BURSTEK™

Serious Internet Security™

bt-WebFilter Administrator’s Guide:

Access Rules

&

Custom Access Policies

Contents

Table of Figures

Administrator's Guide

Custom Access Policies and Access Rules

Introduction

The Custom Access Policies (CAPs) in bt-WebFilter provide the administrator with the ability to control browsing in a number of different ways. The administrator can choose to deny all access except an approved list of URLs and/or Categories, or allow general web access but deny destinations deemed unsuitable for the workplace. Restrictions and Permissions can also be enforced or relaxed based on bandwidth usage, time allotment, time of day, IP Address, username, Active Directory Group, or any combination that is needed.

With so many options you may be wondering where or even how to start. In an effort to help you with those questions, we have published this document. Instead of simply listing the sections and configuration options, this guide will also provide specific examples of how to accomplish certain tasks and then provide real scenarios of how they can work together. It is our sincere hope that after reading this paper, you will gain a better understanding of how Burstek's WebFilter can help you in managing the Web Browsing habits in your environment.

Custom Access Polices vs. Access Rules

Custom Access Policies and Access Rules function together but are two separate items. Access Rules are one level above CAPs. The primary function of the Access Rule is to determine how the user or machine will be identified and the function of the CAP is what level of access the user or machine will have.

To visualize this, it's similar to going to a movie theater to watch a horror movie. Before you are allowed to purchase a ticket, you may have to prove that you are of the correct age. The movie theaters policy is to verify this by ID. If you are old enough, you are sold the ticket and you can now enter the Movie complex.

Congratulations, you have just passed through the 'Access Rules' section. However in order to see the movie you still have to pass by the Ushers who check your ticket and directs you to the proper theater. You are not 'Allowed' to go into another movie if you have not been authorized.

It is the role of the User that is performed by the CAP. Based on the 'ID' that you supply to the 'Access Rule', the CAPs then determine what is and what's not available to you based on that ID.

We will get into this in more detail later in this guide but for now, it is good enough to just know that Access Rules identify the user, while Custom Access Polices determine the type of access for the user.

Well, almost always....

When an Access Rule behaves the same as a Custom Access Policy

Access Rules typically are used to identify a user, however sometimes you may want to have specific configurations for a single user or a small group of users or IP Addresses. Access Rules allow you to do this without creating a completely new Custom Access Policies and can even provide more granular control than a CAP can by itself.

Getting Started

First things first. If you haven't already, you can download a free 30 day fully functional trial of our bt-WebFilter product from our website at http://www.burstek.com. Simply fill out the 'Evaluate' form and you will be sent the account credentials and instructions on where to download the product and install it. You can also find installation videos and more on our support page at http://www.burstek.com/support

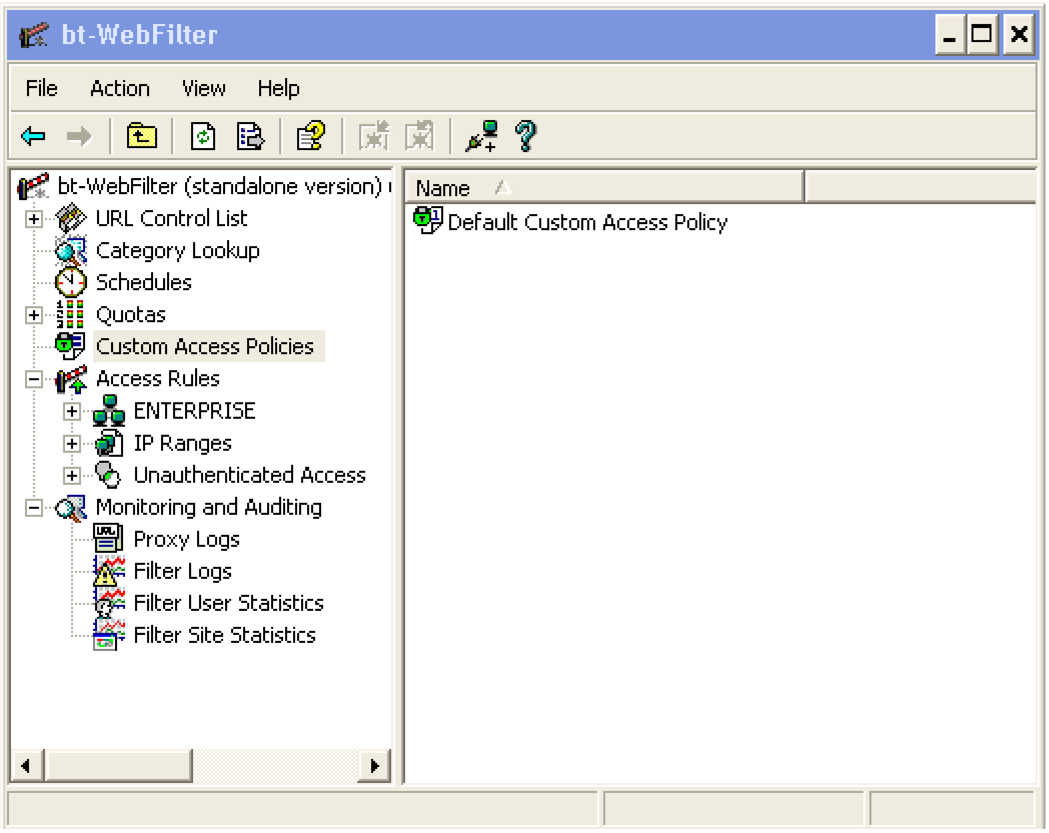


Figure 1 - The bt-WebFilter Interface

After installing the software, the next task is to decide how you want to filter your users. Possible formats are:

- By Active Directory user name or groups
- By and IP or IP Range
- Anonymous users

The Access Rules

There are 3 types of Access Rules (See Figure 2)

Domain Based - Uses Active Directory to identify users. Utilizing the 'Domain Access Rule', you can use domain user names and groups in your Custom Access Policies. You can also combine this with IP Access Rules to customize your environment even further. For example, you may want to allow users to access Social Networking sites from a break room PC but not from the workstations at their desk. Simply add the IP addresses for the workstation PCs to the Custom Access Policy that denies the ‘Social Networking’ Category.

One additional point to make is when using bt-WebFilter Standalone. Since this product contains its own built in Proxy, in order to authenticate Domain Users to access the Proxy, you must configure the Domain Access Rule.

IP Ranges - Performs filtering based on the IP address of the device accessing the system. You can combine IP Address filtering with either Domain Based identification or use it with unauthenticated access.

Unauthenticated Access – If WebFilter is not configured to require Authentication, or in the case of ISA/TMG installations the ‘Authenticated Users’ group is not the only user set configured in the HTTP/HTTPS access rule, all browser traffic will appear to come from ‘Anonymous’. If you are not forcing authentication, then you would use this Access Rule entry to filter. As an example of where this would be deployed, consider a ‘Guest’ Wireless network. You may not require the users to login to your Active Directory, but you still don’t want them to be able to browse to sites that you would normally restrict. In this case you would simply assign a Custom Access Policy to this Access Rule.

NOTE: Registering a Domain Access Rule only does not require users to supply credentials to the proxy server unless the ‘Ask unauthenticated users for identification’ and the ‘Basic with this domain’ options are completed under the ‘Proxy Options’ tab in bt-WebFilter Standalone. In bt-WebFilter for ISA, the ISA/TMG server is the proxy and the Proxy Authentication option is not available. Instead, you must use ISA/TMG Access Rules to force the ISA/TMG Proxy to identify the user.

NOTE: Requiring Authentication via WebFilter Standalone essentially removes the need or the ability to use the ‘Unauthenticated Access’ Access Rule since by requiring authentication before the proxy can be accessed, no user can be Anonymous.

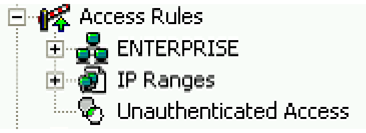
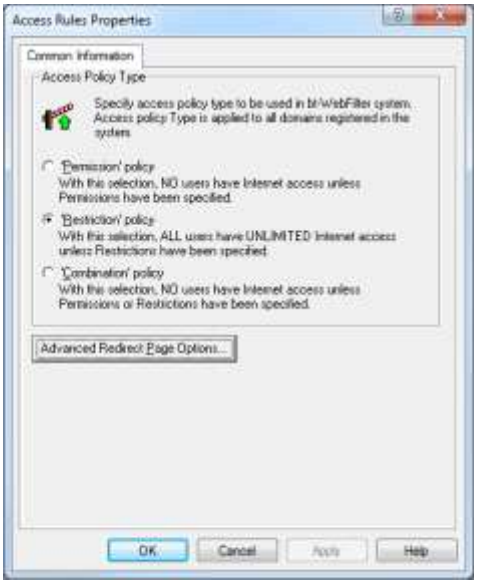


Figure 2 - Access Rules

The Access Rule Properties Window

The properties window for the ‘Access Rules’ container object (see figure 3) allows you to select the Access Policy type when using the ‘Default’ option at the Custom Access Policy level. It also provides the global configuration option for the ‘Advanced Redirect Page Options’ and provides you with the option to view any users who are currently allowed to access a page after using the ‘Proceed to blocked Web site’ option.

WARNING: Setting the ‘Access Rule’ Access Policy Type to ‘Permission’ will deny all web browsing for users (IP, Domain, Anonymous) unless a Custom Access Policy is assigned.



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.

Figure 3 - Access Rule Properties

Access Policy Types

There are three Access Policy Types available:

Permission – Denies all access to Web sites unless specifically allowed. When this option is chosen, any Custom Access Policies that are created and set to use the 'Default' option for the 'Individual Access Policy Type' will take on this behavior for whatever is listed on the 'Apply To' tab.

Restriction – Denies access only to Web sites or Categories that are specified on the Custom Access Policies 'Deny' tab when the CAP is using the 'Default' policy settings under its 'Individual Access Type Properties' page.

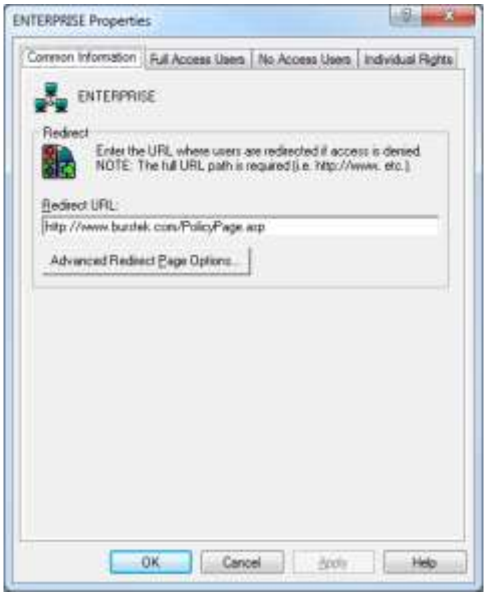
Combination – This is a specialized policy type as it has characteristics of both Restriction and Permission. The basic function of the policy is as Permission in that users are denied access unless specifically allowed. However it also has the ability to 'Deny' parts of Web sites or Categories that have been allowed. This allows you to have more control over Control List Categories at a policy level instead of modifying the contents of the Category itself.

Advanced Redirect Page Options

Burstek supplies several redirect page samples that you may use to customize what users see and how they proceed when they experience a blocked site or Category. Some of these options allow the user to continue on to the restricted Web site (if allowed by the administrator) for a certain amount of time. The Advanced Redirect Page Options is where you can configure the amount of time the users can have access for as well as see who currently is allowed access to specific Web sites.

The Domain Access Rule Properties Window

The Domain Access Rule Properties window (see figure 4) contains the options for configuring Full Access Users, No Access Users, and Individual Rights as well as the option for configuring the Redirect URL and advanced Redirect Page options to be used if not specified at the Custom Access Policy level.



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

Figure 4 – Domain Access Rule Properties

Common Information - Allows you to assign a Redirect page that would be used by users on the 'No Access Users' and 'Individual Rights' tabs. It also is the default used by a Custom Access Policy when no Redirect Page is assigned and restriction is based on Domain user name or group membership.

Full Access Users – Users and/or Groups added to this tab will not be bound by restrictions on any Custom Access Policy that utilizes members from the specified Domain Access Rule.

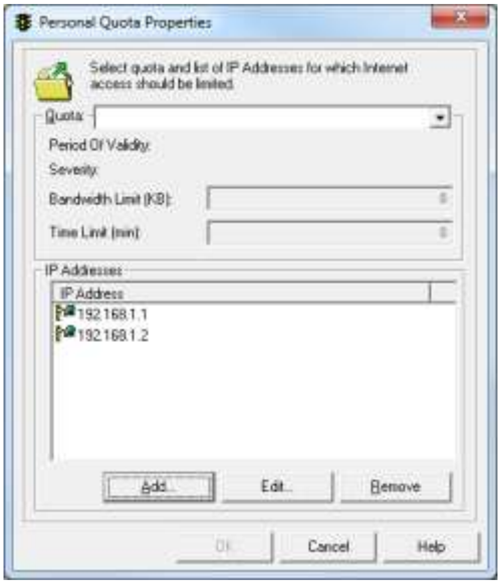
No Access Users - Users and or Groups appearing on this tab will have no access to Web sites and will not be affected by any allow additions on any Custom Access Policies that the user or group is a applied to.

Individual Rights – This tab allows you to configure a single user to be applied to an existing Custom Access Policy or to create a specific policy for the user. All options available to the Custom Access Policy are available to the Individual Access Policy except for Redirect Page options.

The IP Access Rule Properties Window

The IP Access Rule is very similar to the Domain Access Rule as far as the options available however it is used for IP Addresses instead of Domain Names. It also replaces the 'Individual Access Policy' with a 'Personal Quota' option. (see Figure 5). You can set any quota already configured to apply for a single IP or several IP addresses.

NOTE: Quota's set on this tab are not applied on a URL or Category basis and apply to all Web site traffic passing through WebFilter to and from the listed IPs.



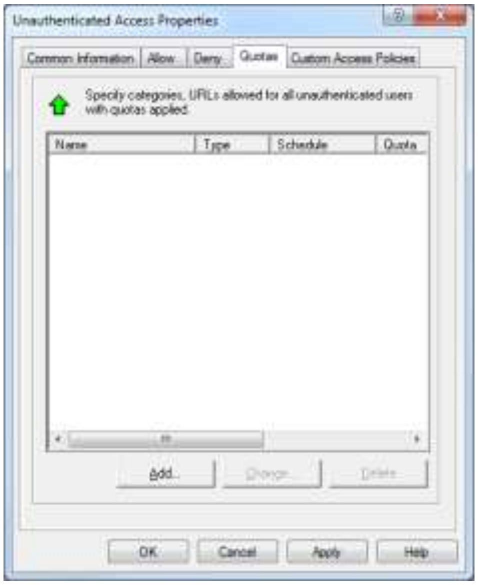
Select quota and list of IP Addresses for which Internet access should be limited.

192.168.1.1
192.168.1.2

Figure 5 - Personal Quota Properties

The Unauthenticated Access Rule Properties Window

This Access Rule contains its own ‘Allow’, ‘Deny’, ‘Quota’, and ‘Custom Access Policies’ tabs (see figure 6) that can be used to limit unauthenticated access. Any configurations entered on this page apply only to requests where the user name is ‘Anonymous’



Specify categories, URLs allowed for all unauthenticated users with quotas applied.

Figure 6 - Unauthenticated Access Rule Quota

Adding an Access Rule

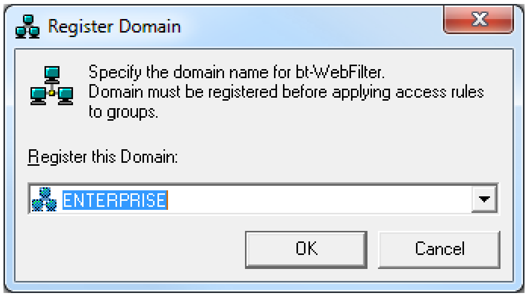
NOTE: The Unauthenticated Access Rule does not have to be ‘Added’ like the Domain and IP Addresses that are to be filtered. If you want to work with this Access Rule, skip directly to the ‘Configuring Access Rules’ section.

To add a Domain Access Rule:

1. In the bt-WebFilter Management Console, right click on the 'Access Rules' container object and select 'Register Domain' from the context menu.
    a. Alternatively you can left click the 'Access Rules' container object and select the 'Register Domain' option from the 'Action' menu item in the MMC toolbar.
2. In the 'Register Domain' window, use the drop down to select the domain you want to use (See figure 7)

NOTE: It is possible to register multiple Domains however the WebFilter server must be able to access these domains and query Directory Services for user and group information. Typically this is accomplished via a Trust to the Domain where bt-WebFilter is installed. For more information on Trusts, please contact Microsoft.

3. After clicking 'OK' you will be presented with the '<insert domain name> Properties' window. Click 'OK' to close this window. (Refer to figure 4).



Register Domain

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

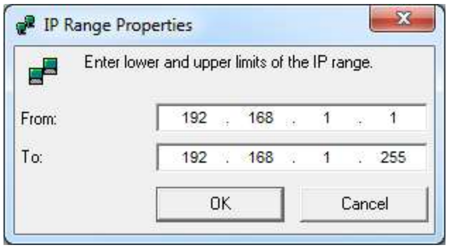
Register this Domain: ENTERPRISE

Figure 7 - Registering a Domain Access Rule

To add an IP Range Access Rule:

1. In the bt-WebFilter Management Console, expand the 'Access Rules' container object and select the IP Ranges object.
2. Right click on the IP Range object and select 'Register IP Range'. Alternatively you can left click the 'IP Ranges' object and select the 'Register IP Range' option from the 'Action' menu item in the MMC toolbar.
3. Enter the starting address in the 'From:' field
4. Enter the ending address in the 'To:' field

NOTE: To enter a single IP address, enter the same value in both the 'From' and 'To' fields.



IP Range Properties

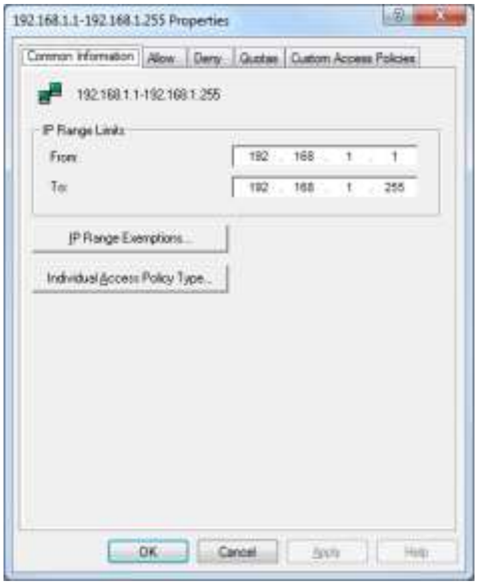
Enter lower and upper limits of the IP range.

From: 192 . 168 . 1 . 1

To: 192 . 168 . 1 . 255

Figure 8 - Adding an IP Range

5. You will then be presented with the ‘<IP Range> Properties’ window. Click ‘OK’ to close this window.



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

Figure 9 - IP Access Rule Properties

Configuring Access Rules

Configure a Domain Access Rule to allow Full Access to a Domain Group or Domain User:

1. Open the WebFilter console and expand the ‘Access Rules’ container
2. Right click on the Domain Access Rule in the list and click ‘Properties’
3. Select the ‘Full Access Users’ tab
4. Click the ‘Add’ button
5. In the ‘Select Users or Groups’ window, type the user name or the group name in the field and click ‘Check Names’. For more information click the ‘Examples’ link above the object names field.
6. Once the names have been validated (Underlined), click ‘OK’
7. Click ‘Apply’ then ‘OK’

Configure a Domain Access Rule for No Access to a Domain Group or Domain User:

1. Open the WebFilter console and expand the ‘Access Rules’ container
2. Right click on the Domain Access Rule in the list and click ‘Properties’
3. Select the ‘No Access Users’ tab
4. Click the ‘Add’ button
5. In the ‘Select Users or Groups’ window, type the user name or the group name in the field and click ‘Check Names’. For more information click the ‘Examples’ link above the object names field.
6. Once the names have been validated (Underlined), click ‘OK’
7. Click ‘Apply’ then ‘OK’

Configure a Domain Access Rule for Individual Rights

NOTE: By adding users to this tab, it allows you to assign individual users to Custom Access Policies or to configure a user to have their own access restrictions.

1. Open the WebFilter console and expand the 'Access Rules' container
2. Right click on the Domain Access Rule in the list and click 'Properties'
3. Select the 'Individual Rights' tab
4. Click the 'Add' button
5. In the 'Select Users' window, type the user name in the field and click 'Check Names'. For more information click the 'Examples' link above the object names field.
6. Once the names have been validated (Underlined), click 'OK'
7. Click 'Apply' then 'OK'

To configure an 'Individual Access Policy' for this user only proceed to next step.

1. On the 'Individual Rights' tab under the properties of the Domain Access Rule, select the user to modify and click 'Edit'.
2. Specify the 'Individual Access Policy Type' that should be applied
3. If using Permission or Combination Policy Types, proceed to step 4. If Using a 'Restriction' Policy type, proceed to step 11

Permission and Combination Individual Access Policies

4. Click the 'Allow' tab.
5. Click 'Add'
6. Select the type of Access Object to allow (URL or Category)
7. Click on the 'Details' tab
8. Depending on the selection in step 6, you will see a list of Categories allowing you to select the ones you wish to apply or a URL box. You can enter multiple URLs or masks by separating them with a ";".
9. Once you make your selections, click the 'Schedule' tab. If you have previously created schedules, this is where you can apply them.

NOTE: You cannot create schedules on this tab. For more information, see 'Schedules' in the user guide.

10. Click 'Apply' and 'OK' then proceed to step 14 below

Restriction Individual Access Policy

11. Click on the 'Deny' tab and click 'Add'
12. Select the type of Access Object to deny (URL or Category)
13. Follow steps 7 through 9 above. When all objects have been added, continue with next step
14. Click on the 'Quotas' tab to assign one or more Quotas to the Individual Access Policy.
15. Click 'Add' at the bottom of the 'Quota' tab.

NOTE: You must create the quotas under the Quota' object in the Management Window before being able to select them in the policy. For more information, see 'Quotas' in the user guide.

16. On the 'Common Information' tab, select the option for URL or Categories.
17. On the 'Details' tab, enter the URL(s) or Categories that will be affected by this Quota
18. On the 'Schedule' tab, select the Schedule that should be applied to this Quota.
19. Click on the 'Quota' tab and select the 'Quota' to be used.
20. Click 'Apply' then 'OK

To assign an individual user to a Custom Access Policy

1. Complete the steps in 'Configure a Domain Access Rule for Individual Rights' earlier in this document
2. On the 'Individual Rights' tab, select the user and click 'Edit'
3. Click the 'Custom Access Policies' tab.
4. Place a check mark in any policies that the user should be applied.

NOTE: If a user is currently explicitly exempted on the Custom Access Policies 'Exempt' tab by exclusion from an Active Directory group, the user will still be subject to the configuration of the Custom Access Policy when added via 'Individual Rights'

Configure an IP Access Rule to allow full Web access to a single IP address or a Range of IPs:

1. Open the WebFilter console and expand the 'Access Rules' container
2. Right click on the 'IP Ranges' Rule in the list and click 'Properties'
3. Select the 'Full Access IPs' tab
4. Click the 'Add' button
5. In the 'IP Range Properties' window, type the starting IP in the 'From' box and the ending IP in the 'To' box. To use a single IP address, enter the same number in both fields
6. Once the IPs have been entered, click 'OK'
7. Click 'Apply' then 'OK'

Configure an IP Access Rule to deny all web access to a single IP address or a range of IPs:

1. Open the WebFilter console and expand the 'Access Rules' container
2. Right click on the 'IP Ranges' Access Rule in the list and click 'Properties'
3. Select the 'No Access IPs' tab
4. Click the 'Add' button
5. In the 'IP Range Properties' window, type the starting IP in the 'From' box and the ending IP in the 'To' box. To use a single IP address, enter the same number in both fields
6. Once the IPs have been entered, click 'OK'
7. Click 'Apply' then 'OK'

Configure a Personal Quota for a single IP address

NOTE: Personal IP Quotas affect all browsing for the IP address. Adding a quota at this level will restrict all URL access to the limits specified in the quota.

NOTE: You must create the quotas under the 'Quotas' object in the Management Window before being able to select them in the policy. For more information, see 'Quotas' in the user guide.

1. Open the WebFilter console and expand the 'Access Rules' container
2. Right click on the 'IP Ranges' Rule in the list and click 'Properties'
3. Click on the 'Personal Quotas' tab
4. Click 'Add'
5. Select an existing quota from the drop down box
6. Click the 'Add' button in the 'IP Addresses' section
7. Enter the IP address that should be applied.

NOTE: Multiple IPs must be entered one at a time.

8. Once completed entering IP addresses, click the 'OK' button.
9. Click 'Apply' and 'OK' at the IP Range Properties window.

Configure an Access Policy for a Single IP or a range of addresses.

(To add an IP Range, see '*To add an IP Range Access Rule:'*)

1. Open the WebFilter console and expand the 'Access Rules' container
2. Expand the 'IP Ranges' object
3. Right click on the IP or range that you want the Access Policy to apply and select 'Properties'
4. Add any IPs that the policy should not be applied to by clicking on the 'IP Range Exemptions' button.
5. Define the 'Individual Access Policy' type for the policy. (See **Access Policy Types** for more information)

NOTE: If you select a 'Permission' or 'Combination' based policy, proceed with step 6. If you chose a 'Restriction' policy, continue with step 12

Permission or Combination based policy

6. Click the 'Allow' tab.
7. Click 'Add'
8. Select the type of Access Object to allow (URL or Category)
9. Click on the 'Details' tab
10. Depending on your selection, you will see a list of Categories allowing you select the ones you wish to apply or a URL box. You can enter multiple URLs and/or Masks by separating them with a ";".
11. Proceed to step 18 below

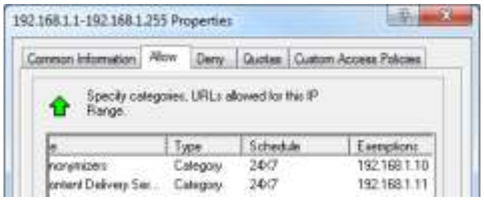
NOTE: If you are using a 'Combination' policy and you want to Deny certain sections of URLs or Categories that you have allowed above, proceed with step 12.

Restriction based policy

12. Click on the 'Deny' tab
13. Click 'Add'
14. Select the type of Access Object to deny (URL or Category)
15. Click on the 'Details' tab

16. Depending on your selection, you will see a list of Categories allowing you select the ones you wish to apply or a URL box. You can enter multiple URLs or Masks by separating them with a “;”.
17. Once you make your selections, click the ‘Schedule’ tab. If you have previously created schedules, this is where you can apply them.
18. On the ‘Exemption’ tab, enter any IP addresses that should be excluded from this specific policy configuration.
19. Click ‘Apply’ and ‘OK’

NOTE: You can have different levels of exemptions in the policy. You can have an IP exemption for the entire policy that you enter on the ‘Common Information’ tab or you can have exemptions for individual URLs or Categories. (See Figure 10)



192.168.1.1-192.168.1.255 Properties

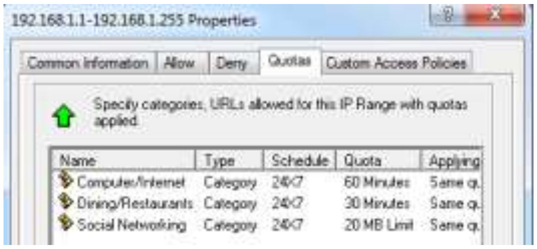
Specify categories, URLs allowed for this IP Range.

e	Type	Schedule	Exemptions
nonymizers	Category	24X7	192.168.1.10
ontent Delivery Ser...	Category	24X7	192.168.1.11

Figure 10 - Multiple IP Exemptions

20. Click on the ‘Quota’ tab and click ‘Add’
21. On the ‘Common Information’ tab, select the option for URL or Categories.
22. On the ‘Details’ tab, enter the URL(s) or Categories that will be affected by this Quota
23. On the ‘Schedule’ tab, select the Schedule that should be applied to this Quota.
24. Click on the ‘Quota’ tab and select the ‘Quota’ to be used.

NOTE: You can configure multiple Quotas in the same policy to allow you to ease restrictions for certain Categories or URLs but have tighter controls on others. (see Figure 11)



192.168.1.1-192.168.1.255 Properties

Specify categories, URLs allowed for this IP Range with quotas applied.

Name	Type	Schedule	Quota	Applying
Computer/Internet	Category	24X7	60 Minutes	Same q.
Dining/Restaurants	Category	24X7	30 Minutes	Same q.
Social Networking	Category	24X7	20 MB Limit	Same q.

Figure 11 - Using multiple Quotas

NOTE: For more information about Quotas, see the White Paper ‘All about Quotas’

25. When finished, click on the ‘Exemptions’ tab.
26. Click ‘Add’ to list any IP addresses that this quota should not apply to. (IP Addresses must be entered one at a time)
27. When finished, click ‘Apply’ then ‘OK’
28. Back on the IP Range Properties page, click on the ‘Custom Access Policies’ tab.
29. Place a checkmark in any Custom Access Policy in which this IP address range should be applied.
30. Once completed, click ‘Apply, and ‘OK’

Configure an Access Policy for 'Unauthenticated Access'.

NOTE: Unauthenticated access occurs when bt-WebFilter Standalone is not configured to require authentication to the proxy or if ISA/TMG allows 'All Users' through the Microsoft Proxy.

1. Open the WebFilter console and expand the 'Access Rules' container
2. Right click on the 'Unauthenticated Access' object and select 'Properties'. You can also left click on 'Unauthenticated Access' and select 'Action' then 'Properties' from the MMC menu item
3. On the 'Common Information' tab, select the 'Individual Access Policy Type' (See **Access Policy Types** for more information) and then any 'Advanced Redirect Page' options you may have.

NOTE: If you select a 'Permission' or 'Combination' based policy, proceed with step 4. If you chose a 'Restriction' policy, continue with step 10

Permission or Combination based policy

4. Click the 'Allow' tab.
5. Click 'Add'
6. Select the type of Access Object to allow (URL or Category)
7. Click on the 'Details' tab
8. Depending on your selection, you will see a list of Categories allowing you select the ones you wish to apply or a URL box. You can enter multiple URLs and/or Masks by separating them with a ";".
9. Proceed to step 15 below

NOTE: If you are using a 'Combination' policy and you want to Deny certain sections of URLs or Categories that you have allowed above, proceed with step 10.

Restriction based policy

10. Click on the 'Deny' tab
11. Click 'Add'
12. Select the type of Access Object to deny (URL or Category)
13. Click on the 'Details' tab
14. Depending on your selection, you will see a list of Categories allowing you select the ones you wish to apply or a URL box. You can enter multiple URLs and/or Masks by separating them with a ";".
15. Once you make your selections, click the 'Schedule' tab. If you have previously created schedules, this is where you can apply them.
16. Click 'Apply' then 'OK'
17. Click on the 'Quota' tab and click 'Add'
18. On the 'Common Information' tab, select the option for URL or Categories.
19. On the 'Details' tab, enter the URL(s) or Categories that will be affected by this Quota
20. On the 'Schedule' tab, select the Schedule that should be applied to this Quota.
21. Click on the 'Quota' tab and select the 'Quota' to be used.

NOTE: You can configure multiple Quotas in the same policy to allow you to ease restrictions for certain Categories or URLs but have tighter controls on others. (see Figure 11)

22. Click ‘Apply’ and ‘OK’
23. Click on the ‘Custom Access Policies’ tab
24. Place a checkmark in any Custom Access Policy in which this IP address range should be applied.
25. Once completed, click ‘Apply, and ‘OK’

Custom Access Policies

Just like Access Rules, Custom Access Polices have three types, Permission, Restriction, and Combination. (For a review of each, see **Access Policy Types** in this document.). Each CAP can only be configured as one type however you can configure multiple CAPs with different Access Types depending on your requirements.

Like Access Rules, Custom Access Policies can be used to filter based on Domain User Names, Groups, IP Addresses, or Anonymous users. The CAPs are the primary method of applying Allow/Deny restrictions, Quotas, and Schedules to Web Users in your environment.

This document will introduce you to the different tabs and fields and provide you with step by step instructions on how to setup several basic types of Custom Access Policies as well as a few examples of using the different types together to provide as much flexibility as may be required by your users.

The Custom Access Policy Properties Page

bt-WebFilter Standalone and ISA/TMG Filter ship with a 'Default Custom Access Policy'. This CAP utilizes the 'Default' policy type (Dependent upon the Access Rules Properties setting) which, for a new install, is a Restriction type. It denies several Categories that Burstek defines as 'Legal Liability' and is applied to 'Unauthenticated Access'. What this means for your organization is that if you set your browser settings to use the server where WebFilter is installed, you would be denied access to XXX and Gambling sites just to name a few.

NOTE: If you are using bt-WebFilter for ISA/TMG you would need a firewall rule that allowed 'All Users' to use HTTP and HTTPS. If your rule instead uses 'Authenticated Users' or domain names, then the traffic would pass through with an actual user name and would not be denied

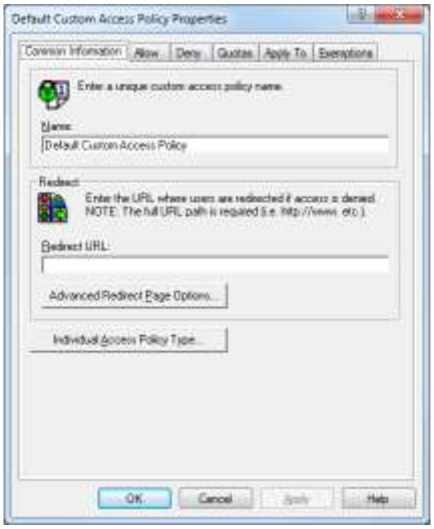
The Common Information Tab

This first tab under the 'Properties' of the Custom Access Policy (see figure 12) defines how this policy will filter users. The tab has 2 configuration buttons labeled 'Advanced Redirect Page Options' and 'Individual Access Policy Type' (IAP). The IAP is the same for the Access Rules previously discussed (see **Access Policy Types**) however if the IAP is set at the CAP level, it overrides the Access Rule level IAP.

The Common Information tab also contains the fields for naming your CAP (I.E. Production – Deny – Social Networking Sites) as well as entering the URL for a redirect page that is displayed to users when a URL or Category is blocked.

NOTE: HTTPS (SSL/443) sites that are blocked cannot be redirected. As a result, the user will only receive a 'Page Cannot be found' message. This is due to the HTTPS protocol which prevents redirection.

When using one of the supplied Advanced Redirect Pages that Burstek Includes with its software, the 'Advanced Redirect Pages Options' button provides you with the ability to specify how long a user should have access to a blocked URL (see figure 13)


Default Custom Access Policy Properties
Common Information
Allow
Deny
Quotas
Apply To
Exemptions

Enter a unique custom access policy name.

Name: Default Custom Access Policy

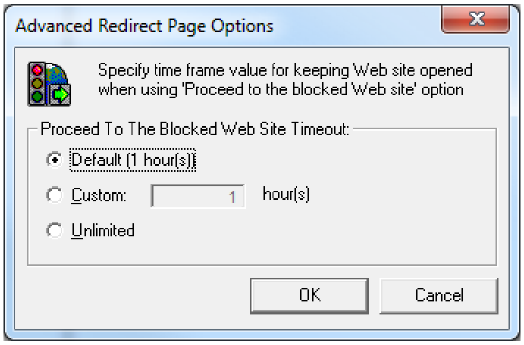
Redirect

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:

Advanced Redirect Page Options...
Individual Access Policy Type...
OK
Cancel
Apply
Help

Figure 12 - CAP Common Information Tab



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)

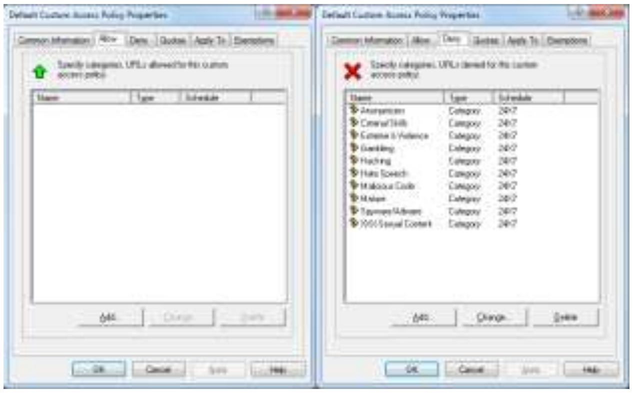
○ Unlimited

Figure 13 – Advanced Redirect Page Options

The ‘Allow’ and ‘Deny’ tabs

The ‘Allow’ and “Deny’ pages are only functional depending on the Access Policy type that is chosen. A permission policy for example, denies all access unless specifically allowed. If used, you would then add entries to the ‘Allow’ tab. A Restriction policy on the other hand only Denies access so the ‘Allow’ tab has no bearing on this type of Access Policy. A Combination Policy, because it is essentially both types in one, will use both the ‘Allow’ and ‘Deny’ tabs.

Adding an entry to either tab will bring up an ‘Access Object Properties’ page which allows you to configure the specifics for the URL or Category that you working with. On this page you can specify the URL(s), Category(s), and the Schedule for when the ‘Allow’ or ‘Deny’ should take place. (see figured 15)



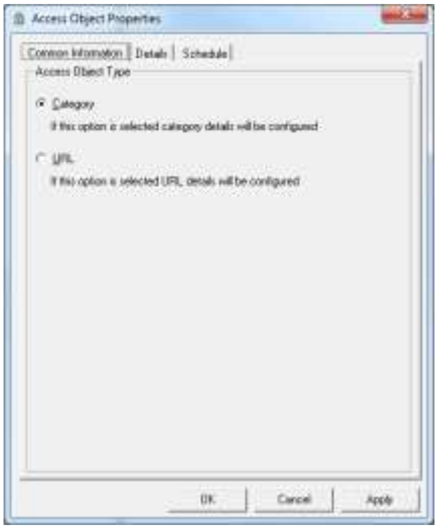
Specify categories, URLs allowed for this custom access policy

Name	Type	Schedule

Specify categories, URLs denied for this custom access policy

Name	Type	Schedule
Anonymizers	Category	24/7
Criminal Skills	Category	24/7
Extreme & Violence	Category	24/7
Gambling	Category	24/7
Hacking	Category	24/7
Hate Speech	Category	24/7
Malicious Code	Category	24/7
Malware	Category	24/7
Spyware/Adware	Category	24/7
XXX Sexual Content	Category	24/7

Figure 14 – Allow and Deny Tabs



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

Figure 15 – Access Object Properties page

If you choose the 'Category' option, when you click on the 'Details' tab, you will see a list of all Categories currently configured in WebFilter allowing you to choose one or more to be applied. If you would like to select multiple Categories however, and you would like them to have different Schedules, you can simply add the Categories for the first Schedule, then go back and add the next Categories for the second Schedule.

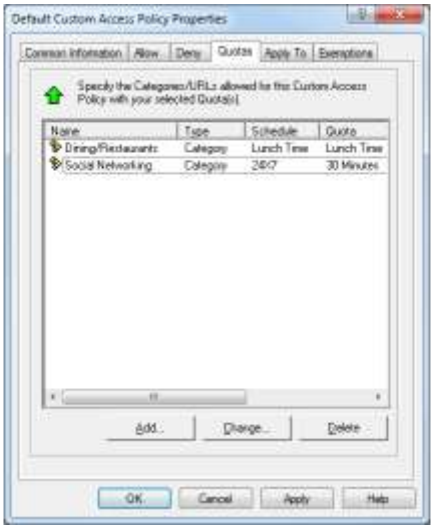
NOTE: Schedules may not be created on the 'Schedule' tab of the Access Object properties page. To configure Schedules, use the 'Schedule' object in the Management Console Tree.

The Quotas Tab

The Quota tab allows you to assign an existing quota to the Custom Access Policy (CAP). Quotas define how much Bandwidth a user or group can use and/or how much Time (in Minutes) they are allowed to access a certain Category or Website. Quotas can also be set for Daily, Weekly, or Monthly resets as well as Strict (Access Denied when limit reached) or Lite (Access permitted but logs generated) severity.

Just like with Schedules, you can set a single Quota for all Categories and URLs on a specific CAP or you can specify different Quotas for each entry in your CAP.

NOTE: Quotas at the Custom Access Policy level affect all users that are applied to the policy. If you need a quota for an individual user, please use the *Individual Rights* option under the Domain Access Rule.



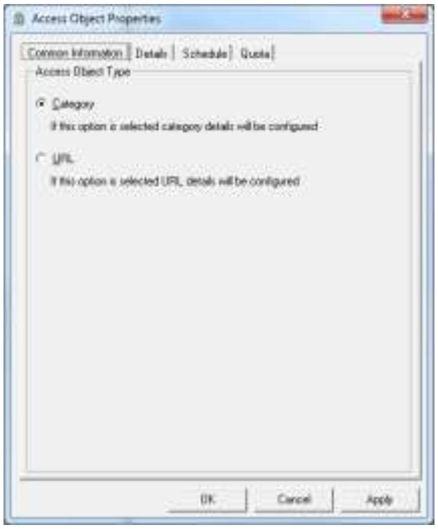
Specify the Categories/URLs allowed for this Custom Access Policy with your selected Quota(s).

Name	Type	Schedule	Quota
Dining/Restaurants	Category	Lunch Time	Lunch Time
Social Networking	Category	24X7	30 Minutes

Figure 16 - Using Multiple Quotas

The Access Object Properties page (see figure 17) displayed when adding a Quota is very similar to the page when adding Categories to Allow/Deny tabs except that there is now a 'Quota' tab that allows you to specify the Quota to be used for these Categories/URLs. (see figures 17 and 18)

For more information regarding Quotas, please refer to the 'Administrators Guide - Using Quotas'



Access Object Type

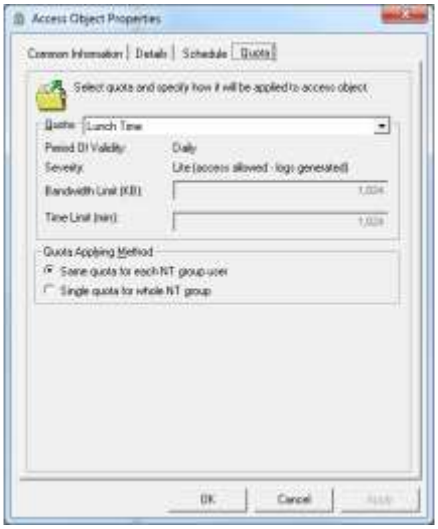
● Category

If this option is selected category details will be configured

○ URL

If this option is selected URL details will be configured

Figure 17 - Quota Access Object Properties Page



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

Quota: Lunch Time

Period Of Validity: Daily

Severity: Lite (access allowed - logs generated)

Bandwidth Limit (KB): 1,024

Time Limit (min): 1,024

Quota Applying Method

● Same quota for each NT group user

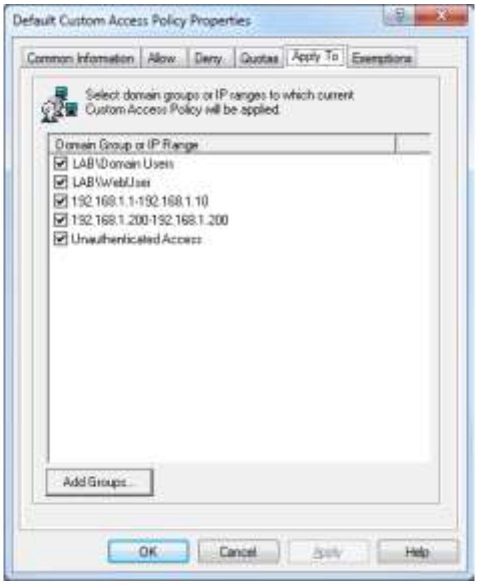
○ Single quota for whole NT group

Figure 18 - Access Object - Quota Tab

The 'Apply To' Tab

The 'Apply To' tab allows you to enter all the IDs that should be governed by this policy. In the figure below (see figure 19), you can see we have an Individual User, an Active Directory Domain Group, an IP Address Range, an Individual IP address and even Unauthenticated Access.

NOTE: This is for demonstration purposes to show that you can utilize multiple IDs on the 'Apply To' tab. In a production environment, if you are requiring user authentication or in the case of WebFilter Standalone, require Proxy Authentication, then anonymous access is not permitted and would not need to be added. Alternately, if you were not requiring authentication, then the Domain User or Domain Group would not need to be added since browser traffic first tries to access anonymously.



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

Domain Group or IP Range

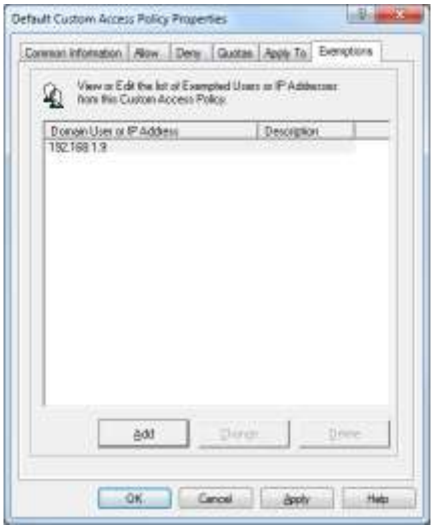
☑ LAB\Domain Users
☑ LAB\WebUser
☑ 192.168.1.1-192.168.1.10
☑ 192.168.1.200-192.168.1.200
☑ Unauthenticated Access

Figure 19 - CAP Apply To Tab

The ‘Exemptions’ Tab

You may wish to simply apply a single Custom Access Policy (CAP) to the Domain Users group or your entire IP address range for simplicity; however, you would also need to exclude certain machines or individuals. The ‘Exemptions’ tab provides this functionality allowing you to exclude users or IP addresses on an ‘as-needed’ basis.

NOTE: When excluding IP addresses, the IP address must be part of the range of IPs configured under the ‘IP Access Rule’. If an incorrect IP address is chosen, an information box will be displayed telling you that the IP address does not belong to any of the selected IP Ranges.



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

Domain User or IP Address	Description
192.168.1.9	

Figure 20 - CAP Exemptions Tab

Configuring Custom Access Policies

Prior to completing any of these steps, you should already have configured the Access Rule (Domain or IP) that you wish to use. If you do not have a Domain or IP Access Rule configured, you will only be able to use the 'Unauthenticated Access' (Anonymous User) in the Custom Access Policy. To configure an Access Rule, please see the 'Access Rules' section in this document.

Additionally, if you will want to use Schedules or Quotas, these need to be configured prior to creating the Custom Access Policy. If the Quotas/Schedules are unavailable during the creation of the CAP, you can modify it at a later time after they have been created.

Configure a Custom Access Policy to block a Category or URL for all specified Users/IP Addresses.

Configure a Custom Access Policy to allow a Category or URL for all specified Users/IP Addresses

Configure a Custom Access Policy to allow access to a Category for a specific bandwidth/period of time

Configure a Custom Access Policy to allow/deny access to a Category or URL during a specific time period

Configure a Custom Access Policy to deny access to unknown URLs

Configure a Custom Access Policy to allow expanded web access on Lunch/Break Room PCs or KIOSKS

Configure a Custom Access Policy to block a Category or URL for all specified Users/IP Addresses.

1. Open the bt-WebFilter Management Console
2. Right click on the 'Custom Access Policies' container object and select 'New Custom Access Policy'
3. On the 'Common Information' tab, type a name for the new policy (I.E. Production – Deny Social Networking)
4. In the 'Redirect URL' field, enter the URL to your internal Web Server where you are hosting your redirect page. (If you do not have this configured, leave this blank)
5. If you are using a Custom Redirect page that allows users to bypass the restriction for a certain amount of time, click the 'Advanced Redirect Page Options' button. If not, continue to step 7
6. Specify how much time the user should be granted access to the web site for and click 'OK'
7. Click on the 'Individual Access Policy Type' button
8. Select the 'Restriction' policy type and click 'OK'
9. Select the 'Deny' tab
10. Click 'Add'
11. Make sure 'Category' is selected for the 'Access Object Type' and click the 'Details' tab. If you want to enter a URL or URL Mask, select the 'URL' option.
12. Scroll down the list until you locate the Category you want to deny access for and place a check mark in the box. If you are using the URL option, enter the URL or Mask in the field provided
13. If you want to use a schedule, select the 'Schedule' tab. Otherwise proceed to step 15
14. On the 'Schedule' tab, select the name of the Schedule that you want to use.
15. Click 'Apply' then 'OK'
16. Click on the 'Apply To' tab
17. If you are applying this policy to a single IP address or User, they should appear in the window. Simply place a check mark in the box next to the item. If you are applying to a Domain Group, Click on the 'Add Groups' button on the bottom of the page.
18. Enter the name of the group in the 'Select Groups' window and click the 'Check Names' button on the right.
19. When the name resolves correctly, click 'OK'. If the name does not resolve, check the spelling and try again or use the 'Advanced' button to locate the group.
20. Click on the 'Exemptions' tab
21. Click the 'Add' button and select either 'User' or 'IP Address' from the list. If you chose 'User' continue with the next step. If you chose 'IP Address' proceed to step 24

WARNING: In step 22, do not use the 'Display Group Members' in organizations where the group could have a very large number of users such as 'Domain Users'. Instead, use the 'Browse' feature.

22. In the 'Select Users' window click 'Display Group Members'. The list of users applied to the group should appear. Locate the user(s) that you want to exclude and click 'Add'
23. When all the names that you want to exclude from the policy have been selected, click 'OK'. You should see the user(s) in the Exemption window. Proceed to step 26
24. In order to exclude an IP address, an IP address range must be selected on the 'Apply To' tab. Enter the IP address of an IP in the range that is applied to the policy. If the IP address does not match the currently configured range, you will receive an information box stating *'IP address does not belong to any of the selected IP ranges'*
25. When the IP address is correctly entered, click the 'OK' button

26. Click 'Apply' then 'OK' on the Custom Access Policy Properties page.

Configure a Custom Access Policy to allow a Category or URL for all specified users/IP addresses

1. Open the bt-WebFilter Management Console
2. Right click on the 'Custom Access Policies' container object and select 'New Custom Access Policy'
3. On the 'Common Information' tab, type a name for the new policy (I.E. Production – Allow Social Networking)
4. In the 'Redirect URL' field, enter the URL to your internal Web Server where you are hosting your redirect page. (If you do not have this configured, leave this blank)
5. If you are using a Custom Redirect page that allows users to bypass the restriction for a certain amount of time, click the 'Advanced Redirect Page Options' button. If not, continue to step 7
6. Specify how much time the user should be granted access to the web site for and click 'OK'
7. Click on the 'Individual Access Policy Type' button
8. Select the 'Permission' policy type and click 'OK'
9. Select the 'Allow' tab
10. Click 'Add'
11. Make sure 'Category' is selected for the 'Access Object Type' and click the 'Details' tab. If you want to enter a URL or URL Mask, select the 'URL' option.
12. Scroll down the list until you locate the Category you want to deny access for and place a check mark in the box. If you are using the URL option, enter the URL or Mask in the field provided
13. If you want to use a schedule, select the 'Schedule' tab. Otherwise proceed to step 15
14. On the 'Schedule' tab, select the name of the Schedule that you want to use.
15. Click 'Apply' then 'OK'
16. Click on the 'Apply To' tab
17. If you are applying this policy to a single IP address or User, they should appear in the window. Simply place a check mark in the box next to the item. If you are applying to a Domain Group, Click on the 'Add Groups' button on the bottom of the page.
18. Enter the name of the group in the 'Select Groups' window and click the 'Check Names' button on the right.
19. When the name resolves correctly, click 'OK'. If the name does not resolve, check the spelling and try again or use the 'Advanced' button to locate the group.
20. Click on the 'Exemptions' tab
21. Click the 'Add' button and select either 'User' or 'IP Address' from the list. If you chose 'User' continue with the next step. If you chose 'IP Address' proceed to step 24

WARNING: In step 22, do not use the 'Display Group Members' in organizations where the group could have a very large number of users such as 'Domain Users'. Instead, use the 'Browse' feature

22. In the 'Select Users' window click 'Display Group Members'. The list of users applied to the group should appear. Locate the user(s) that you want to exclude and click 'Add'
23. When all the names that you want to exclude from the policy have been selected, click 'OK'. You should see the user(s) in the Exemption window. Proceed to step 26
24. In order to exclude an IP address, an IP address range must be selected on the 'Apply To' tab. Enter the IP address of an IP in the range that is applied to the policy. If the IP address does not match the currently configured range, you will receive an information box stating *'IP address does not belong to any of the selected IP ranges'*

25. When the IP address is correctly entered, click the 'OK' button
26. Click 'Apply' then 'OK' on the Custom Access Policy Properties page.

Configure a Custom Access Policy to allow access to a Category for a specific bandwidth/period of time

For this procedure, you will need a Quota already configured for Bandwidth, Time or both. If you have not already done so, please be sure to create the Quota prior to continuing. Instructions on creating Quota can be found in the User Guide or the 'Administrators Guide – Quotas'

1. Open the bt-WebFilter Management Console
2. Right click on the 'Custom Access Policies' container object and select 'New Custom Access Policy'. If you want to use an existing Custom Access Policy, simply select its 'Properties' instead.
3. On the 'Common Information' tab, type a name for the new policy (I.E. Production – Allow Social Networking for 30 Minutes)
4. In the 'Redirect URL' field, enter the URL to your internal Web Server where you are hosting your redirect page. (If you do not have this configured, leave this blank)
5. If you are using a Custom Redirect page that allows users to bypass the restriction for a certain amount of time, click the 'Advanced Redirect Page Options' button. If not, continue to step 7
6. Specify how much time the user should be granted access to the web site for and click 'OK'
7. Click on the 'Individual Access Policy Type' button
8. Select either the 'Permission' or 'Restriction' policy type and click 'OK'
9. Click on the 'Quotas' tab
10. Click the 'Add' button
11. Make sure 'Category' is selected for the 'Access Object Type' and click the 'Details' tab. If you want to enter a URL or URL Mask, select the 'URL' option.
12. Click on the 'Details' tab
13. Select the Category or Categories from the list by placing a checkmark in the box next to each one. If you are using the URL option, enter the URL or Mask in the field provided
14. Select the 'Schedule' tab and select the name of the Schedule that you want to use.
15. Click on the 'Quota' tab
16. Select the Quota from the drop down that should be applied to the Category or Categories selected in step 13
17. Specify how the Quota should be applied under the 'Quota Applying Method'. (Default is Same quota for each NT group user)
18. Click 'Apply' then 'OK'
19. Click on the 'Apply To' tab
20. If you are applying this policy to a single IP address or User, they should appear in the window. Simply place a check mark in the box next to the item. If you are applying to a Domain Group, Click on the 'Add Groups' button on the bottom of the page.
21. Enter the name of the group in the 'Select Groups' window and click the 'Check Names' button on the right.
22. When the name resolves correctly, click 'OK'. If the name does not resolve, check the spelling and try again or use the 'Advanced' button to locate the group.
23. Click on the 'Exemptions' tab
24. Click the 'Add' button and select either 'User' or 'IP Address' from the list. If you chose 'User' continue with the next step. If you chose 'IP Address' proceed to step 27

WARNING: In step 25, do not use the 'Display Group Members' in organizations where the group could have a very large number of users such as 'Domain Users'. Instead, use the 'Browse' feature.

25. In the 'Select Users' window click 'Display Group Members'. The list of users applied to the group should appear. Locate the user(s) that you want to exclude and click 'Add'
26. When all the names that you want to exclude from the policy have been selected, click 'OK'. You should see the user(s) in the Exemption window. Proceed to step 29
27. In order to exclude an IP address, an IP address range must be selected on the 'Apply To' tab. Enter the IP address of an IP in the range that is applied to the policy. If the IP address does not match the currently configured range, you will receive an information box stating *'IP address does not belong to any of the selected IP ranges'*
28. When the IP address is correctly entered, click the 'OK' button
29. Click 'Apply' then 'OK' on the Custom Access Policy Properties page.

This configuration was slightly different in that we do not use the 'Allow' or 'Deny' tabs. Instead, we used the Quota to determine the type of access. Depending on the Individual Access Policy type chosen, the following results are observed.

Permission – With the Permission policy type, the quota will act as an Allow until the configured limits are reached. Once the Bandwidth or Time configured is reached, access to the Category will be denied.

NOTE: Because we did not add any objects to the 'Allow' tab, this policy would prevent all URL access once the Quota was reached.

Restriction – With the Restriction policy type, the quota will act as an Allow until the configured limits are reached. Once the Bandwidth or Time configured is reached, access to the Category will be denied.

In this situation, while both function as a 'Deny', the Policy type is the deciding element. If you have a 'Permission' policy for other Categories and only want to allow this Category for a short period, you simply add the Quota. This removed the need to create a Custom Access Policy just for the Quota.

In the case of a restriction policy where you typically 'Deny' access to this Category, you may want to open it up during lunch or break periods. Again, simply add the quota to this single Category and you do not need to create a new CAP.

Configure a Custom Access Policy to allow/Deny access to a Category or URL during a specific time period

In order to complete this configuration, you will need to configure a 'Schedule' to have available. The schedule can be applied after this however.

1. Open the bt-WebFilter Management Console
2. Right click on the 'Custom Access Policies' container object and select 'New Custom Access Policy'. If you want to use an existing Custom Access Policy, simply select its 'Properties' instead.
3. On the 'Common Information' tab, type a name for the new policy (I.E. Production – Deny Social Networking during Work Hours)
4. In the 'Redirect URL' field, enter the URL to your internal Web Server where you are hosting your redirect page. (If you do not have this setup, leave this blank)

5. If you are using a Custom Redirect page that allows users to bypass the restriction for a certain amount of time, click the 'Advanced Redirect Page Options' button. If not, continue to step 7
6. Specify how much time the user should be granted access to the web site for and click 'OK'
7. Click on the 'Individual Access Policy Type' button
8. Select the 'Restriction' policy type and click 'OK'
9. Select the 'Deny' tab
10. Click 'Add'
11. Make sure 'Category' is selected for the 'Access Object Type' and click the 'Details' tab
12. Scroll down the list until you locate the Category you want to deny access for and place a check mark in the box.
13. Select the 'Schedule' tab.
14. On the 'Schedule' tab, select the name of the Schedule that you want to use.
15. Click 'Apply' then 'OK'
16. Click on the 'Apply To' tab
17. If you are applying this policy to a single IP address or User, they should appear in the window. Simply place a check mark in the box next to the item. If you are applying to a Domain Group, Click on the 'Add Groups' button on the bottom of the page.
18. Enter the name of the group in the 'Select Groups' window and click the 'Check Names' button on the right.
19. When the name resolves correctly, click 'OK'. If the name does not resolve, check the spelling and try again or use the 'Advanced' button to locate the group.
20. Click on the 'Exemptions' tab
21. Click the 'Add' button and select either 'User' or 'IP Address' from the list. If you chose 'User' continue with the next step. If you chose 'IP Address' proceed to step 24

WARNING: In step 22, do not use the 'Display Group Members' in organizations where the group could have a very large number of users such as 'Domain Users'. Instead, use the 'Browse' feature

22. In the 'Select Users' window click 'Display Group Members'. The list of users applied to the group should appear. Locate the user(s) that you want to exclude and click 'Add'
23. When all the names that you want to exclude from the policy have been selected, click 'OK'. You should see the user(s) in the Exemption window. Proceed to step 26
24. In order to exclude an IP address, an IP address range must be selected on the 'Apply To' tab. Enter the IP address of an IP in the range that is applied to the policy. If the IP address does not match the currently configured range, you will receive an information box stating *'IP address does not belong to any of the selected IP ranges'*
25. When the IP address is correctly entered, click the 'OK' button
26. Click 'Apply' then 'OK' on the Custom Access Policy Properties page.

This policy will now deny access or allow it. During the 'Active' times, the Category will be denied however during the 'Inactive' time, the Custom Access Policy will not restrict access to the Category.

In this procedure we use a 'Restriction' policy type however if a 'Permission' policy had been used, during the 'Active' time, the Category would be allowed then denied during the 'Inactive' time.

Configure a Custom Access Policy to deny access to unknown URLs

1. Open the bt-WebFilter Management Console
2. Right click on the ‘Custom Access Policies’ container object and select ‘New Custom Access Policy’
3. On the ‘Common Information’ tab, type a name for the new policy (I.E. Production – Deny Unknown Web Sites)
4. In the ‘Redirect URL’ field, enter the URL to your internal Web Server where you are hosting your redirect page. (If you do not have this setup, leave this blank)
5. If you are using a Custom Redirect page that allows users to bypass the restriction for a certain amount of time, click the ‘Advanced Redirect Page Options’ button. If not, continue to step 7
6. Specify how much time the user should be granted access to the web site for and click ‘OK’
7. Click on the ‘Individual Access Policy Type’ button
8. Select the ‘Permission’ policy type and click ‘OK’
9. Select the ‘Alloy’ tab
10. Click ‘Add’
11. Make sure ‘Category’ is selected for the ‘Access Object Type’ and click the ‘Details’ tab
12. Scroll down the list and place a check mark in every Category that you want to allow access to.
13. If you want to use a schedule, select the ‘Schedule’ tab. Otherwise proceed to step 15
14. On the ‘Schedule’ tab, select the name of the Schedule that you want to use.
15. Click ‘Apply’ then ‘OK’
16. Click on the ‘Apply To’ tab
17. If you are applying this policy to a single IP address or User, they should appear in the window. Simply place a check mark in the box next to the item. If you are applying to a Domain Group, Click on the ‘Add Groups’ button on the bottom of the page.
18. Enter the name of the group in the ‘Select Groups’ window and click the ‘Check Names’ button on the right.
19. When the name resolves correctly, click ‘OK’. If the name does not resolve, check the spelling and try again or use the ‘Advanced’ button to locate the group.
20. Click on the ‘Exemptions’ tab
21. Click the ‘Add’ button and select either ‘User’ or ‘IP Address’ from the list. If you chose ‘User’ continue with the next step. If you chose ‘IP Address’ proceed to step 24

WARNING: In step 22, do not use the ‘Display Group Members’ in organizations where the group could have a very large number of users such as ‘Domain Users’. Instead, use the ‘Browse’ feature.

22. In the ‘Select Users’ window click ‘Display Group Members’. The list of users applied to the group should appear. Locate the user(s) that you want to exclude and click ‘Add’
23. When all the names that you want to exclude from the policy have been selected, click ‘OK’. You should see the user(s) in the Exemption window. Proceed to step 26
24. In order to exclude an IP address, an IP address range must be selected on the ‘Apply To’ tab. Enter the IP address of an IP in the range that is applied to the policy. If the IP address does not match the currently configured range, you will receive an information box stating *‘IP address does not belong to any of the selected IP ranges’*
25. When the IP address is correctly entered, click the ‘OK’ button
26. Click ‘Apply’ then ‘OK’ on the Custom Access Policy Properties page.

In this configuration, we use a 'Permission' policy to allow access to all known sites in the Selected categories. Any URL that does not match a Category is denied.

Configure a Custom Access Policy to allow expanded web access on Lunch/Break Room PCs or KIOSKS

In this Custom Access Policy example, we are going to use several of the configurations previously discussed to perform the following:

- All Workstation PCs should be able to access URLs/Categories that comply with the Company Acceptable Internet Use Policy.
- Lunch/Break room Workstations should be allowed access to Social Networking sites during specific times.
- All Devices should be restricted from certain Categories at all times.

Pre-requisites:

1. Create a Domain Access Rule
2. Create an IP Range for the regular office workstation PCs
3. Create an IP Range for the Lunch/Break room workstations
4. Create a Schedule that is Active for working hours
5. Create a Schedule that Is Active for Break/Lunch hours

Procedure

1. Open the bt-WebFilter Management Console
2. Right click on the 'Custom Access Policies' container object and select 'New Custom Access Policy' or choose the 'Properties' of an existing Custom Access Policy.
3. On the 'Common Information' tab, type a name for the new policy (I.E. Production – Acceptable Use Policy for Desktops)
4. Click on the 'Individual Access Policy Type' button
5. Select the 'Restriction' policy type and click 'OK'
6. Select the 'Deny' tab
7. Click the 'Add' button
8. On the 'Common Information' tab, ensure the 'Category' option is selected.
9. Click the 'Details' tab
10. Select all the Categories that should be denied by placing a checkmark in the box.
11. Click on the 'Schedule' tab
12. Select the Working Hours schedule
13. Click 'Apply' and 'OK'
14. Click on the 'Apply To' tab
15. Add the 'Domain Users' Active Directory group
16. Click 'Apply' and 'OK'
17. Create the second policy by right clicking on the 'Custom Access Policies' container object and select 'New Custom Access Policy'
18. On the 'common Information' tab, type a name for the new policy (I.E. Production – Acceptable Use Policy for Lunch Room Desktops)
19. Click on the 'Individual Access Policy Type' button

20. Select the 'Permission' policy type and click 'OK'
21. Select the 'Allow' tab
22. Click the 'Add' button
23. On the 'Common Information' tab, ensure the 'Category' option is selected.
24. Click the 'Details' tab
25. Select all the Categories that should be allowed by placing a checkmark in the box
26. Click on the 'Schedule' tab
27. Select the Break/Lunch hours Schedule
28. Click 'Apply' and 'OK'
29. Click on the 'Apply To' tab
30. Select the 'IP Address' for the Break/Lunch room PCs by placing a check mark in the box
31. Click 'Apply' and 'OK'
32. Create a third Custom Access Policy by right clicking on the 'Custom Access Policies' container object and select 'New Custom Access Policy'
33. On the 'Common Information' tab, type a name for the new policy (I.E. Production – Acceptable Use Policy DENY ALWAYS)
34. Click on the 'Individual Access Policy Type' button
35. Select the 'Restriction' policy type and click 'OK'
36. Select the 'Deny' tab
37. Place a checkmark next to all categories that should always be denied.
38. Click 'Apply' and 'OK'
39. Click on the 'Apply TO' tab
40. Select the IP Address range for both the regular office workstations and the Lunch/Break room PCs.
41. Click 'Apply' and 'OK'