply login information to gain access to the Internet. Typically this is not needed.

You are now ready to install the application and the next screen will confirm that option. Press 'Install' to continue. The installer will begin copying files.



Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

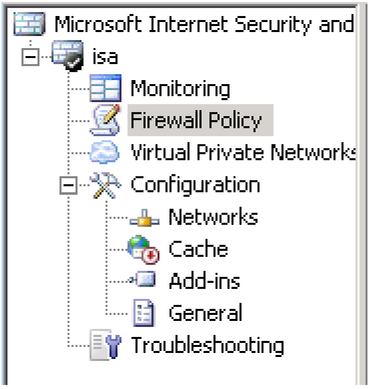
bt-WebFilter Standalone Install 2-6: Ready to Install

7. Once the install finishes copying files you will see the 'InstallShield Wizard Completed' window. Click 'Finish' to exit the installer. You will be prompted to restart your system. Click 'Yes' if you want to restart now or 'No' to restart manually at a later time.

Enabling User Authentication in Microsoft ISA 2006

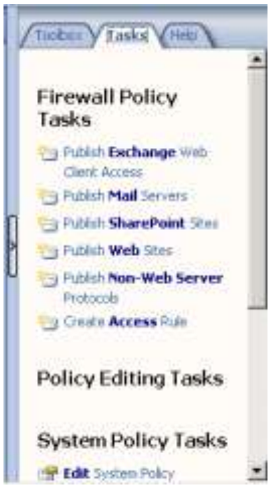
To setup ISA to authenticate users, perform the following steps:

1. Open Microsoft Internet Security and Acceleration Server Management Console. Expand the ISA server and select 'Firewall Policy'



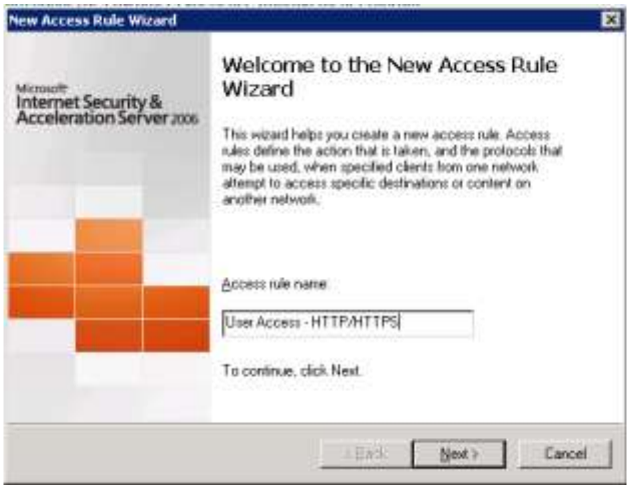
ISA User Authentication 2-1: ISA Management Console

2. On the right side of the screen select the tasks category and select 'Create Access Rule'



ISA User Authentication 2-2: Tasks Tab

3. Provide a name for your access policy and select 'Next'



Welcome to the New Access Rule Wizard

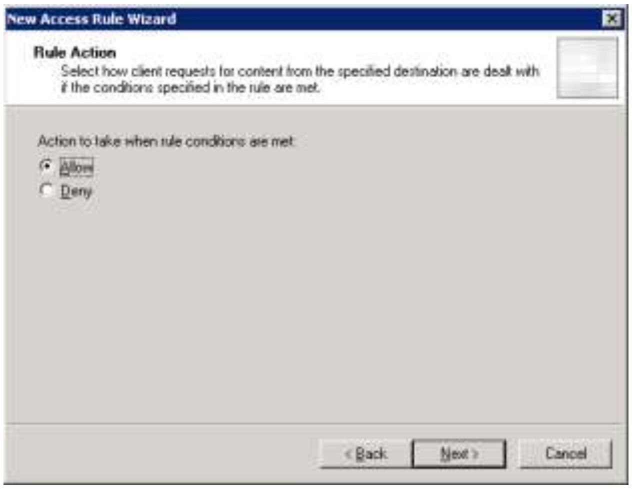
This wizard helps you create a new access rule. Access rules define the action that is taken, and the protocols that may be used, when specified clients from one network attempt to access specific destinations or content on another network.

Access rule name: User Access - HTTP/HTTPS

To continue, click Next.

ISA User Authentication 2-3: New Access Rule Wizard

4. New Access Rule Wizard – Rule Action, select Allow



Rule Action

Select how client requests for content from the specified destination are dealt with if the conditions specified in the rule are met.

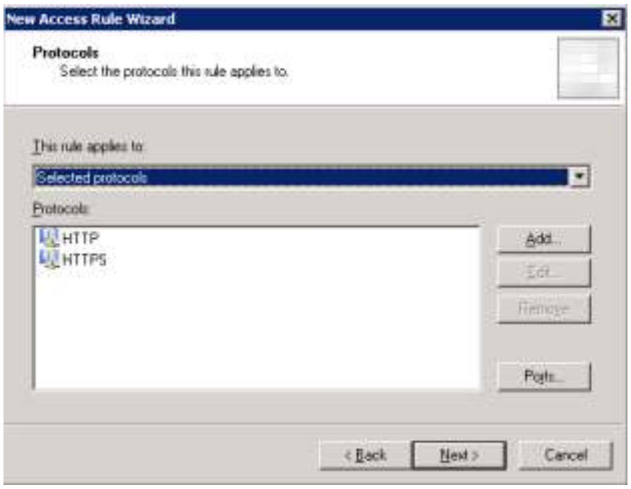
Action to take when rule conditions are met:

● Allow

○ Deny

ISA User Authentication 2-4: Rule Action

5. New Access Rule Wizard – Select Protocols.



New Access Rule Wizard

Protocols

Select the protocols this rule applies to.

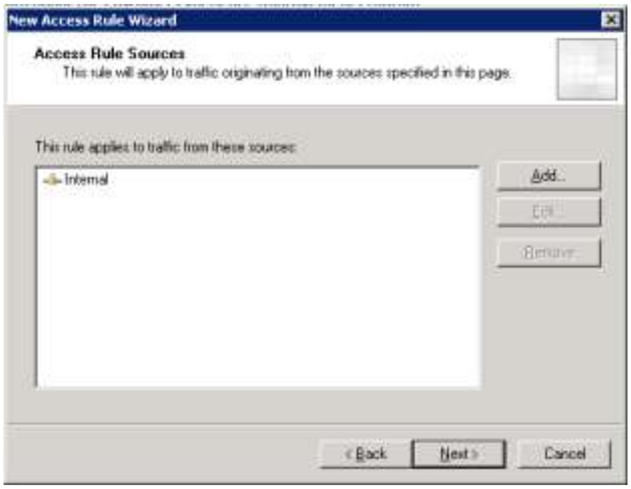
This rule applies to: Selected protocols

Protocols:

- HTTP
- HTTPS

ISA User Authentication 2-5: Protocol Selection

6. New Access Rule Wizard – Access Rule Sources Traffic From, Click Add



New Access Rule Wizard

Access Rule Sources

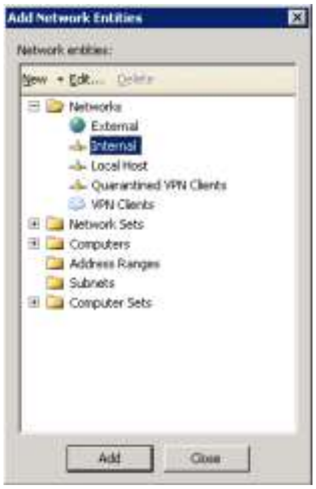
This rule will apply to traffic originating from the sources specified in this page.

This rule applies to traffic from these sources:

- Internal

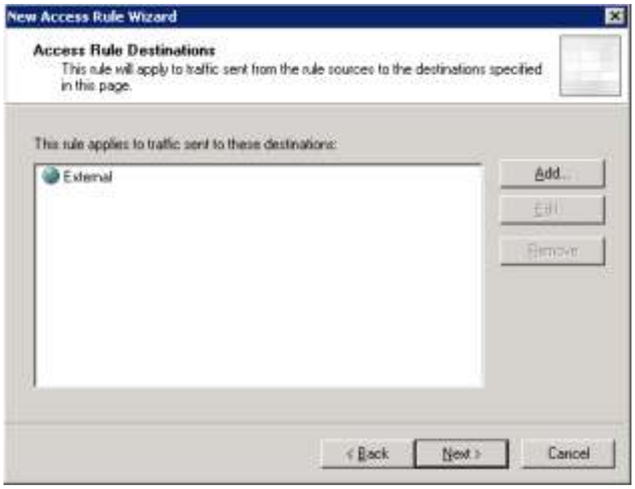
ISA User Authentication 2-6: Access Rule Sources

7. Select 'Internal' and then 'Add'



ISA User Authentication 2-7: Network Entities - Source

8. New Access Rule Wizard – Access Rule Sources Traffic To, Click Add

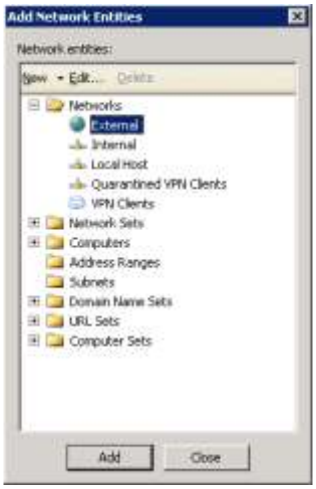


This rule will apply to traffic sent from the rule sources to the destinations specified in this page.

This rule applies to traffic sent to these destinations:

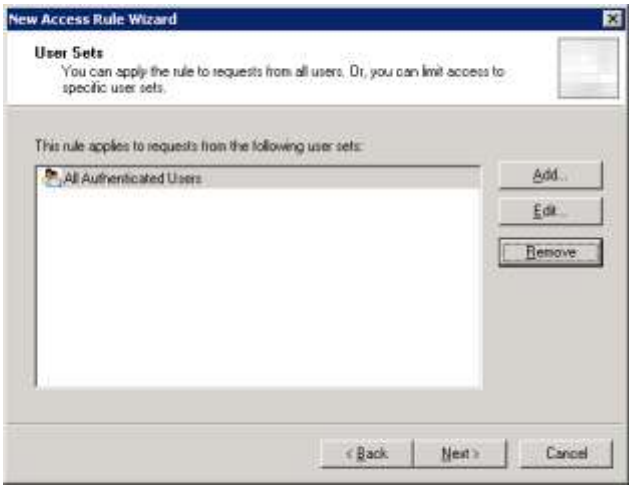
ISA User Authentication 2-8: Access Rule Destination

9. Select 'External' then 'Add'



ISA User Authentication 2-9: Network Entities - Destination

10. User Sets – Click 'Add'



User Sets

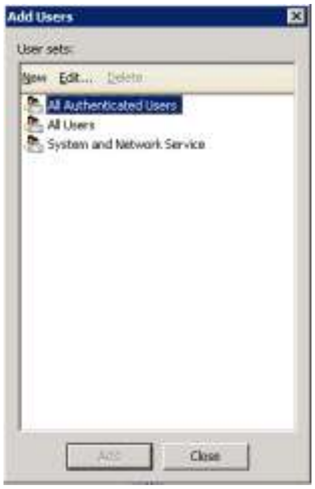
You can apply the rule to requests from all users. Or, you can limit access to specific user sets.

This rule applies to requests from the following user sets:

All Authenticated Users

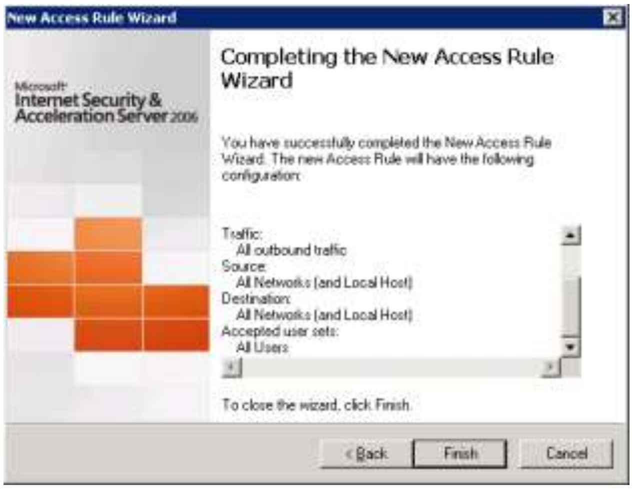
ISA User Authentication 2-10: Access Rule User Sets

11. Select ‘All Authenticated Users’ and click ‘Add’



ISA User Authentication 2-11: Add Users

12. Click ‘Finish’



Completing the New Access Rule Wizard

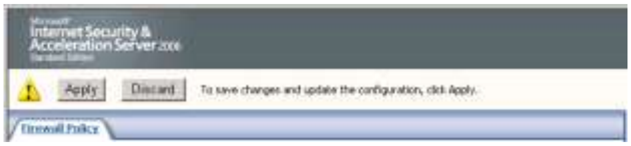
You have successfully completed the New Access Rule Wizard. The new Access Rule will have the following configuration:

```
Traffic:
   All outbound traffic
Source:
   All Networks (and Local Host)
Destination:
   All Networks (and Local Host)
Accepted user sets:
   All Users
```

To close the wizard, click Finish.

ISA User Authentication 2-12: Completing Access Rule Wizard

13. Be sure to hit ‘Apply’ to save changes and update the configuration in ISA.



To save changes and update the configuration, click Apply.

ISA User Authentication 2-13: Appling Changes

Chapter 3 bt-WebFilter Configuration

There are several steps you should consider prior to completing the configuration for bt-WebFilter. Having an general plan on what you want to accomplish ahead of time will make the configuration process easier and prevent you from possibly having to make significant changes later on.

1. Determine how you will be managing authorization for web access.
2. Determine how you will manage access to web categories.
3. Determine any Quota's that you would like to implement.
4. Determine the time that you would want to control access.

Determining Authorization for Web access

This is the first step as it defines how you will be creating your access policies. bt-WebFilter has the capability to control access via Active Directory membership and IP addressing. You can configure bt-WebFilter to use either of these options or a combination of both.

For example, you may want to manage access for users in your organization via their Active Directory accounts or group memberships as well as restrict access by IP's when 'unknown' users are connected to your guest network. This is easily accomplished within bt-WebFilter by creating the proper 'Access Rule.'

Determining Custom Access Policies to control what users can access.

Once you have identified how you will control access, the next step is identifying what access the users will have. Will Internet access be restricted to only authorized websites? Will users be able to surf any website as long as it is not prohibited?

Identifying the access types ahead of time will allow you to identify any potential issues and adjust prior to implementing the policies. For example, blocking the 'Job Search' category for your default organization policy may sound like a good idea when you're looking at the categories, but you may find that Human Resources is no longer able to access websites they need to perform their job functions.

A good starting point is to create a single policy and block only the 'Legal Liability' group of categories. There are 10 Categories blocked out of the box. These include:

- Spyware/Adware
- Criminal Skills
- Cults & Occult
- Extreme & Violence
- Gambling
- Hacking
- Hate Speech
- Weapons
- XXX-Sexual Content
- Malicious Code
- Mature

With these categories blocked and all others open, you can use Burstek's bt-LogAnalyzer to report on the traffic and determine where your users are going and if there is a potential problem.

Determine quota's to be implemented

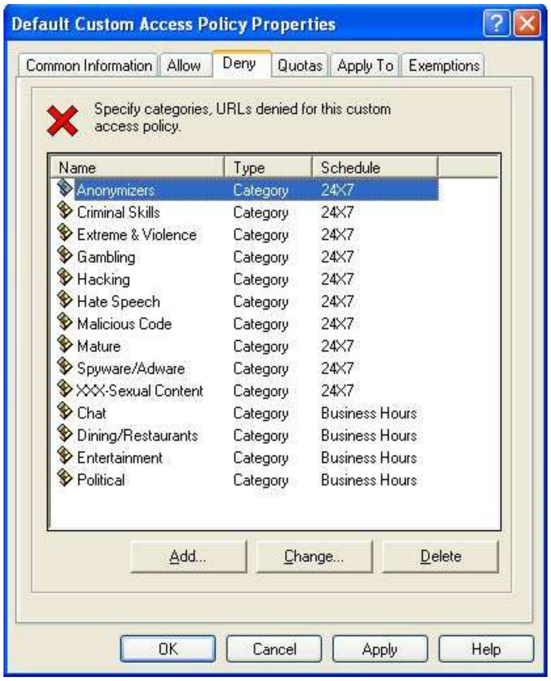
Preventing users from accessing websites may seem heavy handed to some companies and they may want to only limit the amount of time or the amount of bandwidth that users can consume for non-business related sites. bt-WebFilter can assist with this by allowing you to create quotas and assign them to specific Custom Access Policies or to your IP Range Access Rule.

Determine the time of day access will be controlled

Controlling access to Web pages during working hours

A common option is to restrict user browsing to authorized websites during normal business hours and open up a few non-business related URL categories for lunch.

bt-WebFilter gives you the option of setting unique schedules for your individual Web pages or URL Categories.



Specify categories, URLs denied for this custom access policy.

Name	Type	Schedule
Anonymizers	Category	24X7
Criminal Skills	Category	24X7
Extreme & Violence	Category	24X7
Gambling	Category	24X7
Hacking	Category	24X7
Hate Speech	Category	24X7
Malicious Code	Category	24X7
Mature	Category	24X7
Spyware/Adware	Category	24X7
XXX-Sexual Content	Category	24X7
Chat	Category	Business Hours
Dining/Restaurants	Category	Business Hours
Entertainment	Category	Business Hours
Political	Category	Business Hours

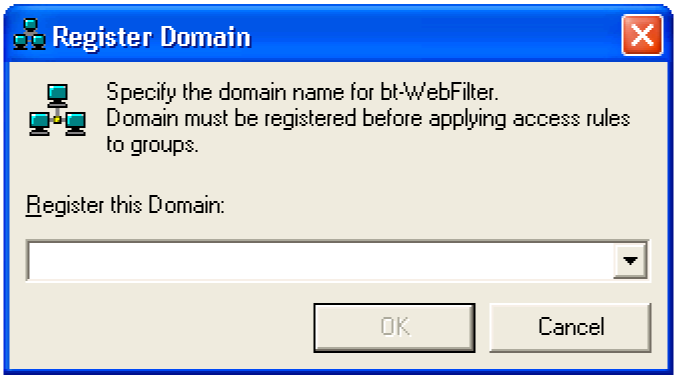
WebFilter Configuration 3-1: Default Custom Access Policy Properties

Setting the Access Rule Type

Registering your domain

To enable you to control access based on your users' logon names, you must register your domain with bt-WebFilter. To do this:

1. Open the bt-WebFilter application and right click on the 'Access Rules' option on the left side of the screen. Click on the option to 'Register Domain.' Figure 3-2 Window will display.



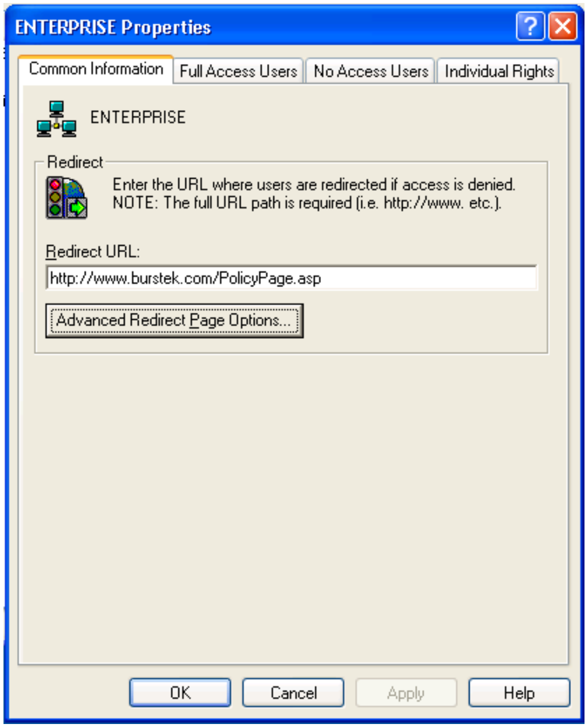
Specify the domain name for bt-WebFilter.
Domain must be registered before applying access rules to groups.

WebFilter Configuration 3-2: Domain Registration

2. Click the arrow to the right of the field and select your domain from the drop down box and click 'OK'

3. The ‘Properties’ page will be displayed. Here you can select additional options such as the redirect page that users will see when a website is blocked as well as individual user rights.

NOTE:
Burstek supplies several asp pages for various redirect options that you can modify to fit your individual needs. You must have access to a Microsoft Web Server to use these page options.



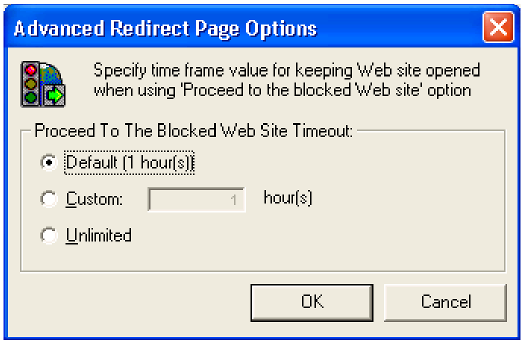
ENTERPRISE Properties

Enter the URL where users are redirected if access is denied.
NOTE: The full URL path is required (i.e. http://www. etc.).

Redirect URL: http://www.burstek.com/PolicyPage.asp

WebFilter Configuration 3-3: Domain Access Rule Properties

4. The ‘Advanced Redirect Page Options’ allows you to set the duration (in hours) that users can access a restricted site. Example, if you use one of the supplied redirect Web pages that allow the user to continue to a site but notify you of the action, you can select how long the site will remain open before being prompted again.



Advanced Redirect Page Options

Specify time frame value for keeping Web site opened when using 'Proceed to the blocked Web site' option

Proceed To The Blocked Web Site Timeout:

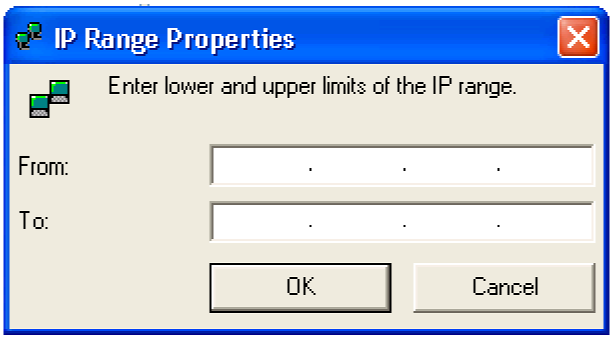
● Default (1 hour(s))
○ Custom: 1 hour(s)
○ Unlimited

WebFilter Configuration 3-4: Advanced Redirect Page Options

Registering an IP Range

To be able to create Access Policies based on IP addresses, you will need to create an Access Rule for the IP range that you wish to filter.

1. Open the bt-WebFilter application and expand the 'Access Rules' option on the left side of the screen.
2. Right click on the 'IP Ranges' option and select 'Register IP Range.'

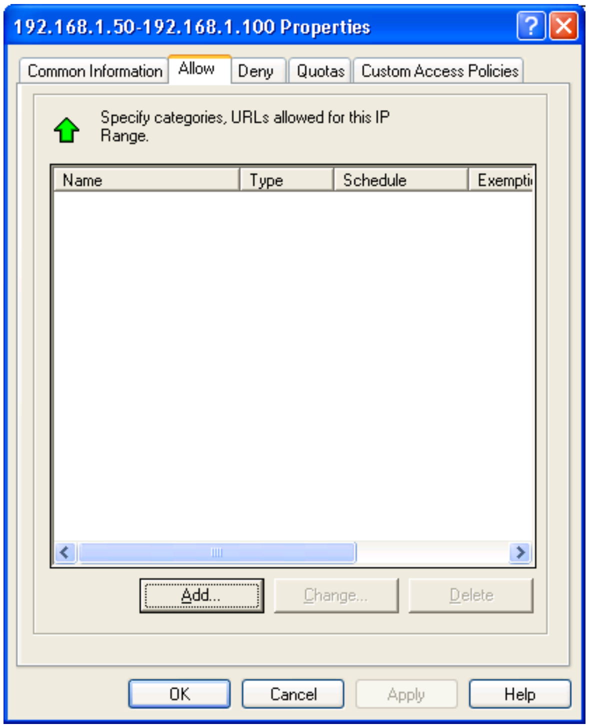


IP Range Properties

Enter lower and upper limits of the IP range.

WebFilter Configuration 3-5: Specifying an IP Range

3. Enter the starting IP address and the ending IP address of the range that you wish to create. You can create multiple IP ranges if you need to. When you have your range set, click 'OK'
4. The properties page for the range you just created will be displayed. From here you can add IP exemptions, change the Access Policy type, Allow or Deny URL's and categories, assign quotas and select the Access Policy you wish to apply.


192.168.1.50-192.168.1.100 Properties

Specify categories, URLs allowed for this IP Range.

Name	Type	Schedule	Exempti

WebFilter Configuration 3-6: IP Range Properties Page

5. When you have completed the configuration options for the IP range, click ‘Apply’ then ‘OK’ You can modify any IP range that you have entered by simply right clicking on the IP range and selecting ‘Properties’

Creating a Custom Access Policy

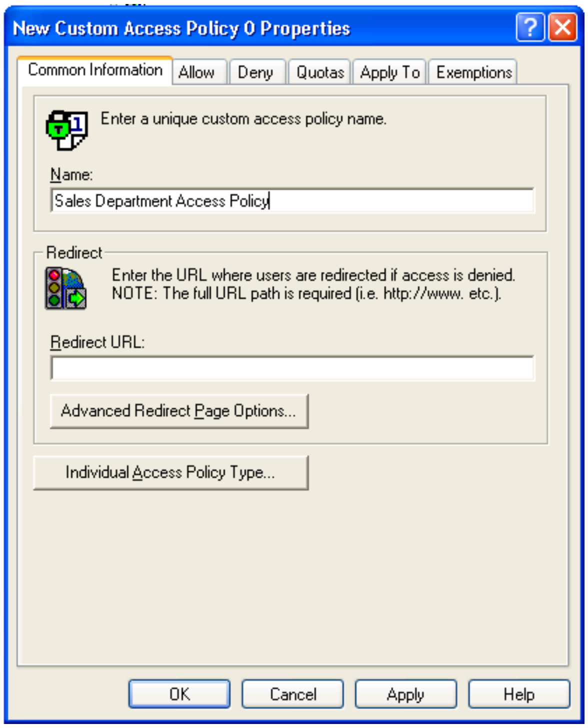
The ‘Custom Access Policy’ section is where you will setup the permissions for access to specific URL’s and Categories. Burstek currently has over 60 predefined Categories that you can select from or you can create your own based on your company’s requirements.

To setup a ‘Custom Access Policy’ follow these steps:

1. Open the bt-WebFilter application and select the ‘Custom Access Policies’ option.
2. On the right side of the console ‘Right Click’ and select ‘New’ then ‘Custom Access Policy’ from the menu.

NOTE:
The Default Custom Access Policy included with bt-WebFilter will block access to categories that are referred to as ‘Legal Liability.’ You can modify this policy or create your own.

3. The ‘New Custom Access Policy’ properties page will appear. Type in a name for your new access policy and click ‘Apply’



New Custom Access Policy 0 Properties

Enter a unique custom access policy name.

Name: Sales Department Access Policy

Redirect

Enter the URL where users are redirected if access is denied.
NOTE: The full URL path is required (i.e. http://www. etc.).

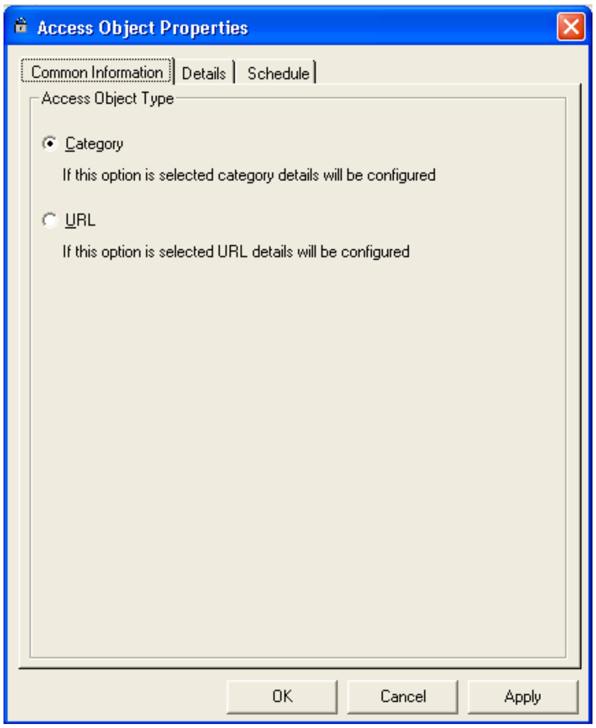
Redirect URL:

WebFilter Configuration 3-7: Custom Access Policy Properties Page

NOTE:

Depending on how you will be controlling access, you may consider naming your policies based on the groups covered. You may also choose to name your policies based on the type of access such as "Allow Access to Job Search Category".

4. By default, the 'Individual Access Policy Type' is set to the 'Default Policy' option. The default global 'Access Policy' is a restriction based policy type. More information regarding this topic can be found in the 'Custom Access Policies' section.
5. Since we are using the default policy type ('Restriction'), the 'Allow' tab is not used. Select the 'Deny' tab and click on the 'Add' button at the bottom of the screen. The 'Access Object' properties page will be displayed.



● Category

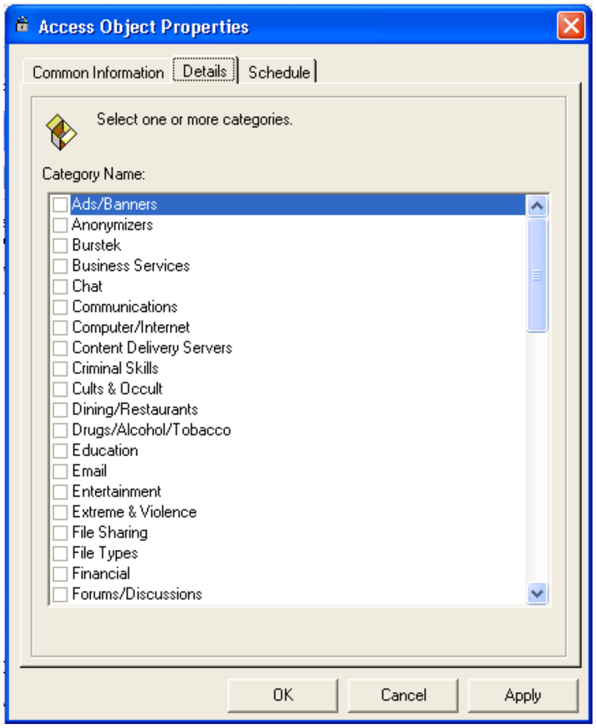
If this option is selected category details will be configured

○ URL

If this option is selected URL details will be configured

WebFilter Configuration 3-8: Access Object Properties - Common Information

6. Select the object type to be used to control access, ‘URL’ or ‘Category,’ and select the details tab.



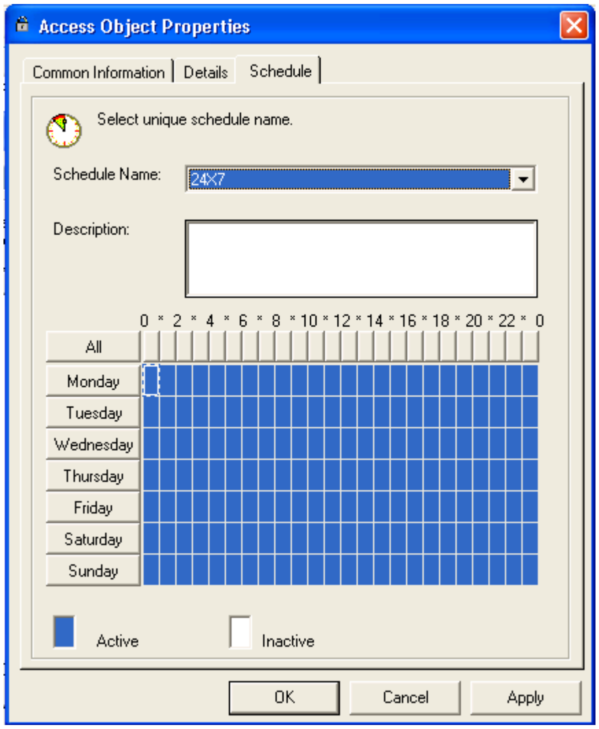
Select one or more categories.

Category Name:

- □ Ads/Banners
- □ Anonymizers
- □ Burstek
- □ Business Services
- □ Chat
- □ Communications
- □ Computer/Internet
- □ Content Delivery Servers
- □ Criminal Skills
- □ Cults & Occult
- □ Dining/Restaurants
- □ Drugs/Alcohol/Tobacco
- □ Education
- □ Email
- □ Entertainment
- □ Extreme & Violence
- □ File Sharing
- □ File Types
- □ Financial
- □ Forums/Discussions

WebFilter Configuration 3-9: Access Object Properties - Details

7. In figure 3-9, a list of individual Categories is displayed from which to select. To determine how a specific website is classified (which category it belongs to), use the ‘Category Lookup’ feature in the main console window.



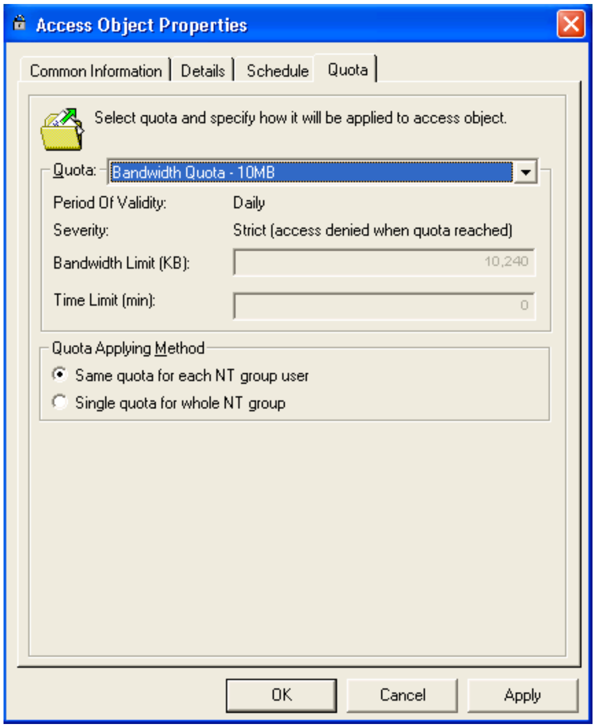
Select unique schedule name.

Schedule Name: 24X7

Description:

WebFilter Configuration 3-10: Access Object Properties - Schedule

8. The schedule tab will allow you to select the schedule name to be used for the Categories or URL’s that you have added. You can change the schedule at any time by going into the Access Policies properties. Since we haven’t created a new schedule yet, click ‘Apply’ and ‘OK’
9. The ‘Quota’ tab is similar to the ‘Allow’ and ‘Deny’ tabs except for the addition of the ‘Quota’ option (See figure 3-11). Here you would select any ‘Time’ or ‘Bandwidth’ quota’s that you define.



Select quota and specify how it will be applied to access object.

Quota: Bandwidth Quota - 10MB

Period Of Validity: Daily

Severity: Strict (access denied when quota reached)

Bandwidth Limit (KB): 10,240

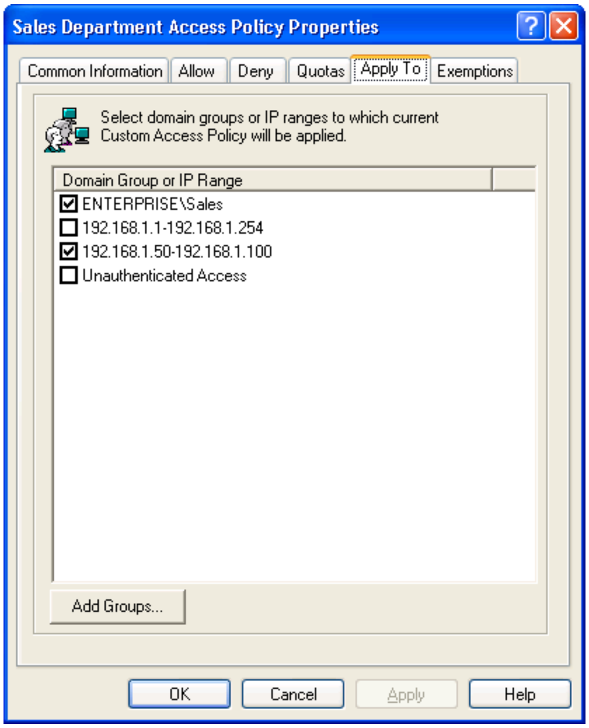
Time Limit (min): 0

Quota Applying Method

● Same quota for each NT group user

○ Single quota for whole NT group

WebFilter Configuration 3-11: Access Object Properties - Quota



Select domain groups or IP ranges to which current Custom Access Policy will be applied.

Domain Group or IP Range

☑ ENTERPRISE\Sales

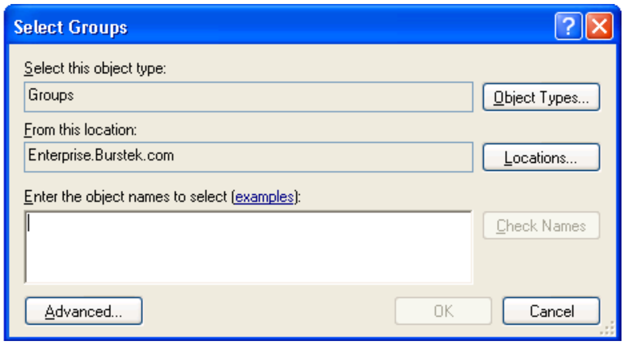
□ 192.168.1.1-192.168.1.254

☑ 192.168.1.50-192.168.1.100

□ Unauthenticated Access

WebFilter Configuration 3-12: Apply To

10. The ‘Apply To’ tab is where you will set the users, groups, and/or IP addresses that this ‘Access Policy’ will apply to. Selecting the ‘Add Groups’ button will launch the ‘Select Groups’ interface as shown in Figure 13. Type in the name of your group and select ‘Check Name’ then ‘Ok’


Select Groups

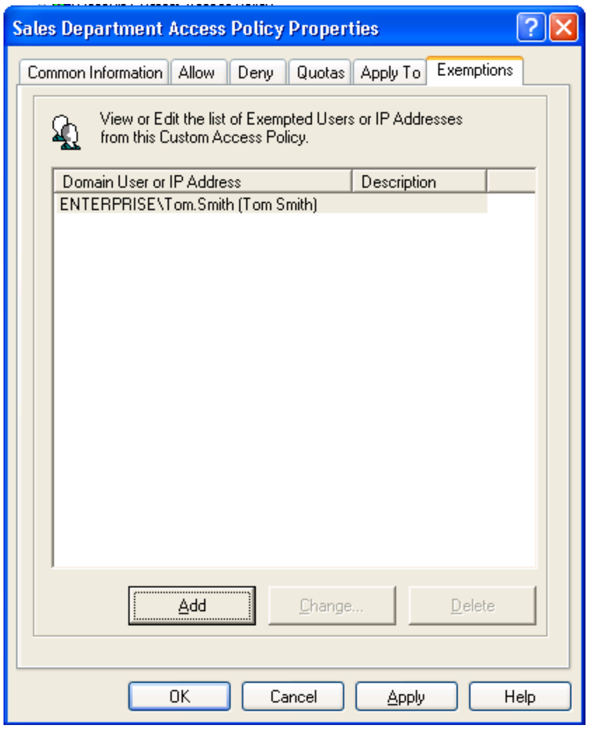
Select this object type: Groups

From this location: Enterprise.Burstek.com

Enter the object names to select (examples):

WebFilter Configuration 3-13: Select Groups

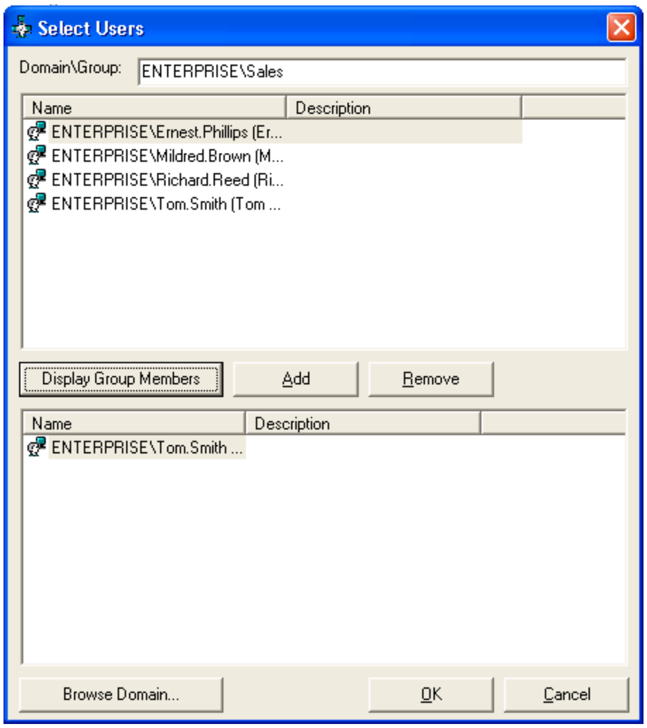
11. Selecting the ‘Exemptions’ tab will allow you to ensure that certain users are exempted from this policy. This can be useful when you want to exclude users that may be in a group that you applied the policy to. For example, if Tom Smith is a member of Enterprise\Sales but this policy does not apply to him, you would set his name on the ‘Exemptions’ tab.
12. To select users for exemption from the policy, click the ‘Add’ button. A small drop down will appear giving you the option of ‘User’ or (if you have an IP Range Access Rule defined) ‘IP Address.’ Selecting the ‘User’ option will open the select user’s window (see figure 3-15). Selecting the ‘IP Address’ will allow you to enter a single IP address as shown in figure 3-16.


Sales Department Access Policy Properties

View or Edit the list of Exempted Users or IP Addresses from this Custom Access Policy.

Domain User or IP Address	Description
ENTERPRISE\Tom.Smith (Tom Smith)	

WebFilter Configuration 3-14: Access Policy Exemptions



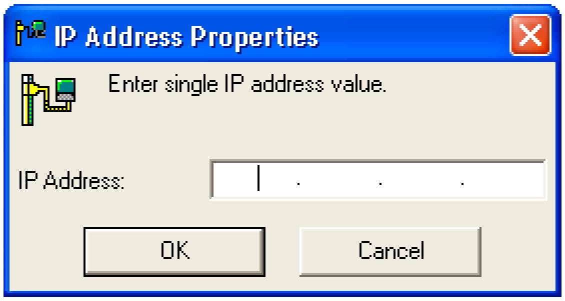
Domain\Group: ENTERPRISE\Sales

Name	Description
ENTERPRISE\Ernest.Phillips (Er...	
ENTERPRISE\Mildred.Brown (M...	
ENTERPRISE\Richard.Reed (Ri...	
ENTERPRISE\Tom.Smith (Tom ...	

Name	Description
ENTERPRISE\Tom.Smith ...	

WebFilter Configuration 3-15: Select Users

NOTE:
Selecting the ‘Display Group Members’ option will show all members of the selected group. You can then scroll through the list of users, select them, and click ‘Add.’



Enter single IP address value.

IP Address: . . .

WebFilter Configuration 3-16: IP Exclusion

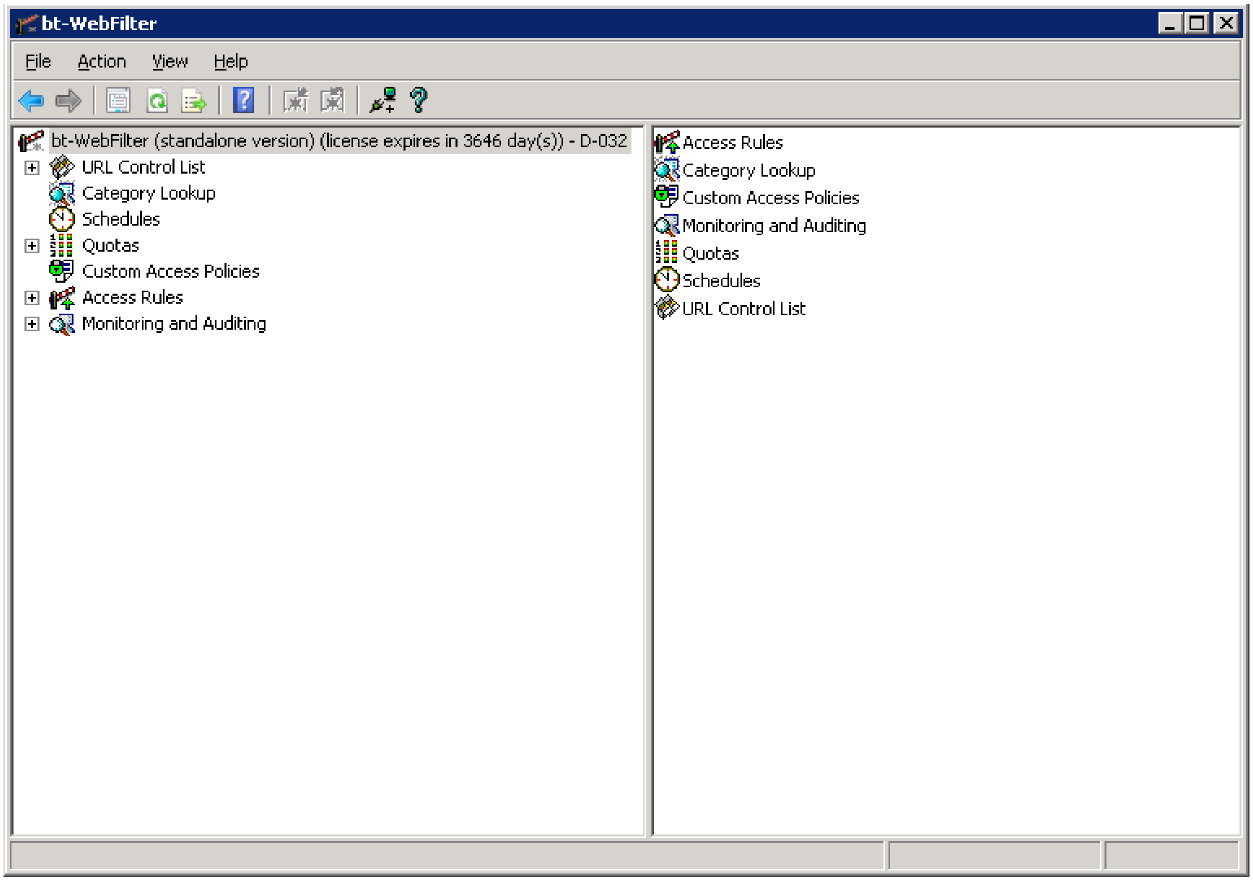
Chapter 4 The bt-WebFilter Console

bt-WebFilter's interface is designed around Microsoft's Management Console. The console is divided into the 'Container' window on the left and the 'Object' window on the right. From here you can manage all aspects of the application and check on the status of traffic moving through bt-WebFilter. The bt-WebFilter container object gives you a quick view of the version you are working with as well as the license expiration time (in days) and the server in which the application is installed

Server Properties

The bt-WebFilter Properties consist of four tabs:

- Storage and Customer Options
- Replication Options
- Proxy Options
- Cache Options
- Email Options



bt-WebFilter Management Console 4-1: Main Window

Storage and Customer Options

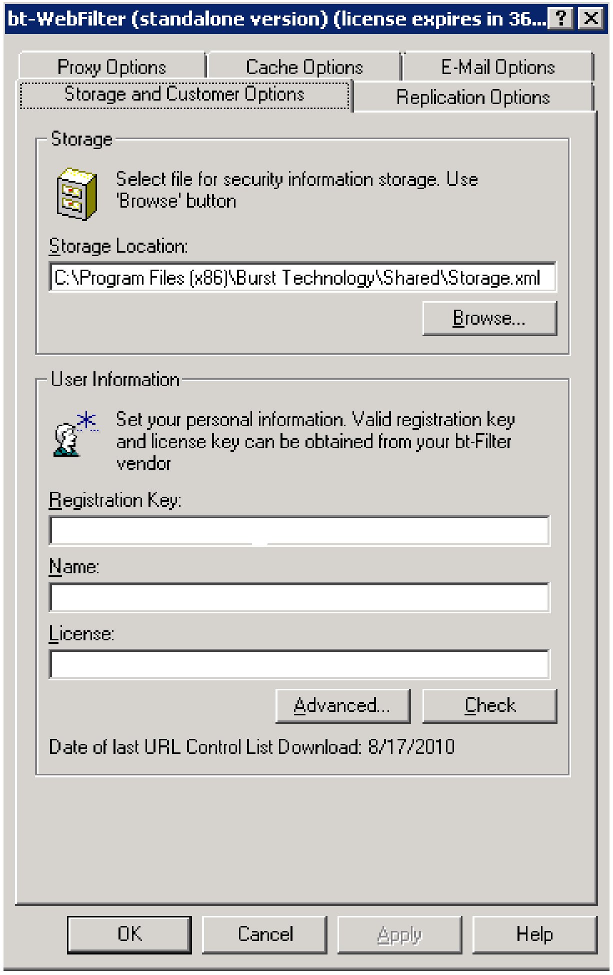
This tab provides the customer with the ability to modify the storage location of the Storage.xml file. This file contains group, user and URL Category information for the bt-WebFilter application.

License information is also stored on this tab. When you first install bt-WebFilter you are provided with a temporary key and license that will allow you full functionality of the product for 30 days. When you purchase the product from Burstek, you will be provided with your permanent licensing information. Enter the information in this location.

The 'Advanced' button allows the user to configure e-mail alerts that will be sent should the actual

To Access the 'Server Properties' section:

1. Open the bt-WebFilter Management Console
2. Right click on the bt-WebFilter container object and select properties. A Window similar to Figure 18 will display.



bt-WebFilter (standalone version) (license expires in 36...

Storage

Select file for security information storage. Use 'Browse' button

Storage Location: C:\Program Files (x86)\Burst Technology\Shared\Storage.xml

User Information

Set your personal information. Valid registration key and license key can be obtained from your bt-Filter vendor

Registration Key:

Name:

License:

Date of last URL Control List Download: 8/17/2010

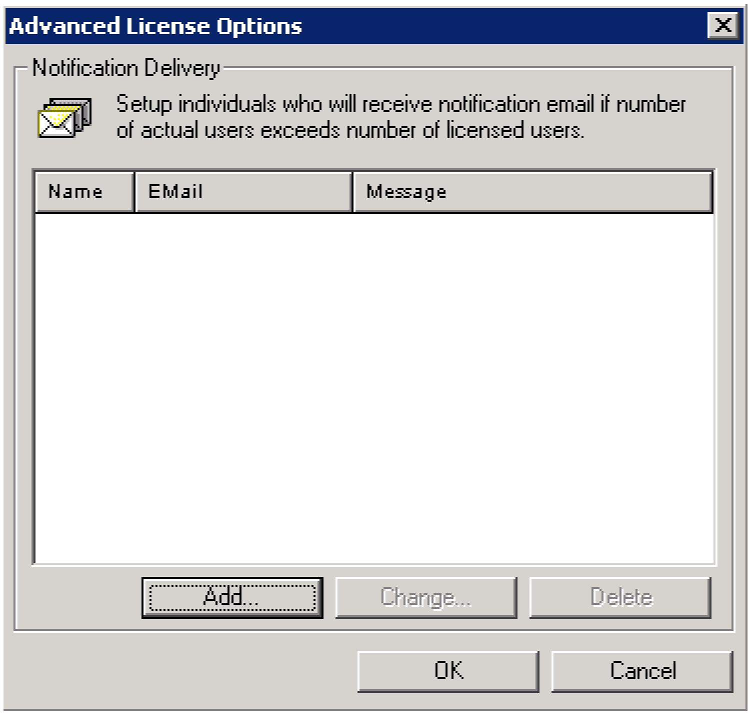
bt-WebFilter Management Console 4-2: Server Properties - Storage and Customer Options

Advanced License Count Options

When purchasing bt-WebFilter, organizations make their purchase based on the number of Internet unique IDs in their organization. When the number of unique IDs is exceeded, bt-WebFilter will not block or filter users that exceed the licensed user count. You can setup bt-WebFilter to send Email notifications if the licensed-user count is exceeded.

The 'Advanced' button allows the user to configure E-mail alerts that will be sent should the actual number of users surpass the licensed number of users.

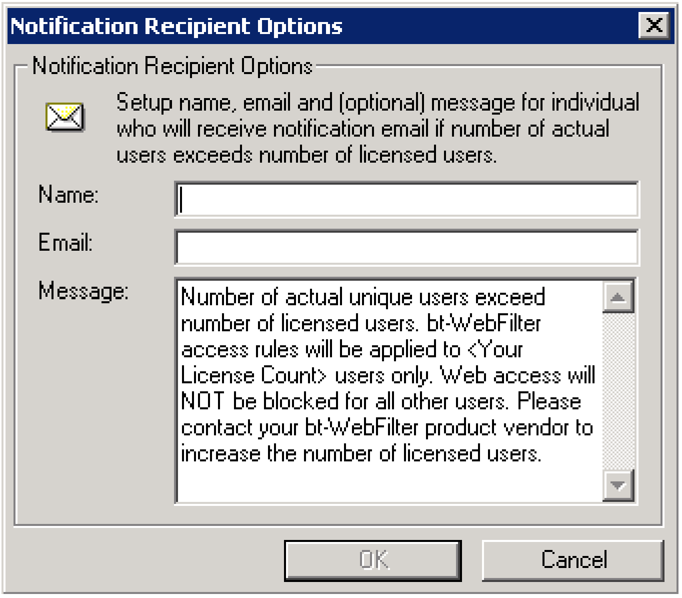
> **NOTE:**
> In order send alerts, you must configure the SMTP server information. Please refer to the 'Configuring E-Mail' section for more information on this topic.


Advanced License Options
Notification Delivery
Setup individuals who will receive notification email if number of actual users exceeds number of licensed users.
Name
EMail
Message
Add...
Change...
Delete
OK
Cancel

bt-WebFilter Management Console 4-3: Advanced License Options - Notification Delivery

To add users or distribution groups for notification:

1. Click on the 'Advanced' button on the 'Storage and Customer'
2. Click on the 'Add' button at the bottom of the 'Advanced License Options' window
3. Type the name and E-mail address of the person or group that you want to receive this type of message. You may also customize the message text.


Notification Recipient Options
Notification Recipient Options
OK
Cancel

Setup name, email and (optional) message for individual who will receive notification email if number of actual users exceeds number of licensed users.

Name:

Email:

Message: Number of actual unique users exceed number of licensed users. bt-WebFilter access rules will be applied to <Your License Count> users only. Web access will NOT be blocked for all other users. Please contact your bt-WebFilter product vendor to increase the number of licensed users.

bt-WebFilter Management Console 4-4: Notification Recipient Options

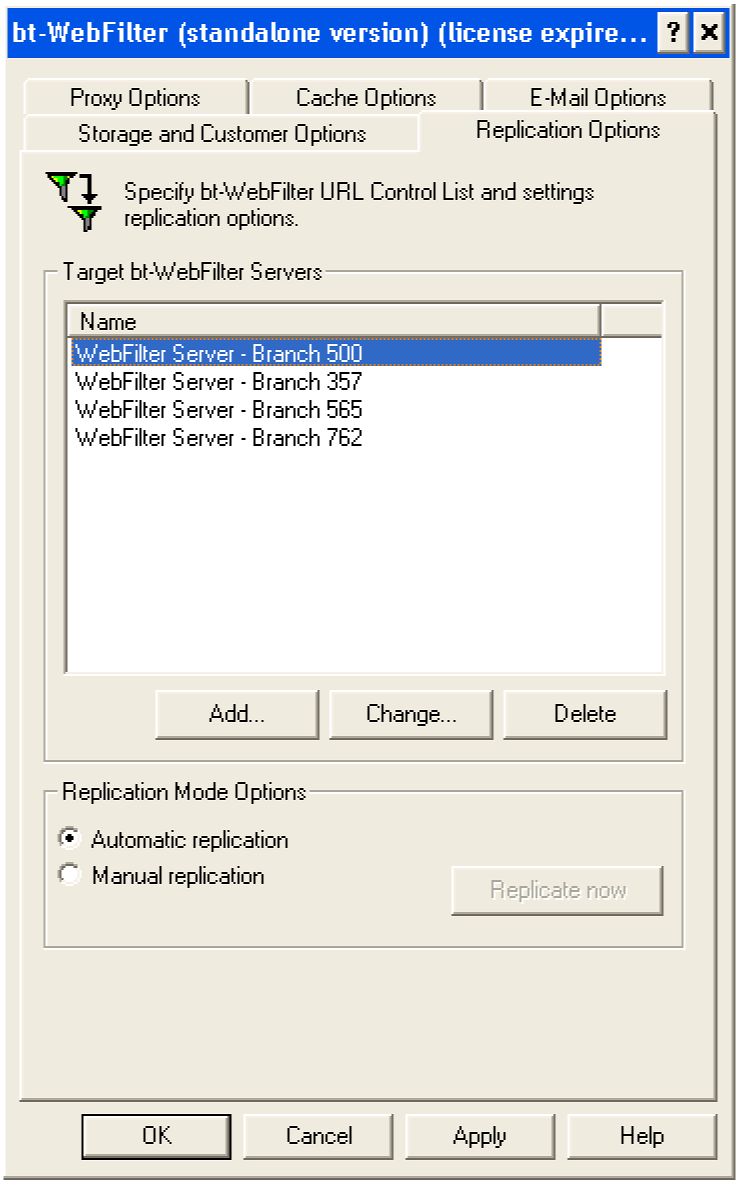
Replication Options

The 'Replication' option tab is used for adding additional bt-WebFilter servers that will receive changes made to the 'Master' server to maintain synchronization. bt-WebFilter will only replicate when a change has occurred on the 'Master' server such as Access Policy changes, Quota modification, Schedule changes, changes to Category includes and excludes, etc.

The Master server should have all the replication partners, the 'Slave' servers should not have this tab populated.

To setup Replication between two or more WebFilter servers:

1. Open the bt-WebFilter Management Console.
2. Right click on the bt-WebFilter container object and select properties. A screen similar to the one in figure 18 will appear.
3. Click on the 'Replication Options' tab.
4. Click on the 'Add' button in the 'Target bt-WebFilter Servers' section.
5. Type in a descriptive name for the target WebFilter server and click 'OK'
6. Set your replication choice.
    a. Automatic Replication – bt-WebFilter will replicate whenever a change is made to the server
    b. Manual Replication – Replication will take place only when the 'Replicate Now' button is pressed.



Specify bt-WebFilter URL Control List and settings replication options.

Target bt-WebFilter Servers

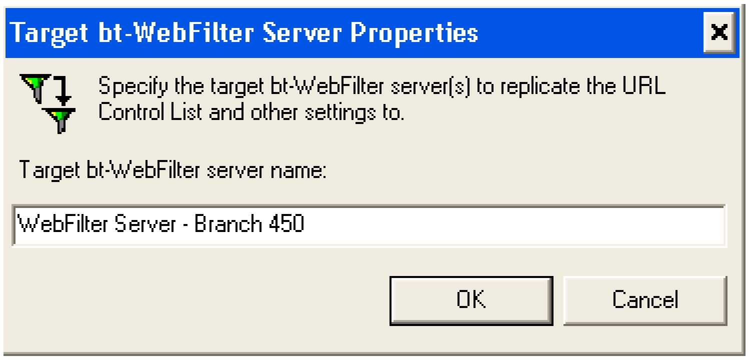
Name
WebFilter Server - Branch 500
WebFilter Server - Branch 357
WebFilter Server - Branch 565
WebFilter Server - Branch 762

Replication Mode Options

● Automatic replication

○ Manual replication

bt-WebFilter Management Console 4-5: Replication Options



Specify the target bt-WebFilter server(s) to replicate the URL Control List and other settings to.

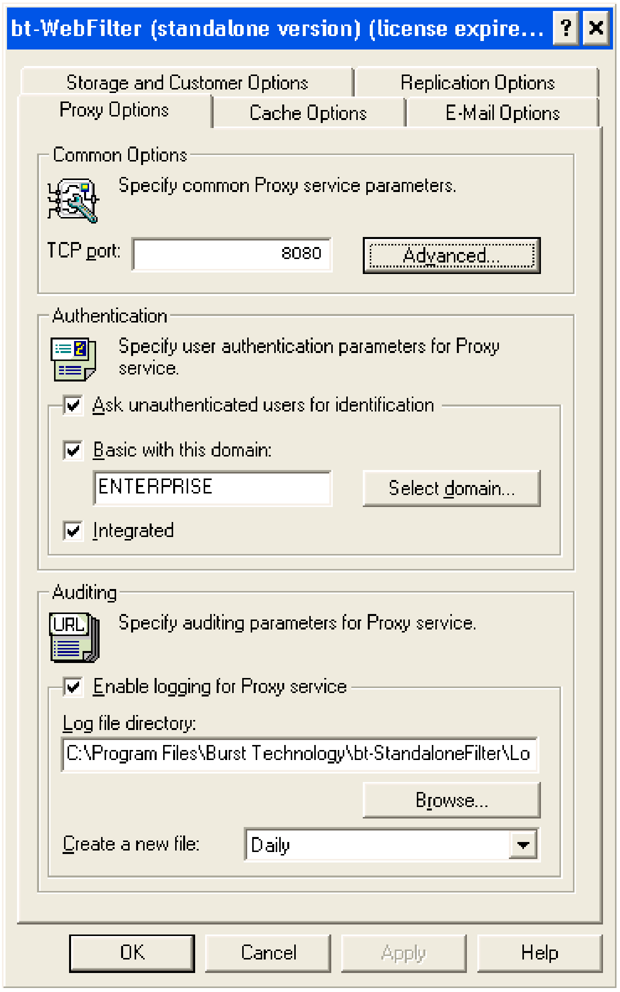
Target bt-WebFilter server name: WebFilter Server - Branch 450

bt-WebFilter Management Console 4-6: Adding a Target server for Replication

Proxy Options – bt-WebFilter Standalone only

When bt-WebFilter is installed in a standalone configuration it becomes your proxy server. As a proxy server, there are several options that need to be configured for correct operation such as the port settings, authentication, and logging. All of these can be found here.

The 'Common Options' section contains the 'TCP port' field where you can specify what port you want the server to listen to requests on.



bt-WebFilter (standalone version) (license expire...

Common Options

Specify common Proxy service parameters.

TCP port: 8080

Authentication

Specify user authentication parameters for Proxy service.

☑ Ask unauthenticated users for identification

☑ Basic with this domain: ENTERPRISE

☑ Integrated

Auditing

Specify auditing parameters for Proxy service.

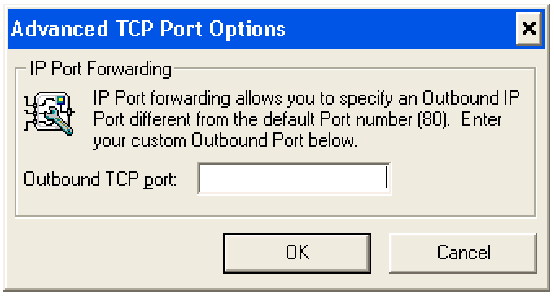
☑ Enable logging for Proxy service

Log file directory: C:\Program Files\Burst Technology\bt-StandaloneFilter\Lo

Create a new file: Daily

bt-WebFilter Management Console 4-7: Proxy Options Tab

The 'Advanced TCP Port Options' button will bring up the option for you to specify an alternate outbound port other than 80.


Advanced TCP Port Options

IP Port Forwarding

IP Port forwarding allows you to specify an Outbound IP Port different from the default Port number (80). Enter your custom Outbound Port below.

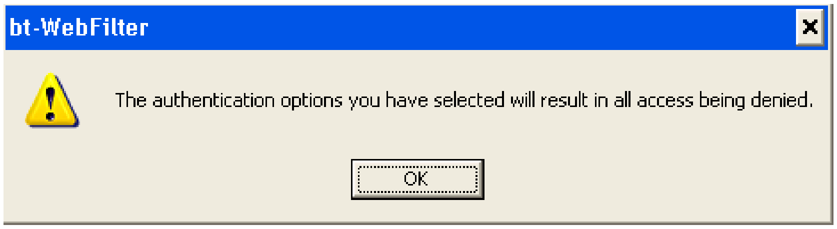
Outbound TCP port:

bt-WebFilter Management Console 4-8: Advanced TCP Port Options

The ‘Authentication’ section allows you to specify whether your users need to authenticate with the proxy server before they are allowed access. If you do not select users to authenticate, only anonymous users will show up in the filter and proxy logs.

- Ask unauthenticated users for identification – This requires authentication to the proxy server and enables selection of one or both of the authentication options.
- Basic with this domain – This option allows the use of Active Directory accounts and groups
- Integrated – Allows pass-through of credentials from logged-in user to be used for authenticating.

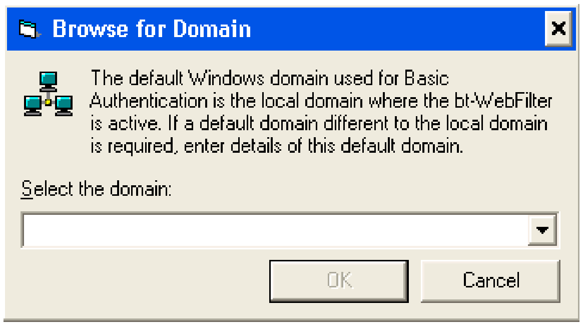
WARNING:
If you select to enable authentication but deselect both authentication types, then bt-WebFilter will block all Web traffic. A warning message is displaying informing you of this possibility.


bt-WebFilter

The authentication options you have selected will result in all access being denied.

bt-WebFilter Management Console 4-9: Authentication Options Warning

To specify your domain, put a check mark in the ‘Basic with this domain’ option and click the ‘Select Domain’ option. You should see your domain in the drop down.



The default Windows domain used for Basic Authentication is the local domain where the bt-WebFilter is active. If a default domain different to the local domain is required, enter details of this default domain.

bt-WebFilter Management Console 4-10: Browse for Domain Dialog

The 'Auditing' section allows you to enable logging for all traffic going through the proxy server and provides you with the ability to choose the location of the logs as well as how often a new log file should be created. The available options are:

- Daily
- Weekly
- Monthly
- Yearly

NOTE:
If you do not enable logging, bt-WebFilter will not show any URL's under the 'Monitoring and Auditing' objects Proxy Logs, Filter Logs, or any Filter Statistics for Users or Sites.

Cache Options

This tab is used to enable and manage the caching options for bt-WebFilter Standalone. To enable caching, put a check mark in the 'Enable Proxy caching' option. You can then modify the storage location as well as the storage size and memory usage for caching. You will also be able to manage caching age based on minimum and maximum times as well as percentage of total cache age.

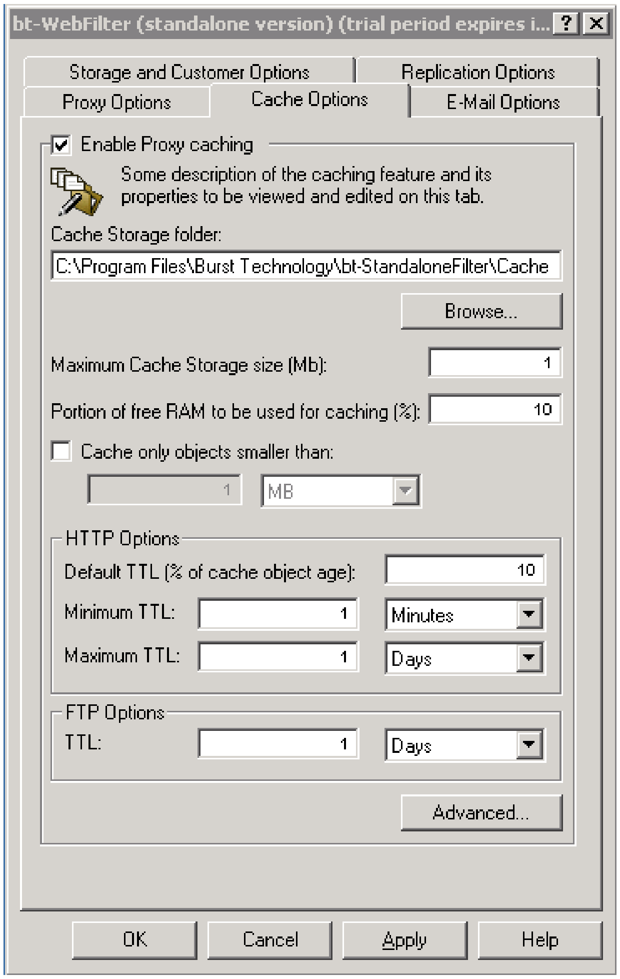
- Maximum Cache Storage Size (Mb): Setting this value will determine how much system storage the application will use to maintain its cache files.
- Portion of free RAM to be used for caching (%): This value can be set to limit the impact of caching on the proxy server.
- Cache only objects smaller than: Enabling this option provides more control over what is actually cached. You can specify sizes in either MB or KB.

HTTP Options

- Default TTL (% of cache object age):
- Minimum TTL:
- Maximum TTL:

FTP Options

- TTL:



☑ Enable Proxy caching

Some description of the caching feature and its properties to be viewed and edited on this tab.

Cache Storage folder: C:\Program Files\Burst Technology\bt-StandaloneFilter\Cache

Maximum Cache Storage size (Mb): 1

Portion of free RAM to be used for caching (%): 10

□ Cache only objects smaller than: 1 MB

HTTP Options

Default TTL (% of cache object age): 10

Minimum TTL: 1 Minutes

Maximum TTL: 1 Days

FTP Options

TTL: 1 Days

bt-WebFilter Management Console 4-11: Cache Options Tab

Advanced Cache Options

Selecting this button allows you to set your cache retrieval and replacement options.

Retrieval Policy:

The Retrieval Policy determines how the Cache serves requests for objects contained in its cache.

Return only valid objects:

- This option will return the objects in the cache if they are valid, otherwise it will send the request to the destination server

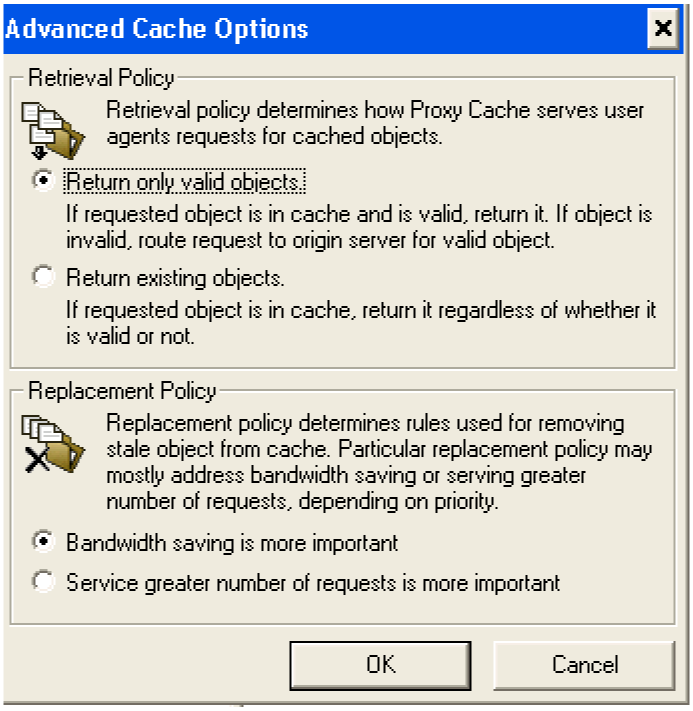
Return existing objects:

- This option will return the cache object regardless of its status. This can help in reducing bandwidth usage in larger environments

Replacement Policy:

The Replacement Policy determines how stale objects are removed from the cache. When selecting the Replacement Policy option, you determine priority between bandwidth usage savings or servicing a greater # of requests.

- Bandwidth saving is more important
- Service greater number of requests is more important



Advanced Cache Options

Retrieval Policy

Retrieval policy determines how Proxy Cache serves user agents requests for cached objects.

● Return only valid objects.

If requested object is in cache and is valid, return it. If object is invalid, route request to origin server for valid object.

○ Return existing objects.

If requested object is in cache, return it regardless of whether it is valid or not.

Replacement Policy

Replacement policy determines rules used for removing stale object from cache. Particular replacement policy may mostly address bandwidth saving or serving greater number of requests, depending on priority.

● Bandwidth saving is more important

○ Service greater number of requests is more important

bt-WebFilter Management Console 4-12: Advanced Cache Options

E-Mail Options

The ‘E-Mail Options’ tab provides the fields necessary for the administrator to configure the settings needed by bt-WebFilter to communicate with a messaging system.

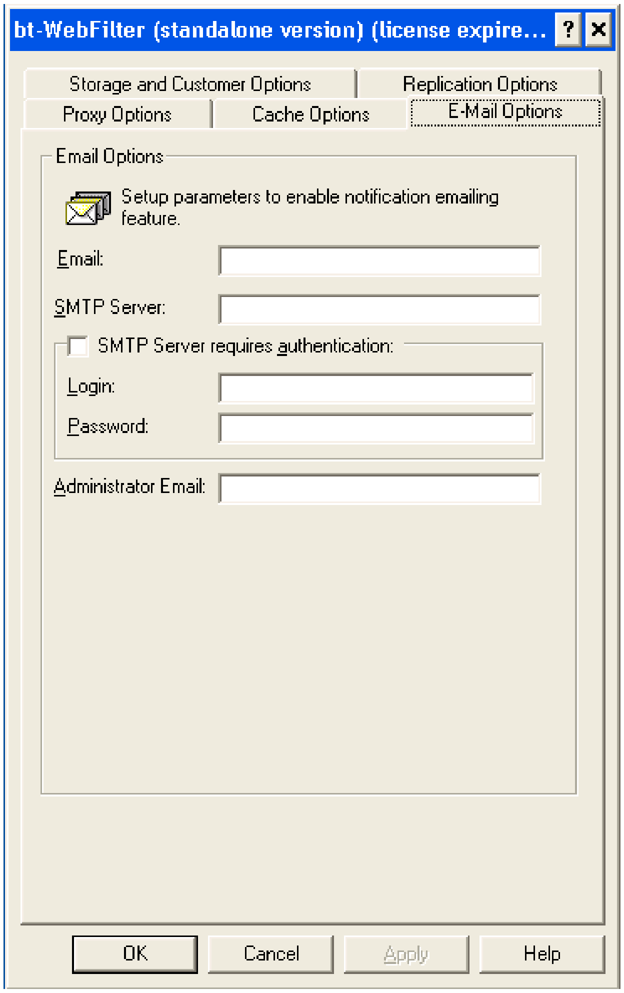
Email: The sending address that WebFilter is to use.

SMTP Server: The IP or Hostname of the E-mail server

SMTP Server requires authentication – Select this if your mail server requires you to login to send E-mail.

- Login:
- Password:

Administrator Email: The person or distribution group that will receive alerts from bt-WebFilter


bt-WebFilter (standalone version) (license expire...
?
Storage and Customer Options
Replication Options
Proxy Options
Cache Options
E-Mail Options
Email Options
Setup parameters to enable notification emailing feature.
Email:
SMTP Server:
SMTP Server requires authentication:
Login:
Password:
Administrator Email:
OK
Cancel
Apply
Help

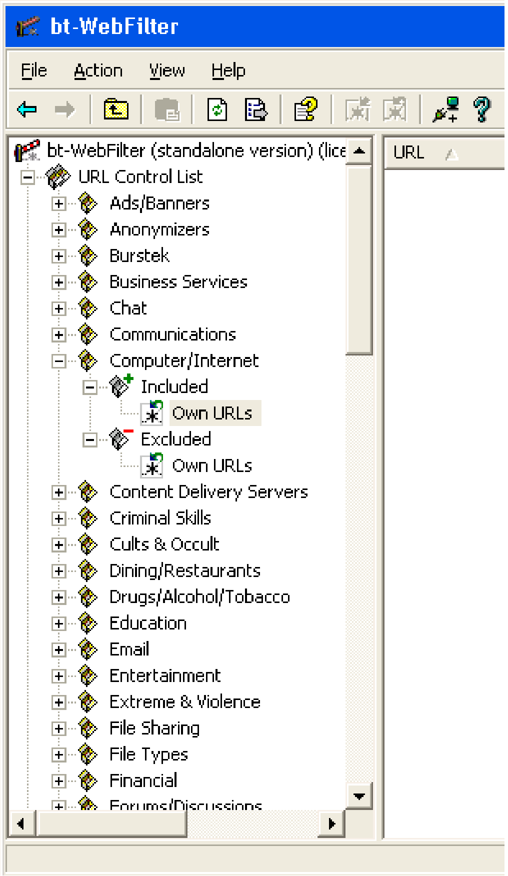
bt-WebFilter Management Console 4-13: E-Mail Options Tab

URL Control List

The URL Control List is at the center of all Burstek's products and contains over 60 predefined categories. URL's are added to individual categories based on their content and then those categories are applied to individual access policies to control and monitor access. Users can create their own set of Categories in this list by selecting 'New' from the context menu. There is no limit on the number of additional custom Categories that can be created.

To view and/or modify the Control List:

1. Open the Management Console
2. Expand the '+' sign next to the 'URL Control List' Container



bt-WebFilter Management Console 4-14: WebFilter's Control List

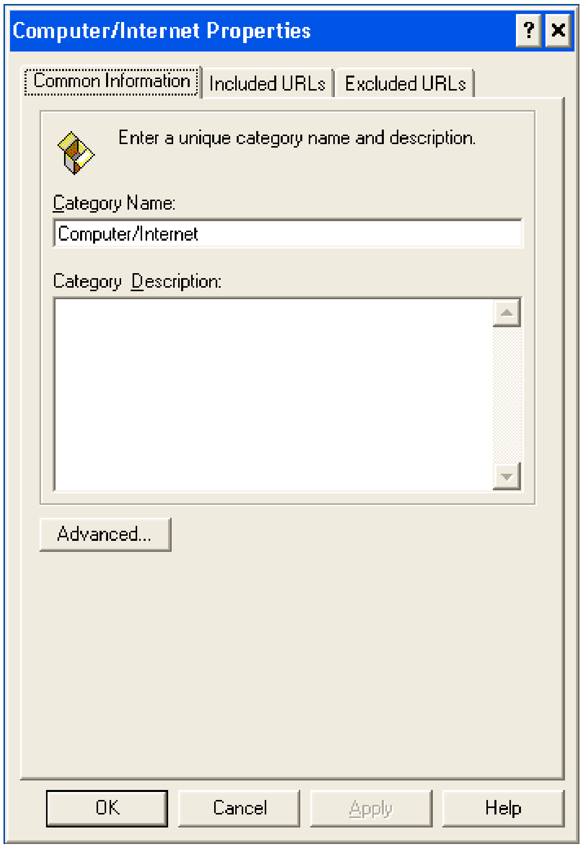
3. Find the Category that you want to modify and either right click and select 'Properties' or click the '+' next to the category to display the 'Included' and 'Excluded' URL objects.

NOTE:

Selecting 'Properties' will bring up a window that will allow you to modify the Category Description, Included URL's, Excluded URL's, and the Category Name.

WARNING:

If you rename a default Category, the next Control List update will add the category back in and you will have a duplicate item; however, no entries on the 'Exclusion' or 'Inclusion' tabs will be overwritten. Always create new custom access policies instead of attempting to rename the defaults.



Enter a unique category name and description.

Category Name: Computer/Internet

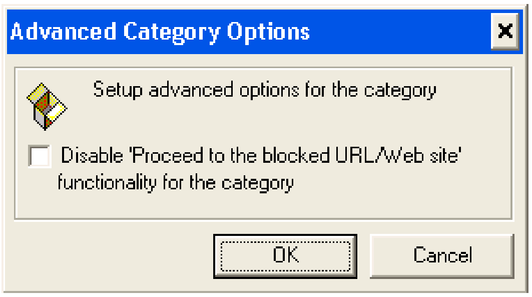
Category Description:

bt-WebFilter Management Console 4-15: URL Control List Category Properties

Common Information

- Category Name:
- Category Description:

Advanced Category Options – This option allows you to use a custom redirect page that may allow users to continue to a Webpage normally; however, if this option is checked, the users would still be denied.



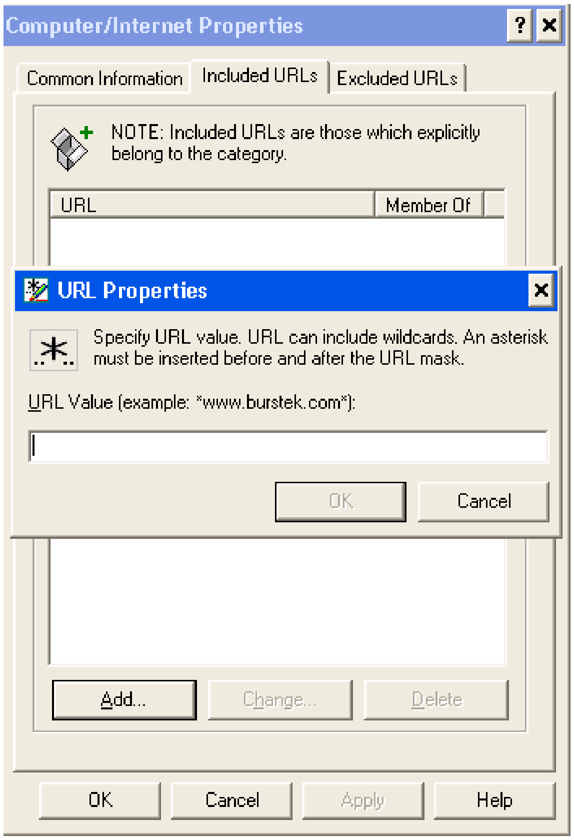
Setup advanced options for the category

□ Disable 'Proceed to the blocked URL/Web site' functionality for the category

bt-WebFilter Management Console 4-16: Advanced Category Options

Included URL’s

The ‘Included URLs’ tab is used to identify Websites that **WILL** explicitly belong to the category.



NOTE: Included URLs are those which explicitly belong to the category.

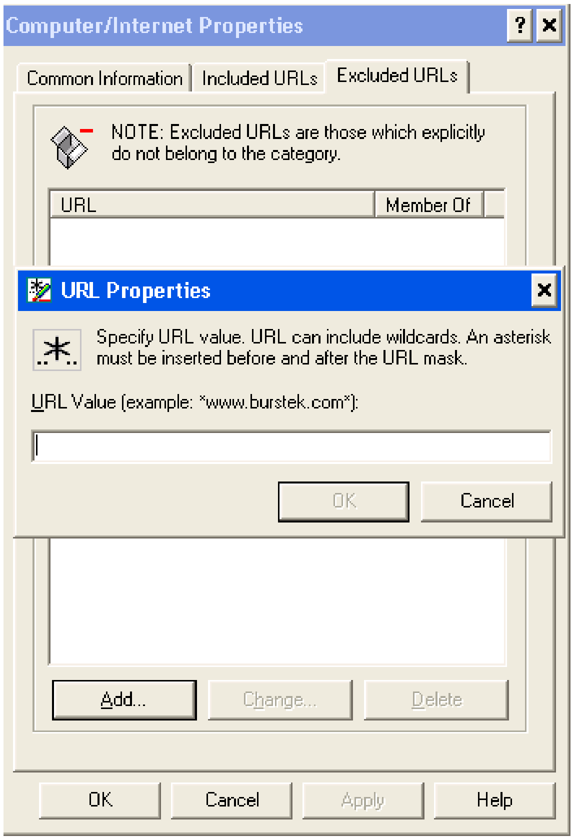
Specify URL value. URL can include wildcards. An asterisk must be inserted before and after the URL mask.

URL Value (example: *www.burstek.com*):

bt-WebFilter Management Console 4-17: Included URL's Tab

Excluded URL’s

The ‘Excluded URLs’ tab is used to identify Websites that **WILL NOT** explicitly belong to the category.

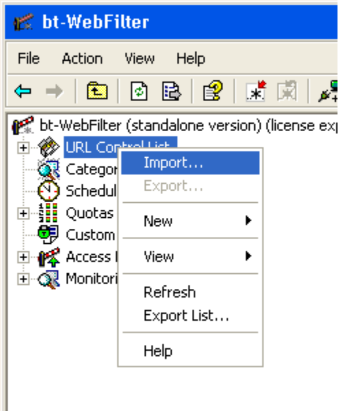

Computer/Internet Properties
Common Information
Included URLs
Excluded URLs
NOTE: Excluded URLs are those which explicitly do not belong to the category.
URL
Member Of
URL Properties
Specify URL value. URL can include wildcards. An asterisk must be inserted before and after the URL mask.
URL Value (example: *www.burstek.com*):
OK
Cancel
Add...
Change...
Delete
OK
Cancel
Apply
Help

bt-WebFilter Management Console 4-18: Excluded URL's Tab

Importing Categories

Burstek updates its URL Control List several times a day and bt-WebFilter allows you to manually import these updates or setup a schedule that will allow for automatic download and import.

To access this feature, from the Management Interface, right click on the 'URL Control List' category and select 'Import.'



bt-WebFilter Management Console 4-19: Importing Category Information

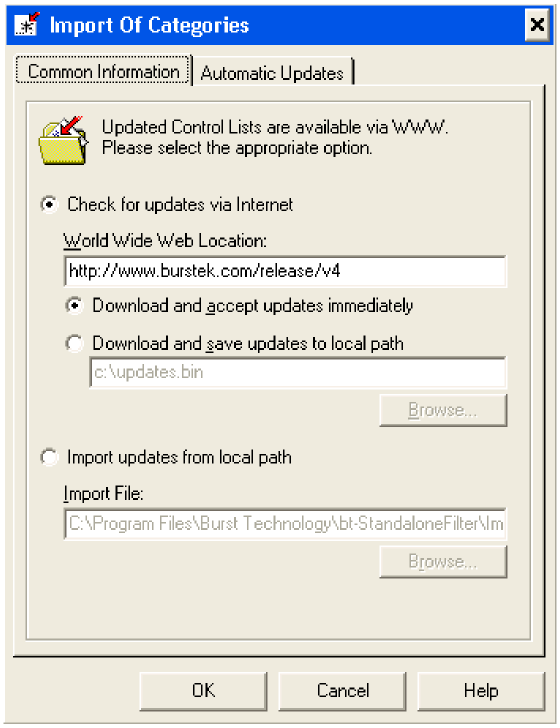
The ‘Import of Categories’ property window will be displayed.

Common Information Tab

This tab contains the fields used to specify where to get the updates and what to do with them. You may download the file manually and save to a specific location to be used at a later time or you can configure bt-WebFilter to download and install them automatically.

Automatic Updates

This tab allows you to specify when and how often bt-WebFilter will check for updates and allows you to disable the option completely if desired.



Import Of Categories

Updated Control Lists are available via WWW.
Please select the appropriate option.

● Check for updates via Internet

World Wide Web Location: http://www.burstek.com/release/v4

● Download and accept updates immediately

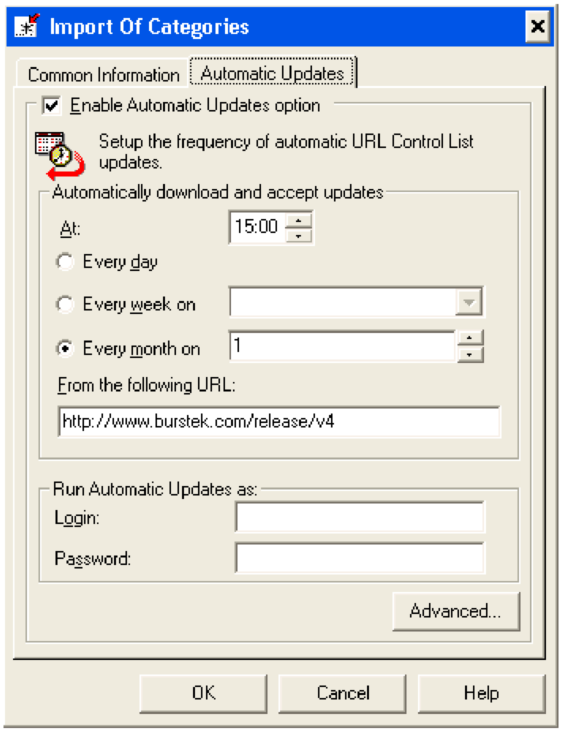
○ Download and save updates to local path: c:\updates.bin

○ Import updates from local path

Import File: C:\Program Files\Burst Technology\bt-StandaloneFilter\Im

bt-WebFilter Management Console 4-20: Import of Categories - Common Information

The ‘Run Automatic Updates as’ option is used when you have an upstream device that requires users to authenticate prior to allowing Internet access.



Import Of Categories

☑ Enable Automatic Updates option

Setup the frequency of automatic URL Control List updates.

Automatically download and accept updates

At: 15:00

○ Every day

○ Every week on

● Every month on 1

From the following URL: http://www.burstek.com/release/v4

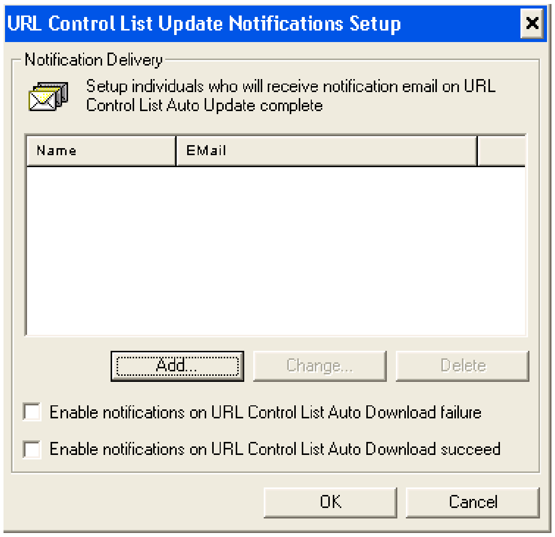
Run Automatic Updates as:

Login:

Password:

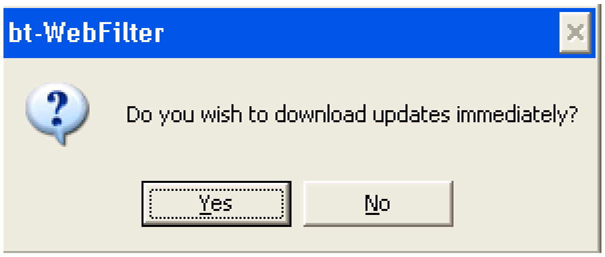
bt-WebFilter Management Console 4-21: Import of Categories - Automatic Updates

The 'Advanced' button brings up the 'URL Control List Update Notification Setup' options. Here you can select who will be notified of a successful or a failed download allowing prompt action to be taken to resolve the issue.


URL Control List Update Notifications Setup
Notification Delivery
Setup individuals who will receive notification email on URL Control List Auto Update complete
Name
EMail
Add...
Change...
Delete
□ Enable notifications on URL Control List Auto Download failure
□ Enable notifications on URL Control List Auto Download succeed
OK
Cancel

bt-WebFilter Management Console 4-22: URL Control List Notifications Setup

Clicking 'OK' when exiting this section of the interface will prompt you to 'Download updates immediately.' If just want this to occur during the schedule that you created click 'No.' However, if you want to verify that the updates will run correctly, click 'Yes' to test.



Do you wish to download updates immediately?

bt-WebFilter Management Console 4-23: Immediate Update Confirmation

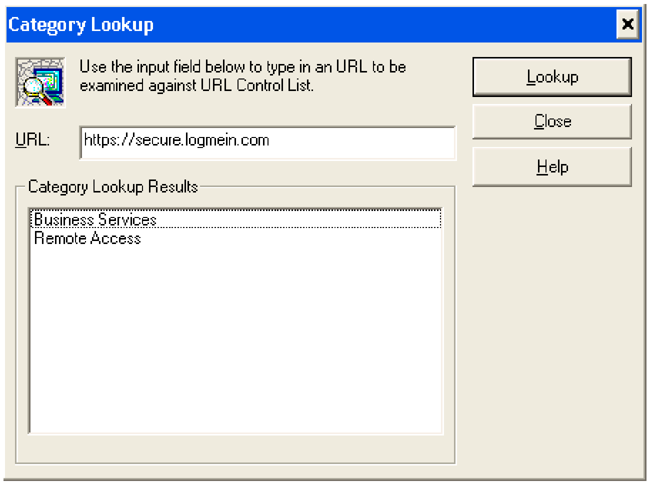
Category Lookup

The 'Category Lookup' container gives you the option to check any URL to determine its category. This allows you to modify the existing categories.

To lookup a URL:

1. Right Click on 'Category Lookup' on the left side of the Management Window.
2. Select 'Category Lookup' from the option window that appears.
3. Type in or copy and paste the URL to be checked into the URL field and click 'Lookup'

The lookup will then respond with the results of its search of categories that the URL matches.


Category Lookup
Use the input field below to type in an URL to be examined against URL Control List.
Lookup
Close
Help
Category Lookup Results

URL: https://secure.logmein.com

Business Services
Remote Access

bt-WebFilter Management Console 4-24: Category Lookup

Schedules

Schedules are used to determine when a restriction or permission on a specific category or URL should be in effect. Using the bt-WebFilter Scheduling properties, you can create templates to assign Internet access policies to different user groups as well as selecting the day(s) of the week and the time of day (24 hour clock) to activate or deactivate the policy.

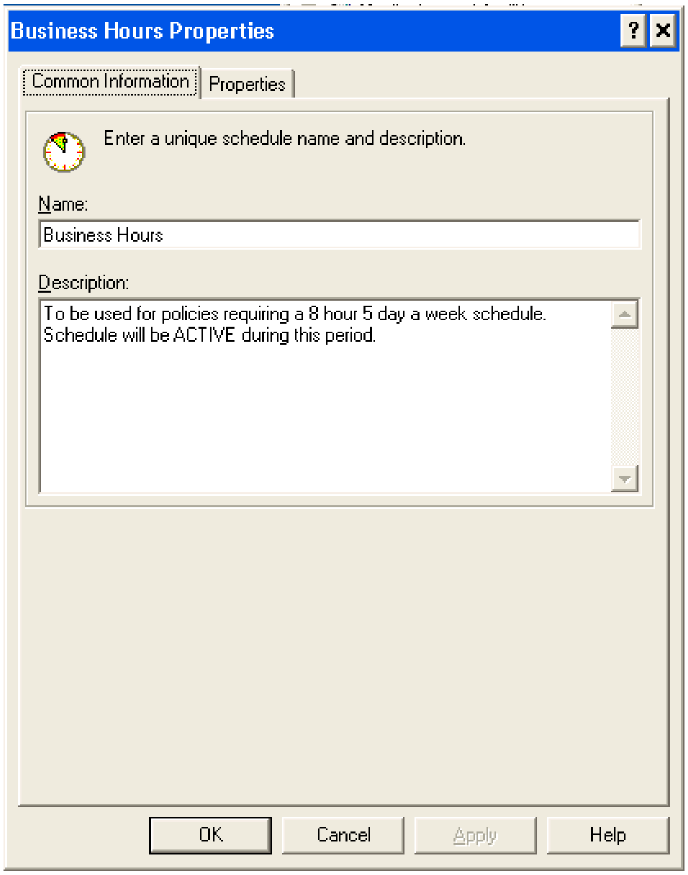
For example, if you wanted to block all access to the Internet except for certain allowed business sites during normal working hours but wanted to allow access to a few extra sites during lunch hours, you would create a ‘Lunch Hour’ schedule and make it active only for the lunch period. You would then add this schedule to the permission type Individual Access Policies allow tab for the specific Categories and or URL(s) to permit access.

NOTE:

If you choose to make the schedule an ‘Inactive’ policy in this example, it would have the opposite effect of allowing access to the sites except during the lunch hour.

To create a new Schedule:

1. Right click on the ‘Schedules’ container and select ‘New’ then ‘Schedule’
2. Type a name and a description for your new schedule



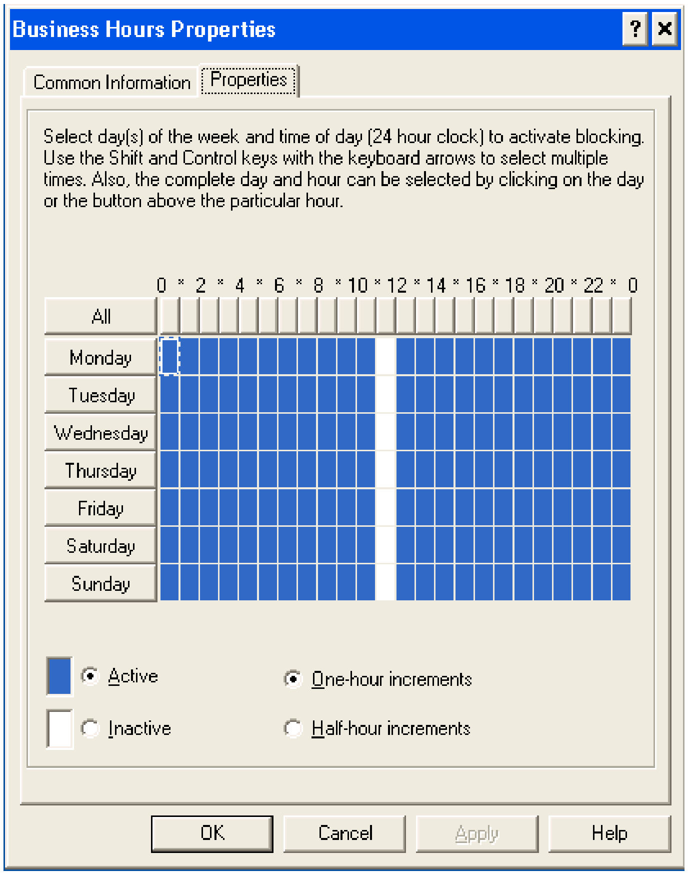
Enter a unique schedule name and description.

Name:
Business Hours

Description:
To be used for policies requiring a 8 hour 5 day a week schedule.
Schedule will be ACTIVE during this period.

bt-WebFilter Management Console 4-25: Custom Schedule - Common Information Tab

3. Click the 'Properties' tab
4. Select the time increments that you want to use
5. Drag your curser over the hours that you want to effect and choose the appropriate type (Active, Inactive)



Select day(s) of the week and time of day (24 hour clock) to activate blocking. Use the Shift and Control keys with the keyboard arrows to select multiple times. Also, the complete day and hour can be selected by clicking on the day or the button above the particular hour.

● Active

○ Inactive

● One-hour increments

○ Half-hour increments

bt-WebFilter Management Console 4-26: Custom Schedule - Properties Tab

6. Click ‘Apply’ then ‘OK’

Quotas

bt-WebFilter allows you to create Quotas to limit time spent on a single Website, Category or a group of Categories; or limit overall bandwidth use. Quotas may be applied to a group or an individual within your organization.

Quota properties

The Quota properties window has the following options:

1. Name of the Quota

2. Period Of Validity – Specifies when the quota should reset its usage data

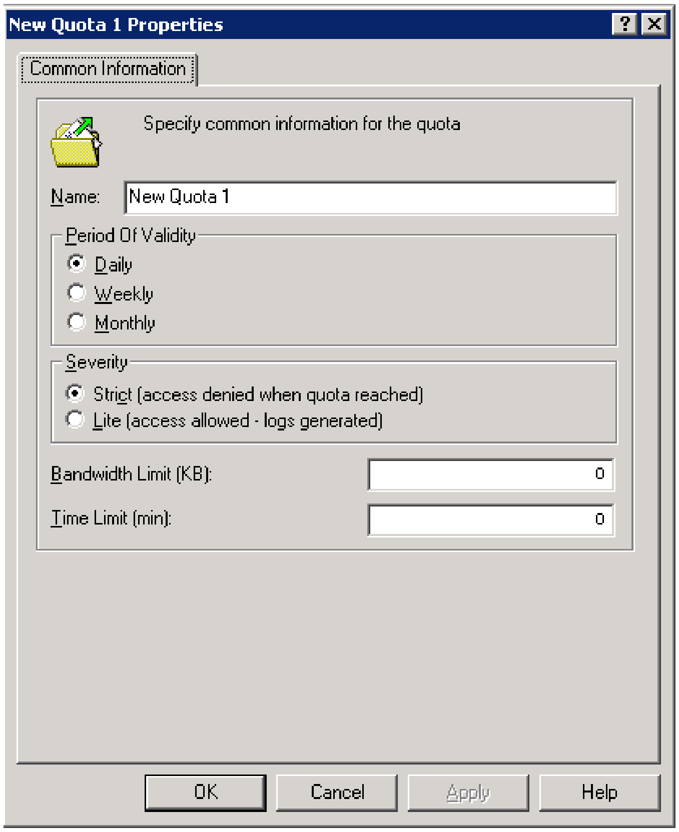
   - Daily
   - Weekly
   - Monthly

3. Severity

   - Strict – when the quota limit is reached, access will be denied for the objects governed by the quota
   - Lite – when the quota limit is reached, access will be granted but logs will be generated for the objects governed by the quota.

4. Bandwidth Limit (KB)

5. Time Limit (min)



New Quota 1 Properties

Common Information

Specify common information for the quota

Name: New Quota 1

Period Of Validity
- ● Daily
- ○ Weekly
- ○ Monthly

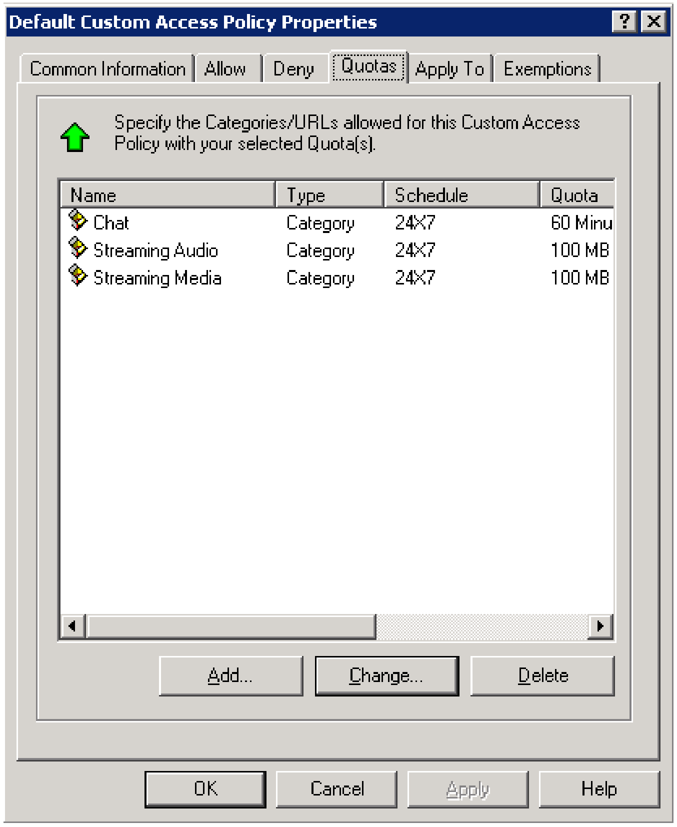
Severity
- ● Strict (access denied when quota reached)
- ○ Lite (access allowed - logs generated)

Bandwidth Limit (KB): 0

Time Limit (min): 0

bt-WebFilter Management Console 4-27: Quota Properties Window

A quota is assigned to ‘Individual Access Policies’ (see the ‘Custom Access Policies section’) and the categories that you want the Quota to apply to. Multiple quotas can be added to the same Individual Access Policy and be applied to different categories. For example, if you want to have a Time based quota for the ‘Chat’ category and a ‘Bandwidth’ based quota for the ‘Streaming Audio’ and ‘Streaming Media categories, all you would need to do is create the individual quotas and assign them to the Individual Access Policy. (See Figure 43)

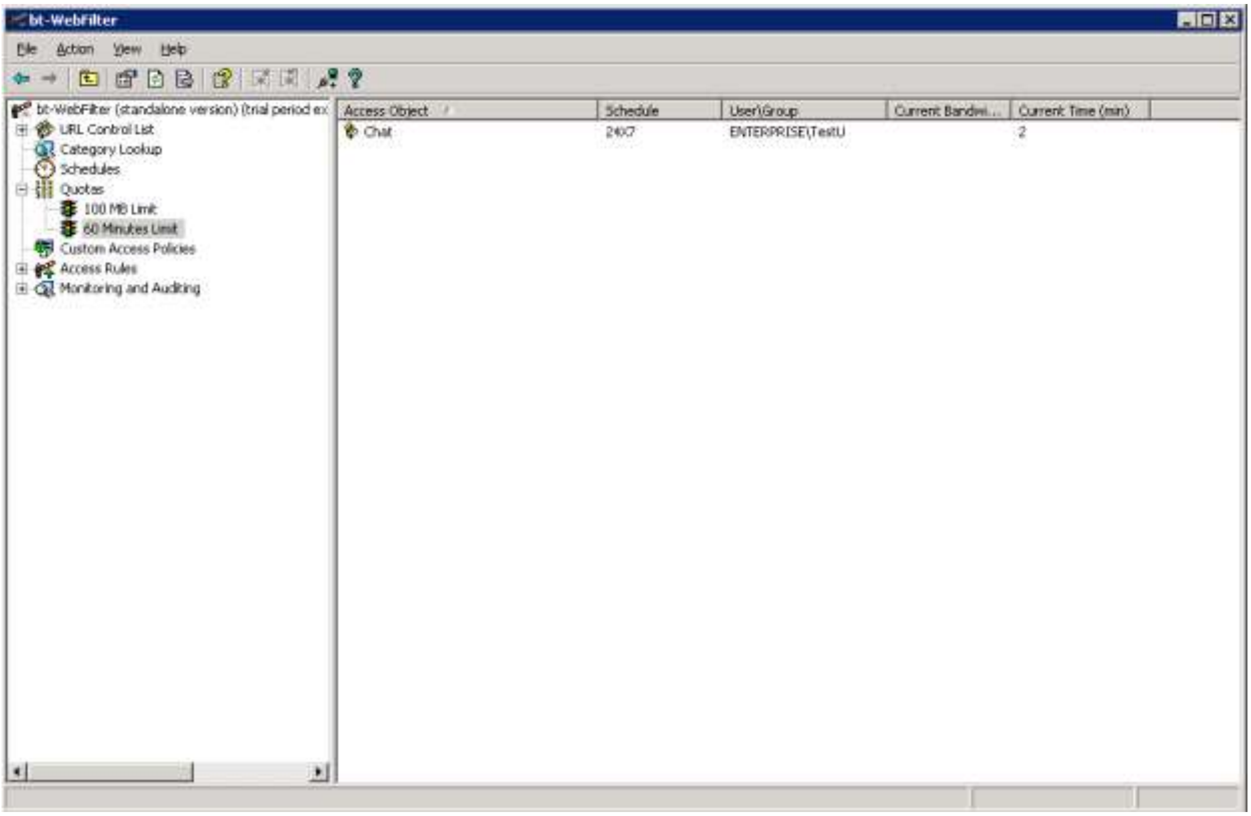


Specify the Categories/URLs allowed for this Custom Access Policy with your selected Quota(s).

Name	Type	Schedule	Quota
Chat	Category	24X7	60 Minu
Streaming Audio	Category	24X7	100 MB
Streaming Media	Category	24X7	100 MB

bt-WebFilter Management Console 4-28: Quota's Applied to Categories

At anytime, you can view the status of users and how their surfing habits are having an effect on the quota. You can also reset the user's quota usage if needed.



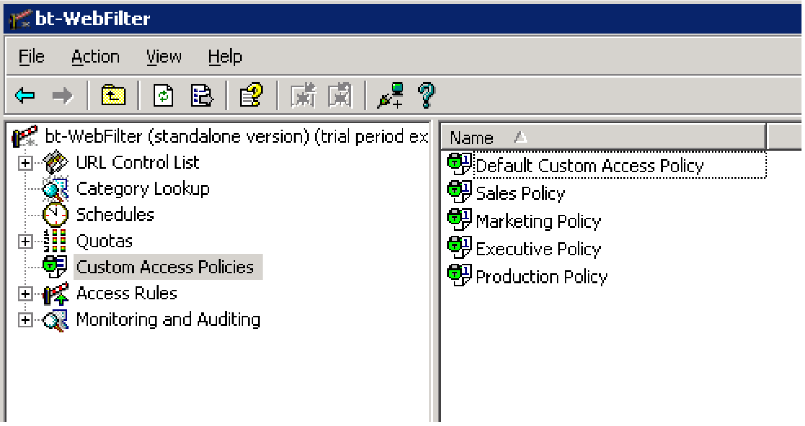
Access Object	Schedule	User\Group	Current Bandwi...	Current Time (min)
Chat	24X7	ENTERPRISE\TestU		2

bt-WebFilter Management Console 4-29: Quota Usage per Access Object

Custom Access Policies

The bt-WebFilter program allows the Administrator to create custom Access Policies and apply the policies to domain groups or IP ranges. While the URL Control List is the heart of the application, the Individual Access Policies are the brain. The Individual Access Policies are the logic that makes the determination on what type of access, who gets access, where do they have access to, what restrictions or permissions come in to play, etc.

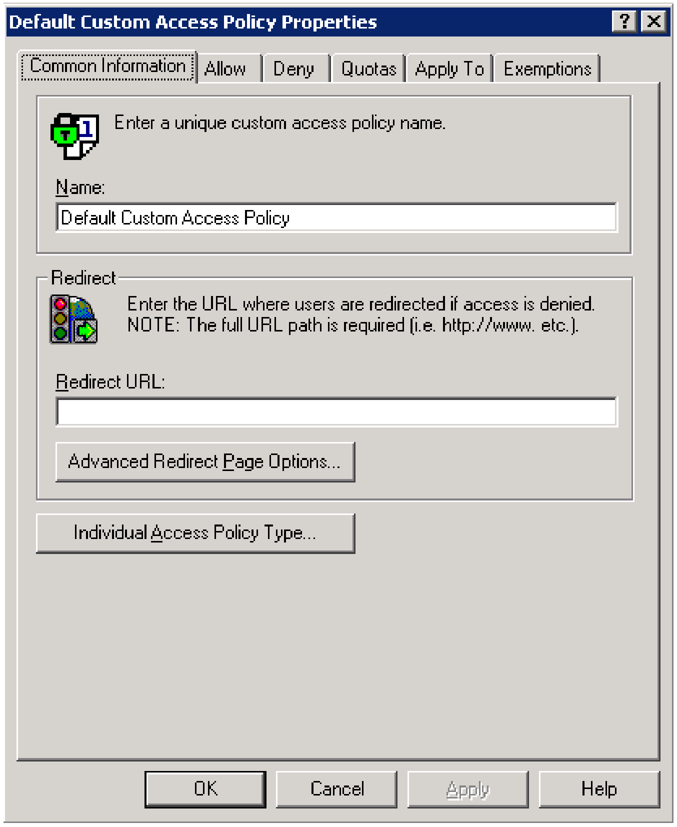
You can set a single Individual Access Policy for your entire organization or you can create an Access Policy for each Department, Security Group, or IP address Range. Figure 45 shows several Individual Access Policies representing multiple departments within a company and a 'Default Custom Access Policy' that can be applied to all users of bt-WebFilter.



bt-WebFilter Management Console 4-30: Custom Access Policy Container

An Individual Access Policy contains six tabs to allow you to configure for your environment and understanding what each one provides you will help you configure bt-WebFilter to provide the best possible operation to your organization.

1. Common Information
2. Allow
3. Deny
4. Quotas
5. Apply To
6. Exemptions



Default Custom Access Policy Properties

Enter a unique custom access policy name.

Name: Default Custom Access Policy

Redirect

Enter the URL where users are redirected if access is denied.
NOTE: The full URL path is required (i.e. http://www. etc.).

Redirect URL:

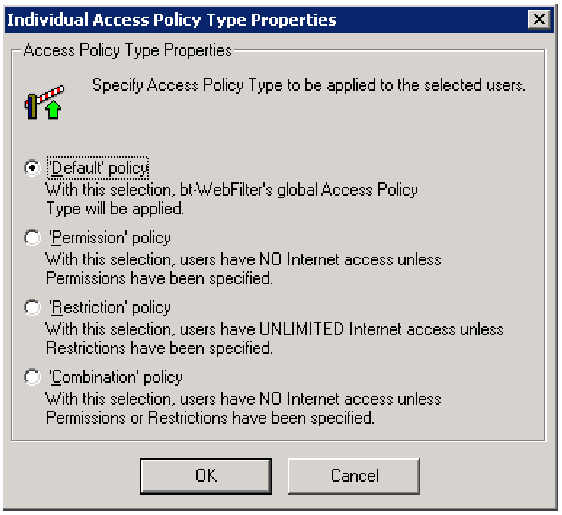
bt-WebFilter Management Console 4-31: Individual Custom Acces Policy - Common Tab

Common Information

This tab provides you with the options of naming your policy, assigning a specific Redirect URL that will affect just this policy, as well as the type of policy that will be used.

If you click on the 'Individual Access Policy Type' you will be presented with four options

- Default Policy – As the name suggests, this is the default configuration for the Individual Policy and it takes on whatever policy type you have set in the 'Global Access Policy' (See 'Access Rules').
- Permission Policy – This policy is similar to an implied DENY. It will deny all URL access unless specifically allowed. Only the 'Allow' tab is used with this policy type.
- Restriction Policy – This policy type is similar to an Explicit deny. It will ALLOW all URL access unless specifically denied. Only the 'Deny' tab is used with this policy type.
- Combination Policy – This policy type functions as a permission policy but uses both the 'Deny' and 'Allow' tabs. By default, this policy functions initially as a Permission policy in that all Web access is prohibited until specifically allowed but also allows for the use of the Deny tab to further restrict an allowed category. A policy of this type would be used to restrict users to a certain portion of a website. For example, the shipping department may need access only the section of a website concerned with shipping and receiving activities.



Individual Access Policy Type Properties

Access Policy Type Properties

Specify Access Policy Type to be applied to the selected users.

● 'Default' policy
With this selection, bt-WebFilter's global Access Policy Type will be applied.

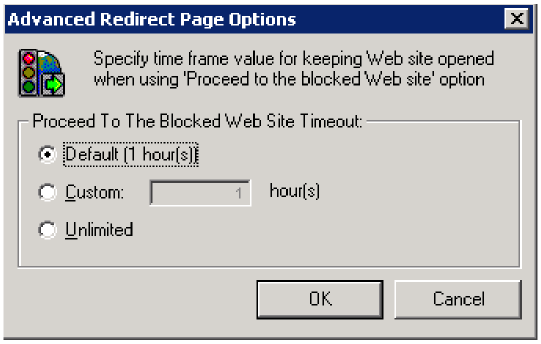
○ 'Permission' policy
With this selection, users have NO Internet access unless Permissions have been specified.

○ 'Restriction' policy
With this selection, users have UNLIMITED Internet access unless Restrictions have been specified.

○ 'Combination' policy
With this selection, users have NO Internet access unless Permissions or Restrictions have been specified.

bt-WebFilter Management Console 4-32: Individual Access Policy Type Properties

The ‘Advanced Redirect Page Options’ allows you to define how to handle blocked websites and for how long access should be provided if the user is allowed to continue.



Advanced Redirect Page Options

Specify time frame value for keeping Web site opened when using 'Proceed to the blocked Web site' option

Proceed To The Blocked Web Site Timeout:

● Default (1 hour(s))

○ Custom: 1 hour(s)

○ Unlimited

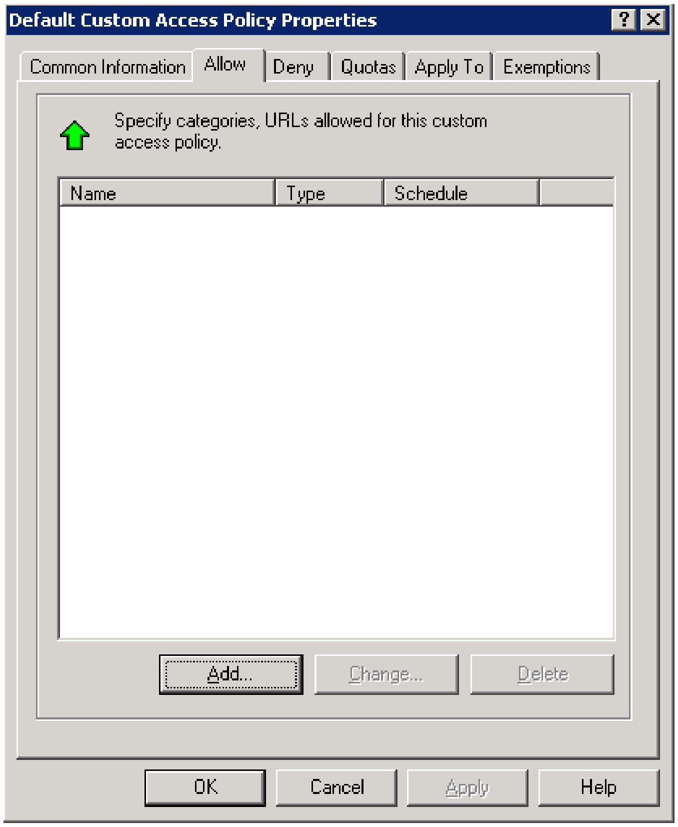
bt-WebFilter Management Console 4-33: Advanced Redirect Page Options

Allow and Deny Tab

If you are using a ‘Permission Policy Type’, the ‘Allow’ tab is where you can add the URL’s and/or categories that you want to provide access to. Click the ‘Add’ button to bring up the ‘Access Object Properties’ page.

If you are using a ‘Restriction Policy Type’, the ‘Deny’ tab is where you can add the URL’s and/or Categories that you want to restrict access to. Click the ‘Add’ button to bring up the ‘Access Object Properties’ page.

Regardless of the Policy Type chosen, the individual tabs used to configure them will function the same.



Specify categories, URLs allowed for this custom access policy.

bt-WebFilter Management Console 4-34: Access Policy Properties - Allow Tab

Allow and Deny Tab – Access Object Properties

Common Information (Figure 4-35)

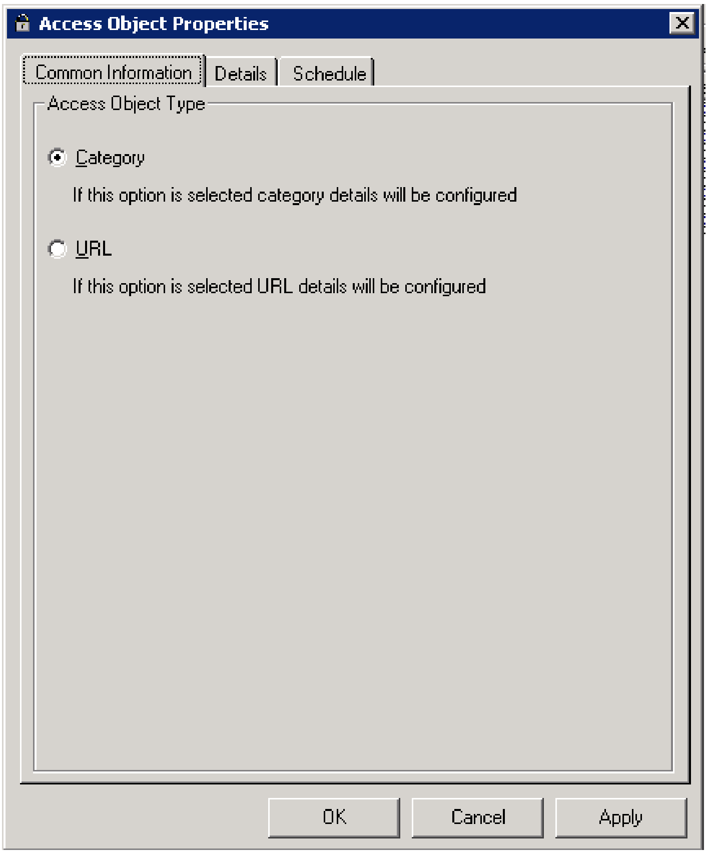
- Category – use this option to set Categories on the 'Details' tab
- URL – use this option to set URL(s) on the 'Details' tab

Details

Depending on the option selected on the 'Common Information' tab the 'Details' a window will display different selection options.

If the 'Category' option is selected, you will be presented with a list of Categories configured within WebFilter. These include both the default Categories as well as any custom Categories that you have created.

If the 'URL' option is selected, you will be presented with a URL box to enter your information. You can enter a full URL or a URL mask. To separate multiple URL's and/or Masks, use a ';' between entries.)



Access Object Properties

Access Object Type

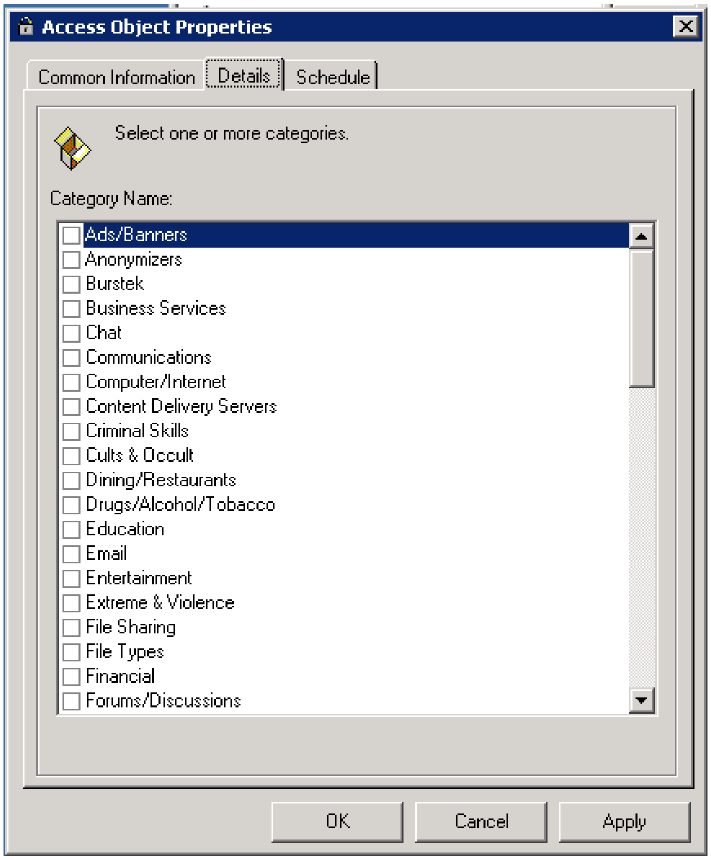
● Category

If this option is selected category details will be configured

○ URL

If this option is selected URL details will be configured

bt-WebFilter Management Console 4-35: Access Object Properties - Common Information

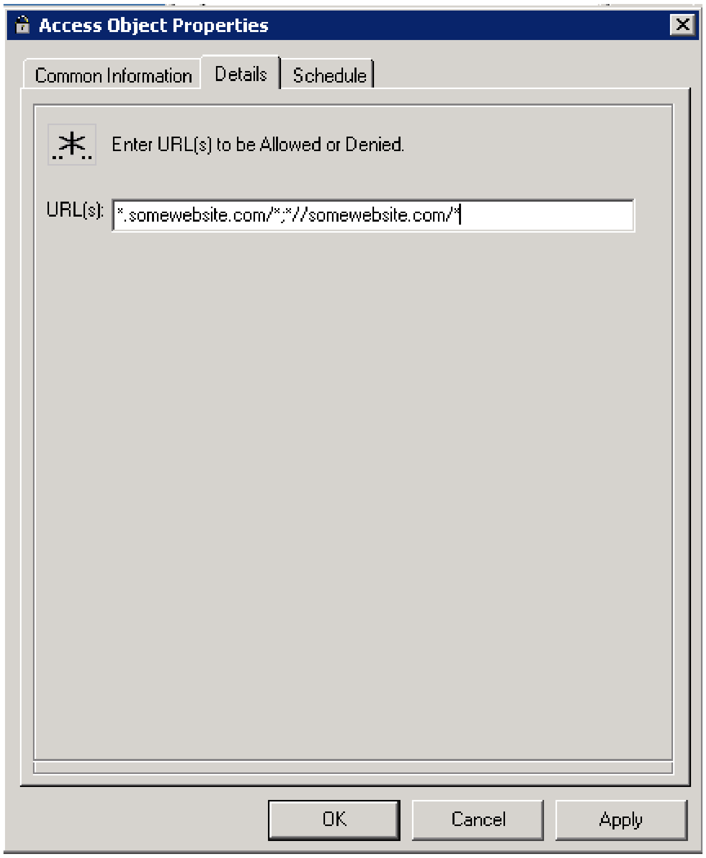


Select one or more categories.

Category Name:

- □ Ads/Banners
- □ Anonymizers
- □ Burstek
- □ Business Services
- □ Chat
- □ Communications
- □ Computer/Internet
- □ Content Delivery Servers
- □ Criminal Skills
- □ Cults & Occult
- □ Dining/Restaurants
- □ Drugs/Alcohol/Tobacco
- □ Education
- □ Email
- □ Entertainment
- □ Extreme & Violence
- □ File Sharing
- □ File Types
- □ Financial
- □ Forums/Discussions

bt-WebFilter Management Console 4-36: Access Object Properties - Details Category Selection



Enter URL(s) to be Allowed or Denied.

URL(s): *.somewebsite.com/*;*//somewebsite.com/*

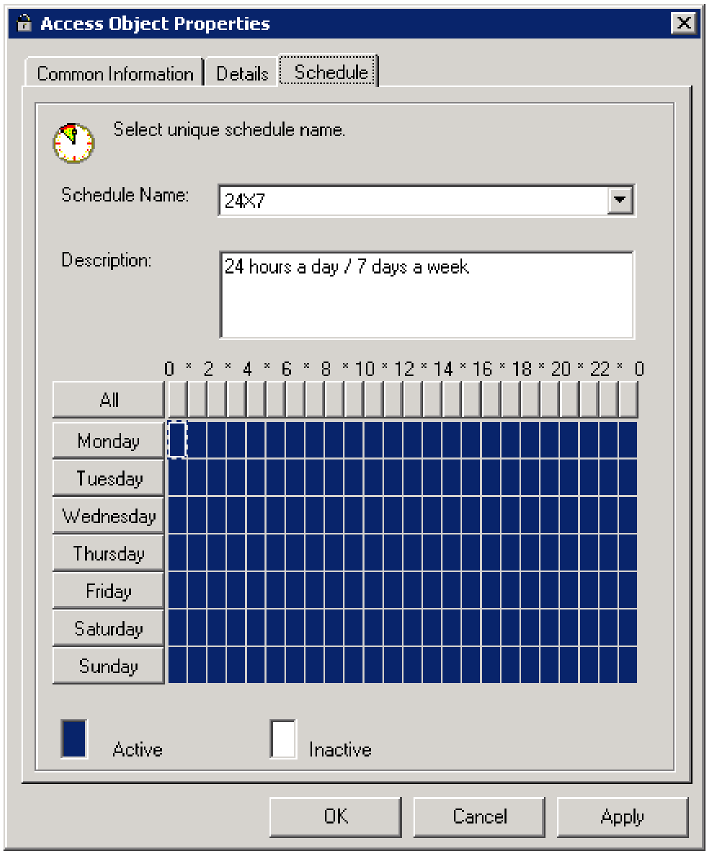
bt-WebFilter Management Console 4-37: Access Object Properties - Details URL Selection

Schedule Tab

Here is where you will set any schedule that you have previously defined. The Schedule entered here will effect only those URL(s) or Categories that you have listed on the 'Details' tab.

Once you select your schedule, you will see the description (if entered) as well as the Active/Inactive times for the schedule. (See Figure 53)

> **NOTE:**
> You are unable to modify Schedules directly at this location. If you wish to change the properties of a Schedule, you must do so on the Schedule itself in the 'Schedules' container.



Schedule Name: 24X7

Description: 24 hours a day / 7 days a week

bt-WebFilter Management Console 4-38: Access Object Properties - Schedule Selection

Quotas

This tab allows you to assign quotas to the Individual Access Policy. When you click ‘Add’ an ‘Access Object Properties’ page will appear similar to the one for the ‘Allow’ and ‘Deny’ tabs except there will also be a ‘Quota’ tab. All other tabs work the same way as previously described; however, you can now specify a Quota to be assigned to your selections.

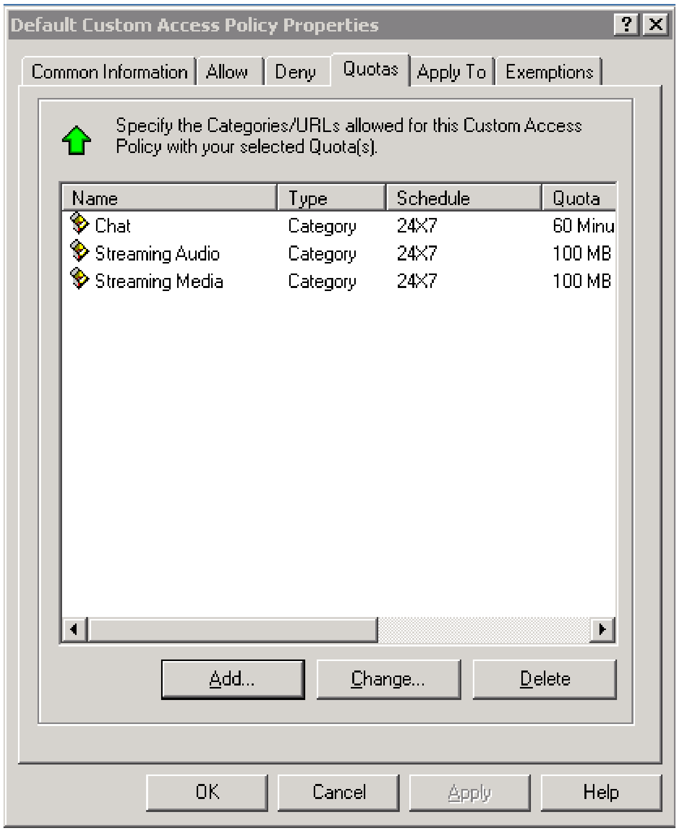
As with the ‘Schedule’ tab, once you select a quota most of the information will be unavailable for modification. If you need to change the Quota you will need to return to the ’Quotas’ container and make the appropriate object changes.

WARNING:

Modifying a Quota that is part of several Individual Access Policies may result in unexpected results since the change would apply to all of the configured policies. It may be easier to create quotas based on the actual Individual Access Policy to which they are applied.

Quota Applying Method

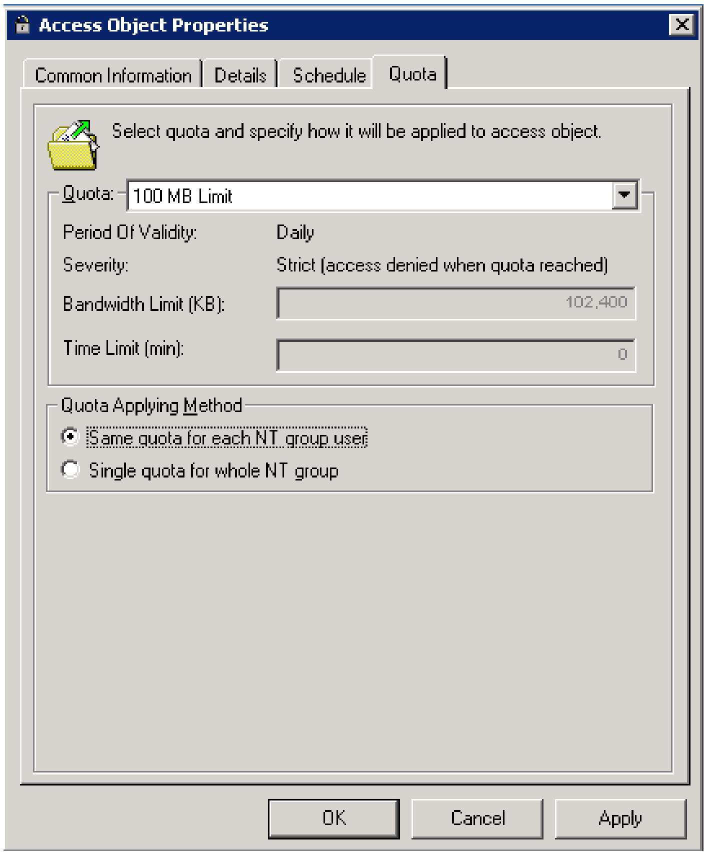
- Same quota for each NT group user – Each user will have their own quota limits.
- Single quota for whole NT group – Each user will share quota limits.



Specify the Categories/URLs allowed for this Custom Access Policy with your selected Quota(s).

Name	Type	Schedule	Quota
Chat	Category	24X7	60 Minu
Streaming Audio	Category	24X7	100 MB
Streaming Media	Category	24X7	100 MB

bt-WebFilter Management Console 4-39: Access Policy Quota Tab



Select quota and specify how it will be applied to access object.

Quota: 100 MB Limit

Period Of Validity: Daily

Severity: Strict (access denied when quota reached)

Bandwidth Limit (KB): 102,400

Time Limit (min): 0

Quota Applying Method

● Same quota for each NT group user

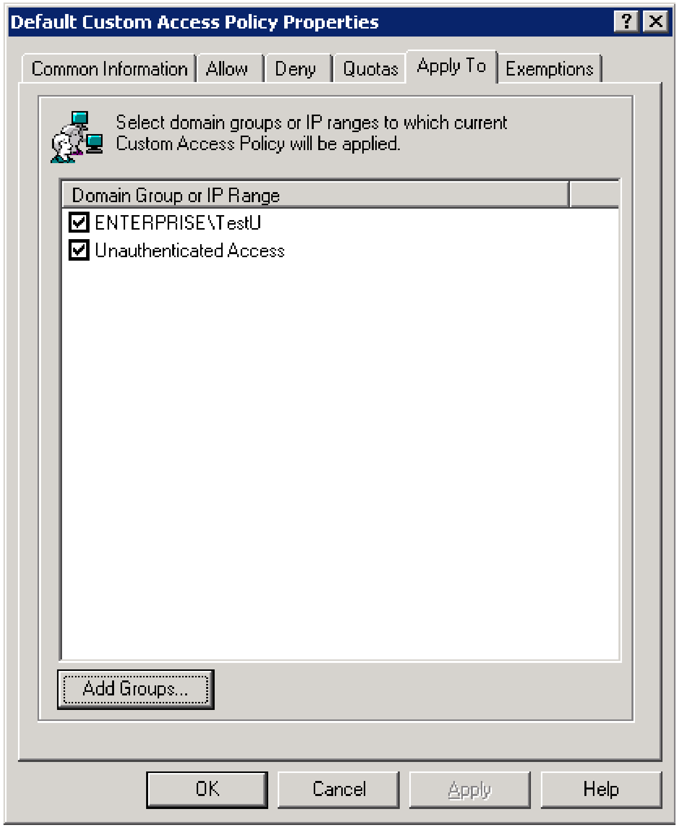
○ Single quota for whole NT group

bt-WebFilter Management Console 4-40: Access Object Properties - Quota's Tab

Apply To and Exemptions Tabs

The 'Apply To' and 'Exemptions' tabs are where the groups and users are set that will be affected by the Individual Access Policy. Clicking on the 'Add Groups' option will bring up the 'Select Groups' window allowing you to enter group names.

> **NOTE:**
> To be able to add an individual user name to the 'Apply To' or 'Exemptions' tab, you must first add the user under the 'Access Rule' for the domain. (See 'Access Rules' for more information regarding this.

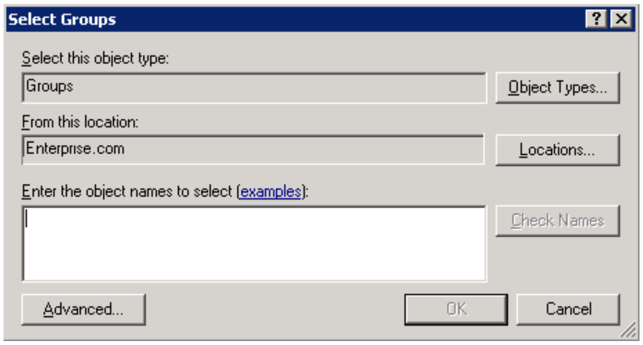


Select domain groups or IP ranges to which current Custom Access Policy will be applied.

☑ ENTERPRISE\TestU

☑ Unauthenticated Access

bt-WebFilter Management Console 4-41: Custom Access Policy - Apply To Tab



Select this object type: Groups

From this location: Enterprise.com

Enter the object names to select (examples):

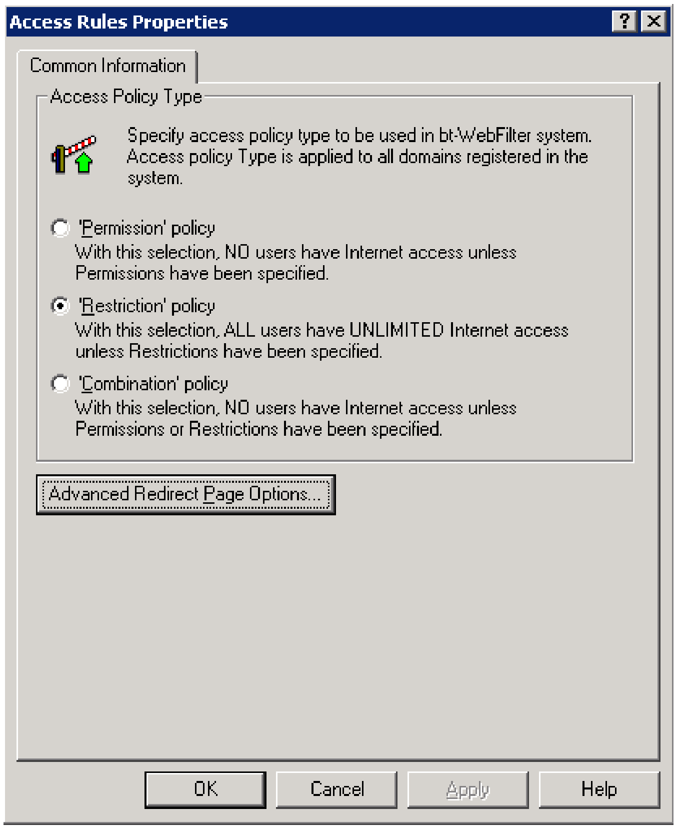
bt-WebFilter Management Console 4-42: Custom Access Policy - Select Groups

Access Rules

The ‘Access Rules’ container is where the administrator can add domains, IP address, set the Global Access Policy, and allow you set the default ‘Advanced Redirect Page Options.’

The ‘Global Access Policy Type’ is the same as the ‘Individual Access Policy Types’ except that it applies to all objects that are set to ‘Default Policy.’ If you have an ‘Individual Access Policy’ that has the ‘Default’ policy type selected, this setting determines how the policy will react.

- Default Policy – As the name suggests, this is the default configuration for the Individual Policy and it takes on whatever policy type you have set in the ‘Global Access Policy’ (See ‘Access Rules’).
- Permission Policy – This policy is similar to an implied DENY. It will deny all URL access unless specifically allowed. Only the ‘Allow’ tab is used with the policy type.
- Restriction Policy – This policy type is similar to an Explicit deny. It will ALLOW all URL access unless specifically denied. Only the ‘Deny’ tab is used with this policy type.
- Combination Policy – This policy type functions as a permission policy but uses both the ‘Deny’ and ‘Allow’ tabs. A policy of this type would be used to restrict users to a certain portion of a website. For example, the shipping department may need access only the section of a website concerned with shipping and receiving activities.



Specify access policy type to be used in bt-WebFilter system. Access policy Type is applied to all domains registered in the system.

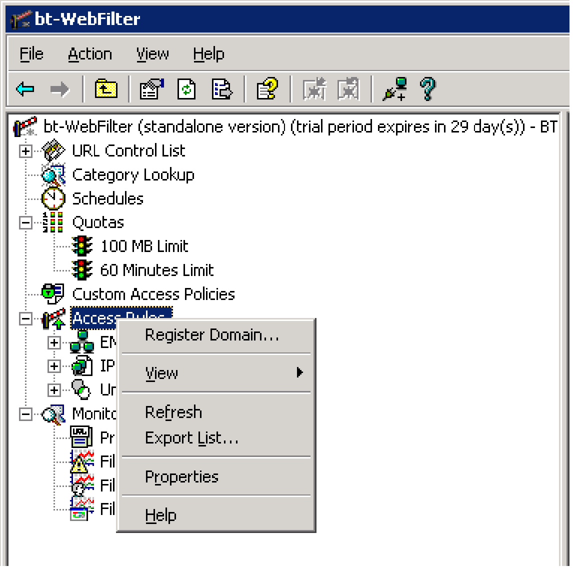
○ 'Permission' policy
With this selection, NO users have Internet access unless Permissions have been specified.

● 'Restriction' policy
With this selection, ALL users have UNLIMITED Internet access unless Restrictions have been specified.

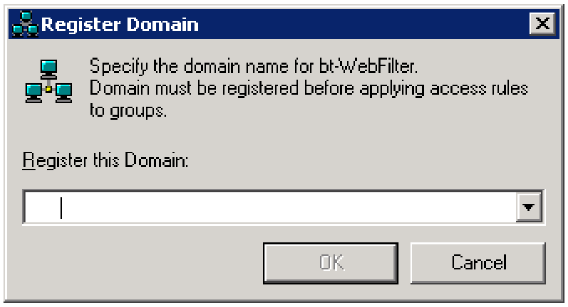
○ 'Combination' policy
With this selection, NO users have Internet access unless Permissions or Restrictions have been specified.

bt-WebFilter Management Console 4-43: Access Rule Properties

To access the 'Global Access Policy,' right click on the 'Access Rules' container and select 'Properties. From this context menu, you can also register your domain to allow bt-WebFilter to use Active Directory accounts in its policies.



bt-WebFilter Management Console 4-44: bt-WebFilter Access Rules Menu Options



Register Domain

Specify the domain name for bt-WebFilter.
Domain must be registered before applying access rules to groups.

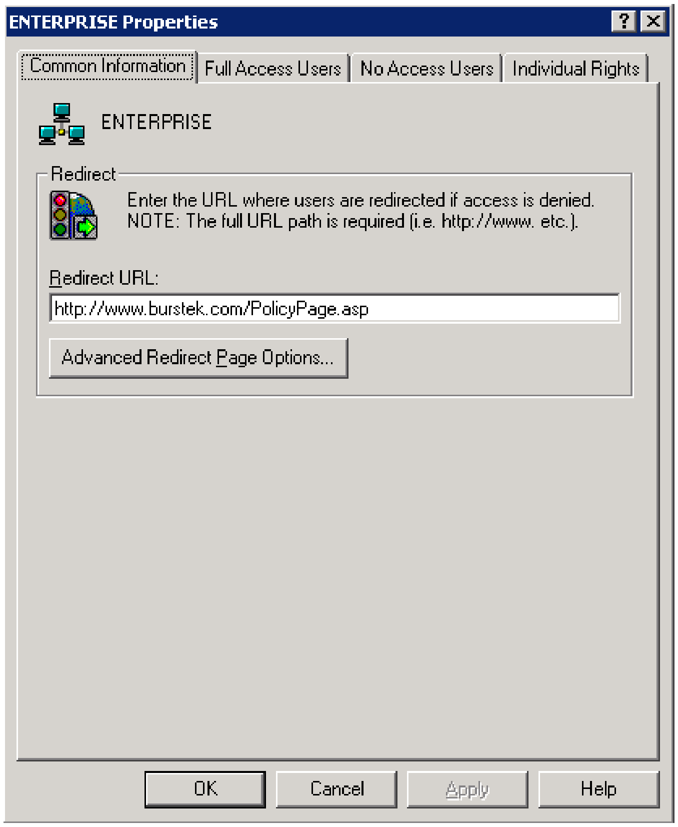
Register this Domain:

bt-WebFilter Management Console 4-45: Domain Registration

Domain Properties

The properties page for you domain has four tabs.

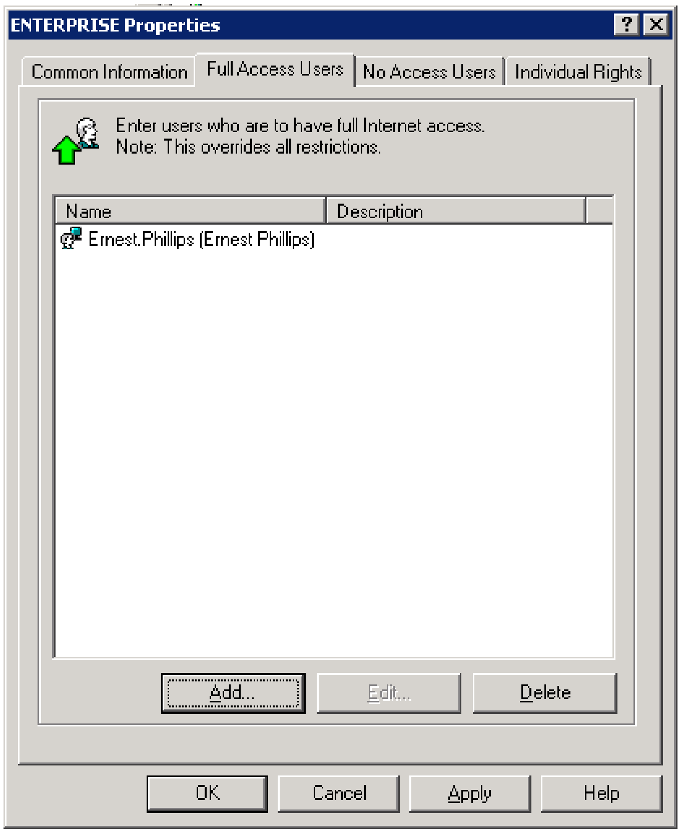
- Common Information – This tab allows you to specify a 'Redirect URL' for the entire domain. This would be the default redirect but you can override this on the Individual Access Policies.
- Full Access Users – This tab will allow you to specify users that will have full access to any website and/or category. Users on this tab will be exempt from all policies even if they are added on the 'Apply To' tabs for Individual Access Policies.
- No Access Users – This tab is will allow you to specify users that will have NO access to any website and/or category. Users on this tab will be exempt from all policies even if they are added on the 'Apply To' tabs for Individual Access Policies.
- Individual Rights – This tab will allow you to specify users that you would wish to add independently to an Individual Access Policy instead of via group membership. Users entered into this tab will be displayed on the 'Apply To' tab on each Individual Access Policy.



Enter the URL where users are redirected if access is denied. NOTE: The full URL path is required (i.e. http://www. etc.).

Redirect URL: http://www.burstek.com/PolicyPage.asp

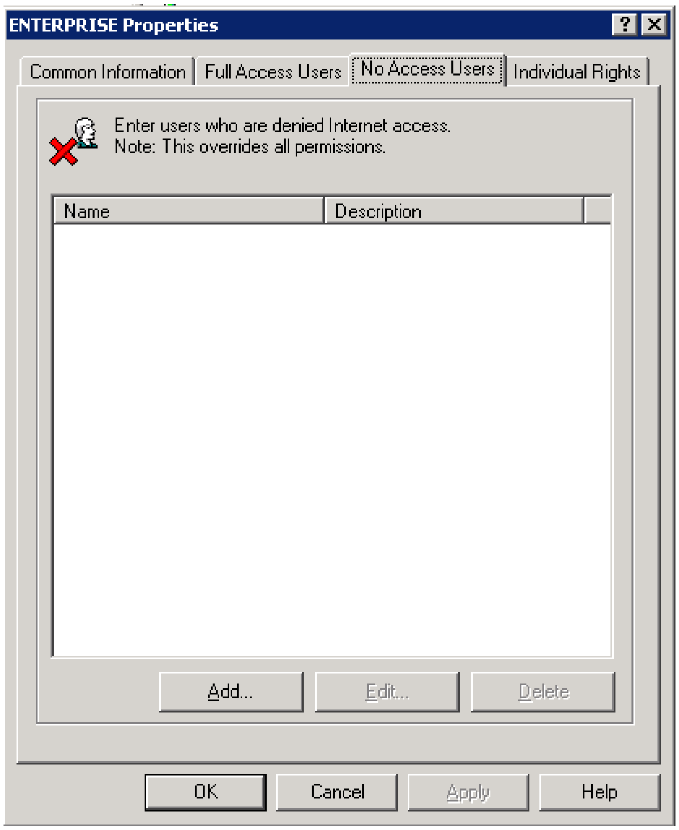
bt-WebFilter Management Console 4-46: Access Rule Domain Properties 'Common Information' Tab



Enter users who are to have full Internet access.
Note: This overrides all restrictions.

Name	Description
Ernest.Phillips (Ernest Phillips)	

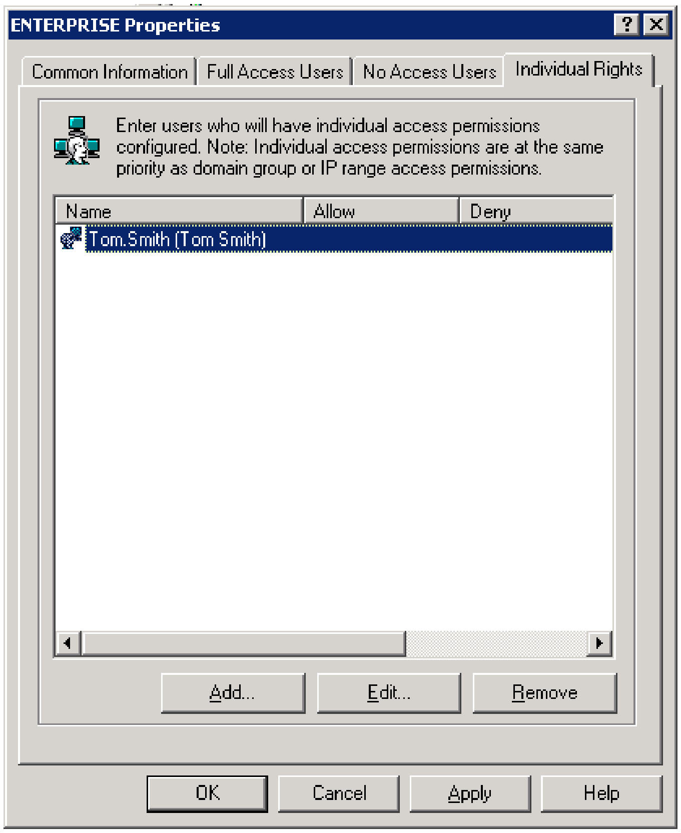
bt-WebFilter Management Console 4-47: Access Rule Domain Properties 'Full Access Users' Tab



Enter users who are denied Internet access.
Note: This overrides all permissions.

Name	Description

bt-WebFilter Management Console 4-48: Access Rule Domain Properties 'No Access Users' Tab



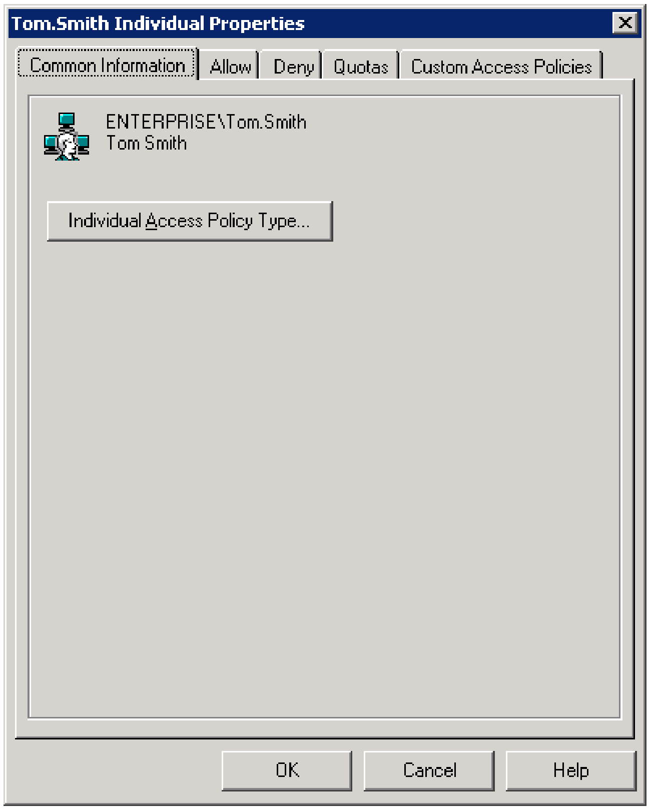
Enter users who will have individual access permissions configured. Note: Individual access permissions are at the same priority as domain group or IP range access permissions.

Name	Allow	Deny
Tom.Smith (Tom Smith)		

bt-WebFilter Management Console 4-49: Access Rule Domain Properties 'Individual Rights' Tab

The ‘Individual Rights’ tab provides you with additional information regarding the user. This will allow for more granular control of users and allows you to set Custom Access Policy type settings on a per user basis. All of the options that effect ‘Individual Access Policies’ can be applied here.

- Common Information
- Allow Tab
- Deny Tab
- Quotas
- Custom Access Policies

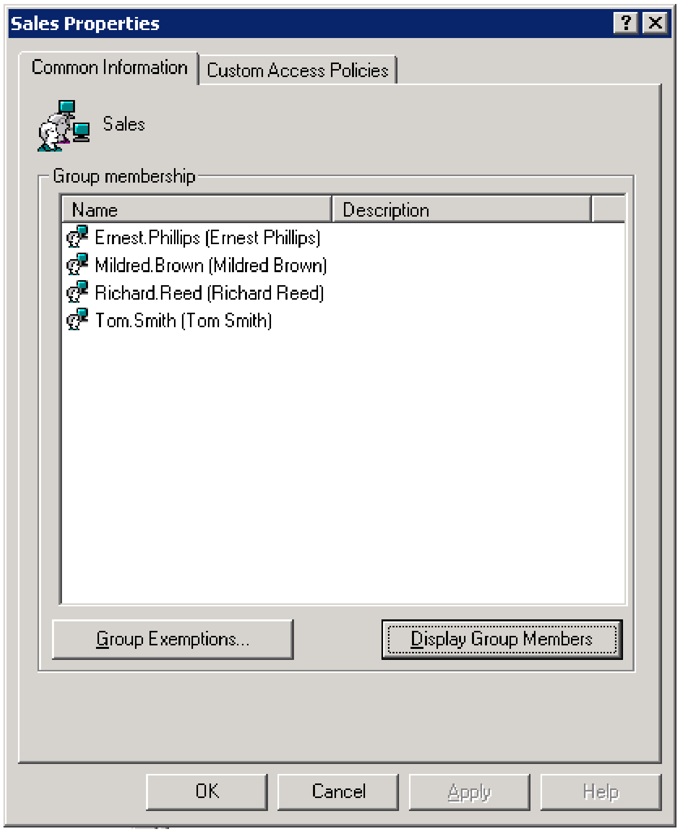


ENTERPRISE\Tom.Smith
Tom Smith

bt-WebFilter Management Console 4-50: Access Rule Individual User Rights Properties

Once you register your domain, you will be able to view the list of Active Directory groups in your organization by expanding the domain container. You can then select the group properties and modify it directly to exempt users from any bt-WebFilter policies already applied to it.

- Common Information – On this tab you can set the exemptions for any of the group's users. Exempting a user from the group will prevent any policies that the group is a member of from being applied. You can view all the members of the group by simply clicking on the 'Display Group Members' button.
- Custom Access Policies – On this tab you can view all of the Individual Access Policies that the group is a member of.

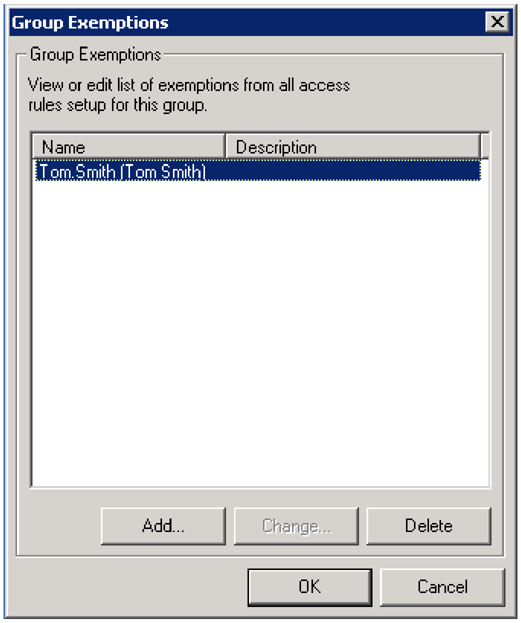


Sales

Group membership

Name	Description
Ernest.Phillips (Ernest Phillips)	
Mildred.Brown (Mildred Brown)	
Richard.Reed (Richard Reed)	
Tom.Smith (Tom Smith)	

bt-WebFilter Management Console 4-51: Access Rule Domain Group Properties 'Common Information' Tab

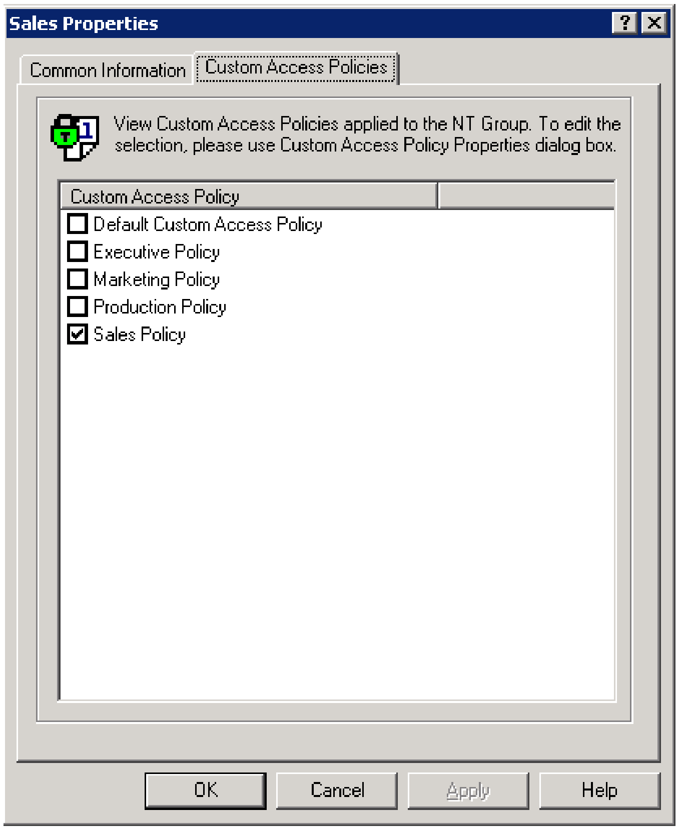


Group Exemptions

View or edit list of exemptions from all access rules setup for this group.

Name	Description
Tom.Smith (Tom Smith)	

bt-WebFilter Management Console 4-52: Access Rule Domain Group Properties 'Group Exemptions'



View Custom Access Policies applied to the NT Group. To edit the selection, please use Custom Access Policy Properties dialog box.

Custom Access Policy

- ☐ Default Custom Access Policy
- ☐ Executive Policy
- ☐ Marketing Policy
- ☐ Production Policy
- ☑ Sales Policy

bt-WebFilter Management Console 4-53: Access Rule Domain Group Properties 'Custom Access Policies'

IP Ranges

‘IP Range Access Rules’ work very similar to ‘Domain Access Rules’ and have many of the same configuration tabs.

Selecting the properties of the ‘IP Ranges’ Access Rules container will display a window like figure 4-54. Here you can set the same information that you would under the ‘Domain Access Rule’. Instead of an ‘Individual User Rights’ tab, there is a ‘Personal Quotas’ tab.

Personal Quotas – This tab allows you select a Quota for each IP address that you add to the ‘IP Address’ list. You can also add multiple Quotas for the same IP address.

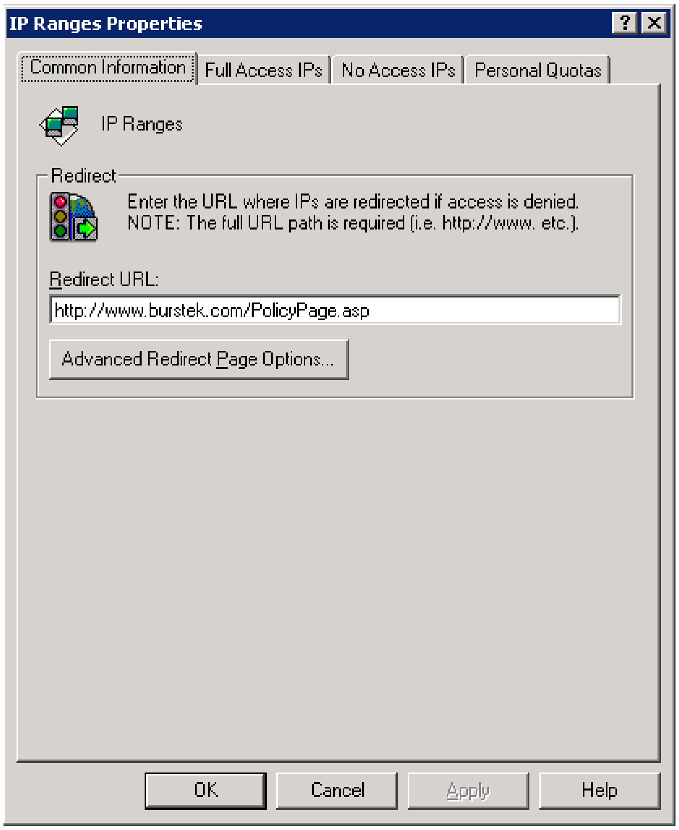
When you register an IP Range, you modify the properties of the range the same as you would the ‘Domain Properties.’ You can register a single IP or multiple IP’s depending on the requirements of your environment. Just like with a DHCP scope, you can add the entire range that you want to work with, then use the ‘IP Range Exemptions’ button to exclude addresses that should not be included.

Unauthenticated Access

This 'Access Rule' is used to control how users that do not authenticate to bt-WebFilter (or ISA) should be handled. The 'Unauthenticated Access' rule has the same configuration options as the previously mentioned Access Rules.

NOTE:

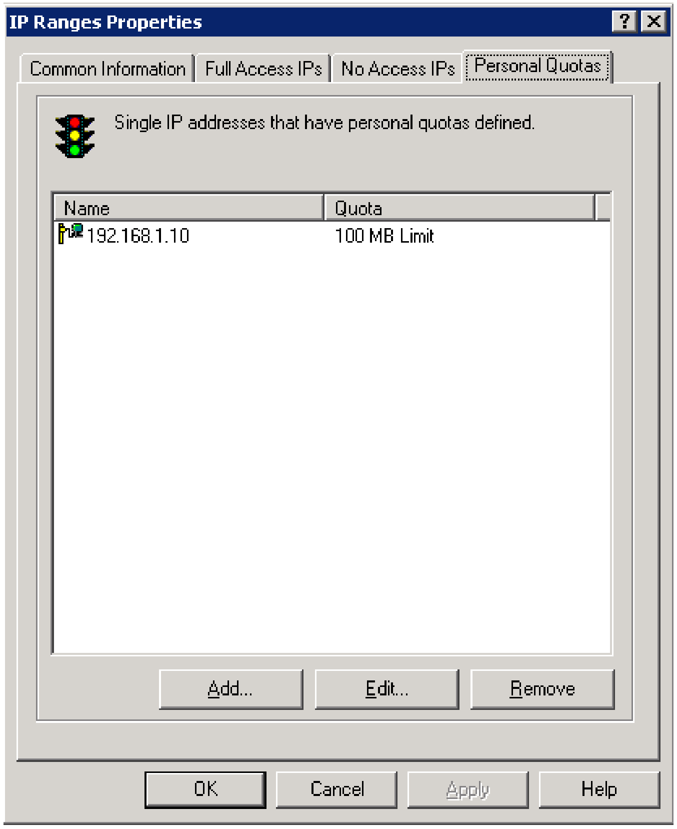
When using bt-WebFilter Plug-in, ISA will handle the authentication of users. bt-WebFilter only uses the Domain User name or IP to determine what access the user should then have.



Enter the URL where IPs are redirected if access is denied.
NOTE: The full URL path is required (i.e. http://www. etc.).

Redirect URL: http://www.burstek.com/PolicyPage.asp

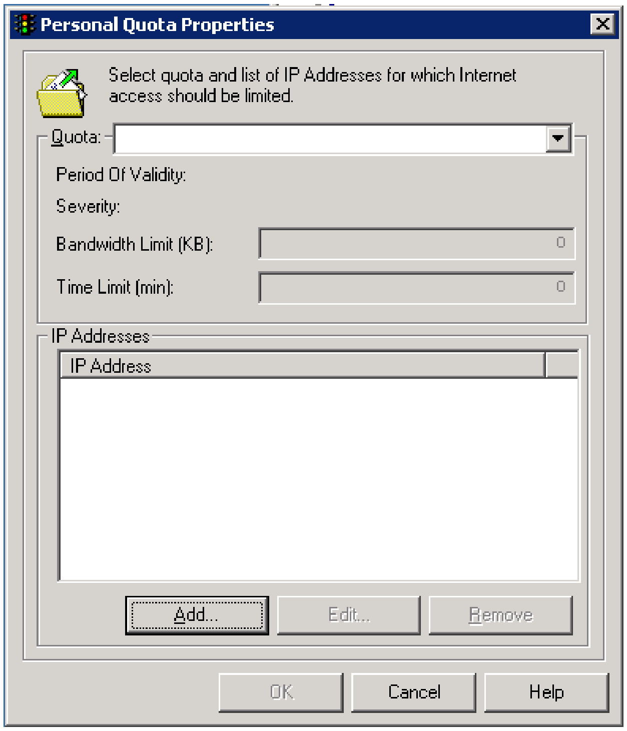
bt-WebFilter Management Console 4-54: IP Range Properties Page



Single IP addresses that have personal quotas defined.

Name	Quota
192.168.1.10	100 MB Limit

bt-WebFilter Management Console 4-55: IP Range Properties Page 'Personal Quotas' Tab



Select quota and list of IP Addresses for which Internet access should be limited.

Quota:

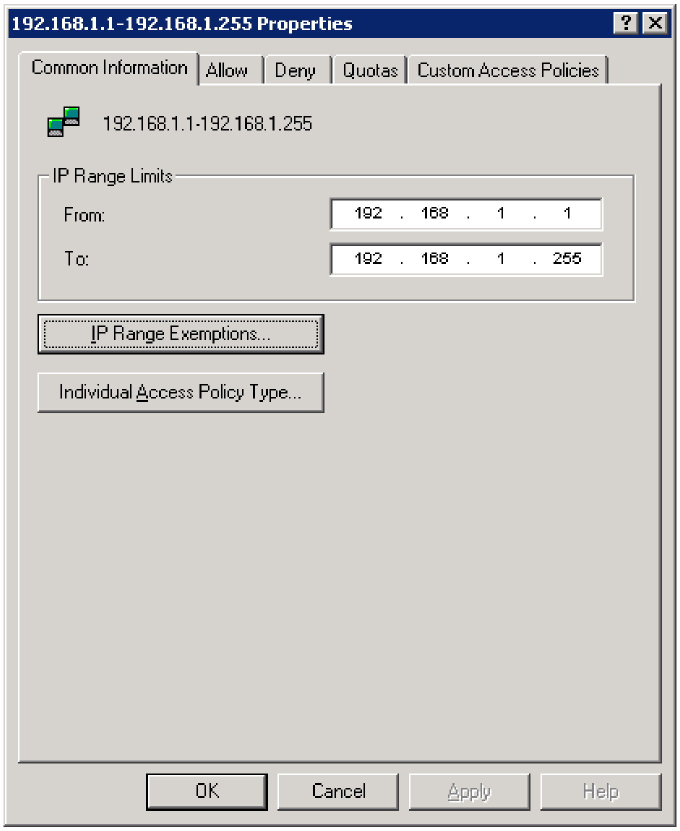
Period Of Validity:

Severity:

Bandwidth Limit (KB): 0

Time Limit (min): 0

bt-WebFilter Management Console 4-56: IP Range 'Person Quota Properties' Page



192.168.1.1-192.168.1.255 Properties

192.168.1.1-192.168.1.255

IP Range Limits

From: 192 . 168 . 1 . 1

To: 192 . 168 . 1 . 255

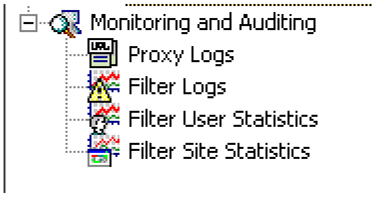
bt-WebFilter Management Console 4-57: IP Range Scope Propeties Page

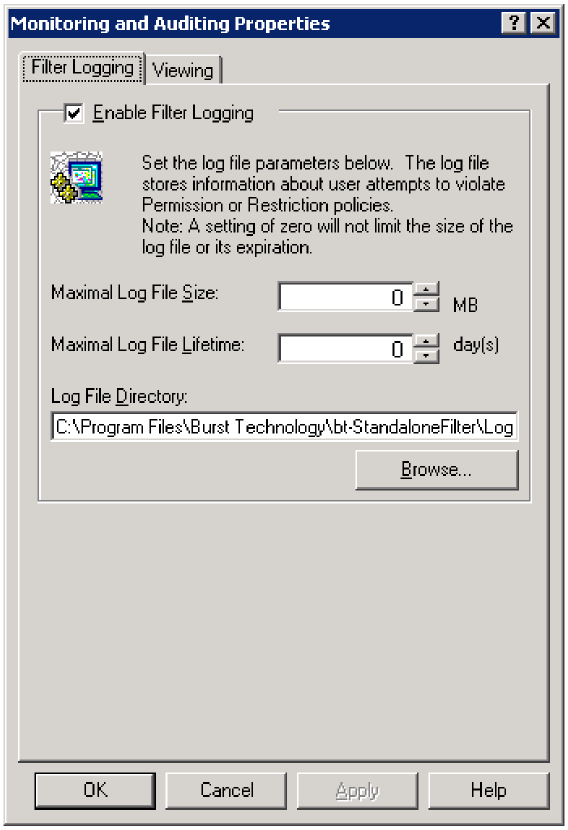
Monitoring and Auditing

bt-WebFilter has a built in monitoring and auditing feature with of the following sections:

- Proxy Logs (bt-WebFilter Standalone only)
- Filter Logs
- Filter User Statistics
- Filter Site Statistics

The properties of the 'Monitoring and Auditing' container provides you the option of enabling logging, setting log file size and retention, and setting the Log File Directory. You can also filter the events that you see by date, category, and/or user.





Monitoring and Auditing Properties

☑ Enable Filter Logging

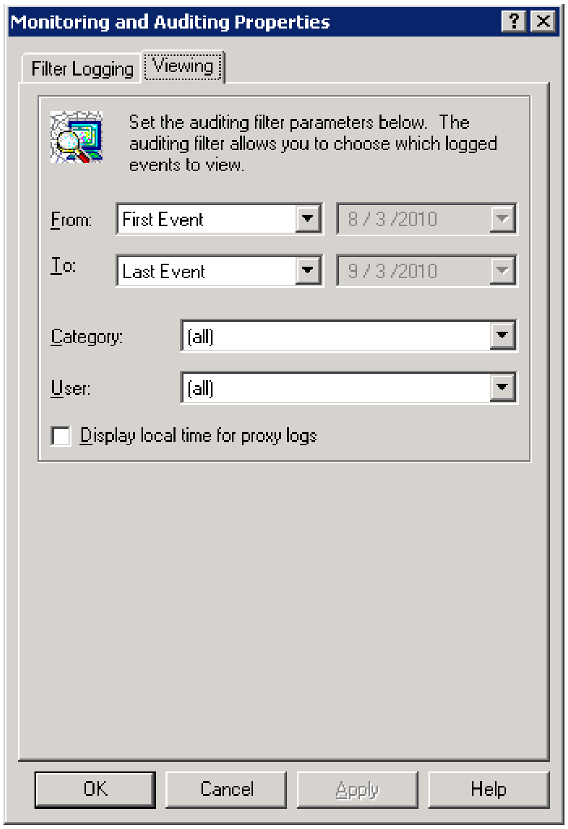
Set the log file parameters below. The log file stores information about user attempts to violate Permission or Restriction policies.
Note: A setting of zero will not limit the size of the log file or its expiration.

Maximal Log File Size: 0 MB

Maximal Log File Lifetime: 0 day(s)

Log File Directory:
C:\Program Files\Burst Technology\bt-StandaloneFilter\Log

bt-WebFilter Management Console 4-58: Monitoring and Auditing Properties 'Filter Logging' Tab



Monitoring and Auditing Properties

Set the auditing filter parameters below. The auditing filter allows you to choose which logged events to view.

From: First Event 8 / 3 /2010

To: Last Event 9 / 3 /2010

Category: (all)

User: (all)

□ Display local time for proxy logs

bt-WebFilter Management Console 4-59: Monitoring and Auditing Properties 'Viewing' Tab