Wavecrest**CyBlock**®Cloud

CyBlock CB by Wavecrest

Secure Web Filtering and Monitoring

Wavecrest

Getting**Started**

www.wavecrest.net

Copyright
Copyright © 1996-2021, Wavecrest Computing, Inc. All rights reserved. Use of this product and this manual is subject to license. Information in this document is subject to change without notice.
904 East New Haven Avenue, Melbourne, FL 32901 USA
www.wavecrest.net

Trademarks
The following are trademarks, registered trademarks, or service marks of Wavecrest Computing, Inc.: Wavecrest Computing, Inc., CyBlock® App, CyBlock® Appliance, CyBlock® Client, CyBlock® Cloud, CyBlock® Directory Agent, CyBlock® ISA, CyBlock® Software, Cyfin®, and OtherWise™. All other trademarks mentioned are the property of their respective owners.

Getting Started

Getting Started Checklist

This checklist is provided for getting CyBlock Cloud up and running. It involves the following steps:

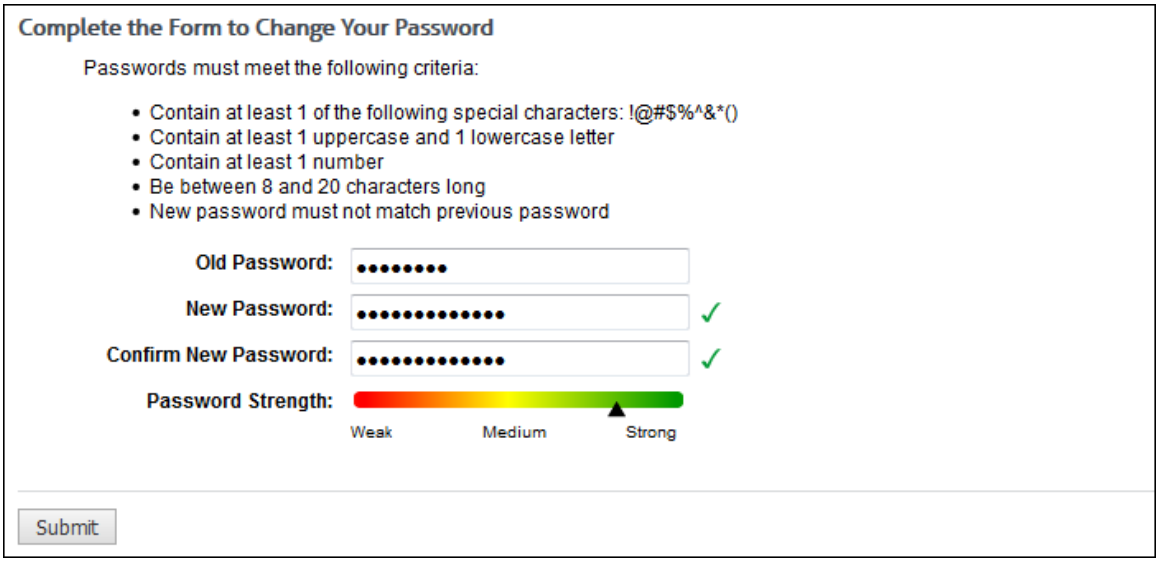
- **Change the Default Password** - Change the Administrator password.
- **Configure IE/Chrome Browsers** - Set Internet Explorer/Chrome browsers to use the PAC file.
- **Configure Firefox Browsers** - Set Firefox browsers to use the PAC file.
- **Configure Authentication** - Specify NTLM or cookie authentication for your network definitions.
- **Install the Wavecrest Certificate** - Receive CyBlock's blocking message on https sites and avoid certificate errors.
- **Test the Product for Blocking** - Test CyBlock's blocking feature.
- **Generate Some Log Files** - Browse the Internet in order to create some log files.

  In this step you will generate and record some Web activity. Browse the Internet with your configured browser for about five minutes. For example, go to wavecrest.net, espn.go.com, msn.com, amazon.com, and cnn.com.
- **Run the Web Monitor Report** - View Web traffic live.
- **Create and Run a Site Analysis Report** - Create a high-level summary report–one that is useful for identifying suspect areas.

Change Your Password

This page allows you to update the password for your account. You are required to do this before using the product in order to change the temporary password assigned by the system. You may also use this page to change your password at any time.

1. The Change Your Password page is triggered in many ways including:
   - When adding a logon account.
   - When logged on, hovering over your account and clicking the key icon on the Manage Logon Accounts page.



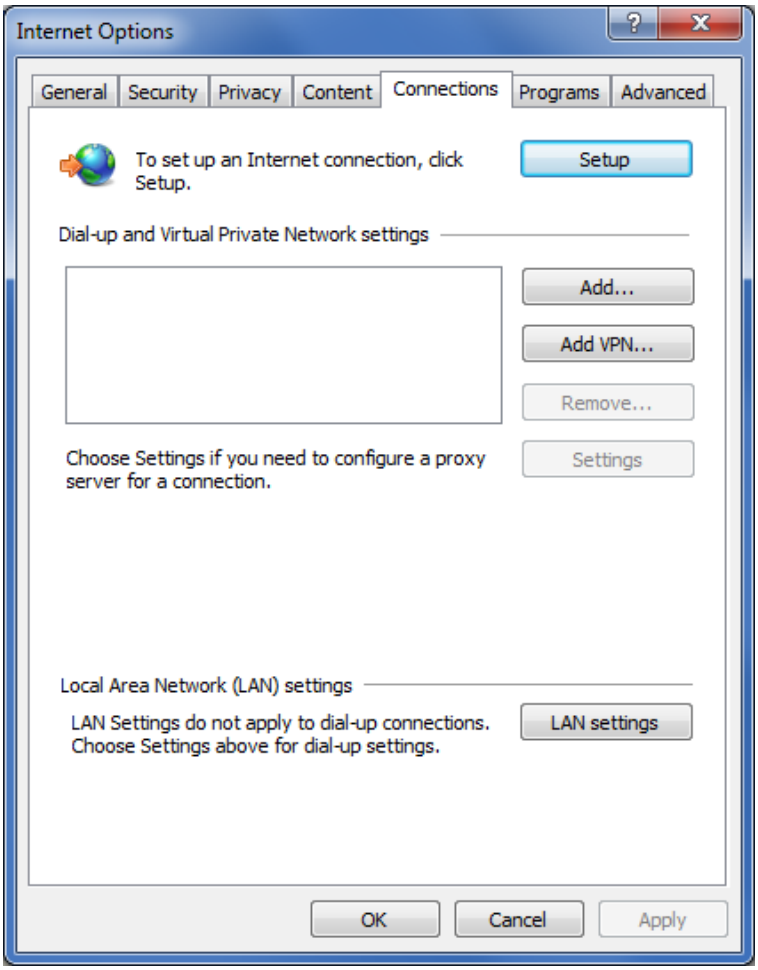
2. In the **Old Password** field, type the current password for the account.

3. In the **New Password** field, type the new password for the account. As you type the new password, a red x will display to the right of the field and change to a green check mark when the password criteria have been met. The password must meet the following criteria:
    - Contain at least 1 of the following special characters: !@#$%^&*()
    - Contain at least 1 uppercase and 1 lowercase letter
    - Contain at least 1 number
    - Be between 8 and 20 characters long
    - Must not match previous password
4. In the **Confirm New Password** field, retype the new password to confirm it. As you type the password, a red x will display to the right of the field and change to a green check mark when the confirmation password matches the new password. The Submit button will also be enabled.
5. The **Password Strength** indicator evaluates your password's strength automatically and displays how strong your password is from *Weak* to *Strong*.
6. Click **Submit** to apply your change.

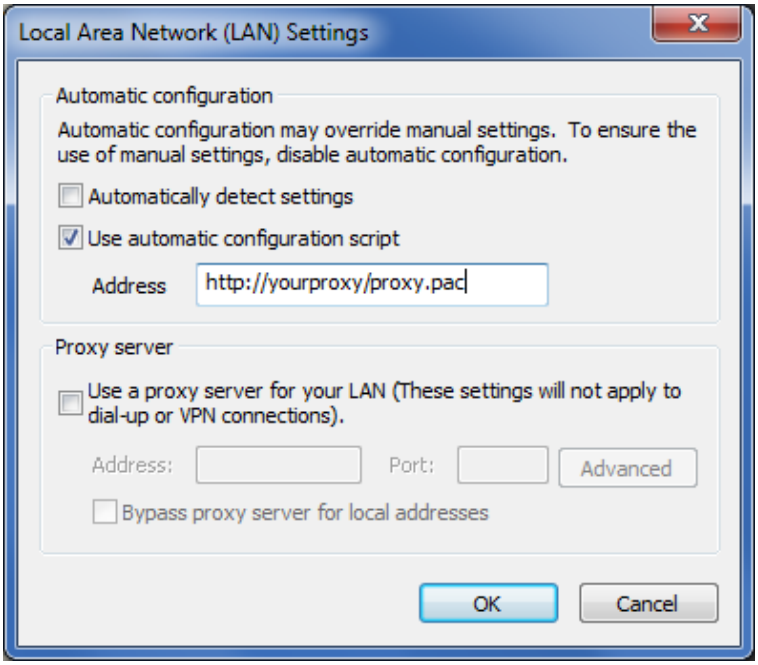
Set Internet Explorer/Chrome Browser Settings Using the PAC File

NOTE: The Chrome browser uses the same proxy settings as Internet Explorer.

1. Open your Internet Explorer or Chrome browser.
2. Continue with one of the following:
    - In Internet Explorer, click the **Tools** menu. Then, click **Internet options**. The Internet Options dialog box will appear.
    - In Chrome, in the top right, click the **Customize and control Google Chrome** icon. Then click **Settings**.
        - At the bottom, click **Show advanced settings**.
        - Under **Network**, click **Change proxy settings**. The Internet Properties dialog box will appear.



3. Click the **Connections** tab and then the **LAN settings** button.

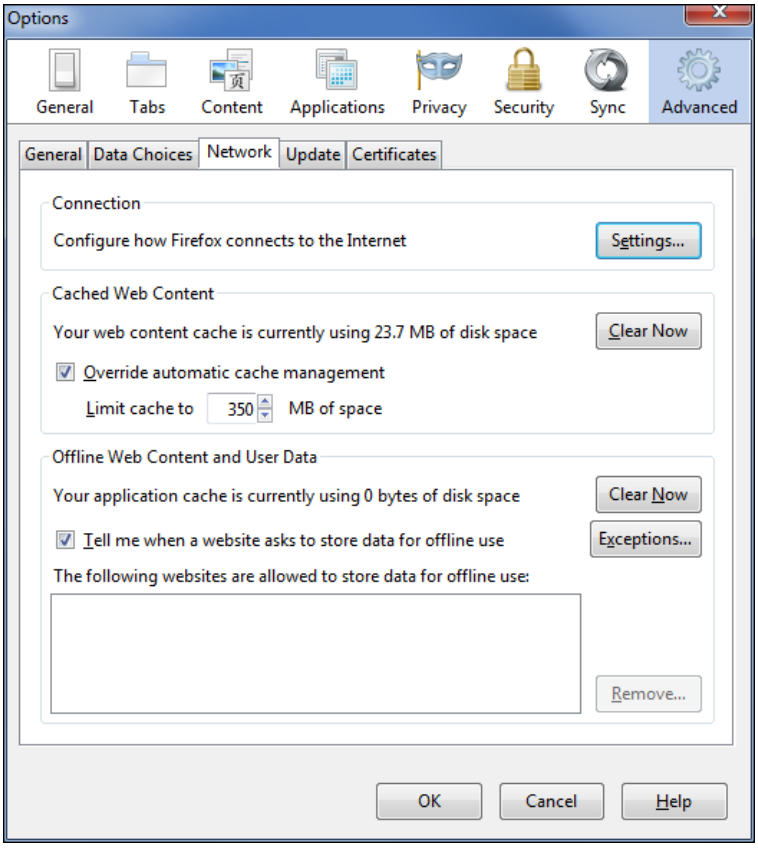


4. Select the **Use automatic configuration script** check box.

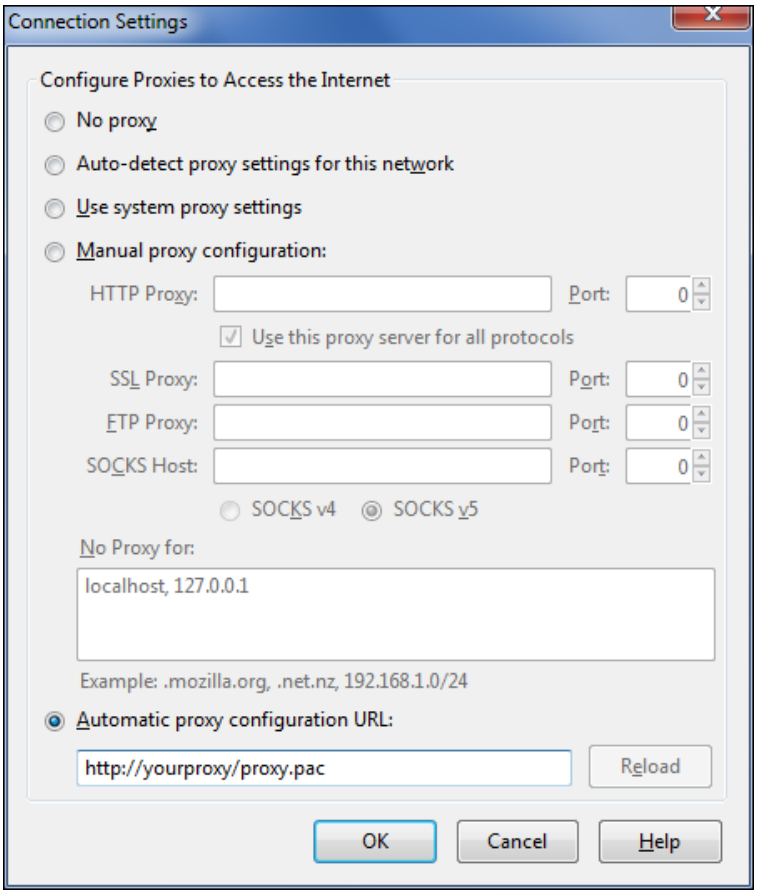
5. Type the PAC URL (located on the **Settings - Proxy - PAC File** screen) in the **Address** field.
6. Click **OK** to save your settings.

Set Firefox Browser Settings Using the PAC File

1. Begin by opening your Mozilla Firefox browser.
2. Click the **Tools** menu, and then click **Options**.



3. Make sure that the **Advanced** icon is selected. Then click the **Network** tab and click the **Settings** button under **Connection**.

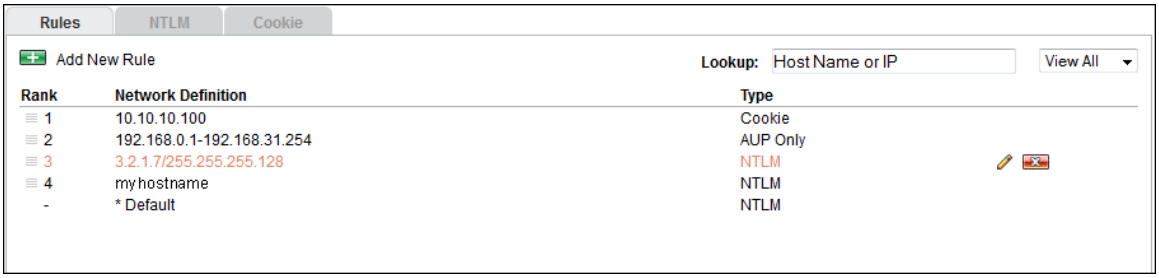


4. Select the **Automatic proxy configuration URL** option.
5. Type the PAC URL (located on the **Settings - Proxy - PAC File** screen) in the **Automatic proxy configuration URL** field.
6. Click **OK** to save your settings.

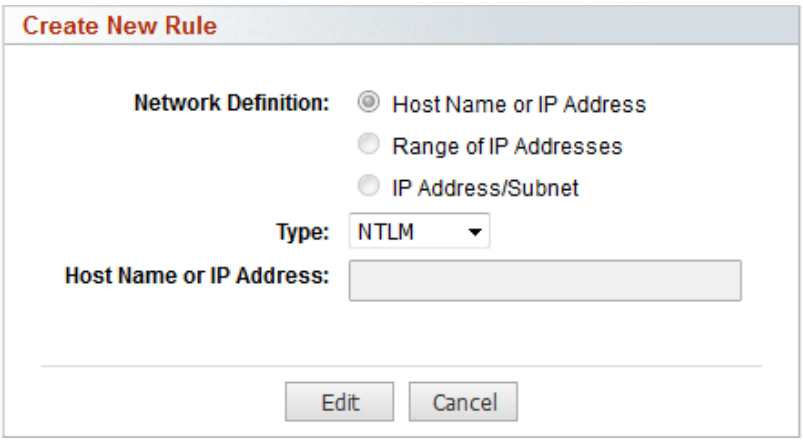
Authentication Rules

The Rules tab allows you to create authentication rules for various network definitions, such as an individual IP address, a range of IP addresses, and a host name. You may set authentication to NTLM, Cookie, AUP Only, or Disabled.

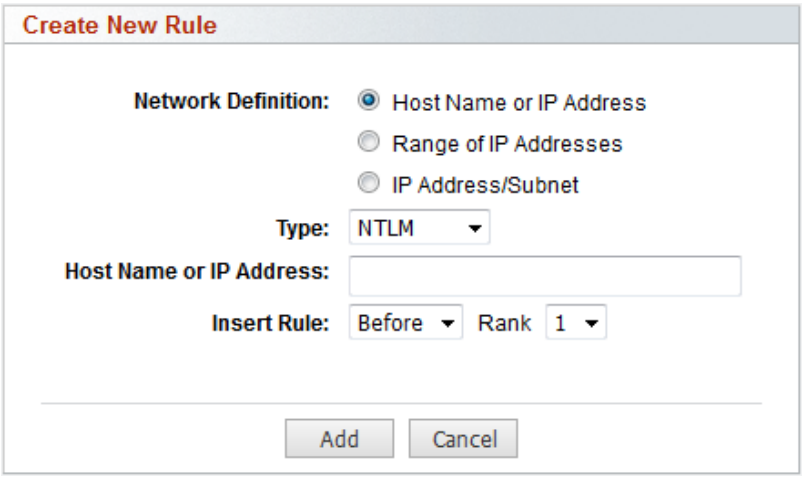
1. Go to **User Management - Authentication**. The Rules tab is displayed.



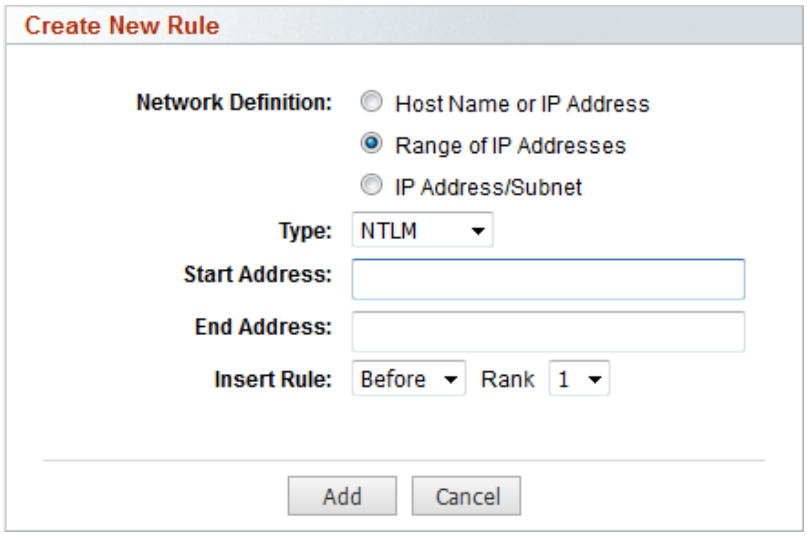
2. The default authentication (* Default) NTLM is displayed and is always set to the lowest priority and therefore last in the list. It can be modified, but not be deleted.
3. To change the default authentication, hover over the rule line and click the pencil icon.



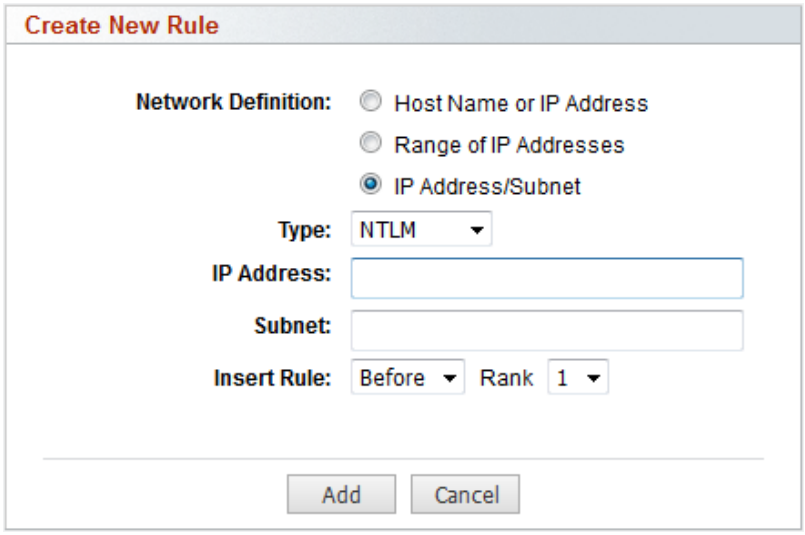
4. In the dialog box, you may only change the **Type** field. Select an authentication type from *NTLM*, *Cookie*, *AUP Only*, and *Disabled*. Click **Edit**.
5. To create a rule, click the **Add New Rule** green plus icon.



6. For the **Network Definition** field, select **Host Name or IP Address**, **Range of IP Address**, or **IP Address/Subnet**.
7. In the **Type** field, select *NTLM*, *Cookie*, *AUP Only*, or *Disabled*.
8. Complete the fields as follows:
   - If you selected **Host Name or IP Address**, type the host name or IP address in the **Host Name or IP Address** field.
   - If you selected **Range of IP Addresses**, in the **Start Address** field, type the first address in the range. In the **End Address** field, type the last address in the range.



- If you selected **IP Address/Subnet**, enter the IP address and subnet in the respective fields.

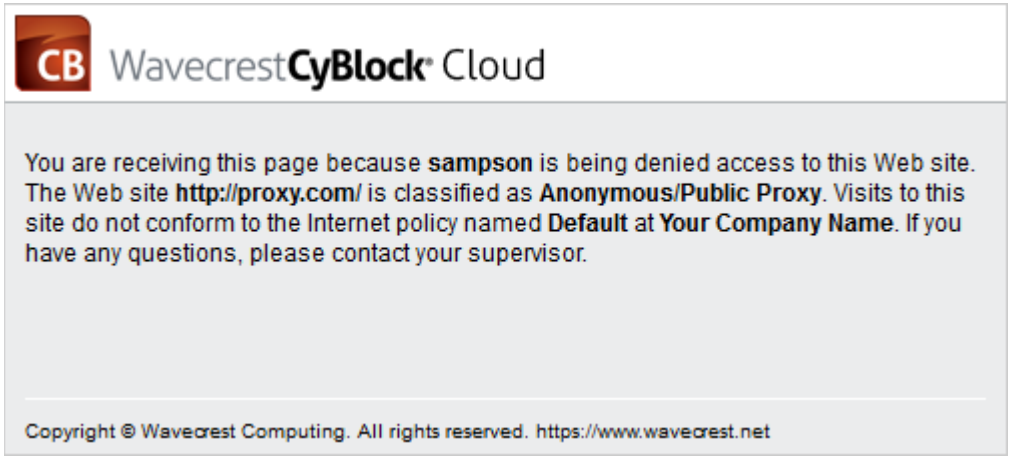


9. The **Insert Rule** fields allow you to specify where the new rule should appear in the list. Select *Before* or *After* and the rank number of an existing rule.
10. Click **Add**. Continue adding more rules as necessary. If a new rule overlaps an existing rule, a message will be displayed.
11. To sort the rules, click the drag icon and drag the rule to where you want it.
12. To edit a rule, hover over the corresponding line and click the pencil icon.
13. To delete a rule, hover over the corresponding line and click the red x icon.
14. If you have a long list of rules, you may search for a host name or IP address by entering it in the **Lookup** field and pressing ENTER. Click **Back to Rules list** to return to the list of rules.
15. To change the view of the rules, select *NTLM*, *Cookie*, *AUP Only*, or *Disabled* in the filter field. The default is *View All*.

Test the Product for Blocking

In this step, you will test the product's default blocking policy.

1. Open your browser and try to browse to www.proxy.com. Anonymous/Public Proxy, Malware, and Pornography are the categories blocked in CyBlock's default blocking policy.
2. A message similar to the one below should appear on your screen. This lets you know that the policy is in effect and working.

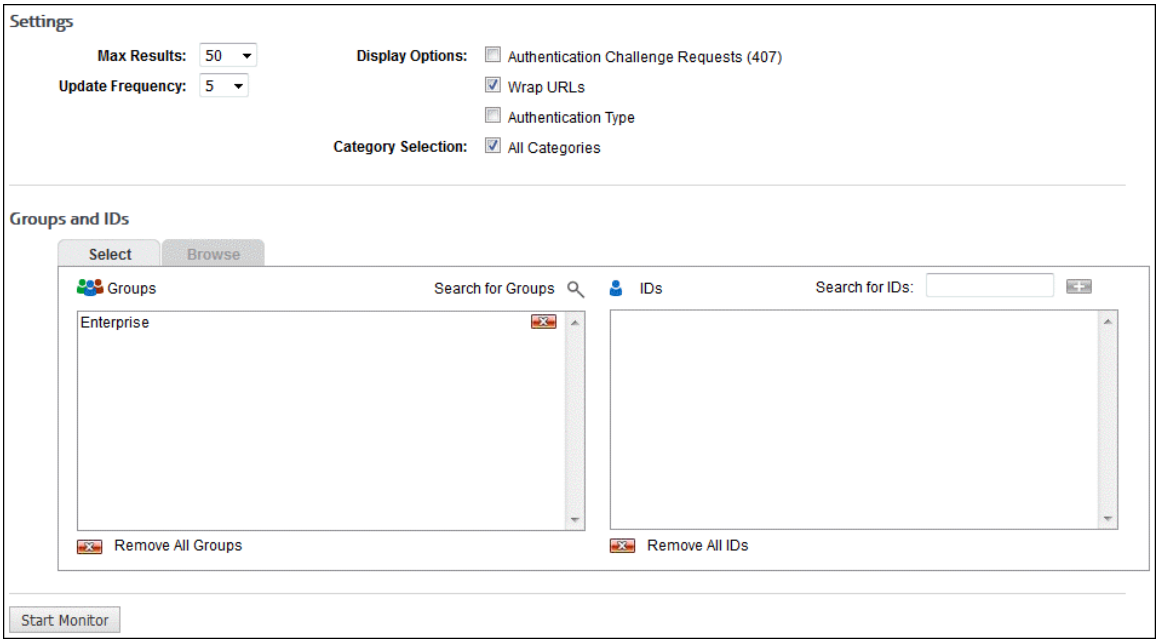


NOTE: If you are unsure about a URL's assigned category, you can use the product's Check URL feature. Go to the **Categorization - Check URL** screen, and enter the URL that you are uncertain about.

Real-Time Web Monitor

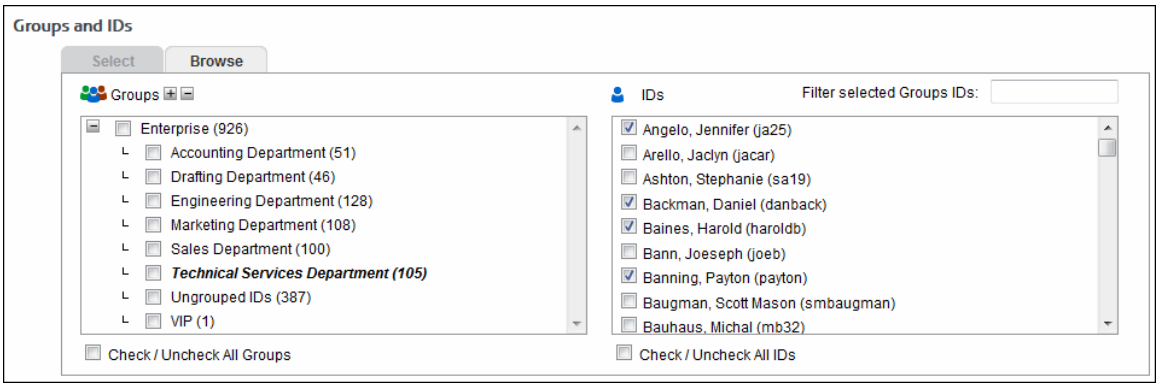
This page lets you establish settings for the Real-Time Web Monitor and run it in order to monitor live Web traffic as it is occurring on your network.

1. Go to **Real-Time Monitors - Web**. The Real-Time Web Monitor page is displayed.



2. Under **Settings**, in the **Max Results** field, select the maximum number of URLs you want to see on the Real-Time Web Monitor. Any URLs that exceed this number are dropped from the list of results.
3. In the **Update Frequency** field, select how frequently you want the screen to update in seconds.

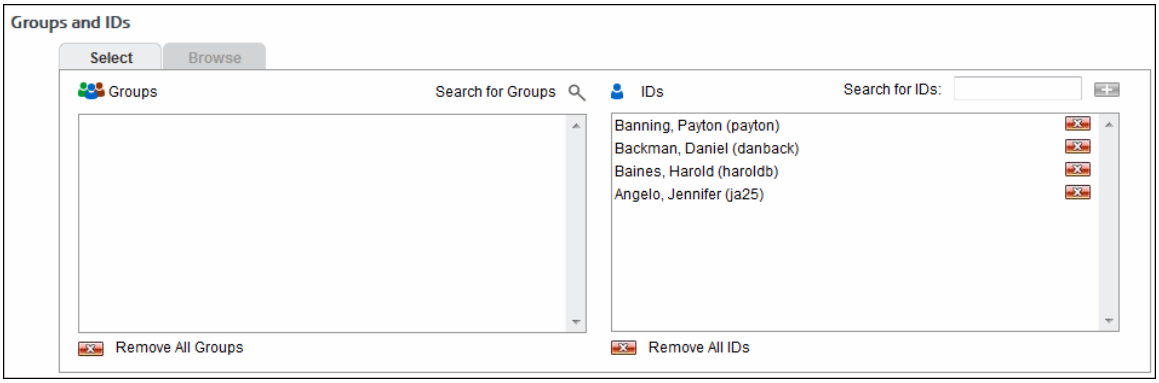
4. For **Display Options**, select **Authentication Challenge Requests (407)** to see these entries.
5. The **Wrap URLs** check box is selected by default to display long URLs on multiple lines. Clear the check box if you do not want the URLs in the list to wrap. In this case, they will be displayed on one line.
6. Select **Authentication Type** to see the type of proxy authentication for each user.
7. For **Category Selection**, the **All Categories** check box is selected by default.
    - To select specific categories, clear the check box and click the first category in the list box. Then hold down CTRL and click the additional categories you want to view.
    - To unselect a category, hold down CTRL and click the selected category.
8. Under **Groups and IDs** on the Browse tab, choose groups and IDs by selecting their corresponding check box. To view IDs in a group, click the group name.



Other options include:

- **Expand or collapse groups:** To expand and view group tiers, click the plus icon. To expand or collapse all groups, click the plus or minus icon next to **Groups**.
- **Search for a specific ID:** If you know the ID names you want to filter, you can search for and select them using the **Filter selected Group's IDs** field. Begin typing the ID or name of a user. Users with a matching ID or name will be displayed in the **IDs** box. Select the check boxes for the IDs you want.
- **Check/Uncheck all groups and/or all IDs:** Use the check boxes below the **Groups** and **IDs** boxes to select or unselect all groups and IDs displayed.

The groups and IDs that you have selected will appear on the Select tab.

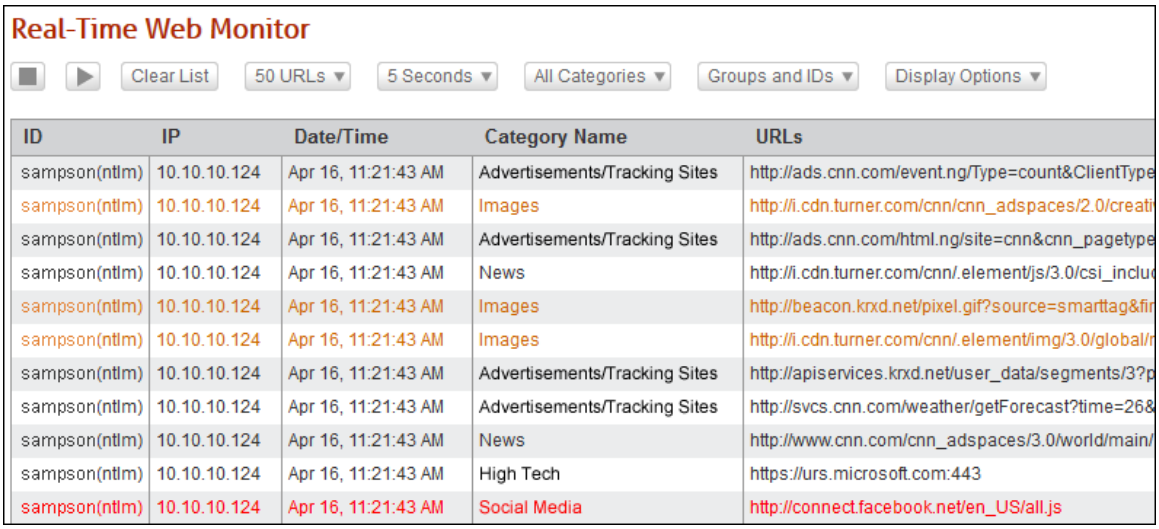


9. To delete a group or ID, click the corresponding red x icon. To delete all groups or IDs, click the **Remove All Groups** or **Remove All IDs** red x icon.
10. On the Select tab, you may enter an ID in the **Search for IDs** field.

- If the ID is not in your groups and IDs but has data, it will be added to your Ungrouped IDs group.
- With authentication enabled, if the ID is an IP address or an IP address with a wildcard, all user names for that IP address will be displayed except any user names in your VIP group. If no user names exist, the IP address will be displayed.
- If the ID contains a wildcard (e.g., *name, name*, or 10.10.10.*), the following occurs:
  - If the wildcard entry exists in your groups and IDs, new users only matching the wildcard entry (e.g., *name) will be displayed in the monitor and will not be added to Ungrouped IDs.
  - If the wildcard entry does not exist in your groups and IDs, new users matching the wildcard entry will not be displayed in the monitor and will be added to Ungrouped IDs.

11. Click **Start Monitor** to run the Real-Time Web Monitor. The Real-Time Web Monitor is displayed and will continue updating.
    - **Stop** and **Pause**/**Resume** icons are available at the top to allow you to stop, pause, or resume updating the list.
      - If you click **Stop**, you are returned to the Real-Time Web Monitor page as when you initially accessed the page.
      - If you do not click **Stop** and navigate away from the Real-Time Web Monitor, the monitor stops running.
    - The **Clear List** button clears the displayed results and restarts the monitor.
    - The remaining buttons at the top of the page allow you to change your settings at any time for the maximum results, update frequency, categories, groups and IDs, 407 challenge requests, URL wrapping, and authentication type. The monitor will continue updating.
      - If no categories are selected, the **All Categories** check box is selected by default.
      - If no groups or IDs are selected, *Enterprise* is selected by default.
12. The monitor displays the following information:
    - In the **ID** column, the default variable hyphen (-) is displayed when authentication is off. "-(ip)" is displayed when authentication is off and authentication type is on. The column also displays the user name making the request with the proxy authentication type used, and "-(407)" if those options were selected.
    - If an IP address is selected from **Groups and IDs**, all user names associated with this address are displayed in the **ID** column.
    - The **IP** column displays the IP address of the computer from which the request originated.
    - The **Date/Time** column is sorted in descending order.
    - The **Category Name** column displays the categories blocked for Web filtering and content type filtering. 407 challenge requests and cookie authentication redirects (http://my.cyblock/auth.php?redir=) are displayed with category "Noncategorized/Other."
    - The **URLs** column displays the URLs of all Web requests (i.e., http and https).
    - Requests that were denied due to Web filtering are displayed in red; those denied due to content type filtering are displayed in orange.

    Below is an example of the Real-Time Web Monitor.



Run a High-Level Summary Report

NOTE: Reporting is not avaliable in Lite version.

High-level reports give summarized information on employee Web use. They give you the information needed to locate problem areas, but do not show the actual URLs visited. The audit detail (or low-level) reports give full URLs.

This section covers how to run a Site Analysis report, one of our recommended reports, but these instructions will work for any high-level report you wish to run. This report depicts the same Web site visits in multiple different ways:

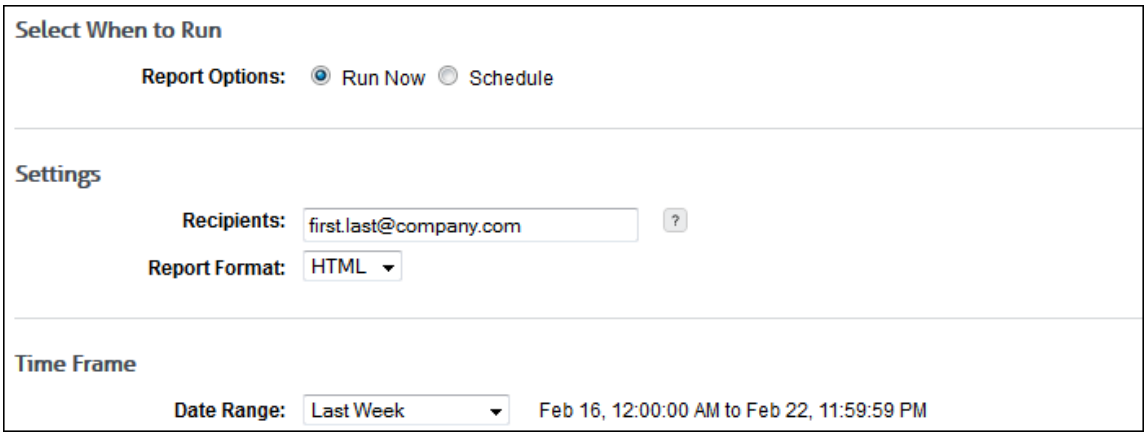
- Total visits by acceptability classification (acceptable, unacceptable, neutral)
- Total visits by content category (Shopping, Pornography, etc.)
- Total visits by group
- Total visits by user
- Total visits by user, per category

NOTE: For descriptions of all high-level reports, see the appendix.

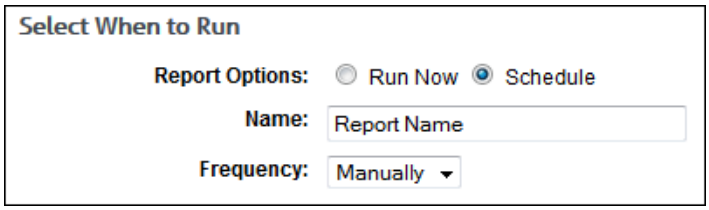
1. Go to **Reports - Manager**. The Report Selection page is displayed if no recently run or scheduled reports exist.

   NOTE: If reports exist, the Manage Reports page is displayed. Click the green plus icon to go to the Report Selection page.

2. Under **Recommended Reports** or **High-Level Summary Reports**, click **Site Analysis**. The Create Report page is displayed.



3. Under **Select When to Run**, for the **Report Options** field, select **Run Now** or **Schedule**.
    - **Run Now** - Use this option if you want to run the report at this time. The report will be sent via e-mail and will be displayed as a recently run report on the Manage Reports page.
    - **Schedule** - Use this option if you want to set up the report to run manually at a later time or schedule the report to run automatically at a specific time.



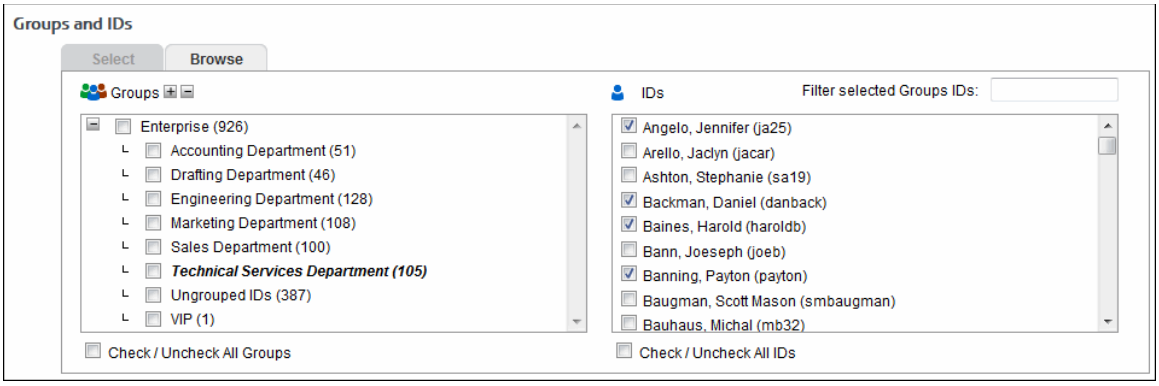
        - In the **Name** field, type an appropriate name for the report. The name limit is 75 characters.
        - In the **Frequency** field, select *Manually* if the report will be run manually at a later time, or select the schedule for the report, that is, *Daily*, *Weekly*, or *Monthly*.
            - If you selected *Daily*, select the specific hour and time of day that you want the report to run daily.
            - If you selected *Weekly*, select the day of the week, and specific hour and time of day that you want the report to run weekly.
            - If you selected *Monthly*, select the day of the month, and specific hour and time of day that you want the report to run monthly.
4. Under **Settings**, the **Recipients** field is populated with your e-mail address by default, that is, the one you logged on with.

    NOTE: If you wish to send the report to multiple e-mail addresses, enter the addresses separated by a comma or semicolon with no spaces. Duplicate addresses are not allowed.
5. In the **Report Format** field, select *HTML* or *PDF*.
6. Under **Time Frame** in the **Date Range** field, select from the following predefined time frames of data: *Yesterday*, *Previous 24 Hours*, *Last 7 Days*, *Last Week*, or *Last Month*, or select *Custom* to set a specific date range.
    - All predefined time frames end at 11:59:59 P.M., except *Previous 24 Hours* which ends one second before the current hour.
    - When scheduling a report, the **Date Range** options are based on the **Frequency** selection, that is, they are less than the frequency. For example, you cannot schedule a report to run daily with a date range of *Last Month*. Select the appropriate date range.

- *Custom* is only available if the **Run Now** option was selected or the **Frequency** field was set to *Manually*.
- The data that is displayed depends on your available log file data and the stored low-level/summary data limits set in your customer account (e.g., 6 months/1 year).
  - The low-level limit applies to data displayed in reports.
  - The summary limit applies to data displayed in Dashboard charts.
- If you selected *Custom*, set a start date/time and stop date/time.
  - The **Start** and **Stop** fields show the previous date range that was selected.
  - Click the **Start** calendar icon to select the start date of the data you want. The calendar shows days up to the previous date range with the first day of that date range selected. The calendar begins on the first date of your log files.

    NOTE: In Internet Explorer 10, if you have log files in only the current year, the drop-down arrow disappears when you click the year field.
  - Click the **Stop** calendar icon to select the stop date of the data you want. The calendar shows days beyond the previous date range. The calendar begins on the start date that you selected.
  - Select the specific hour and time of day for the start and stop dates.

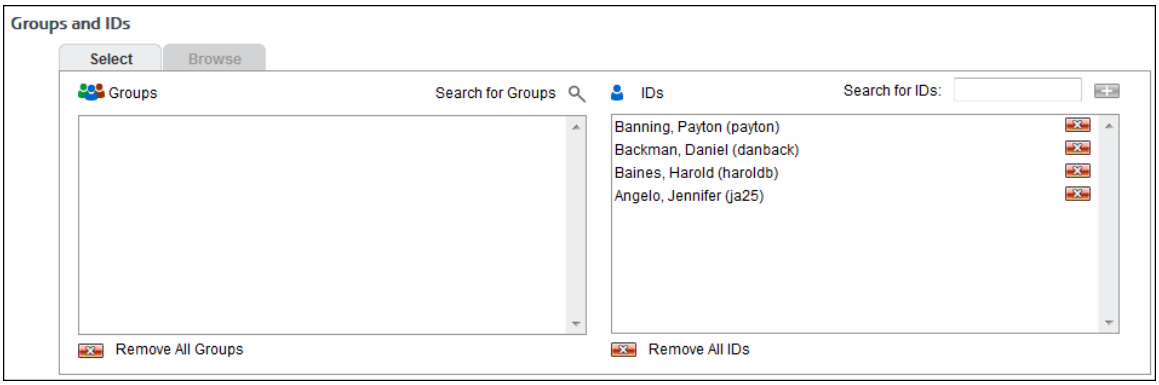
7. Under **Groups and IDs** on the Browse tab, choose groups and IDs by selecting their corresponding check box. To view IDs in a group, click the group name.



Other options include:

- **Expand or collapse groups:** To expand and view group tiers, click the plus icon. To expand or collapse all groups, click the plus or minus icon next to **Groups**.
- **Search for a specific ID:** If you know the ID names you want to filter, you can search for and select them using the **Filter selected Group's IDs** field. Begin typing the ID or name of a user. Users with a matching ID or name will be displayed in the **IDs** box. Select the check boxes for the IDs you want.
- **Check/Uncheck all groups and/or all IDs:** Use the check boxes below the **Groups** and **IDs** boxes to select or unselect all groups and IDs displayed.

The groups and IDs that you have selected will appear on the Select tab.



8. To delete a group or ID, click the corresponding red x icon. To delete all groups or IDs, click the **Remove All Groups** or **Remove All IDs** red x icon.
9. On the Select tab, you may enter an ID in the **Search for IDs** field.
    - If the ID is an IP address or an IP address with a wildcard, all user names for that IP address will be reported on except any user names in your VIP group. If no user names exist, the IP address will be reported on.
    - If the ID contains a wildcard, e.g., *name or name*, users matching the wildcard entry, but not existing in your groups and IDs, will be reported on and not be added to your Ungrouped IDs group.
    - If the ID is not in your groups and IDs but has data, it will be added to your Ungrouped IDs group.
10. Click **Run Now** to create and send the report via e-mail.
11. If you selected the **Schedule** option, the **Schedule and Run** and **Schedule** buttons are available.
    - Click **Schedule and Run** to schedule and send the report.
    - Click **Schedule** to only schedule the report.
12. Click **Back** to return to the previous page.

    Below is an example of a Site Analysis report.

Report Highlights

Description	Information
Data Source	10.10.10.116
Total IDs With Visits	819
Total Visits	85,739
Total Hits	354,363
Total Bytes	2.98 GB
Total Denied Requests	301
Total Denied Hits	595

Top Classifications

Classification	Time Online %	Visits ▼	Visits %
1) Unacceptable	32%	38,569	45%
2) Acceptable	53%	35,716	42%
3) Neutral	14%	11,454	13%
Totals		85,739	

Top Categories

Category	Time Online %	Visits ▼	Visits %
1) Search Engines	18%	9,309	11%
2) News	6%	6,436	8%
3) Shopping	5%	6,367	8%
4) High Tech	8%	4,868	6%
5) Sports	4%	4,790	6%
6) Social Media	3%	4,504	6%
7) Financial	8%	4,502	6%
8) Video Streaming	4%	4,294	5%
9) Games	3%	3,839	5%
10) Education/Reference	5%	3,165	4%

Wavecrest Computing
904 East New Haven Avenue
Melbourne, FL 32901
toll-free: 877-442-9346
voice: 321-953-5351
fax: 321-953-5350

All information subject to change without notice.
© Copyright 2021 Wavecrest Computing
Incorporated. All rights reserved.